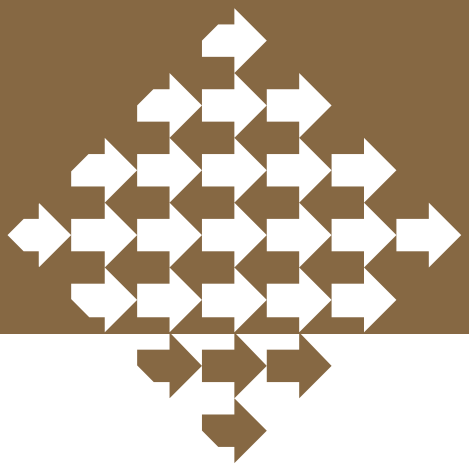


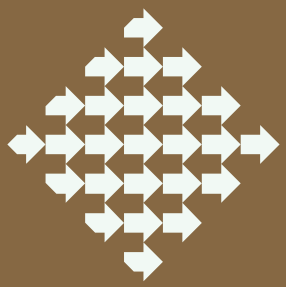
Štiriintrideseta
delavnica o telekomunikacijah

ZAUPANJA VREDEN INTERNET

TRUSTED INTERNET

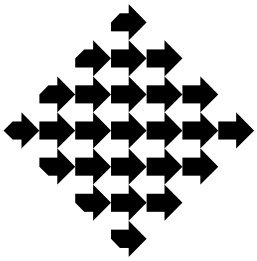
14. in 15. maja 2018

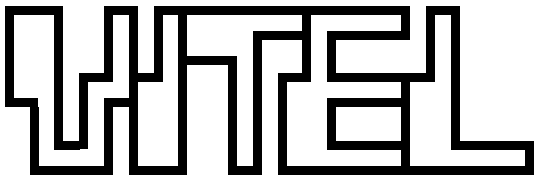
Brdo pri Kranju



Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije

SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE





Štiriintrideseta delavnica o telekomunikacijah

34th Workshop on telecommunications

ZAUPANJA VREDEN INTERNET

TRUSTED INTERNET

ZBORNIK REFERATOV

PROCEEDINGS

14. in 15. maj 2018 Brdo pri Kranju, Slovenija

Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije
Stegne 7
1521 Ljubljana, Slovenija
www.drustvo-sikom.si

34. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

34 Workshop on Telecommunications VITEL

PROCEEDINGS

Vsi referati v tem zborniku so recenzirani.

All papers in this proceedings have been peer reviewed.

Organizirata / *Organised by*: Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije

Pokrovitelj / *Sponsored by:* IEEE Communications Society

Uredila / *Editors*: Tomi Mlinar, Nikolaj Simič

Priprava za tisk / *Prepress:* Tomi Mlinar, Nikolaj Simič

Naslovnica / *Cover design:* Nikolaj Simič, Filip Samo Balan, Aleksander Vreže

Izdajatelj / *Publisher:* Slovensko društvo za elektronske komunikacije

Tisk / *Printing house:* Tiskarna DTP, d. o. o., 2018

Število izvodov / *Copies:* 100

ISSN 1581–6737

Programski in organizacijski odbor delavnice

Programme and Organizing Committee

Programski odbor delavnice

Programme Committee

Tomi Mlinar, predsednik
Ana Robnik
Ivica Kranjčevič
Nikolaj Simič
Janez Keršmanc

Organizacijski odbor delavnice

Organizing Committee

Nikolaj Simič, predsednik
Ivica Kranjčevič
Tomi Mlinar

Zgodovina delavnic o telekomunikacijah VITEL

History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost*, Brdo pri Kranju
2012: 28. *Pametna mesta*, Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju
2015: 31. *Kritična infrastruktura in IKT,* Brdo pri Kranju
2016: 32. *Pametna omrežja informacijske družbe,* Brdo pri Kranju
2017: 33. *Omrežja 5G za digitalno preobrazbo*, Brdo pri Kranju

Zgodovina mednarodnih simpozijev VITEL

History of International Telecommunication Symposium VITEL

1992: *VITEL*, Ljubljana
1994: *Subscriber Access*, Ljubljana
1996: *Broadband Communications Prospects and Applications*, Ljubljana
1998: *Mobility and Convergence Communication Technologies*, Ljubljana
2000: *Technologies and Communication Services for the Online Society*, Ljubljana
2002: *NGN and Beyond*, Portorož
2004: *Next Generation User*, Maribor
2006: *Content and Networking*, Ljubljana
2008: *DVB–T and MPEG4*, Bled
2010: *Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Foreword

Številne razprave, ki so si po svojem bistvu nasprotne, tečejo v dveh smereh: kako zagotoviti, da bo ostala uporaba interneta neodvisna od lastnikov elektronskih omrežij oz. ponudnikov storitev, ki omogočajo dostop do raznovrstnih vsebin na svetovnem spletu, in kako hkrati to omrežje dovolj nadzorovati, da bo možnost zlorab (kraja identitete, finančne mahinacije, lažne novice itd.) kolikor je mogoče zmanjšana. Govorimo torej o nevtralnosti interneta in kibernetski varnosti, z novimi tehnologijami, kot je tehnologija veriženja blokov, pa se bomo vedno pogosteje spraševali tudi o osebni odgovornosti.

Evropski parlament in Evropska komisija sta konec leta 2015 sprejela Uredbo št. 2015/2120, s katero so določili ukrepe za dostop do odprtega interneta. Odprt in nediskriminatoren dostop do interneta naj bi bil gonilo napredka. Nevtralnost interneta pomeni, da morajo ponudniki vsem uporabnikom enakopraven dostop do interneta brez omejevanja ali motenja in to ne glede na prejemnika, pošiljatelja in vsebino. Operaterji lahko omejujejo ali poslabšujejo pretok prometa v izjemnih primerih (npr. za ohranjanje varnosti v omrežju, odpravljanje preobremenitev v omrežju ali za izpolnjevanje nacionalnih aktov ali aktov Unije) in le toliko časa, kot je to nujno potrebno. Kot ugotavlja naš nacionalni regulator AKOS, je za nevtralnost interneta največja grožnja t. i. plačana prednost, ko operaterji elektronskih komunikacij primorajo ponudnike vsebin v plačilo določenega nadomestila, da se izognejo blokiranju ali omejevanju pretoka njihovih podatkov. V avgustu 2017 je AKOS izdal Priporočila za izvajanje Uredbe, kjer med drugim določa, da naj ponudniki dostopa do interneta v pravne akte zapišejo največjo običajno razpoložljivo in minimalno hitrost, ki jo lahko ponudijo svojim uporabnikom. K transparentnosti nudenja storitev bo od julija naprej pripomoglo tudi merilno orodje AKOSTestNet, s katerim bodo lahko uporabniki preverili nekatere parametre omrežja, kot so pritočna in odtočna hitrost, zakasnitev, jakost signala, test prenašanja govora v obliki VoIP, preverjanje razpoložljivosti domenskih strežnikov, blokiranje določenih vrat UDP in TCP ter druge parametre.

Kibernetski prostor je skupek v omrežje povezanih zmogljivih računalnikov, na katerih povezana ali nepovezana programska oprema omogoča raznovrstne storitve in hranjenje obsežnih količin podatkov, ki se dnevno analizirajo in služijo rednim delovnim, proizvodnim in drugim procesom. Obdelani podatki se načeloma uporabljajo v pozitivne namene, mnogokrat pa se tudi zlorabljajo. Zlorabe so raznovrstne, od takšnih, ki nam le upočasnijo vsakdanje delo, do takšnih, ki imajo jasne cilje, kot so npr. premoženjski (prestrezanje gesel in dostopanje do bančnih računov), politični (vplivanje na izid volitev), gospodarski (omejevanje konkurenčnih podjetij, vdori, kraje). Dokler je to omrežje omejeno, je varnost še nekako obvladljiva, ko pa je t. i. intranetno omrežje podjetja povezano v internet, se varnostna grožnja pomnoži. Danes je internet osnovna podlaga za finančno poslovanje (elektronska banka, plačevanje računov ...), e-storitve države (plačevanje davkov, zdravstvene storite, volitve ...), hranjenje in izmenjavo medijskih podatkov (fotografij, video in zvočnih posnetkov), trgovanje z vrednostnimi papirji, valutami in drugimi finančnimi instrumenti, nakupovanje (osnovnih življenjskih dobrin, vstopnic, letalskih vozovnic ...) in druga, povsem vsakdanja opravila. Ker se podjetja zavedajo pomembnosti varne izmenjave podatkov, namenjajo svojim IT-oddelkom vedno več finančnih virov, kriptoznanost pa postaja ena od pomembnejših niš sodobne znanosti. Analitska hiša Gartner predvideva, da bodo podjetja v letu 2018 investirala dobrih 96 milijard dolarjev v varnost na splošno, v prihodnjih letih pa bo področje varnostnih testov, najemanja zunanjih IT-strokovnjakov in obvladovanje informacijske varnosti eden najhitreje rastočih segmentov varnosti.

Ker so tveganja za zlorabe stalno prisotna, je na vseh področjih, tako zasebnem kot poslovnem, pomembna preventiva. Med preventivne ukrepe spadajo dosledno posodabljanje programske opreme, dobri požarni zidovi, uporaba sistemov za preprečevanje vdorov v omrežje, ustrezna protivirusna zaščita, kriptiranje komunikacij, avtentikacija in avtorizacija uporabnikov na več ravneh in nenazadnje dobro izobraženi zaposleni, ki so pogosto prva obrambna linija pred kibernetskimi napadi.

Tehnologija veriženja blokov, ki je danes najbolj znana kot podlaga kriptovalute bitcoin, je ena od oblik novih decentraliziranih tehnologij. Slabosti omenjene tehnologije so: velikanska poraba energije, izjemne obremenitve komunikacijskih omrežij, dolgi časi opravljanja transakcij, varnostne pomanjkljivosti v sami programski kodi in podobno. Prednosti te tehnologije pa so: za zdaj ni posebnih administrativnih omejitev, sega preko državnih meja, ni centralnega upravljanja in nadzora, podatki so zabeleženi na stotinah računalnikov po svetu, možnost zlorab je majhna itd. Pred začetkom uporabe tehnologije veriženja blokov se moramo zavedati, da se ravno z decentralizacijo, ki je bistvo te tehnologije, prenaša odgovornost na posameznike. S klasičnimi institucijami, kot so banke, zavarovalnice in upravne enote, imamo posrednika, ki običajno za denar posreduje med dvema strankama. Odgovornost, da bo transakcija ali pogodba sklenjena, varnost zagotovljena in sledljivost v prihodnosti na voljo obema stranema, je na ramenih te institucije. Z decentraliziranimi tehnologijami pa je vsak uporabnik odgovoren za to, da varno hrani svoj varnostni ključ, si naredi varnostno kopijo, skrbi za delovanje svoje strojne opreme in, kar je najbolj pomembno, ima vso potrebno IT-znanje za delo z decentralizirano tehnologijo.

Znanje IT-tehnologij je vse bolj pomembno za vsakega posameznika posebej, zato ga bo morala država že zelo zgodaj sistemsko vključiti v izobraževalni proces. Bistveno vprašanje, ali smo posamezniki res pripravljeni sprejeti težo odgovornosti za vsa svoja dejanja ter za vso svojo materialno in intelektualno lastnino, še vedno ostaja. Banke, zavarovalnice in javne institucije bodo v novem svetu tehnoloških sprememb in decentralizacije morale korenito spremeniti svojo filozofijo delovanja, če bodo sploh želele obstati in dejansko ponuditi državljanom tisto, za kar so ustanovljene.

V tem zborniku so zajeti prispevki, ki podrobneje obdelujejo področja kibernetski varnosti, nevtralnosti interneta, novo evropsko uredbo o varovanju podatkov, kriptografijo, dobre strani in izzive tehnologije veriženja blokov in druga področja, tesno povezana z omenjenimi.

Brdo pri Kranju, 14. maja 2018

dr. Tomi Mlinar
predsednik programskega odbora

Kazalo prispevkov

Table of contents

14. 5. 2018

NEPROFITNA DRUŽBA – UTOPIJA ALI NUJNOST 11
Sašo Tomažič

GDPR MALO DRUGAČE 17
Igor Osolnik

REGULACIJA KLJUČNIH ELEMENTOV INTERNETA (VARNOST IN ZASEBNOST) 21
Katja Kmet

ZAGOTAVLJANJE VARNOSTI KOMUNIKACIJSKIH OMREŽIJ IN STORITEV 27
Urban Kunc

NADZOR ALI SVOBODA? 33
Tony Štupar, Katja Mohar Bastar

KVANTNI INTERNET 35
Boštjan Batagelj

VARNOST NA PODROČJU DEVOPS – ŽE V FAZI NAČRTOVANJA 41
Mojca Ciglarič

ZAGOTAVLJANJE KIBERNETSKE VARNOSTI 45
Janez Anžič, Rok Peršak

IMPLEMENTACIJA ZAHTEV GDPR V PRAKSI S POSEBNIM POGLEDOM NA ZDRAVSTVENO-MEDICINSKE PODATKE 51
Igor Osolnik, Andrej Orel

15. 5. 2018

THE CASUAL LOOP BETWEEN INFORMATION DISORDER AND TRUST ON THE INTERNET 57
Tanja Pavleska

CAN WE TRUST CRYPTOGRAPHERS? 63
Samed Bajrić

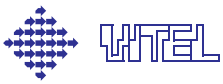
SECURITY IN THE CASE OF A WEBRTC-BASED MEDIA SERVER 67
Valerij Grašič, Ana Robnik, Grega Prešeren

VARNOSTNI VIDIK ISKRATELOVEGA NFV-OBLAKA PRI UPRAVLJANJU IDENTITET IN DOSTOPA 73
Grega Prešeren, Gregor Koritnik, Jože Orehar, Ignac Zupan

DEMISTIFIKACIJA TEHNOLOGIJE VERIŽENJA BLOKOV 77
Tadej Hren

IOT IN VERIGE PODATKOVNIH BLOKOV V SODOBNIH OMREŽJIH IKT 79
Rudolf Sušnik, Peter Zidar, Primož Prevc, Gregor Bobnar

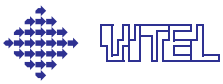
SECURITY RESILIENCE TESTING 83
Mirko Ivančič



PRISPEVKI

ARTICLES

14. 5. 2018



Neprofitna družba – utopija ali nujnost

Sašo Tomažič, Univerza v Ljubljani, Fakulteta za elektrotehniko

Povzetek — V tem prispevku govorim o glavnem vzroku za nastanek ekonomskih kriz in ukrepih, ki bi bili potrebni, da bi se krizam v prihodnje lahko izognili. Je kratek povzetek misli, ki so podrobneje predstavljene v moji knjigi *Imagine – Neprofitna družba: utopija ali nujnost* [1], predvsem v poglavjih, ki govore o pomenu denarja in reformi denarnega sistema. V knjigi ugotavljam, da je glavni vzrok za nastanek kriz v dogmi sodobne ekonomije, da mora kapital prinašati dobiček. Da bi kapital lahko prinašal dobiček, je potrebna eksponentna gospodarska rast, ki je dolgoročno nevzdržna. Dejstvo, da je denar poleg osnovne funkcije menjalnega sredstva pridobil tudi funkcijo kapitala, ki prinaša dobiček, je problem še zaostril, vrhunec pa je problem dosegel, ko so dobile komercialne banke pravico do izdaje novega denarja v obliki kreditov, za katere zaračunavajo obresti, ki jih tudi teoretično ni mogoče pokriti, zato svetovni dolg neprestano narašča [3]. Za stabilnost družbenoekonomskega sistema se bomo morali nujno odpovedati dobičku iz kapitala in preiti v družbenoekonomski sistem, ki sem ga poimenoval »neprofitna družba«. Med prvimi ukrepi, ki vodijo v to smer, je reforma denarnega sistema in načina izdajanja denarja. Digitalizacija družbe tako reformo poenostavlja, vendar kriptovalute, ki so nastale s tem namenom, tega problema žal ne rešujejo.

Ključne besede — ekonomska kriza, finančna kriza, dobiček iz kapitala, denar, obresti, dolg, kriptovaluta, neprofitna družba

Abstract — In this article, I talk about the main cause of economic crisis and the measures that would be necessary to avoid them in the future. It is a summary of the ideas presented in detail in my book *Imagine non-profit society: utopia or necessity* [2], especially in the chapters on money and the reform of the monetary system. In the book, I find that the main reason for the reoccurring crises lies in the dogma of the modern economy that capital must yield profit. For capital to generate profits, exponential economic growth, which is unsustainable in the long run, is required. The fact that the money has obtained the function of profit-yielding capital only exacerbated the problem, which culminated when commercial banks were given the right to issue new money in the form of interest-bearing loans. Because interest cannot be covered, even theoretically, global debt is continuously increasing [3].

To stabilize the socio-economic system, we should renounce the profit from capital and transit to the socio-economic system, which I named "non-profit society." Among the first measures leading in this direction is the reform of the monetary system and the methods of issuing money. The digitization of society simplifies this reform. However, the cryptocurrencies, which were invented for this purpose, do not solve the problem.

Keywords — economic crisis, financial crisis, profit from capital, money, interest, debt, cryptocurrency, non-profit society

I. UVOD

Obdobjem blaginje in visoke gospodarske rasti v kapitalizmu sledijo obdobja kriz in recesije. V zadnjih sto letih je prišlo tako do številčnih kriz, od depresije leta 1920/21 v ZDA in zloma na Wall Streetu leta 1929, ki mu je sledila velika depresija, ki se je končala šele z drugo svetovno vojno, do posojilne in dolžniške krize v osemdesetih letih v ZDA, črnega ponedeljka leta 1987, poka balona .com leta 2000, Irske bančne krize leta 2008 in seveda finančne krize istega leta, katere posledice čutimo še danes.

Prvi je ta problem obdelal J. C. L. de Sismondi [4], ki je kot glavni razlog kriz navajal preveliko proizvodnjo in premajhno potrošnjo, do česar pride predvsem zaradi velikega prepada med revnimi in bogatimi. J. M. Keyens je bil prepričan, da se prosti trg ne uravnava sam in je zato nujno potrebna intervencija države [5]. Predvidel je celo, da bi morali skrajšati delovnik na 15 ur na teden, da bi lahko dosegli polno zaposlitev. Njegova teorija je imela velik vpliv na makroekonomsko politiko po drugi svetovni vojni, v tako imenovani zlati dobi kapitalizma, vse do leta 1979, ko je ponovno začela prevladovati ideja prostega trga (laisez faire).

Ekonomisti so razvili številne makroekonomske modele, od najbolj preprostih teoretičnih, z majhnim naborom spremenljivk, do dinamičnih stohastičnih modelov splošnega ravnovesja, ki slonijo na agentih (gospodinjstva, podjetja, banke ipd.), ki težijo k uresničevanju vsak svojih ciljev in na ta način simulirajo ekonomsko dogajanje v realnem svetu. Različni modeli so prosto dostopni v spletni skladovnici makroekonomskih modelov [6].

Skupno vsem tem modelom je, da so rezultati, ki jih dobimo, odvisni od predpostavk, ki smo jih naredili pri njihovi izgradnji. Te predpostavke so lahko pravilne ali pa tudi napačne, vendar je zelo malo verjetno, da bi bile vse predpostavke pravilne, kot na primer, da bi vsi cilji agentov v modelu ustrezali dejanskim ciljem akterjev v realnem gospodarstvu. Verjetno ravno zato nobeden od teh modelov ni predvidel krize leta 2008.

Večina sodobnih ekonomistov meni, da so krize v ekonomskem sistemu nekaj neizbežnega, kot naravni pojavi, da so del tako imenovanega poslovnega ciklusa oziroma tako imenovane ekonomske fluktuacije. Vendar družbeno-ekonomski sistem ni naravni pojav. Družbenoekonomski sistem smo ustvarili sami in sami vanj vgradili nestabilnost, zato verjamem, da ga lahko tudi sami preoblikujemo in naredimo stabilnega.

V tem prispevku želim pokazati, da je glavni razlog za nestabilnost ekonomskega sistema dobiček iz kapitala, ki v sistem vnaša pozitivno povratno vezavo. Če se želimo izogniti naslednjim, vedno globljim krizam ali celo ekološki katastrofi, se bomo morali odpovedati dobičku iz kapitala in bomo morali preiti v nov družbenoekonomski sistem, ki ga imenujem neprofitna družba. Tak prehod pa ne more biti skokovit, ne more se zgoditi z revolucijo, temveč je za to potrebna evolucija. Zgoditi se mora korak za korakom.

Eden prvih korakov v tej smeri bi lahko bila reforma denarnega sistema, ki sedaj podpira dobiček iz kapitala in celo močno stopnjuje njegove posledice. Digitalizacija družbe, ki je že doslej močno vplivala na denarni sistem, obenem omogoča tudi, da ga je preprosto transformirati v primernejšega, to je v sistem, v katerem denar služi zgolj kot menjalno sredstvo in ne kot kapital, ki prinaša dobiček. Žal kriptovalute, ki naj bi izboljšale denarni sistem, ne dosegajo

tega cilja in imajo v trenutni izvedbi še celo vrsto drugih pomanjkljivosti.

II. DOBIČEK IZ KAPITALA

Kapital mora prinašati dobiček. To je neovrgljiva resnica, aksiom, ki ga ni treba dokazovati, saj je samoumeven, dogma, ki je dana po bogu, zato o njej ne smemo dvomiti. To je sam temelj kapitalizma. Brez tega temelja ekonomija ne more delovati. Brez dobička ni motiva za investicije, brez investicij ni razvoja, brez razvoja ni napredka. Brez investicij začne tudi obstoječa infrastruktura hitro propadati.

To trdijo sodobni ekonomisti. To učijo nadobudne mlade ekonomiste na vseh ekonomskih šolah od Oxforda do Harvarda. To zatrjujejo Nobelovi nagrajenci iz ekonomije. Ali lahko potem temu kdorkoli oporeka?

Oglejmo si sedaj dobiček iz kapitala iz kritične razdalje. Da bi kapital lahko prinašal dobiček, je nujno potrebna tudi stalna gospodarska rast. V sodobni ekonomski znanosti se je nekako uveljavilo splošno prepričanje, da potrebujemo za normalno delovanje ekonomskega sistema (v katerem kapital prinaša dobiček) vsaj 2 % letno rast realnega gospodarstva. To na prvi pogled ni videti prav hitra rast, vendar pa bi moralo pri p % letni rasti gospodarstvo rasti v skladu z izrazom:

$$G(n) = G_0(1 + p/100)^n$$

kjer je z G_0 označen trenutni obseg gospodarstva in z $G(n)$ obseg gospodarstva čez n let. To je eksponentna funkcija. Pri eksponentni funkciji obstaja tako imenovan podvojitveni čas, to je čas, v katerem bi se moral obseg gospodarstva podvojiti. Podvojitveni čas n_p izražen v letih lahko zelo preprosto izračunamo po približnem izrazu:

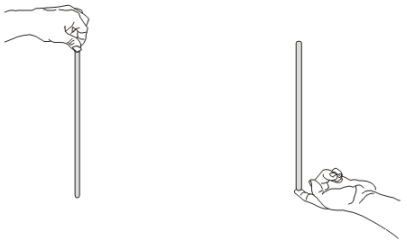
$$n_p = 70/p \text{ let}$$

Podvojitveni čas pri 2 % letni rasti je torej približno 35 let. Vsakih 35 let bi se moral tako obseg gospodarstva podvojiti, kar pomeni, da bi moral biti obseg gospodarstva čez 350 let že 1.024-krat večji, kot je danes in čez 700 let kar 1.048.576-krat večji kot danes. Čez 350 let bi morali potrošiti približno tisočkrat več in čez 700 let kar milijonkrat več, kot potrošimo danes. Verjetno je vsakomur razumljivo, da je to nemogoče. Izraba obnovljivih naravnih virov je namreč omejena in že sedaj smo blizu te meje, če je še nismo presegli. Tudi obremenjenost okolja z odpadki in onesnaženjem je že presegla sprejemljivo mejo. Poleg tega je omejena tudi naša sposobnost potrošnje, saj je že sedaj potrebno stalno umetno ustvarjanje potreb z reklamiranjem vedno novih in novih proizvodov, ki morajo čim prej zastarati, da jih lahko nadomestimo z novimi.

Ker gospodarstvo ne more eksponentno rasti, obenem pa trenutni ekonomski sistem zahteva rast za normalno delovanje, nujno prihaja do kriz, kjer se obseg gospodarske dejavnosti močno zmanjša in vojn, kjer se veliko stvari uniči, kar omogoči ponovno gospodarsko rast.

Dobiček iz kapitala vnaša v ekonomski sistem pozitivno povratno vezavo. Dobiček se prišteje osnovnemu kapitalu, ki zato prinaša še večji dobiček, ki se zopet prišteje osnovnemu kapitalu in tako naprej in tako naprej. Iz teorije sistemov je znano, da je pozitivna povratna vezava nestabilna. Sistemi s pozitivno povratno vezavo slej ko prej dosežejo svojo mejo in izgorijo ali pa usahnejo. Zato v naravi ne najdemo sistemov s pozitivno povratno vezavo.

Neoliberalni ekonomisti so prepričani, da se prosti trg sam uravnava in se sam po sebi postavi v ravnovesno točko, to je točko, v kateri je ponudba enaka povpraševanju. Vendar je to velika zmota. Ker je v sistem vgrajena pozitivna povratna vezava, je ta sistem nujno nestabilen. Res je sicer, da imajo tudi sistemi s pozitivno povratno vezavo lahko ravnovesno točko, vendar je to ravnovesje labilno, kar pomeni, da vsak odmik iz ravnovesne točke pahne sistem v eno ali drugo skrajnost, kot je to za primer palice prikazano na sliki 1.



Slika 1: Stabilno in labilno ravnotežje

Da bi obdržali palico v labilnem ravnovesju (slika 1, desno) je potrebna regulacija, za katero potrebujemo tudi nekaj spretnosti. Na podoben način je potrebna regulacija tudi zato, da se ekonomski sistem obdrži v ravnovesni točki. Taka regulacija predstavlja negativno povratno vezavo, ki je sicer načeloma lahko stabilna. Ker pa prihaja regulacija, ki jo izvajajo vlade s sprejemanjem različnih zakonov, z veliko zakasnitvijo, ekonomski sistem niha. Tudi iz teorije sistemov je namreč znano, da sistemi z zakasnjeno negativno povratno vezavo nihajo, pri čemer je frekvenca nihanja odvisna od zakasnitve v povratni vezavi.

Ker so zakasnitve v regulaciji ekonomskega sistema različne, ta ne niha z neko stalno frekvenco, temveč si obdobja blagostanj in kriz sledijo v na videz naključnih intervalih.

Edini način, da bi sistem naredili stabilen, brez neželenega nihanja, je, da iz sistema odstranimo pozitivno povratno vezavo, kar pomeni, da se moramo odpovedati dobičku iz kapitala in postopoma preiti v neprofitno družbo. Tak prehod ne more biti skokovit, temveč mora potekati postopoma v več korakih, ki so natančneje opisani v [1]. Med prvimi koraki v tej smeri je zagotovo prenova denarnega sistema, ki je na kratko predstavljena v naslednjih dveh razdelkih.

III. DENARNI SISTEM

V svoji osnovi predstavlja denar sredstvo, ki olajšuje menjavo dobrin. Vendar denar že dolgo ni več zgolj menjalno sredstvo, temveč je prevzel tudi funkcijo kapitala, ki prinaša dobiček. Denar se posoja za obresti, ki se prištejejo osnovnemu dolgu. To je tako imenovan obrestno obrestni račun, pri katerem dolg narašča po enaki funkciji, kot smo jo zapisali za eksponentno rast gospodarstva. Pri 5 % obrestni meri se dolg podvoji v 14 letih in bi tako že v 280 letih narasel približno milijon krat.

Res je sicer, da si nihče ne izposodi denarja za 280 let, da bi mu dog narasel milijon krat, vendar pa to v ničemer ne

zmanjšuje problema. V trenutnem denarnem sistemu ustvarjajo nov denar centralne banke in ga za obresti posodijo državam. Poleg denarja, ki ga izdajajo centralne banke, pa so dobile pravico izdajanja denarja tudi komercialne banke. Te izdajajo nov denar v obliki posojil pravnim in fizičnim osebam, seveda ravno tako za obresti. Kar okrog 95 % denarja v obtoku je denar, ki ga ustvarijo komercialne banke.

Ves denar v obtoku torej predstavlja dolg, bodisi dog centralnim ali pa komercialnim bankam. Torej na ves denar v obtoku stalno tečejo obresti. Dolga, ki izvira iz obresti, nikakor ni mogoče poplačati, saj je zaradi obresti celoten dolg vedno večji od celotne količine denarja v obtoku. Da bi bilo mogoče ta dolg poplačati, bi morale banke izdati nov denar, ki pa predstavlja hkrati nov dolg. Doga pač ne moremo poplačati z novim še večjim dolgom. Zato v svetu dolg stalno narašča. Po oceni Mednarodnega denarnega sklada je dolg realnega sektorja finančnemu sektorju ob koncu leta 2016 znašal kar 152 trilijonov dolarjev, kar je 225 % bruto svetovnega proizvoda.

Delno se dolgovi sicer sproti odpisujejo, ko gredo podjetja ali celo države v stečaj, vendar kljub temu dolg stalno narašča, kar slej ko prej pripelje do dolžniške in posledično tudi do finančne in splošne gospodarske krize. Večina sicer meni, da so bile za krizo leta 2008 odgovorne banke in zavarovalnice, ki so izdajale vrednostne papirje, sestavljene iz visoko tveganih hipotekarnih kreditov. Ti so bili ocenjeni z oceno tveganja AAA, ki predstavlja izredno nizko tveganje in jo ima običajno samo denar. Vendar pa pravi vzrok za krize leži mnogo globlje, v samem temelju obstoječega ekonomskega sistema, v dogmi, da mora kapital prinašati dobiček. Neodgovorno ravnaje bank in zavarovalnic je krizo samo zakasnilo. Brez takega ravnanja bi do krize prišlo že mnogo prej, vendar še zdaleč ne bi bila tako globoka.

IV. PRENOVA DENARNEGA SISTEMA

Da bi se izognili dolžniškim krizam, ki jih prinaša obstoječi denarni sistem, bi bila potrebna njegova temeljita prenova. V prvi fazi bi bilo potrebno izvesti tako imenovano seigniorage reformo, ki sta jo predlagala J. Huber in J. Robertson [7]. Seigniorage je francoski izraz za pravico do izdajanja denarja. Za predlagano reformo bi bila potrebna dva ukrepa:

1. Nov denar, ki ga izdajajo centralne banke, ko začne primanjkovati denarja v obtoku, bi moral iti neposredno v državni proračun kot nepovratna sredstva in ne kot posojilo. Vlada bi dala ta denar v obtok, tako da bi ga potrošila in z njim pokrivala del svojih obveznosti.
2. Komercialnim bankam bi morali onemogočiti izdajo kreditov, ki ne bi temeljili na denarju, prejetem od centralne banke. To pomeni, da bi komercialnim bankam preprečili izdajo novega denarja v obliki kreditov, denarja, ki danes predstavlja okrog 95 % vsega denarja v obtoku.

Centralne banke bi se v skladu s sprejeto in javno objavljeno denarno politiko neodvisno od trenutne vlade odločale, koliko novega denarja je treba dati v obtok in kdaj je to potrebno. Vlade ne bi smele imeti nobenega vpliva na te odločitve. Po drugi strani pa centralne banke ne bi smele imeti vpliva na to, kako vlade porabijo ta denar. Vlade bi porabile denar v skladu s svojimi zavezami in prioritetami. Lahko bi ga uporabile za zmanjševanje davkov, za razbremenitev gospodarstva in za povečanje socialne varnosti ali pa bi ga vložile v infrastrukturne projekte. Ta denar bi postal del državnega proračuna in bi ga vlade lahko trošile na enak način, kot trošijo denar, ki ga dobijo v državno blagajno po drugih poteh. Smotrno trošenje tega denarja bi še vedno ostalo odgovornost vlad.

Komercialne banke bi smele posojati samo denar, ki bi ga dejansko imele, to je denar, ki bi ga izdale centralne banke. Posojale bi lahko zgolj svoj lastni denar in tistega, ki bi ga imeli na varčevalnih računih njihovi komitenti. Banke ne bi smele pripisati denarja na nek račun, ne da bi hkrati zmanjšale isti znesek denarja na drugem računu. Tako bi ohranjale skupno količino denarja v obtoku. Povečanje zneska na enem računu, ne da bi se sočasno zmanjšal znesek na drugem računu, bi veljalo za ponarejanje, enakovredno ponarejanju papirnatega denarja.

Taka reforma bi rešila velik del problemov trenutnega monetarnega sistema. Ker denar v obtoku ne bi več predstavljal dolga, na katerega tečejo obresti, dolg ne bi neprestano naraščal, kar bi bistveno zmanjšalo verjetnost dolžniških kriz. Kljub temu pa taka reforma še ne bi odvzela denarju vloge kapitala, ki prinaša dobiček, torej ne bi rešila osnovnega problema obstoječega denarnega sistema.

V. DIGITALIZACIJA DENARJA

Digitalizacija sama po sebi ni niti dobra niti slaba, to je odvisno od tega, v kakšen namen se uporablja. Na podoben način kot ogenj, ki je lahko izredno dober, ko nas ogreje in izredno slab, ko nam zgori hiša.

V denarnem sistemu digitalizacija ni nič novega. Večina poslovanja namreč že sedaj poteka brezgotovinsko. Večina denarja tudi ne obstaja v fizični obliki, temveč so to samo številke v informacijskih sistemih bank. Kašen pa je pomen tega denarja, kako in kdo ga izdaja pa ni več stvar digitalizacije, temveč je stvar politike oziroma splošnega konsenza.

A. Kriptovalute

Ko je leta 2008 Satoshi Nakamoto[1] objavil članek o elektronskem »peer to peer« denarju bitcoin [8], se je začelo obdobje kriptovalut, ki je počasi preraslo v pravo evforijo. Bitcoin naj bi odpravil vse probleme obstoječega denarnega sistema.

Žal bitcoin in druge kriptovalute, na načine, kot se uporabljajo danes, ne odpravljajo osnovnega problema obstoječega denarja, saj mu ne jemljejo funkcije kapitala. Ravno nasprotno; kriptovalute so s časom postale izrazito špekulativno sredstvo, ki se jim vrednost spreminja hitreje in bolj kot kateri drugi valuti. Mnoge deklarirane prednosti kriptovalut pa so se izkazale celo kot njihove slabosti.

Decentralizacija

Decentralizacijo štejejo mnogi za največjo prednost kriptovalut, ki so osnovane na verigi blokov, saj izločajo potrebo po neki centralni avtoriteti ali zaupanja vredni tretji strani, torej tu ni treba nikomur zaupati.

V praksi večina uporabnikov uporablja programsko opremo, ki so jo razvili programerji ustvarjalca posamezne kriptovalute. Sicer gre večinoma res za programe z odprto

[1] Satoshi Nakamoto je psevdonim. Nihče pravzaprav ne ve ali gre tu za eno osebo ali pa je v ozadju neka organizacija.

kodo, vendar ima izredno majhen odstotek uporabnikov dovolj znanja in časa, da bi to kodo lahko preverili. Večina uporabnikov uporablja že prevedene različice programov, za katere ni nobene garancije, da delujejo na enak način kot njihova odprtokodna verzija. Namesto da bi zaupali bankam, morajo v tem primeru uporabniki zaupati programerjem. Ali so ti res vedno zaupanja vredni? Ali so bolj kredibilni kot banke, ki so kljub vsem pomanjkljivostim regulirane in nadzorovane?

Večina uporabnikov kupuje in prodaja kriptovalute preko menjalnic in imajo pri njih tudi svoje elektronske denarnice. Menjalnicam morajo zato zaupati na enak način, kot morajo zaupati bankam.

Varnost

V verigi blokov se transakcije potrjujejo z večino glasov oziroma z večino vloženega dela v obliki računske moči. Veliki rudarji kriptovalut imajo pod svojo kontrolo toliko moči, da so sposobni preglasovati vse druge. Pri nekaterih kriptovalutah so celo podjetja, ki so jih ustvarila, edini rudarji, kar pomeni, da imajo vedno na voljo večino računske moči.

Večina uporabnikov hrani svoje elektronske denarnice na svojih osebnih računalnikih ali pa v menjalnicah. Varnost pred vdori je v obeh primerih bistveno bolj vprašljiva kot pri bankah, ki imajo na tem področji dolgoletne izkušnje in strogo regulacijo. To potrjujejo tudi številni vdori v menjalnice in kraje ogromnih količin kriptovalut.

Omejena končna količina bitcoinov

Količina bitcoinov je sicer res omejena, vendar pa ni omejeno število različni kriptovalut. V zadnjem času smo priča pravi inflaciji novih kriptovalut. Večina teh valut pa deluje na načelu piramidnih shem. Zgodnji vlagatelji služijo na račun poznih vlagateljev.

Hitre in poceni transakcije

Pri kriptovalutah, ki so osnovane na verigi blokov, kot jo je zasnoval Satoshi, se varnost transakcij zagotavlja z dokazom vloženega dela. Potrebno vloženo delo se s časom stalno povečuje, zato je za potrjevanje transakcij potrebna ogromno energije, ki se porablja popolnoma nesmiselno, obenem pa postajajo transakcij vedno dražje, njihovo potrjevanje pa traja vedno dlje. Za potrjevanje enega bloka transakcij v omrežju bitcoin je trenutno potrebno več energije, kot jo porabi povprečno gospodinjstvo v enem dnevu.

Anonimnost

Uporabniki kriptovalut lahko ostajajo anonimni. Na prvi pogled izgleda to zelo dobra in želena lastnost; vse dokler ne pride do zlorab in prevar. Takrat je prevarante zelo težko ujeti. Zato so postale kriptovalute zelo primerne za kriminalne združbe in ilegalno trgovino. To potrjujejo tudi padci vrednosti bitcoina, ki sovpadajo z odkritji in zaprtji ilegalnih tržnic na črnem spletu.

Ireverzibilnost transakcij

Transakcij, ki so potrjene v verigi blokov, ni mogoče več preklicati, kot je mogoče preklicati transakcije, ki jih izvedemo s kreditno kartico ali bančnim nakazilom. To ščiti prodajalca, ker kupec ne more preklicati plačila, ko je enkrat prejel blago, ki ga je kupil. Vendar pa je ostal pri tem kupec popolnoma nezaščiten in nima možnosti preklica, če mu prodajalec ne dobavi blaga, ki ga je kupil, ali pa če je to blago neustrezno. Zaščita kupca se je spremenila v zaščito prodajalca, ki pa je v transakciji običajno močnejša stranka. Poleg tega pa tudi denarja, ki je bil ukraden z vdorom v menjalnico, ni mogoče več vrniti in ta ostane na enem ali več anonimnih računih.

Vidimo lahko, da kriptovalute ne rešujejo problemov, ki so značilni za obstoječ denarni sistem, temveč jih celo poglabljajo. Vendar pa digitalizacija omogoča tudi izvedbo sistema lokalne izmenjave (LETS – Local Exchange Trade System) v katerem nastopa denar izključno kot sredstvo, ki olajšuje izmenjavo dobrin in nima več funkcije kapitala, ki prinaša dobiček.

B. Sistem lokalne izmenjave

V sistemu blagovne menjave ni potrebe po denarju, vendar je taka menjava izredno nepraktična, saj je za izmenjavo blaga za blago potrebna sočasnost in vzajemnost potreb. Ker v taki menjavi denar ne nastopa, tudi ne more prevzeti funkcije kapitala. Problem nesočasnosti v blagovni menjavi je dokaj preprosto rešiti. Če bi na primer kmet rad zamenjal svoj krompir za striženje, vendar krompirja še ni pridelal, striženje pa potrebuje sedaj, lahko frizerju za striženje napiše zadolžnico v protivrednosti striženja. Kasneje, ko kmet pridela svoj krompir, lahko frizer s to zadolžnico pri njem »kupi« krompir v protivrednosti, ki je napisana na zadolžnici.

Zadolžnica v zgornjem primeru igra vlogo denarja. Vendar tega denarja ni ustvarila banka, temveč ga je ustvaril kmet po potrebi, in ko jo je dobil nazaj, jo je uničil in tako ta denar vzel iz obtoka. Če to pogledamo na drug način, vidimo, da se je kmet pri frizerju zadolžil za striženje in potem dolg povrnil s krompirjem. Vendar na ta dolg ne tečejo obresti, saj sta obe strani zainteresirani za izmenjavo. Enkrat nastopi striženje pred krompirjem, drugič pa lahko kmet frizerju »proda« večjo količino krompirja in od frizerja dobi zadolžnico, s katero lahko plačuje striženja v prihodnosti. Pri taki izmenjavi je lahko udeleženo tudi več strank. Frizer lahko potrebuje popravilo pri mehaniku, mehanik potrebuje krompir od kmeta in kmet potrebuje striženje pri frizerju, tako da lahko naredijo krožno izmenjavo.

Z naraščanjem števila strank v izmenjavi in njihovimi različnimi potrebami bi se tak sistem močno zapletel in bi bil s papirnatimi zadolžnicami neizvedljiv. Digitalizacija oziroma uporaba ustreznega informacijskega sistema pa omogoča, da je izvedba takega sistem preprosta tudi pri poljubno velikem številu v menjavah udeleženih strank. V svetu že sedaj deluje več kot petsto sistemov lokalne izmenjave (LETS – Local Exchange Trade System), med katerimi je največja švicarska banka WIR. Oglejmo si sedaj nekoliko podrobneje delovanje LETS.

1. S sistemom opravlja tako imenovana banka LETS. Vendar ta banka ne izdaja novega denarja niti ne posaja denarja. Njena vloga je zgolj vloga notarske službe, ki beleži transakcije. To storitev lahko uporabnikom sistema tudi zaračunava, vendar neodvisno od velikosti transakcij. Lahko zaračuna članstvo ali pa število transakcij.
2. V sistemu lahko sodelujejo zgolj člani. Ti so lahko fizične ali pravne osebe.
3. Ker gre za sistem izmenjave, ima vsak v tem sistemu dvojno vlogo. V posamezni transakciji lahko nastopa kot kupec ali kot prodajalec. Člani ne morejo biti samo kupci ali samo prodajalci.

4. Vsak član ima v sistemu svoj račun. Sredstva na računu se vodijo v lokalni valuti sistema. Lokalna valuta ima svoje ime in oznako koz na primer WIR frank (CHW) v banki WIR.
5. Iz praktičnih razlogov je kupna vrednost enote lokalne valute prilagojena kupni vrednosti enote denarja, ki ga izdaja centralna banka (npr. EUR, USD, CHF, ipd.).
6. Ko uporabnik odpre račun, je njegov račun prazen. Stanje na računu je enako 0.
7. Pri nakupu blaga ali storitve se protivrednost lokalne valute prenese z računa kupca na račun prodajalca. Stanje na računu kupca se za ustrezen znesek zmanjša, hkrati pa se za isti znesek poveča stanje na računu prodajalca.
8. Stanje na računu je lahko pozitivno ali negativno. Negativno stanje pomeni dolg, pozitivno stanje pa dobropis (zadolžnice kupcev), ki jih ima prodajalec.
9. Vsota vsega denarja na vseh računih v sistemu je vedno enaka 0, saj se pri vsaki transakciji znesek, ki se na nekem računu odšteje od stanja, prišteje stanju na nekem drugem računu.
10. Poslovanje v tem sistemu je izključno brezgotovinsko. Poteka lahko na osnovi nakazil preko spletnega bančništva ali na osnovi posebnih plačilnih kartic.

Na LETS lahko gledamo kot na sistem organizirane menjave ali pa kot na sistem vzajemnega kreditiranja. Člani, ki imajo na svojem računu pozitivno stanje, kreditirajo tiste, ki imajo na računu negativno stanje. Sam sistem zgolj beleži trenutno stanje kreditov. Vzajemni krediti so brezobrestni. Vsak član sistema lahko nekaj časa nastopa kot kreditojemalec (kadar ima na računu negativno stanje) in nekaj časa kot kreditodajalec (kadar ima na računu pozitivno stanje). Na ta način vsakdo v sistemu ustvarja svoj denar po potrebi in za ustvarjanje denarja niso več zadolžene banke, ki s posojanjem denarja, ki ga ustvarjajo iz nič, kujejo ogromne neupravičene dobičke.

Denarna politika v takem sistemu je izjemno preprosta. Izvaja se preko dveh omejitev, to je z omejitvijo negativnega stanja na računih, kar preprečuje, da bi se ljudje pretirano zadolžili in omejitvijo pozitivnega stanja, kar preprečuje, da bi se začel denar kopičiti na enem mestu in bi na ta način prišlo do pomanjkanja denarja v obtoku.

Prednost LETS je tudi v tem, da ga je možno uvesti lokalno, kot komplementaren sistem in zato ni treba takoj spreminjati celotnega globalnega denarnega sistema. Lahko pa se kot komplementarna valuta uvede tudi na nacionalni ali celo na meddržavni ravni. Že v bivši Jugoslaviji je za izmenjavo z bivšo Sovjetsko zvezo na podoben način deloval klirinški dolar.

Samo uvajanje sistema na nacionalni ravni bi bilo izredno preprosto, saj že trenutno obstaja celotna infrastruktura, ki je potrebna za njegovo delovanje. Plačevanje v LETS se po tehnični plati v ničemer ne razlikuje od poslovanja z bančnimi nakazili in kreditnimi karticami. Uvajanje takega sistema je torej zgolj vprašanje politične volje.

V takem sistemu, če je uveden na nacionalnem nivoju, je tudi pobiranje davkov izredno preprosto in popolnoma transparentno. Denarja namreč tu ni mogoče skriti v davčne oaze, ali pa se izogniti davku z gotovinskimi plačili. V takem sistemu je primernejši prometni davek, ki se obračuna na vsako transakcijo, kot pa davek na dodano vrednost, ki se obračunava sedaj.

V Švici z banko WIR poslujejo predvsem mala in srednje velika podjetja. Ravno to jim je omogočilo, da so brez večjih težav prebrodila razne finančne krize. V času finančnih kriz je poslovanje s franki WIR v Švici naraslo iz običajnih približno 5 % na skoraj 15 % celotnega prometa.

VI. ZAKLJUČEK

Ugotovili smo, da je glavni razlog za nastanek ekonomskih kriz v dobičku iz kapitala, ki je vgrajen v sam temelj kapitalizma. Dobiček iz kapitala vnaša v sistem pozitivno povratno vezavo, ki dela sistem nestabilen. Občasno ravnovesje sistema je labilno, zato je potrebna stalna regulacija in prosti trg ne more delovati.

Izdajanje novega denarja v obliki posojil in posojanje za obresti sta dva mehanizma, ki omogočata ustvarjanje dobičkov in močno povečujeta vliv pozitivne povratne vezave. Za prehod v neprofitno družbo bi bila zato nujno potrebna reformna denarnega sistema. Kriptovalute, ki so obetale pozitivno spremembo na tem področju, niso prava rešitev. Izdaja komplementarne valute v obliki LETS bi lahko močno ublažila negativne učinke pozitivne povratne vezave, ki jo ustvarja dobiček iz kapitala, kar bi predstavljalo korak nasproti pravičnejši in stabilnejši družbi.

Upam lahko, da bo kdo od vplivnih politikov prebral ta prispevek in se zavzel za pozitivne spremembe. Tehnološke rešitve namreč obstajajo, potrebna je zgolj politična volja. Morda pa celo neka od strank vključi take spremembe v svoj program v predvolilni kampanji. Nujno, vendar tudi utopično.

LITERATURA

[1] Sašo Tomažič, Imagine – Neprofitna družba: utopija ali nujnost, Createspace 2017, elektronska verzija Smashwords 2017, https://www.smashwords.com/books/view/715792

[2] Sašo Tomažič, Imagine – Non-Profit Society: Utopia or Necessity, Createspace 2017, elektronska verzija Smashwords 2017, https://www.smashwords.com/books/view/714355

[3] Current global public debt, https://debtclock.s3.amazonaws.com/index.html, dostopano c.

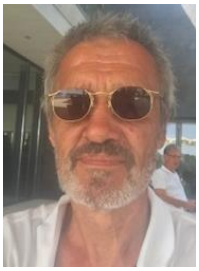
[4] Sismondi, J. C. L., Nouveaux principes d'économie politique ou de la richesse dans ses rapports avec population, seconde edition, Delaunay, Paris, 1827.

[5] Keynes, J. M., The General Theory of Employment, Interest, and Money, Prometheus Books 1997 (originalno objavljeno 1936).

[6] The Macroeconomic Model Data Base, http://www.macromodelbase.com/, dostopano 30.4. 2018.

[7] Huber, J. Robertson, J., Creating new money. A monetary reform for the information age. New Economics Foundation. London, http://www.jamesrobertson.com/book/creatingnewmoney.pdf

[8] Nakamoto, S., A Peer-to-Peer Electronic Cash System, bitcoin.org 2008, https://bitcoin.org/bitcoin.pdf



Sašo Tomažič je redni profesor na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer predava oziroma je predaval predmete iz področja elektronskih vezij, telekomunikacij, informacijskih sistemov in obdelave signalov. Je dolgoletni predstojnik Katedre za telekomunikacije in predstojnik laboratorija za informacijske tehnologije. V zadnjem času se v veliki meri posveča tudi problematiki obstoječega družbenoekonomskega sistema in ukrepom, ki bi bili potrebni za prehod v stabilnejšo, ekološko vzdržno in pravično družbo. Na to temo je imel od leta 2006 večje število vabljenih predavanj doma in v tujini.

GDPR malo drugače

Igor Osolnik, Marand d.o.o., Ljubljana

Povzetek — Ta članek opisuje ozadje sprejema Splošne uredbe o varstvu osebnih podatkov (GDPR) – Uredba EU 2016/679, predvsem namene, ki so vodili odločevalce k sprejemu te uredbe in ključne novosti uredbe.

Ključne besede — GDPR, Uredba, varstvo osebnih podatkov.

Abstract — This article explains background for the adoption of the General Data Protection Regulation (GDPR)-EU Regulation 2016/679, focusing on purposes for adoption and new key elements.

Keywords — GDPR**,** data protection, 25th May, 2018

I. UVOD

Ozadje sprejema Splošne uredbe o varstvu osebnih podatkov (v nadaljevanju uredbe GDPR): gre za eno izmed sistemskih uredb Evropske Unije, ki zaokrožuje pred več leti predvideno tako imenovano evropsko digitalno agendo, ki poleg varstva osebnih podatkov vključuje še (vsaj):

- področje elektronskega podpisovanja (uredba eIDAS),
- uvedbo enotnih vseevropskih e-računov,
- deregulacijo in liberalizacijo elektronskih plačilnih storitev in sistemov (PSD-2) ter
- novejše, vendar ohlapno urejanje pravic intelektualne lastnine.

Evropska komisija je pred leti zaznala izrazit konkurenčni upad evropskih ponudnikov IKT storitev na svetovnem trgu. Spomnimo se samo usode Nokie (za transformacijo iz evropskega paradnega konja in enega največjih svetovnih proizvajalcev naprednih telefonov v marginaliziranega grdega račka IKT industrije ni bilo potrebno veliko časa). Z zadevno regulativo so skušali na podlagi idej in vizije Evropske komisije postaviti temelje enotnega digitalnega trga IKT storitev v evropskem prostoru in na tak način prispevati k dvigu konkurenčnosti evropskih IKT družb na globalnem trgu. Istočasno je poskušala Evropska komisija s sprejetjem takšne regulative odgovoriti na izzive enormnega povečanja podatkov v obtoku, vsakodnevne uporabe mobilnih telefonov in naprav, množične uporabe interneta in eksplozivne rasti števila uporabnikov socialnih omrežij. Direktivo o varstvu osebnih podatkov 95/46/ES, sprejeto leta 1995, je že v času sprejemanja Evropske digitalne agende temeljito povozil čas – samo za primerjavo in zgodovinski vpogled v takratno stanje tehnike: leta 1995 je manj kot 1 % Evropejcev uporabljalo internet (vir:[1]) in do prvih okornih »pametnih« telefonov, množičneje uporabljenih v določeni državi – na Japonskem – je moral preteči še cel olimpijski ciklus 4 let (vir:[2]).

II. IZVEDBA

Vseh naštetih področij z izjemo področja plačilnih storitev in sistemov (PSD-2), kjer je bila sprejeta direktiva, se je Evropska unija lotila s sprejetjem uredb. Direktiva in uredba se med seboj ločita v eni ključni lastnosti: sprejeta uredba velja neposredno in je zavezujoča v vseh pravnih redih držav članic Evropske Unije, direktiva pa zahteva implementacijo v pravni red države s sprejemom zakona po predvideni nacionalni parlamentarni proceduri. Sam nacionalni zakon lahko tudi precej odstopa od določil direktive. Že iz same razlike med direktivo in uredbo je bil jasno razviden namen evropskih odločevalcev pri tematiki urejanja varovanja osebnih podatkov: spraviti sicer heterogeno zakonodajo vseh držav članic Evropske Unije, ne oziraje se na politične, geografske in zgodovinske posebnosti posameznih članic, na skupni imenovalec in zagotoviti enotno uporabo pravil o varstvu osebnih podatkov – od Portugalske do Poljske in od Švedske do Grčije.

S sprejetjem uredbe GDPR je Evropski Uniji po sicer dolgotrajnem postopku uspel veliki met. Uredba je bila sprejeta 27. 4. 2016 in je pričela veljati 20. dan po objavi v Uradnem listu Evropske unije, **uporablja pa se od 25. 5. 2018**. Kar dve leti trajajoče prehodno obdobje (od veljavnosti do praktične uporabe uredbe), zgovorno dokazuje, da so do sprejema uredbe spoštovanje varstva osebnih podatkov v različnih evropskih državah v Evropski uniji zelo različno dojemali in temu primerno posvečali pozornost. Kakorkoli že vseobsežna uredba z rekordnim številom amandmajev je uredila:

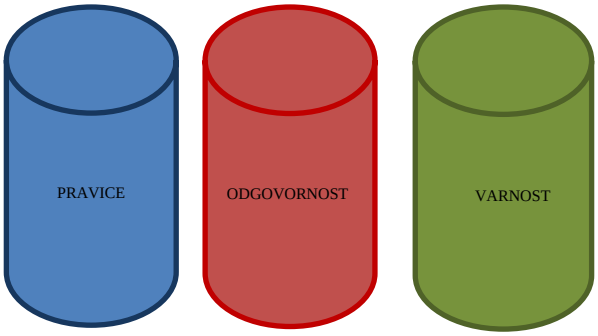
- tako imenovane vse navezne okoliščine, glede veljavnosti, saj se uredba aplicira tako na pravne osebe (v vlogi upravljavca ali obdelovalca osebnih podatkov), ki imajo sedež znotraj Evropske Unije ali kadar le-te nudijo blago ali storitve državljanom Evropske Unije;
- enotna in harmonizirana pravila za celotno Evropsko Unijo,
- enoten nadzor neodvisnih nadzornih organov in skupno ukrepanje nadzornih organov ter medsebojno sodelovanje,

[1] http://europa.eu/rapid/press-release_IP-12-46_en.htm.
[2] https://en.wikipedia.org/wiki/Smartphone

– enotno višino glob in ostalih sankcij za kršitev.

Trije vsebinski stebri GDPRGDPR temelji na treh vsebinsko zaokroženih stebrih:

a. pravice posameznika;
b. odgovornost upravljavca ali obdelovalca osebnih podatkov;
c. varnost osebnih podatkov.



A. *Pravice posameznika*

Poleg do sedaj že znanih in uveljavljenih pravic posameznikov, ki so izhajali iz direktive 95/46/ES in slovenskega zakona o varstvu osebnih podatkov (ZVOP-1) kot so: pravica dostopa posameznika do osebnih podatkov na katerega se nanašajo osebni podatki, pravica do popravka netočnih podatkov, pravica do ugovora…, GDPR zagotavlja še dve novi pravici in sicer:

– pravica do pozabe, kar dejansko pomeni izbris vseh podatkov, vezanih na posameznika,
– pravica do prenosljivosti podatkov.

Namen pravice do pozabe je jasen: varovanje pravice posameznika do zasebnosti in možnost popolnega izbrisa morebitnih neprijetnih vsebin ali okoliščin, vezanih na posameznika. Le-te se običajno nenadzorovano razširjajo predvsem prek interneta in bi lahko posameznika spremljale skozi daljše obdobje in tako bistveno vplivalo na njegovo pravico do zasebnosti. Tovrstno pravico je na podlagi tožbe posameznika že pred veljavnostjo uredbe zagotavljalo tudi Evropsko sodišče za človekove pravice, sedaj pa je tudi izrecno zapisana in zakonsko urejena.

Pravica do prenosljivosti podatkov je odgovor snovalcev uredbe GDPR na množično širjenje in uporabo internetnih socialnih omrežij. Namen je bil omogočiti posamezniku enostaven in brezplačen prenos vseh svojih podatkov, oziroma podatkov, ki jih poseduje upravljavec v »strukturirani, splošno uporabljani in strojno berljivi obliki« od enega ponudnika k drugemu. S tovrstno pravico so želeli preprečiti odvisnost posameznika od enega samega (največjega) ponudnika socialnih omrežij. Pri pravici do prenosljivosti podatkov se sedaj predvsem trgovcem, ki so leta oblikovali in investirali v programe za nagrajevanje zvestobe svojih kupcev (kartice, promocije, kuponi za popuste, nagradne igre…), poraja vprašanje, na kakšen način jo omogočiti v praksi: ali zagotoviti vse podatke, ki so jih pridobili o posamezniku (vrsta nakupa, vrednost, frekvenca nakupa, nakupovalne navade…), ali le tiste, ki jim jih je posredoval posameznik sam. Trgovcem je namreč jasno, da bi zahtevi posameznika po prenosu podatkov v veliki večini primerov sledil prenos le-teh k njihovi neposredni konkurenci.

Ob tej dilemi se je treba jasno zavedati, da pravica do varstva osebnih podatkov ni absolutna pravica, ampak jo je vedno treba tehtati in presojati tudi skozi očala pravic drugih posameznikov in zakonitih/legitimnih interesov gospodarskih družb, organizacij in državnih organov.

B. *Odgovornost upravljavca ali obdelovalca osebnih podatkov*

Tu je odgovornost mišljena v najširšem pomenu te besede in sicer kot način zagotavljanja vsesplošne transparentnosti obdelav osebnih podatkov posameznikov in zagotavljanja verodostojnosti upravljavca ali obdelovalca osebnih podatkov. Vsaka obdelava osebnih podatkov mora biti zakonita, poštena in pregledna: vse informacije in sporočila, ki se nanašajo na obdelavo osebnih podatkov, morajo biti posamezniku lahko dostopne in razumljive ter izražene v jasnem in preprostem jeziku. Osebni podatki morajo biti zbrani za določen in izrecen ter vnaprej znan namen in se ne smejo nadalje obdelovati na način, ki ni združljiv s prvotnim namenom. Obdelovati se smejo samo osebni podatki, ki so dejansko potrebni za dosego namena – najmanjši obseg podatkov (minimizacija obdelave osebnih podatkov). Osebni podatki, ki se obdelujejo, morajo biti točni, zato jih je treba posodabljati in se lahko obdelujejo (kar vključuje tudi hrambo) samo tako dolgo, kot je potrebno za dosego namena, za katerega so bili pridobljeni. Osebne podatke je treba obdelovati na način, ki zagotavlja ustrezno varnost in zaupnost osebnih podatkov, ki vključuje tudi ukrepe za preprečitev nedovoljenega dostopa do osebnih podatkov ali nepooblaščene uporabe osebnih podatkov in opreme za obdelavo.

V okviru odgovornosti v širšem smislu je v vsakem konkretnem primeru treba natančno opredeliti tudi vlogo upravljalca osebnih podatkov in obdelovalca osebnih podatkov, da ustreza vsakokratnemu dejanskemu stanju. Opredelitev vlog in predvsem razmejitev odgovornosti med upravljalcem in obdelovalcem, je treba urediti pisno – s pogodbo (običajno s pogodbo o obdelavi osebnih podatkov). Tovrstna pogodba med upravljavcem in obdelovalcem naj bi urejala vsaj še naslednja področja njunega medsebojnega sodelovanja: vsebino in trajanje obdelave, naravo in namen obdelave, vrsto osebnih podatkov in kategorije posameznikov, na katere se nanašajo osebni podatki.

C. *Varnost osebnih podatkov:*

V zvezi z obdelavo osebnih podatkov je treba sprejeti ustrezne tehnične in organizacijske ukrepe, da bi se zagotovila izpolnitev zahtev iz uredbe GDPR. Kaj uredba razume pod terminom tehnično organizacijski ukrepi:

– Psevdonimizacija osebnih podatkov,
– Kriptiranje osebnih podatkov,
– Ukrepi, ki zagotavljajo zmožnost zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo (npr. zagotavljanje dostopov do informacijskih sistemov, ki so možni samo z uporabo uporabniškega imena in gesla in tako omogočajo zaupnost in sledljivost dostopov),
– Ukrepi, ki zagotavljajo zmožnost pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru

fizičnega ali tehničnega incidenta (npr. izvedba varnostnih kopiranj in zmožnost obnove podatkov, …),
– Postopki rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave (npr. posodabljanje sistemov z varnostnimi popravki, protivirusna zaščita e-poštnih rešitev, pametna požarna pregrada z zaščito dostopa, občasna izvedba zunanjih penetracijskih testov in testiranje odpornosti informacijskih sistemov).

Vsekakor je za vsak subjekt lahko dobra osnova za zagotavljanje primerne stopnje varnostnih standardov imetništvo certifikata ISO 27001.

Kako lahko subjekti sicer dokazujejo izpolnjevanje zahtev uredbe GDPR po izvedbi ustreznih tehnično organizacijskih ukrepov in s tem posledično primernosti zagotavljanja varnosti podatkov? Najlažje to storijo s pristopom k tako imenovanem kodeksu ravnanj ali z izvajanjem odobrenega mehanizma potrjevanja.

Namen kodeksov ravnanj je pravilna uporaba uredbe GDPR ob upoštevanju posebnih značilnostih in specifičnega delovanja posameznih sektorjev. Kodeks ravnanj pripravijo cehovska združenja upravljavcev ali obdelovalcev osebnih podatkov, potrdi pa ga nadzorni organ, če oceni, da kodeks zagotavlja zadostne in ustrezne zaščitne ukrepe.

Odobreni mehanizem potrjevanja pa pomeni pridobivanje pečatov in označb (beri: certificiranje), da so dejanja obdelave izvajana s strani upravljavcev in obdelovalcev osebnih podatkov v skladu z uredbo GDPR. Tovrstno potrjevanje je prostovoljno in ne odvezuje ali zmanjšuje odgovornosti upravljavca ali obdelovalca za skladnost z uredbo GDPR, vendar pa dokazuje določeno (visoko) mero skrbnosti upravljavca ali obdelovalca. Potrdilo izda praviloma nadzorni organ za obdobje treh let, po preteku zadevnega obdobja pa ga je potrebno za enako obdobje podaljšati.

Zaenkrat mi ni znan noben primer, da bi bil kakšen izmed kodeksov ravnanj že sprejet ali pa da bi odobreni mehanizem potrjevanja že zaživel v praksi, čeprav je povpraševanje na trgu zelo veliko.

III. ZAKLJUČEK

Vezano na uredbo GDPR in datum njene uporabe v praksi, ki se nezadržno bliža in zato pri podjetjih v glavnem poraja nelagodje, saj jo velika večina gospodarskih družb in organizacij občuti predvsem kot dodatno (birokratsko) delo, je dobro imeti na umu, da so bili osnovni nameni snovalcev uredbe dobrohotni, da gre za občutljivo tematiko, ki zadeva skoraj slehernega posameznika in da sta od veljavnosti uredbe pa do njene uporabe pretekli celi dve leti. Verjamem, da tudi, če bi bilo to obdobje še daljše, to ne bi bistveno vplivalo na splošno percepcijo o (ne)potrebnosti nove uredbe.

Kakorkoli že, 25. 5. je pred vrati. In zagotovo bo to lep dan: če že ne iz razlogov nostalgičnih spominov (bivši dan mladosti), pa zato, ker je petek. In v petek je vse lažje, tudi soočenje in življenje z novo uredbo.

Vir za sliko: https://www.finance.si/8861399

ZAHVALE

Hvala Slovenskemu društvu za elektronske komunikacije, da so me kot izrazitega družboslovca povabili k sodelovanju na delavnici in mojemu delodajalcu Marand d.o.o., ki je tovrstno sodelovanje omogočil.

LITERATURA

[1] Priročnik udeleženca »Pooblaščena oseba za varstvo osebnih podatkov (DPO) GDPR, DPO Seminar«,

Igor Osolnik je diplomiral na Pravni Fakulteti v Ljubljani leta 1998, leta 2003 pa je opravil še državni pravniški izpit. Vseh do sedanjih 20 let delovne dobe je preživel kot pravnik v različnih gospodarskih družbah: Energoplan d.d., BTC d.d., UniCredit Banka Slovenija d.d. (prej Bank Austria Creditanstalt), Halcom d.d. in Marand d.o.o. Je tudi občasni predavatelj na Združenju Bank Slovenije.

Regulacija ključnih elementov interneta (nevtralnost in zasebnost)

Katja Kmet, Agencija za komunikacijska omrežja in storitve RS

Povzetek — Članek obravnava pregled evropske in slovenske zakonodaje na področju internetne nevtralnosti in novi predlog normativne ureditve varovanja zasebnosti v elektronskih komunikacijah.

Ključne besede —nevtralnost, Uredba (TSM), Smernice BEREC, ZEKom-1, ePrivacy

Abstract — The article deals with a review of European and Slovenian legislation in the field of Internet neutrality and a new proposal for a normative regulation of privacy protection in electronic communications.

Keywords — net neutrality, Net neutrality Regulation, BEREC Guidelines, ZEKom-1, ePrivacy

I. UVOD

Dve leti je v veljavi UREDBA (EU) 2015/2120 EVROPSKEGA PARLAMENTA IN SVETA z dne 25. novembra 2015 o določitvi ukrepov v zvezi z dostopom do odprtega interneta (v nadaljevanju: Uredba). In kaj je prinesla novega v pravno ureditev? Slovenija je bila ena izmed dveh članic Evropske Unije, ki je nevtralnosti interneta uzakonila že pred sprejemom Uredbe. Zakon o elektronskih komunikacijah (v nadaljevanju: ZEKom-1) iz decembra leta 2012 je ureditev povzel po takrat še predlogu Direktive, ki je tekom postopka sprejemanja postala Uredba, torej neposredno uporabljiva v vseh državah članicah.

Uredba želi vsakemu Evropejcu zagotoviti možnost dostopa do odprtega interneta, vsem ponudnikom vsebin in storitev pa ustvariti okoliščine v katerih bodo lahko zagotavljali svoje storitve prek visokokakovostnega odprtega interneta. V skladu z Uredbo v EU ni dovoljeno blokiranje, upočasnjevanje in diskriminiranje internetnega prometa s strani ponudnikov internetnih storitev (ISP), razen v treh predvidenih izjemah: skladnost s pravnimi obveznostmi, zagotavljanje celovitosti omrežja, upravljanje prometa v primeru začasno preobremenjenega omrežja ali v izjemnih razmerah. Zakaj sploh bi ponudniki internetnih storitev želeli vplivati na internetne podatke in njihov pretok v omrežju? Razlogov je veliko, med vidnejši so dobiček, drugi lastni interesi, nenaklonjenost določenim političnim opcijam, vplivanje na javno mnenje, in podobno. Želeli bi blokirati aplikacije, ki konkurirajo njihovim lastnim ali povečati svoj dobiček, tako da prisilijo ponudnike storitev ali ustvarjalce vsebin, da plačajo več, da bi se izognili blokiranju ali upočasnitvi njihovih podatkov. Ravno slednja, t.i. plačana prioritizacija (»paid prioritization«) je za odprt, nevtralen internet najnevarnejša.

Cilj Uredbe so skupna pravila za zaščito enake in nediskriminatorne obravnave prometa pri zagotavljanju storitev dostopa do interneta ter s tem povezanih pravic končnih uporabnikov in zaščita končnih uporabnikov ter zagotavljanje neprekinjenega delovanja internetnega ekosistema kot gonilo inovacij. Uredba EU o odprtem internetu daje končnim uporabnikom neposredno pravico do dostopa in distribucije zakonitih vsebin in storitev po svoji izbiri, prek svoje storitve dostopa do interneta.

II. PREGLED DOLOČIL UREDBE (EU) 2015/2120 EVROPSKEGA PARLAMENTA IN SVETA Z DNE 25. NOVEMBRA 2015 O DOLOČITVI UKREPOV V ZVEZI Z DOSTOPOM DO ODPRTEGA INTERNETA

Če se najprej osredotočimo na varovanje pravic končnih uporabnikov, ki so v celotnem internetnem ekosistemu najšibkejši člen. Uredba jim za uveljavljanje svojih pravic za dostop do informacij in vsebin ter njihovega razširjanja in do uporabe ter zagotavljanja aplikacij in storitev po svoji izbiri daje možnost sklepanja dogovorov s ponudniki storitev dostopa do interneta v zvezi s tarifami za določeno količino podatkov in podatkovne hitrosti storitve dostopa do interneta. Hkrati pa prepoveduje kakršne koli poslovne prakse ponudnikov storitev dostopa do interneta, ki bi omejevale uveljavljanje teh pravic in bi na ta način zaobšle določbe Uredbe. Takšni dogovori lahko vključujejo nekatere značilnosti storitve dostopa do interneta, kot so cena, količina podatkov ali podatkovna hitrost, nikakor pa ne smejo omejevati uporabnikove pravice do uporabe odprtega interneta. V praksi to pomeni, da uporabnik lahko sklepa pogodbe za različne hitrosti dostopa do interneta, ponudnik pa mu ne sme ponujati storitve, ki bi na primer vključevala samo del interneta (blokiranje posameznih spletnih strani na ravni omrežja).

Ponudniki storitev dostopa do interneta pri zagotavljanju storitev dostopa do interneta morajo obravnavati ves promet enako, brez diskriminacije, omejevanja ali motenja ter ne glede na pošiljatelja in prejemnika, vsebino, do katere se dostopa ali ki se razširja, aplikacije ali storitve, ki se uporabljajo oziroma zagotavljajo, ali terminalsko opremo, ki se pri tem uporablja. To pomeni, da je prednostna obravnava prometa posameznih vsebin v okviru storitve dostopa do interneta prepovedana. Hkrati enako obravnavanje dovoljuje razumno vsakodnevno upravljanje prometa v skladu s objektivno utemeljenimi tehničnimi zahtevami, ki mora biti neodvisno od ponora ali cilja prometa in kakršnih koli komercialnih razlogov. Skupna pravila omrežne nevtralnosti tako pomenijo, da ponudniki storitev dostopa do interneta ne morejo izbrati »zmagovalcev« ali »poraženčev« na internetu

ali se odločati, katere vsebine in storitve naj bodo uporabnikom na voljo. Prav tako ponudniki storitve dostopa do interneta ne smejo za samo razširjanje vsebine (storitve ali aplikacije) po internetu (dodatno) zaračunavati.

Uredba tudi pojasnjuje zahteve glede zagotavljanja t.i. specializiranih storitev, s posebnimi zahtevami glede kakovosti, ki jih ponujajo ponudniki dostopa do interneta in ponudniki vsebin in aplikacij. Upoštevati je treba nekatere zaščitne ukrepe, da se prepreči negativen vpliv teh storitev na odprt internet. Specializirane storitve ne smejo nadomestiti storitev dostopa do interneta in jih je mogoče zagotoviti le, če ima ponudnik dovoljšno zmogljivost omrežja, da jih ponuja poleg storitev dostopa do interneta in z njihovim zagotavljanjem ne sme ogroziti dostopnosti ali splošne kakovosti storitev dostopa do interneta za končne uporabnike.

Uredba ponudnikom storitev dostopa do interneta ne preprečuje uvajanja ukrepov za razumno upravljanje prometa. Da bi se takšni ukrepi šteli za razumne, morajo biti pregledni, nediskriminatorni in sorazmerni ter ne smejo temeljiti na poslovnih razlogih, temveč na objektivno različnih zahtevah glede tehnične kakovosti storitev za posamezno vrsto prometa. Takšni ukrepi ne spremljajo posameznih vsebin in se ne izvajajo dlje, kot je to potrebno. Če ukrepi za upravljanje prometa temeljijo na komercialnih razlogih, ukrep upravljanja prometa ni razumen. Očitni primer tega bi lahko bil tam, kjer ISP zaračunava uporabo različnih kategorij prometa ali ukrep upravljanja odraža poslovne interese ISP-a, ki sam ali v partnerstvu z nekim izvajalcem ponuja določene aplikacije. Za dokazovanje upravičenosti upravljanja prometa ni potrebno dokazovati komercialnih razlogov, zadostuje ugotovitev, da ukrep upravljanja prometa ne temelji na objektivnem kriteriju različnih tehničnih zahtev QoS.

Nediskriminatorni ukrepi upravljanja prometa ne preprečujejo izvajalcem ISP-jev, da z namenom optimizacije splošne kakovosti in uporabniške izkušnje uporabljajo ukrepe za upravljanje prometa, ki razlikujejo med objektivno različnimi kategorijami. Nediskriminatorno je enako obravnavanje prometa s podobnimi tehničnimi zahtevami (QoS), pa tudi različno obravnavanje prometa z različnimi tehničnimi zahtevami (QoS), če je takšno obravnavanje objektivno utemeljeno. Samo dejstvo, da gre za šifriran promet pa ne pomeni objektivne utemeljitve različnega obravnavanja s strani ponudnikov internetnih storitev.

Pri presoji, ali je ukrep upravljanja prometa sorazmeren se upošteva legitimen cilj, kot je povečati učinkovito rabo omrežnih virov in optimizacijo celotne kakovosti prenosa. Uporabljen ukrep mora biti primeren in potreben za dosego tega cilja (dokazuje operater), hkrati pa ne obstaja manj moteč in enako učinkovit alternativni način upravljanja za doseganje istega cilja (npr. enako obravnavanje brez uvajanja kategorij prometa) z razpoložljivimi omrežnimi viri.

Med dovoljene ukrepe upravljanja prometa spada tudi vpeljevanje ukrepov za upravljanje prometa, ki razlikujejo med objektivno različnimi kategorijami prometa. Kakršno koli takšno razlikovanje za optimizacijo splošne kakovosti in uporabniških izkušenj je dovoljeno le na podlagi objektivno drugačnih tehničnih značilnosti glede kakovosti storitve (npr. parametri, ko so: zamuda, tresenja, izgube paketov in pasovna širina) pri posamezni kategoriji prometa in ne na podlagi komercialnih razlogov. Zato morajo biti tako razlikovalni ukrepi sorazmerni glede na namen - optimizacija splošne kakovosti in morajo enako obravnavati enakovreden promet. Takih ukrepov se ne sme ohranjati dlje, kot je to potrebno, da se:

- zagotovi skladnost s pravom Unije ali nacionalnim pravom (zakonodaja, odločitve nacionalnih organov, sodišč, etc.),
- ohranja celovitost in varnost omrežja, storitev, ki se zagotavljajo prek tega omrežja in terminalske opreme končnih uporabnikov,
- prepreči bližajočo preobremenjenost omrežja in ublaži učinke izrednih ali začasna preobremenitev v omrežju, če se enakovredne kategorije prometa obravnavajo enako.

Med temami, ki zadnje čase močno burijo duhove tako med regulatorji kot med operaterji, je zahteva Uredbe, ki za razumno upravljanje prometa prepoveduje uporabo tehnik (temeljitega) pregledovanja/spremljanja vsebine podatkovnega prometa (DPI), ki se prenaša preko storitve dostopa do interneta. Nasprotno pa ukrepi za upravljanje prometa, ki spremljajo vidike, ki niso specifični za vsebino - generična vsebina - niso prepovedani. Tehnike spremljanja informacije v glavi IP-paketa in v glavi transportnega protokola (ang. transport layer protocol header, npr. TCP), štejejo za generične vsebine. To pa ne velja za posebno vsebino, ki jo zagotavljajo sami končni uporabniki (kot so besedilo, slike in video).

Ponudniki storitev dostopa do interneta morajo končnim uporabnikom zagotoviti transparentne in enostavno dostopne informacije o storitvah dostopa do interneta ter z njimi povezanih pogojih, ki bodo slednjim omogočile sprejem informiranih odločitev glede obsega, vrste in kakovosti storitev, za katere sklepajo naročniške pogodbe, ter učinkovito uveljavljanje pravic, ki se nanje nanašajo. Transparentnost pri ponujanju storitve dostopa do interneta je ena najbolj pomembnih zahtev, ki jih uvaja Uredba, saj uporabniku omogoča informirano odločitev pri izbiri ponudnika storitve. Za dosego izpolnjevanje te zahteve morajo operaterji objaviti:

- informacije o tem, kako bi lahko vplivali ukrepi upravljanja prometa, ki jih uporablja ta ponudnik, na kakovost storitve dostopa do interneta, na zasebnost končnih uporabnikov in varstvo njihovih osebnih podatkov;
- jasno in razumljivo razlago o tem, kako količinske omejitve prometa (»data cap«), hitrost in drugi parametri kakovosti storitev v praksi vplivajo na storitev dostopa do interneta, še zlasti glede uporabe vsebin, aplikacij in storitev;
- jasno in razumljivo razlago o tem, kako lahko specializirane storitve, ki jih je naročnik naročil v praksi, vplivajo na njegovo storitev dostopa do interneta;
- jasno in razumljivo razlago minimalne, običajno razpoložljive, maksimalne in oglaševane hitrosti prenosa podatkov v fiksnih omrežjih ali ocenjene maksimalne in oglaševane hitrosti prenosa podatkov v primeru mobilnih omrežij, in kako lahko pomembna odstopanja od objavljenih hitrosti prenosa vplivajo na izvajanje pravice končnih uporabnikov na podlagi Uredbe;

- jasno in razumljivo razlago pravnih sredstev, ki so potrošniku na voljo v skladu z nacionalno zakonodajo v primeru rednega in ponavljajočega razhajanja med dejanskim delovanjem storitve dostopa do interneta glede hitrosti ali drugih parametrov kakovosti storitev in zmogljivostjo, navedeno v pogodbi.

Nacionalni regulatorji imajo ključno vlogo pri zagotavljanju, da lahko končni uporabniki dejansko uveljavljajo svoje pravice na podlagi te Uredbe in da se spoštujejo pravila o zaščiti dostopa do odprtega interneta. V ta namen velja za nacionalne regulatorje obveznost spremljanja izvajanja Uredbe na nacionalni ravni in letno poročanje BEREC in Evropski komisiji. Na podlagi določil Uredbe so bile 30. avgusta 2016 izdane tudi Smernice BEREC (BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules)[1], (v nadaljevanju: Smernice BEREC), ki so namenjene zlasti zagotavljanju usmeritev nacionalnim regulativnim organom pri izvajanju njihovih obveznosti.

III. PRIPOROČILO AGENCIJE V ZVEZI Z IZVAJANJEM DOLOČIL UREDBE

Agencija je avgusta leta 2017 izdala Priporočilo v zvezi z izvajanjem določil Uredbe (EU) 2015/2120 Evropskega parlamenta in Sveta z dne 25.11.2015 glede zagotavljanja storitev dostopa do interneta (v nadaljevanju: Priporočilo), katerega glavni namen je spodbuditi ponudnike storitev dostopa do interneta, da z objavo popolnih, razumljivih, primerljivih in ažurnih informacij o storitvi dostopa do interneta zagotovijo podlago, ki bo omogočala učinkovito zaščito pravic končnih uporabnikov na tem področju. Agencija je operaterjem že v času priprave Priporočila pojasnila, da bo takšni obliki mehke regulacije kmalu sledil tudi zavezujoč predpis, česar pa se bo agencija v sodelovanju z operaterji lotila v letošnjem letu.

Med pomembnejšimi določili Priporočila so definicije hitrosti:

- maksimalna hitrost (teoretično najvišja hitrost prenosa podatkov, ki je naročniku dejansko dosegljiva vsaj enkrat dnevno),
- običajno razpoložljiva hitrost (hitrost dostopa do interneta, ki jo naročnik lahko pričakuje večino časa v dnevu; agencija priporoča, da je to 90% časa dneva, izven vršnih ur in da znaša vsaj 80% maksimalne hitrosti),
- minimalna hitrost (najnižja dejanska hitrost storitve dostopa do interneta, razen v primeru izpada omrežja ali napake na njem),

Pomemben korak v smeri transparentnosti pri ponujanju storitev, še zlasti za končne uporabnike, bo nadgrajeno merilno orodje AKOSTestNet. Z njim sicer že danes lahko končni uporabniki preverjajo nekatere parametre, ki kažejo na kvaliteto storitve dostopa do interneta, med njimi najpomembnejše so pritočna in odtočna hitrost, zakasnitev, jakost signala in nekaj testov glede nevtralnosti interneta, kot so prenos govora po omrežju IP (VoIP test), test nespremenjene vsebine, transparentnost povezave, preverjanje razpoložljivosti domenskih strežnikov, blokiranje določenih vrat UDP in TCP[2]. Takšno merilno orodje končni uporabniki potrebujejo za preverjanje izpolnjevanja pogodbenih določil s strani ponudnikov storitev. Do konca junija bo agencija njegovo delovanje in tehnične značilnosti že lahko predstavila tudi vsem ponudnikom storitev dostopa do interneta.

Pri nadzoru izvajanja same Uredbe pa so agenciji v veliko pomoč še zlasti končni uporabniki, ki pri uporabi storitev dostopa do interneta naletijo na zelo različne težave. Tudi na podlagi informacij, ki jih agencija prejme na ta način, se pričnejo postopki, v katerih se ugotavljajo kršitve.

IV. AKTIVNOSTI REGULATORJEV

Od uveljavitve Uredbe dalje predstavlja njeno izvajanje velik izziv, ne samo za operaterje ampak tudi za regulatorje.

V samem začetku smo se vsi skupaj veliko ukvarjali z vprašanjem prenove določil (obstoječih) naročniških pogodb. V Sloveniji nekoliko izstopamo tudi glede prakse, da se naročniške pogodbe sklepajo za nedoločen čas, to pomeni, da po preteku obdobja vezave, dogovorjene zaradi prejema nekakšne ugodnosti, naročniško razmerje avtomatično brez aktivnega ravnanja naročnika, teče dalje. V naročniških pogodbah so ponudniki storitev dostopa do interneta morali na novo definirati pogodbene hitrosti: minimalno, običajno razpoložljivo in maksimalno. V splošnih pogojih pa pojasniti tehnike upravljanja prometa, če jih uporabljajo, in ostale zahteve iz 4. člena Uredbe. Po Priporočilu agencije, kjer so definirane tudi njihove vrednosti, je sedaj potrebno na posameznem priključku izmeriti dejansko hitrost prenosa podatkov, preden se ta vrednost lahko zapiše v pogodbo, saj je za operaterja zavezujoča. Uporabniki pa so upravičeni brez kakršnih koli nadomestil preiti na paket z nižjo hitrostjo, če jim operater ne more več zagotavljati do sedaj v pogodbi navedene. Podobno velja tudi v drugih državah članicah. Do decembra 2017 so nekatere parametre glede hitrosti definirale tudi še nekatere druge države članice:

- Hrvaška: minimalna hitrost je 70% maksimalne,
- Finska: minimalna hitrost je 70% maksimalne,
- Litva: minimalna hitrost je 20% maksimalne,
- Slovaška: minimalna hitrost je 40% maksimalne in normalno razpoložljiva hitrost je 90% maksimalne hitrosti.

V letošnjem letu je agencija tudi s pomočjo informacij, ki nam jih sporočajo končni uporabniki, pričela z analizo politike blokiranja »vrat«. Znano je namreč, da ponudniki storitev dostopa do interneta, razlog o varnosti omrežij in storitev izkoriščajo za komercialne namene. Iz odgovorov na

[1] https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

[2] https://www.akostest.net/sl/

podlagi vprašalnikov in z analizo podatkov, zbranih z lastnimi merilnimi orodji, je agencija pridobila nekatere informacije o različnih praksah operaterjev. Ugotoviti je mogoče, da se operaterji na splošno poslužujejo blokiranja, vendar tudi, da to počno zelo različno, za kar ni objektivno utemeljenega razloga. Pri tem ravnanju pa se ponudniki storitev dostopa do interneta v Sloveniji prav nič ne razlikujejo od ostalih ponudnikov v EU. Zato je agencija konec leta 2017 predlagala, da države članice enotno pristopijo k reševanju problematike blokiranja vrat in da se glede tega vprašanja oblikujejo enotne smernice, ki naj jih glede na njuno vlogo v odnosu do regulatorjev pripravita v sodelovanju BEREC in ENISA, v delovnih skupinah, v katerih sodelujemo predstavniki vseh regulatorjev. Nekatere države članice, kot je na primer Finska, se s to tematiko ukvarjajo že dlje časa. Februarja letos pa so objavili tudi Priporočilo[3] za filtriranja internetnega prometa zaradi varnosti.

Že kmalu po uveljavitvi Uredbe pa so se regulatorji po Evropi morali spopasti s problematiko presoje zakonitosti dogovorov in poslovnih praks operaterjev v zvezi s tarifami za določeno količino podatkov in podatkovne hitrosti. Uredba regulatorjem nalaga dolžnost ukrepanja zoper poslovne prakse, ki bi zaradi svojega obsega privedle do tega, da bi bila izbira, ki je na voljo končnim uporabnikom, v praksi bistveno zmanjšana. Pri presojanju dogovorov in poslovnih praks mora regulator med drugim upoštevati tržni položaje ponudnika storitev dostopa do interneta in ponudnika vsebin, aplikacij in storitev ter posredovati, kadar bi dogovori ali poslovne prakse ogrozili bistvo pravic končnih uporabnikov. Splošnost določb Uredbe je zahtevala bolj podrobno ureditev, kot jo sedaj najdemo v Smernicah BEREC, tudi zaradi čim bolj poenotenega pristopa regulatorjev pri izvrševanju svojih nalog in s tem namenom. V Evropski Uniji namreč veliko operaterjev svoje storitve ponuja v več različnih državah članicah. Z vidika pravne predvidljivosti in pravne varnosti različne odločitve regulatorjev v podobnih primerih res niso zaželene.

Največ preglavic regulatorjem povzroča posebna oblika poslovne prakse, imenovana ničelna tarifa (»zero rating«). V takšnem primeru ponudnik internetnih storitev za podatkovni promet, povezan z določeno aplikacijo ali kategorijo, ne zaračunava porabljenih količin (so brezplačne in se ne vštevajo v zakupljeno količino). Regulatorji (npr. NMHH-Madžarska, PTS-Švedska) so se najprej spopadli s primeri, ki očitno kršijo določila Uredbe (3/3. člen). Gre za ponudbe ničelne tarife, kjer so vse aplikacije blokirane (ali upočasnjene) potem, ko je dosežena zgornja meja zakupljenih količin podatkov, razen aplikacij/vsebin z ničelno tarifo. Takšne oblike poslovne prakse so regulatorji po Evropi že prepovedali, enako je odločila tudi agencija.

Pri presoji zakonitosti posamezne poslovne prakse ponudnika, regulator zlasti presoja v kolikšni meri ta omejuje prosto izbiro končnih uporabnikov dostop do odprtega interneta, s postavljenimi komercialnimi in tehničnimi pogoji. Ukrepanje je potrebno kadar ta bistveno zmanjšuje možnost izbire in pa tudi, ko gre za omejevanje uveljavljanja pravic končnih uporabnikov, skladno s 3/1. členom Uredbe. Pri odločanju regulator, poleg tržnih deležev ponudnika vsebin in ponudnika storitev dostopa do interneta, upošteva (potencialne) učinke na obseg in raznolikost vsebin in aplikacij, ki jih končni uporabniki lahko uporabijo, ali sta obseg in raznolikost aplikacij, ki jih lahko izbirajo končni uporabniki, zmanjšana v praksi, ali se končnega uporabnika spodbuja k uporabi točno določenih aplikacij in podobno. Ponudnik storitev dostopa do interneta lahko uporabi ali ponudi ničelno tarifo za celotno kategorijo aplikacij, npr. vse video vsebine ali vse aplikacije za pretakanje glasbe (»music streaming«) ali samo za nekatere (npr. lastne storitve, eno posebno aplikacijo za socialne medije, najbolj priljubljeno video ali glasbeno aplikacijo). V slednjem primeru končnemu uporabniku ni omogočeno brezplačno uporabljanje drugih aplikacij in je s tem njegova prosta izbira iz ekonomskega stališča močno omejena in se njegova prosta izbira dejansko bistveno zmanjša.

V nadzornih postopkih so regulatorji v zadnjem letu že sprejeli nekaj odločitev s katerimi so posegli na trg in od ponudnikov storitev zahtevali spremembo ponudbe ali jo celo prepovedali. Pri presoji zakonitosti ponujanja ničelne tarife za celotno kategorijo aplikacij regulatorji zlasti preverjajo odprtost platform z vidika potencialnih novih ponudnikov te vrste vsebin. Uredba namreč kot končnega uporabnika varuje tudi ponudnike vsebin. Nenazadnje smo danes pravzaprav vsi uporabniki interneta tudi ustvarjalci internetnih vsebin. Z vidika varovanja pravic končnih uporabnikov pa je pri ničelnih tarifah pomembna tudi vključena količina zakupljenih podatkov v paketu. V praksi to pomeni, da ponudba bolj omejuje prosto izbiro uporabnika, če se z ničelno tarifo ponujajo video storitve, v ceno paketa pa je vključena zgolj manjša količina podatkov, ki zadošča le za nekaj ur uporabe tovrstnih storitev, ki niso vključene v ničelno tarifo. Preverja pa se tudi samo izvajanje storitev iz vidika kakovosti. Tako je na primer avstrijski regulator oziroma upravni organ, ki ima v Avstriji pooblastila za izvajanje nadzornih postopkov, operaterju prepovedal degradacijo kakovosti storitev, ki so se ponujale kot ničelne storitve[4]. Odpirajo pa se že nova vprašanja, kot je zagotavljanje ničelnih storitev v roamingu itd.

V. SMERNICE BEREC V POSTOPKU REVIZIJE

Na trg prihajajo nove tehnologije in z njimi nove storitve. Evropska komisija je s pomočjo zunanjih izvajalcev že pričela s postopkom revizije Uredbe v luči njene ustreznosti za razvoj in prihajajoče tehnologije. BEREC pa v letošnjem letu izvaja pregled Smernic BEREC. Nekaj pomembnejših vprašanj je naslovil tudi na širšo javnost[5], ki je bila do 25. 4.

[3] https://www.viestintavirasto.fi/en/cybersecurity/informationsecuritynow/2018/02/ttn201802091159.html

[4] https://www.rtr.at/en/pr/PI20122017TK

[5] https://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/8012-consultation-paper-on-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines

2018 pozvana k predložitvi komentarjev, med drugim na naslednje teme:

- Ali so Uredba in Smernice vplivale na vašo odločitev glede (ne)uvedbe nove ali prenehanja zagotavljanja kakšne storitve?
- Ali so smernice dovolj jasne in zagotavljajo dodatno obrazložitev k Uredbi?
- Ali so določila Uredbe glede dovoljenih komercialnih praks dovolj jasna? Je metodologija presoje dovoljenosti t.i. ničelne storitve (»zero rating«) s strani regulatorjev dovolj jasna? Je vplivala na vpeljevanje novih storitev in aplikacij na internetu? Ali metodologija analiziranja dovolj upošteva potencialne daljnosežne posledice izvajanja takšnih komercialnih praks?
- Ali so določila Smernic glede ukrepov razumnega in izrednega upravljanja prometa dovolj jasna?
- Ali besedilo Smernic vpliva na razvoj omrežnih tehnologij, ki se ponujajo na trgu?
- Ali so določila glede specializiranih storitev dovolj jasna? Ali vplivajo na pojav in razvoj teh storitev na trgu?
- Ali so zahteve glede transparentnosti dovolj jasne, še zlasti glede hitrosti mobilnega interneta?
- Na kakšen način bi BEREC lahko pomagal končnim uporabnikom pri tem, da dejansko prejmejo storitve, ki so jih naročili in plačali?
- Ali so Uredba in Smernice dovolj fleksibilne za uvajanje novih tehnologij, ki se bodo ponujale v omrežjih 5G?
- Ali so pravila za upravljanje prometa in specializirane storitve v Smernicah in Uredbi dovolj jasna za uvajanje novih tehnologij, kot sta omrežno rezinjenje (network slicing) in računalništvo na robu (edge computing)?

Do konca letošnjega leta bo tudi na podlagi izsledkov predmetnega javnega posvetovanja jasno ali se bodo Smernice BEREC spreminjale že pred pričetkom postopka spreminjanja Uredbe.

VI. NA KRATKO ŠE O ZASEBNOSTI

Evropska Komisija je 10. 1. 2017 pripravila predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (Uredba o zasebnosti in elektronskih komunikacijah), na kratko tudi *ePrivacy*. Glavni razlog za pripravo nove zakonodaje na tem področju je uveljavitev Uredbe EU št. 2016/679 (v nadaljevanju: GDPR) in zastarelost zakonodajnega okvira (Direktiva 2002/58/ES), ki danes pokriva to področje. S prihodom novih tehnologij in še zlasti novih storitev je potrebno zaupnost komunikacij urediti na novo. Načela in glavne določbe Direktive 2002/58/ES ne sledijo razvoju tehnološke in tržne realnosti, kar je povzročilo nedosledno ali neučinkovito zaščito zasebnosti in zaupnosti v zvezi z elektronskimi komunikacijami. Na trgu so se pojavile nove elektronske komunikacijske storitve, ki so s potrošniškega vidika nadomestljive s tradicionalnimi storitvami, vendar jim po sedanji zakonodaji ni potrebno izpolnjevati enakih pravil. Razvoj prinaša nove tehnike, ki omogočajo sledenje spletnemu obnašanju končnih uporabnikov, ki jih Direktiva 2002/58/ES ne pokriva.

V predlogu tako *ePrivacy* določa pravila v zvezi z varstvom temeljnih pravic in svoboščin fizičnih oseb pri zagotavljanju in uporabi elektronskih komunikacijskih storitev, zlasti pravic do spoštovanja zasebnega življenja in komunikacij ter varstva fizičnih oseb v zvezi z obdelavo osebnih podatkov ter pravila glede varstva temeljnih pravic in svoboščin pravnih oseb pri zagotavljanju in uporabi elektronskih komunikacijskih storitev in zlasti njihovih pravic do spoštovanja komunikacij. Gre za *lex specialis* glede na splošno uredbo o varstvu podatkov. Podrobno opredeli in dopolni področje elektronskih komunikacijskih podatkov, ki se štejejo za osebne podatke. Vse zadeve, ki se nanašajo na obdelavo osebnih podatkov in jih ta ne obravnava posebej, so zajete v GDPR. Predlog *ePrivacy* tako ureja:

- podatke o elektronskih komunikacijah, ki so opredeljeni kot osebni podatki (določa posebna pravila glede posebnih namenov obdelave),
- obdelavo vsebine elektronskih komunikacij pri prenosu in metapodatkov elektronskih komunikacij, ki se ustvarjajo v zvezi z zagotavljanjem in uporabo elektronskih komunikacijskih storitev,
- informacije, ki se obdelujejo ali oddajajo ali shranjujejo v terminalski opremi končnih uporabnikov,
- dajanje na trg programske opreme, ki omogoča elektronske komunikacije, vključno s pridobivanjem in prikazovanjem informacij na internetu,
- ponudbo javno dostopnega imenika končnih uporabnikov elektronskih komunikacijskih storitev,
- pošiljanje ali predstavljanje neposrednih tržnih sporočil končnim uporabnikom.

Uredba je še v postopku sprejemanja, zato njen končni tekst še ni poznan. V trialogu ostaja odprtih nekaj vprašanj, kot so definicija storitve medosebne komunikacije (interpersonal communications service), pomožne storitve (ancillary feature), obseg zaščite komunikacij med napravami (machine-to-machine), idr.

Pomemben napredek z vidika varovanja zasebnosti komunikacij pa vsekakor predlog Uredbe prinaša, saj bodo pri uporabi storitev zaščiteni tudi uporabniki t.i. povrhnjih (OTT) storitev, kot tudi gostujoči na brezžičnih tehnologijah (hot spots) v javnih in pol javnih prostorih, ne glede na to ali so takšna omrežja zaščitena z gesli ali ne.

VII. ZAKLJUČEK

Pomembnosti internetne/omrežne nevtralnosti se v Sloveniji in Evropi precej dobro zavedamo. Z veseljem se lahko ozremo tudi na nekatere druge kontinente, kjer takšno mišljenje delijo z nami (npr. Indija, Argentina, Kanada) in manj ko pogledamo razmere v ZDA. Evropa je prepoznala tudi pomembnost varovanja podatkov in k spoštovanju zasebnosti z GDPR že zavezala tudi neevropske ponudnike storitev, ki se zagotavljajo preko interneta. S prihodom *ePrivacy* in novim Evropskim zakonikom o elektronskih komunikacijah (European Electronic Communication Code – EECC) se bo še bistveno bolj izboljšalo tudi varovanje zasebnosti in zaupnosti vseh, tudi t.i. komunikacijskih

storitev OTT. Z novimi zahtevami glede transparentnosti delovanja operaterjev pa se bo še dodatno izboljšala možnost uporabnikov za informirano odločitev pri izbiri ponudnika elektronskih komunikacijskih storitev.

LITERATURA

[1] Zakon o elektronskih komunikacijah, (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US in 81/15, 40/2017) - neuradno prečiščeno besedilo ZEKom-1)

[2] UREDBA (EU) 2015/2120 EVROPSKEGA PARLAMENTA IN SVETA z dne 25. novembra 2015 o določitvi ukrepov v zvezi z dostopom do odprtega interneta

[3] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules

[4] Priporočilo v zvezi z izvajanjem določil Uredbe (EU) 2015/2120 Evropskega parlamenta in Sveta z dne 25.11.2015 glede zagotavljanja storitev dostopa do interneta.

[5] BEREC Report on the implementation of Regulation (EU) 2015/2120 and BEREC Net Neutrality Guidelines

[6] Consultation paper on the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines

[7] UREDBA EVROPSKEGA PARLAMENTA IN SVETA o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES, https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52017PC0010

[8] UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)

Katja Kmet je vodja Sektorja za nadzor operaterjev pri Agenciji za komunikacijska omrežja in storitve. Po izobrazbi je univ. dipl. pravnica in je na agenciji zaposlena 16 let. S svojim delom je pričela na oddelku za reševanje sporov, nato je 8 let opravljala naloge inšpektorja za telekomunikacije in sedaj 5 let vodi Sektor za nadzor operaterjev. Zadnja 3 leta se intenzivno ukvarja s področjem internetne nevtralnosti, tudi kot aktivna članica delovne skupine pri združenju Evropskih regulatorjev elektronskih komunikacij BEREC. Je tudi članica delovne skupine Article 13a pri organizaciji ENISA. Pri svojem delu spremlja in se dodatno izobražuje tudi na področjih tehničnega razvoja omrežij in storitev naslednje generacije, varstvom zasebnosti ter varnosti omrežij in storitev.

Zagotavljanje varnosti komunikacijskih omrežij in storitev

Urban Kunc, Agencija za komunikacijska omrežja in storitve RS

Povzetek — Članek obravnava pregled evropske in slovenske zakonodaje in zakonskih obveznosti, ki jih imajo operaterji elektronskih komunikacij na področju zagotavljanja varnosti omrežij in storitev.

Ključne besede — varnost, celovitost, ENISA, ZEKom-1, NIS Direktiva

Abstract — This article deals with a review of European and Slovenian legislation and legal obligations for undertakings providing end-users electronic communication services in the area of network and service security.

Keywords — security, integrity, ENISA, ZEKom-1, NIS Directive

I. UVOD

Telekomunikacije so danes eden ključnih gradnikov družbe. Predstavljajo hrbtenico, ključno infrastrukturo, na podlagi katere delujejo vse sfere družbe in gospodarstva in je hkrati tudi instrument funkcioniranja in izražanja. Zagotovitev varnosti in celovitosti te infrastrukture, kot tudi zagotavljanje zasebnosti komunikacij, je zato postala ena od primarnih in prioritetnih nalog Evropske komisije. Varnost omrežij in informacij postaja vse bolj pomembna za evropsko, kot tudi slovensko gospodarstvo in družbo. Informacijske sisteme lahko ogrozijo varnostni incidenti, ki so lahko posledica človeških napak, naravnih dogodkov, tehničnih okvar in vedno več tudi zlonamernih napadov. Ti incidenti so vse obsežnejši, pogostejši in velikokrat nepredvidljivi.

V letu 2009 sprejeta reforma evropskega regulatornega okvirja elektronskih komunikacij (EU Direktiva 2009/140/ES, v nadaljevanju Okvirna direktiva) je med drugim zaradi pomembnosti telekomunikacij kot kritične infrastrukture v regulatorni okvir med drugim vključila tudi določila o zagotavljanju varnosti in celovitosti. V njem je naslovila vsa podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve, da morajo sprejeti ustrezne tehnične in organizacijske ukrepe za ustrezno obvladovanje tveganja za varnost omrežij in storitev. Ti ukrepi se morajo sprejeti predvsem zaradi preprečitve in zmanjšanja učinka varnostnih incidentov na uporabnike in medsebojno povezana omrežja. Reforma je bila prenešena v večino držav članic EU, vključno s Slovenijo, ki je omenjeno obveznost vključila v Zakon o elektronskih komunikacijah (v nadaljevanju ZEKom-1).

V pripravi pa je tudi že nov Evropski zakonik o elektronskih komunikacijah, ki prinaša med drugim tudi določene spremembe na področju zagotavljanja varnosti in celovitosti omrežij.

II. ZAKONODAJA IN STANDARDI

ZEKom-1 obravnava varnost omrežij in storitev v VII. poglavju. Agencija za komunikacijska omrežja RS (v nadaljevanju agencija) je na podlagi določil ZEKom-1 v letu 2013 sprejela še Splošni akt o varnosti in celovitosti, s katerim je podrobneje uredila izvajanje določb predmetnega VII. poglavja ZEKom-1. Predmetni splošni akt se je v letu 2015 dopolnil in spremenil, predvsem v tem, da poleg obstoječih obveznosti naslavlja tudi delovanje omrežij v izjemnih stanjih. Trenutni veljavni je Splošni akt o varnosti omrežij in storitev ter delovanje v izjemnih stanjih (Ur.l. RS, št. 75/13 in 64/15; v nadaljevanju Splošni akt [2]).

Tako VII. poglavje ZEKom-1 kot Splošni akt obravnavata dve ključni določili, ki jih morajo spoštovati vsi operaterji:

- obveznost sprejema in izvajanja ustreznih tehničnih in organizacijskih ukrepov, s katerimi se obvladuje tveganja za varnost omrežij in storitev ter
- obveznost obveščanja in poročanja agenciji v primeru kršitev varnosti ali celovitosti.

V praksi za operaterje to pomeni, da morajo vpeljati dobro prakso upravljanja varovanja informacij in neprekinjenega poslovanja, pri čemer je varovanje informacij sestavni del vseh bistvenih poslovnih in podpornih procesov ter postopkov v okviru opredeljenega obsega.

III. SUVI IN SUNP

Standardov in dobrih praks na področju informacijske varnosti je precej, kljub vsemu pa je študija[1] Evropske Agencije za varnost omrežij in informacij (ENISA) ugotovila, da je med operaterji ISO/IEC 27001, poleg PCI DSS in ITIL, ena od najbolj uporabljanih dobrih praks na področju informacijske varnosti. Temu vedenju je sledila tudi agencija, ki v Splošnem aktu sicer ni predpisala specifičnega standarda, ki bi ga morali vpeljati operaterji, je pa v veliki meri sledila sistemskemu pristopu in okvirju, ki ga obravnava družina standardov ISO/IEC 27000.

Splošni akt operaterjem nalaga, da morajo vzpostaviti sistem upravljanja varovanja informacij (v nadaljevanju: SUVI), kot tudi sistem neprekinjenega poslovanja (v nadaljevanju SUNP). Le-ta mora vsebovati:

- varnostno politiko in politiko neprekinjenega poslovanja, ki vključuje izpolnjevanje zakonodajnih in pogodbenih obveznosti;
- obseg in meje SUVI in SUNP z vidika značilnosti poslovanja, organizacije, lokacije, velikosti, tehnologije;

[1] ENISA: Shortlist of network and information security standards: https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards/view

– navodila za izvajanje analize in varnostnih tveganj, vključno z metodologijo, ki jo je operater izbral za izvajanje analize varnostnih tveganj, kriterije za izbor varnostnih tveganj;
– navodila za izvajanje analize vpliva na poslovanje in obravnave tveganj za neprekinjeno poslovanje, vključno z metodologijo, s katero izvaja analizo tveganj in kriterije za izbor ukrepov za visoko ocenjena tveganja in obravnavo preostalih tveganj;
– varnostni načrt, ki vključuje opredelitev vseh tveganj, opredelitev verjetnosti uresničitve groženj, opredelitev stopnje negativnih učinkov, potrebne ukrepe in način organiziranja varnosti znotraj operaterja vključno s zagotavljanjem ustreznih kadrovskih virov;
– načrt za zagotavljanje celovitosti omrežja in neprekinjenega izvajanja storitev, vključno s postopki, ki v najkrajšem možnem času omogočijo ponovno izvajanje storitev;
– zapise o incidentih, notranjih presojah in vodstvenih pregledih SUVI in SUNP, s katerimi analiziramo in merimo stanje ukrepov in uvajamo korektivne ukrepe;
– dokumentiran sistem, ki obravnava vse postopke in procese , krovno politiko ter omogoča spremljanje, merjenje, analiziranje in vrednotenje sistema SUVI in SUNP.

IV. VARNOSTNI UKREPI

Nezanesljiva programska ali strojna oprema, človeška napaka, podnebne spremembe, teroristični in kibernetski napadi in drugi dogodki so dogodki, ki lahko povzročijo izpad ali ohromitev delovanja storitev. Incident, kot je opredeljen v splošnem aktu, je tako eden ali več neželenih ali nepričakovanih dogodkov, za katere je verjetno, da bodo ogrozili varnost omrežij in storitev ali celovitost omrežja. Merjenje vpliva incidenta ni enostavno, saj je potrebno vzeti v obzir številne dejavnike, tako tiste na strani podjetja (operaterja), kot tiste na strani uporabnikov in družbe. Pri sami evalvaciji incidenta tako lahko ocenjujemo, kakšen vpliv ima incident na poslovanje operaterja, na zakonodajne in regulatorne obveznosti, kakšen ima vpliv na končne naročnike, kateri so bili razlogi za incident in drugi dejavniki.

Evropska komisija je določila in pooblastila ENISO, da z zagotavljanjem strokovnega znanja in svetovanja ter spodbujanjem izmenjave najboljših praks ter harmoniziranim pristopom prispeva k višji ravni varnosti elektronskih komunikacij v Evropi. ENISA ima tako tudi ustrezna pooblastila in sredstva, da sama oz. skupaj z nacionalnimi regulatornimi organi ocenjuje raven varnosti evropskih omrežij in storitev in na podlagi groženj in analiz pripravlja ustrezna priporočila in dobre prakse, ki so v pomoč tako operaterjem, komisiji, kot tudi regulatorjem.

V okviru ENISE je tako nastala tudi strokovna delovna skupina »Article 13a«, ki združuje predstavnike evropskih regulatorjev in strokovnjake ENISE. Ime skupine (»Article 13a«) se navezuje na 13a člen Okvirne direktive, ki obravnava varnost in celovitost, glavni namen skupine pa je, da se skozi odprti dialog med vsemi deležniki dogovori o usklajeni in učinkoviti implementaciji in nadzoru določil predmetnega člena, vključno s poročanjem in izmenjavo informacij.

V okviru dela skupine »Article 13a« je bila izdana vrsta dokumentov, med drugim tudi:

– Tehnične smernice za vzpostavitev minimalnih varnostnih ukrepov [4] ter
– Tehnične smernice za poročanje o varnostnih incidentih [5]

Omenjena dokumenta podrobneje pojasnjujeta določila 13a Okvirne direktive in sta v pomoč regulatorjem in operaterjem pri ocenjevanju ustreznosti implementiranih varnostnih ukrepov, analiziranju in ublažitvi pogostih vzrokov za incidente ter opredeljujeta proces ocenjevanja vpliva in poročanja incidentov.

Tehnične smernice za vzpostavitev minimalnih varnostnih ukrepov uvodoma pojasnjujejo posamezne pojme, nato pa se predstavi 25 ključnih varnostnih ciljev, ki so razporejeni v sedem ločenih domen. Za vsako od prepoznanih varnostnih ciljev so navedeni varnostni ukrepi, katere je smiselno uvesti in presojati v okviru inšpekcijskega nadzora agencije oz. pooblaščenega revizorja. Dokument se navezuje na družino mednarodnih varnostnih standardov za upravljanje informacijske varnosti ISO/IEC 27000, podaja primernost uporabe posameznega standarda s posamezno varnostno kategorijo ter podaja pregled še drugih varnostnih standardov, ki so relevantni za sektor elektronskih komunikacij.

V. OBVEZNOST POROČANJA

Tako Okvirna direktiva, ZEKom-1, kot Splošni akt obvezujejo operaterje, da obvestijo pristojni nacionalni organ (agencijo) o vseh kršitvah varnosti omrežij in storitev ali celovitosti, če so te pomembno vplivale na delovanje javnih komunikacijskih omrežij ali izvajanje javnih komunikacijskih storitev. Nadalje ima agencija tudi obveznost, da glede na stopnjo kršitve obvešča naprej nacionalno kontaktno točko za obravnavo varnostnih incidentov (SI-CERT), po potrebi še ENISO kot tudi druge nacionalne regulatorne organe v drugih državah. V primeru, da gre za kršitev oz. incident, katere razkritje je v javnem interesu, potem mora agencija o tem obvestiti javnost ali to naložiti operaterju. Agencija zbira in analizira prejeta poročila, najbolj kritične primere pa tudi v anonimizirani obliki enkrat letno pošlje ENISI in Evropski Komisiji.

Kot povedano uvodoma v prejšnjem poglavju, merjenje učinka in vzrokov nastanka posameznega incidenta ni enostavno, saj pri tem nastopajo različni dejavniki, ki se razlikujejo od operaterja do operaterja v odvisnosti od storitev, ki jih zagotavlja, kot od števila uporabnikov, ki uporabljajo te storitve. Osnovni namen priporočila o poročanju incidentov je zagotoviti na evropskem nivoju harmonizirani način poročanja in evalvacije incidentov. Na podlagi analize tovrstnih poročil lahko tako regulator na nacionalnem ali ENISA na evropskem nivoju:

– identificira pomembne varnostne incidente, ki imajo pomemben vpliv,
– prepozna glavne vzroke varnostnih incidentov,
– pridobi vpogled v pripravljenost posameznih operaterjev (oz. držav) na varnostne dogodke,
– pridobiva izkušnje in znanja,
– prepozna varnostne trende,
– pregleduje in ocenjuje učinkovitost obstoječih ukrepov,
– pripravlja boljša in ustreznejša priporočila.

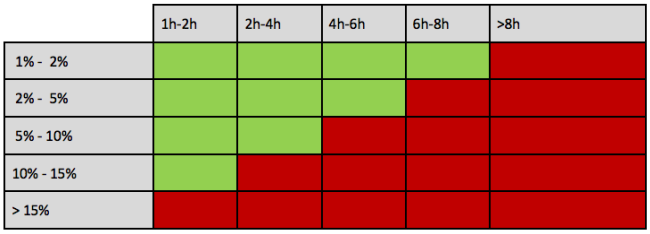
Predmetno priporočilo ENISE in skupine »Article 13« opredeljuje varnostni incident, kot dogodek, ki ima

pomemben vpliv na delovanje omrežja in izvajanje storitev. Z vidika izvajanja storitev to vključuje dogodke, ki vplivajo na neprekinjenost delovanja ali kakovost zagotavljanja vnaprej določene ravni storitev, kot ima tudi vpliv na varnost uporabnikov in z operaterjem povezana omrežja. Vsaka država ima diskrecijsko pravico, da določi, kako bo vrednotila incidente in kateri dogodek je za posameznega regulatorja pomemben oz. tako izjemen, da ga je treba priglasiti. ENISA je kot glavna kazalnika opredelila trajanje incidenta in število prizadetih po posamezni storitvi, dodatno pa tudi vpliv dogodka na zagotavljanja storitve klica v sili in vpliv na druga omrežja.

Priporočilo ENISE glede dolžine trajanja in števila prizadetih predlaga uporabo relativnih ali pa absolutnih vrednosti. Relativna vrednost, za katero se je odločila tudi agencija, upošteva tako čas trajanja incidenta kot število prizadetih uporabnikov, absolutna vrednost, ki je predvsem uporabna v državah z več milijoni uporabnikov, pa temelji na zmnožku časa izpada in števila prizadetih (npr. 60 milijonov uporabnikov minut). Splošni akt nalaga operaterjem, da morajo obveščati agencijo, ko je incident presegel eno od naslednjih vrednosti:

- vpliv je trajal več kot eno uro in je prizadel več kot 15 % vseh naročnikov posameznega operaterja po posamezni storitvi,
- vpliv je trajal več kot dve uri in je prizadel več kot 10 % vseh naročnikov posameznega operaterja po posamezni storitvi,
- vpliv je trajal več kot štiri ure in je prizadel več kot 5 % vseh naročnikov posameznega operaterja po posamezni storitvi,
- vpliv je trajal več kot šest ur in je prizadel več kot 2 % vseh naročnikov posameznega operaterja po posamezni storitvi,
- vpliv je trajal več kot osem ur in je prizadel več kot 1 % vseh naročnikov posameznega operaterja po posamezni storitvi

Slika 1 prikazuje zgoraj navedene referenčne vrednosti še v grafični obliki.



Slika 1: Presežene referenčne vrednost, kot je potrebno poročati incident agenciji

Trajanje in število prizadetih je vezano na naslednje ključne posamezne storitve:

- govorne storitve preko fiksnega omrežja,
- govorne storitve preko mobilnega omrežja,
- širokopasovne storitve preko fiksnega omrežja,
- širokopasovne storitve preko mobilnega omrežja.

Navezujoč se na priporočilo ENISE Splošni akt opredeljuje naslednji nabor podatkov, ki jih je treba poročati ob takem dogodku, in sicer:

- čas nastanka in trajanja incidenta,
- oceno števila prizadetih naročnikov po posamezni storitvi,
- statistično regijo prizadetih uporabnikov,
- vpliv na omrežje (prizadeti del omrežja in prizadeta sredstva) in storitve,
- vpliv na druga povezana omrežja in operaterje,
- vpliv na zagotavljanje storitve klica v sili na številke 112, 113 in 116 000,
- popis vzrokov in posledic incidenta,
- izvedeni ukrepi po incidentu.

Poleg trajanja in števila prizadetih je pomemben podatek primarni vzrok in posledic incidenta. ENISA je identificirala 5 ključnih primarnih vzrokov in sicer: človeška napaka, sistemska napaka, naravne nesreče in dogodki, zlonamerna dejanja in tretja oseba. Operater mora v poslanem poročilu natančno pojasniti razloge, ki so botrovali dogodku in kako je ukrepal, da bi ublažil vpliv dogodka na uporabnike in povezana omrežja. Dobra praksa in varnostni standardi svetujejo organizacijam, da incidente analizirajo z namenom, da ugotovijo vzroke dogodka in pripravijo nove ukrepe, ki bi v prihodnje zmanjšali verjetnost ponovitve. Poročilo zato tudi vsebuje podatke, katere aktivnosti po dogodku je operater izvedel in kaj se je iz njega naučil oz. katere ukrepe je sprejel in implementiral. Le-te lahko agencija tudi preverja ob morebitnem inšpekcijskem nadzoru. V letu 2017 smo na podlagi postavljenih kriterijev od operaterjev prejeli 11 tovrstnih poročil o incidentih. Glavni razlogi za incidente so bili pretrgani optični kabli, sistemska napaka, izpad električnega napajanja in naravna nesreča (npr. vetrolom, žled itd.). Glede na število ocenjenih prizadetih uporabnikov in trajanja dogodka smo ocenili, da nobeden ni presegel vrednosti, da bi jih bilo potrebno poročati ENISI in Komisiji. ENISA je število prizadetih in čas trajanja incidenta navezala na število vseh uporabnikov na nacionalnem nivoju po posamezni storitvi, agencija pa je število prizadetih in čas trajanja navezala na število naročnikov po posameznem operaterju in po posamezni storitvi. To se je izkazalo v praksi kot primerna izbira, saj je zelo velikih izpadov oz. incidentov relativno malo.

Agencija v okviru svojih pristojnosti in določil 141. člena ZEKom-1 od operaterjev tudi sprejema obvestila zaradi prekinitev ali napovedanih dograditev, posodobitev ali vzdrževanj omrežij. Z njimi morajo biti primarno seznanjeni uporabniki storitev, agencija pa pri tem izvaja le evidenco in statistiko. V letu 2017 je tako prejela 526 tovrstnih obvestil, pri čemer je bilo prijavljenih 156 okvar, 212 posodobitev, 158 vzdrževanj in 41 dograditev. V primerjavi z lanskim letom beležimo 20 % porast tovrstnih obvestil.

VI. DIREKTIVA O VISOKI RAVNI VARNOSTI OMREŽIJ IN INFORMACIJ

Okvirna direktiva naslavlja le operaterje elektronskih komunikacij. Zaradi vse večje odvisnosti družbe in gospodarstva od informacijsko – komunikacijskih tehnologij ter porasta kibernetskega kriminala pa je bilo nujno, da se zagotovi visoko raven varnosti omrežij in informacij tudi na drugih vitalnih delih družbe in gospodarstva, ne samo na strani operaterjev elektronskih komunikacij. Leta 2016 je bila tako sprejeta Direktiva o ukrepih za zagotavljanje visoke ravni varnosti omrežij in informacij v Uniji (Direktiva EU 2016/1148/ES – v nadaljevanju: NIS Direktiva). NIS Direktiva je stopila v formalno veljavo z avgustom 2016, do 9. maja 2018 pa mora biti prenesena v lokalno zakonodajo. Z njo Komisija naslavlja izvajalce bistvenih storitev ter

ponudnike digitalnih storitev, ki morajo sprejeti ustrezne ukrepe za obvladovanje varnostnih tveganj. Enako kot morajo operaterji poročati pomembne varnostne dogodke agenciji, morajo tudi izvajalci bistvenih storitev in ponudniki digitalnih storitev priglasiti resne incidente nacionalnim pristojnim organom. Diskrecijska pravica vsake države je, da določi izvajalce bistvenih storitev s področja energetike, transporta, bančništva, infrastrukture finančnega sektorja ter zdravstva. Le-te mora država določiti do maja 2018. Druga veja NIS Direktive se nanaša na ponudnike digitalnih storitev kot so platforme za e-trgovanje, portali za spletna plačila, družabna omrežja, iskalniki, računalniške storitve v oblaku ter prodajalne z aplikacijami.

Slovenija prenaša NIS Direktivo z Zakonom o informacijski varnosti (v nadaljevanju: ZIV), ki je trenutno (april 2018) v javni obravnavi. Poleg že omenjenih zavezancev ZIV naslavlja tudi izvajalce bistvenih storitev, ki delujejo v sistemu varstva pred naravnimi nesrečami, obrambe in notranje varnosti, ki morajo sprejeti potrebne organizacijske, logično-tehnične in tehniške ukrepe, s katerimi lahko zagotovijo celovitost, zaupnost in razpoložljivost omrežja in informacijskih sistemov. V javnem posvetovanju je tudi Zakon o kritični infrastrukturi, ki dopolnjuje varnost informacijsko-komunikacijskih sistemov v državi. Kot že ime samo pove, zakon naslavlja vso kritično infrastrukturo Republike Slovenije in potrebne ukrepe, ki bodo omogočali učinkovito zagotavljanje neprekinjenosti in celovitost delovanja.

VII. EVROPSKI ZAKONIK O ELEKTRONSKIH KOMUNIKACIJAH

Regulatorni okvir elektronskih komunikacij je bil nazadnje posodobljen leta 2009. V tem času se je sektor v marsičem spremenil in preobrazil. Povezljivost do javnih komunikacijskih omrežij je praktično že povsod zagotovljena, bodisi preko fiksnih ali mobilnih omrežij. Zaradi povečane konkurence na trgu se povečuje hitrost dostopa, kot tudi nabor in kakovost storitev. Tako potrošniki kot gospodarstvo čedalje bolj odvisni od podatkov in internetnega dostopa, klasična telefonija pa predstavlja le eno od množice storitev na trgu. Vse prisotna povezljivost je omogočila prihod ponudnikov OTT[2] storitev (angl. Over-the-top), ki postajajo resna konkurenca obstoječim ponudnikom. Le-ti ponujajo širok nabor aplikacij in storitev preko interneta, ki vključuje tako govorne kot oblačne storitve ter komunikacijo in storitve ljudi z napravami in med napravami (M2M/IoT). Prav tako delovanje omrežja in njegovih funkcij vedno bolj prevzemajo virtualizirane programske rešitve (SDN/NFV), ki bodo pomembno vplivale na varnost, celovitost in razpoložljivost omrežij in storitev. Vse te in še druge spremembe narekujejo posodobitev regulatornega okvirja, ki je sedaj predstavljen v novem Evropskem zakoniku o elektronskih komunikacijah (European Electronic Communication Code – EECC), v nadaljevanju Evropski zakonik). Le-ta je v svojem predlogu poenoten z NIS Direktivo, Evropsko direktivo o zasebnosti in elektronski komunikaciji (angl. e-Privacy Directive) in Splošno Uredbo o varstvu podatkov (angl. General Data Protection Regulation - GDPR). EECC nadalje združuje skupaj prej štiri ločene direktive. To so: Okvirna direktiva, Direktiva o dostopu, Direktiva o odobritvi in Direktiva o univerzalni storitvi.

Ena od pomembnejših sprememb v povezavi z zagotavljanjem varnosti je nova definicija elektronskih komunikacijskih storitev. Ta po novem vključuje: internetni dostop, storitve, ki v celoti ali delno temeljijo na prenosu signalov in medosebne komunikacije. S terminom medosebne komunikacije (angl. Interpersonal communications) Komisija želi naslavljati elektronske komunikacijske storitve, ki omogočajo medosebno in interaktivno izmenjavo informacij. Le-te temeljijo bodisi na javnih telefonskih številkah iz nacionalnega ali mednarodnega številskega prostora ali pa so od njih popolnoma neodvisne. Vključuje tradicionalne govorne storitve, storitve pošiljanja sporočil, skupinske pogovore in podobno ter uporabljajo javno komutirano ali paketno IP omrežje. Ker se pomembnost medosebnih komunikacij povečuje, je treba tudi zagotoviti, da zagotavljanje varnosti teh komunikacij odraža njihovo specifično vlogo v družbi ter ekonomski vpliv. Ponudniki tovrstnih storitev bodo zato morali z novim Evropskim zakonikom zagotavljati ustrezno raven varnosti glede na nivo tveganja, ki ga vnašajo. Ker ponudniki medosebnih komunikacij (še) ne morejo vplivati na sam prenos signalov preko omrežij, je načeloma tudi nivo tveganja nižji kot pri tradicionalnih komunikacijskih storitvah, zato bodo lahko varnostno zahteve nižje kot pri tradicionalnih ponudnikih. Z novim Evropskim zakonikom se obveznosti ponudnikov javnih komunikacijskih omrežij in storitev z vidika zagotavljanja primerne in proporcionalne ravni varnosti bistveno ne spreminjajo. Termin zagotavljanja varnosti omrežij in storitev sicer po novem ne vključuje samo zagotavljanja njihove celovitosti, temveč vključuje tudi zagotavljanje razpoložljivosti, zaupnosti in avtentičnosti. Z vidika poročanja pa je v Evropskem zakoniku nova obveznost in sicer bo moral ponudnik ob vsakem incidentu regulatornem organu podati oceno vpliva incidenta na gospodarstvo (% izgube BDP) ter družbo in njene aktivnosti (vpliv na subjekte, ki upravljajo s kritično infrastrukturo, nujne storitve, tveganje za javno varnost,...). Ponudniki bodo morali tudi obvestiti svoje končne uporabnike o incidentu, jih seznaniti s tveganjem in kakšne morebitne zaščitne ukrepe bi morali sprejeti, po potrebi tudi zagotoviti šifriranje komunikacije od konca do konca.

VIII. ZAKLJUČEK

Zagotavljanje visoke ravni informacijske in komunikacijske varnosti v širšem pomenu je zmožno toliko, kot njegov najšibkejši člen, zato bo potrebno varnostne mehanizme, kot jih naslavljajo varnostni standardi, vpeljati v vse ključne člene infrastrukture, vključno z elektronskimi komunikacijami. Večina večjih in zrelejših operaterjev se tega zaveda, zato z organizacijskimi in tehničnimi ukrepi tveganja že naslavlja in jih umešča med svoje pomembne upravljavske procese.

LITERATURA

[1] Zakon o elektronskih komunikacijah, (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US in 81/15, 40/2017) - neuradno prečiščeno besedilo ZEKom-1)

[2] Splošni akt o varnosti omrežij in storitev ter delovanje v izjemnih stanjih (Ur. l. RS, št. 75/13 in 64/15) - neuradno prečiščeno besedilo

[2] OTT – Over-The-Top

[3] Direktiva 2009/140/ES Evropskega parlamenta in Sveta z dne 25. novembra 209, http://www.akos-rs.si/files/APEK_eng/Legislation/l-33720091218sl00370069.pdf
[4] ENISA, Technical guideline on Security Measures, https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[5] ENISA, Technical guideline on Incident Reporting, https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
[6] EPRS, European Parliamentary Research Service, The new European electronic communications code, dosegljivo na: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/593562/EPRS_BRI(2016)593562_EN.pdf
[7] ENISA: Shortlist of networks and information security standards: https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards/view

UPORABLJENE KRATICE

Kratica	Angleški pomen	Slovenski pomen
EECC	European Electronic Communications Code	Evropski zakonik elektronskih komunikacij
IoT	Internet of Things	Internet stvari
GDPR	General Data Protection Regulation	Splošna uredba o varstvu podatkov
M2M	Machine-to-machine	Stroj - stroj
NIS (Directive)	The Directive on security of network and information systems	Direktiva o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji
NFV	Network Functions Virtualization	Virtualizacija omrežnih funkcij
OTT	Over-the-top	Povrhnje storitve
SDN	Software Defined Networks	Programsko definirano omrežje
SUNP	Business Continuity management System	Sistem neprekinjenega poslovanja
SUVI	Information Security Management System	Sistem upravljanja varovanja informacij

Urban Kunc dela na Agenciji za komunikacijska omrežja in storitve RS v Sektorju za nadzor operaterjev. Ukvarja se s tehničnimi vprašanji regulacije in nadzora operaterjev elektronskih komunikacij. Sodeluje v mednarodnih ekspertnih skupinah s področja varnosti (ENISA Article 13a), omrežne nevtralnosti (BEREC Net Neutrality EWG) in storitve klica v sili 112. V svojem prostem času v okviru Zavoda go6 in Slovenskega foruma omrežnih strokovnjakov (SINOG) organizira konference in delavnice s področja omrežnih tehnologij.

Nadzor ali svoboda?

Tony Štupar, Katja Mohar Bastar, SOEK

Povzetek — Ta članek opisuje, kako se je v slovenskem telekomunikacijskem prostoru oblikoval koncept nevtralnega interneta, razvoj prakse regulacije, kaj nam prinaša prihodnost, kakšne so potrebe tehnološkega razvoja in kakšna regulacija bi po mnenju operaterjev bila res potrebna.

Ključne besede — 5G, regulacija, nevtralnost interneta, zero-rating, investicije.

Abstract — This paper describes the formation of the net neutrality principles in the Slovenian telecommunications sector, development pf the regulatory practices, outlook for the future, the requirements for implementation of the technological progress and the type of regulation which is in view of operators appropriate.

Keywords — 5G, net neutrality, regulation, zero-rating, investment.

I. UVOD

Telekomunikacije predstavljajo enega izmed stebrov digitalizacije, na katerem se s kompetencami razvijajo storitve industrije 4.0, zato bo nujno zagotoviti, da bodo ukrepi regulacije sorazmerni dejanskem stanju na trgu, da bo regulacija dejansko delala za javni interes, ki je med drugim interes državljana, da bo imel napredne storitve in da bo živel v napredni in bogati državi prihodnosti. Stihijska, populistična in dogmatična regulacija je z navedenimi cilji v nasprotju.

II. POVEZAVA MED INTERNETNO NEVTRALNOSTJO IN 5G

Glede na študijo TNO nujnost mobilnih povezav raste hkrati z rastjo omrežij in storitev. Hkrati pa se razvijajo številna področja našega življenja, kot je mobilnost, transport, zdravje, proizvodnja, mediji in javna varnost.

Vse te storitve pa zahtevajo po meri narejena omrežja z nizkimi zakasnitvami, visoko zanesljivostjo ali majhno energetsko porabo. V trenutnem omrežju 4G operaterji le stežka zadostijo vsem tem zahtevam, ki povzročajo tako tehnične ovire kot visoke stroške. Zato je bila razvita nova generacija mobilnih komunikacij, 5G, ki bo zadostila aplikacijskim potrebam in omogočila mobilnim operaterjem tehnične možnosti za zagotavljanje storitev prihodnosti.

Vendar pa so mobilna omrežja, tudi 5G, podvržena zahtevam Uredbe 2015/2120, ki postavlja pravila nevtralnosti interneta. Na podlagi uredbe je BEREC objavil smernice za njeno implementacijo. Tako uredba kot smernice poudarjata odprt dostop do interneta. V ta namen so oblikovana natančna pravila za zaščito internetnih storitev. Vodilo je, da mora operater, torej ISP, ves promet upoštevati enakovredno, kar pa zanika glavni namen razvoja 5. generacije mobilnih storitev, ki predvideva prilagodljivo povezljivost vertikal in aplikacij. Uredba in smernice postavljajo pravila in posebne pogoje za upravljanje s prometom, diferenciacijo in posebne storitve. Vendar pa industrija intenzivno opozarja na nevarnost zaustavitve inovacij, ki se ne morejo gibati v ozko parametriziranem okolju.

III. RAZVOJ REGULATIVE NA PODROČJU NN

Že Zakon o elektronskih komunikacijah, ki je začel veljati 2013, je Slovenijo postavil na zemljevid borbe za nevtralnost interneta, ki je poleg Nizozemske močno izstopala po zahtevnosti zakonodaje in njenega izvajanja.

Striktna interpretacija pravil je postavila operaterje elektronskih komunikacij v položaj, ko so bili zaradi želje ponuditi svojemu uporabniku storitve na podlagi ne-zaračunavanja prenosa podatkov (zero rating), kar je bilo v svetu močno razširjeno in razen na Nizozemskem tudi sicer nikjer prepovedano, kaznovani zaradi nejasne očitane kršitve. Nejasnost je bila povzročena zaradi odsotnosti neposrednih dokazov kršitev oz. negativnih posledic za trg ali potrošnike. Zakon je bil sprejet 2013, nadzori so se pričeli v letu 2015, ko smo operaterji skozi združenje SOEK pričeli z intenzivnimi pogovori z regulatorjem, javnostjo in predstavniki civilne družbe in argumentirali svoja stališča.

Reakcija operaterjev je bila obrambna. Zavračanje kazni je izhajalo iz strokovnih znanj o neutemeljenosti posega na trg, ki so bila postavljena nasproti ideološkim prepričanjem, saj so bile zero-rated storitve po našem mnenju v korist končnim uporabnikom, katerim se vedno trudimo nuditi kakovostne, uporabne in napredne storitve za nizko ceno, ki jo dirigira konkurenčno okolje. Samo-regulacija, ki jo povzroča konkurenčni pritisk, namreč preprosto pomeni, da bi uporabniki operaterja, ki bi deloval v škodo uporabnikov, preprosto zapustili.

Reakcija ni predstavljala niti zavračanja ustrezne regulacije. Operaterji smo pozdravili usmeritve Evropske komisije iz leta 2015, ki so temeljile na transparentnosti z namenom zagotavljanja hitrega razvoja in inovativnega okolja, s čimer lahko Evropa končno tekmuje z Azijo in ZDA. S takšnim poslanstvom je leta 2015 Evropska Komisija objavila TSM uredbo, ki je uvedla način komunikacije s končnimi uporabniki, ki imajo pravico vedeti, po kakšni oglaševani, maksimalni, dejanski in minimalni hitrosti se jim širokopasovno pretakajo podatki.

IV. NOVE SMERNICE V NAPAČNO SMER

8. marca 2018 pa je v javno posvetovanje smernice, kako naj regulatorji izvajajo uredbo, objavil tudi BEREC. Smernice so zaskrbljujoče: končnim uporabnikom se onemogoča prosta izbira, operaterjem se onemogoča učinkovito upravljanje omrežij za zagotavljanje kakovostnih, varnih in zanesljivih storitev, nekonsistentnost z Uredbo pa je očitna tri leta po njenem sprejetju, ko je večinoma že

implementirana v operaterskih sistemih, hkrati pa predstavljajo ponovno oviranje inovacij na področju 5G.

Predlagatelji regulacije bi morali razumeti, da obstaja veliko število storitev, ki ne predstavljajo storitev množičnega trga za končne uporabnike, pa se vendarle nudijo preko mobilnih omrežij, zato operaterji nujno potrebujejo določeno mero fleksibilnosti, da bi v takšne storitve lahko investirali. Prav tako mora regulacija v korak s časom. Podatkovni promet še vedno strmo narašča. Za učinkovito delovanje omrežij so nujna posodabljanja, kjer pa se bodo v okvirih zahtev smernic izgubile priložnosti za povečano učinkovitost prenosa podatkov.

Investicije, ki se pričakujejo s strani telekomunikacijskih operaterjev, bodisi za izgradnjo optičnega omrežja, nakup frekvenčnega spektra, opreme in postavitve delujočega, kakovostnega, varnega, nevtralnega omrežja, se z vsako zahtevo zgolj povečujejo. Ob zahtevi nevtralnega interneta bi morali regulatorji ponuditi ustrezna orodja ali rešitev za dodatne kapacitete, ki bodo lahko zagotovile nemoten pretok podatkov skozi skorajda pasivno cev, morda – čeprav smo to točko že prestopili, pa vsaj toliko svobode, da bi bilo upravljanje s prometom in načrtovanje omrežij možno brez naročanja pravnih mnenj.

ZAHVALE

Zahvaljujeva se članom SOEK, ki so sodelovali pri pripravi prispevka in zgodovine, ki jo v prispevku opisujeva.

LITERATURA

[1] Dr P.A. Nooren, Dr N.W. Keesmaat, A.H. van den Ende, A.H.J. Norp, 5G and Net Neutrality: a functional analysis to feed the policy discussion, 2018

[2] Evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines, 2018

Kvantni internet

Boštjan Batagelj, Laboratorij za sevanje in optiko, Katedra za informacijske in komunikacijske tehnologije, Fakulteta za elektrotehniko, Univerza v Ljubljani

Povzetek — Besedna zveza »kvantni internet« označuje novo omrežje, kjer se, za razliko od vsem poznanega interneta, informacije prenašajo s pomočjo stanj kvantnih delcev ter se namesto internetnega protokola uporabljajo protokoli, ki so osnovani na fizikalnih zakonitostih iz kvantnega sveta. V kvantnem internetu se za prenos informacije med vozlišči uporablja kvantna komunikacija, kjer je informacija kodirana s pomočjo dvonivojskega kvantnomehanskega sistema – vektorja stanja kvantnega delca, ki ga imenujemo kvantni bit ali krajše kubit. Sedanje internetno omrežje uporablja varnostne mehanizme s klasičnimi kriptografskimi metodami, ki se v celoti zanašajo na zahtevnost matematičnih algoritmov, medtem ko so v kvantnem internetu uporabljeni varnostni protokoli kvantne kriptografije, ki temeljijo na osnovnih lastnostih kvantne mehanike. Izvedbe temeljijo na dejstvu, da kvantnih delcev ni mogoče pomeriti, ne da bi jim pri tem spremenili kvantno stanje, ali na prepletenosti kvantnih stanj dveh delcev. Pri prvem se najpogosteje uporabljata protokola BB84 in B92, v drugem pa protokol E91. Pri metodah za distribucijo kvantnega ključa je, za razliko od klasičnih kriptografskih metod, mogoče razkriti zlonamernega prisluškovalca.

Ključne besede — kvantni internet, kvantna komunikacija, kvantna kriptografija, distribucija kvantnega ključa

Abstract — The phrase "quantum internet" denotes a new network where, unlike the familiar internet, information is transmitted by means of quantum particle states, and instead of the internet protocol, there are new protocols based on physical laws from the quantum world. In the quantum internet, quantum communication is used for the transmission of information between nodes, where information is encoded by means of a two-level quantum-mechanical system, i.e., a quantum-state vector of a quantum particle, called a quantum bit, or a qubit for short. The current internet network uses security mechanisms based on classic cryptographic methods that rely entirely on the complexity of mathematical algorithms, while quantum-cryptography security protocols are based on the basic properties of quantum mechanics. The constructions are based on the fact that quantum particles cannot be displaced without changing their quantum state or the entanglement of the quantum states of the two particles. In the former, the protocols BB84 and B92 are the most commonly used, while in the latter, it is the protocol E91. Unlike conventional cryptographic methods, it is possible to reveal a malicious eavesdropper by using methods for distributing the quantum key.

Keywords — quantum internet, quantum communication, quantum cryptography, quantum key distribution

I. UVOD

Informacijsko komunikacijske tehnologije se pred neavtorizirani zlonamernimi nepridipravi zaščitijo s pomočjo požarnih zidov ali algoritmov umetne inteligence, ki preprečujejo dostop določeni vrsti prometa ali izločajo sumljiv promet na osnovi anomalij. Možnosti, da malopridnež prestreza podatke medtem, ko potujejo med pošiljateljem ter prejemnikom, ter jih bere ali celo spreminja (kali njihovo verodostojnost), se izognemo z uporabo šifriranja podatkov in avtentikacije. Dobro varovanje sporočila ne temelji na tajnosti šifrirnega postopka, temveč na tajnosti šifrirnega ključa, pri čemer je za uporabnika sprejemljiv samo tisti šifrirni postopek, ki je za poznavalca ključa izvedljiv v realnem času. Varnost podatkov, ki se prenašajo in shranjujejo v sodobnih informacijsko komunikacijskih tehnologijah, je zagotovljena predvsem z uporabo matematično zahtevnih šifrirnih algoritmov in ustrezno dolžino šifrirnega ključa. Nepoznavalec šifrirnega ključa kljub uporabi velikih računalniških zmogljivosti ne more izvesti postopka dešifriranja v doglednem času.

Ob pravilni uvedbi težko zlomljivim zaščitnim tehnikam elektronskega šifriranja, ki varujejo podatke na višjem nivoju, zdaj prihaja v dopolnitev kvantno šifriranje, ki omogoča tudi teoretsko nezlomljivo varovanje podatkov na samem fizičnem nivoju s pomočjo kvantne komunikacije. Medtem ko klasično šifriranje uporablja različne matematične metode za zaščito podatkov, kvantno šifriranje temelji na uporabi zakonov kvantne fizike za doseganje absolutne varnosti. S tem vstopamo v kvantno območje telekomunikacij in računalništva, kjer tradicionalni zakoni fizike ne veljajo več, namesto njih pa veljajo zakoni kvantne mehanike. Telekomunikacijske povezave, ki temeljijo na kvantnih komunikacijah za prenos kvantnega ključa, tvorijo novo omrežje, ki ga označujemo z besedno zvezo »kvantni internet«.

Največkrat se kvantna komunikacija ne uporablja za šifriranje sporočil, kot morda zavaja ime. Pošiljanje šifrirnih sporočil je lahko izvedeno prek javnega omrežja. Sam prenos je varen, kolikor je pač varen uporabljen algoritem. Prvotni in osnovni namen kvantnega komunikacijskega kanala je razdeljevanje šifrirnih ključev, pri čemer se za absolutno varno pošiljanje ali izmenjavo uporabijo lastnosti kvantnih delcev.

II. ZGODOVINA KVANTNE FIZIKE

Trenutno poteka, kar nekateri imenujejo, "druga kvantna revolucija". Prva kvantna revolucija se je začela v zgodnjih desetletjih 20. stoletja z odkritjem osnovnih zakonov podatomske realnosti – v katerem se delec iz sveta atomov (kvantni delec) lahko obnaša kot delec ali kot valovanje (dualnost val-delec). Osnovni principi kvantne mehanike so *načelo nedoločenosti* (gibanje delca je nemogoče opisati s tirom), *načelo statističnega opisa* (govorimo lahko le o verjetnosti za dogodke), *načelo nerazločnosti* (ne moremo razločiti dveh delcev enake vrste) in *načelo superpozicije* (vsota dveh različnih rešitev problema je tudi rešitev). Kvantna teorija pravi, da nekatere količine (na primer energija) ne morejo imeti katerekoli vrednosti (da niso zvezne količine), temveč le celo število določenih najmanjših delov, ki jih imenujemo kvanti.

Pionirsko znanstveno delo v prvi kvantni revoluciji so opravili nobelovci Planck, Einstein, Millikan, Heisenberg in Schrödinger. Vse skupaj je začel Max Planck, ki je leta 1900 zapisal postulat, da je elektromagnetno energijo mogoče izsevati v obliki kvantov, ali z drugimi besedami, da je energija lahko zgolj celoštevilski večkratnik osnovne enote – kvanta. [1] Leta 1905 je Albet Einstein pojasnil pojav fotoefekta s pomočjo kvantiziranosti svetlobne energije, kjer je povedal, da z večanjem moči vpadne svetlobe (od določene frekvence dalje) narašča število kvantov energije – fotonov, z večanjem frekvence pa se povečuje energija posameznega fotona. [2] Einsteinovo delo je nadaljeval Robert Andrews Millikan, ki je leta 1914 dokazal kvantno naravo elektronov in določil osnovni električni naboj elektrona ter točno določil Planckovo konstanto. [3] Leta 1927 je Werner Karl Heisenberg zapisal eno od temeljnih načel kvantne mehanike – Heisenbergovo načelo nedoločenosti, ki v kvantni fiziki določa, da je nemogoče istočasno s poljubno natančnostjo poznati določene pare spremenljivk, kot sta na primer lega ali gibalna količina izbranega delca. [4] Pomemben doprinos na področju kvantne mehanike je imel tudi Erwin Schrödinger, ki je znan po razlagi superpozicije z miselnim paradoksom poskusa z mačko in njegovi Schrödingerjevi valovni enačbi. [5] Tehnološko so se začetne ideja uporabile za izdelavo sodobnih elektronskih naprav, kot so elektronska vezja, sončna celica, laser, atomska ura, slikanje z magnetno resonanco in elektronski ter tunelski mikroskop.

V drugi kvantni revoluciji znanstveniki uporabljajo kvantna pravila za osnovne ideje informacijske tehnologije. Mogoče lahko zapišemo, da se je druga kvantna revolucija začela leta 1981, ko je ameriški fizik (tudi nobelovec) Richard Feynman zatrdil, da klasični številski računalniki nikoli ne bodo zmogli v celoti simulirati kvantnih pojavov, in predlagal idejo kvantnega računalnika, ki bi bil tega zmožen. Nedvomno pa je druga kvantna revolucija dobila svoj zagon leta 1994, ko je Peter Shor zapisal najbolj slaven algoritem na področju kvantne informacijske teorije. [6] Z njim je pokazal, da bi kvantni računalniki lahko rešili problem faktorizacije v doglednem času, kar bi omogočilo enostavno razbitje RSA (Rivest–Shamir–Adleman) sheme. Shorov algoritem, ki bi z uporabo nekaj deset tisoč kubitov nalogo faktorizacije opravil v minuti, je povzročil pravo raziskovalno mrzlico in tekmo v postavitvi poskusov, kjer bi s pomočjo kvantne komunikacije na daljavo prenesli kvantni ključ (angl. quantum key distribution – QKD). Zagnanost se v zadnjih letih še stopnjuje, saj je lani Daniel J. Bernstein objavil kvantni algoritem, za katerega trdi, da izvaja faktorizacijo števil še hitreje kot Shorov algoritem. [7]

S pričetkom novega stoletja so raziskovalci postavili nekaj pilotnih omrežij, ki omogočajo prenos kvantnega ključa in uporabljajo kvantne protokole. Leta 2001 je ameriška DARPA (angl. Defense Advanced Research Projects Agency) začela postavljati kvantno omrežje za namene izvedbe varne komunikacije. [8] Omrežje je sestavljeno iz več različnih fizičnih nivojev, ki vsebujejo fazno modulirane laserje in prepletena stanja fotonov ter so fizično izvedena z optičnimi vlakni ali prostozračno optično povezavo. Od leta 2003 do 2008 so številne evropske inštitucije sodelovale na projektu SECOQC (angl. Secure Communication based on Quantum Cryptography), kjer so razvili in na Dunaju postavili omrežje s kvantnimi povezavami, ki uporablja repetitorje in na ta način omogoči prenos kvantnega ključa preko dolgih razdalj. [9] Maja 2009 je bilo na Kitajskem prikazano hierarhično kvantno omrežje, ki ga sestavlja hrbtenično omrežje štirih vozlišč. Hrbtenična vozlišča so preko optične infrastrukture povezana s pomočjo kvantnega usmerjevalnika. [10] V letih med 2009 in 2011 je bilo vzpostavljeno Ženevsko omrežje »SwissQuantum«, ki je povezovalo CERN in Ženevsko univerzo. Namen projekta »SwissQuantum« je bila uporaba tehnologije, razvite v evropskem projektu SECOQC in drugih svetovnih kvantnih omrežij ter prikaz povezovanja kvantnega omrežja z obstoječim telekomunikacijskim omrežjem. [11] Leta 2010 so številne organizacije iz Japonske in Evropske unije postavile in testirale omrežje Tokyo QKD, kjer se je šifriranje izvajalo na dovolj zmogljivi zvezi, da je končni uporabnik lahko uporabljal varne govorne in videokonferenčne zveze. Predhodna omrežja so namreč ločeno prenašale kvantni ključ in koristne podatke. Leta 2013 je bilo Tokijsko omrežje preizkušeno tudi na okoljske spremembe. [12] Septembra 2017 je bila na Kitajskem uradna otvoritev omrežja za prenos kvantnega ključa preko 2000 km med Pekingom in Šanghajem z 32-timi vmesnimi vozlišči, ki ga dopolnjuje tudi prvi kvantni satelit, izstreljen avgusta 2016 z imenom Micius (poimenovan po starem kitajskem filozofu). [13]

III. UPORABA STANJ KVANTNIH DELCEV

Klasično računanje in prenos informacij temeljita na manipulaciji s binarnimi podatki, ki jih predstavljajo biti. Leti lahko zavzamejo eno od dveh diskretnih vrednosti – bodisi logično enico »1« ali logično ničlo »0«. Kvantne informacije uporabljajo kvantne bite ali kubite, ki so v superpoziciji obeh stanj istočasno, kar pomeni, da so hkrati v logičnem stanju »1« in »0«. Ta kombinacija kvantnega stanja je prvi izmed več konceptov, ki tvorijo osnovo druge kvantne revolucije. Kvantni delci torej lahko istočasno obstajajo v več različnih stanjih. Kubit med meritvijo sam "izbere" eno stanje ali drugega – naključno, čeprav je verjetnost odvisna od superpozicije obeh merjenih stanj. Ko je meritev izvedena, se superpozicija uniči in kubit je potisnjen v klasično stanje.

Za lažjo ilustracijo kubitov si je najbolj enostavno predstavljati umišljeno kroglo – tako imenovano Blochovo sfero, ki se v kvantni mehaniki uporablja za opis stanja dvonivojskih sistemov. Točka na krogli predstavlja stanje dvonivojskega sistema. Severni pol predstavlja logično stanje »1«, južni pol pa logično stanje »0«. Danes poznan bit je lahko na enem od dveh polov krogle in lahko zaseda eno ali drugo stanje. Če sta stanji zastopani z enako verjetnostjo, imamo opravka z verjetnostnimi biti (angl. probability bits – pbits). Kubit pa istočasno obstaja na katerikoli točki krogle. Na prvi pogled izgleda, da lahko pri prenosu informacij s pomočjo kubitov prenašamo enormne količine informacij v precej kratkem času, ter da v spomin kvantnih računalnikov lahko shranimo enormne količine informacij in ob tem porabimo veliko manj energije od klasičnih računalnikov. Pričakuje se, da bodo kvantni procesorji precej hitrejši (tudi do milijon krat hitrejši) od današnjih procesorjev, vendar le pri določenih operacijah, kot so faktorizacija in iskanje po seznamu. V resnici so kubiti v obeh logičnih stanjih istočasno, kar pomeni, da bi z enim kubitom zaradi superpozicije stanj prenesli dva klasična bita informacije.

Izvedbo kubita je mogoče doseči s pomočjo različnih kvantnih delcev na več načinov. V ta namen se najpogosteje uporablja polarizacija fotona, koherentno stanje stisnjene svetlobe [14], spin elektrona (spintronika) [15] v

supeprevodnih materialih ali ujete ione v vakumskih kletkah. Kot tehnološko najbolj izvedljivo se kaže, da bi kvantni računalniki uporabljali spine elektronov, medtem ko se bo za prenos kvantnih informacij najverjetneje uporabljala svetloba.

Svetloba je elektromagnetno valovanje, dejansko pa jo lahko obravnavamo kot korpuskularno sevanje, kar pomeni, da je svetloba sestavljena iz fotonov [16] – najmanjši gradnik ali kvant svetlobe. Foton je nedeljiv energijski del, ki se širi s hitrostjo svetlobe v mediju, po katerem potuje, ima nično mirovno maso ter lastno gibalno in vrtilno količino, kar vse mu daje izrazito korpuskularen značaj. Elektromagnetno polje fotona lahko zapišemo na več načinov glede na to, da je valovanje po svoji obliki zelo različno. Polje razvrščamo v rodove, ki so linearno neodvisne rešitve valovodne enačbe. Polje ima smer (polarizacijo), amplitudo, frekvenco in fazo ter določeno rodovno prostorsko porazdelitev.

Omenjene lastnosti svetlobe lahko uporabimo za kvantno komunikacijo oz. kvantno razdeljevanje ključa, pri tem pa ima najpomembnejšo vlogo prav nedeljivost fotona, katerega lastnost je, da je zelo občutljiv na vsak merilni poseg. Iz tega razloga ga vsak zunanji merilni poseg, ki je lahko tudi poskus prisluškovanja na optični zvezi, poruši, pokvari informacijo in izda prisluškovalca. Ker je ključ, kodiran s kvantnim stanjem posameznega fotona, nemogoče identično replicirati, prejemnik z lahkoto ugotovi, ali je bil skrivnostni ključ ukraden. Ta način obema stranema – pošiljatelju in prejemniku – omogoča izmenjavo kode po javnem komunikacijskem kanalu s popolno varnostjo prenosa.

V nasprotju z obstoječimi klasičnimi shemami za razdeljevanje ključa razdeljevanje kvantnega ključa ne potrebuje varnega prenosa, temveč lahko poteka po javnem in popolnoma nevarovanem optičnem omrežju. Izkoriščajo se lahko prostozračne optične povezave ali optične vlakenske zveze, kjer se ključ lahko prenaša preko transportnega optičnega omrežja z multipleksiranjem valovnih dolžin [17] ali preko dostopovnega pasivnega optičnega omrežja [18-19]. Kvantni ključ je ustvarjen neposredno in sočasno pri pošiljatelju in prejemniku. Poleg tega je ustvarjen iz popolnoma naključnih zaporedij, kar je zahtevna naloga pri klasični shemi razdeljevanja ključa.

IV. PRENOS KVANTNEGA KLJUČA S POMOČJO FOTONOV

Izvedbe prenosa kvantnega ključa lahko temeljijo na dejstvu, da kvantnih delcev ni mogoče pomeriti, ne da bi jim pri tem spremenili kvantno stanje, ali pa so osnovane na prepletenosti (ang. entanglement) kvantnih stanj dveh delcev, pri čemer se izkorišča povezanost njunih stanj. Pri obeh se za kvantno stanje fotona lahko uporablja spreminjanje (moduliranje) polarizacije, kvantni protokoli pa so različni. Pri prvem se najpogosteje uporabljata protokola BB84 in B92, v drugem pa protokol E91.

Glede na polarizacijsko stanje fotona ločimo linearno ali krožno polarizirano komunikacijsko metodo. Linearni komunikacijski sprejemni sistem s pomočjo polarizacijskega delilnika enoumno ločuje vertikalno in horizontalno polarizirane fotone, ki se jih zaznava na dveh ločenih detektorjih. Oddan foton je lahko tudi krožno polariziran, pri čemer je krožna polarizacija sestavljena iz dveh linearnih ortogonalnih polarizacij (vertikalne in horizontalne). Če krožno polariziran foton vpade na polarizacijski delilnik, z enako verjetnostjo izmerimo vertikalno oziroma horizontalno polarizacijo, ker ima krožno polariziran foton obe polarizaciji zastopani z enako, 50 odstotno verjetnostjo.

Prvi protokol, ki je bil razvit za kvantno distribucijo ključa, sta predstavila C. Bennett in G. Brassard že leta 1984, po čemer protokol imenujemo BB84. [20] Oddajnik v točki A in sprejemnik v točki B uporabljata izvor posameznih fotonov, kjer je mogoče za vsak foton posebej določiti eno od štirih polarizacijskih stanj. Iz točke A je potrebno najprej poslati v točko B vlak zaporednih fotonov, ki bodo naključno polarizirani glede na izbrane pogoje v oddajniku. Sprejemna naprava v točki B se nastavlja v naključnem zaporedju, kar pomeni, da sta obe linearna (dve stanji) in krožna (dve stanji) metoda zastopani z enako verjetnostjo. Po opravljeni meritvi se iz točke B v točko A sporoči uporabljeno sprejemno sekvenco. Vsakokrat, ko je bila v točki B uporabljena enaka sprejemna nastavitev, kot je bila oddajna, je bit oziroma časovno okno veljavno. Oddajnik seveda ne ve ničesar o prejemnikovih rezultatih merjenja polarizacije, samo posreduje mu, ob katerih časovnih trenutkih je bila uporabljena enaka polarizacijska metoda. Prisluškovalec, ki spremlja promet na javno odprtem kanalu, si ne more prav nič pomagati. Iz zajetih sporočil ne more izvedeti, kakšno polarizacijo je uporabil oddajnik, niti s kakšno polarizacijo je meril sprejemnik ob vsakem časovnem oknu. Pri tem je vredno omeniti še, da na začetku ne sprejemna ne oddajna stran ne vesta, kakšna bo končna vrednost ključa, saj nastane šele po validaciji časovnih oken. Zaradi uporabe posameznih fotonov v oddajnem nizu je ob prisluškovanju nemogoče odkriti ključ. Če je prisluškovalec na kvantnem kanalu pasiven, s svojim merjenjem 'porablja' fotone, kar sprejemnik zazna kot prazna časovna okna, pri aktivnem prisluškovanju pa malopridnež po sprejemu oddaja ponarejene fotone, kar se izraža v nizkem izkoristku protokola (25 % namesto 50 %). Tako se odkrije prisluškovalec, dobljeni rezultati pa se zavržejo. S tem prisluškovalec sicer ne pridobi ključa, otežkoči ali onemogoči pa njegov prenos.

Protokol B92 za kvantno razdeljevanje ključa je leta 1992 predstavil Charles H. Bennett. [21] V nasprotju z njegovim predhodnikom, BB84, pri implementaciji potrebujemo le dve, toda vnaprej določeni polarizacijski stanji na oddajni in sprejemni strani. Razdeljevanje ključa na podlagi protokola B92 je eno najbolj razširjenih, saj je protokol mogoče prirediti za kodiranje bitov s fazo svetlobnega signala, kar je veliko lažje realizirati kot kodiranje s polarizacijo. [22-23] Razdeljevanje ključa poteka tako, da se oddajnik in sprejemnik že vnaprej dogovorita, kakšna dva tipa polariziranih fotonov bosta oddajala. Komunikacijska oprema za izvedbo protokola B92 je identična opremi, uporabljeni pri protokolu BB84, razlika je le v tem, da se pošilja fotone v le dveh mogočih polarizacijskih stanjih. Sprejem je izveden bodisi po linearni bodisi po krožni komunikacijski metodi in zaznan na pravem detektorju. S tem preprostim pravilom se na sprejemni strani sprejetemu bitu takoj preveri veljavnost. Po končanem prenosu se iz sprejemnika sporoči v oddajnik, katera časovna okna so veljavna, s čimer tudi oddajna stran pridobi ključ. Izkoristek izmenjave ključa po protokolu B92 je v idealnem primeru le 25 %, pri protokolu BB84 pa je bil 50 %.

Leta 1991 je Artur Ekert objavil protokol E91, ki temelji na prepletenosti kvantnih delcev. [24] Glavni omrežni element je centralni izvor prepletenih fotonov, ki se ločijo in pošljejo v točko A in točko B. Fotona sta kvantno prepletena,

če sta njuni stanji povezani. Prepletena stanja so popolnoma korelirana. Rezultat posamezne meritve ostaja povsem naključen in posledično nepredvidljiv. Katero od obeh kombinacij bosta strani izmerili, je nemogoče napovedati – vemo le, da sta verjetnosti enaki. Vendar z meritvijo stanja enega fotona pridobimo informacijo o stanju drugega fotona, čeprav je ta prostorsko daleč stran. Foton pred meritvijo ni imel merjenega stanja, temveč ga je šele meritev prisilila v izbiro. Obenem pa je meritev na enem fotonu vsilila tudi drugemu fotonu, da izbere ustrezno stanje. To bi se naj zgodilo v trenutku, kar pomeni, da je mogoče s prepletenostjo podatke pošiljati z nadsvetlobno hitrostjo. Zaradi prepletenosti kvantnih stanj delec v točki B ve rezultat meritve v točki A in se odloči, kako se bo orientiral (bodisi komplementarno glede na izbiro v točki A, bodisi naključno v primeru nekompatibilne baze). Kot kaže, obstaja nekakšno delovanje na daljavo, kar je povsem v neskladju s klasičnimi predstavami o lokalnosti. Kvantno prepletenost je napovedal že Einstein, a tudi sam vanjo ni čisto verjel. Vsakršen poskus prisluškovanja uniči omenjeno korelacijo, kar je mogoče tudi zaznati.

V. INŽENIRSKI SKLEP

V prispevku so opisani postopki prenosa šifrirnega ključa pri kvantnem šifriranju, kjer je varnost vnaprej zagotovljena z naravnimi zakoni kvantne mehanike in omogoča varovanje podatkov na fizični ravni. Kvantno komunikacijo je mogoče osnovati na Heisenbergovem načelu nedoločenosti ali zakonitosti kvantne prepletenosti, pri čemer se uporabljajo različni protokoli za kvantno razdeljevanje ključa. Pri protokolu BB84 so potrebna štiri polarizacijska stanja, kar je tehnološko težje doseči, zaradi česar je zaenkrat bolj praktičen protokol B92, ki ga je mogoče prilagoditi za fazno modulacijo svetlobe.

Praktična inženirska izvedba prenosa šifrirnega ključa s pomočjo Heisenbergovega načela nedoločenosti naleti na kar nekaj težav. Zaradi absorpcije in sipanja se na optični prenosni poti nekaj fotonov naključno izgubi, kar ima za praktično posledico izgubo podatkov. V izogib temu inženirji uporabljajo svetlobne vire, ki generirajo svetlobne impulze, v katerih pa je večje število fotonov. S tem, ko je komunikacija realizirana s svetlobnim impulzom namesto s posameznim fotonom, je v negotovost postavljen pojem absolutne varnosti. Po teoriji se absolutna varnost prenosa zagotovi z dejstvom, da je posamezni foton nedeljiv. Ker impulz fotonov vsebuje več fotonov, le-ta postane deljiv in s tem je varnost postavljena pod vprašaj.

Ob praktični uvedbi se je treba zavedati, da idealni izvori in detektorji posameznih fotonov ne obstajajo. Fotoni prihajajo v fotodiodo naključno s Poissonovo porazdelitvijo. Pravimo, da je fotodetekcija naključen proces, ki se pokorava Poissonovi gostoti verjetnosti. Za številski prenosni sistem, ki se ovrednoti kot razmerje med napačno sprejetimi biti in številom vseh oddanih bitov, mora za sistemsko zahtevo 10^{-9} biti število elektronov v svetlobnem detektorju enako 21, kar predstavlja idealno kvantno mejo sprejema pri 100 % izkoristku sprejemnika. Detektorji posameznih fotonov imajo izkoristek v razredu 10 %. Ob zavedanju te ranljivosti se kažejo kot bolj perspektivne metode kvantne prepletenosti.

Predstavljene praktične implementacije nakazujejo razvoj v smeri množične uporabe kvantnih komunikacij, k čemur pričajo tudi standardizacijske aktivnosti [25], ki bodo na področju kvantnih komunikacij vzpostavile red in združljivost tehnologij, kar bi omogočalo lažje nadgrajevanje obstoječih in na novo postavljenih omrežij kvantnega interneta.

LITERATURA

[1] "The Nobel Prize in Physics 1918". Nobelprize.org. Nobel Media AB 2014. Web. 2 May 2018. http://www.nobelprize.org/nobel_prizes/physics/laureates/1918/

[2] "The Nobel Prize in Physics 1921". Nobelprize.org. Nobel Media AB 2014. Web. 2 May 2018. http://www.nobelprize.org/nobel_prizes/physics/laureates/1921/

[3] "The Nobel Prize in Physics 1923". Nobelprize.org. Nobel Media AB 2014. Web. 2 May 2018. http://www.nobelprize.org/nobel_prizes/physics/laureates/1923/

[4] "The Nobel Prize in Physics 1932". Nobelprize.org. Nobel Media AB 2014. Web. 2 May 2018. http://www.nobelprize.org/nobel_prizes/physics/laureates/1932/

[5] "The Nobel Prize in Physics 1933". Nobelprize.org. Nobel Media AB 2014. Web. 2 May 2018. http://www.nobelprize.org/nobel_prizes/physics/laureates/1933/

[6] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), IEEE Computer Society Press (1994), 124-134.

[7] D. J. Bernstein, N. Heninger, P. Lou, L. Valenta, "Post-quantum RSA", PQCrypto 2017.

[8] Chip Elliott, "The DARPA Quantum Network", Quantum Physics, 2004.

[9] Raziskovalni projekt SECOQC na spletu, http://www.secoqc.net/ (dostopano 5. 5. 2018)

[10] Fangxing Xu et al. "Field experiment on a robust hierarchical metropolitan quantum cryptography network", Chinese Science Bulletin, vol. 54, no. 17, pp. 2991–2997, July 2009.

[11] D. Stucki, M. Legre et al. "Long-term performance of the SwissQuantum quantum key distribution network in a field environment". New Journal of Physics, vol. 13, no. 12, 2011.

[12] K. Shimizu et al., "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," JLT, vol. 32, no. 1, pp. 141-151, 2014.

[13] Rachel Courtland, "China's 2,000-km quantum link is almost complete", IEEE Spectrum, Vol. 53, No. 11, pp. 11-12. 2016.

[14] Osamu Hirota, "Squeezed light", Elsevier, 1992.

[15] V. Sverdlov et al., "Spintronics as a Non-Volatile Complement to Modern Microelectronics", Inf. Midem, Vol. 47, No. 4. pp. 195-210, 2017.

[16] J. Budin, "Optične komunikacije – z osnovami optike", Fakulteta za elektrotehniko, Ljubljana, 1998, str. 71-82.

[17] M. Vidmar, "Optical-fiber communications: components and systems", Informacije Midem, Vol. 31, No. 4. pp. 246-251, 2001.

[18] B. Batagelj, "Pasivno optično dostopovno omrežje s časovnim razvrščanjem", Ljubljana: Založba FE in FRI, 2011.

[19] S. Aleksic et al., "Quantum key distribution over optical access networks," NOC-OC&I, Graz, 2013, pp. 11-18, 2013.

[20] C.H. Bennet, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, Indija, str. 175-179, 1984.

[21] C. H. Bennet, "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, Vol.68, str. 3121-3124, 1992.

[22] O. L. Guerreau, et al., "Longdistance QKD transmission using single-sideband detection scheme with WDM synchronization", IEEE J. Sel. Top. Quantum Electron., vol. 9, št. 6, str. 1533-1540, 2003.

[23] Jurij Tratnik, Boštjan Batagelj, "Predstavitev ideje kvantnega šifriranja in pregled osnovnih tehnik kvantnega razdeljevanja ključa", Elektrotehniški vestnik, vol. 75, no. 5, pp. 257-263, 2008.

[24] Artur K. Ekert, "Quantum cryptography based on Bell's theorem", Physical review letters, vol. 67, no. 6, pp. 661-663, 1991.

[25] ETSI White Paper, "Quantum Safe Cryptography and Security", 2015

Boštjan Batagelj je docent na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer predava predmete satelitske komunikacije in navigacija, optične komunikacije in radijske komunikacije. Raziskovalno delo opravlja v Laboratoriju za sevanje in optiko, kjer se med drugim ukvarja s fizičnim nivojem prenosnih in dostopovnih telekomunikacijskih omrežjih, zasnovanih na radijski in optični tehnologiji. Je avtor več kot 300 člankov, osmih patentnih prijav in sodeluje v domačih ter mednarodnih raziskovalnih projektih s področja optičnih in radijskih komunikacij.

Varnost na področju DevOps - že v fazi načrtovanja

Mojca Ciglarič, Fakulteta za računalništvo in informatiko, Univerza v Ljubljani

Povzetek — Na področju DevOps je bila varnost v začetku bolj obrobnega pomena. Ko pa je začela prodirati na površje, se je moral izraz DevOps razširiti v DevSecOps. Pojasnili bomo, kaj pomeni ta nova kratica in kako se povezuje s principi sistemov, varnih že od faze zasnove dalje (security by design).

Ključne besede — devOps, devSecOps, varnost v zasnovi

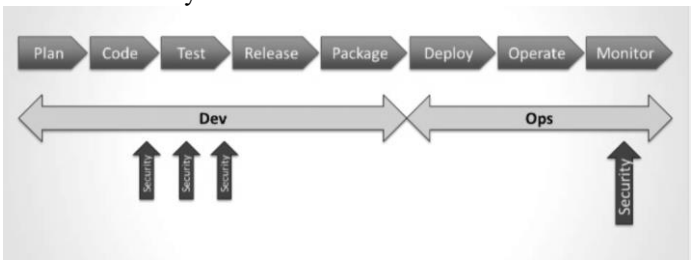
Abstract — In a DevOps area, security did not use to be the most important issue. However now things have changed, DevOps gained a new branch called DevSecOps and we hope for a new generation of secure systems as a result. In the paper we explain how DevSecOps relates to the paradigm Security by Design and what does it mean practically.

Keywords — devops, devSecOps, security by design

I. UVOD

Skovanka "DevOps" je v zadnjem času vseprisotna. Pomeni nov profil v računalniški industriji, naj bo vmesni člen ali hibrid med razvijalcem in sistemskim inženirjem, ki poskrbi za avtomatizacijo in orkestracijo. Če smo v preteklosti naleteli na situacije, ko je za slabo delovanje aplikacije programer krivil sistemska inženirje, ki niso znali primerno pripraviti infrastrukture, sistemski inženir pa razvijalce, ker niso znali napisati aplikacije tako, da bi optimalno izkoriščala razpoložljive vire, je DevOps dvoživka, ki razume obe strani, razvijalsko in sistemsko, in poskrbi, da do opisane težave ne more priti. Drugače povedano, je potrebno že ob začetku načrtovanja programske opreme razmišljati o tem, na kakšni infrastrukturi bo tekla. Pri načrtovanju infrastrukture pa, kakšne platforme in aplikacije bo podpirala.

Vendar pa kratica DevOps ni samo to. Pomeni tudi gibanje in naravnanost IT podjetij, ki želijo pri svojih izdelkih in v svoji organizaciji doseči presežke tako v kakovosti izdelkov kot tudi v kakovosti odnosov in poslovnih rezultatih in se zato ne bojijo postavljati novih trendov, preizkušati novih modelov in vzpostavljati inovativnih procesov. Prednosti so otipljive: manj trenj in večja kohezija v razvojnih timih, hitrejši razvojni cikli in večja kvaliteta izdelkov. Vodilni principi so agilnost, avtomatizacija, trajne izboljšave in preizkušanje novih idej, zanesljivost in razpoložljivost, v zadnjem času pa se vedno glasneje poudarja tudi varnost. Tako močno poudarja, da se je skovanka DevOps razširila v DevSecOps. »Sec« v sredini seveda predstavlja angleško besedo Security, varnost. Po istem načinu razmišljanja, kot smo prišli do dvoživke med razvijalcem in sistemskim administratorjem, ugotavljamo, da je potrebno tudi na varnost misliti že ob začetku načrtovanja programske opreme. Torej potrebujemo nov profil dvoživke, ki bo varnostni strokovnjak in bo delal v razvojni ekipi. Z njegovo pomočjo bomo varnost na sliki razvojnega cikla, kjer si faze sledijo od leve protu desni, pomaknili bolj v levo. To ponazarja novo paradigmo na področju varnih sistemov »shift left«. Po mantri »shift left testing« (premik testiranja že v začetne faze razvoja programske opreme) je v drugi polovici leta 2017 bloge in webinarje preplavila njena nova različica, »shift left security«.



Slika 1: Premik varnosti v levo v življenjskem ciklu. Vir: SANS / Qualys [6].

II. VARNOST ŽE V FAZI NAČRTOVANJA

Izraz varnost nam lahko pomeni veliko različnih stvari, med katere na področju razvoja programske opreme štejemo zlasti trajno pripravljenost aplikacije, da zagotovi ustrezen nivo zaupnosti, integritete pri hranjenju podatkov in razpoložljivosti takrat, ko jo uporabnik potrebuje.

Varnost tradicionalno ni bila nujno zajeta v fazi načrtovanja produkta. Morda se nanjo kdaj pomisli in se zajame v fazi načrtovanja najbolj očitne vidike varnosti, na primer uporabo digitalnih potrdil pri vstopu v spletno banko. Celostno načrtovanje varnosti pa je bilo nekoč razen redkih izjem prepuščeno procesu krpanja nekje v zadnjih fazah razvojnega cikla ali celo v razvoj druge ali tretje izdaje produkta, po načelu »Naredimo najprej glavno funkcionalnost, bomo že potem dodali varnost.«Tudi v zagonskih podjetjih, kjer je močno gonilo čim hitrejši vstop na trg, razmišljanje o varnosti redko srečamo v zgodnjih fazah načrtovanja izdelkov.

Izkušnje iz večjih podjetij pa kažejo, da se prav na področju varnosti najbolj obrestuje proaktivnost, torej vključevanje varnosti že v zasnovo z mislijo na končni izdelek. V nasprotju z reaktivnostjo, ki pomeni krpanje lukenj in odgovarjanje na obstoječe napade, proaktivnost prinaša zaščito izdelka po vsej površini.

Organizacija OWASP (The Open Web Application Security Project), neprofitna organizacija, ki se ukvarja z dvigom stopnje varnosti programskih izdelkov, že več kot 15 let razvija in dopolnjuje vodič za razvoj varnejših programov, OWASP Development Guide. Ta vodič vsebuje glavne principe varnega pristopa že v fazi načrtovanja, ki jih navadno imamo v mislih, ko rečemo "Security by Design". Morali bi jih že vsi poznati, pa jih vseeno na kratko ponovimo:

1. Zmanjševanje površine napada. (Vsaka nova funkcionalnost pomeni potencialno površino napada. Primer: če neko polje za vnos podatkov lahko uporablja vsakdo, je verjetnost za napad SQL injection večja, kot če ga lahko uporabljajo samo avtenticirani uporabniki. Če lahko podatke pridobimo drugod in vnosno polje umaknemo, pa smo to površino napada minimizirali).
2. Varne privzete nastavitve (privzete nastavitve lahko uporabnik spreminja in če želi, nastavi tudi manj varno)
3. Čimmanj privilegijev (uporabnik ima dovoljenja za dostop le do tistih virov in v tolikšni meri, kot ga res potrebuje za svoje delo)
4. Obramba v globino (več kontrol, ki zmanjujejo tveganja z različnih vidikov, je bolje kot ena sama)
5. Varen neuspeh (ang. secure fail): v primeru napak se mora aplikacija obnašati varno.
6. Ne zaupajmo storitvam: zunanje storitve oziroma storitve zunanjih ponudnikov – glede na to, da so zunaj našega nadzora, jim ne smemo zaupati in jih moramo obravnavati kot potencialen vir napada.
7. Ločevanje dolžnosti/odgovornosti (ang. segregation of duties): uporabniki naj imajo zgolj uporabniške pravice, upravitelji pa zgolj upravljalske. Uporabnik ni hkrati tudi upravitelj.
8. Izogibanje tančicam skrivnostnosti (ang. security by obscurity): s skrivanjem uporabljenih varnostnih metod in mehanizmov se varnostni nivo zvišuje le navidezno. Resnično varnost dosežemo z njihovo pravilno uporabo, ne s skrivanjem.
9. Preprostost: preveč kompleksne sisteme težko razumemo, težko vzdržujemo in površina napada je velika. Kjer le moremo, se držimo poenostavljanja.
10. Korektno reševanje in odpravljanje varnostnih težav: za mnoge varnostne težave obstajajo preizkušene rešitve in vzorci (ang. design patterns). Tudi če se zdi takšna rešitev zahtevna v primerjavi s hitro improvizacijo, se na dolgi rok bolj izplača.

i. Startup pristop k varnosti

Ne želimo posploševati, vendar pa je za zagonska (ang. startup) podjetja značilno, da želijo s svojim produktom čimprej na trg, da ga trg preizkusi in bodisi čimprej sprejme, bodisi zavrne. Za trg se šteje primeren že minimalno delujoč izdelek, ki ga bomo že kasneje izpilili, če ga seveda trg sprejme. Če ga ne, pa vsaj nismo vanj vložili preveč dela. Tak izdelek se popularno imenuje “MVP” – Minimum Viable Product. Seveda si v množici minimalnih zahtev, ki jih mora izpolnjevati tak MVP, varnostne zahteve le težko priborijo svoje mesto. Posledica je vztrajno ohranjanje dinamike razvoja, kjer se varnost v izdelek dodaja šele v zadnjih fazah, ko se temu res ne moremo več izogniti.

Zakaj je to slabo? Tako kot v fazi načrtovanja zasnujemo aplikacijsko arhitekturo, je potrebno enako zgodaj zasnovati tudi varnostno arhitekturo produkta. Varnostna arhitektura zagotavlja aplikaciji temeljne mehanizme, s katerimi ta lahko izpolni funkcionalne zahteve s področja varnosti: zaupnost podatkov, integriteto podatkov, zagotovitev dostopnosti do podatkov za upravičene uporabnike – in le zanje – takrat, ko jih ti potrebujejo. Tako kot stavbi ne moremo dozidati temeljev naknadno, tako tudi programskemu produktu ne moremo naknadno določati arhitekture, saj bi to pomenilo nesorazmeren napor ali stroške.

ii. Varnost v Internetu stvari

Internet stvari je področje, ki je v zadnjih letih doživelo eksploziven napredek. Poleg tehnološkega razvoja je pomemben tudi politični potisk, saj področje spodbujajo močni akterji, industrija, Evropska skupnost, telekomunikacijski sektor in podobno. V borbi za vodilna mesta na vlaku IoT so organizacije sprejemale določene kompromise, ki so varnost potisnili v drugi plan in posledično so prve IoT platforme in izdelki nepopravljivo varnostno zanemarjene. Ker gre v številnih implementacijah za prototipe na področjih, kjer varnost ne more biti kompromis (avtomobilska industrija, energetika, telekomunikacije, ipd.), so se kmalu zaslišali glasni pozivi k sistematičnem izboljševanju kakovosti na vseh stopnjah, od razvoja in gonilnikov za najpreprostejše senzorje, do zahtevnih platform in integracijskih vmesnikov.

III. NOVE POBUDE NA PODROČJU NAČRTOVANJA VARNOSTI

Na srečo ni ostalo le pri pozivih, ampak se je področje dejansko že začelo urejati. Kot primer si bomo v nadaljevanju pogledali poročilo »Secure by Design: Improving the Cybersecurity of Consumer IoT«, ki ga je izdalo britansko ministrstvo za digitalizacijo 29. marca 2018. Dokument je del uresničevanja britanske varnostne strategije, ki ima za cilj, da država postane najbolj varna na svetu za življenje in posel. Področje IT znotraj te strategije zavzema opazno in pomembno mesto. Pristop k reševanju varnostne problematike zavzema popolnoma novo stališče, ki uporabnike razbremenjuje skrbi za varnost tako, da pričakuje vgradnjo varnosti in transparentnosti že na sistemskem nivoju.

Poleg pregleda priložnosti in tveganj na področju IoT ter zavzemanja za paradigmo varnosti že v fazi načrtovanja omenjeno poročilo prinaša osnutek vodil »Code of Practice«, ki predstavljajo skupek trinajstih izhodišč za varno zasnovo sistemov. Ta kodeks naj ne bi nadomestil številnih standardov in varnostnih priporočil, ki jih pripravljajo razna strokovna združenja in mednarodne organizacije, ampak predstavlja skupen okvir, v katerega se le te lahko umeščajo. Poglejmo si teh 13 vodil:

1. Ni privzetih gesel. Vsako geslo mora nastaviti uporabnik sam in ni načina, da se ga ponastavi na neko privzeto vrednost.
2. Vzpostaviti politiko za razkrivanje ranljivosti. Vsa podjetja, ki izdelujejo IoT produkte, morajo imeti javno objavljeno vstopno točko, kamo lahko raziskovalci ali druge zainteresirane osebe javijo odkrite ranljivosti njihovih produktov.
3. Nadgradljiva programska oprema (poprodajne nadgradnje). Vsaka programska oprema mora imeti enostavno možnost zamenjave ali nadgradnje, saj le tako lahko poskrbimo za varnostne popravke in odpravo ranljivosti. Konec življenjske dobe in s tem podpore je

treba najaviti dovolj vnaprej, nenadgradljive komponente pa mora biti možno izolirati ali zamenjati.

4. Varna hramba gesel, ključev, inicializacijskih vektorjev in drugih varnostno občutljivih podatkov. Ti podatko morajo biti shranjeni v varni, zaupanja vredni shrambi na napravi ali znotraj storitve, nikakor pa ne smejo biti zakodirani v programsko kodo.
5. Varna komunikacija, zlasti za varnostno občutljive vsebine. Komunikacija, tudi ko gre na primer za oddaljeno upravljanje in nadzor, mora biti kriptirana z dovolj močno kriptografsko metodo, s ključi pa je potrebno upravljati v skladu z dobrimi praksami.
6. Zmanjševanje površine napada (čim manj privilegijev, vrata (port), ki se ne uporabljajo, naj bodo zaprta, dostop do sistema le kadar je to potrebno, na voljo le tiste storitve, ki se dejansko uporabljajo, program naj nima nepotrebnih dovoljenj »za vsak primer«...)
7. Preverjanje integritete programske opreme: vsako nadgradnjo, novo namestite, pa tudi obstoječo programsko opremo mora biti možno v vsakem trenutku preveriti z vidika njene celovitosti in pristnosti. Če je zaznana težava, mora naprava to takoj javiti administratorju, pri tem pa se ne sme vključiti v omrežje bolj, kot je potrebno za to obvestilo.
8. Zaščita osebnih podatkov v skladu z zakonodajo. Če naprave in storitve obdelujejo osebne podatke, morajo biti pridobljeni pravilno in zakonito, uporabnik pa mora biti obveščen o tem, katere podatke se zbira ter kako in zakaj se uporabljajo. Imeti mora tudi enostavno možnost, da jih kadarkoli umakne.
9. Sistemi naj bodo odporni na izpade. Marsikateri IoT sistem je varnostno kritičen ali pa celo življenjsko pomemben (sistemi za varnostni nadzor, medicinski sistemi). V primeru napada ali nujnih varnostnih popravkov tak sistem ne sem postati niti za kratek čas nerazpoložljiv, zato je že od začetka načrtovanja potrebno planirati ustrezno redundanco in druge mehanizme za zviševanje odpornosti.
10. Nadzor podatkov, ki se zbirajo (telemetrija, monitoring, promet...). Sistemi, ki s pomočjo oddaljenih senzorjev zbirajo večje količine različnih podatkov (telemetrija), naj jih tudi sproti pregledujejo in preverjajo morebitne anomalije, saj so te pogosto prvi znak varnostnega incidenta. Tako lahko morebitne težave zaznamo že zgodaj, s tem zmanjšujemo varnostno tveganje in posledice napada.
11. Brisanje osebnih podatkov z naprav naj bo uporabnikom enostavno. Če uporabnik napravo ali storitev preneha uporabljati, mora imeti na voljo jasna navodila, kako odstraniti iz sistema vse svoje osebne podatke.
12. Namestitev in vzdrževanje naprav in storitev naj bosta za uporabnika jasna in enostavna, vsebujeta minimalno število potrebnih korakov in sledita dobre prakse s področja uporabnosti (ang. usability).
13. Preverjanje vhodnih podatkov. Za vse podatke, ki se prenašajo med omrežji, napravami in storitvami, prek uporabniških ali aplikacijskih vmesnikov, je potrebno zagotoviti preverjanje in shraniti in procesirati le tiste podatke, ki so preverjeno veljavni. To zagotavlja, da sistema ni možno onesposobiti z injektiranjem napačno oblikovanih podatkov.

Vidimo lahko, da se vodila v nezanemarljivi meri ujemajo s priporočili OWASP, ki smo jih povzeli v začetku članka in ki so z nami že kako desetletje. Kljub temu smo bili v marsikaterem IoT sistemu priča banalnim varnostnim pomanjkljivostim, ki bi se jim zagotovo izognili, če bi ta priporočila dejansko upoštevali.

IV. Stanje v Sloveniji

V Sloveniji se na področju varnosti srečujemo z velikim pomanjkanjem varnostnih strokovnjakov. Nimamo niti primernega študija, ki bi zainteresirane študente izobrazil v tej smeri, država pa kljub nekaterim pobudam ne kaže namenov, da bi financirala tak študij. Kadrovskega primanjkljaja ne zaznavajo le IT podjetja, ampak je to tudi eno od ključnih treh področij pobude Digitalna Slovenija. Tudi v strategiji pametne specializacije imamo kot ključno navedeno področje kadrov, vendar pa je pri pripravi akcijskih načrtov država izobraževalne aktivnosti izločala iz načrtov.

Skupne Strategije kibernetske varnosti nimamo, pravzaprav imamo štiri ločene strategije, ki jih pripravljajo akterji različnih ministrstev in uradov. ZVOP-2 (še) ni bil sprejet in na področju ravnanja z osebnimi podatki se viša napetost pred skorajšnjim začetkom uporabe uredbe GDPR. Redka podjetja z vrhunskimi varnostnimi strokovnjaki so preobremenjena, obenem pa ne dobijo ustrezno izobraženih svežih kadrov. Glede na povedano je jasno, da področje varnosti sicer lahko razumemo, vendar bomo imeli težave, preden bomo opisane principe lahko resnično začeli uporabljati v praksi na način, da bomo dosegli kritično maso.

V. Zaključek

V članku smo pojasnili nekatere aktualne pojme, ki se danes povezujejo s področjem kibernetske varnosti. Opisali smo gibanje DevOps in naraščajočo vlogo varnosti znotraj njega, ter razmišljanje o vlogi in mestu varnosti v razvoju izdelkov privedli do paradigme »varnost v načrtovanju« oziroma angleško Security by Design. Povzeli smo vodila, ki jih je treba upoštevati za varno načrtovane izdelke, obenem pa izpostavili problematiko, s katero se ob tem soočamo v Sloveniji. Brez sistematičnih vlaganj v ozaveščanje uporabnikov in izobraževanje varnostnih strokovnjakov in razvijalcev bomo še naprej zgolj opazovali, kam se premikajo bolj vizionarske države.

Literatura

[1] Spletna stran OWASP - The Open Web Application Security Project, www.owasp.org, dostop aprila 2018.

[2] A. Cavoukian, M. Dixon, Privacy and Security by design: an Enterprise Architecture Approach, IPC and Oracle, 2013. Dostopno na : https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

[3] Secure by Design: Improving the cyber security of consumer Internet of Things Report, https://www.gov.uk/government/publications/secure-by-design. 29.3.2018.

[4] Developer Zone - spletna stran Dzone, Security Zone, DevOps Zone. https://dzone.org, dostop aprila 2018.

[5] DevSecOps Manifesto, DevSecOps Blog: https://www.devsecops.org, dostop aprila 2018.

[6] John Pescatore, Chris Carlsson, 2017 Cybersecurity Trends: Making Progress by Aiming Ahead of the Target. SANS/Qualys, 2017. Dostopno na www.slideshare.net, april 2018.

Izr. prof. dr. **Mojca Ciglarič** je vodja Laboratorija za računalniške komunikacije in prodekanja za gospodarske zadeve na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Deluje na področju komunikacij, porazdeljenih sistemov in varnosti. Je tudi članica izvršilnega odbora Sekcije za kibernetsko varnosti pri ZIT, GZS.

Zagotavljanje kibernetske varnosti

Janez Anžič, Rok Peršak, Telekom Slovenije

Povzetek — Članek je namenjen zagotavljanju kibernetske varnosti v okolju skladnosti poslovanja, neprekinjenega poslovanja in informacijske varnosti v podjetjih. Opredeljene so posamezne aktivnosti v pripravi, preprečevanju, odkrivanju, odzivanju in obnovitvi poslovanja na procesu zagotavljanja kibernetske varnosti, tako za interne potrebe kot za trg.

Ključne besede — Načrtovanje-priprava, procesi, orodja, zaposleni, preprečevanje, odkrivanje, odzivanje in obnovitev, kibernetski napad, tveganje, kibernetska varnost, informacijska varnost.

Abstract — The purpose of this article is to provide cyber security in the environment of business compliance, business continuity and information security in companies. Procedures are defined in the preparation, prevention, detection, response and restoration of operations in the process of providing cyber security, both for internal needs and for the market.

Keywords — Preparation, processes, tools, people, prevention, detection, response and restoration, cyber-attack, risk, cyber security, information security.

I. UVOD

Tako kot se povečuje uporaba informacijskih tehnologij v celotnem okolju, se temu primerno dogaja razvoj na področju IoT, 5G, verig podatkovnih blokov, … Z večjo hitrostjo se izvajajo tudi različne zlorabe na področju varnosti informacijskih tehnologij, ki so vedno bolj napredne, tehnološko dovršene, prikrite, inovativne. Zloraba informacijsko-komunikacijskih tehnologij se izvaja na gospodarskem, političnem in zasebnem področju.

Motiv za zlorabo informacijsko komunikacijskih tehnologij je različen, od premoženjske koristi, zlonamernosti, dokazovanja, konkurenčne prednosti, onemogočanja delovanja kritične infrastrukture do geopolitičnih prednosti.

Namen zlonamernežev je, da uporabnikom zbrišejo podatke, jih zaklenejo, onemogočijo poslovanje, delovanje, pri tem pa uporabljajo različne metode napadov (socialni inženiring, ribarjenje, zlonamerne kode, viruse, DDoS (Distributed Denial-of-Service), …)

Proces zagotavljanja kibernetske varnosti razdelimo na pet posameznih korakov:

- **Priprava** – Organizacija mora upravljati tveganja kibernetske varnosti za sisteme, sredstva, podatke. V skladu s svojo strategijo upravljanja tveganj in poslovnimi potrebami je potrebno določiti vire, ki podpirajo kritične funkcije in s tem povezana tveganja kibernetske varnosti. Organizacije morajo tako določiti ustrezno politiko upravljanja tveganj in sprejeti naloge za ustrezno upravljanje tveganj.
- **Preprečevanje -** razvijati in izvajati ustrezne zaščitne ukrepe za zagotavljanje storitev sistemov in kritične infrastrukture. Zmožnost omejitve ali zadržanja vpliva potencialnega dogodka kibernetske varnosti. Primeri rezultatov te naloge vključujejo: identitete, pravice, varovanja podatkov in informacij, ustrezne tehnologije, ki podpirajo na primer varovanje podatkov, ozaveščanje, izobraževanje uporabnikov.
- **Odkrivanje -** razvijati in izvajati ustrezne dejavnosti za ugotavljanje pojava dogodka kršenja kibernetske varnosti. Odkrivanje omogoča pravočasno zaznavo varnostnih incidentov in neprekinjeno spremljanje sistemov in infrastrukture in zaznavo odstopanj. To opravljamo s pomočjo raznih tehnologij kot so požarni zidovi in orodij za upravljanje z dogodki kot je SIEM (Security information and event management).
- **Odzivanje -** razvijati in izvajati ustrezne dejavnosti za ukrepanje v zvezi z odkritim dogodkom ali s kršitvijo kibernetske varnosti. S pomočjo odzivanja pripravimo vse potrebno za zmanjšanje vpliva varnostne kršitve, se pravi načrtujemo odziv na varnostne kršitve, odpravimo varnostni incident ter se po odpravi pripravimo na izboljšavi tega dela procesa.
- **Obnovitev –** izvajanje ustreznih ukrepov za obnovitev poslovanja, sistema, vira, kritične infrastrukture, ki so bile prizadete zaradi dogodka varnostnega primera.

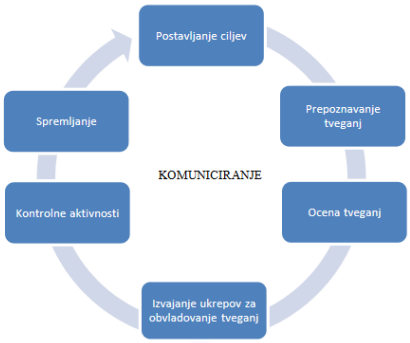
Vsem petim korakom procesa upravljanja kibernetske varnosti je vedno skupna izboljšava na vseh korakih, kot tudi priprava na ustrezno komunikacijo v primeru varnostnega dogodka.

II. NAČRTOVANJE – PRIPRAVA

Večina organizacij ugotavlja, da kršitve varstva podatkov in drugi incidenti v zvezi z varnostjo na področju informacijsko-komunikacijskih tehnologij predstavljajo poslovno kritično operativno tveganje. Razširjenost in resnost takšnih kršitev navajajo različne raziskovalne, varnostne in druge organizacije ali organi. Stroški varnostnega incidenta so lahko zelo visoki (finančno gledano , se lahko razširijo v več milijonov eurov), prav tako pravne obveznosti, regulatorna izpostavljenost in škoda zaradi izgube zaupanja.

Ustrezne priprave omejijo verjetnost nastanka takega incidenta in škoda zaradi takega dogodka je neprimerno manjša.

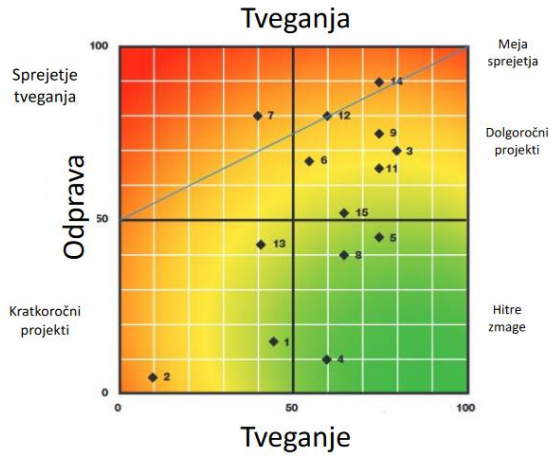
Obvladovanje tveganj je sistematičen in stalen proces, njegov namen je maksimiranje verjetnosti želenih dogodkov (priložnosti) in minimiziranje verjetnosti nezaželenih dogodkov (nevarnosti). Potek procesa je prikazan v spodnjem diagramu.



Slika 1: Upravljanje tveganj

Prepoznavanje in strukturiranje tveganj je začetna faza v procesu obvladovanja tveganj. Cilj prepoznavanja tveganj je identificiranje vseh možnih tveganj, ki lahko vplivajo na doseganje poslovnih ciljev. Dejavniki tveganj so lahko zunanji (okolje, politični, gospodarski, tehnološki, …) ali notranji (zaposleni, tehnologija, procesi, …).

Vsako prepoznano tveganje je potrebno bolj podrobno analizirati, s čimer se določita pomembnost tveganja in potrebni ukrepe. Cilj ocenjevanja tveganj je določitev pomembnosti oziroma stopnje tveganja. Tveganja z najvišjo stopnjo so tista tveganja, ki imajo največji vpliv na poslovanje in jih je potrebno prednostno obravnavati. Tveganja (R) ocenimo in razporedimo na podlagi dveh meril: VERJETNOSTI (P) in VPLIVA (C). R = P x C. Tveganje nato predstavimo v obliki matrike, kjer določimo verjetnost tveganja in njegov vpliv, ki je v večini primerov opredeljen v denarju.

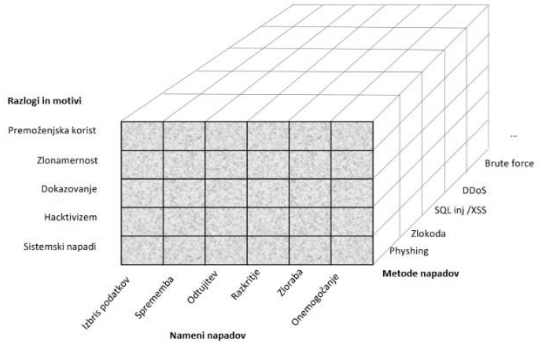


Slika 2: Matrika, ki nam pomaga upravljati s tveganji

Glede na opravljene ocene tveganj ter tehtanja stroškov in koristi (načelo gospodarnosti), se postavijo prioritete in izbere najprimernejši način obvladovanja tveganj, ki bo zagotovil, da bo tveganje po izvedenih ukrepih na ravni želene izpostavljenosti tveganju. Pri tem tveganja obvladujemo na način, da ga opustimo, ga zmanjšamo z nekim ukrepom, prenesemo na tretjo osebo (zavarovanje) ali ga kot takega sprejmemo.

Tveganja nato redno spremljamo na podlagi izvedenih ukrepov, spreminjamo na podlagi novih podatkov, novih razmer, sprememb tako na zunanjem kot notranjem področju, vodimo registre. Pri upravljanju tveganj so nam v pomoč standardi ali priporočila ISO, ISA, NIST, BS in drugih.

Tveganja na področju kibernetske varnosti so v zadnjih letih ocenjena z najvišjo stopnjo. Zato je na področju upravljanja s tveganji za zagotavljanje kibernetske varnosti potrebno sprejeti različne ukrepe na vseh področjih, kjer je neka organizacija izpostavljena preveliki stopnji tveganja.



Slika 3: Motivi in nameni napadov

Zato organizacija potrebuje program upravljanja tveganj na naslednjih področjih:

- izobraževanje in usposabljanje zaposlenih o uporabi končnih naprav (mobilnih terminalov, prenosnih računalnikov),
- politika uporabe lastnih naprav v omrežju organizacije,
- oddaljen dostop za potrebe mobilnosti uporabnikov,
- upravljanje konfiguracij takih delovnih postaj in mobilnih terminalov, omrežnih elementov, kjer je potrebno shranjevati varnostne kopije,
- po potrebi preverjanje ponovne nastavitve, zadnje verzije sprememb so v večini primerov zaželene.

Vzpostavljena mora biti evidenca vseh virov, ki organizaciji omogoča poslovanje in za vsak vir narejena ocena tveganja v primeru varnostnih tveganj ter predlagan ukrep za zmanjšanje tveganj.

Najpomembnejše je področje končnih naprav, kjer mora organizacija imeti sprejeto politiko dostopa do lastnega omrežja, politiko vklapljanja različnih USB naprav, kriptiranja podatkov, testiranja odziva zaposlenih, upravljanja z dostopovnimi pravicami in gesli končnih uporabnikov.

Na procesu upravljanja z incidenti naj ima organizacija izdelan plan komunikacije za različne stopnje odkritih varnostnih incidentov ter vplivov na poslovanje, vzpostavljeno metriko, ki omogoča upravljanje procesa upravljanje z varnostnimi incidenti.

III. PREPREČEVANJE

Podjetja in organizacije pri svojem poslovanju uporabljajo različna sredstva. Pri tem se izraz sredstvo v skladu s standardi ISO s področja varovanja informacij uporablja zelo na široko, saj je sredstvo pravzaprav vse, kar ima za podjetje določeno vrednost (ISO 27000).

Sredstva delimo na:

- fizična sredstva (računalniška strojna oprema, naprave za komunikacijo in hrambo, nosilci podatkov, zgradbe in lokacije),
- programska sredstva (operacijski sistemi, programske aplikacije in storitve, ki obdelujejo, shranjujejo ali posredujejo informacije, in razvojna orodja),
- informacijska sredstva (znanje ali podatek, ki ima določeno vrednost za podjetje),

– storitve (informacijski sistemi za obdelavo in hrambo informacij,
– podporni sistemi: ogrevanje, osvetlitev, fizično varovanje, elektrika in klimatske naprave),
– človeški viri (zaposleni v podjetju, ki imajo veščine, znanje in izkušnje).

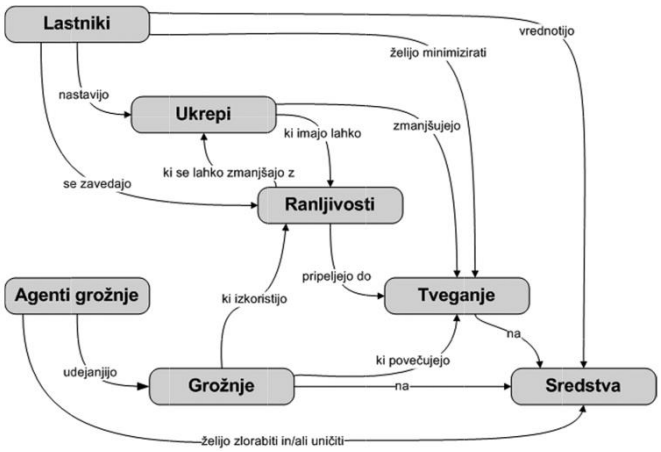
Glavni cilj vodenja informacijske varnosti je upravljanje z **zaupnostjo**, **celovitostjo**, **razpoložljivostjo, avtentičnostjo in neovrgljivostjo** posameznih sredstev. In prav vsako sredstvo je vir potencialnih tveganj ali groženj, ki jih moramo v skladu z metodologijo, omenjeno v prejšnjem poglavju, upravljati.

Najpogosteje se tveganja zmanjšujejo z investicijami v varnostne ukrepe in rešitve. Varnostni ukrepi so aktivnosti, postopki ali mehanizmi, ki zmanjšujejo verjetnost ali posledico varnostnih incidentov, na tveganje pa vplivajo različno. Lahko odkrivajo in preprečujejo incidente, odvračajo grožnje, omejujejo tveganja, popravljajo nastalo škodo zaradi incidenta, pomagajo pri okrevanju po incidentu, izvajajo nadzor ali ozaveščajo.

Glede na učinke lahko varnostne ukrepe razvrstimo v tri glavne skupine: preventivne, korektivne in detekcijske ukrepe. Preventivni ukrepi zmanjšujejo število uspešnih incidentov in s tem verjetnost za incident, korektivni ukrepi zmanjšujejo izgubo v primeru incidenta, detekcijski ukrepi pa skrajšajo čas, v katerem se incident zazna, in omogočajo zbiranje podatkov za nadaljnje analize.

Preventivni ukrepi so: varnostna politika, kriptografija, varna arhitektura omrežja in aplikacij, ažurno posodabljanje programske opreme s popravki, požarni zidovi, sistemi za preprečevanje vdorov v omrežju, DDoS zaščita, mehanizmi overjanja in avtorizacije uporabnikov, protivirusna programska oprema. Med preventivne ukrepe uvrščamo tudi razna testiranja glede ranljivosti sistemov ter izobraževanja in testiranja zaposlenih na razne tehnike napadov.

Kateri ukrep izberemo je, odvisno od odnosa in razmerja med varnostjo in uporabnostjo, ki si med seboj nasprotujeta.



Vir: ISO 15408

Slika 4: Visokonivojski pogled na verigo groženj in tveganj [4]

IV. ODKRIVANJE

Odkrivanje varnostnih in potencialno varnostnih incidentov poteka na več nivojih. Grožnje lahko odkrivamo proaktivno ali pa reaktivno. SIEM lahko uporabimo v obeh primerih.

SIEM je orodje ali sistem orodij, čigar osnovna funkcija je zbiranje dnevniških zapisov (event logov, logov, syslogov, itd.) iz raznorodnih sistemov. Zapise obdela, jih normalizira (prikaže v človeku prijazni obliki), ustrezno agregira in prikaže v obliki varnostnih dogodkov.

Na trgu je veliko izbire, od osnovnih pregledovalnikov dnevniških zapisov do kompleksnih sistemov, katerih dodana vrednost je uporaba umetne inteligence za odkrivanje potencialnih ranljivosti, samodejno posodabljanje pravil za kreiranje varnostih dogodkov, možnosti razširitev itd.

Učinkovitost orodja SIEM je odvisna od več faktorjev: kakovosti dnevniških zapisov, kakovostnega odstranjevanja šuma (false positive), ustreznega povezovanja potencialnih varnostnih dogodkov z aktualnim dogajanjem v svetu (odkrite nove ranljivosti, grožnje kibernetskih napadov, politične dejavnosti, trenutnega kotiranja podjetij, …). Vse to v ospredje pomembnosti postavi človeka, ki je, seveda ustrezno podkovan, najbolj učinkovit pri odkrivanju ranljivosti.

Poskrbeti je torej treba za sprotno dodajanje in odstranjevanje virov dnevniških zapisov, iskanje novih in izboljševanje starih mehanizmov za odkrivanje morebitnih varnostnih dogodkov, predvsem pa za neumorno ločevanje zrnja od plevela v poplavi vseh dogodkov, ki jih prikazuje orodje, za kar pa so potrebne izkušnje, znanje ter v veliki meri iznajdljivost posameznika.

Klasične antivirusne in anti-malware programske rešitve se za odkrivanje groženj opirajo na baze podatkov, primerjajo vsebine datotek s podatki iz baze in zelo dobro poskrbijo za sprotno čiščenje ter zaščito. Vse to velja samo v primerih, da je nekdo grožnjo nekoč že odkril, jo preučil in vnesel v bazo. Tudi izmenjava baz podatkov poteka v današnjih časih bolj ali manj brez vidnejšega vrtičkanja. Vsi ti mehanizmi so v primeru novih groženj, ali včasih tudi variacij nekaterih že poznanih groženj, popolnoma neuporabni. Razmišljati je treba o spremljanju obnašanja vsakega procesa posebej. Tudi takšne rešitve obstajajo, učinkovitost teh pa je v veliki meri odvisna od iznajdljivosti programerjev na obeh straneh zakona.

Proaktivno lahko morebitne grožnje odkrivamo s t. i. penetracijskimi testi in testi ranljivosti. Gre za vnaprej dogovorjeno in avtorizirano obliko odkrivanja ranljivosti sistemov, kjer se v prvem koraku najde varnostne luknje, pripravi nek načrt vdora, kasneje pa se ta vdor tudi izvede.

V. ODZIVANJE

Največji izziv pri nepoznanih grožnjah je oceniti resnost grožnje in možne posledice. Način odzivanja mora biti usklajen z varnostno politiko podjetja.

Najpogostejši viri groženj so uporabniki. Težko je na prvi pogled oceniti, ali je šlo za načrtno zlorabo ali mogoče samo za trenutno nepazljivost in neznanje uporabnika.

Kvaliteten kader, ki uporablja ustrezne programske rešitve, je predpogoj za pravočasen in predvsem pravi odziv. Orodje je le del enačbe, napačna interpretacija morebitnega varnostnega dogodka lahko vodi v iskanje izvora groženj, ki to niso. Posledica tega je predvsem izguba časa, resursov in celo neopravičeno motenje delovnih procesov, upad učinkovitosti, izguba zaupanja in kompetentnosti.

Najprej se torej ugotovi resnost grožnje in obseg ter glede na njeno klasifikacijo izvede prve ukrepe. Pri grožnjah z visoko stopnjo resnosti je treba najprej poskrbeti, da se

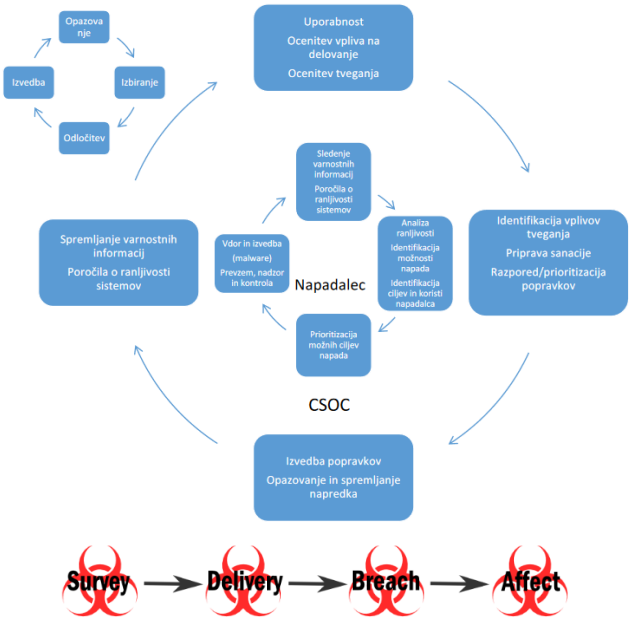
varnostna grožnja zajezi z ustrezno izolacijo sistema. Izvede se obveščanje in vse, kar je potrebno, za nemoteno izvajanje forenzičnih raziskav na viru grožnje. Samo z ustrezno forenzično raziskavo lahko podobne grožnje preprečimo tudi v prihodnje. Vsak postopek in vsako najmanjšo informacijo ob reševanju varnostnega incidenta je treba sproti beležiti v ustreznem informacijskem sistemu (ticketing system).

Slika 5: Upravljanje z incidenti

VI. OBNOVITEV

Uspešen kibernetski napad lahko traja več ur, dni, tednov. Posredna škoda nastaja še več mesecev po napadu na področju odtekanja informacij, vpliva na ugled in vrednost blagovnih znamk. Verjetnost, da so tudi varnostne kopije poškodovane, je tudi zelo velika. Po podatkih Gartnerja ima samo tretjina podjetij pripravljen plan za odziv na kibernetski napad. Pri teh podjetjih, ki imajo pripravljen plan, se ugotavlja, da imajo priprave opravljene za enostavne napade, ali napade enega samega tipa. Osnovo za pripravo na obnovitev nam lahko predstavlja veriga napadalcev, ko se pripravljajo na kibernetski napad. Vključuje zbiranje informacij o tarči, analizo zbranih informacij in izbor tehnike napada, dostavo – v končne naprave prek ribarjenja, instalacijo po več virih ali sredstvih ter skrivanje, nadzor in prevzem ter izvršitev napada. Notranji krog predstavlja korake napadalca. Zunanji krog zaščita pred napadom.

Veriga napadalcev je prikazana v celoti na naslednji sliki.



Slika 6: Veriga delovanja napadalcev

V vsaki točki, kjer morebitni napadalec vidi svojo priložnost, je potrebno v podjetjih opredeliti vpliv na poslovanje (BIA-business impact analysis). Za vsako sredstvo/vir je potrebno pripraviti vse potrebno za različne ocene tveganj (zaželena je kombinacija zahtevnejših možnih tveganj), načrt okrevanja virov, načrt okrevanja storitev, načrt kriznega komuniciranja.

Prvi del imenujemo pripravljalna oziroma načrtovalska faza, drugi del, ko se napad že zgodi, pa odziv in obnovitev poslovanja.

Za pripravljalno fazo je značilno, da se pripravljamo na naslednjih področjih:

– organizacije – organiziranosti, analiz in planov,
– zagotavljanja odpornosti posameznih sredstev (zaščita podatkov)
– krizno komunikacijsko upravljanje.

V pripravi organiziranosti se ustrezno postavi odlično sodelovanje med CSIRT (Computer security incident response teams)/CSOC (Cyber Security Operations Center) in ekipo SOP (skupina za okrevanje poslovanja), pri čemer so člani lahko medsebojno pomešani. Ustanovi se enotni tim za krizno vodenje, pregleduje se sposobnost ekip in virov, ki so potrebni za obnovo poslovanja, preverja se sodelovanje med načrtovalci in operativo v podjetjih. Na področju analiz in planov preigravamo različne scenarije varnostnih in kibernetskih napadov in njihov vpliv na BIA, pregledujemo odziv in obnovitvene procedure (DR, Disaster Recovery), pogosto izvajamo vaje na različnih področjih posameznih sredstev, ki sestavljajo poslovanje podjetja. Izvajamo teste ranljivosti, penetracijske teste, izvajamo teste socialnega inženiringa (na primer e-mail za ribarjenje), izvajanje scenarijev različnih napadov in preverjanja pripravljenosti. Vse to izvajamo na podlagi priporočil ISO 22301, 27001, NIST in drugih standardov. Na področju krizno komunikacijskega upravljanja se pripravi komunikacijski načrt v odvisnosti od velikosti in vpliva kibernetskega napada.

V obnovitveni fazi, kjer se napad dogaja, je potrebno glede na vpliv na BIA tesno sodelovanje med upravljanjem neprekinjenega poslovanja (strokovnjaki za vire), SOP in CSIRT ekipo v podjetju, ali celo na nacionalnem nivoju. Na podlagi priprav v prejšnji fazi se odloči, kdo bo vodil koordinacijo obnovitve (član SOP). Glede na resnost napada lahko to skupino vodi CIO (chief information officer/ CISO (chief information security officer). Glede na vpliv napada se sprožijo ustrezne obnovitvene procedure DR, izvedejo se prve forenzične preiskave, se obnovi poslovanje in zaščiti dokaze. Naloga ekip je, da se v skladu z organiziranostjo čim prej vzpostavi normalno obratovanje organizacije ali podjetja. Ob koncu napada je potrebno ustrezne podatke predati pristojnim organom, vladnim ustanovam, zavarovalnici, …

Nato se pripravi natančna analiza, poišče se dobre in slabe strani reakcije na kibernetski napad in sprejme ustrezne ukrepe za izboljšanje priprave, preprečevanja, odkrivanja, odzivanja in obnovitev poslovanja.

VII. SKLEP

Zagotavljanje informacijske in kibernetske varnosti je velik izziv v digitaliziranem svetu. Sredstev – virov, ki jih v podjetjih ali organizacijah uporabljamo pri vsakodnevnem delu, je izjemno veliko. Zato je potrebno preveriti in oceniti tveganja na vseh področjih delovanja podjetja (kadri, procesi

orodja, tehnologija). Pripraviti, uvajati in upravljati je potrebno z vsakim sredstvom v poslovanju podjetja ali organizacije. Potrebna je velika mera preventive v izvajanju raznih testov, nameščanju popravkov, izobraževanju in zavedanju kompetentnosti slehernega kadra v podjetju (socialni inženiring). Pri tem so nam v pomoč razna orodja in okolja, ki nas zaščitijo pred zlonamernimi in nepooblaščenimi zlorabami. Pripravljen mora biti komunikacijski načrt v primeru kibernetskega napada, kader mora biti sposoben zajeziti vpliv, shraniti dokaze in povrniti poslovanje podjetja v normalno stanje.

Akcije za zagotavljanje kibernetske varnosti lahko strnemo v dve področji dela, ki se morata izvajati vzporedno, in sicer taktično in strateško delovanje. Pod taktično delovanje štejemo takojšnjo reakcijo na varnostni dogodek, njegovo izolacijo, odpravo, nadaljnje pojavljanje in obnovitev poslovanja. Strateško delovanje pa je preventiva, testiranje, vaje, upravljanje in vodenje ter izvajanje nalog skladno z vodenjem upravljanja s tveganji.

Podjetjem ali organizacijam lahko Telekom Slovenije ponudi izvedbo zagotavljanja kibernetske varnosti v skladu z najvišjo stopnjo varnosti in skladno z mednarodno priznanimi certifikacijami.

LITERATURA

[1] https://www.nist.gov/cyberframework
[2] https://www.sans.org/
[3] http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/DSI2020_Strategija_Kibernetske_Varnosti.pdf
[4] http://maksi2.ef.uni-lj.si/zaloznistvoslike/440/E-verzija_Monografija_Bojanc in soav_Informacijska varnost v podjetniskem okolju_feb2015.pdf
[5] www.gartner.com
[6] https://www.enisa.europa.eu/
[7] Interna dokumentacija Telekoma Slovenije, d.d.

mag. Janez Anžič, MBA je direktor oddelka operativno storitvenega centra, kjer vodi delo na področju nadzora omrežja, operativno kibernetskega centra in tehnične pomoči vsem segmentom uporabnikom ter upravljanja sprememb v omrežjih. Ima več kot 21 let delovnih izkušenj na področju informacijsko komunikacijskih tehnologij. Vodil je različne projekte uvedbe informacijsko komunikacijskih tehnologij ter različne organizacijske enote: Sektor za razvoj in upravljanje storitev, Sektor za razvoj in načrtovanje omrežij, Oddelek za OSS sisteme in razvojno raziskovalne projekte. Pogosto je predaval na različnih domačih konferencah in simpozijih. Poučuje tudi na višji strokovni šoli. Magistriral je leta 2002 na Univerzi v Ljubljani, Leta 2009 je zaključil MBA izobraževanje na IEDC šoli na Bledu.

Rok Peršak je vodja tima v Operativno storitvenem centru na področju Upravljanja sprememb ter Operativnega centra za kibernetsko varnost. Ima 11 let delovnih izkušenj na področju tehnične pomoči uporabnikom, kjer je opravljal različne, večinoma organizacijske in tehnične funkcije. Diplomiral je leta 2016 po študijskem programu Organizacija in management, smer Informatika v organizaciji in managementu.

Implementacija zahtev GDPR v praksi s posebnim pogledom na zdravstveno – medicinske podatke

Igor Osolnik, Andrej Orel, Marand d.o.o., Ljubljana

Povzetek — Ta članek opisuje praktičen način izvedbe projekta za skladnost z zahtevami GDPR v gospodarski družbi.

Ključne besede — GDPR, Uredba, projekt, varstvo osebnih podatkov

Abstract — This article explains implementation of the GDPR requirements in company.

Keywords — GDPR**,** data protection, project.

I. UVOD

Pred slabim letom sem (Igor Osolnik) zamenjal delodajalca in v Marand d.o.o., (družba, ki zagotavlja napredne informacijske storitve, sisteme in produkte) kot edini pravnik, zasedel delovno mesto svetovalca za pravne zadeve. Pravnim zadevam se je jeseni pridružil še delokrog skladnosti poslovanja, v obliki vodenja projekta za skladnost poslovanja z določili Splošne uredbe o varstvu osebnih podatkov (v nadaljevanju uredba GDPR) v Marand d.o.o. Čeprav imam skoraj dve desetletji pravniških izkušenj na različnih delovnih mestih, pri čemer sem zadnjih nekaj let preživel v IKT branži, je nova zadolžitev predvsem zaradi nepoznavanja vseh sodelavcev in procesov v družbi, predstavljala zanimiv izziv. Zavedal sem se, da bo »bančni pristop« v smislu produciranja (pre)številnih in ne preveč življenjskih pravil kontraproduktiven. Ker več glav več ve, se mi je zdelo najbolj primerno skupno – ekipno delo in zato sem po posvetovanju z izkušenejšimi kolegi, sklical uvodni »GDPR sestanek«, ki so se ga udeležili predstavniki vseh večjih organizacijskih enot v družbi. Na njem smo skupaj dorekli:

- poimensko sestavo projektne skupine (vsak izmed vodij organizacijske enote je sodelovanje v projektni skupini prevzel nase ali pa nominiral svojega podrejenega),
- frekvenco sestankov,
- finančne resurse,
- končni rok za dokončanje projekta GDPR.

Ob prebiranju uredbe GDPR mi je kmalu postalo jasno, da se bom moral za potrebe usmerjanja projekta GDPR dodatno usposobiti in izobraziti s pridobitvijo specializiranega znanja s področja varstva osebnih podatkov. Ob podpori uprave sem se udeležil več intenzivnih seminarjev, ki so mi dodatno širili obzorja in dali dodatna praktična znanja.

V okviru podjetja Marand d.o.o. je potrebno poudariti, da je na »core business« razvoj računalniške programske opreme s področja zdravstva. Uredba GDPR posebej obravnava t.i. občutljive osebne podatke, kamor sodijo predvsem tisti osebni podatki, ki so tako ali drugače povezani s človekovim tako fizičnim kot duševnim zdravjem. Sami s tovrstnimi podatki sicer ne upravljamo, vendar pa jih obdelujemo, predvsem v fazi produkcijskega testiranja. Poleg tega pa je njihov upravljavec naš naročnik, kateremu smo, kot strokovnjaki (tudi) s področja varovanja osebnih podatkov, dolžni nuditi ustrezno svetovanje in podporo pri njihovem delu.

Vir za sliko[1]

II. IZVEDBA PROJEKTA

Kje začeti? Kateri je prvi korak na dolgi poti realizacije projekta? Če želimo vedeti, s katerimi podatki upravljamo ali jih obdelujemo, zagotovo na prvem mestu potrebujemo enotno evidenco vseh zbirk osebnih podatkov, ki jih obdelujemo, oziroma s katerimi upravljamo. Dobra štartna osnova pri vzpostavljanju tovrstnih evidenc je zbirka osebnih podatkov, ki so jih morali zavezanci poročati informacijskemu pooblaščencu, skladno z določili Zakona o varstvu osebnih podatkov (ZVOP-1). S temi zbirkami je upravljal informacijski pooblaščenec in so bile javno dostopne na njegovi spletni strani[2]. Po pregledu zbirk, ki so že bile prijavljene pri informacijskem pooblaščencu, je naša projektna skupina, vsaka na svojem organizacijskem področju, preverila, katere zbirke osebnih podatkov resnično še upravlja ali obdeluje. Dejansko ni minil sestanek projektne skupine, ne da bi se število na novo evidentiranih zbirk povečalo vsaj za eno. Na tak način smo skozi več iteracij vzpostavili posodobljen in ažuren »register evidenc obdelav osebnih podatkov« (v nadaljevanju: register). Register smo razdelili na dva ločena sklopa: zbirke podatkov, s katerimi Marand upravlja in zbirke podatkov, kjer je Marand obdelovalec. S tako opravljeno delitvijo se je v naslednjem koraku takoj izluščila tudi ustrezna podlaga za zakonito obdelavo osebnih podatkov: pri upravljanju lastnih osebnih podatkov je šlo v veliki večini primerov za zakonsko podlago

[1] Vir za sliko: https://www.hvidra-sb.hr/index.php/126-realiziran-projekt-podrska-socijalnom-ukljucivanju-i-zaposljavanju-marginaliziranih-skupina-skolovanje-prekvalifikacija-osposobljavanje

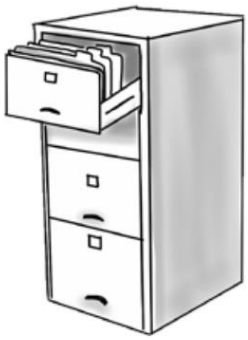
[2] https://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/pregled-zbirk/

(le redko za soglasje), v vlogi obdelovalca pa je šlo praviloma za pogodbeno obdelavo osebnih podatkov. V vlogi obdelovalca smo kmalu ugotovili, da imamo opravka z dvema vrstama podatkov:

– z osebnimi podatki in
– s t.i. posebno vrsto osebnih podatkov, kot jih imenuje uredba GDPR (tudi občutljivi podatki). Ti podatki so npr.: podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje, članstvo v sindikatu, podatki v zvezi z zdravjem…

Obdelavi posebne vrste osebnih podatkov (zdravstveni podatki), smo namenili še posebno pozornost: v okviru projektne skupine smo kot prvi ukrep skladno z načelom minimizacije iz uredbe GDPR omejili dostope do posebne vrste osebnih podatkov le na tiste zaposlene, ki take dostope resnično potrebujejo za izvajanje pogodbenih obveznosti, posodobili smo sistem gesel in vzpostavili internetno povezavo, na kateri se nahaja ažurni seznam zaposlenih z njihovimi individualiziranimi dostopovnimi pravicami za potrebe obdelave osebnih podatkov. Tekom projekta je tako register vztrajno pridobival na pomenu in se širil po vsebini ter na koncu postal ključni dokument celotnega projekta. Z vidika projekta je bilo smiselno vzpostaviti centraliziran dokument, ki smo mu glede na potrebe zgolj dodajali nove »funkcionalnosti«. Tako smo register postopoma dodatno opremili z rubrikami iz katerih so bili razvidni:

– namen obdelave;
– roki hrambe podatkov;
– pravna podlaga za obdelavo podatkov;
– kategorija posameznikov, na katere se osebni podatki nanašajo;
– skrbnik področja…



Vir za sliko registra[3]

Marand je že mnogo pred uredbo GDPR v zvezi z obdelavo zdravstvenih osebnih podatkov zagotavljal dosledno psevdonimizacijo le-teh in jo tudi ustrezno vgradil v samo arhitekturo svojih informacijskih rešitev, namenjenih zdravstvenemu sektorju. Uredba GDPR psevdonimizacijo podatkov postavlja na sam vrh tehnično organizacijskih ukrepov, ki zagotavljajo ustrezno raven varnosti (glej 32. člen uredbe GDPR). Psevdonimizacija pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati določenemu ali določljivemu posamezniku. Z drugimi besedami: gre za maskirane podatke v ločenih podatkovnih bazah, ki za osebo, ki bi morebiti namerno ali po naključju dostopala do njih, nima nikakršne uporabne vrednosti, saj iz psevdonimiziranih podatkov ne more ugotoviti, na katerega posameznika se nanašajo ali za kakšno vrsto zdravstvenega podatka po vsebini gre. Psevdonimizacija z ločitvijo baz in s povratnim ključem učinkovito zagotavlja ustrezno raven varnosti podatkov, pri čemer pa ne ovira vsakdanjega dela osebja v zdravstvu. Anonimizirani podatki pa so tisti podatki, pri katerih je proces le enosmeren in po tem, ko se jih anonimizira, ne obstaja več nikakršna naknadna ali povratna možnost identifikacije posameznika (anonimizirani podatki zato skladno z 26.členom uvodnih določb niso predmet uredbe GDPR).

Istočasno s prevetritvijo postopkov pri posebni vrsti osebnih podatkov smo na področju marketinga preverili tudi ustreznost dosedanjih soglasij in jih uskladili z zahtevami uredbe GDPR (privolitev mora biti podana v ločeni izjavi od siceršnjih splošnih pogojev, soglasje mora biti v jasnem in preprostem jeziku, kadarkoli ga je mogoče enako enostavno preklicati, kot je bilo dano, dokazno breme o obstoju soglasja je na obdelovalcu osebnih podatkov, soglasje ne sme biti pogojevano s storitvijo…).

Uredba GDPR na več mestih v zvezi z obdelavo osebnih podatkov poudarja sprejem ustreznih tehničnih in organizacijskih ukrepov, ki jih morata zagotavljati tako upravljavec kot obdelovalec osebnih podatkov. Ker Marand nastopa tako v eni kot v drugi vlogi, smo konkretne tehnično organizacijske ukrepe, ki jih izvajamo poleg že opisane psevdonimizacije, zapisali še v register ali pa se v njem sklicevali na politike, ki jih izvajamo skladno z ISO standardom 27001.

III. ZDRAVSTVENI PODATKI

Kot je bilo že v uvodu zapisano, sodi večina osebnih podatkov, ki so povezani z zdravstvenim stanjem neke osebe, med občutljive osebne podatke. Le-ti so v posebne členu GDPR taksativno našteti. Ta del uredbe je eden izmed redkih konkretnih delov, saj uredba podaja bolj smernice in principe varovanja osebnih podatkov, kakor pa predpisuje konkretne ukrepe. Le-ti naj bi bili določeni v okviru zakonodaje posameznih držav članic.

Poglejmo si, kaj pravi člen (9. člen GDPR – posebne vrste podatkov), ki govori o občutljivih osebnih podatkih:

> *Prepovedani sta obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.*

Striktno gledano so skoraj vsi, v citatu navedeni osebni podatki, zdravstveni podatki. Rasa in etničnost vplivata na primer na absorpcijo zdravil in drugih preparatov, versko ali filozofsko prepričanje pa na stil prehranjevanja. Poenostavljeno rečeno so vsi medicinski podatki, pridruženi neki konkretni osebi, občutljivi podatki.

V gornjem citatu piše, da je obdelava takšnih podatkov prepovedana. Seveda pa mora biti v našem primeru neki »ampak« in ta se skriva v naslednjih alinejah istega člena GDPR:

[3] Vir za sliko registra: https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/kopiranje-osebnih-dokumentov-in-prepisovanje-podatkov-iz-osebnih-dokumentov/

> *...obdelava je potrebna za namene izpolnjevanja obveznosti in izvajanja posebnih pravic upravljavca ali posameznika, na katerega se nanašajo osebni podatki, na področju delovnega prava ter prava socialne varnosti in socialnega varstva, če to dovoljuje pravo Unije ali pravo države članice ali kolektivna pogodba v skladu s pravom države članice, ki zagotavlja ustrezne zaščitne ukrepe za temeljne pravice in interese posameznika, na katerega se nanašajo osebni podatki;*

in pa…

> *...obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugega posameznika, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno ni sposoben dati privolitve.*

Pričujoča dva citata dovoljujeta t.i. redno zdravstveno obdelavo (s privolitvijo posameznika) in pa izredno (brez privolitve, kar je pomembno predvsem v primerih nuje (nesreče…) in drugih primerih, kjer bi obvezno pridobivanje soglasja ogrozilo človekovo zdravje.

Za zaključek tega poglavja je potrebno opozoriti še na poseben vidik obdelave zdravstvenih podatkov in sicer v raziskovalne namene. V teh primerih GDPR dovoljuje bolj sproščeno obdelavo občutljivih osebnih podatkov (tudi brez pristanka posameznika), vendar pa je potrebno pred tem poskrbeti za resnično anonimizacijo, kjer ni načina, da s posamezno zbirko podatkov pokažemo na konkretnega posameznika.

Še na en vidik je treba pokazati: obdelava zdravstvenih podatkov v okviru kriminalističnih postopkov. Tukaj pristanek posameznika seveda ni smiseln, za to pa obstaja posebna EU direktiva, ki še vedno ohranja zasebnost posameznika, saj je z GDPR v Evropi (na žalost samo!) zasebnost (privacy) postala temeljna človekova pravica.

IV. ZAKLJUČEK

V zadevnem prispevku sva želela predstaviti konkretno izvedbo projekta za skladnost poslovanja z določili uredbe GDPR v gospodarski družbi in predstaviti primer dobre prakse medsebojnega sodelovanja v družbi: moči sva združila sodelavca s tehničnega in pravnega področja, z različno dolgim stažem in izkušnjami pri delodajalcu ter tako družno prispevala k uspešni izvedbi projekta.

Skozi projekt in skozi pridobljene izkušnje sva spoznala dve dejstvi, na kateri se nama zdi ob zaključku tega prispevka potrebno še posebej opozoriti in sicer:

- da je najbolje porabljeni čas tisti, ki je namenjen ozaveščanju sodelavcev o pomembnosti varstva osebnih podatkov, še zlasti posebne vrste osebnih podatkov,
- da uredba GDPR sili upravljavce in obdelovalce osebnih podatkov v kontinuiran proces aktivnosti, spremljanja in izboljšav že vzpostavljenih procesov in da torej ne gre za enkratno dejanje (npr. sprejem pravilnika, popis procesov, podpis izjav o varstvu osebnih podatkov…), kot je najpogostejša pavšalna percepcija.

Vir za sliko[4]

ZAHVALE

Avtorja se zahvaljujeva podjetju Marand d.o.o., kjer sva zaposlena, ker nama je omogočilo temeljito usposabljanje in pridobivanje znanj, potrebnih za implementacijo Uredbe (GDPR) v tako zahtevnih okoljih, kot je zdravstvo. Podjetju se zahvaljujeva tudi, da nama je omogočilo pripravo pričujočega članka in udeležbo na konferenci VITEL 2018 v organizaciji Slovenskega društva za elektronske komunikacije.

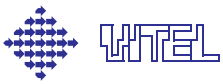
Igor Osolnik je diplomiral na Pravni Fakulteti v Ljubljani leta 1998, leta 2003 pa je opravil še državni pravniški izpit. Vseh do sedanjih 20 let delovne dobe je preživel kot pravnik v različnih gospodarskih družbah: Energoplan d.d., BTC d.d., UniCredit Banka Slovenija d.d. (prej Bank Austria Creditanstalt), Halcom d.d. in Marand d.o.o. Je tudi občasni predavatelj na Združenju Bank Slovenije.

[4] http://cdnsba.org/all/education-in-canada/best-practices-artssmarts

PRISPEVKI

ARTICLES

15. 5. 2018



The causal loop between information disorder and trust on the Internet

Tanja Pavleska, Laboratory for Open Systems and Networks, Jozef Stefan Institute, Ljubljana

Abstract — This article explains the link between **information disorder** (represented by misinformation, disinformation and malinformation) and **trust** on the Internet, from both socio-economic and technological perspective. The topics are analysed through information/content type that is a popular online representative of the problem: the **fake news** phenomenon and the **fact-checking** initiatives trying to combat it. The article introduces a conceptual framework for reasoning about information disorder and establishes its connection to trust. Finally, it presents the key findings from an empirical study on the performance of the European fact-checking organizations and extracts important stakeholder recommendations.

Keywords — trust, information disorder, fake news, fact-checking, empirical study

Povzetek — Ta članek pojasnjuje povezanost med informacijsko motnjo (povzročeno z napačnimi informacijami, dezinformacijami in škodljivimi informacijami) in zaupanjem na Internetu, tako s socialno-ekonomskega kot tudi s tehnološkega vidika. Teme so analizirane na primeru popularnega tipa informacij, poimenovanega lažne novice ter s pobudami za preverjanje dejstev. Članek uvaja konceptualni okvir za razmišljanje o informacijskih motnjah in njihovo povezavo z zaupanjem. Na koncu predstavi ključne ugotovitve iz empirične študije o uspešnosti evropskih organizacij za preverjanje dejstev in povzema pomembna priporočila za ustreznih deležnikov.

Ključne besede — zaupanje, informacijska motnja, lažne novice, preverjanje dejstev, empirična študija

I. INTRODUCTION

The advent of the information and communication technologies opened up a myriad of opportunities for people to create and distribute content through multiple services and platforms. However, not all actors take advantage of the bright side of the Internet. In fact, very often they create and spread (purposefully or not) content of dubious veracity or unverified origin. This type of content is what has popularly become classified as "fake news". *Fake news is often simply defined as spreading false content for political purposes.* However, from a broader perspective, fake news may refer to rumours, gossip or generally, information that is dubious or completely misleading. The most controversial property of fake news is undoubtedly their potential to influence how society as a whole or groups within society behave and perceive reality. This not only impacts the quality of contents on the web, but undermines the trust of the users in the platforms, in the applications and in the other users creating and sharing content. As reported in the Reuters Institute Digital News Report [1], only a quarter (24 %) of the respondents think "social media do a good job in separating facts from fiction, compared to 40 % for the news media."

These developments in the online world, however, do not imply that traditional media are immune to fake news reporting (Edelman Trust Barometer 2018[1]). Media presentation of reality and journalism work have in particular been largely questioned because distrust in media as a factor for social progress is on the rise. Thus, it is of little surprise that we have witnessed the emergence of dozens of fact-checking organizations in Europe over the last several years [2, 3, 4].

Although many articles and studies report on some aspects of these activities, tools, organizations and their work, there is no study, let alone a holistic one, that either determines factors for measuring performance or inspects the influence of those factors on any aspect of the performance of fact-checking efforts. Yet, the relevance of this particular issue seems to be approachable by a multitude of disciplines:

- Economically, one can speak about the efficacy of the efforts, their social impact, return of investment, value for money, effect on consumer behaviour, risk assessments, or their contribution to the Internet and media development in general.
- Politically, one may investigate questions like: Which entities deserve public/civil support and how is this provided in the most transparent and sustainable way? What are the practical implications of their functioning? or more specific questions, such as: What is the correlation between information disorder and the political developments in a country? How can regulation impact and be impacted by these efforts? How are fundamental rights affected by the success or failure of these initiatives?
- Psychologically and inter-disciplinary, investigating these issues may provide deeper and novel insights into the human bias phenomena, the role of social behaviour and groupthink (echo chambers), the formation of social networks in the proliferation of a certain piece of information, the emergence and undermining of trust, etc.

Research has, nevertheless, provided arguments for negative perceptions on the general usefulness and trustworthiness of these organizations by social media users [3], mainly stemming from transparency issues.

II. THEORETICAL BACKGROUND

Developing and arguing over a case concerned with fake news, hoaxes, fact-checking, clickbait (monetization and traffic attraction), is often encumbered by the absence of a conceptual common ground on the concepts underlying that context. Some suggest novel terms, such as attention hacking [5]. Others prefer more general terms, such as distribution of

[1] https://www.edelman.com/trust-barometer

harms, as coined by Rubin et al. in [6]. According to [5], fake news "generally refers to a wide range of disinformation and misinformation circulating online and in the media." In media markets' theories fake news is defined as "distorted signals uncorrelated with the truth" that emerge in the market because it is "cheaper to provide than precise signals" [7]. From a political economy perspective, fake news has a long history that is bound to the commodification of journalism in a market economy [8]. Some researchers like Wardle and Derakhshan oppose the use of the term "fake news" per se [9]. In their view, it is a conceptually inadequate and politically abused term. In the same vein, Marwick et al. call for a larger focus on attention and frame hacking, providing a perspective that is more oriented towards data infrastructure manipulation sensitivity rather than vague discussions on veracity, truth and objectivity [5]. Therefore, Wardle and Derakhshan introduce a new conceptual framework, defining what they prefer to call the key terminology of information disorder: misinformation, disinformation and malinformation, and distinguishing between information that is false and information that is designed to harm [9]. In our study, we follow Wardle and Derakhshan's conceptual framework for information disorder and adopt the following definitions:

Definition 1: Misinformation occurs when false information is shared, but no harm is meant.

Definition 2: Disinformation is when false information is knowingly shared to cause harm.

Definition 3: Malinformation is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

Clearly, fake news can be of a detriment to the social momentum of the Internet. Moreover, it can equally bring harm to the public as any other type of harmful content. Despite the inconsistencies of the definitions, there seems is a consensus that the current communication environment within and between many countries worldwide is much more politically and socially challenged than in the past periods of grey and black propaganda, conspiracy theories and fabricated content. In a society where the virtual and the real world cannot be divided by a clear line, these developments directly affect the social fabric of the world democracy.

III. FAKE NEWS AND FACT-CHECKING

Considering the variety of stakeholders concerned by the problem, several initiatives and organizations were also established with the common objective of raising awareness and addressing challenges related to trust and truth in the digital age: the NGO First Draft[2] (in 2016), global Partner Network of journalism (e.g. BBC, Reuters), human rights (e.g. Amnesty International) and technology (e.g. YouTube) organizations, to name a few. To join these efforts at a European level, in November 2017 the European Commission (EC) announced its next step in the fight against fake news: setting up a High-Level Expert Group and launching a public consultation[3]. Some EU member states had already taken measures to combat information disorder. For example, the Czech Republic set up a specialist "anti-fake news" police unit called Centre Against Terrorism and Hybrid Threats, which have been operating since 2017. Both Italian and Slovak police announced fight against fake news in January 2018. Simultaneously, Sweden engaged in plans to create a new public authority tasked with countering disinformation and boosting the population's resilience in the face of possible influence operations, called "psychological defense" (psykologiskt försvar) authority. Similarly, in January 2018 the United Kingdom revealed plans to establish a new "national security communications unit" to curb the presence of hoax news stories online and stop social media campaigns from foreign adversaries. These initiatives have currently no special institutional or legal background. A debate could be opened on whether an effort to make them institutional would result in approval by the public and what repercussions would it have on human rights, national security and public safety.

There is no single definition of what the objectives of fact-checking organizations are, or even a single description summarizing their basic features. A variety of approaches among scientists exist to determine and describe these organizations. A recent study divides the universe of fact-checking services into three general categories based on their areas of concern: 1) political and public statements in general; 2) online rumours and hoaxes and 3) specific topics, controversies [3], particular conflicts or narrowly scoped issues and events. Most recent data counted 137 active fact-checking projects around the world – up from 114 in early 2017. A third of them are located in the USA [2]. In Europe alone, 34 permanent sources of political fact-checking have been identified as active in 20 different European countries, from Ireland to Turkey [4]. These organizations are categorized in terms of their mission and their methods. By this categorization, Graves and Cherubini found that fact-checking outlets occupy a spectrum between reporters, reformers, and a third – overlapping category of organizations cultivating a role of independent experts [4].

Fact checkers around the globe have also formed an entire professional network. The International Fact-Checking Network (IFCN) is a unit of the Poynter Institute dedicated to bringing together fact-checkers worldwide[4]. The IFCN was launched in September 2015 to support fact-checking initiatives by promoting best practices and exchanges among organizations in this field. The association also adopted a Code of principles in 2016. The principles represent professional commitments to non-partisanship and fairness, transparency of sources, transparency of methodology and open and honest corrections. These comprise the principles and values on which the activities of fact-checking organizations are premised; notwithstanding the fact that these organizations are similar to journalistic and other associations (like non-governmental organizations), they have not adopted criteria for the self-assessment of their performance. Moreover, only part of the European fact-checkers joined this global network.

Analysing more in depth these organizations, some scholars explore the methodology they use. Rubin et al. provide a map of the current landscape of veracity assessment methods, their major classes and goals [6]. Two major categories of methods exist: 1. Linguistic Approaches in which the content of deceptive messages is extracted and

[2] https://firstdraftnews.com/about/#network
[3] http://europa.eu/rapid/press-release_IP-17-4481_en.htm
[4] https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles

analysed to associate language patterns with deception; and 2. Network Approaches in which network information, such as message metadata or structured knowledge network queries can be harnessed to provide aggregated deception measures. Interestingly, most of the insights on deception research originate from disciplines without detection automation in mind.

IV. METHODOLOGY

Despite their diversity, the functional characteristics of fact-checking organizations are denoted by their names. Experts have (rightly) observed that, while mis/dis/mal-information spreading is mainly dominated by very active users, the fact-checking is still a more grass-roots activity [10]. Furthermore, one serious drawback of the fact-checking and debunking activities is related to the fact that human observers perform poorly in the detection of fake news, and machines even slightly outperform humans on certain tasks [11, 12]. The mathematical modelling of information diffusion processes showed that there is a threshold value for the fact-checking probability that guarantees the complete removal of the hoax from the network which does not depend on the spreading rate, but only on the gullibility and forgetting probability [13]. This also raises a series of fundamental issues: how efficient are the tools and platforms aimed to combat information disorder? Which factors affect their performance and how to evaluate this in the first place?

To answer to these questions, we define a methodology of work that includes: systematizing the components of a fact-checking system into a taxonomy, defining the factors that influence the performance of fact-checkers, identifying indicators to evaluate the performance, and empirically validating all of these through concrete evaluation of European fact-checking organizations. Here, we only briefly describe these methodological steps, and only devote special attention to presenting the results from the empirical study in the next section.

By drawing analogies to the computational trust systems and supporting them with relevant proofs, we determined the following three main components that any future fact-checking system needs to integrate: *Information gathering*, *Decision-making* and *Response*. Then, based on an extensive literature and case-studies review of approaches in a variety of contexts, we identified the following performance indicators for the operational and functional characteristics of fact-checkers: *internal coordination*, *external coordination*, *tracking impact*, *tracking progress*, *clarity of objectives*, *accounting for transparency*, *self-assessment procedures* and *incentives policy*. The analysis of the identified indicators is either implicitly or explicitly embedded into the analysis of the effectiveness and efficiency indicators whose maximization is the most desirable performance aspect. These are also the major aspects integrated into a special dedicated Questionnaire[5] for evaluation of fact-checkers' performance. The Questionnaire was distributed to all EU fact-checking organizations. The results and the analysis are part of the empirical study presented in the following section.

[5] https://goo.gl/forms/IWcSpy6yOZ9Rv4KF2

V. EMPIRICAL STUDY

The scientific validity of the above described methods and approaches depends on the cooperation of the target organizations and the maturity of their projects. As a primary database of fact-checking organizations we used the list compiled by Graves and Cherubini in [4] and additional extended searches. Thus, 50 European organizations were approached, located in 27 countries. The majority of the organizations were contacted through their official website or through their publicly available emails. In 12 cases, however, online form was the only available form of communication. In addition, Facebook was used to establish contact with 7 of them, appearing to be the only possible way. The period of contacting all of the organizations was throughout December 2017 and April 2018. Despite the online communication, we also asked local contacts for help in several cases, such as in Finland, Italy, Latvia, Norway, Poland and UK. The feedback rate (number of feedbacks vs. the overall number of surveys distributed), although not very high, allowed us to carry out highly relevant and statistically meaningful analysis. This paper summarises the key findings and recommendations from these performance analyses. The analysis is approached in a multidisciplinary manner and embraces the expertise and experience of people with diverse backgrounds helping to tackle the issues elaborated in this study[6].

A. Key findings

The activities of fact checking initiatives (FCIs) represent an unalienable part of the process of the fight against information disorder. These grass root initiatives should be supported and encouraged to evolve further.

- The biggest reported challenges for FCIs include insufficient stakeholders' awareness on the issues related to information disorder and lack of adequate resources. FCIs should be encouraged to publicise widely information about their activities, methods and outcomes. On the other hand, the appropriate financing of these organizations depending on their ethical and transparent behaviour should be perceived as an important element of the successful fight against fake news.
- Although there is a clear general goal set for all of the investigated FCIs, there is a lack of clarity on the part of the organizations in the sub-goals and objectives that concern the internal processes of the organizations' operation. This demands considerable improvement of the organizational culture and practices pursued by these structures.
- The number of debunked news/hoaxes (last three-months average) varies highly across countries and is very much context dependent – influenced by both the general political situation and ad hoc events (e.g. elections).
- Majority of FCIs are 'specialized' in a single content type. Specific visual content (photos, YouTube), although known to have far greater impact in the proliferation of fake news than text, is addressed to a lesser extent.
- The extent to which automated and semi-automated software are employed in these projects is very low, although there are already complete end-to-end

[6] The extensive analysis with graphical representation of the results are available at: http://compact-media.eu/wp-content/uploads/2018/04/Performance-assessment-of-fact-checking-organizations_A-critical-overiview-Full-Research-1-1.pdf

computational fact-checking solutions available. Most of the FCIs do pay attention to revision of tools, but there is still a significant number of them that have not yet considered this option. IT companies can help in this respect providing advice and technical support to these organizations.

- The majority of the FCIs select their target sources and media by some predefined criteria, the most common of which is 'public interest about the fact-checked information'. Furthermore, most of the FCIs employ some mechanisms for information source evaluation (credibility, independence, etc). However, even those that do pay attention to the independence of sources rely only on human-expertise and subjective evaluations.
- Almost all of the projects envisage political and human impact, and most of them are aware of the societal impact the work may have in general. Yet most of the FCIs do not track, monitor and evaluate any impact, which may jeopardize in practice the long-term results and, generally, the far reaching effect envisaged.
- Many of the FCIs provided evidence of agenda-setting impact (e.g. legacy media referencing the results of their work) as part of their effectiveness assessment. This, in and of itself, speaks of the importance of fact-checking efforts in complementing the existing strategies for combating information disorder.
- Considering the distribution of users reached over the duration of a given project, it can be noticed that most of the projects have similar rate of expansion of their user base, with the oldest projects having significantly larger audience.
- Little considerations were reported with regard to sustainability plans and long-term goals of the FCIs.
- There appears to be strong collaboration among most of the EU FCIs reported by the respondents of the survey. However, there is also a significant overlap in the domain of acting when there are two or more separate FCIs in a single country.
- The transparency of the majority of FCIs (in terms of methodology, funding and operation) remains blurred. There is little willingness to be transparent about key information by the majority of FCIs in Europe. This calls for appropriate guarantees for higher openness and transparency of the activities of these organizations, more intense civil society and public involvement.
- The number of people engaged in the fact-checking process varies greatly among organizations (from 3 to 30). We noted that almost two thirds of the FCIs report that their staff has been increasing over time.
- There is high interest and potential for involvement into the regulatory issues related to the combating of information disorder online on both national and European level. Concise national and EU strategies in this respect should be elaborated that include the FCIs.

B. Key Recommendations

The key recommendations extracted based on the empirical study address the main stakeholders on whose active cooperation the successful fight against information disorder depends:

i. The public sector

On the basis of our observations and conclusions, a case can be made that efficient and effective efforts for combating information disorder demands for more focused and persistent efforts on the part of the states and the European institutions and may soon become an element of a general set of cybersecurity measures. In this respect, the idea of enlarging the scope of the Budapest Convention on Cybercrime through the adoption of a new additional protocol or amending the existing Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems can be considered as a possible solution in extreme cases of information disorder. In the EU context, the revision of the Audio-visual Media Services Directive leading to harmonised measures against fake news distribution could be seen as a proper step forward.

Fact-checking and debunking activities, although helpful, do not solve the urgent and persistent problems with information disorder which imperil basic social principles and values. There is a need for a fundamental change in the communication policies (e.g. causal explanations), educational policies (e.g. in media literacy curricula) and in the regulatory policies and practices. Effective implementation of the policies adopted through a complex set of measures is mostly needed on a national and European level.

ii. The business sector

The business sector should follow and support the overall process of combating information disorder, including through the direct support of the FCIs. Businesses should be vigilant and creative in responding adequately. They should strive to bootstrap the adoption of new software solutions and to facilitate the technical support and advice to the organizations that target and fight information disorder. Although social platforms are used to promote and disseminate the work of the FCIs, an interactive mode of promotion could be an obvious point where improvements can be sought and achieved.

iii. Civil society

The efforts of a stronger and independent civil society should underpin the process of awareness-raising among stakeholders and the public at large in order to give more credibility to the FCIs' work and raise the publicity of the issues related to combating information disorder. At the same time, the civil society debate over the activities of FCIs is an essential element of the overall scrutiny in a democratic society aiming at greater openness and transparency, and with that, facilitating the trust establishment among people, platforms, organizations, institutions, and societies per se.

iv. Fact-checking and debunking organisations and initiatives

FCIs should broaden their methodological means for approaching fact-checking issues. This includes relying on variety of experts from different fields, and being open for employing novel approaches including computational semantic analysis. The latter even appears to be urgent, considering the limited, imperfect, slow and costly human-based approaches to fact-checking, and, moreover, the emergence of artificial intelligence techniques for creation

and distribution of fake news and information in general. In this respect, cooperation with IT companies and the business sector at large proves crucial.

FCIs should increase and adjust their efforts in wider coverage of specific visual (photos) and audio-visual (video) materials. Finally, there is a need for proper sustainability and business plans of the FCIs to be in place.

v. Information Technologies community

The technical community should support the innovation efforts of FCIs and enable them to be up-to-date with their operational and methodological means, but also effective and efficient in their fight against information disorder. The support must come through concrete solutions and products adjustable to the context of operation of the FCIs.

vi. Academic community

The academic community must put efforts in the exploration of the structure, organizational culture and functions of FCIs with the purpose of improving their performance. Carrying out fast-track, yet complex scientific performance assessment of all EU FCIs based on alternative methodologies (possibly in comparison with other non-EU FCIs) is both desirable and efficient in dealing with emergent information disorder issues. It would be also useful to carry out performance assessment of EU FCIs based on additional set of criteria/indicators, such as economic indicators (e.g. ROI, cost per output, etc. at least as indicative measures).

vii. The media

The media on a national, European and global level should give larger publicity to the work and achievements of FCIs. The cooperation between the media accountability bodies and the network of FCIs can prove to be a fruitful undertaking in the process of combating fake news and information disorder in general.

C. Discussion

Although performance analysis was at the heart of the empirical study, the study itself supports a more general hypothesis: although lack of trust is mainly connected to transparency issues, the root of the problem goes few steps back – to the provision of incentives for fact-checking organizations to be transparent in the first place. This implies having the willingness to share both the results and the problems rising from the organizations' work. This, in turn, calls for proper inter-relations between all stakeholders concerned by the information disorder problem. It is only by a systemic approach that the complete chain of trust can be established in the content, the platforms, the service-providers, and the whole Internet value-chain. The human-centricity of all the systems and the blurred borders between providers and consumers in the digital age calls for a holistic approach in the design, analyses, and the maintenance of technological systems on which the whole society relies. Among the most important realizations of this work, however, is that trust is not something that can be embedded into the design of the systems, but something that emerges out of the interactions among the entities comprising the systems. Therefore, the study extracts specific stakeholder recommendations for combatting the problem of information disorder and revitalizing the trust chains on the Internet.

VI. CONCLUSION

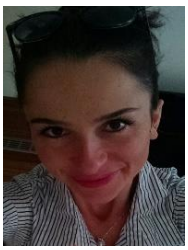
The study analysed the problem of information disorder on the Internet through the fake news phenomenon and established its relation to the socio-economic phenomenon of trust. It is a contribution to the development of fact-checking systems, the combat against information disorder in general, but more importantly, to the debate on how to make the Internet a trustworthy habitat of both virtual and non-virtual entities.

ACKNOWLEDGMENTS

The author would like to acknowledge that this work was supported by the EU H2020 CSA project COMPACT, with Grant agreement No 762128 and was performed as part of the activities within the project. The author also expresses her thankfulness for and acknowledges the contribution and help by Dr. Bissera Zankova and Dr. Andrej Skolkay in carrying out the presented study.

REFERENCES

[1] Nielsen, R. Kleis. Digital News Report 2017. Oxford: Reuters Institute for the Study of Journalism, 2017.
[2] Stencel, M., "A big year for fact-checking, but not for new U.S. fact-checkers." Reporterslab, https://reporterslab.org/big-year-fact-checking-not-new-u-s-fact-checkers, 2017.
[3] Bae Brandtzaeg, P. and A. Følstad. „Trust and Distrust in Online Fact-Checking Services." Communications of the ACM 60 (9): 65-71, 2017.
[4] Graves, L. and F. Cherubini. The Rise of Fact-checking Sites in Europe. Reuters Institute for the Study of Journalism, 2016.
[5] Marwick, A. and R.Lewis. Media Manipulation and Disinformation Online. Data & Society Research Institute, 2017.
[6] Rubin, V. L., Y. Chen, and N. J. Conroy. "Deception detection for news: Three types of fakes." Proc. Assoc. Info. Sci. Tech. 52: 1–4, 2015.
[7] Allcott, H and M. Gentzkow. „Social media and fake news in the 2016 election." Journal of Economic Perspectives 31 (2): 211-236, 2017.
[8] Hirst, M. "Towards a political economy of fake news." The Political Economy of Communication 5(2): 82–94, 2017.
[9] Wardle, C. and H. Derakhshan. Information Disorder. Toward an interdisciplinary framework for research and policymaking. Strasbourg: Council of Europe, 2017.
[10] Chengcheng Shao, G. Luca Ciampaglia, A. Flammini and F. Menczer. "Hoaxy: A Platform for Tracking Online Misinformation." In Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion)., Republic and Canton of Geneva, Switzerland, 2016.
[11] Rubin, V.L., and N. Conroy. "Discerning truth from deception: Human judgments & automation efforts." First Monday 17: 3–5, 2012.
[12] Wineburg, S., S.McGrew, J.Breakstone, and T. Ortega. Evaluating Information: The Cornerstone of Civic Online Reasoning. Stanford Digital Repository, 2016.
[13] Tambuscio, M., G.Ruffo, A. Flammini, and F. Menczer. "Fact-checking Effect on Viral Hoaxes: A Model of Misinformation Spread in Social Networks." In Proceedings of the 24th International Conference on World Wide Web (WWW '15 Companion), 977-982. New York, NY: ACM, 2015.



Tanja Pavleska is a researcher at the Laboratory for Open Systems and Network, Jožef Stefan Institute, Ljubljana. She graduated from the Faculty for Electrical Engineering and Information Technologies, Skopje, Macedonia. She obtained her PhD from the Jozef Stefan International Postgraduate School in the area of Computational trust and reputation systems, with special emphasis on the user behaviour in the online social platforms. Her main interests are in trust and reputation management, information disorder, user behaviour in crowdsourcing and content delivery platforms, cybernetics and complexity principles in online systems, and probability theory in user behaviour modelling.

Can we trust cryptographers?

Samed Bajrić, Jožef Stefan Institute, Laboratory for Open Systems and Networks

Abstract — This article explains which cryptographic primitives can be trusted. Cryptographic algorithms are useful only if they are secure and we can trust them. There are lots of algorithms like that but we are not always allowed to use them. The primitives recommended by the cryptographic community are those which have been chosen after an international competition. Within such an open contest, like AES and the SHA-3 selection processes, all proposals have been carefully analysed by all participants. In addition, the only cryptanalysis and security evaluations can bring confidence in a primitive.

Keywords — cryptographic primitives, AES, SHA-3, cryptanalysis

Povzetek — Ta članek opisuje, katerim kriptografskim primitivom lahko zaupamo. Kriptografski algoritmi so uporabni le, če so varni in jim lahko zaupamo. Obstaja veliko algoritmov, ki jih ne moremo uporabljati. Primitivi, ki jih priporoča kriptografska skupnost, so tisti, ki so bili izbrani po mednarodnem tekmovanju. V okviru takega odprtega natečaja, kot so postopki izbire AES in SHA-3, so vsi udeleženci skrbno analizirali vse predloge. Poleg tega, edino ocena kriptoanalize in varnosti lahko prinese zaupanje v kriptografske primitive.

Ključne besede — kriptografski primitivi, AES, SHA-3, kriptoanaliza

I. INTRODUCTION

The world is run on codes and ciphers. From emails to automated teller machines (ATMs), entertainment and shopping online, cryptography inhabits our every waking moment. In fact, life as we know it would be practically impossible without it. Cryptography is a cornerstone of everyday digital security as it aims at ensuring confidentiality and integrity of digital communications. Its fundamental objective is to enable communications over an insecure channel in such a way that a potential adversary cannot understand what is being conveyed [14]. These tasks are achieved by using public key cryptography and symmetric cryptography where the two parties that want to communicate share a common key.

Symmetric block ciphers are the most widely used cryptographic primitives. Block ciphers used as basic components in the construction of hash functions, message authentication codes, pseudorandom number generators, as a part of various cryptographic protocols, etc. As these primitives are widely used, it is of outermost importance to evaluate the actual security level they ensured, and cryptanalysis aims at testing these security levels. This task usually consists in mounting attacks for recovering secret keys or a part of them.

In this paper we briefly discussed which cryptographic primitive can be trusted. In particular, in Section II. some attacks against the cryptographic primitives are given. A hash function competition is described in Section III. Some conclusion remarks are given in Section IV.

II. ATTACKS AGAINST THE CRYPTOGRAPHIC PRIMITIVES

The first and most important rule for the designer of a cryptographic primitive is called Kerckhoff's Principle: "A cryptographic system should be secure even if everything about the system, except the key, is public knowledge." Much of the theoretical work in cryptography concerns cryptographic primitives with basic cryptographic properties, and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called cryptosystems or cryptographic protocols, which guarantee one or more high-level security properties. Note however, that the distinction between cryptographic primitives and cryptosystems is quite arbitrary. For example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

While it is supposedly hard to attack the full cryptographic algorithm, it is much easier to attack the cryptographically weak intermediate variables. For example, Transport Layer Security (TLS) [6] and its predecessor Secure Socket Layer (SSL) [7] are two important cryptographic, certificate based protocols that satisfy secure communication in a network channel. They are widely used in many areas such as online banking systems, online shopping, e-mailing, military systems or governmental systems. Some vulnerabilities and attacks towards these protocols are listed below.

- Rivest cipher four (RC4) is a very widely-deployed stream cipher, but its usage in particular applications such as TLS and Wi-Fi Protected Access (WPA) has recently come under heavy attack. An attack targets two unknown bytes of plaintext that are located close to sequences of known plaintext bytes, a situation that arises in practice when RC4 is used in TLS [8].
- Logjam attack against the TLS protocol. The attack is due to a flaw in the TLS protocol rather than an implementation vulnerability [2]. The attack affects all modern web browsers; 8.4 % of the top 1 Million domains were initially vulnerable.
- SLOTH [5] is an acronym for the loss of security due to the use of obsolete and truncated hash constructions in mainstream Internet protocols. It is part of a series of recent attacks on the use of legacy crypto constructions such as collision in MD5.

Another major disaster caused by cryptography is MIFARE contactless cards developed by NXP [12]. Ten billions of these chips have been sold. They have been used

in the most major transportation networks, physical and logical access control, government and corporate IDs, but they have been broken, because they use a very bad encryption algorithm.

The natural question is whether cryptographers can be trusted? The first situation is when cryptographers say that a primitive is broken, and do not trust them and do not use it. Even in this simple situation it is not so easy to trust cryptographers, because everybody knows that those guys are a little bit paranoid. This observation will be considered in the following subsections.

A. Broken cryptographic primitives

Cryptanalysis is the study of techniques for breaking a cryptographical primitive. When evaluating the strength of a cipher, we generally compare it to the generic attack of exhaustively searching over all possible keys to find the right one. This attack is called exhaustive key search. No practical cipher will be more secure than the time it takes to test all keys, so in a sense, this is the highest achievable strength of a cipher. For instance, the Spritz is a stream cipher proposed by Rivest and Schuldt at CRYPTO 2014 [13]. It is intended to be a replacement of the popular RC4 stream cipher and hence the design for Spritz was chosen meticulously, with special attention given to the fact that known weaknesses of RC4 do not carry over. The authors in [3] calculated the probability of an algorithm to recover the internal permutation. Their estimated evaluation suggests that we need approximately 2^{1247} assignments to recover the internal state which is much better than the exhaustive key search 2^{1730} operations. Besides, that is significantly more than the estimated number of atoms in the Universe raised to the fourth power. Therefore, does it really make a sense to say that this cipher is broken? The answer depends on what cryptographers mean by the term ‘broken’. When a primitive does not have an ideal behaviour, then cryptographers mean that the primitive is broken. Moreover, an ideal behaviour means that the primitive behaves like a function which has been randomly chosen from the set of all functions having the same parameters.

B. Hash functions

A hash function transforms an arbitrarily long input into a fixed length digest. This construction is secure if it satisfies three conditions: collision resistance, preimage resistance, and second preimage resistance. Collision resistance is achieved if it is computationally impossible to build two messages that hash to the same value. Preimage resistance means that it is computationally infeasible to reverse a hash function, i.e. to find a message that hashes to a given digest. Finally, second preimage resistance requires that given an input and its digest it is hard to find a different input with the same digest.

Hash functions are used in many important security-critical applications like digital signatures, timestamps, message authentication codes and authentication protocols. Attacks against hash functions [11] may thereby have a large influence on the overall security of electronic services. Several hash functions like MD5 and SHA-1 that are still in use in some applications today have been successfully attacked in terms of collisions. As replacing a hash function in widely used applications tends to be very costly, it is extremely important to know what exactly the practical consequences of the collision attacks are. Finding a collision for a hash function does not necessarily mean that the hash function is insecure in every possible application. Some applications may just need preimage resistance of second preimage resistance, not the full collision resistance. For example, SHA-1 with 160-bit output, cannot be more than 2^{160} secure preimage resistant, nor 2^{80} secure collision resistant (due to the Birthday attack). Another example is MD5 with 128-bit output, is no more than 2^{128} secure pre-image resistant, nor 2^{64} secure collision resistant (due to the Birthday attack). Therefore, even if we think that this kind of attack is not practical, because it has a huge time complexity, then we should take it into account because attacks reveal some unexpected behaviour. A behaviour which has not been expected by the designers is usually very bad sign, because it often opens doors to more see flows and a very good rule is that the attacks always get better, they never get worse.

III. OPEN PUBLIC COMPETITIONS

The SHA-3 cryptographic hash function standard was released by NIST in August 2015 [9]. SHA-3 is a subset of the broader cryptographic primitive family Keccak [4] designed by G. Bertoni at el. Namely, during 2006–2012, NIST organized a hash function competition in order to choose a new hashing algorithm for the upcoming hash standard, SHA-3. The reason was not to replace SHA-2 as no practical attacks were known against SHA-2. However, successful attacks against MD5 and the earlier version of SHA-1 showed that more hash functions are needed, possibly with the structure that deviates from the standard Merkle-Damgard design. Indeed, Keccak is based on the so-called sponge design that is somewhat different from all the previous hash functions. After a setup period, admissions were to be submitted by the end of October 2008. Keccak was accepted as one of the 51 candidates. In July 2009, 14 algorithms were selected for the second round. Keccak advanced to the last round in December 2010. During the competition, entrants were permitted to "tweak" their algorithms to address issues that were discovered. On October 2012, exactly 4 years after the submission deadline, Keccak was selected as the winner of the competition.

Recently, NIST specifies four types of SHA-3-derived functions: cSHAKE, KMAC, TupleHash and ParallelHash, each defined for a 128- and 256-bit security strength [10]. cSHAKE is a customizable variant of the SHAKE function. KMAC (Keccak Message Authentication Code) is a variable-length message authentication code algorithm based on Keccak; it can also be used as a pseudorandom function. TupleHash is a variable-length hash function designed to hash tuples of input strings without trivial collisions. ParallelHash is a variable-length hash function that can hash very long messages in parallel. All four functions defined above have these properties in common:

- They are all derived from the functions specified in Federal Information Standard 202;
- All support variable-length outpusts of any bit length. KMAC, TupleHash, and ParallelHash have additional property that any change in the requested output length completely changes the function. Even with identical inputs, otherwise any of these functions when called with different requested output lengths, will, in general, yield unrelated outputs;

– All support user-defined customization strings.

Similarly, for the Advanced Encryption Standard (AES) which has been standardized after a similar open competition [1], consisting of ten rounds, and some attacks against on five and six rounds have been published by the designers themselves in the submitted document. Then, during the competition attack on 7 rounds has been improved by several sets of offers. Nowadays, twenty years after the submission of AES, we are only able to attack seven rounds out of ten rounds of the function. Therefore, this is a very good security primitive.

A. No public analysis, no trust

Conversely, if some cryptographic primitive does not benefit from a public analysis, as we described above, then there is no reason to standardize it. For instance, if someone looks at the design of CRYPTO-1 developed by NXP [12], then it can be seen that it has a proprietary design but the specification were kept secret. This is a typical situation where there is no reason to trust the primitive, because it is well known that CRYPTO-1 is no more secure.

More interestingly, two block ciphers SIMON and SPECK, which have been proposed by the U.S. National Standard Agency (NSA) in 2013 are dedicated to a low-cost devices. Both perform exceptionally well across the full spectrum of lightweight applications, but SIMON is tuned for optimal performance in hardware, and SPECK for optimal performance in software. The NSA has been pushing Simon and Speck really hard as standards, but it did not happen. The International Organization for Standardization (ISO) last year decided not to approve the NSA encryption algorithms Speck and Simon after expressing concerns that the NSA was able to crack the encryption techniques and would thus gain a back door into coded transmissions.

IV. CONCLUSION

An open public competition is a favourite process in cryptography for finding and defining new standards or recommending new cryptographic primitives. Therefore, the public analysis is the only security argument that has to be considered. Have in mind that a critical thinking is something which is essential for our everybody's life and that is the same in cryptography. Cryptanalysis is essential for the security.

REFERENCES

[1] Announcing the Advanced Encryption Standard (AES). National institute of standards and technology, 2001.

[2] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thome´, L. Valenta *et al.* Imperfect forward secrecy: How diffie-hellman fails in practice. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, Denver, USA, 2015.

[3] S. Banikad, and T. Isobe. Cryptanalysis of the full Spritz stream cipher. Fast Software Encryption: 23rd international conference, Bochum, Germany, 2016.

[4] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche. The Keccak sponge function family: specifications summary. 2011.

[5] K. Bhargavan, and G. Leurent. Security losses obsolete and truncated transcript hashes (CVE-2015-7575). miTLS.org.

[6] T. Dierks and E. Rescorla. The transport layer security (TLS). Protocol version 1.2. RFC 5246, 2008.

[7] A. Freier, P. Karlton, and P. Kocher. The secure sockets layer (SSL). Protocol version 3.0 – 1996. RFC 6101, 2011.

[8] N. J. AlFaradan, D. J. Bernstein, K. G. Paterson, B. Poettering, and J. C. N. Schuldt. On the security of RC4 in TLS and WPA. In Proceedings of the 22nd USENIX conference on security, Berkley, USA, 2013.

[9] M. J. Dworkin. SHA-3 standard: permutation-based hash and extendable-output functions. Federal Information Processing Standards, 2015.

[10] J. Kelsey, S. Chang, and R. Perlner. SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash. NIST Special Publication 800-185, December 2016.

[11] S. Marc. Attacks on hash functions and applications. PhD Thesis, 2012.

[12] NXP Semiconductors. MIFARE Standard 4KByte Card IC functional specification, 2007.

[13] R. Rivest and J. Schuldt. Spritz - a spongy RC4-like stream cipher and hash function. http:// people.csail.mit.edu/ rivest/pubs/RS14.pdf

[14] W. Stallings. Cryptography and network security. Prentice Hall, fifth edition, 2011.

Samed Bajrić has received the Ph.D. degree in mathematics from University of Primorska, FAMNIT, Koper, Slovenia, in 2014. His main research interests include stream cipher design and in a particular the design of cryptographic Boolean functions. He is currently with Laboratory for Open Systems and Networks, Jožef Stefan Institute, Ljubljana, Slovenia.

Security in the case of a WebRTC–based media server

Valerij Grašič, Ana Robnik, Grega Prešeren, Iskratel, Kranj

Abstract — A role of the media servers in legacy telecommunication networks has been related to audio content. The media server was in a secure network, which simplified the security policy. When integrating video and collaboration tools, specifically the WebRTC, into the media server, the security issue becomes more complex. Additional security requirements arise in case of upgrading the media server to support WebRTC. Each element in architecture has its role, and thus also affects security itself. We are interested in what are those elements which are vulnerable and what role they can play on the network and what are attack vectors. Above all, we are interested in an appropriate security policy that can be put in place. This includes the connection types, necessary measures and implementation scenarios for devices on the internet connected to a media server in a safe area. We have also considered security dilemmas for public safety systems. We have found that WebRTC also offers viable security for these cases.

Keywords — Media server, audio, video, WebRTC, security

Povzetek — Vloga medijskega strežnika v dosedanjih telekomunikacijskih omrežjih je bila povezana z avdio vsebinami. Medijski strežnik je bil v varnem omrežju, kar je poenostavljalo politiko varnosti. Ob vključevanju videa in orodij za sodelovanje, konkretno WebRTC, v sam medijski strežnik, postaja tudi vprašanje varnosti bolj kompleksno. Pojavljajo se dodatne varnostne zahteve v primeru nadgradnje medijskega strežnika za podporo WebRTC. Vsak element v arhitekturi ima svojo vlogo, s tem pa tudi vpliva na samo varnost. Zanima nas, kateri elementi in v kakšnih vlogah lahko nastopajo v omrežju, katere so možne ranljivosti in vektorji napada. Predvsem pa nas zanima primerna politika varnosti, ki jo moremo udejanjati. Ta vključuje načine priključevanja, ukrepe in scenarije izvajanja te politike pri povezovanju naprav v internetu do medijskega strežnika v varnem območju. Proučili smo tudi dileme v zvezi z varnostjo za sisteme javne varnosti. Ugotovili smo, da WebRTC nudi primerno varnost tudi za te primere.

Ključne besede — medijski strežnik, avdio, video, WebRTC, varnost

I. INTRODUCTION

In the telecommunications system, a media server is also an essential element that acts as an aggregator of information. Video, audio, photos and books, and other types of media can all be accessed via an IMS (IP Multimedia Subsystem) and NGN (Next-generation Network) network by using media servers that manage the media efficiently. We are moving from an environment dominated by audio to an environment where a wide range of real-time communications is going to be present. In such an environment, the video is becoming more and more critical from various perspectives. WebRTC (Web Real-Time Communication) [1] is an opportunity for telcos to sell enterprises WebRTC-based hosted telephony services as a substitute for traditional PBX systems. Additionally, for the enterprise market WebRTC opens the doors to new market channels with high potential such as social networking, video streaming services, healthcare, gaming and others.

In TDM environment with audio services, we approached security quite differently compared to how it is done (or should be done) today in IP internet environment with rich communications services. However, when using virtualisation and opening network to the whole IP world, new security concerns are increasingly appearing. The security issues become even more complicated when moving toward real-time communications over the internet, which integrate data, collaboration and video as it is a case of WebRTC.

All this is even more critical because of the anticipated growth of WebRTC technology usage. WebRTC is widely deployed across all the major browsers, both on desktop and mobile, and has already re-shaped the world of real-time communications. Recently, YouTube has also opened the door to WebRTC as a way to start a live stream [2]. In addition, according to the report from Future Market Insights (FMI) [3] the global WebRTC solutions market is going to increase at a CAGR of 45.2 percent from 2015 to 2025. At this time, it is going to reach over $22 billion.

II. MEDIA SERVER ARCHITECTURE

A. *A media server in a virtualised environment*

CSP (Cloud Services Platform) [4, 5] is Iskratel cloud-services platform that guarantees high availability and geo-redundancy of cloud services for different industry verticals on an open, ETSI NFV (Network Function Virtualisation)-compliant architecture. It enables grouping of services from different industry verticals into unique solutions. CSP entirely follows the standard ETSI NFV [6] architecture and runs on the COTS (Commercial off-the-shelf) platform such as HP or Lenovo.

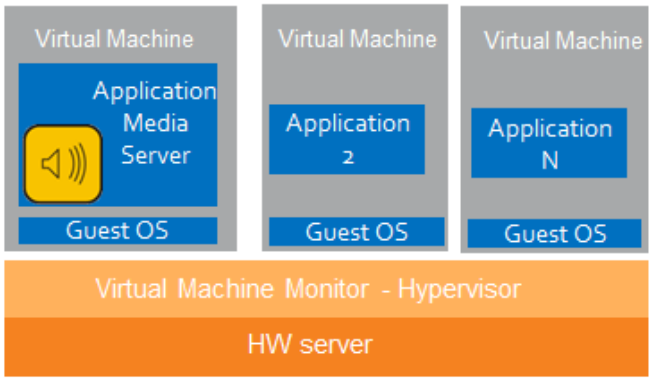
The MS (Media Server) resides on CSP as a stand-alone, virtualised network function. Virtualization uses KVM (Kernel-based Virtual Machine) hypervisor system. The system platform uses Linux operating system (WindRiverLinux 7). It includes programs and libraries of logging packages, startup tests, and alarms.

Picture 1 shows media server in a virtualised environment. The media server is one of the applications, which reside on a separate virtual machine.

B. *Audio-based architecture*

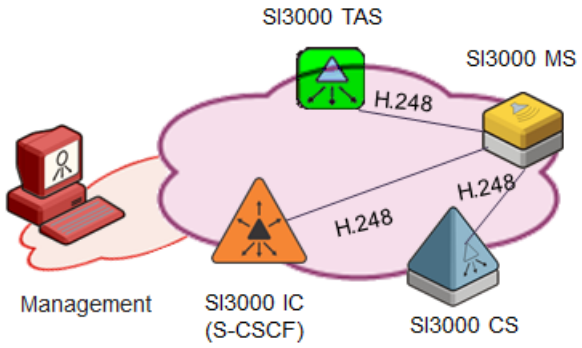
Main functionalities of media server are DTMF (Dual-tone multi-frequency signalling) generation and detection of tones, announcements, transcoding, audio conferencing, and RTP proxy. Additionally, different media actions can be

logically combined and embedded in a service logic execution environment using VoiceXML (Voice Extensible Markup Language). The media server supports different codecs for audio and video.



Picture 1: Media server in a virtualised environment

Media server acts as the MRF (Media Resource Function) in IMS environment. Connection to the environment, as for softswitch (in NGN environment), S-CSCF (Serving-Call Session Control Function) or TAS (Telephony Application Server) (in IMS environment) is based on H.248 protocol. The transport protocol for H.248 is UDP. The S-CSCF is essentially a SIP proxy augmented with the triggering point for user services hosted on application servers. TAS provides core telephony application and a large number of supplementary services as standard IMS Application Server. Product management is carried out via Iskratel product MNS (Management Node System). Picture 2 shows the media server within the network.



Picture 2: Media server within the network

The media server functionality uses GStreamer [7], which represents a set of open-source libraries that condition the main functionality of the media server. GStreamer has support for WebRTC for real-time audio/video streaming to and from web browsers, experimental support for the next-gen royalty-free AV1 video codec and Video4Linux. It also has support for the SRT (Secure Reliable Transport) video streaming protocol.

C. WebRTC based architecture

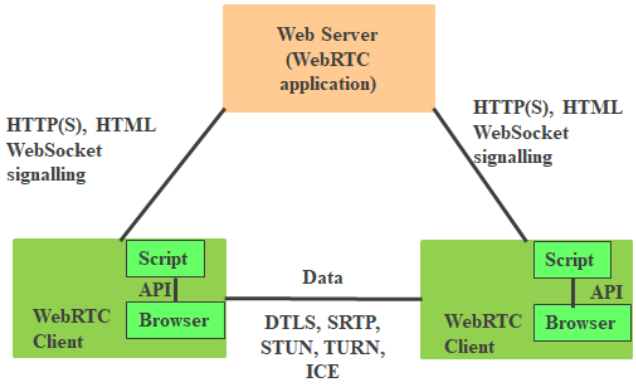
WebRTC is an open source project based on open source API (Application Programming Interfaces). It enables real-time communication over the internet. WebRTC makes video calls possible not only between WebRTC clients (browsers) but including also SIP or GSM terminals. It supports HTML5. WebRTC uses different standards and protocols.

Three standardisation bodies contribute to WebRTC standardisation. IETF (Internet Engineering Task Force) takes care about media plane, overall architecture and security framework, W3C (World Wide Web Consortium) takes care about HTML5 JavaScript API for browsers and 3GPP (3rd Generation Partnership Project) integrates WebRTC access into IMS.

The architecture of WebRTC consists of the web server, web browsers, STUN (Session Traversal Utilities for NAT) and TURN (Traversal Using Relays around NAT) servers and protocols connecting these elements. Picture 3 shows such an architecture. WebRTC can work in both centralised and decentralised, peer-to-peer (P2P) mode, which allows media and data to be exchanged directly between peers. Using an SFU (Selective Forwarding Unit) allows peers to upload media and data streams only once. When used, the user or peer send media and data from one user or peer to a server that acts as a relay point for all the other peers connected to that server. The server then "multiplexes" the streams and distributes them to the receiving peers.

The significant components of WebRTC are:

– getUserMedia, which makes possible for the browser or the native app to get access to the device camera or microphone,
– RTCPeerConnection, which makes audio or video calls possible by the device (remote peer),
– RTCDataChannel, which makes possible a peer-to-peer communication to be established between the devices by using browsers or native app.



Picture 3: WebRTC architecture

The system transports audio and video over an encrypted media connection in a compressed format by using standard codecs. The client-side application script (JavaScript) invokes a W3C specified browser API that instructs the browser to transfer audio or video between local devices (which can be a microphone, speaker, camera or display) and a remote endpoint via IETF defined protocols.

In our case, we have used Janus [8]. It is an open source implementation of WebRTC, promoted by Meetecho, a company born [9] in 2009 as an academic spin-off. Janus is a PaaS (Platform as a Service).

The central part is the Janus WebRTC server, uniquely equipped with its "video room" plug-in:

– Through its multiple plug-ins, it can add different behaviours and logic, from SFU (Selective Forwarding

Unit) to MCU (Multipoint Control Unit), Gateway, and recording.
– It does not impose any signalling on your application, and it implements support out of the box for quite a number of signalling transport protocols such as REST (Representational State Transfer), Web Services, MQTT (Message Queuing Telemetry Transport), etc.
– Thanks to a C code base, it scales down, so it is possible to have a full server running on a Raspberry Pi, and many other IoT options.

To communicate to Janus, the system engineers can use JSON-based protocol called the Janus API. This "signalling" protocol can be transported over different "transport" protocols. Such an example is SIP over WS (WebSocket), where SIP is the signalling protocol, and WS is the transport protocol [10].

III. SECURITY FOR THE MEDIA SERVER

A. *Security for a virtualised environment*

Hosting multiple virtual networks on a shared network infrastructure introduces new security challenges. Security in virtualised environment is based on network virtualisation security, networking security, and Virtual Network Function (VNF) security, all of them comprise an Iskratel security architecture.

Each entity in this security architecture operates by different management units, and hence we assume a mutual distrust among them. The network infrastructure is vulnerable to attacks originating from the hosted virtual networks or users associated with them. Elements used for networking security are firewalls, Session Border Controllers and Network Intrusion Detection Systems. VNF security is based on NFV framework, as defined in ETSI GS NFV 004. Part of this is communication security, which uses SSH (Secure Shell), TLS (Transport Layer Security), HTTPS (Hyper Text Transfer Protocol Secure) and bridging security domains (public, guest, management and data).

B. *Security for audio-based media server*

Audio-based media server addresses the following security dilemmas:

– Media server connectivity towards Call servers,
– Media server connectivity towards Management node,
– Security issues in conjunction with GStreamer within the media server.

A connection to a call server is based on H.248 protocol, which is text-based protocol. The security issues are related to the port and payload of the protocol.

While managing and supervising media server via MNS the following protocols are used for information and raw data exchange:

– SSH is used for transmission of system configuration data between MNS and MS.
– SNMP (Simple Network Management Protocol) V3 is used for transmission of information about current alarms and error flags.
– sFTP is used for transferring log files with alarms and errors history of program and configuration files or trace files, and for uploading custom VoiceXML files to media server.
– The administration procedures use cryptographic protocols as SSL (Secure Sockets Layer) by default.
– For management purposes, MS uses dedicated "management interface" separated from user traffic. MS administrator can use only this interface, and for changing configuration, the administrator uses the dedicated user id and password.

GStreamer [7] has support for both RTP (Real-time Transport Protocol) and RTSP (Real Time Streaming Protocol). Its RTP/RTSP stack has been over years widely used in production deployments of a variety of mission-critical and low-latency scenarios, from small embedded devices to large-scale video conferencing and command-and-control systems. It also has support for the SRT (Secure Reliable Transport) video streaming protocol. GStreamer's RTSP server (gst-rtsp-server) is a feature-rich and easy-to-use library that allows applications to implement a complete RTSP server with just a couple of lines of code. It is multi-threaded, scalable and flexible, and provides support for static or dynamic mount points, authentication, RTX (re-transmission), encryption (SRTP, secure RTP), UDP unicast and multicast and also TCP interleaving, seeking, and optionally integration for advanced resource management and control.

C. *Security for WebRTC based architecture*

i. *Elements of the security architecture*

The security of WebRTC is a complex matter consisting of several parts [11]. The elements of the security architecture of WebRTC are:

– Network Address Translation (NAT),
– Interactive Connectivity Establishment (ICE),
– Session Traversal Utilities for NAT (STUN),
– Traversal Using Relays around NAT (TURN),
– Datagram Transport Layer Security (DTLS).

To prevent common cyber attacks it is also essential to utilize encryption, authentication and certificates.

ii. *Encryption*

Unlike legacy PSTN systems, or NGN, where encryption was only an option, within WebRTC encryption is mandatory and is a significant contributor to end-to-end security for both consumers and enterprises.

iii. *NAT*

WebRTC takes place almost entirely within the browser, the only exception is when the browser requests resources from backend servers in order to establish a peer to peer connection or work around a firewall or NAT.

iv. *ICE, TURN and STUN*

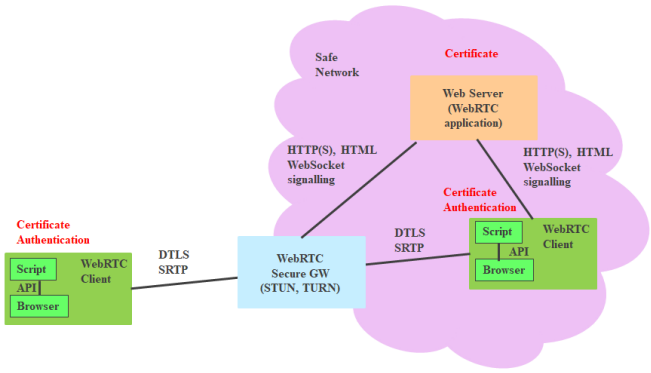
Most NATs/Firewalls are directly managed by browsers using the ICE (Interactive Connectivity Establishment) principles, in most cases without inserting a media relay (such as a TURN server). ICE is a framework for WebRTC.

RFC5245 defines ICE as a technique for NAT traversal for typically UDP-based media streams established by the offer/answer model. ICE is an extension of the offer/answer model and works by including a multiplicity of IP addresses and ports in SDP (Session Description Protocol) offers and answers, which are then tested for connectivity by peer-to-peer connectivity checks.

STUN, defined in RFC 5389, is one of the critical services that ICE uses to connect to private corporate networks. It is STUN's task to discover network address translators as well as IP addresses and port numbers on host networks. STUN also transports the information back to the host. The STUN servers are necessary for setting up direct links between users. Each WebRTC connection uses STUN.

There are some cases where STUN is not sufficient. When this happens, ICE uses the TURN protocol to establish real-time connection. Essentially, TURN helps make connections work when P2P connections would otherwise be blocked due to specific security settings. To work correctly, one needs to install a third party TURN server in-between the two end users, to relay information back and forth. It takes over where peer-to-peer connections are going to fail. Using TURN can add latency and other performance issues, but TURN servers are often mandatory for enterprise solutions and help dramatically increase connection success rates. RFC5766 defines TURN in detail.

.



Picture 4: Proposed WebRTC security architecture.

In our case, the operator can put both servers in one place and set them up at the edge of a secure network. Such a particular element is WebRTC security gateway (GW). Picture 4 shows proposed WebRTC security architecture.

v. *SRTP and DTLS*

WebRTC media is always encrypted using either DTLS-SRTP (defined in RFC 5764) in case of audio and video or using SCTP (defined in RFC 4960) encapsulated in DTLS (defined by RFC 6347) in case of data.

SRTP (Secure Real-time Transport Protocol) provides a framework for encryption and message authentication of media packets.

DTLS (Datagram Transport Layer Security) protocol is a variation of the TLS protocol. It is used to prevent interference or interception during WebRTC sessions on packet-switched networks.

The aim of the use of DTLS is to generate the keys used by SRTP. The DTLS certificate fingerprint(s) must be signalled in the SDP.

WebRTC utilises SRTP [11] for the encryption of media streams, rather than DTLS. This is because SRTP is a lighter-weight option than DTLS. Once the initial ICE checks have concluded (or specifically, some of them), the two peers will start to setup one or more secure channels. Initially, a DTLS handshake is performed on all channels that are established by ICE. For the data channels, this step alone is sufficient as plain simple DTLS is used for encryption. For the media channels, however, further steps are taken. Once the DTLS handshake completes, the keys are "exported" and used to key SRTP for the media channels. At this stage, both parties know that they share a set of secure data and media channels with keys which are not known to any malicious third-party.

Use of SDES (SDP Security Descriptions for Media Streams) is no longer allowed, it was the option previously favoured by WebRTC.

vi. *Ports used*

The topical issue of security is the usage of ports. Table 1 lists the ports used for WebRTC and description of their use.

Table 1: Ports for WebRTC

Firewall Ports	Network Protocol	Application protocol	Description
3478	UDP	STUN service	Used for NAT traversal
3479	UDP	STUN service	Used for NAT traversal
16384-32768	UDP	RTP/RTCP multimedia streaming	Used for audio/video data in SIP, Verto, and other protocols
5066	TCP	WebSocket	Used for WebRTC
7443	TCP	WebSocket	Used for WebRTC

vii. *Authentication of the user*

The WebRTC standard does not specify authentication and therefore a user can be authenticated via any solution. WebRTC can be plugged into existing mechanisms via its peer identity API.

In WebRTC [12], authentication is decoupled from the website allowing users to validate each other directly using third-party identity providers. User's privacy and security highly depend upon the mechanism used for end-to-end authentication. To achieve security and enhance user privacy it is also essential to define trust between various entities involved in WebRTC security architecture.

viii. *Certificates*

Certificates are essential elements of the system. WebRTC offers secure calling through a protocol known as WSS (Web Socket Secure). Browsers are increasingly requiring WebRTC apps in order to meet these WSS security standards before voice or video calls are initiated. To enable WSS, a SSL certificate is needed. The owner of the WebRTC server should provide such a certificate.

The Janus application already has all the necessary support for the utilization of certificates.

IV. SECURITY FOR A WEBRTC BASED MEDIA SERVER IN CASE OF CRITICAL COMMUNICATIONS

WebRTC has been proposed for critical communications in many EU research and innovation projects, the most significant are NEXES [18] and EMYNOS [17]. The results of these European projects show that WebRTC is playing a significant role in public safety and in building a rich emergency applications ecosystem, capable of delivering more and better functionalities for citizens and emergency services. It is possible to use location-based services and

safeguard interactions enabling text communications, audio, and video communications. WebRTC data channel also allows a more in-depth insight into previously existing communications, when responding to emergency calls. The next generation of emergency services supporting Total Conversation (voice, real-time text, video and data) and rich emergency data exchange between citizens, Public Safety Answering Points (PSAPs), Emergency Response Organisations (EROs) and First Responders (FRs) contribute to enhance overall emergency situational awareness and interoperability of emergency services.

A good example of using WebRTC for critical communications is shown in [13]. In 2017 [14] ETSI, in partnership with EENA (the European Emergency Number Association), has organised the second NG (Next Generation) Emergency Services Plugtests™ event. The scope extends to content-rich emergency callings, such as video calling and Total Conversation. It was possible to make emergency calls and video calls using WebRTC callers and WebRTC call takers.

The 5G technologies and services [15] for critical communications are still in the early phases of development, although some of the standards are already available. However, it is likely that WebRTC services delivered over 5G are going to benefit from improvements such as much lower latency, higher bandwidth, ultra-high reliability, guaranteed security, trust, identity and privacy. For example, 5G could enable person-to-person or person-to-group UHD (Ultra High Definition) mobile video communication via WebRTC. Today, this use case would put a very high load on the network or probably would not work at all, but, with 5G, pervasive video, such as collaboration in 3D cyber-office, may well be a likely use case.

WebRTC [16] has a potential impact on both the way the public interacts with the emergency services and internal communications within emergency service organisations, including providing support to first responders. The fact that WebRTC provides the full media stack, including voice, video and data, and uses strong security, makes WebRTC very well suited for use in public safety applications. It is easy to see how WebRTC technology can be used to enhance the way in which the public communicates with emergency service organisations, for example, by adding high quality, secure video capabilities to emergency calling applications. WebRTC applications can also be used to enhance operational effectiveness and situational awareness, by providing prosperous, secure and contextual-based communications for use between emergency responders and the control room.

There is little doubt [16] that WebRTC is going to be the dominant technology for real-time collaboration applications deployed in the cloud over the next few years. It also has some unique properties that make it particularly suitable for use within emergency service related applications, including the built-in encryption and identity features, and the promise of being widely available via browser, without any installation. Given that WebRTC provides ‘always on’ encryption and integrity protection for the media, it would seem that WebRTC is an ideal technology for enhancing the communications between first responders and the control room as well as between emergency service organisations.

V. CONCLUSION

Having been designed with security in mind, WebRTC enforces or encourages important security concepts in all main area, also for media servers. We have started from a virtualised environment and audio-based media server, looking then at WebRTC in more detail.

The media server presented already supports security requirements starting with security by design. Within WebRTC several security measures have been already provided. Therefore, the media server, even in the case of WebRTC, is a safe solution for moving toward a real-time communication world. To summarise, this also means that connection of telco world, based on IMS, is possible with WebRTC. Moreover, it gives good enough security for the end users and the operators. The media server which uses WebRTC is a good solution, both from a technical and a security perspective, for the public safety systems such as NG112. It is no surprise that WebRTC is nowadays becoming more and more important and useful for emergency systems.

The challenge for the future is related to monitoring the practice and the use of WebRTC, and elimination of possible dilemmas that are going to arise regarding security issues.

ACKNOWLEDGEMENTS

We would like to thank our colleagues Miha Polak, Aleš Okršlar, Roman Lotrič and Ignac Zupan, who helped us with tips on safety issues for WebRTC.

REFERENCES

[1] Heavy Reading Insider, WebRTC: Get Ready for the Next Telecom Revolution, Vol. 14, No.6, June 2014
[2] YouTube Does WebRTC – Here’s How https://webrtchacks.com/youtube-does-webrtc-heres-how/
[3] Future Market Insights, https://www.reportbuyer.com/product/3356732/web-real-time-communication-webrtc-solution-market-global-industry-analysis-and-opportunity-assessment-2015-2025.html
[4] V. Grasic, Use of virtualisation in the transition of a telecommunication network toward 5G, Int. J. Digit. Technol. Econ., Nr 2, 2017
[5] G. Prešeren, G. Koritnik, J. Orehar, I. Zupan , Vidiki varnosti Iskratelovega NFV-oblaka pri upravljanju identitet in dostopa, Vitel, Brdo pri Kranju, May 2018
[6] ETSI, Network Functions Virtualisation, White paper, http://portal.etsi.org/NFV/NFV_White_Paper.pdf, October 2012
[7] GStreamer, https://gstreamer.freedesktop.org/documentation/
[8] Janus, https://janus.conf.meetecho.com/docs/rest.html
[9] L. Miniero, A Tale of Two Worlds: Bridging SIP and WebRTC With Janus, Kamailio World, May 2016
[10] A. Amirante, T. Castaldi, L. Miniero, and S. P. Romano. 2014. Janus: a general purpose WebRTC gateway. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications* (IPTComm '14). ACM, New York, NY, USA, Article 7
[11] A Study of WebRTC Security, http://webrtc-security.github.io/
[12] I. T.Javed, K. Toumi,. N.Crespi, Browser-to-browser authentication and trust relationships for webrtc. in *The Tenth International Conference on MobileUbiquitous Computing, Systems, Services and Technologies, UBICOMM*, 2016
[13] J. Strle, Next Generation 112 Emergency Services, 12th International Crisis Management Conference, Ljubljana, June 2017
[14] ETSI, Technical Report, 2nd NG112 Emergency Services Plugtest, Sophia Antipolis, France, March 2017
[15] GSM Association, WebRTC to complement IP Communication Services, White paper, February 2016
[16] EENA, WebRTC and Emergency Services, EENA Technical Committee Document, 2016,
[17] EU project EMYNOS - nExt generation eMergencY commuNicatiOnS, https://www.emynos.eu/

[18] EU project NEXES - NEXt generation Emergency Services, http://nexes.eu/

Valerij Grašič is a product manager at Iskratel, with more than 20 years of experience in the telecommunications. During this period he has been involved in various projects and in various roles, which include research, development, and testing of telecommunication system for customers and projects around the world. His domains are NGN, IMS and 5G networks, security, public safety systems, including information and alarm systems, eCall, artificial intelligence based analytics, and audio and video-based media servers to support public safety systems. He has published multiple articles in the field of telecommunications in conferences and journals.

During the past seven years **Ana Robnik** worked as a telecommunications consultant, leading also a research group "Raziskovalna skupina ISKRATEL" at ARRS and coordinating Iskratel's effort in standardization organizations. After receiving her B. Sc. degree in applied mathematics from the Faculty of Mathematics, Physics and Mechanics, and her M. Sc. degree in computer science from the Faculty of Computer and Information Science, University of Ljubljana, Slovenia, she started her career in the research department Iskra Kibernetika before joining the IT department in Iskratel. She has more than 20 years of experience in telecommunications and leadership. She led the development of the management and monitoring systems for network elements of Iskratel portfolio, in co-operation with international and domestic companies and external research groups. She has been participating in various national, EU and international operations. She coordinates the Safety vertical within Strategic Research and Innovation Partnership Smart Cities and Communities in Slovenia.

Grega Prešeren has been working in cybersecurity since the beginning of his professional career, primarily on security auditing IT and OT systems, security assessments and penetration tests (pentests), and consultancy on managing technological vulnerabilities. He has lead and performed over 70 security assessments of IT networks, IT services, web, mobile and other applications, industrial control systems etc. since his first employment in company Astec in 2010. He was a member of cybersecurity team in company S&T Consulting, where he worked as a cybersecurity consultant. Since 2017 he manages cybersecurity in products and solutions in company Iskratel. He holds many professional certificates in the field of cybersecurity (GXPN, GMON, GWAPT, GICSP) and IT networks (CCNP, CCNA Security, CCAI). He also teaches courses mainly on application security and frequently presents at cybersecurity conferences.

Vidiki varnosti Iskratelovega CSP oblaka pri upravljanju identitet in dostopa

Grega Prešeren, Jože Orehar, Gregor Koritnik, Ignac Zupan, Iskratel, d. o. o., Kranj

Povzetek — Računalništvo v oblaku je postalo realnost, ki smo jo sprejeli in se o njej ne sprašujemo več. Vedno bolj, ko se uporabniku ni potrebno zavedati, kje se fizično izvaja uporabljena storitev in kje se nahajajo podatki, do katerih dostopa, bolj pomemben postaja vidik zagotavljanja varnosti takih storitev. Ker tehnologije, ki omogočajo računalništvo v oblaku silijo uporabnika, da je agnostičen do lokacije, sta nadzor nad dostopom do oblaka in upravljanje z identiteto uporabnika dva od najpomembnejših dejavnikov zagotavljanja varnosti v oblaku. Iskratel je zaradi svojih poslovnih potreb iz odprtokodnih komponent zgradil lastno, platformo za računalništvo v oblaku CSP (Cloud Services Platform), ki je skladna z ETSI NFV. S širjenjem storitev, ki gostujejo na tej platformi, smo prišli do spoznanja, da enostavne metode nadzora nad uporabniki ne zadoščajo več za zagotavljanje želene opravilnosti oblačne platforme. Članek povzema Iskratelovo rešitev z uporabo odprtokodnega programja FreeIPA in Keycloak, ki omogoča centralno upravljanje z identitetami in enotno prijavo uporabnikov v oblak.

Ključne besede — Oblačne storitve, oblačna platforma, avtentikacija, avtorizacija, Iskratel CSP, ETSI NFV, IPA, LDAP, VNF, SSO

Abstract — Cloud computing has become a reality that we have accepted and we no longer ask about it. More and more, when user does not need to be aware of where the service is being physically executed and where the accessed data is located, the aspect of ensuring the security of such services becomes more important. Because cloud computing technologies force users to be location agnostic, controlling cloud access and user identity management are two of the most important security aspects in the cloud. Iskratel provides its own ETSI NFV compliant cloud computing platform for its customers, called CSP (Cloud Services Platform), built from open-source components. By expanding the number of services that are hosted on the platform we have come to the conclusion that simple methods for controlling users are no longer sufficient. The article summarizes Iskratel's solution using open-source software FreeIPA and Keycloak that enable central identity management and a single sign-on of user in the cloud.

Keywords — Cloud services, cloud platform, authentication, authorization, Iskratel CSP, ETSI NFV, IPA, LDAP, VNF, SSO

I. CSP PLATFORMA

Virtualizacija omrežnih funkcij, na kratko NFV (Network Functions Virtualisation), je koncept omrežne arhitekture, ki z uporabo tehnologij IT virtualizacije virtualizira celotna področja funkcij omrežnih vozlišč v gradnike, ki so povezani ali veriženi med seboj tako, da ustvarijo komunikacijske storitve.

Odgovor Iskratela na ta izziv je bil razvoj lastne oblačne NFV platforme. Iskratelova CSP oblačna platforma je v zrelem stanju in dobro sprejeta pri Iskratel kupcih. Temelji na standardu ETSI NFV in je sestavljena iz štirih glavnih delov:

- infrastruktura NFVI (NFV Infrastructure), ki zagotavlja sloj IaaS,
- upravitelj infrastrukture VIM (Virtualised Infrastructure Manager),
- orkestrator, ki skrbi za življenjski cikel omrežnih storitev in omogoča njihovo veriženje v kompleksnejše omrežne storitve,
- upravitelj VNFM (VNF Manager), ki skrbi za življenjski cikel virtualiziranih (omrežnih in ostalih) funkcij.

Vgrajena varnost v oblačni platformi CSP na nivoju infrastrukture je izdelana po priporočilih STIG (Security Technical Implementation Guide), pri čemer smo zajeli vsa najpomembnejša priporočila. Izkazala se je za izjemno pomembno, ko so platformo CSP začeli intenzivno uporabljati naši kupci.

II. MOTIVACIJA

Z naraščanjem števila virtualnih računalnikov in rešitev, ki tečejo v sklopu Iskratelove CSP platforme, smo se soočili z dejstvom, da je izredno težko nadzorovati in upravljati z uporabniki in pravicami na sistemu, če to ni rešeno preko centralnega dostopa.

Celovito rešitev smo našli v enotni prijavi uporabnikov v sistem, ki jim hkrati centralno urejamo tudi pravice dostopa do posameznih funkcij in delov sistema.

Pri obsežnih in kompleksnih NFV postavitvah v oblaku, ki vključujejo tudi več 1000 virtualnih strežnikov povezanih v omrežne storitve, je upravljanju z vsemi virtualnimi računalniki potrebno posvetiti posebno pozornost. Del te naloge smo rešili z avtomatizacijo upravljanja omrežnih storitev preko orkestratorja, drugi del pa naslavlja upravljanje varnosti in dostopa. Eden od ključnih vidikov upravljanja je upravljanje z identitetami, avtentikacijo uporabnikov ter avtorizacijskimi mehanizmi, s katerimi preprečimo, da uporabnik izvede neželene akcije, za katere nima pooblastil.

K rešitvi pristopamo celovito. Rešitev vključuje upravljanje z identitetami na aplikativnem nivoju in upravljanje sistemskih identitet na nivoju operacijskega sistema in sistemskih storitev kot je npr. spletni strežnik, aplikacijski strežnik, podatkovna baza, ipd., kar je bilo do sedaj decentralizirano.

Podobno velja za upravljanje same virtualizacijske platforme CSP.

III. CILJ ENOTNEGA UPRAVLJANJA Z IDENTITETAMI

Cilj vpeljave enotnega upravljanja z identitetami v CSP oblačno platformo je bil centralizacija identitet v skupno imeniško strukturo (ang. Directory Service), ki omogoča upravljanje identitet na enem mestu v celotnem življenjskem ciklu, ki vključuje ustvarjanje uporabniškega računa, določitev začetnega gesla, upravljanje politike gesel,

dodelitev pravic uporabniku, odvzem pravic uporabniku, ukinitev ali zaklep uporabniškega računa, ipd..

IV. KONCEPT REŠITVE

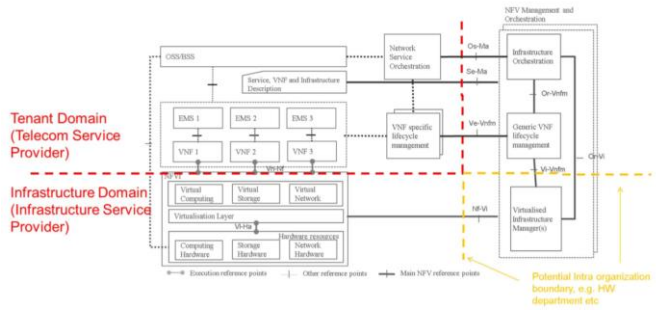
V enotno upravljanje identitet vključujemo naslednje funkcionalnosti oblačnih storitev:

– orkestracija (ang. Orchestration) VNF, ki vključuje tudi virtualne računalnike,
– sistemska infrastruktura VNF (operacijski sistemi in sistemske storitve),
– upravljavske aplikacije telekomunikacijskih in drugih storitev.

Za orkestracijo smo iz nabora orkestratorjev Tacker, Cloudify, Open Baton, izbrali Open Baton. Open Baton je izbran, ker je od vseh najbolj skladen s standardom ETSI NFV in je odprtokoden.

Keystone je privzeti ponudnik identitet v OpenStack in ga ohranjamo v rešitvi za zagotavljanje avtentikacije in avtorizacije pri klicih programskih vmesnikov iz MANO funkcionalnosti (NFVO – NFV Orchestrator, VNFM, VIM). Keystone je za potrebe enotne avtentikacije povezan z zunanjim ponudnikom identitet, ki je tudi primarni ponudnik identitete za upravljanje CSP oz. oblaka.

Zaradi ponujene možnosti nakupa in uporabe posameznega dela celovite rešitve, n.p. le CSP oblačna platforma ali le VNF funkcije kot so vIMS, vSCB in druge, smo storitve AAA (Authentication, Authorization, and Accounting) ločili za ponudnika virtualne infrastrukture in uporabnika virtualne infrastrukture (ang. Tenant), ki je v primeru vIMS ponudnik telekomunikacijskih storitev virtualnih omrežnih funkcij. Po ETSI priporočilih to ustreza ločevanju med *Tenant* domeno in *Infrastructure* domeno, kot prikazuje Slika 1.



Slika 1: Ločitev domene ponudnika virtualne infrastrukture in uporabnika virtualne infrastrukture [1]

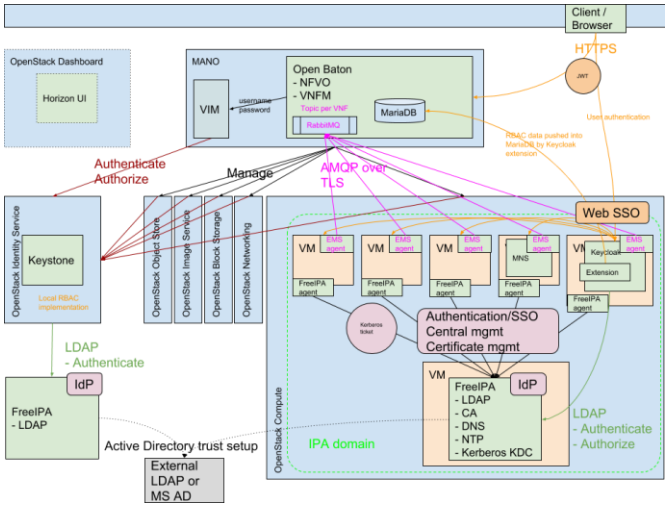
Zaradi poenostavitev pri upravljanju smo za implementacijo AAA za obe domeni uporabili enake tehnologije, ki omogočajo tudi združevanje oz. integracijo obeh domen, v kolikor bi kupec to želel.

Dodatno pa je omogočena integracija z že obstoječimi imeniki (ang. Directory Services), tipično Microsoft Active Directory, v kolikor kupec to potrebuje.

V. OPIS REŠITVE

Keystone izvaja avtentikacijo z uporabo protokola LDAP (Lightweight Directory Access Protocol) v instanco FreeIPA (Free Identity, Policy and Audit) za infrastrukturno domeno. Zaradi tega ni bilo potrebno pripraviti sprememb v MANO funkcionalnostih (NFVO, VNFM, VIM), saj gredo vsi klici še vedno do Keystone, ta pa transparentno izvaja avtentikacijske klice naprej v FreeIPA (LDAP).

Ker smo želeli za vse spletne aplikacije, tudi za orkestrator, uvesti enotno prijavo (ang. Single Sign-On), smo v rešitev integrirali še Keycloak. Avtentikacija za prijavo v orkestrator OpenBaton se torej izvede preko Keycloak, ki je tudi povezan s FreeIPA, ponovno preko protokola LDAP. Keycloak uporabniku spletne aplikacije izda digitalno podpisan žeton JWT (JSON Web Token), ki vsebuje podatke o uporabniku in njegovih pravicah. Pravice so zapisane v obliki LDAP skupine, ki ima znotraj aplikacije privilegije izvajanja posameznih akcij. Uporabnikov brskalnik avtomatsko pošlje JWT žeton na Open Baton, ki žeton najprej verificira (digitalni podpis ter čas izteka oz. ang. Expiry time) ter nato uporabniku dovoli izvajanje le avtoriziranih akcij. Integracija Keycloak in Open Baton ni mogoča le z nastavitvami obeh. V ta namen smo razvili posebno programsko razširitev (ang. Extension), ki poskrbi za zapis avtorizacijskih podatkov iz Keycloak v podatkovno bazo Open Baton, ki je realizirano s tehnologijo MariaDB. To pomeni, da so vsi avtentikacijski in avtorizacijski podatki primarno zapisani in se urejajo na enem mestu, to je v LDAP imeniku strežnika FreeIPA.



Slika 2: Rešitev centralnega upravljanja z identitetami v CSP oblačni platformi

Enotna prijava na nivoju operacijskega sistema virtualnih omrežnih funkcij je preko FreeIPA agenta podprta za veliko večino operacijskih sistemov. Virtualno omrežno funkcijo vključimo v ta sistem tako, da vanjo namestimo odjemalca »FreeIPA agent« in jo vključimo v t.i. IPA domeno, ki je analogna Windows domeni, vendar z manj funkcionalnostmi in s podporo za operacijski sistem Linux. Vključitev v IPA domeno lahko izvede administrator FreeIPA strežnika. Zaradi nujnosti po avtomatizaciji zagona nove instance NS (Network Service), ki vključuje eno ali več omrežnih funkcij na enem ali več virtualnih računalnikih, smo to funkcionalnost dodali v orkestrator. To pomeni, da se pri dodajanju novega NS vključitev v IPA domeno izvede avtomatsko in transparentno preko orkestratorja. Enotna avtentikacija v IPA domeni, ki je v tem primeru ekvivalentna ETSI Tenant domeni, se izvaja s protokolom Kerberos, ki temelji na izdaji avtentikacijskih in avtorizacijskih žetonov.

IPA domena omogoča poleg enotne prijave tudi delno centralno upravljanje z operacijskimi sistemi in sistemskimi storitvami NS. Podprto je tudi centralno upravljanje vseh

VNF s sudo politiko, ki omogoča uporabniku izvajati določene ukaze s pravicami, ki so močnejše od njegovih.

Dodajanje ali prilagoditev aplikacij na enotno AAA domeno pomeni uporabo standardiziranih rešitev in protokolov kot sta LDAP in Kerberos. Za vse navedene protokole že obstajajo programske knjižnice (ang. Library), ki močno poenostavijo in pohitrijo prilagoditev aplikacij.

VI. ZAKLJUČEK

S centralnim upravljanjem z identitetami tako Tenant kot Infrastrukturne domene smo naslovili in rešili dvoje izzivov. S personifikacijo dostopa do posameznih funkcij in delov sistema smo močno izboljšali varnost sistema kot celote, saj je vsak uporabnik s svojim unikatnim računom poznan kot ena identiteta na celotnem sistemu in je tudi kot ta identiteta v celoti odgovoren za svoje postopke. Hkrati s tem pa omogočamo tudi hitrejše in lažje reševanje morebitnih varnostnih incidentov zaradi razkritja gesel posameznih uporabnikov, ker je geslo zapisano samo enkrat v sistemu in se tudi spreminja na enem mestu za celotni sistem.

LITERATURA

[1] http://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/003/01.02.01_60/gr_NFV-SEC003v010201p.pdf
[2] https://www.freeipa.org/page/Documentation
[3] https://www.keycloak.org/documentation.html

AVTORJI

Jože Orehar je avtor oblačne platforme CSP in je v podjetju Iskratel glavni arhitekt za rešitve v oblaku in postavljanje oblačnih platform. Ima preko 25 let izkušenj na področjih razvoja programske opreme s poudarkom na arhitekturi, vodenju razvojnih skupin in podatkovnih strežnikih. Zadnje desetletje pa posveča največ svoje pozornosti in časa arhitekturam na področju virtualizacije in oblačnih rešitev. Pri rešitvah postavlja v ospredje odprto kodo in sodelovanje. Sodeluje s Fakulteto za računalništvo v Ljubljani, s katero je izpeljal več raziskovalnih projektov na temo oblačnih rešitev, podprtih tudi s strani EU. Zaključil je študij računalniškega inženirja na Fakulteti za računalništvo v Ljubljani.

Ignac Zupan je diplomiral na Fakulteti za elektrotehniko v Ljubljani in je v Iskratelu zaposlen od leta 1997. V začetku je delal v sektorju za sistemsko programsko opremo, kjer je sodeloval pri prvi implementaciji produktov xDSL in VoIP, sedaj pa dela v produktnem vodenju. Njegova področja dela so povezovanje Iskratelovih naprav in rešitev v IP-omrežja, omrežna varnost, varnost storitev VoIP ter arhitektura rešitev v oblaku. V zadnjih nekaj letih deluje kot produktni vodja Iskratelove oblačne platforme CSP in je avtor in produktni vodja Iskratelovega mejnega krmilnika sej (SBC).

Grega Prešeren se od vsega začetka profesionalne kariere primarno ukvarja z revizijami varnosti informacijskih in industrijskih sistemov, varnostnimi pregledi in vdornimi (penetracijskimi) testi, ter svetovanjem pri obvladovanju tehnoloških ranljivosti. V podjetju Astec je od leta 2010 vodil in izvedel več kot 50 varnostnih pregledov omrežij, IT storitev, spletnih, mobilnih in drugih aplikacij, industrijskih sistemov ipd. Od leta 2015 bil je član varnostne ekipe v podjetju S&T Svetovanje, kjer je opravljal vlogo svetovalca za kibernetsko varnost, od leta 2017 naprej pa je odgovoren za kibernetsko varnost rešitev in produktov v podjetju Iskratel. Je nosilec več strokovnih certifikatov s področja informacijske, industrijske in aplikacijske varnosti (GXPN, GMON, GWAPT, GICSP) in informacijskih omrežij (CCNP, CCNA Security, CCAI). Izvaja tudi izobraževanja s področja aplikacijske varnosti in večkrat letno predava na konferencah s področja kibernetske varnosti.

Gregor Koritnik se je pridružil Iskratelovi ekipi leta 2012. Še pred tem se je ukvarjal z vzdrževanjem IT infrastrukture malih in srednjih podjetij s poudarkom na varnosti informacijskih sistemov od vzdrževanja varnostnih kopij podatkov, podatkovnih baz, IP omrežja, požarnih zidov, imeniških direktorijev in kontrole dostopov. V Iskratelu je začel z verificiranjem Iskratelove VoIP varnostne rešitve in pri tem z izvajanjem različnih penetracijskih testov in izvajanjem DOS napadov pomagal razvojni ekipi pri izboljšavi funkcionalnosti varnostne rešitve. Trenutno se kot del razvojne ekipe ukvarja z varnostjo na oblačni platformi s centralno avtentikacijo in avtorizacijo sistemskih uporabnikov in centralnim managementom izdajanja certifikatov, privatnih ključev in kriptiranja povezav.

Demistifikacija tehnologije veriženja blokov

Tadej Hren, Arnes SI-CERT

Povzetek — Ta članek poskuša obrazložiti tehnologijo veriženja blokov z uporabniškega vidika ter implementacije v širši javnosti. Pri popularizaciji te tehnologije se pogosto poudarja zgolj pozitivne aspekte, na negativne pa se premalo opozarja. Zaradi tega med uporabniki zaradi neznanja prihaja do pogostih napak, katerih posledice imajo lahko zelo hude negativne učinke.

Ključne besede — veriženje blokov, tehnologije porazdeljene glavne knjige, Bitcoin, decentralizirana aplikacija, varnostne ranljivosti, pametne pogodbe

Abstract — This article tries to explain blockchain technology from the users aspect and its widespread implementation. Popularisation of these new technologies most of the times emphasizes only positive aspects, and neglects negative ones. Because of that, users often make mistakes, often with very serious negative consequences.

Keywords — blockchain, distributed ledger technology, Bitcoin, decentralized application, vulnerabilities, smart contracts.

I. UVOD

Pri vprašanju varnosti tehnologije veriženja blokov (v nadaljevanju: blockchain) moramo ločiti med dvema vidikoma: varnost same tehnologije ter varnost pri uporabi tehnologije.

Kar se tiče varnosti tehnologije, kakšnih večjih težav tu ne beležimo. Če vzamemo kot vzorčni primer blockchain tehnologije njeno prvo implementacijo, to je omrežje Bitcoin, v času obstoja tega omrežja še nikoli ni prišlo do primera zlorabe omrežja na tak način, da bi napadalcu uspelo spremeniti transakcijo, ki se nahaja nekaj blokov (običajno 6) za zadnjim potrjenim blokom v verigi blokov. Vseeno pa ne smemo zanemariti nekaj primerov zlorabe omrežja, ki pa so se zgodili.

Ena najhujših zabeleženih zlorab Bitcoin omrežja se je zgodila v avgustu 2010, ko je neznancu uspelo narediti veljavno transakcijo [1], ki je bila tudi potrjena, in ki je iz 0,5 Bitcoina generirala približno 184 milijard Bitcoinov. Ob dejstvu, da protokol omejuje število vseh Bitcoinov na 21 milijonov, je šlo tu za očitno zlorabo. Napadalec je v programski opremi našel ranljivost tipa integer overflow, zaradi katere je pri seštevanju dveh velikih pozitivnih števil v outputu transakcije prišlo do prekoračitve pomnilniškega prostora, namenjenega hranjenju spremenljivke, tako da je bil seštevek teh dveh števil zgolj 0,5, kar se je ujemalo z vhodno vrednostjo (input transakcije). Popravek za omenjeno ranljivost je bil izdan v petih urah od sporne transakcije v obliki t.i. »soft fork« spremembe kode. Ta je po novem vključevala tudi preverjanje, ali število Bitcoinov v transakciji presega 21 milijonov, ter v tem primeru transakcijo označi kot neveljavno.

Zaenkrat je bilo v omrežju Bitcoin javno objavljenih 25 hujših programskih napak [2], ki jih uvrščamo med varnostne pomanjkljivosti. Pri uporabi blockchain in drugih DLT tehnologij (Distributed Ledger Technologies) tako ne smemo zanemariti dejstva, da gre tu v osnovi za računalniške programe, ti pa praviloma vedno lahko vsebujejo varnostne pomanjkljivosti.

Tabela 1: Število varnostih pomanjkljivosti Bitcoina po letih

Leto	2010	2011	2012	2013	2014 – 2017
Št. ranljivosti	5	1	7	9	3

II. DECENTRALIZIRANE APLIKACIJE

Drug vidik varnosti tehnologije pa je njena uporaba v praksi. Pri tem si lahko kriptovalute predstavljamo kot sredstvo za »poganjanje« decentraliziranih aplikacij: kriptovaluta Bitcoin poganja decentralizirano omrežje Bitcoin, Ether poganja decentralizirano aplikacijo Ethereum, itn. Kaj sploh je decentalizirana aplikacija? Njeno nasprotje je centralizirana aplikacija, ki si jo lahko predstavljamo kot storitev, ki ima centralnega koordinatorja – ponudnika oz. posrednika, ki ponuja oz. upravlja to storitev. Centralizirani aplikaciji sta npr. iskalnik Google in omrežje. V svetu izven informacijske tehnologije lahko centralizirano aplikacijo predstavimo npr. v obliki bolnišnice, ki posreduje med zdravniki in pacienti, ali pa trgovino, ki posreduje med proizvajalci in potrošniki.

Po drugi strani si decentralizirano aplikacijo lahko predstavljamo kot storitev, ki nima tega centralnega koordinatorja. Taki primeri sicer že zdaj obstajajo tudi izven blockchain tehnologije. Decentralizirana aplikacija bi npr. lahko izgledala tako, da potrošniki hrane ne bi več kupovali v trgovini, ampak neposredno pri proizvajalcih. Blockchain tehnologija pa uporabnikom omogoči to, da se lahko posrednika izloči iz mnogo drugih storitev, pri katerih to do sedaj sploh ni bilo mogoče.

Blockchain tehnologija uporabnikom npr. omogoča to, da ti svoje zdravniške dokumentacije ne bodo shranjevali v bolnišnicah, ampak bodo lahko zdravstveno dokumentacijo imeli pri sebi, ter se bodo sami odločali, kdo in kdaj bo imel vpogled vanjo. Uporaba kriptovalut omogoča uporabnikom, da lahko postanejo sami svoja banka – sprejemajo plačila in plačujejo račune, ne da bi imeli odprt račun na banki.

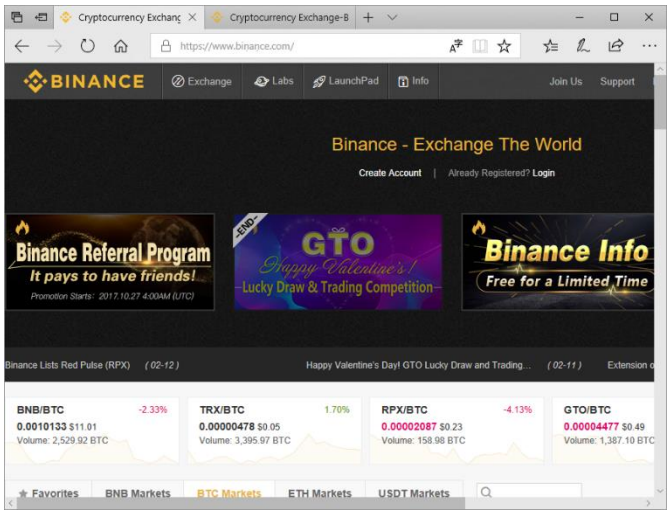
III. PROBLEMI DECENTRALIZIRANIH APLIKACIJ

Blockchain tehnologija tako daje uporabnikom nove možnosti, ki do sedaj niso bile mogoče. Ali bodo uporabniki pripravljeni sprejeti te možnosti, je pa drugo vprašanje. Kajti blockchain tehnologija s seboj prinaša tudi veliko novih težav, ki jih do sedaj, pred uporabo te tehnologije, sploh nismo poznali.

Težava je namreč v tem, da ker decentralizirana aplikacija nima posrednika, to posledično pomeni, da če želi uporabnik enako mero varnosti, bo moral sam poskrbeti za varnost, ki mu jo je pred tem zagotavljal posrednik (in kateremu je uporabnik za to storitev običajno tudi plačeval). In če bodo uporabniki pri tem naredili napake, bodo morali sami odgovarjati zanje. V praksi je takih napak zelo veliko, običajno pa so posledica nezadostnega znanja.

Primeri najpogostejših napak uporabnikov, ki jih srečujemo v praksi:

- pomanjkanje varnostne kopije kripto denarnice, oz. neustrezna varnostna kopija;
- kraja sredstev iz kriptodenarnic kot posledica phishing napadov;
- nakazila sredstev na napačne naslove kriptodenarnic.



Slika 1: Primer lažne phishing strani ene od kripto borz

Pri tem te težave niso omejene zgolj na kriptovalute, ampak na vse aplikacije, ki temeljijo na novih tehnologijah porazdeljene glavne knjige. Npr. ena od pogosto omenjenih storitev, ki bi lahko delovala na blockchain tehnologiji, je zemljiška knjiga. Če bi se ta v obliki neke »pametne pogodbe« prenesla na blockchain, bi to pomenilo, da bi vsi lastniki prejeli zasebne ključe, s katerimi bi dokazovali lastništvo svoje nepremičnine. Dostopa do teh zasebnih ključev ne bi smela imeti nobena druga oseba ali inštitucija (v nasprotnem primeru namreč ne moremo več govoriti o decentralizirani storitvi). Kaj bi se zgodilo v primeru, da lastnik nepremičnine izgubi zasebni ključ? Novega ne more prejeti, saj mu ga ne more podeliti nobena inštitucija. Če to pomeni, da ostane z nepremičnino, ki je ne more odsvojiti, se je na tem mestu treba vprašati, ali se lahko ta odgovornost prenese na uporabnike, ter ne nazadnje, ali smo uporabniki sploh pripravljeni sprejeti tako odgovornost?

Povsem enake dileme obstajajo tudi pri drugih t.i. »pametnih pogodbah«, pri katerih je stanje pogodbe definirano z vrednostjo spremenljivk računalniškega programa. Varnost take pogodbe je tako odvisna od varnosti samega programa. V praksi se izkaže, da zelo veliko »pametnih pogodb« vsebuje varnostne pomanjkljivosti, ki nepooblaščeni osebi omogočajo uporabo na način, ki ni bil mišljen ob njegovi pripravi [3]. Poleg tega so »pametne pogodbe« imutabilne (nespremenljive), kar pomeni, da jih po njihovi implementaciji v blockchainu ni mogoče več spreminjati.

IV. ZAKLJUČEK

Vsaka nova tehnologija prinaša tako koristi kot slabosti. V primeru blockchain tehnologije je razkorak med pozitivnimi in negativnimi aspekti še posebej izrazito velik. Če oz. ko bomo začeli uporabljati to tehnologijo v širšem obsegu, ne smemo videti zgolj koristi, ampak moramo prepoznati in sprejeti tudi slabosti.

LITERATURA IN VIRI

[1] Value overflow incident, https://en.bitcoin.it/wiki/Value_overflow_incident
[2] Common Vulnerabilities and Exposures, https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures
[3] Finding The Greedy, Prodigal, and Suicidal Contracts at Scale https://arxiv.org/pdf/1802.06038.pdf

IoT in verige podatkovnih blokov v sodobnih omrežjih IKT

Rudolf Sušnik, Peter Zidar, Gregor Bobnar, Primož Prevec, Telekom Slovenije

Povzetek — Članek je namenjen pregledu uporabe tehnologije veriženja podatkovnih blokov (angl. blockchain) v telekomunikacijah. Ta tehnologija bo še posebej primerna v internetu stvari, kjer je potrebno spremljati in beležiti podatke, ki prihajajo z različnih naprav in senzorjev.

Ključne besede — blockchain, IoT, verige podatkovnih blokov, internet stvari.

Abstract — This article explains usage of blockchain technology in telecommunications. This technology will be suitable for IoT solutions, where data from different devices and sensors is collected and stored.

Keywords — blockchain, IoT, security

I. UVOD

Uporaba tehnologij interneta stvari in veriženja podatkovnih blokov se vse bolj uveljavlja. Napovedi **Napaka! Vira sklicevanja ni bilo mogoče najti.** (Gartner) kažejo, da bo leta 2030 veriženje podatkovnih blokov v svetovnemu gospodarstvu prispevalo kar za 3100 milijard USD vrednosti. Po drugih analizah [2] naj bi globalno tržišče interneta stvari zraslo iz 157 milijard USD v letu 2016 na 457 milijard v letu 2020. Na tem področju se bodo torej dogajale revolucionarne spremembe, ki bodo vplivale na številna področja našega življenja.

Uporaba omenjenih tehnologij naj bi zamajala temelje logistike, proizvodnih procesov, trgovanja, financ in zdravstva. Kljub napredku, ki bo posledica omenjenih tehnologij, bo njihovo uvajanje potekalo počasneje, če ne bo zagotovljena ustrezna varnost. Potencialna varnostna tveganja so namreč enostavno prevelika. Naprave vključene v internet stvari lahko namreč napadalcu omogočijo dostop do ogromne količine zaupnih ali občutljivih podatkov.

Varnostna tveganja se razlikujejo po okolju, v katerem se nahajajo naprave interneta stvari (IoT). To je lahko okolje pametnega oziroma povezanega doma, kjer bi morebitni napadalec lahko dostopal do video podatkov v stanovanju uporabnika in do različnih merilnikov temperature, dima, osvetljenosti, porabe električne energije in drugih naprav, ki izdajajo informacijo o življenjskih navadah uporabnika in o njegovi prisotnosti v stanovanju. V bolnišničnem okolju je kritična zaščita občutljivih podatkov o zdravju uporabnika in o njegovi zdravstveni zgodovini. Številne povezane naprave bi lahko izdale občutljive podatke o trenutnem srčnem utripu, krvnem tlaku, nivoju sladkorja v krvi in EKG. Nepooblaščen dostop do teh podatkov gotovo ni zaželen. V tovarniškem okolju oziroma okolju ponudnika električne energije je lahko nepooblaščen dostop do interneta stvari še bolj nevaren. Napadalec bi lahko načrtno sabotiral merilne naprave z namenom onemogočanja njihovega delovanja ali bi prevzel nadzor nad upravljanjem tovarne, kar bi lahko bilo katastrofalno. Na ta način bi bilo mogoče izvršiti zelo učinkovit kibernetski napad na celotne države.

II. STORITEV IOT

Najprej si poglejmo, kaj je storitev IoT. Gre za sestavljeno storitev, ki jo sestavlja več med seboj nivojsko povezanih gradnikov IoT. Tipični gradniki storitve IoT so terminalne naprave z vgrajenim senzorjem, komunikacijska povezava, agregacijsko omrežje, platforma IoT, podatkovna baza za shranjevanje merskih podatkov in aplikacija IoT s poslovno logiko. Za večjo dodano vrednost lahko storitev IoT uporablja še dodatno obdelavo pridobljenih podatkov s sistemi strojnega učenja in umetne inteligence. Vsi dodatni sistemi, ki nam iz zajetih merskih podatkov omogočajo pridobiti dodatne informacije, lahko neki storitvi IoT še dodajo vrednost.

Z razvojem IoT se povečuje tudi zahtevnost storitev IoT. Zahtevnost se povečuje pri zmogljivosti sistema IoT, kjer se zahteva najvišja razpoložljivost, kratki odzivni časi in visoka kapaciteta. Prav tako je zahtevana visoka varnost, ki mora zagotavljati identiteto izvora podatkov, anonimnost podatkov, njihovo šifriranje in preprečiti ponarejanje podatkov.

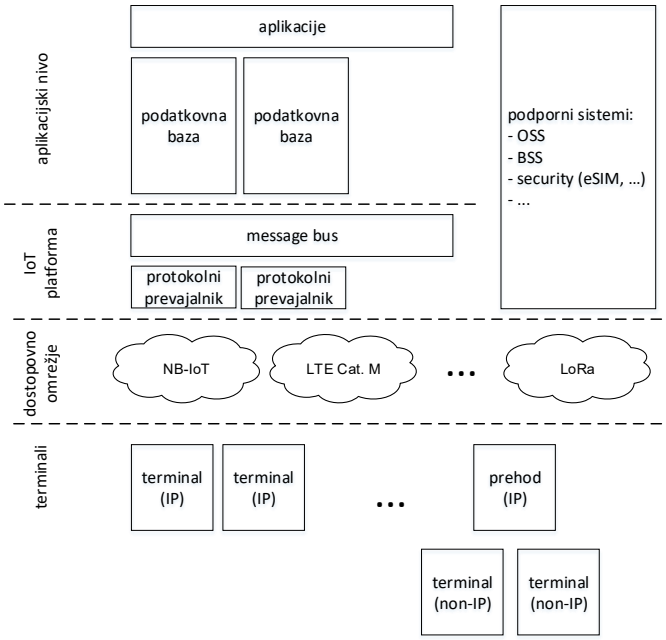
Današnji sistemi IoT zagotavljajo našteto možnosti z namenskimi omrežji IoT. Namensko omrežje IoT zagotavlja zaščiten kanal za dostop do podatkov. Komunikacija IoT poteka po ločenem omrežju. Naprave IoT se v omrežje dodajajo na avtoriziran način, sporočila IoT se usmerjajo in urejajo znotraj platform IoT. Vsi podatki se nahajajo v namenskih skladiščih in so pretežno dostopni samo eni aplikaciji. Namenska omrežja IoT so sicer robustna in varna a zaradi tega tudi kompleksna in zato cenovno niso najučinkovitejša.

Takšna struktura storitve IoT se zato zdi neprimerna, še zlasti za delovanje v prihajajoči generaciji omrežja 5G, ki bodo povezovala tudi ne-licenčna omrežja, kjer ni nadzora nad terminalnimi napravami. Zato je potrebno pripraviti vse potrebno, da se bo omogočalo tovrstne storitve tudi zunaj namenskih omrežij IoT.

III. ARHITEKTURA IOT

Kot je omenjeno v prejšnjem poglavju, lahko arhitekturo IoT razčlenimo po omrežnih slojih. Na fizičnem in povezovalnem sloju je na voljo veliko število različnih tehnologij, med njimi so takšne, ki so zasnovane s ciljem podpore napravam IoT (npr. NB-IoT, LTE kategorija M, LoRa, Sigfox, Zigbee, …), v uporabi pa so tudi splošne tehnologije, ki sicer niso bile zasnovane z mislijo na IoT, vendar so se v konkretnih primerih izkazale za primerne (npr.

LTE, GSM, WiFi). Pri slednjih velja pripomniti, da v okviru IoT nimajo dolgoročne perspektive in jih bodo nadomestile učinkovitejše različice, ki so že v temelju načrtovane za podporo IoT.



Slika 1: Arhitektura omrežja IoT

Izbira fizične/povezovalne tehnologije je odvisna od namena uporabe. Tako so pomembni zlasti parametri, kot so poraba energije, odzivnost (latenca), največja hitrost prenosa podatkov, sposobnost dvosmerne komunikacije in prehajanje med celicami brezžičnega ali mobilnega omrežja.

Na omrežnem sloju je tudi v internetu stvari ključnega pomena protokol IP, vendar obstaja več tehnologij, kjer terminalna naprava ne komunicira po protokolu IP, pač pa se terminalna naprava povezuje na prehod (gateway), ki v imenu terminalne naprave po protokolu IP posreduje podatke v omrežje. Tipični predstavnik takšne arhitekture je LoRa, medtem ko npr. tehnologija NB-IoT omogoča tako povezljivost IP kot ne-IP do terminalne naprave. Kadar arhitektura vsebuje prehod iz omrežja ne-IP v omrežje IP, je prehod običajno dimenzioniran tako, da deluje kot agregator, tj. nanj se povezuje večje število terminalov ne-IP.

Elementi arhitekture IoT, ki podpirajo protokol IP, tj. terminali in prehodi, posredujejo podatke na t.i. *message bus*, ki predstavlja neke vrste konvergentni nivo agregacije in usmerjanja podatkov. *Message bus*, ki je realiziran kot t.i. *broker*, usmerja podatke tako, da prispejo na ustrezno končno točko. *Broker* deluje po principu objavi/naroči (publish/subscribe), za kar se pogosto uporabljajo protokoli kot je npr. MQTT (ang. Message Queuing Telemetry Transport). Ideja takšne arhitekture je, da nimamo vertikalnih silosov, kjer bi v vsakem primeru na specifičen način reševali komunikacijo od izvora do ponora, pač pa uvedemo platformo IoT, ki poenostavi tako načrtovanje kot upravljanje omrežja IoT. V skladu s sodobnimi trendi v telekomunikacijah, platforma IoT ni centraliziran sistem, saj je z virtualizacijo oz. s pristopi »cloud computing & fog computing« mogoče na lažji način zagotoviti potrebne zmogljivosti za omrežje IoT – konkretno npr. s procesiranjem na robu omrežja (angl. Mobile Edge Computing - MEC).

Terminali, uporabljajo različne transportne in aplikacijske protokole, ki niso neposredno združljivi s protokolom, ki ga uporablja *broker*. Zato so v platformo IoT integrirani protokolni prevajalniki, ki so lahko precej specifični.

Kot omenjeno, *broker* usmerjajo podatke od izvora proti ponoru. Slednji so v omrežjih IoT običajno najrazličnejše baze podatkov in aplikacije, ki obdelujejo zbrane podatke. Zbrani podatki ali rezultati obdelave podatkov lahko služijo kot novi podatki, ki jih je potrebno dostaviti istemu ali drugemu terminalu, zato seveda komunikacija preko platforme IoT deluje dvosmerno.

Vzporedno z opisanimi postopki prenašanja aplikacijskih podatkov delujejo postopki upravljanja terminalnih naprav, ki zagotavljajo nadzor nad delovanjem terminalov, posodabljanje programske opreme terminalov, zagotavljanje varnosti na omrežnem nivoju, dodeljevanje pravic terminalov (avtentikacija, avtorizacija, profiliranje) in zaračunavanje. Gre za podobne postopke oz. način delovanja, kot je sicer uveljavljen v komunikacijskih omrežjih (tj. uporaba sistemov OSS/BSS).

S stališča varnosti je naloga omrežja in platforme IoT, da zagotovi varnost na omrežnem nivoju, medtem ko aplikacije lahko na aplikacijskem nivoju poskrbijo za dodatno zaščito pri prenosu podatkov. Varnostni mehanizmi, ki jih zagotavljata omrežje in platforma, so za končne uporabnike, tj. terminale in podatkovne baze/aplikacije, transparentni. Podobno velja tudi obratno – omrežje in platforma nimata vpliva na varnostne postopke/protokole aplikacijskega sloja.

IV. UPORABA VERIG PODATKOVNIH BLOKOV V IOT

Za reševanje težav kompleksnosti in varnosti v današnjih omrežjih IoT se zdi primerna uporaba tehnologije veriženja podatkovnih blokov. Tehnologija veriženja podatkovnih blokov prinaša povsem nov pristop pri tvorjenju storitvenega omrežja. Storitveno omrežje je sedaj sestavljeno iz omrežja zaupanja vrednih sodelujočih naprav in aplikacij IoT. V takšnem omrežju so vse transakcije podpisane in dostopne vsem sodelujočim. Tako postane izvor vseh podatkov znan in ga je možno preveriti. Zagotovljena je tudi integriteta podatkov, saj jih ni mogoče potvarjati. Z ustrezno naravnanimi pravicami je mogoče zagotoviti tudi anonimnost in skriti podatke pred neupravičenimi deležniki. Prav tako je možen tudi nadzor in avtoriziran vpogled v podatke, v kolikor je to zahtevano.

Nova omrežja so lahko tudi avtomatizirana, saj se nove naprave dodaja glede na zaupanje ostalih sodelujočih v verigi podatkovnih blokov. Na osnovi zaupanja med sodelujočimi v omrežju podatkovnih blokov lahko dodajamo nove aplikacije za povečanje poslovne vrednosti omrežja.

A. Prednosti blokovnih verig v IoT

Tako lahko s tehnologijo veriženja podatkovnih blokov rešimo več problemov obstoječih omrežij IoT:

- omogočimo avtentikacijo naprav IoT, ki so zaradi zahtevane nizke cene nemalokrat zelo enostavne in ne omogočajo vgradnjo osnovnih varnostnih standardov.
- evidentiranje IoT naprav v omrežju z verigo podatkovnih blokov je avtomatizirano, saj se zaradi avtomatskega kataloga sproti osvežuje in vsebuje vse potrebne podatke, kot so identifikacijska številka,

lokacija, programska verzija, tip senzorja in zgodovina popravil.
- preverjamo in avtoriziramo lahko meritve senzorjev. Meritve so vedno avtorizirane in njihov izvor je znan, saj se beleži vsaka transakcija.
- verige podatkovnih blokov služijo kot vmesnik za varno izmenjavo podatkov med napravami IoT in aplikacijami.
- ker so verige podatkovnih blokov distribuirana rešitev, je omrežje IoT manj ranljivo ter bolj odporno za manipulacije s podatki.
- stroški se zmanjšajo, ker ni potrebna postavitev in vzdrževanje robustnega kompleksnega okolja ustreznih vmesnikov, podatkovnih baz, omrežij in naprav.
- mogoča je revizija vseh pridobljenih podatkov in njihovih sprememb. Vse obdelave podatkov so zapisane v verigi podatkovnih blokov.

B. Pomanjkljivosti blokovnih verig in rešitve v IoT

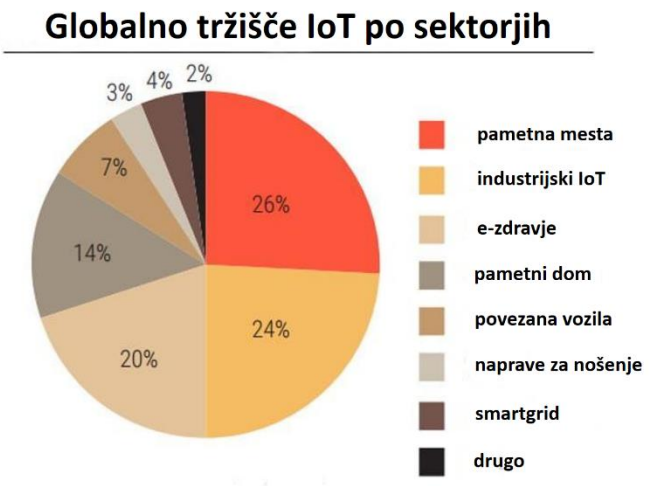
Tehnologija veriženja podatkovnih blokov ima tudi nekatere pomanjkljivosti. Ena ključnih je ta, da pri transakciji katerekoli vrednosti nastopijo transakcijski stroški, potreben pa je tudi določen čas za potrditev transakcije. Plačevanje stroškov transakcije, ki so večji od dejanske transakcije ni smiselno, prav tako so problematične transakcije, ki potekajo predolgo. Poleg tega je mogoče v verigah podatkovnih blokov poleg ostalih podatkov shranjevati tudi nezakonite vsebine, kar lahko ogrozi njihove implementacije, ki tega ne preprečujejo.

Zato je bila za potrebe omrežij IoT razvita kriptovaluta IOTA, ki ima javno distribuiran dnevnik vseh transakcij (angl. ledger), ki hrani transakcije v posebni prepleteni strukturi (angl. tangle)[3]. Na ta način odpadejo stroški energijsko potratnega rudarjenja oziroma potrjevanja transakcij. Namesto tega vsaka transakcija pomaga pri potrjevanju prejšnjih transakcij, kar omogoča izvedbo mikrotransakcij praktično brez stroškov. Ker IOTA ne uporablja tipične verige blokov, je procesorska moč potrebna za potrjevanje transakcij izredno majhna in primerna za nizko energijske senzorje. Varna transakcija podatkov in plačil je osnova za inovativne aplikacije ter poslovne modele IoT, kot na primer za mobilnost in industrijo 4.0.

Bosch je decembra 2017 naznanil sodelovanje s fundacijo IOTA z namenom podpore novih poslovnih modelov namenjenih internetu stvari [4].

V. PROJEKTI IN TESTIRANJA IOT

V Telekomu Slovenije smo v letu 2017 vzpostavili testno okolje IoT, ki je na voljo tudi zainteresirani strokovni javnosti oz. razvijalcem rešitev IoT, ki želijo preizkusiti svoje izdelke ali ideje v realnem telekomunikacijskem okolju. V ta namen je bila na treh baznih postajah aktivirana tehnologija NB-IoT (dve bazni postaji na območju Ljubljane ter ena v Mariboru) [5]. Hkrati v laboratoriju Brihtalab vzpostavljamo okolje za razvoj in preizkušanje gradnikov platforme IoT.



Slika 2: Tržišča IoT (vir: GrowthEnabler Analysis)

V okviru programa FP-7 smo v Telekomu Slovenije v evropskem projektu SUNSEED [6] razvili celoten sistem omrežja IoT, ki je zagotavljal podporo distribucijskemu elektro-energetskemu omrežju, tj. smart-grid. Razvili smo platformo IoT, ki je zagotavljala usmerjanje podatkov v podatkovno bazo ter v aplikacije, ki so na podlagi zbranih podatkov napovedovale stanje v elektro-energetskem omrežju in potrebne ukrepe. Pri tem so bile uporabljene različne dostopovne tehnologije (3G, 4G, satelitske komunikacije,…), prav tako pa je bilo poskrbljeno za varnost komunikacije.

VI. SKLEP

Tehnologija verige podatkovnih blokov bo prinesla pomembne spremembe pri delovanju omrežij IoT. Ta omrežja bodo delovala kot distribuirani poslovni sistemi z napravami IoT, kot izvori avtentičnih podatkov in avtoriziranimi poslovnimi aplikacijami, kot uporabniki informacij. Tak sistem bo necentraliziran in odprt za širitev. Pri njegovem delovanju pa bo zagotovljena potrebna varnost in zasebnost.

LITERATURA

[1] http://www.livemint.com/Home-Page/4TDOQ9nliOBE5qq2jOQfGI/Bankings-great-disruptor-Why-blockchain-is-the-way-forward.html
[2] https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#11e51fbc1480
[3] https://iota.org/IOTA_Whitepaper.pdf
[4] http://www.bosch-presse.de/pressportal/de/en/robert-bosch-venture-capital-makes-first-investment-in-distributed-ledger-technology-137411.html
[5] Telekom Slovenije vzpostavlja testno okolje za testiranje rešitev interneta stvari na osnovi tehnologije Narrowband-IoT, http://www.telekom.si/o-podjetju/za-medije/Telekom-Slovenije-vzpostavlja-testno-okolje-za-testiranje-resitev-interneta-stvari-(internet-of-things)-na-osnovi-tehnologije-Narrowband-IoT
[6] Projekt SUNSEED, http://sunseed-fp7.eu/

Dr. **Rudolf Sušnik** je razvojni inženir z več kot 15 let delovnih izkušenj iz gospodarskega in raziskovalnega okolja. Glavna področja njegovega raziskovalnega in razvojnega dela zajemajo brezžične komunikacije, mobilna omrežja, satelitske komunikacije, v zadnjem času pa tudi tehnologije 5G in IoT. V preteklosti je sodeloval v večini projektov Telekoma Slovenije s področja brezžičnih komunikacij, prav tako pa je pogosto predavatelj na domačih in mednarodnih konferencah. Doktoriral je na Univerzi v Ljubljani, leta 2007.

Mag. **Peter Zidar** je vodja razvojnih projektov v Telekomu Slovenije. Ima več kot 23 let delovnih izkušenj na področju telekomunikacij in IT. Od leta 2000 je bil zaposlen pri Mobitelu, kjer je med drugim vodil projekte razvoja lokacijskih storitev, Uverture in postavitve spletnega portala Planet. Med leti 2003 in 2005 je vodil Sektor za projekte. Od leta 2008 do 2016 je bil predsednik operaterske skupine mednarodne organizacije UMTS Forum, v katerem je bil tudi član upravnega odbora. V vlogi predstavnika UMTS Foruma in Telekoma Slovenije je kot govornik nastopil že na 35 mednarodnih konferencah po vsem svetu.

Mag. **Gregor Bobnar** je razvojni inženir, ki dela v testno razvojnem laboratoriju Telekoma Slovenije. Ima že več kot 10 let delovnih izkušenj s področja IKT. Po začetnem navdušenju nad omrežno tehnologijo se je kasneje usmeril na področje VoIP. Sodeloval je pri razvoju in testiranju uspešnih iOS aplikacij. V zadnjem času raziskuje in preskuša tehnologije interneta stvari ter z zanimanjem spremlja temo o verigah podatkovnih blokov. Magistriral je na Univerzi v Ljubljani, leta 2016.

Primož Prevec je razvojni inženir, zaposlen v oddelku za razvoj tehnologije jedrnega omrežja Telekoma Slovenije. Ima več kot 20 let izkušenj pri razvoju in implementaciji velikih telekomunikacijskih sistemov. Danes se ukvarja s sistemi sporočanja SMS, MMS, in vmesniškimi prehodi za razvijalce aplikacij. Sodeluje tudi pri oblikovanju storitev IoT in vpeljavi novih tehnologij za podporo IoT v Telekomu Slovenija.

Security resilience testing

Mirko Ivančič, Amiteh, Ljubljana

Abstract — In this paper we explore traditional approaches to assessing security investments, look at the financial benefits of testing, and debunk the excuses that keep IT organizations from validating their security infrastructure and deployment processes. We also introduce new solutions and best practices for staying a step ahead of the evolving threat landscape.

Keywords — resilience, attacs, security, testing

I. INTRODUCTION

This paper covers benefits of security resilience testing such as knowing for certain that:

- the organization is selecting the most optimized and cost-effective security for your one-of-a-kind network;
- the organization has right-sized investments to meet the organization's business and security needs;
- the network has the high level of security resilience needed to defend against attacks;
- the organization's personnel and the enterprise network will be ready when inevitable attacks occur.

"Resilience" is defined as the ability to bounce back, and when it comes to security, every second needed to defend and recover from attacks can cost millions of dollars. Most enterprises are now spending heavily to deflect crippling cyber attacks that impact their revenues and reputation, but without a viable means of testing before they invest and validating future changes.

II. DOES BUYING THE "INDUSTRY BEST" MEAN ANYTHING ANYMORE?

Ask any IT manager how they make new security investment decisions and most will answer, "We buy from the industry's leaders," or "We buy the best solutions in the industry." But in a world of one-of-a-kind application-driven networks, does "industry-best" mean anything anymore?

For example, according to the 2014 Gartner Magic Quadrant for Enterprise Network Firewalls by year-end 2014, this will rise to 35% of the installed base, with 70% of new enterprise edge purchases being NGFWs [2]. This prediction means many equipment manufacturers will be beefing up their marketing to capture a share of the sales growth, while enterprises toil over their next major IT purchasing decision.

The reality is that all vendor technologies are engineered with biases and objectives, with the hope of mass adoption. For example, most NGFWs include support for AppID, IPS, AV, and even APT sandboxing. These are compute-intensive applications that respond differently based on the applications and user behavior they see, as well as the biases that go into their engineering. These are not cookie-cutter functions and won't necessarily perform well in your network using only the default configuration.

So while the information captured in quadrant-type reports may be suitable for vendor marketing purposes, the product comparisons they contain may not be as relevant as you'd like them to be in planning your network. Vendors may slice and dice information to tout themselves as market leaders recognized by industry analysts, but the findings are largely based on an analyst's review of data sheets, conversations, and other anecdotal information.

While it's not directly stated, the implication of high rankings in these reports is an "industry-best" label, but there's an inherent conflict between what the analyst report portrays and the nature of how well devices meet a company's one-of-a-kind network needs. There is no "one-size-fits-all solution;" the promise of a magic box for the masses just doesn't exist.

Analyst and sponsored third-party reports may define a "best" based on a single, generalized synthetic criteria, but so what? Their findings don't reflect the needs for your unique network and business objectives, so why should they impact your important buying decisions?

Instead, the challenge is determining what "industry-best" means for your particular network. Like it or not, the decision—along with the justification behind it—may fall squarely on you, and there's only one proven way to protect yourself, and your network, from ever-growing risk. Since you can't rely on the "magic" in the quadrants, what can you do?

Enterprise IT managers are realizing that the same fundamentals they learned at school about good design practices – including testing (or verification/validation) – remain essential amidst the realities of today's threat landscape and hectic IT lifecycle management.

Testing validates or debunks what you think you know, and uncovers what you don't (but need to) know. Relying on anything else, including sponsored lab reports and vendor data sheets, amounts to guessing. And that's dangerous.

III. DEBUNKING MYTHS ABOUT ENTERPRISE TESTING

Technical schooling teaches that testing is an integral and essential part of good design practice; that it proves or disproves our assumptions, and validates design objectives.

More importantly, testing uncovers unknowns we may not have considered as inputs in designing complex systems. This proves especially vital for security, where failures to protect an organization may have financial, legal, and job-retention ramifications. Rigorous high-fidelity security resilience testing conducted in a safe environment is a must prior to rolling out new technologies and architectures, before the stakes become too high.

To date, some IT and security professionals have chosen, or had no choice but to have their live production networks serve as the test bed, and to use support line ticketing to gauge the success or failure of the implementation.

In rolling out a NGFW using the vendor's default configuration, or a new patch to existing technology, such an approach might easily result in IT being forced to do a costly rollback when the help desk ticket logs go beyond what can be ignored. Worse yet, the company's name may be splashed throughout the media in yet another headline about failed security.

The object of vendor testing is to verify the functions and performance advertised on data sheets in the context of a reproducible, fixed use-case. Test methodologies are largely driven by marketing with the objective of substantiating the biggest, most eye-catching parameters.

For example, vendors may use industry standards like RFC2544 (UDP/TCP) or RFC3511 (HTTP) to validate performance. Both of these standards are more than 10 years old and use synthetic transport streams with artificial data in the payload. In contrast, modern networks are content-aware and driven by applications.

The real performance of a content-aware next-generation technology will behave radically differently when passing a string of "AAAA" to a pair of IP address and ports, versus application traffic from thousands of users setting up and tearing down multiple sessions. Understanding application and user behavior using deep packet inspection (DPI) is compute-intensive and cache-inefficient versus synthetic traffic that is easily hardwareaccelerated and cache-efficient. Second, when it comes to security effectiveness, the parameters are captured while no real workloads are active. This is not a valid use-case for your network. Detecting threats is like finding needle in a haystack; without a haystack, it's easy to find the needle. Pile on the hay, and it's a different story.

For example, do attacks come on Saturday at 2 AM when there is little activity on your network, or it is more likely that you'll experience a **distributed denial of service (DDoS)** attack or exfiltration at the most precarious time – when there are thousands of critical transactions that need to be defended? Vendors can't give you these performance numbers on a data sheet.

What about interworking? How can any vendor give assurance that their technology will seamlessly interoperate in your complex environment?

Only by testing against the variables of real-world traffic mixes and conditions can you can answer these critical questions for yourself in your one-of-a-kind network.

Wrong again. Penetration testing and vulnerability assessments are critical steps used as evidence of compliance with requirements for securing a network. But "in compliance" doesn't necessarily equal "secure." Penetration testing has many benefits, but does not cover all critical elements of security resilience.

What about knowing how a security technology or the network will behave under real-user workload while under attack? How about the ability of your network and security/IT personnel to defend against DDoS during peak customer hours? What about determining the best technologies to bring into your network and right-size your investment?

Only realistic testing of security technologies or the whole network using valid workloads and attacks—at scale – lets you be sure the network will bounce back during and after an attack, stay resilient, and determine which devices are best as you build out your system.

For sure, security professionals are under tremendous pressure and are often understaffed. Time is fixed, and needs to be managed. But in the end, effective use of time is best explained in the simple time-proven adage: "Measure twice, cut once."

Following best practices means carefully planning, designing, implementing, and testing up front. Validating results ahead of time will dramatically reduce the huge time-sink of daily firefighting. Intuitively we all know this is true, but often emphasize urgent reactive firefighting over vital proactive steps that will minimize future firefighting.

In the past, building robust testing platforms like those used by vendors has been difficult and cost-prohibitive for the enterprise, in terms of both implementing test technologies and allocating the manpower needed to conduct tests. Massive racks of servers were typically required to model user behavior and create realistic traffic loads, and introducing realistic security attacks into the test bed was nearly impossible.

Simulate a DDoS attack at scale? The only options were to conduct functionality testing at small scale, or resort to low-level brute-force packet-generation tools to flood ports. Fortunately, the ecosystem and best practices for testing has advanced quite a bit.

Today, technologies are available to enable testing at enterprise-wide scale by generating realistic traffic that effectively models your unique network as well as attacker behavior. A comprehensive testing can now be conducted using low-cost appliances or virtualized software that can be loaded onto servers or reside in the cloud and be shared by users at multiple locations.

Networks, services, applications, and attacks change constantly. Looking back on a organization's network two years ago—its size, the average bandwidth consumed by users, the applications and services used—what percentage remains the same today? In today's world of ever-changing threats, perpetual patch rollouts, virtualization, and other challenges, a two-year statement on change may be as narrow as one hour ago.

Testing is now the only way to ensure the network is secure and resilient to attack. "Knowing," versus "guessing," is the only safe way to decide which technologies will result in secure and resilient networks that pay off in the near term as well as the long run.

IV. THE VALUE OF TESTING

A. Maximize Security Investment with an Onsite PoC

Acquiring new security technologies is an important and highly visible stage during which real-world testing can dramatically impact the bottom line. Consider Infonetics Research report [3] reinforcing the company's 2013 forecast for enterprise data center spending on security. The report projected average spending on security products would reach $17M. This number might vary according to how a network scales, and the functions being secured. Now consider the selection process for procuring those security products. Typically, IT organizations will research available products and send out a request for information (RFI) with the goal of narrowing the search to two or three vendor solutions. At this point, some level of more detailed research and evaluation of each solution typically begins.

But as we discussed earlier, vendor data sheet performance numbers are not a good estimation of how devices will perform on your particular network, running your particular network traffic. To get meaningful performance numbers that lead not only to the purchase of the best gear for your implementation, but also to significant cost-savings, enterprises must conduct onsite head-to-head bakeoffs, more about why and how to do data driven proof of concepts in [4]. The following diagram portrays a real PoC that Ixia helped conduct which showed the deviation in performance of a set of industry-leading NGFW products when real-world simulated workloads were applied. As the diagram illustrates, the synthetic TCP workload doesn't tell much other than to validate the bestcase data sheet numbers provided by the vendors. However, once the real-world workloads were applied with the target features enabled on the security product, a great deal of light is shed on how each technology and its compute-intensive algorithms will behave in a real network.

Head-to-head throughput performance comparison when handling real-world workloads that go beyond best-case TCP workloads. As we've seen, device vendors develop their technologies with specific problems in mind that they're aiming to prove they help solve. Then they take these products to market as general solutions with the hope of reaching a wide customer base. The reality is that performance and security effectiveness will never be the same in any two networks. Selecting the right technology that best matches your network needs, and then right-sizing that investment, will add quantifiable dollars to the bottom line.

The price variance among NGFWs is evidence that selecting the right device can have a profound impact on investment costs. By way of example, let's choose four competing NGFW solutions that enterprises commonly evaluate today - evidenced by their inclusion in the NSS Labs NGFW Security Value Map [5]. Pricing is publically published by a common reseller.

These devices all have different functionality, performance, and capacity, so this is by no means a scientific apples-to-apples comparison, but it does show widely varying costs for solutions advertising similar benefits.

Using simple math based on the $17M average data center security spend mentioned above, it works out that there would be a huge cost variance if all the products satisfied an IT department's need; however, it is not very likely that all products will satisfy your particular needs. Generalizing that all security product categories have similar price variance, and doing simple calculations, reveal that knowing which solution satisfy your needs at the lowest cost could result in significant cost-savings. If you could spend $5M annually—rather than $17M—to satisfy your security needs, surely that kind of savings would offset the cost of conducting your own PoC. But the financial benefits of testing don't end there.

B. The ABCs of Negotiating

Whether for a personal or work purchase, everyone wants a good deal. Negotiating is an art-form whose roots lie in information. PoCs reveal quantifiable data on performance, security effectiveness, and actual feature viability. Getting the right data to your purchasing department provides a decided but fair advantage in negotiating, and removes the need to be heavyhanded or come from a weak position making unjustifiable demands.

With the stakes approaching $17M in annual security spend, a 15%, 10%, 5%, or even 3% discount has very significant impact to the bottom line. Testing strengthens IT's negotiating position, resulting in another significant financial gain.

C. Right-Sizing Investments

Without knowing exactly how a security solution will perform in your network, the only option is to guess and work off of a derating factor. By nature, de-rating is conservative and forces you to buy up, rather than down. Depending on the technology and historic experience with a vendor, you may choose 30% or even 70% de-rating from the data sheet.

Let's take one of the above vendor solutions as an example of sizing. Without confidence in top-end performance scaling, you would need to scale out by adding another product, or scale up by upgrading to the next higher SKU. Either way, the cost impact is significant. Performance and cost do not scale linearly, so scaling up may be more expensive than scaling out. As we've seen, de-rating and guessing is a costly strategy.

Testing your technologies and network with real-world workloads while under attack will give you the data needed to more efficiently right-size investments.

V. THE NOT-SO-HIDDEN COSTS OF FAILING TO TEST

The real world, as we know, can be harsh. The media is littered with companies, all with good intentions of securing their networks, who quickly succumb to attack. Afterwards, the organization, customers, and other stakeholders consider what went wrong, and how to keep it from happening again. What's surprising is that many front-page incidents are based on well-understood attack strategies that have not changed much over the years, other than to become more targeted and persistent. In DDoS attacks, for example, strategies from the '90s are still used today, intensified by the ease of creating massive and long-duration campaigns.

Post-mortems conducted recently after major breaches at Target and Sony did not reveal any new exotic attack vectors, but the impact was clearly costly and far-reaching.

And while the cost of having customers be afraid to do business with you may not be quantifiable, other costs are:

A. The Cost of Downtime

The cost of security incidents can be partially quantified for enterprises in the form of lost productivity due to unplanned downtime.

Attacks and network incidents are inevitable in today's application and threat-driven environment. The time it takes to defend and restore to full operation is critical, and the dollar-impact math simple.

DDoS attacks in particular take the cost of downtime to the extreme. The volume of DDoS attacks is on the rise, and they continue to grow in size and complexity using application-layer strategies. Attack timing and duration is most problematic as these attacks are conducted at critical times in the targeted organization's business window and, if successful, cause the equivalent of unplanned downtime.

The Prolexic Q1 2014 Global DDoS Attack Report [6] revealed that DDoS attacks average 17 hours. This amount of time is staggering in and of itself, and the cost of resulting downtime even more onerous:

Average DDoS Outage: 17 hours
Cost: $5,712,000

Once again, security resilience achieved via security resilience testing can make the difference between timely recovery and going out of business.

B. Rollbacks Are Setbacks

Patching and upgrading technologies is a common occurrence in modern networks, and critical to securing networks, devices, and applications. Unfortunately, most of us have experienced a fair number of patch, feature, and even equipment rollbacks.

Rollbacks are embarrassing first, and second, they add substantial cost to your operations. No one intends for firmware updates to be brought back to a previous state, so personnel time has to be diverted from what was planned to deal with the unplanned.

Additionally, equipment and security effectiveness is compromised for the periods of time during which technologies are inaccessible. These issues can be mitigated if the patch or upgrade is tested against the previous baseline in the staging phase of the rollout, all with the same due-diligence as when the technology is first brought into the organization.

The impact of rollbacks is not easily quantified in dollars as most of the costs have extreme variability:

- labor ($75-$150/hour);
- travel, if required;
- support ticket management from complaining users;
- troubleshooting hours for tier 1-3 support;
- taking products out of service during the unplanned rollback;
- and the like.

We'll leave it to the organization to estimate in its own context whether these events should be seen as inefficiencies or catastrophic events that can rip apart a business' bottom line. In any case, these are just some of the costly occurrences that real-world testing can help eliminate or substantially reduce.

VI. VIRTUALIZING INDUSTRY-BEST TECHNIQUES

In recent years, platforms used to validate security resilience and device performance have scaled to fit the needs of the enterprise. Smaller, lower cost chassis, testing as a service (TaaS), and subscription-based services for keeping threat databases updated have made it easier for companies that don't maintain pre-deployment labs to avail themselves of the industry's more powerful performance validation.

Ixia BreakingPoint can deliver powerful PoC capabilities on the compact PerfectStorm One platform. For ongoing protection, Ixia's Application and Threat Intelligence (ATI) Subscription Service delivers:

– 6,000+ live security attacks;
– 35,000+ pieces of live malware;
– 180+ evasion classes;
– DDoS and botnet simulation;
– Real-world applications;
– 250+ application protocols;
– Social, P2P, voice, video, Web, enterprise business applications, gaming, mobile, storage workloads;
– Bi-weekly software updates and enhancements;
– Research into emerging vulnerabilities.

VII. CONCLUSION

A network resilient to attacks, misconfiguration, bottlenecks caused by integration, and changes from user behavior and patching can be the difference between an inconvenient incident and going out of business for many organizations. Testing technologies, networks, and the reactions of security personnel with simulated real work-loads, at scale, provides advanced knowledge on how your organization and its technology will fare under attack, and define its breaking points. With this knowledge in hand, you can adjust configurations, architectures, and policies to ensure defenses are working properly and will bounce back within a reasonable timeframe.

As we've seen, there is a high price to pay for a network that is not resilient – not only to attacks, but inefficient lifecycle and change management processes. Testing is a critical component of every organization's battle to ensure network security resilience that can handle the worst global attackers dish out.

REFERENCES

[1] Making Dollar$ and Sense Out of Enterprise Security Testing, White Paper, IXIA
[2] Gartner, Magic Quadrant for Enterprise Network Firewalls, Greg Young, Adam Hils, Jeremy D'Hoinne, 15 April 2014
[3] http://www.infonetics.com/pr/2013/Enterprise-Data-Center-Security-Survey-Highlights.asp
[4] http://info.ixiacom.com/Enterprise_IT_6_Steps_Data_Driven_Proof_of_Concept.html
[5] https://www.nsslabs.com/next-generation-firewall-security-value-mapdownload
[6] http://www.prolexic.com/kcresources/attack-report/prolexic-quarterly-globalddos-attack-report-q114/A4-Q12014-Global-Attack-Report.pdf

Mirko Ivančič je diplomiral leta 1978 na ljubljanski Fakulteti za elektrotehniko, smer telekomunikacije in se zaposlil v podjetju Iskra Elektrozveze, kjer je vodil oddelek merilne tehnologije. Leta 1984 se je kot inženir za podporo tehničnih računalnikov zaposlil v Hermesu, v sektorju zastopstva za Hewlett-Packard. Od 1986 do 1992 je bil odgovoren za prodajo testno-merilne opreme za področje Hrvaške, nato je postal vodja servisa in leta 1993 član uprave Hermes Plus, d. d. in direktor podpore za vse HP-jeve izdelke za področje Slovenije, Hrvaške, Makedonije in delno Slovaške. Leta 1996 je postal direktor merilne skupine za prodajo in podporo elektronske, medicinske in kemijsko-analitske merilne opreme. Leta 1997 je zapustil Hermes in po letu dni dela v podjetju Spes postal direktor Venture, podjetja za razvoj, proizvodnjo in trženje plovil. Leta 2002 se je pridružil Avektisu, takratnemu slovenskemu zastopniku podjetja Agilent Technologies (bivši HP), kot vodja prodaje elektronske merilne opreme. Od leta 2010, ko je Agilentov partner za Slovenijo postal Amiteh d.o.o., pa dela pod okriljem tega podjetja.

Podporniki

Sponzors

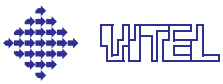
Iskratel

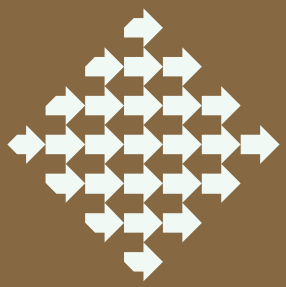
Telekom Slovenije

AKOS

Univerza v Mariboru, FERI

Univerza v Ljubljani, FE





Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije