KIBERNETINIO SAUGUMO Apžvalga

KENKĖJIŠKOS VEIKLOS KIBERNETINĖJE ERDVĖJE – GRĖSMĖS TECHNOLOGINIAMS VISUOMENĖS PAGRINDAMS

>> 4 p.

VIRTUALIOS ERDVĖS SAUGUMAS – IŠŠŪKIS IR JAV, IR EUROPAI

>> 24 p.

2016 m. gruodžio mėnesio specialusis priedas

etp frakcija Europos parlamente

KIBERNETINIO SAUGUMO SITUACIJOS LIETUVOJE APŽVALGA IR TENDENCIJOS 16

KIBERNETINIŲ ATAKŲ LIETUVOJE ATVEJAI IR KAIP Į JUOS REAGUOJAMA

27

APIE ELEKTRONINĮ BALSAVIMĄ PAPRASTAI 37

KOVŲ ARENA – KIBERNETINĖ ERDVĖ

21

33

DERAMO ELGESIO ELEKTRONINĖJE ERDVĖJE TAISYKLĖS

KAIP LIETUVOJE ĮGYVENDINAMA E. VALDŽIA? 41

I viršelis • www.flicr.com, Blogtrepreneur nuotrauka
III viršelis • ELP frakcijos Europos parlamente nuotrauka
IV viršelis • ELP frakcijos Europos parlamente nuotrauka

Redaktorė: Romena ČIŪTIENĖ

Rašykite mums adresu: redakcija@apzvalga.eu
Leidinį remia ELP frakcija
www.apzvalga.eu
Tiražas 8000 egz. Spausdino UAB „Petro ofsetas“
2016 m.
ISSN 1392-6721
Leidinys nemokamas

Turinys

3 | Prof. L. TELKSNYS. Kibernetinis saugumas

4–15 | V. BUTRIMAS. Kenkėjiškos veiklos kibernetinėje erdvėje – grėsmės technologiniams visuomenės pagrindams

16–18 | L. GRINIUS. Kibernetinio saugumo situacijos Lietuvoje apžvalga ir tendencijos

18–20 | R. ČIŪTIENĖ. Kibernetinio saugumo aplinka Lietuvoje

21–24 | A. GRAŽELIS. Kovų arena – kibernetinė erdvė

24–26 | L. KOJALA. Virtualios erdvės saugumas – iššūkis ir JAV, ir Europai

27–29 | P. SAUDARGAS. Kibernetinių atakų Lietuvoje atvejai ir kaip į juos reaguojama

29–31 | A. KOMAR. Tinklų ir informacinių sistemų saugumo direktyva – didžiulės ambicijos ir neapibrėžtos priemonės

31–32 | J. ŠVAGŽLYS. Išmanieji elektros tinklai: problemos ir perspektyvos. Enisa studijos apžvalga

33–36 | M. LAURINAITIS. Deramo elgesio elektroninėje erdvėje taisyklės

37–40 | K. AGAFONOV. Apie elektroninį balsavimą paprastai

41–44 | S. KLIMANSKIS. Kaip Lietuvoje įgyvendinama e. valdžia?

45–46 | R. VAITKEVIČIENĖ. Seminaras „Vieningai skaitmeninei Europos rinkai saugi skaitmeninė tapatybė“

KIBERNETINIS SAUGUMAS

Prof. Laimutis TELKSNYS, Lietuvos mokslų akademijos Technikos mokslų skyriaus Elektronikos ir infomatikos mokslų sekcijos pirmininkas

pixabay.com, geralt nuotrauka

Pasaulį apglėbė kompiuterių tinklai. Jie atvėrė neišsemiamas galimybes našiau dirbti, patogiau gyventi, įdomiau ilsėtis, efektyviau spręsti šių veiklų valdymo – kibernetines – problemas. Kompiuterių tinklai, informacinės technologijos gyventojams, įmonėms, įstaigoms, organizacijosms tampa veiksmingais ekonominės ir socialinės gerovės puoselėjimo įrankiais.

Toliau auga kompiuterių tinklų galimybės. Didėja jų reikšmė visose žmonių gyvenimo srityse. Kompiuterių tinklai yra atviri įvairiai naudingai veiklai. Deja, kompiuterių tinklai gali būti panaudojami ir kenksmingai, pavojingai veiklai. Pavyzdžiui, įvairios paskirties techninių, ekonominių, socialinių valdymo sistemų darbo trikdymui, neteisėtam informacijos grobimui ir sklaidai. Atakų metu siunčiama, pavyzdžiui, daugybė užklausų iš įvairių interneto taškų, taip siekiant sutrikdyti kompiuterių tinkle veikiančias sistemas. Kibernetinių grėsmų šaltiniais gali būti priešiškos valstybės, teroristinės organizacijos, organizuotos nusikalstamos grupuotės, pavieniai programišiai, tiesiog vagys. Vadinamosios kibernetinės atakos tapo nauju, moderniu pavojingu ginklu, galinčiu suparalyžiuoti ne tik atskirų įstaigų, gamybos, prekybos, transporto, ryšių, elektros, vandens tiekimo įmonių, bet net ir valstybių veiklą.

Kibernetinės atakos ypač pavojingos šalims, turinčioms gerai išvystytus kompiuterių tinklus, jų plėtrai būtiną informacinių technologijų plačiajuosčių tinklų infrastruktūrą. Lietuva kaip tik ir yra tokia šalis. Lietuvos 98 procentus teritorijos apima informacinių technologijų plačiajuostis optinis tinklas.

Kibernetikos atakos jau rengiamos prieš Lietuvos institucijas. Su kibernetinėmis atakomis susidūrė Lietuvos Respublikos Prezidentūra, Seimas, Užsienio reikalų ministerija, Krašto apsaugos ministerija, Vidaus reikalų ministerija, Teisingumo ministerija, Žemės ūkio ministerija, Finansų ministerija, Kultūros ministerija, Sveikatos apsaugos ministerija. Atakas taip pat patyrė Valstybinė mokesčių inspekcija, Žemės ūkio informacijos ir kaimo verslo centras, Vaikų išlaikymo fondas, Centrinė projektų valdymo agentūra. Programišiai atakavo taip pat kai kurias žiniasklaidos priemones, komunalinių paslaugų įmones. Todėl privalu būti tvirtai pasiruošusiems atremti kibernetines atakas. Svarbu nedelsiant stiprinti prevencines Lietuvos kibernetinio saugumo priemones, skatinti gyventojus aktyviai dalyvauti stiprinant Lietuvos kibernetinį saugumą.

Lietuvos mokslų akademijos technikos mokslų skyrius aktyviai rūpinasi Lietuvos kibernetiniu saugumu. Jau kelerius metus rengia metinius seminarus kibernetinio saugumo klausimais. Bendrauja su Lietuvos Respublikos krašto apsaugos ministerija, kitų valdžios žinybų, mokslo, studijų bei verslo atstovais. Rūpinasi, kad būtų rengiami ir įgyvendinami nutarimai, stiprinantys Lietuvos kibernetinį saugumą. Lietuvos mokslų akademijoje šiais metais įvyks Europos Komisijos aukščiausio lygio ekspertų pasitarimas kibernetinio saugumo klausimais. Pasitarime dalyvaus ir Lietuvos atstovai.

Šio leidinio tikslas - supažindinti su kibernetinio saugumo ypatumais kuo daugiau įvairaus amžiaus Lietuvos kaimo ir miesto gyventojų. Leidinys pasieks visas Lietuvos mokyklas ir bibliotekas. ■

KENKĖJIŠKOS VEIKLOS KIBERNETINĖJE ERDVĖJE – GRĖSMĖS TECHNOLOGINIAMS VISUOMENĖS PAGRINDAMS

Vytautas BUTRIMAS , Nacionalinės ryšių reguliavimo tarnybos tarybos narys, NATO Energetinio saugumo kompetencijos centro kibernetinio saugumo ekspertas

ĮVADAS

Kibernetinė erdvė 21 amžiuje tapo pagrindine palankia aplinka, kurioje vyksta šiuolaikinės industrinės visuomenės socialinė, politinė, kultūrinė ir ekonominė veikla. Galima įvardinti bet kokią veiklą, pradedant biuro darbuotojo, atliekančio finansų sistemos įrašą, tvarkant kredito korteles, priklausančias milijonams žmonių, ir baigiant inžinieriaus, stebinčio geležinkelio sistemą, saugiai ir laiku pervežančią tūkstančius keleivių iš vienos vietos į kitą. Visa tai egzistuoja kibernetinėje erdvėje, ten, kur ši veikla gauna gyvybę. Informacijos ir telekomunikacinių technologijų (ITT) pažanga leido asmenims tiek darbo vietose, tiek ir namuose dirbti ir bendrauti produktyviau internetiniame pasaulyje, naudojant asmeninius kompiuterius ir mobiliuosius duomenų apdorojimo įrenginius. Didelių sistemų kontrolė, leidžianti nuotoliniu būdu stebėti ir reguliuoti sudėtingus ir integruotus nacionalinius elektros ir vamzdynų tinklus iš vienos vietos, turi didelę reikšmę šiuolaikinės visuomenės raidai. Šis produktyvumas taip pat sumažino darbuotojų, kurių būtų reikėję tokioms sudėtingoms sistemoms valdyti ir aptarnauti, skaičių. Tiesa, atsiskleidė ne tik privalumai ir dabartinės galimybės, naudojant sujungtus prietaisus, bet ir tamsioji kibernetinės erdvės pusė - pažeidžiamumas ir pavojai, nevienodai juntami šių technologijų vartotojų, tačiau grėsmingi. Buvo nustatyta nauja tarpusavio priklausomybė ir besinaudojantys kibernetine erdve piliečiai ir šalys gali tai jausti.

Greitai atsirado pirmieji šių silpnųjų vietų išnaudotojai – tai studentai, kompiuterių įsilaužėliai, kurie norėjo parodyti savo sugebėjimus, krėsdami juokus su kai kuria programine įranga. Vėliau kenkėjiški šios naujos, suteikiančios didžiules technologines galimybes įrangos vartotojai ėmė naudotis saugumo architektūros trūkumais, turėdami tikslą tiesiogiai prisijungę pasisavinti pinigus. Tai lėmė elektroninių nusikaltimų ekonomikos atsiradimą. Šiandien valstybės ir/arba tie, kuriuos jos remia, taip pat tapo susijusios su kenkėjiškomis kibernetinėmis veiklomis (nuo kibernetinio šnipinėjimo iki kibernetinių ginklų). Kibernetiniai incidentai ir kibernetinės atakos iškėlė visiškai naujų, sudėtingų nacionalinio saugumo klausimų, liečiančių visuomenės ateities gerovę ir privatumą. Šie iššūkiai ir jų sprendimo būdai turės didelį poveikį interneto ateičiai ir mūsų gyvenimo

Alas Gore'as buvo vienas iš interneto įkūrėjų.

[1] šiame straipsnyje pateikti vertinimai ir idėjos išimtinai priklauso autoriui ir jie negali būti laikomi Lietuvos Respublikos Krašto apsaugos ministerijos, ar kitos organizacijos, su kuria autorius yra susijęs, oficialia pozicija

būdui, kuris dabar yra glaudžiai susijęs su šiomis naujomis ir dinamiškomis technologijomis. Šiame straipsnyje pagrindinis dėmesys bus skiriamas valstybių veiksmams, nes jos iki šiol turi struktūras ir išteklius, galinčius lemti interneto ateitį ir mūsų gyvenimo būdą. Taip pat bus siūlomi sprendimai, kaip valdyti galimus pavojus.

KIBERNETINĖS ERDVĖS GRĖSMĖS IR PLĖTRA

Internetas ir vieta, kurioje jis egzistuoja (daugelis vadina tai kibernetine erdve), nuėjo ilgą kelią per gana trumpą laiką. 1990-ųjų pradžioje JAV, kai daugelis gyventojų namų kompiuteriams prijungti prie įvairių elektroninių skelbimų lentų naudojo modemus, viceprezidentas Alas Gore'as kalbėjo apie informacinio „greitkelio" plėtojimą[2]. Daugelis turbūt sieja Alą Gore'ą su klimato kaitos supratimu, bet jis taip pat buvo vienas iš interneto įkūrėjų. Alas Gore'as sekė savo pasiūlymu ir siekė priimti teisės aktus, padėjusius pamatus infrastruktūros plėtrai, suteikusiai galimybę internetui tapti bendra šiandienos technologija[3]. Interneto perspektyva, kaip buvo pasiūlyta 1990-ųjų pradžioje, pranoko visus lūkesčius. Tai nėra tik informacijos rinkimo priemonė. Internetas tapo aplinka, kurioje vyksta šiuolaikinio pasaulio pagrindinė veikla. Minėtas pažadas parodė, kad internetas turi daug bendro su senovės Biblijos pažadu apie rojų. Šiame sode yra daug gražių dalykų - skanių duomenų bitų ir baitų, tačiau čia taip pat egzistuoja ir žalčiai gundytojai.

Kibernetinės atakos prieš individualų informacinių technologijų (IT) vartotoją

Reikia nepamiršti, kad interneto pirmasis „tinklas į tinklą" jungimas buvo grindžiamas pasitikėjimu. Iš esmės tai prasidėjo nuo informacinių technologijų administratorių sutarimo tarpusavyje sujungti jų valdomas IT sistemas. Apsikeitimo informacija nauda buvo įvertinta iš karto. Niekas tuo metu nemanė, kad šio naujojo ryšio vartotojas (ir vėliau daug vartotojų) blogai elgsis. Pirmasis kenkėjiškas elgesys kibernetinėje erdvėje prasidėjo nuo studentų išdaigų, kai jie išbandė bendrą koncepciją (paskleidė *Brain* (Smegenų) virusą diskeliuose) arba parodė įsilaužėlio sugebėjimus vartotojui (parodė pranešimą aukos kompiuterio ekrane: *Virusas Kavos parduotuvė*). Vėliau kenkėjiškas programas ėmė kurti nusikaltėliai, siekdami užsidirbti, pradedant nuo brukalų, kai siūlomos pardavimo paslaugos, iki tokio ardomojo elgesio, kaip pavyzdžiui, dokumentų ir duomenų gadinimas aukos kompiuteryje.

Kibernetiniai išpuoliai prieš ypatingos svarbos (CI) infrastruktūros objektus[9]

Vėliau kibernetiniai nusikaltėliai nusitaikė ne tik į individualius kompiuterių vartotojus, tačiau ir į tarpusavyje sujungtas informacines sistemas, kuriomis naudojasi bankai, vyriausybė, pramonė ir kitos, remiančios visuomenės veiklą, institucijos. Šios informacinės sistemos yra vadinamos „labai svarbiomis", nes trikdžiai jų veikloje gali daryti įtaką šalies ūkio ir visuomenės gerovei. Pvz., po nusikaltėliškų kibernetinių išpuolių prieš vienos ligoninės sistemą Jungtinėse

Tunne Kelam

„Sekdama geru policijos bendradarbiavimo pavyzdžiu, Europos Sąjunga privalo įveikti savo nenorą aktyvinti kibernetinį bendradarbiavimą. Šalys narės privalo padidinti savo pasirengimą ir lankstumą šioje sferoje. Tik aktyviai dirbant šia kryptimi, bus galima sukurti pasitikėjimo atmosferą, bendradarbiaujant super jautrioje kibernetinėje erdvėje."

Amerikos Valstijose ligoninės gydytojams ir administratoriams[10] buvo sumažinta prisijungimo prie paciento duomenų apimtis. Nustatyta tvarka (prieiga ir persiuntimas į pacientų duomenų korteles, laboratorijų darbas, rentgenas) ligoninėje buvo taip išgadinta, kad kai kurie pacientai turėjo būti perkelti į kitą ligoninę[11]. Įtariama, kad sutrikdymo priežastimi buvo kenkėjiška programa, priklausanti išpirkos reikalaujančių virusų šeimai, užšifruojančiai duomenis kompiuteriuose[12]. Ši ligoninė sumokėjo daugiau nei 17.000 USD kibernetinę išpirką, norėdama gauti raktą[13]. Lietuvos ligoninėse taip pat yra

[2] http://vlib.iue.it/history/internet/algorespeech.html

[3] https://en.wikipedia.org/wiki/Al_Gore_and_information_technology

[4] Stoll, C., Gegutės kiaušinis (The Cuckoo's Egg), pp. 27, 350. Pocket Books, Div. Of Simon and Shuster 1990.

[5] http://malware.wikia.com/wiki/Brain

[6] http://home.mcafee.com/virusinfo/virusprofile.aspx?key=291#none

[7] https://archive.org/details/DEFCON_19_The_History_and_the_Evolution_of_Computer_Viruses

[8] https://archive.org/details/DEFCON_19_The_History_and_the_Evolution_of_Computer_Viruses

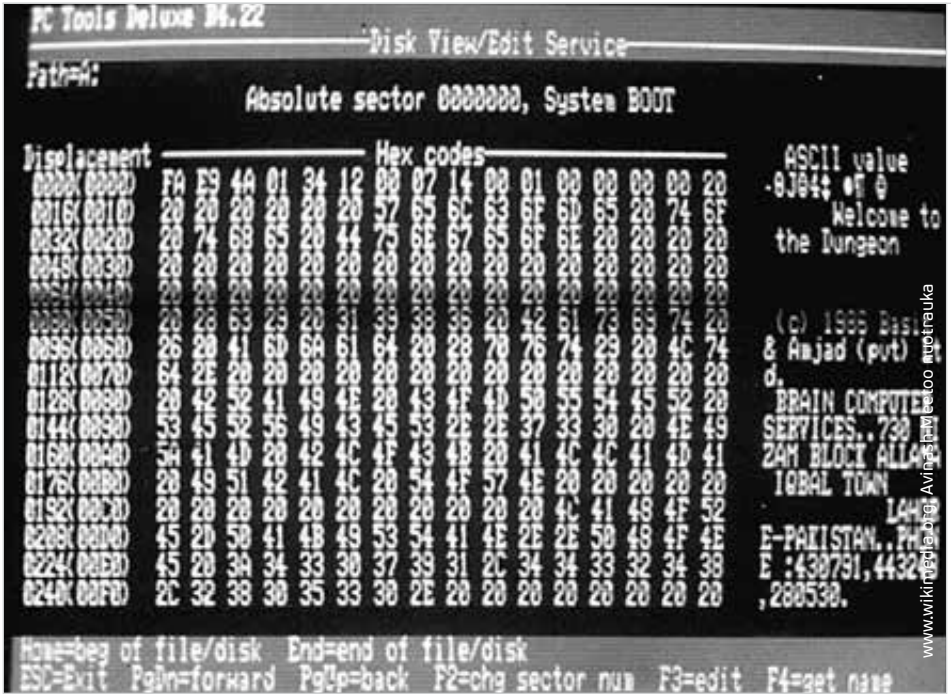
[9] Ypatingos svarbos infrastruktūra - tai objektai, teikiantys svarbiausias paslaugas, kurios yra [tautos] pagrindas ir yra [a] šalies ekonomikos, saugumo ir sveikatos pagrindas. Mes suprantame tai kaip elektros energiją,, kuria naudojame savo namuose, kaip vandenį, kurą mes geriame, transportą, kuris mus veža, parduotuves, kuriose mes apsiperkame, ir komunikacijos sistemas, kuriomis mes pasitikime, norėdami palaikyti ryšį su draugais ir šeima. JAV Dept of Homeland Security https://www.dhs.gov/what-critical-infrastructure 2016-03-01.

[10] Įsilaužta į ligoninę prašant išpirkos, http://cyberwarzone.com/hospital-hacked-and-held-for-ransom/

[11] Ibid.

[12] Hackett, R.., http://fortune.com/2016/02/16/hollywood-hospital-hack-ransom/ , February 16, 2016

[13] Pritchard, J., Hospital Ransomware Attack Alarms Cybersecurity Experts (Ligoninių atakos, prašant išpirkos, neramina kibernetinio saugumo ekspertus) http://www.newsfactor.com/story.xhtml?story_id=111003TV5J0I# February 2,, 2016



Pirmasis kenkėjiškas elgesys kibernetinėje erdvėje prasidėjo nuo studentų išdaigų, kai jie išbandė bendrą koncepciją (paskleidė *Brain (Smegenų)* virusą diskeliuose).

galimos tokios rizikos, ypač susikūrus e. sveikatos sistemai[14]. 2015 m. pabaigoje Lietuvos kibernetinė policija paskelbė, kad išpirkos reikalaujantis virusas buvo aptiktas kai kurių Lietuvos institucijų apskaitos sistemose[15]. Buvo pranešta, kad apskaitos duomenys bus atrakinti, sumokėjus 4 bitkoinus[16] (tuo metu jų vertė buvo apie 1860 USD[17]). Neturėtų stebinti tai, kad finansinės įstaigos taip pat nukentėjo nuo sudėtingų kibernetinių nusikaltėlių išpuolių. 2013 m. gruodžio mėn. buvo įsilaužta į „Target" parduotuvių nuolaidų tinklą, pavogti kreditiniai daugiau nei 100 milijonų klientų duomenys ir buvo padaryta 140 milijonų dolerių žala įmonei[18]. 2015 m. vasario mėn. IT saugumo bendrovė „Kaspersky Lab" paskelbė ataskaitą apie tarptautinių kibernetinių nusikaltėlių gaują „Carbanak", organizavusią tiesioginius išpuolius prieš bankus. Šiai grupei puikiai sekėsi skverbtis į finansinės kontrolės sistemas, naudojamas tarptautiniuose SWIFT ir automatizuotose banko sandorių transakcijose. Apskaičiuota, kad daugiau nei milijardas dolerių buvo pavogta tiesiai iš bankų Rusijoje, JAV, Vokietijoje, Kinijoje, Ukrainoje[19]. Lietuvos finansų įstaigos taip pat patyrė kibernetinių atakų, tačiau jos buvo daug mažesnės apimties nei minėtieji incidentai. 2012 m. sausio mėn. Lietuvos bankas patyrė atsisakymo aptarnauti (*Denial of Service* (DOS) ataką viešoje interneto svetainėje, tuo apsunkinant vartotojų patekimą į svetainę[20]. Nereikia pamiršti, kad Lietuvos bankai taip pat yra susieti su tarptautinėmis bankininkystės ir operacinėmis sistemomis, tokiomis kaip SWIFT[21] ir potencialiai yra taip pat pažeidžiami.

Socialiai motyvuotų programišių protesto veiksmai ir sutrikimai kibernetinėje erdvėje

Skirtingos formos grėsmę saugumui ir kibernetinei saugumo erdvei sukėlė kompiuterių įsilaužėliai, naudojantys savo įgūdžius dėl jiems svarbių socialinių priežasčių ar norėdami padaryti ką nors bloga. Skirtingai nuo kibernetinių nusikaltėlių, šių užpuolikų nedomina finansinė nauda, juos daugiau valdo noras lygiuotis į komiksų superherojus ar elektroninius linčiuotojus, siekiančius išspręsti tai, kas suvokiama esant negerai. Šie socialiai motyvuoti hakeriai arba „haktivistai" aiškiai neidentifikuoja savęs, vykdydami tam tikrą visuomeninį kibernetinį išpuolį prieš informacines sistemas, priklausančias tiems, kuriuos jie teisia dėl, jų nuomone, asmenų arba institucijų įžeidimo. Grupės ir (arba) asmenys, veikiantys kibernetinėje erdvėje ir neidentifikuojančios savęs, tokios kaip „Anonymous"[22], sužlugdė kibernetinės erdvės taiką. Geras šios veiklos pavyzdys - tai 2013 m. balandžio mėn. įvykęs Sveno Olafo Kamphuiso suėmimas. Kamphuisas buvo interneto prieglobos tarnybos, kuri buvo *Spamhaus.com*

[14] Lietuvos e sveikatos sistema pradeda veikti, http://www.15min.lt/naujiena/aktualu/sveikata/lietuvos-e-sveikatos-sistema-pradeda-veikti-541-507348 , 2015 birželio 3d.

[15] Lietuvoje plinta duomenis šifruojantis kompiuterinis virusas, Policijos departamento naujienos, http://www.policija.lt/index.php?id=34995, 2015-08-26

[16] 21 Hill, Kasmir. Ką aš sužinojau apie Bitcoin gyvendamas iš jų savaitę (Things I Learned About Bitcoin From Living On It For A Week) http://www.forbes.com/sites/kashmirhill/2013/05/09/25-things-i-learned-about-bitcoin-from-living-on-it-for-a-week-/#d67c83d27ca6 2013 gegužės 9 (May 9, 2013)

[17] Palmer, D., From Worst to First: Bitcoin's Price Ends 2015 on Top (Nuo blogiausio iki pirmojo: Bitkoinų kaina baigiasi 2015, http://www.coindesk.com/bitcoin-price-in-2015-doom-and-gloom-give-way-to-positive-years-end/ , December 29, 2015.

[18] Nepapasakota tikslinės atakos istorija. Žingsnis po žingsnio (The Untold Story of the Target Attack Step by Step), Aorato Labs, https://aroundcyber.files.wordpress.com/2014/09/aorato-target-report.pdf 2014

[19] Carbanak APT Didysis banko apiplėšimas (The Great Bank Robbery) Kaspersky Lab 'HW, Moscow p. 3-4. https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf 2015 Vasaris.

[20] Lietuvos centrinis bankas nukentėjo nuo kibernetinių išpuolių http://phys.org/news/2012-01-lithuanian-central-bank-cyber-attack.html , 2012 Sausio 27 d.

[21] SWIFT globalus komunikacijų tinklas, palengvina 24 valandų saugų tarptautinį mokėjimo nurodymų keitimąsi tarp bankų, centrinių bankų, tarptautinių korporacijų ir pagrindinių vertybinių popierių įmonių (Worldwide Interbank Financial Telecommunications: Global communication network that facilitates 24-hour secure international exchange of payment instructions between banks, central banks, multinational corporations, and major securities firms). http://www.businessdictionary.com/definition/SWIFT.html , 2016-03-01
Dar šiuo klausimu galite skaityti: http://www.businessdictionary.com/definition/SWIFT.html#ixzz41eIEwCqi

[22] http://www.anonews.co/10-things-everyone-should-know-about-anonymous//

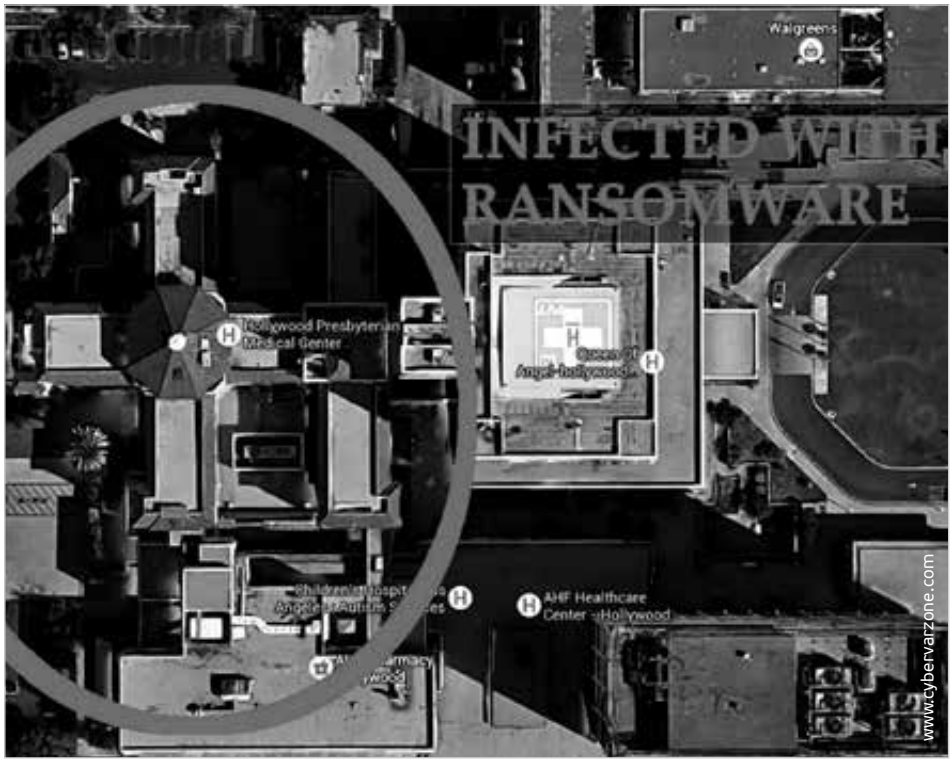
kompanijos juodajame sąraše; operatorius. *Spamhaus.com* kovoja su šlamštu, viešindama šiukšles siuntinėjančių svetainių operatorius. Protestuodamas S. O. Kamphuisas, įtariama, prisidėjo prie vienos didžiausių iki to laiko interneto svetainių atsisakymo aptarnauti (Denial of service) atakos, nukreiptos į svetainę Spamhaus, sukūrimo.[23] „Priežastis" paviešinta p. Kamphuis, Olandijos gyventojo, sulaukė dėmesio ir pritarimo iš Anglijoje gyvenančio p. Seth'o Nolano-McDonagh'o, kuris taip pat buvo suimtas už tai, kad prisidėjo organizuojant šią atsisakymo aptarnauti ataką[24]. Šie asmenys sieja save su socialiai motyvuota „haktivistų", kurie įsilaužimus atlieka „anonimiškai", veikla, kuri, panašu, yra aptinkama ir Lietuvoje. Vieną šeštadienio popietę su šeima vaikščiojau po Vilniaus Gedimino prospektą, pagrindinę Vilniaus gatvę. Mūsų dėmesį atkreipė taiki demonstracija, vykstanti šalia Vinco Kudirkos (gydytojo, sukūrusio Lietuvos himną) skulptūros, esančios prieš Vyriausybės rūmus. Mane labai nustebino tai, kad keli protestuotojai minioje stovėjo dėvėdami „Guy Fawkes" kaukes, kurios dažnai yra siejamos su internetine „haktivistų" grupe „Anonymous"[25]. Grupės, įsilaužusios į „Sony Corporation" dėl teisinių veiksmų, kurių korporacija ėmėsi bandydama apsiginti nuo įsilaužėlių, modifikavusių „Sony Playstation" konsolę[26]. Mane nusmelkė šaltukas ir pagalvojau, „Anonymous" jau čia, Vilniuje, Lietuvoje. Mes tikrai nesame izoliuoti ir apsaugoti nuo kenkėjiškos veiklos kibernetinėje erdvėje.

Kibernetinis šnipinėjimas

Informacijos ir ryšių technologijų, sukūrusių šiandienos internetą, suderinimas leido sukurti naują informacijos erą. Informacijos vertė buvo aprašyta įvairiais būdais. Thomasui Jeffersonui, parašiusiam kolonijinės Amerikos nepriklausomybės deklaraciją, informacija buvo tarsi skydas, saugantis nuo despotizmo, kaip „demokratijos valiuta"[27], tuo tarpu Victor'ui Kiamui, kažkada vadovavusiam „Remington" įmonei, informacija buvo raktas į verslo sėkmę ir buvo vadinama „derybininko didžiausiu ginklu"[28]. Kita citata (autorius nežinomas) informacija apibūdinama lyginant praeitį su dabartimi ir suteikiant dar gilesnę prasmę: „Akmens amžius buvo paženklintas protingu nesudėtingų įrankių naudojimu; informacijos amžius iki šiol buvo paženklintas sudėtingų įrankių neprotingu naudojimu"[29].

Pramoninis šnipinėjimas

Kibernetinis šnipinėjimas, siekiant pavogti pramonines paslaptis iš ekonomiškai ir techniškai pažangesnės šalies, tapo besivystančiųjų šalių naudingu laiko ir išteklių taupymu, siekiant tapti klestinčia ir konkurencinga šalimi. Ši veikla tapo ypač akivaizdi aukštųjų technologijų ir gynybos pramonėse. 2009 m. buvo pranešta, kad įtariama, jog Kinijos vyriausybės remiami įsilaužėliai įsibrovė ir pavogė informaciją iš JAV vyriausybės ir rangovo informacinės sistemos apie naująjį naikintuvą[30]. Nuo tada kitos bendrovės (pvz., *Google, Booz Allen, Sony, VISA, Nissan, Mastercard*) patyrė tokių pačių išpuolių ir, pasak buvusio Nacionalinės saugumo agentūros direktoriaus generolo Keitho Briano Alexanderio ,



Po nusikaltėliškų kibernetinių išpuolių prieš vienos ligoninės sistemą Jungtinėse Amerikos Valstijose ligoninės gydytojams ir administratoriams buvo sumažinta prisijungimo prie paciento duomenų apimtis.

[23] Gilbert, D., Olandai įtaria, kad Sven Olaf Kamphuis areštuotas už didžiausią kibernetinę ataką interneto istorijoje (Dutch Suspect Sven Olaf Kamphuis Arrested for Biggest Cyber Attack in Internet History), http://www.ibtimes.co.uk/articles/461848/20130426 spamhaus-suspect-arrests-spain-kamphuis.htm April 26, 2013

[24] Muncaster, P., Britų Spamhaus DDoS paaugliai vaikšto laisvi (British Spamhaus DDoS Teen Walks Free), http://www.infosecurity-magazine.com/news/ british-spamhaus-ddos-teen-walks/ 13 July 2015.

[25] Yin, S., 'Anonymous' atakuoja Sony, siekdami paremti PS3 hakerius ('Anonymous' Attacks Sony in Support of PS3 Hackers, PC Mag, https://en.wikipedia.org/wiki/ Anonymous_(group) , April 4, 2011.

[26] http://www.pcmag.com/article2/0,2817,2383018,00. asp

[27] Žinomų citatų knyga, interneto šaltinis, Haythem Khalil (Book of Famous Quotes), on-line source, Haythum Khalid http://www.famous-quotes.com/topic. php?tid=631

[28] Ibid.

[29] Ibid. Skirta „Anonymous" (Attributed to „Anonymous")

[30] Gorman, S., Cole, A., Dreaazen, Y., Kompiuterių šnipai pažeidžia Fighter Jet projektą (Computer Spies Breach Fighter Jet Project),http://www.wsj.com/articles/ SB124027491029837401 April 21, 2009

šios vagystės vertė atitinka „didžiausią turto perkėlimą istorijoje"[31]. Kadangi atakos prasideda elektroninėje erdvėje, jas identifikuoti (priskirti) ir nubausti įsilaužėlius yra labai sudėtinga. Visgi 2014 m. gegužės mėn. JAV Teisingumo departamentas žymaus įvykio atveju, kai viena šalis pareiškia ieškinį dėl kibernetinio šnipinėjimo kitai, oficialiai apkaltino penkis Kinijos kariuomenės atstovus įsilaužimu į kompiuterius ir vertingų prekybos paslapčių iš pirmaujančios plieno, branduolinės ir saulės energijos įmonės vagyste[32]. Šis atvejis yra geras didėjančio kibernetinio šnipinėjimo tarptautiniuose santykiuose pavyzdys. Lietuva jokiu būdu nėra izoliuota nuo tokios veiklos. 2014 m. Valstybės saugumo departamentas savo pranešime dėl grėsmių Lietuvos nacionaliniam saugumui konkrečiai nurodė, kad „kibernetinį šnipinėjimą ir kenkėjišką kibernetinę veiklą vykdančios Rusijos saugumo ir žvalgybos tarnybos kelia grėsmę Lietuvos ypatingos svarbos infrastruktūroms ir įslaptintos informacijos saugumui. Dėl padidėjusios įtampos tarp valstybių, kaip paminėta pavyzdyje apie JAV vyriausybės įtarimų dėl kibernetinio šnipinėjimo pateikimo Kinijos kariuomenės atstovams, aukščiau minėtas kibernetinio šnipinėjimo atvejis gali būti interpretuojamas kaip karinis aktas. Tai JAV iš tiesų apgalvojo priskirdama kibernetinio šnipinėjimo incidentą Rusijai, pasitelkusiai aktyvią kibernetinio šnipinėjimo programą veikti kitoje šalyje.[34] Kai kas gali greitai atmesti kibernetinį šnipinėjimą kaip karinį veiksmą, sakydamas, kad šnipinėjimas turi senas tradicijas ir yra dažnai praktikuojamas bei priimtas


https://upload.wikimedia.org/wikipedia/commons/4/4c/Guy-fawkes.png

„Guy Fawkes" kaukės dažnai yra siejamos su internetine haktivistų grupe „Anonymous".

kaip „realaus pasaulio" praktika. Tai ne visai tas atvejis, kai šnipinėjimas vyksta elektroniniu būdu kibernetinėje erdvėje. Skirtingai nuo tradicinio šnipinėjimo, kai žmogus pavagia informaciją, kibernetinio šnipinėjimo veikla yra unikali ta prasme, kad elektroniniam šnipui įsiskverbus į sistemą, labai mažai pastangų reikia, norint pakeisti šnipinėjimo veiklą (dokumentų atsisiuntimą) sabotažu. Tai vadinama pasiruošimu mūšiui. Kai įsilaužėliai įsiskverbia į sistemą ir įsikuria joje - tai jau labai mažas skirtumas tarp šnipinėjimo ar sabotažo. Tai tik *ENTER* klavišo paspaudimo klausimas, skiriantis elektroninio dokumento vagystę nuo sistemos sunaikinimo toje vietoje, kurioje ji yra. Šis mūšio lauko paruošimas, jei yra aptinkamas aukos, gali būti labai provokuojantis ir krizės kontekste lengvai peraugantis į rimtas konflikto formas. Tai ypač aktualu, kai yra nusitaikoma į šalies ypatingos svarbos infrastruktūros objektus.

Kenkėjiškos šalių veiklos kibernetinėje erdvėje kelia grėsmę nacionaliniam saugumui, ekonomikai ir visuomenės gerovei

Iki 2010 m. dauguma kenkėjiškų kibernetinių veiklų buvo vykdomos kibernetinių nusikaltėlių, socialiai motyvuotų hakerių, taip pat vyko vyriausybių šnipinėjimas kitoms vyriausybėms ir šnipinėjimas tarp verslo konkurentų. Labai nedaugelis tada galėjo įsivaizduoti, kad kibernetinės erdvės ginklai gali būti naudojami kaip nusivylusių valstybių

[31] Rogin, J., NSI vadovas: Kibernetiniai nusikaltimai sudaro "didžiausią turtų perdavimą istorijoje (NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history" http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/ 2012 liepos 9 (July 9, 2012.)

[32] Nakashima, E., Wan, W., JAV skelbia pirmuosius kaltinimus užsienio šalims dėl kibernetinio šnipinėjimo (US announces first charges against foreign country in connection with cyberspying) https://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html 2014 gegužės 19 (May 19, 2014)

[33] Grėsmių Lietuvos nacionaliniam saugumui vertinimas 2014, p. 7 State Security Department, http://www.vsd.lt/Files/Documents/635633000992101250.pdf , 2015

[34] Elkus A., „Moonlight Maze" in Healey J. ed., A Fierce Domain: Conflict in Cyberspace, 1986-2012, Cyber Conflicts Studies Association, 2013., p. 152-160.

[35] Kushner, D., Tikroji Stuxnet istorija (The Real Story of Stuxnet) http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet , 2013, vasario 26

[36] Valstybė identifikuoti kaip Stuxnet autorius atliko pirmiausia saugumo tyrėjas Ralph Langner kovo 2011 metu Ted kalbos metu (.State identified as author of Stuxnet done first by security researcher Ralph Langner in March of 2011 during Ted Talk). See http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon

svarbūs užsienio politikos tikslai, siekiant įgyvendinti užsienio politikos priemones, kai tradicinės diplomatijos naudoti nesiseka. Antivirusinių bendrovių pranešimai, prasidėję 2010 metų vasarą apie *Stuxnet*[35], sudėtingą internetinį kirminą, kurį sukūrė valstybė, nusitaikiusi į ypatingą kitos valstybės infrastruktūrą[36], labai pakeitė mūsų supratimą apie tai, koks gali būti pavojingas kenkėjiškas elgesys kibernetinėje erdvėje.

Nerimą sukėlė nauja ir labai rafinuota savo forma kenkėjiška programinė įranga, galinti veikti nepastebimai ir įveikti saugumo priemones, vykdydama atakas, nukreiptas prieš pramoninės įrangos kontrolės sistemas, suardant minėtą įrangą. *Stuxnet* – tai buvo takoskyra, pakeitusi kibernetinio saugumo kraštovaizdį.[37] Ši kenkėjiška programa buvo specialiai suprogramuota priežiūros kontrolės ir duomenų surinkimo (SCADA) valdymui ir programuojamų loginių valdiklių sistemų, atitinkančių tam tikrus kriterijus, perėmimui. Jei šie kriterijai atitinka (branduolinio sodrinimo įrenginys Irane), *Stuxnet* perima valdymo sistemas ir sukelia įrangos (centrifugų) veiklos sutrikimus ir sunaikina ją. Kai šis virusas patenka į sistemą, jis saugos jutikliams ir automatinėms saugos sistemoms išsiuntinėja neteisingus duomenis apie teisingą valdymą, kai jo iš tikrųjų jau nebėra. Virusas naikina įrenginius, nors operatoriai valdymo salėje vis dar stebi sistemos monitorius, rodančius kad viskas veikia normaliai. Neįmanoma susilaikyti nepaklausus, ar *Stuxnet* tipo ataka gali sukelti pakopinių avarijų, lemiančių visišką energijos gamybos įmonės ar net visą ypatingos svarbos infrastruktūros objektų sektorių uždarymą?

Stuxnet sukūrė precedentą. Modernus kibernetinis ginklas, rodantis kad į tai yra įsitraukusi valstybė, buvo sukurtas ir nukreiptas į tikslą, pasiekiant rezultatą. Buvo parodyta bendra idėja ir nebuvo galima nustatyti, kas tai padarė! Įsilaužėliui atrodytų, kad tikslas buvo pasiektas (branduolinio sodrinimo programos Irane vėlavimai ir sutrikimai) su mažiausiomis sąnaudomis. Buvo įrodyta, kad kibernetinis ginklas yra veiksminga priemonė po žeme esančiam įrenginiui neutralizuoti, ir neturi reikšmės, ar jis buvo sujungtas su internetu. Virusas gali būti įterpiamas į darbuotojo nešiojamąjį kompiuterį per infekuotą atmintuką. Deja, vėlesni įvykiai parodė, kad buvo pasinaudota kitų įsilaužėlių pavyzdžiu. 2012 m. gruodžio mėn. buvo surengta kibernetinė ataka prieš kitų šalių ypatingos svarbos infrastruktūros objektus. Didžiausia pasaulio naftos bendrovė „Saudi Aramco“ patyrė tikslinį kibernetinį išpuolį prieš įmonės kompiuterius. Šis kibernetinis ginklas, vadinamas *SCHAMOON* arba „valikliu“, švariai išvalė duomenis iš daugiau kaip 30.000 kompiuterių kietųjų diskų. Ši ataka palietė tik įmonės administracijos kompiuterius ir neturėjo įtakos ypatingos svarbos infrastruktūros objektams, susijusiems su naftos gavyba ir perdirbimu. „Saudi“ įmonė šį kibernetinį išpuolį priėmė kaip ataką, grasinusią ne tik ypatingos svarbos energetikos infrastruktūrai, bet ir visai jos ekonomikai.[38] Nors ir nebuvo jokių įtikinamų įrodymų, buvo stipriai įtariama, kad svetima vyriausybė buvo atsakinga už šią kibernetinę ataką[39]. Šis incidentas sujudino kibernetinio saugumo bendruomenę ir energetikos pramonę. Pranešimas vėl buvo sustiprintas: kibernetinės atakos – tai labai patraukli, veiksminga, nebrangi, sukelianti minimalią netiesioginę žalą priemonė, skirta sukelti nuostolių konkurentams. Pasitvirtino ir tai, kad įsilaužėliui nieko nemalonaus nenutinka, jis nėra kažkaip viešai suvaržomas ar nubaudžiamas.

Nors įsilaužusiems į „Saudi Aramco“ pavyko ištrinti kompiuterių duomenis bendrovės tinkle, pasak *Stuxnet* kūrėjų, atrodo, kad įsilaužėliai neturėjo pakankamai žinių, reikalingų sudėtingesnėms sisteminėms gamybos operacijoms ir sistemoms sutrikdyti. Veikiai šis pavyzdys buvo pritaikytas atakuojant kitą ypatingos svarbos infrastruktūros objektą gamybos sektoriuje. 2014 m. pabaigoje Vokietijos vyriausybės Federalinis IT departamentas (BS) paskelbė kibernetinio saugumo incidentų, įvykusių per pastaruosius metus, ataskaitą. Vienas iš šios ataskaitos skyrių atskleidė kibernetinį įsilaužimą, įvykusį neįvardintoje Vokietijos plieno gamykloje ir padariusį fizinės žalos liejykloje[40]. Įsilaužimas aprašytas kaip patekimas į įmonės arba bendrovės tinklus ir vėliau į įmonės gamybos valdymo sistemas. Operatoriams supratus, kad kažkas vyksta neįprastai, jie jau nebesugebėjo išjungti liejimo įrenginio ir tai padarė realių nuostolių. Ataskaitoje apibūdinami įsilaužėlių įgūdžiai kaip „labai pažengusių, turinčių ne tik klasikinio IT saugumo žinių, bet ir pramonės valdymo sistemų bei gamybos procesams reikalingų išsamių techninių žinių“. Šis aprašymas gali būti naudojamas apibūdinant tikslinę kiberataką (Advanced Persistent Threat (APT). APT išpuoliai nėra finansiškai motyvuoti, tačiau jie yra labai sudėtingi ir ilgalaikiai. Jie nesibaigia tol, kol tikslas nėra pasiektas. Manoma, kad vyriausybės tiesiogiai užsako ar remia APT išpuolius[41]. Atrodytų, kad tokią skverbimosi į internetą taktiką, pažeidžiant įmonių tinklą ir taip patenkant į

[37] Detaliau apie STUXNET žr.: (For a more detailed analysis of STUXNET see:) http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

[38] AL Arabiya with AFP, Saudi Aramco sako, kad kibernetiniai išpuoliai nusitaikė į Karalystės ekonomiką („Saudi Aramco says cyber-attack targeted kingdom's economy“), Al Arabiya News, http://english.alarabiya.net/articles/2012/12/09/254162.html , 09 12 2012.

[39] Perlroth N., Kibernetinės Saudo firmos atakos metu, JAV mato kad Iranas kovoja prieš („In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back „), New York TImes, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html , 23 10 2012.

[40] IT saugumo padėtis Vokietijoje 2014 m, Federalinė informacijos saugumo tarnyba (The State of IT Security in Germany 2014, Federal Office for Information Security) (Bundesamt für Sicherheit in der Informationstechnik – BSI) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 ,p. 31, November 2014

valdymo sistemas ir gamybinius tinklus, geba atlikti dar bent keli įsilaužėliai. 2015 m. gruodžio 23 d. prieš pat Šv. Kalėdas Ukrainos vyriausybės institucijos ir elektros energijos įmonės pradėjo siųsti pranešimus apie elektros energijos tiekimo nutraukimą Vakarų Ukrainos regionuose. Pasak vienos elektros energetikos įmonės atstovų, daugiau nei 80,000 klientų buvo nutrauktas elektros energijos tiekimas po to, kai 27 elektros energijos pastotės buvo atjungtos nuo tinklų[42]. Pradinė, tačiau nepatvirtinta kai kurių pateiktų operatorių duomenų saugumo kompanijų analizė parodė, kad pastotės buvo atjungtos dėl kibernetinių išpuolių, nukreiptų prieš elektros tinklų valdymo sistemas[43]. Jungtinių Amerikos Valstijų vidaus saugumo departamentas, konsultavęs Ukrainos valdžios institucijas, apibūdino šį išpuolį kaip „sinchronizuotą ir koordinuotą, tikriausiai sekantį išsamius žvalgybinius aukos tinklus"[44]. Išanalizavus atakos duomenis, jie pasirodė esantys panašūs į kibernetinį įsilaužimą į Vokietijos plieno gamyklą. Kaip kompanija „BSI" anksčiau pranešė, įsibrovimas prasidėjo įmonės tinkle ir persikėlė į gamybos (SCADA – priežiūros, kontrolės ir duomenų rinkimo sistemos) tinklus ir neleido operatoriui valdyti bei prižiūrėti sistemą[45]. Kaip pranešė Ukrainos saugumo tarnyba, dar kartą buvo įtarta, kad svetima valstybė buvo bent iš dalies atsakinga už kitą išpuolį prieš ypatingos svarbos infrastruktūros objektus[46]. Įrodymų apie Rusijos atakų šaltinius buvo gauta išanalizavus kenkėjiškų programų kodą, kuris atskleidė, kad tai yra kenksminga programa *BlackEnergy*, kurios ataka susijusi su rusų[47] „Sandworm" grupe[48]. Tačiau, kaip ir ankstesnių kibernetinių išpuolių prieš ypatingos svarbos infrastruktūros objektus metu, kai, siekiant imtis teisinių veiksmų nubausti įtariamus atakos organizatorius, buvo įtarta valstybė, jokių įtikinamų įrodymų nebuvo pateikta. Lietuvos ypatingos svarbos infrastruktūros operatoriai ir mes, žmonės, kurie naudojamės vandens, šilumos ir elektros energijos tiekimo paslaugomis, turėtume žinoti, kad išpuolių prieš šias gyvybiškai svarbias sistemas, kaip ir prieš kitų šalių ypatingos svarbos infrastruktūros objektus, gali būti vykdoma ir pas mus. Yra žmonių, kurie, kaip ir ypatingos svarbos infrastruktūros objektų operatoriai, mano, kad jų naudojami tinklai ir sistemos nėra prijungti prie interneto. Du Jungtinių Amerikos Valstijų valdymo sistemų inžinieriai nusprendė patikrinti prielaidą, kad ypatingos svarbos infrastruktūros objektų valdymo sistemos nėra prijungtos prie interneto. 2013 m. du patyrę kontrolės sistemos inžinieriai pritaikė *Shoda*n paieškos įrenginį „matomų" valdymo sistemų paieškai internete. Jų paskelbtos išvados buvo gana netikėtos. Jie galėjo patvirtinti, kad per 2 mln. prietaisų 211 šalių atsiliepė į jų užklausas. Lietuvos ypatingos svarbos infrastruktūros sektoriuose beveik 2000 įrenginių reagavo į užklausą iki *Shine* projekto uždarymo 2014 m. sausio mėn.[49] projektas buvo uždarytas ne dėl to, kad autoriai nebegavo naujų atsakymų į pateiktas užklausas, o todėl, kad jie pasiekė savo tikslą ir įrodė, kad kai kurie įtaisai, priklausantys ypatingos svarbos infrastruktūros sektoriaus pramonės valdymo sistemoms, iš tiesų buvo „matomi" internete ir potencialiai prie jų galima buvo prisijungti bei jais manipuliuoti.

Valstybinė priežiūra

Kenkėjiškos kibernetinės valstybių veiklos neapsiriboja tik žala išorės taikiniams, jos taip pat gali būti nukreiptos kitoms šalims sekti ar net savo pačių piliečiams šnipinėti. 2010 m. gruodžio mėn. prasidėjus Arabų pavasario demonstracijų bangai, sukrėtusiai Artimuosius Rytus, autoritarinės vyriausybės, pajutę protestuotojų grėsmę, siekė bent iš dalies apsiginti, naudodamos technologines priemones. Pavyzdžiui, tęsiantis demonstracijoms Egipte, Vyriausybė nusprendė atjungti interneto ir mobiliojo ryšio telefono paslaugas, norėdama sutrikdyti demonstracijų organizatorių gebėjimą bendrauti su pasekėjais ir koordinuoti protestus[50]. Vėliau pasirodė pranešimų, kad Artimųjų Rytų vyriausybės naudojo Vakaruose sukurtas kenkėjiškas sekimo programas, tokias kaip *Finfisher*, kurios skirtos įtariamųjų ir valdžiai neįtinkančiųjų bei dalyvaujančiųjų demonstracijose piliečių šnipinėjimui[51]. Vakarų vyriausybės, turinčios ilgą demokratinių tradicijų

[41] Blue, V., Microsoft - JAV vyriausybė yra „progresyvi nuolatinė grėsmė (Microsoft: US government is an 'advanced persistent threat') http://www.zdnet.com/article/microsoft-us-government-is-an-advanced-persistent-threat/ December 6, 2013.

[42] Karpatų energetika po kibernetinių atakų (Прикарпатські енергетики оговтуються після кібератаки), http://www.oe.if.ua/showarticle.php?id=3415&id_cat=2 , 12.01.2016

[43] Assante, M., Patvirtinimas apie koordinuotą Ukrainos elektros tinklo ataką (Confirmation of a Coordinated Attack on the Ukrainian Power Grid) https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid , 2016 sausio 9,

[44] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[45] The State of IT Security in Germany 2014, Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3 ,p. 31, November 2014

[46] СБУ попередила спробу російських спецслужб вивести з ладу об'єкти енергетики України (Security has warned the Russian special services try to bring down energy facilities Ukraine) , Прес-центр СБ України , http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=170951&cat_id=39574 28 грудня 2015.

[47] Ward, S., iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign http://www.isightpartners.com/2014/10/cve-2014-4114/ October 14, 2014

[48] Hultqvist, J., Sandworm komanda ir išpuoliai prieš Ukrainos energetikos tarnybą (Sandworm Team and the Ukrainian Power Authority Attacks http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/ , , 2016 m. Sausio 7 d.

[49] Shine rezultatų ataskaita (Shine Findings Report), Infracritical. http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014 , 1 October 2014

[50] Richtel, M., Egiptas atjungia daugumą interneto ir mobiliojo telefono paslaugų (Egypt Cuts Off Most Internet and Cell Service) http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=0 ,2011 sausio 28 (JAN. 28, 2011)

istoriją, negalėjo atsispirti galimybėms prieiti prie asmeninės informacijos apie ryšius ir veiklą, kai šią informaciją buvo galima rasti internete. Šie įsibrovimai buvo pateisinami nacionaliniu saugumu, susijusiu su karu prieš terorizmą. Atsižvelgiant į viešąją nuomonę, pradžioje šie įsibrovimai buvo palaikomi arba apie juos nebuvo nieko žinoma. Padėtis pakito, kai 2013 m. vasarą buvęs JAV Nacionalinės saugumo agentūros (NSA) rangovas Edwardas Snowdenas, atskleidė įslaptintąją informaciją, parodydamas kokios sudėtingos ir plačios yra Vyriausybės stebėjimo ir šnipinėjimo galimybės.

Ukrainos elektros tinklai – vieni pirmųjų patyrę koordinuotą kibernetinę ataką, perimant infrastruktūros valdymą.

Pono Edwardo Snowdeno paslapties paviešinimas

E. Snowdeno paslapties paviešinimas, net jei tai yra tik pusė tiesos, turėtų priversti rimtai susirūpinti visus interneto vartotojus arba visus piliečius, bendraujančius kibernetinėje erdvėje. Šis straipsnis yra per trumpas, kad būtų galima išsamiai aprašyti p. Snowdeno iškeltas vyriausybės priežiūros bei privatumo sekimo problemas, jas paviešinus. Jei galima būtų trumpai apibendrinti, p. Snowdenas parodė, kad vyriausybės turi techninių galių stebėti, rinkti, apdoroti duomenis, rastus kibernetinėje erdvėje. Pateiktos konkrečios problemos, kurias paviešino p. Snowdenas ir kurias gali įgyvendinti vyriausybės, yra naujos, su kuriomis galbūt daugelis iš mūsų niekada nebuvome susidūrę:

- telekomunikacijų paslaugų teikėjai, teikiantys Vyriausybei informaciją apie telefono skambučius šalies viduje ir už jos ribų;
- komunikacijos srauto iš pirmaujančiųjų interneto kompanijų (pvz. *Microsoft, Google, Facebook, Youtube, Skype* ir *Apple*) serverių surinkimas;
- programinės įrangos milijonų žmonių duomenų bazių, surinktų e. pašto adresų, internetinių pokalbių ir naršymo istorijų paieškai naudojimas, neturint įgaliojimų;
- vyriausybės išmokos saugumo bendrovėms už susilpninto šifravimo sistemų kūrimą ir pardavimą klientams. Šios sistemos leidžia lengviau iššifruoti duomenis ir prie jų nesąžiningai prieiti žvalgybos agentūroms;
- pasaulio mobiliųjų telefonų sekimo vietos (5 milijardų įrašų per dieną);
- įsiskverbimas ir duomenų srautų kopijavimas visuose šviesolaidiniuose kabeliuose, perduodančiuose informaciją tarp duomenų centrų[52].

Yra tam tikrų požymių, kad įtariamos veiklos, kurias atskleidė p. Snowdenas, yra paplitusios ir turi rimtų pasekmių tarptautiniam saugumui. Vienas toks pavyzdys - tai tariamas kibernetinis įsilaužimas, vykęs 2013 m vasarą „Belgacom“, Belgijoje įsikūrusioje telekomunikacijų bendrovėje. „Belgacom“ ir jos dukterinės įmonės yra pagrindinis Europos ir pasaulio telekomunikacijų paslaugų teikėjas, turintis sąsajų su ryšių infrastruktūromis kitose pasaulio dalyse. Jos užsakovai - tai NATO ir Europos Sąjunga, turinčios savo būstines ir daug susijusių institucijų Belgijoje. Šis kibernetinis įsilaužimas yra rimtas pavojus programinei įrangai. Įsilaužėlis pasiekė ryšių centrą. Bet ką, ką labai slaptas „Belgacom“ tinklo operatorius galėjo padaryti, įdiegtoji kenkėjiška programa galėjo padaryti tą patį... Ji turėjo visus raktus, visus slaptažodžius ir visišką kontrolę[53]. Išpuolio rafinuotumas parodė, kad svetima valstybė buvo už tai atsakinga, tačiau įtariamos šalys nepriklausė „įprastinėms įtariamosioms“ šalims, tokioms kaip Šiaurės Korėja, Kinija ar Rusija. Sąrašo viršuje buvo Belgijos sąjungininkai[54]. Rimčiausi

[51] Toor A., Brandom, R., Šnipas įrenginyje (A Spy in the Machine), http://www.theverge.com/2015/1/21/7861645/finfisher-spyware-let-bahrain-government-hack-political-activist, 2015-01-21.

[52] Volz, D, Viskas, ką mes sužinojome iš Edward Snowden 2013 (Everything We Learned From Edward Snowden in 2013), The Guardian, http://www.nextgov.com/defense/2013/12/everything-we-learned-edward-snowden-2013/76106/?oref=nextgov_defense_it ,2013 gruodžio 31 (December 31, 2013).

[53] Koot, M., Belgakom – ant katastrofos slenkščio (Belgacom – „On the brink of catastrophe“) translation, Matthijs R. Koot's Notebook, https://blog.cyberwar.nl/2013/09/belgacom-on-the-brink-of-catastrophe-translation/#comment-130374 , 2013-09-23 to 2014-12-13.

p. Snowdeno informacijos atskleisti ženklai yra akivaizdūs, ypač tada kai tai siejama su *Stuxnet* operacija. Viską įvertinus, net jei *Stuxnet* būtų buvusi veiksminga operacija, ji negalėtų būti sėkminga be reikšmingo žvalgybos tarnybų indėlio. Norint parengti modernesnį kibernetinį ginklą ir sėkmingai nutaikyti jį į inžinerines sistemas, reikia surinkti daug žvalgybinės informacijos. Jei p. Snowdeno paslapties atskleidimas mums ką nors papasakotų, tai būtų siejama su tuo, kad šalių vyriausybės turi didžiulius žvalgybinės informacijos rinkimo pajėgumus. Galiausiai aiškėja, kad *Stuxnet* tipo išskirtinis kibernetinių ginklų vystymasis ateityje labiau įmanomas, nei yra tikimasi.

Iškyla esminis klausimas, ką daryti, kai kenkėjiškas elgesys kibernetinėje erdvėje tampa įpročiu. Jau tampa įprasta, kad džiaugiamasi, kai po sėkmingo įsibrovimo ar išpuolio prieš valstybės ypatingos svarbos infrastruktūros objektus kaltininkas yra nenustatomas arba lieka nenubaustas. Ar tokios veiklos nėra potenciali grėsmė taikai, nesant veiksmingos tarptautinės kontrolės pasaulyje?

Edward Snowden

KODĖL VALSTYBĖS VEIKLA KIBERNETINĖJE ERDVĖJE YRA SVARBUS KLAUSIMAS VISIEMS KIBERNETINĖS ERDVĖS VARTOTOJAMS?

Valstybės, turinčios skirtingus kibernetinius pajėgumus, rodo mums dvi[55] skirtingas veido išraiškas. Pirmoji yra labai draugiška ir susirūpinusi, kai norima pasidalinti apie didėjančias grėsmes, kylančias kibernetinėje erdvėje. Antroji išraiška yra piktavališka, aktyviai prisidedanti prie šių grėsmių plitimo. Trečioji išraiška yra sunkiai numatoma, bet ji akivaizdi, kaip ir astrofizikoje juodosios skylės. Tai polinkis į autoritarizmą, išreikštą piliečių laisvių ir privatumo sumažėjimu, naudojant šias naujas technologijas, įgalinančias sekti privatų piliečių gyvenimą ir naudoti tai kaip galimybę kontroliuoti skirtingas nuomones. Šias tris išraiškas skirtingais būdais demonstruoja kibernetinės pasaulio supervalstybės. Į šį trumpą sąrašą patenka Rusija, Kinija, JAV, Australija ir Jungtinė Karalystė[56]. Pavyzdžiui, Rusija ir Kinija yra lyderės, siūlančios valstybėms apriboti kibernetinėje erdvėje savo kenkėjiškus veiksmus, galinčius pažeisti ypatingos svarbos infrastruktūros objektus ir daryti nuostolių nacionalinei ekonomikai bei visuomenės gerovei. 2011 m. rugsėjo mėn. 12 d. Rusija ir Kinija vadovavo Šanchajaus bendradarbiavimo organizacijai rengiant pasiūlymą Jungtinių Tautų Generalinei asamblėjai „Tarptautinis informacijos saugumo elgesio kodeksas“. Laišką pasirašiusieji, tarp kurių taip pat buvo Tadžikistanas ir Uzbekistanas, išreiškė bendrą susirūpinimą dėl grėsmių kitų valstybių ypatingos svarbos infrastruktūros objektų gerovei dėl kenkėjiškų valstybių veiklos elektroninėje erdvėje. Laiško Elgesio kodekso skyriuje šios valstybės specialiai pasiūlė „Nenaudoti ICT[57], įskaitant tinklus, priešiškai veiklai ar agresijos aktams atlikti ir nekelti grėsmės tarptautinei taikai ir saugumui. Nedauginti informacinių ginklų ir su tuo susijusių technologijų“[58]. Jungtinės Valstijos taip pat užėmė priešakines pozicijas ieškodamos būdų, kaip susidoroti su tokiomis pačiomis problemomis. Pavyzdžiui, JAV vyriausybė 2011 m. gegužės mėn. paskelbė savo Tarptautinę strategiją

[54] Spiegel staff, GCHQ nusitaikė į netikrus LinkedIn inžinierių puslapius (GHCQ targets engineers with fake linkedin pages), http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821-druck.html 11/11/2013

[55] Yra „trečioji pusė“ arba vyriausybių (ypač autoritarinių) pagunda valdyti skirtingas nuomones ir leisti piliečiams teigiamai žiūrėti į valdančią Vyriausybę (There is also a „third face“ or the temptation governments (especially authoritarian ones) have to use high technology to contol dissent and insure citizens have a favorable view of the government currently in power). The topic of state surveillance vs privacy is beyond the scope of this article..

[56] Healey, J., Lyginant Nacionalines elgesio kibernetinėje erdvėje normas (Comparing Norms for National Conduct in Cyberspace) http://www.atlanticcouncil.org/en/blogs/new-atlanticist/comparing-norms-for-national-conduct-in-cyberspace , 2011 birželio 20 (June 20, 2011)

[57] ICT's: informacinės ir ryšių technologijos (information and communication technologies)

[58] Tarptautinis informacijos saugumo elgesio kodeksas (International Code of Conduct for Information Security), http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t858323.shtml , 2011/09/12

kibernetinėje erdvėje[59]. Joje tarptautinei bendruomenei buvo skelbiamas toks tikslas: „skatinti atvirą, sąveikaujančią, saugią ir patikimą informacinę ir komunikacinę infrastruktūrą, palaikančią tarptautinę prekybą ir komerciją, stiprinančią tarptautinį saugumą ir skatinančią laisvą išraišką ir inovacijas. Norėdami pasiekti šį tikslą, mes sukursime ir palaikysime aplinką, kurioje atsakingo elgesio normos lemia šalių veiksmus, palaiko partnerystę ir remia teisinę valstybę kibernetinėje erdvėje.“[60]

Jungtinė Karalystė taip pat parodė malonią išraišką pasauliui ir pasidalino tuo pačiu susirūpinimu, kaip ir kitos kibernetinės supervalstybės, pvz., ragindama vyriausybes atitinkamai veikti kibernetinėje erdvėje, vadovaujantis nacionaline ir tarptautine teise“[61]. Tai yra kilnūs ir mandagūs žodžiai bei pasiūlymai. Deja, tai tik viena pusė. Kita pusė yra mažiau matoma negu pirmoji, kai veikla nei matoma, nei girdima.

Ši antroji pusė yra susijusi su valstybių kenkėjiška veikla kibernetinėje erdvėje, kai paveikiami kitų valstybių ypatingos svarbos infrastruktūros objektai. Infrastruktūra yra tas ypatingai svarbus turtas, kurį suardžius arba sugadinus, galima paveikti šalies ekonomiką, nacionalinį saugumą ir visuomenės gerovę.

Rusija ir Kinija, išreikšdamos geranoriškumą ir turinčios bendradarbiavimo ketinimų, susijusių su bendromis kylančiomis kibernetinėje erdvėje grėsmėmis, parodė savo antrąją, mažiau pageidautiną pusę. Abiejų šalių vyriausybės buvo susijusios su grupėmis, užsiimančiomis kibernetiniais nusikaltimais ir (arba) kibernetiniu šnipinėjimu. Kinijos karinės pajėgos yra susijusios su kibernetiniais kariniais daliniais, vadinamais PLA daliniu 61398, koks neseniai buvo įvardintas viešame pranešime[62]. Rusijos vyriausybės kibernetiniai daliniai[63] buvo mažiau išviešinti, bet pagal skelbiamą informaciją pasirodė ne mažiau veiksmingai nei kitos kibernetinės jėgos. Kibernetinių atakų kaltininkai, sukėlę dalį Ukrainos elektros tinklo griūties 2015 m. gruodžio 23-iąją, yra numanoma *Sandworm* komanda[64]. Grupė, kuri, manoma, seniai remiama Rusijos[65] vyriausybės[66].

Jungtinės Valstijos taip pat parodė savo kitą pusę. Tuo pačiu metu, kai JAV vyriausybė pasiūlė bendradarbiauti kuriant „aplinką, normuojančią atsakingus elgesio vadovų veiksmus, palaikančius partnerystę, ir remiančius teisėtumą kibernetinėje erdvėje”[67], pasaulis sužinojo apie pirmąją valstybę, sukūrusią kibernetinį ginklą, specialiai nukreiptą prieš kitos šalies ypatingos svarbos infrastruktūros objektus. *Stuxnet* kenkėjiškos programos atradimas 2010 metais ir jos taikymas sukėlė fizinį centrifugų pakenkimą Irano branduolinės energetikos objekte, kurį plačiai aprašė tiek žiniasklaida, tiek ir techniniai specialistai[68]. Daugelis specialistų mano, kad *Stuxnet* plėtra ir taikymas į numatytą taikinį yra glaudžiai susijusi su JAV[69]. Kaip tauta, siejama su lyderyste laisvajame pasaulyje ir skatinanti demokratiją, leidžia stebėtis painiava, sukelta, viena vertus, raginant skatinti atsakingą elgesį internete ir, kita vertus, parodant kitą pusę – visuomenės neapsaugojimą nuo *Stuxnet*. Valstybės sukurtas kibernetinis ginklas kitos valstybės fiziniam taikiniui sunaikinti vis dar nėra tinkamai įvertintas, bet tikrai turės poveikį ateities tarptautiniam saugumui[70]. Kitos kibernetinės supervalstybės veikia panašiu principu. Pavyzdžiui, Australijos signalų direktoratas siekia, kad kiekvienas žinotų, kam jis skirtas. Jų interneto svetainės *motto* yra „Atskleisdami jų paslaptis - apsaugosite savąsias“[71].

PASIŪLYMAI, KAIP VALDYTI MŪSŲ YPATINGOS SVARBOS INFRASTRUKTŪROS OBJEKTŲ KIBERNETINES GRĖSMES

Nėra jokių taisyklių, kaip elgtis kibernetinėje erdvėje, ir jei jos būtų, nėra jokių valdžios atstovų, priverčiančių jas

[59] Baltieji rūmai, Tarptautinė strategija kibernetinei erdvei (The White House, International Strategy for Cyberspace) , http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , 05 2011.

[60] Ibid. Psl 8 (Page 8).

[61] JK Užsienio reikalų sekretoriaus William Hague kalba Miuncheno konferencijoje (U.K. Foreign Secretary William Hague speech to Munich Conference), https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road 2011 vasario 4 (4 February 2011).

[62] Mandiant, APT1 Atskleistas vienas iš Kinijos kibernetinio šnipinėjimo dalinių (Exposing One of China's Cyber Espionage Units) , http://intelreport.mandiant.com/ , 2013.

[63] Sridharan V., Rusija steigia "Cyber Warfare“ karinį dalinį („Russia Setting up Cyber Warfare Unit Under Military“), International Business Times, http://www.ibtimes.co.uk/articles/500220/20130820/russia-cyber-war-hack-moscow-military-snowden.htm , 20 08 2013.

[64] Hultquist, J., Sandworm komanda ir Ukrainos energetikos tarnybų atakos (Sandworm Team and the Ukrainian Power Authority Attacks), http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/

[65] Finkle, J., JAV įmonė kaltina Rusijos "Sandworm" hakerius dėl Ukrainos energijos nutraukimo (U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage) http://mobile.reuters.com/article/idUSKBN0UM00N20160108 , 2016 sausio 7 (Jan 7, 2016)

[66] Zetter, K., Viskas, ką mes žinoti apie Ukrainos elektrinės hakerius (Everything We Know About Ukraines Power Plant Hack) http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ , 01.20.16

[67] Baltieji rūmai, Tarptautinė strategija kibernetinei erdvei (The White House, International Strategy for Cyberspace) , http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf , 05 2011.

[68] For a comprehensive analysis of Stuxnet read R. Langner's article „To kill a centrifuge“, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf November 2013

[69] Sanger, D., Obama Order Sped Up Wave of Cyberattacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 ,JUNE 1, 2012.

[70] For a further discussion of Stuxnet's implications read Butrimas, V., National Security and International Policy Challenges in a Post Stuxnet World Military Academy of Lithuania, 2014., pp. 11-31. http://www.degruyter.com/view/j/lasr.2014.12.issue-1/issue-files/lasr.2014.12.issue-1.xml

[71] Australijos vyriausybė, Gynybos departamentas (Australian Government, Department of Defence), http://www.dsd.gov.au/ 2013. (Website)

vykdyti. Per pastaruosius 25 interneto augimo metus kelionė „informacijos greitkeliu“ tapo pavojinga. Šiandien ji tapo „greitkelio apiplėšimų“ vieta tiems, kurie juo keliauja (dėl nusikaltimų kibernetinėje erdvėje), keliai pilni „kamščių“ dėl atsisakymo aptarnauti (DOS), kelius blokuoja protestuotojai (haktivistai), keliautojai sustabdomi ir apieškomi pareigūnų (vyriausybės duomenų rinkimas ir priežiūra), trikdomi „tankų“ (valdžios), stumiančių kitus vairuotojus nuo kelio (kenkėjiška valstybių kibernetinė veikla). Šis paskutinis aspektas yra susijęs su grėsmėmis aukštosiomis technologijomis pagrįstai infrastruktūrai, remiančiai atskiros šalies ekonomiką, nacionalinį saugumą ir visuomenės gerovę. Šie teikiami siūlymai yra pirmieji valstybių neteisėtų veiklų kibernetinėje erdvėje valdymo žingsniai.

- Šalys susitaria susilaikyti nuo kenkėjiškos kibernetinės veiklos, nukreiptos prieš ypatingos svarbos civilinę infrastruktūrą (finansines sistemas, energetikos, komunalinių paslaugų valdymo sistemas, telekomunikacijų tinklus). Noras apsaugoti šalių nacionalinę ekonomiką ir civilius gyventojus nuo finansinių nuostolių ar fizinės žalos turėtų būti bendras visoms tautoms. Tam tikros valstybės veikla kibernetinėje erdvėje gali būti klaidingai suprantama ir įnešti nestabilumo. Pavyzdžiui, „loginės bombos“ arba „nesąžiningumas“ šalies ypatingos svarbos informacinėje infrastruktūroje gali būti supainioti su „pasirengimo mūšiui“ veikla ir gali sukelti greitą įtampos eskalavimą. Kibernetinė veikla, nukreipta prieš ypatingos svarbos infrastruktūras kitoje valstybėje, taip pat gali turėti reikšmingą tarpvalstybinį ir net regioninį poveikį finansinėms sistemoms, elektros tinklams, vamzdynams ir kitoms šiuolaikinėms, ypatingos svarbos infrastruktūroms.

Tai nėra pirminis pasiūlymas. Tai jau buvo paminėta tiek Rytų, tiek ir Vakarų pasiūlymuose. Buvęs kelių JAV prezidentų patarėjas nacionalinio saugumo klausimais p. Richardas Clarke'as, panaudojo savo patirtį branduolinės ginkluotės kontrolės klausimais kibernetinėje srityje, aptardamas tai neseniai išleistoje knygoje „Kibernetinis karas“ („Cyber War“).[72] Kalba apie kibernetinių ginklų nenaudojimą prieš ypatingos svarbos infrastruktūros objektus taip pat yra įtraukta į Šanchajaus bendradarbiavimo grupės pasiūlymus dėl tarptautinio elgesio kodekso, pasiūlyto Jungtinėms Tautoms 2011 m.[73]

Apribojimai taip pat reikalauja atsakomybės pripažinimo, atsižvelgiant į partnerystės įsipareigojimus. Tai veda prie kito siūlymo.

- Įsipareigojimas prisiimti nacionalinę atsakomybę už kenkėjiškas kibernetines atakas, vykstančias valstybėms pavaldžiose elektroninėse erdvėse ar einančias tranzitu per jas. Tikslas yra šalims susitarti sukurti nacionalinius kibernetinio saugumo pajėgumus (institucijas, įstatymus, procedūras) ir priimti būtiniausius įsipareigojimus, siekiant užtikrinti nacionalinės kibernetinės erdvės saugumą. Dėmesys turėtų būti skiriamas valstybės įsipareigojimams ištirti ir reaguoti į incidentų, atsirandančių arba einančių tranzitu per jų kibernetinę erdvę, kilmę. Pavyzdžiui, šalys turėtų garantuoti, kad nacionaliniai interneto paslaugų teikėjai (IPT) ir teisėsaugos institucijos imtųsi atitinkamų žingsnių prieš asmenis, grupes ir / arba informacijos ir ryšių technologinę įrangą, dalyvaujančią kibernetinėse atakose. Tai taip pat nėra nauja idėja. Autoriai Jungtinėse Amerikos Valstijose jau ironiškai aptarė valstybių nuopelnus, prisiimant atsakomybę už tai, kas vyksta ar tranzitu eina per jų kibernetinį pavaldumą. Tokio politinio mąstymo pavyzdžiai - tai Chriso C. Demchako ir Petero Dombrowskio dokumentai apie kibernetines sienas ir priklausomybes. Jie teigia, kad kibernetinė erdvė nebėra valstybinė erdvė arba prerijos, kur visi gali klajoti ir elgtis kaip tinkami. Priskyrimo problema yra susijusi su atsakomybe ir prievole. Siekiant valdyti šalių netinkamą elgesį kibernetinėje erdvėje, yra svarbu sukurti aukštesnio lygio galimybę ir tikimybę būti sugautiems, negu yra dabar. Kibernetinių sienų nustatymas ir valstybės kontrolė padarys daug, kad būtų sudarytos sudėtingesnės sąlygos įsilaužėliams. Tam iki šiol nesėkmingi bandymai apkaltinti turėtų būti pakeisti galimybe nustatyti tikruosius įsilaužėlius, o ne jų darbo vietas – „kuri valstybė, jei tokia yra, už tai atsakinga"[75]. Pilna atsakomybė, reaguojant ir tiriant ataką, neturėtų būti užkraunama aukai, bet tai turi būti skirta esantiems arčiausiai problemos šaltinio.

- Reikalingas įgyvendinimo ir praktikos stebėjimo mechanizmas, siekiant garantuoti aukščiau minėtų dviejų pasiūlymų veiksmingumą. Norėdamos atlikti šį darbą, valstybės turi sukurti ekspertų ir institucijų koaliciją, norinčią stebėti ir informuoti apie kibernetinės erdvės elgesio taisyklių nustatytus pažeidimus. Pateikta informacija veiks kaip „švelnus spaudimas“ ir sutelks visuomenės dėmesį į dalyvaujančios valstybės nesugebėjimą vykdyti savo tarptautinius įsipareigojimus. Galimą stebėsenos ir ataskaitų teikimo institucijų steigimo modelį galima rasti Konvencijoje dėl cheminio ginklo kūrimo, gamybos, kaupimo ir panaudojimo uždraudimo bei jo sunaikinimo. Per 190 šalių pasirašė ją nuo 1997 m. Tai sudaro 98 proc. pasaulio gyventojų. Tuo

[72] Clarke R., Kibernetiniskaras Kita grėsmė nacionaliniam saugumui ir ką daryti (‚Cyber War: The Next Threat to National Security and What to do About it), Harper Collins, 2010. p. 268-271.

[73] Ministry of Foreign Affairs of the People's Republic of China, Kinija, Rusija ir kitos šalys pateikia tarptautinio elgesio kodekso informacijos saugumo dokumentą Jungtinėms Tautoms) „China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations", Ministry of Foreign Affairs of the People's Republic of China, http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm 13 09 2011.

[74] Demchak C., Dombrowski P., („Rise of a Cybered Westphalian Age"), Strategic Studies Quaraterly Vol. 5. No.1 p. 54-57, http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf 2011.

[75] Healey J., ed., Nuožmusis domenas: Konfliktas elektroninėje erdvėje (A Fierce Domain: Conflict in Cyberspace), 1986 to 2012, Cyber Studies Conflict Association, 2013, p. 265.

Jungtinių Tautų pasirašyta konvencija dėl cheminio ginklo gali būti geru pavyzdžiu, kaip susitarti ir dėl kibernetinių atakų.

pagrindu buvo sukurta Cheminio ginklo uždraudimo organizacija, kurios tikslas yra stebėti ir sekti Konvencijos įgyvendinimą. Konvencija dėl cheminio ginklo gali tarnauti kaip naudingas modelis, svarstant trijų minėtų pasiūlymų įgyvendinimą.

IŠVADA

Daug pastangų įdėjo Lietuva, norėdama tapti energetiškai nepriklausoma valstybe, ką rodo plaukiojanti saugykla su dujinimo įrenginiu (FSRU) I*ndependence*, prišvartuota Klaipėdos uoste[76]. Būtų kvaila galvoti apie tai, kaip apie laivą su suspaustų suskystintų gamtinių dujų konteineriais, kuriam reikia apsaugos ir stebėjimo kamerų, suteikiančių FSRU saugumą. Šiame įrenginyje yra daug sudėtingos technologinės įrangos, pradedant dujų generatoriais, naudojamais tiekti šaldymo sistemoms energiją, reikalingą išlaikyti suslėgtas dujas prie -161^{0} C , baigiant FSRU monitoringo ir kontrolės įranga[77]. Tai gali būti netyčia ar tyčia pažeidžiama, atsiradus kibernetinių gedimų inžinerinėse sistemose, esančiose įrenginyje bei uoste. Kalbant apie Lietuvos ypatingos svarbos infrastruktūros kibernetinio saugumo užtikrinimą, be to, žinant vietinius incidentus, mums taip pat reikia žinoti, kas vyksta likusiame pasaulyje. Vien todėl, kad kibernetinis incidentas vyksta tolimoje šalyje, jokiu būdu nereikėtų galvoti, kad „tai negali atsitikti čia“. Atvirkščiai, mes turėtume manyti, kad privalome ne tik mažinti kibernetinių incidentų pavojų, bet taip pat turėtume įgyvendinti priklausančias veiklas, kaip kibernetinės erdvės kaimynai, skatindami draugišką ir saugią kibernetinės erdvės kaimynystę visiems. Statymai tampa labai dideli. Neseniai buvo pranešta, kaip viena suinteresuotoji užbaigti sunkias derybas su kita valstybe šalis buvo pasirengusi naudoti kibernetiką, kaip galutinę priemonę priversti kitą šalį priimti pozicijas. Buvo sukurtas planas nesėkmės atvejui, jeigu tos derybos nepavyktų. Plane buvo numatyti kibernetiniai išpuoliai prieš kitų valstybių ypatingos svarbos infrastruktūros objektus, tokius kaip oro gynybos bei ryšių sistemos ir elektros tinklai[78]. Šios nekontroliuojamos problemos mastas reikalauja ne techninio, bet saugumo politikos sprendimo. Inžinieriai negali išspręsti šios problemos – kaip fizikai, sukūrę atominę bombą, negalėjo patys išspręsti branduolinių ginklų neplatinimo problemos, taip ir šiandienos kibernetinio saugumo problemos negali išspręsti kibernetinio saugumo specialistai. Saugumo politikos formuotojai turi suvokti ypatingą šiuolaikinio pasaulio priklausomybę nuo pažeidžiamų technologijų ir bendradarbiauti su kitų šalių politikos formuotojais bei pateikti sprendimą, kaip išvengti bendro pavojaus - netinkamo valstybių elgesio kibernetinėje erdvėje. ■

[76] Verslo Korėja, HHI suteikia pavadinimą pirmajam pasaulyje plaukiojančiam dujų saugojimo įrenginiui (Business Korea HHI Holds Naming Ceremony for World's First Floating Storage and Re-gasification Unit), http://www.businesskorea.co.kr/english/news/industry/3394-world%E2%80%99s-first-lng-fsru-hhi-holds-naming-ceremony-world%E2%80%99s-first-floating-storage 2014 vasario 20 (20 February 2014)

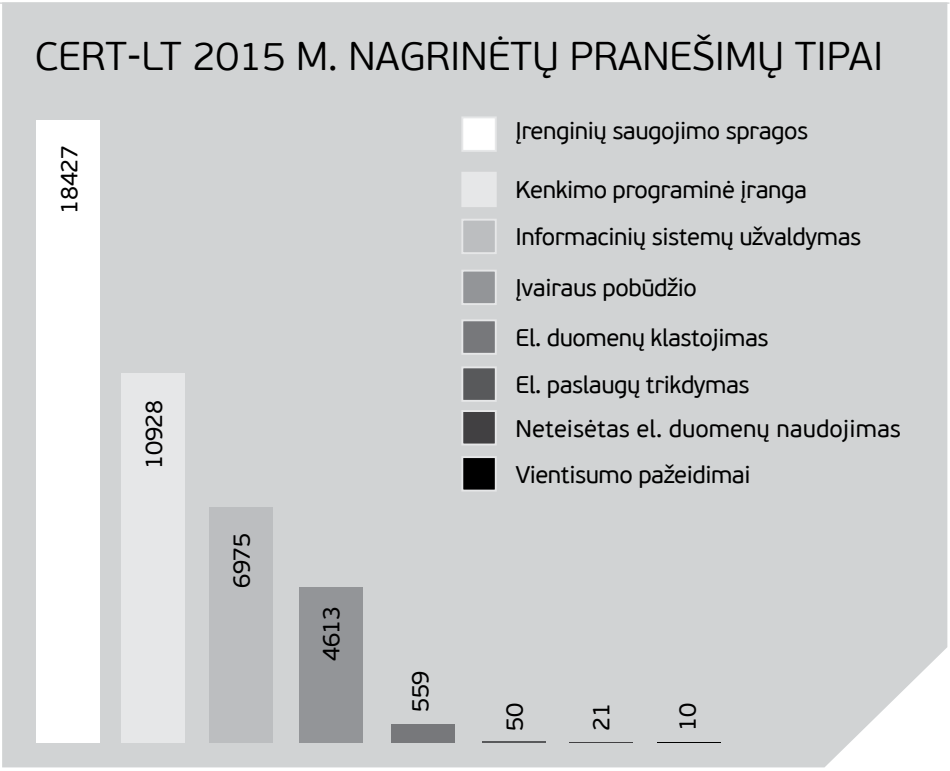
[77] NAUDOJIMOSI SUSKYSTINTŲ GAMTINIŲ DUJŲ TERMINALU TAISYKLĖS, UAB Klaipėdos nafta http://www.sgd.lt/fileadmin/user_upload/SGD/Terminalo_taisykles/Priedas_Nr._3_-_Operatoriaus_technines_salygos.pdf ,

[78] SANGER, D., Mazzetti, M. JAV Turėjo kibernetinio puolimą planą, jei Irano atominis ginčas būtų privedęs prie konflikto (US Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict), http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?_r=0 2016 vasario 16 (February 16, 2016)

KIBERNETINIO SAUGUMO SITUACIJOS LIETUVOJE APŽVALGA IR TENDENCIJOS

Lukas GRINIUS

Elektroninė erdvė įgyja vis didesnę reikšmę – pasaulio gyventojų pasiekiamumas nuolat auga, gerinamas susisiekimas, optimizuojama daugybė procesų. Pagal plačiajuosčio interneto prieigos galimybes, šiuo aspektu Lietuva pirmauja Europoje – 2013 m. interneto prieigos paslaugų, teikiamų plačiajuosčiu ryšiu, skvarba pasiekė 38,5 proc. gyventojų. Atidžiau paanalizavę kitus duomenis, galime pastebėti, kad šioje srityje pirmaujame ne tik Europoje, bet ir visame pasaulyje – ypač pagal naujos kartos tinklų plėtrą ir prieigą.



Elektroninė erdvė Lietuvoje susiduria ir su iššūkiais. Tai tampa ne tik patogia darbo ar laisvalaikio erdve, bet ir galimybe įsibrovėliams pasinaudoti, kaip ideologizavimo, informacijos grobimo, tinklų darbo trikdymo sfera. Kaip pastebima 2014 m. valstybės nacionalinio saugumo vertinimo ataskaitoje, kibernetinio saugumo grėsmės tik augs, ypač iš Lietuvai priešiškų šalių.

„Didžiąją dalį kibernetinių incidentų, nukreiptų prieš Lietuvos valstybės institucijų automatizuoto duomenų apdorojimo (toliau – ADA) sistemas ir tinklus, 2014 metais vykdė užsienio valstybių žvalgybos ir saugumo tarnybos, su tarnybomis susiję ar šių tarnybų kontroliuojami ir remiami kibernetiniai įsibrovėliai.“ (GNSV, 2014)

Pagal D. Shoemakerį ir A. Conkliną, kibernetinis saugumas susijęs su procesų, susijusių su kylančių kibernetinių grėsmių identifikavimu bei sąnaudomis pagrįstų kontrpriemonių taikymu, kūrimu ir palaikymu. Susirūpinimas dėl elektroninės erdvės daugelyje valstybių nuosekliai auga. Tad kyla esminis klausimas, koks esamas saugumo lygis ir su kokiomis grėsmėmis susiduria Lietuvos valstybė bei paprasti piliečiai.

TEISINIS REGLAMENTAVIMAS

Nacionaliniu mastu elektroninę erdvę reglamentuoja Lietuvos Respublikos kibernetinio saugumo įstatymas, Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa, patvirtinta LR Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796, bei kiti įstatymai.

Teisinis reglamentavimas dėl augančių internetinių atakų ženkliai patobulintas. Prieš metus priimtas Kibernetinio saugumo įstatymas kur kas aiškiau apibrėžia institucijas, atsakingas už kibernetinio saugumo politiką. Įstatymu įtvirtintos jų kompetencijos, funkcijos, teisė bei pareigos, nustatytos elektroninių ryšių paslaugų teikėjų pareigos bei atsakomybė, kibernetinio saugumo užtikrinimo sistema. Jame apibrėžiami minimalūs techniniai kibernetinio saugumo reikalavimai. Kaip pabrėžia Krašto apsaugos ministerija, šalyje naujas įstatymas suformavo teisinį pagrindą ir įtvirtino valią bendromis pastangomis ginti Lietuvos kibernetinę erdvę.

Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa siekiama užtikrinti Lietuvos gyventojų ir asmenų, esančių Lietuvoje, saugumą kibernetinėje erdvėje, taip pat pagerinti valstybės elektroninių išteklių saugumą bei veiksmingą funkcionavimą.

Teisinis reglamentavimas stipriai sustiprėjo, įsteigtas Kibernetinio saugumo centras, tačiau visiškai užtikrinti saugumo neįmanoma. „Iš saugos pusės, nėra tokios sąvokos kaip absoliutus saugumas – yra visada rizikos vertinimas ir pagal tą riziką yra kompromisai tarp resursų ir kokybės. Amerikiečiai yra pasakę, kad 5 proc. grėsmių išliks – kaip besistengtum, bet viskas atsiremia į finansus ir darosi ekonomiškai nenaudinga“, – pastebėjo Ryšių ir informacinių sistemų tarnybos direktorius Rimtautas Černiauskas.

Vis dar trūksta viešojo bei privataus

sektoriaus bendradarbiavimo, ne visuomet pakankamas finansavimas. Tad labai svarbu gerinti priemonių paketą, skirtą kibernetiniam saugumui, ir nuolatos atsinaujinti. Elektroninė erdvė yra bene dinamiškiausia bei greičiausiai besikeičianti sritis, todėl būtina nuosekliai tobulinti priemones ir įstatyminę bazę.

KIBERNETINĖS GRĖSMĖS

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (toliau – CERT-LT) 2015-iais ištyrė 41 583 incidentus. Palyginti su 2014-iais (36 136), pranešimų buvo gauta 15 procentų daugiau ir bene dvigubai daugiau nei 2012 metais (21 416).

Kaip pastebima CERT-LT, didelė Lietuvos kibernetinio saugumo problema (18 427 pranešimai per 2015 m.) buvo ir yra įrenginiai, kurie paprastai priklauso fiziniams asmenims ir turi saugumo spragų. Reikėtų pažymėti, kad dažniausiai tokios spragos nekelia tiesioginės grėsmės įrenginių savininkų duomenų saugumui, tačiau sudaro sąlygas piktavaliams naudoti įrenginius paskirstytųjų paslaugos trikdymo (angl. Distributed Denial of Service, DDoS) atakų metu kaip atakų stiprintuvus.

Ekspertai pastebi, kad be kibernetinio saugumo ne ką mažiau svarbi sklandi tinklų veikla. 2013 m. Lietuvos Respublikos ryšių reguliavimo tarnybos (RRT) užsakymu pirmą kartą Lietuvoje atlikta nacionalinio interneto tinklo infrastruktūros saugumo ir veiklos patikimumo galimybių studija atskleidė, kad kritiniai interneto tinklo elementai yra infrastruktūra (*domain name, IP address, IP address ranges, routes and autonomies systems*), kuri yra tiesiogiai susijusi su šių sektorių elektroninėmis sistemomis internete: 1) informacijos ir ryšių technologijos; 2) energetikos; 3) finansų sistemos; 4) viešojo sektoriaus; 5) gėlo vandens ir maisto tiekimo; 6) sveikatos priežiūros; 7) transporto.

Debesų kompiuterija - kita ganėtinai nauja paslauga. Saugomi duomenys ir galima žala ypač domina kibernetinius nusikaltėlius. Vis dažniau atakuojami šios paslaugos tiekėjai. Tokios atakos žala yra ypač didelė – vienam duomenų prieglobos paslaugų tiekėjui padaryta žala kaip domino nusirita per daugelį svetainių.

Bene didžiausia problema, kad debesų kompiuterijos veikla praktiškai nereguliuojama. Tiek Lietuvoje, tiek ES trūksta minimalių informacijos apsaugos reikalavimų ar rekomendacijų šios paslaugos teikėjams. Taip pat trūksta informacijos ir paslaugų vartotojams.

PAVOJAI IŠ RYTŲ

Grėsmių nacionaliniam saugumui vertinimo ataskaitoje pabrėžiama, kad didžiausios grėsmės Lietuvai atkeliauja iš rytų kaimynės. „Rusijos žvalgybos ir saugumo tarnybos, ypač FSB bei Gynybos ministerijos struktūriniai padaliniai ir su šiais padaliniais susiję subjektai („hacktivistai“, kriminalinio pasaulio atstovai, patriotiniai įsilaužėliai ir pan.) turi didžiausius kibernetinius pajėgumus, nukreiptus rinkti informaciją, trikdyti Lietuvos ADA sistemų ir tinklų funkcionavimą, juos užvaldyti, tikrinti Lietuvos atsakingų institucijų gebėjimą gintis.“

Elektroninė erdvė Rusijai tampa ypač svarbi, plečiant šnipinėjimo tinklą bei pasisavinant slaptą informaciją. Kaip pabrėžiama ataskaitoje, Rusija, naudodama kibernetinius pajėgumus, užvaldydama ir eksploatuodama kompiuterius, kompiuterinę įrangą, telekomunikacijų įrenginius, ADA tinklus ir sistemas, mobiliuosius įrenginius ir kitą informacinių technologijų įrangą, siekia įgyti pranašumą gynybos, politikos, ekonomikos, technologijų ir kitose srityse.

Rusijos subjektų, veikiančių kibernetinėje erdvėje, taikiniai be gynybos sistemų gali būti:

- vyriausybės įstaigos, ypač užsienio reikalų, ūkio, energetikos ministerijos;
- telekomunikacijų sistemos, pramonės ir kritinės infrastruktūros objektai, kurių veiklos sutrikdymas turėtų kritinę reikšmę;
- žiniasklaida. (GNSV, 2014)

Kibernetinis šnipinėjimas - kita rytų kaimynų dažnai naudota priemonė, siekiant apkrėsti kompiuterius, sistemas ir tinklus įvairiomis šnipinėjimui skirtomis programomis. Kaip teigiama grėsmių nacionalinio saugumo vertinimo ataskaitoje, tokių programų veikla arba jų pėdsakų buvo aptikta daugelio Lietuvos valstybės institucijų ADA sistemose, tinkluose, naudotojų įrenginiuose. Nusikaltėliai aktyviai veikė ne tik Lietuvos kibernetinėje erdvėje, tačiau ir visoje Europoje.

Ypač dažnai kenkėjiškos programos pasklinda per USB laikmenas. Vykusiame G20 lyderių susitikime, kaip įtariama, Rusija išdalino kenkėjiškomis

Dailytech.com nuotr.

programomis infekuotas USB laikmenas. Pasak specialistų, tokiomis „dovanomis“ apsikeisti įprasta ir tai yra dažna specialiųjų tarnybų taktika, šnipinėjant aukštus valstybių atstovus.

KIBERNETINIO SAUGUMO TENDENCIJOS

Nusikaltimų skaičius elektroninėje erdvėje Lietuvoje auga. 2015 metais CERT-LT užfiksavo kur kas daugiau pažeidimų nei praėjusiais metais – lyginant su 2012 metais, bene dvigubai.

Daugiausia spragų egzistuoja įrenginių saugumo srityje. Taip pat buvo užfiksuota daug kibernetinių incidentų, susijusių su kenkimo programine įranga. Pastaruoju metu yra pastebimas šių incidentų skaičiaus mažėjimas dėl taikomų prevencinių priemonių, tačiau bendras nusikaltimų skaičius vis tiek išlieka gana aukštas.

Pastaruoju metu Lietuvoje kreipiama daug dėmesio nusikaltimų elektroninėje erdvėje prevencijai. Pagrindiniai sprendimai, susiję su kibernetinio saugumo stiprinimu, yra Nacionalinė programa kibernetinio saugumo plėtrai 2011–2019 m. bei nuo 2015 metų sausio 1 dienos įsigaliojęs Kibernetinio saugumo įstatymas. Tiesa, nusikaltimų skaičius vis dar didėja.

Nors ateityje kibernetinių nusikaltimų atvejų gausės, pozityviai nuteikia, kad skiriamas dėmesys kibernetiniui saugumui Lietuvoje auga, įsipareigota skirti didesnį finansavimą. Ypač trūksta Lietuvos mokslininkų ir akademinės bendruomenės indėlio. Kibernetinių incidentų mastas ir, ypač, auganti jų įtaka tinklams bei IS turi būti vertinama kaip rimta ir nuolatinė grėsmė. Tai reikalauja nuolatinio sisteminio valstybės indėlio. ■

Remtasi Lietuvos Respublikos nacionaliniu elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio, Ryšių reguliavimo tarnybos, Grėsmių nacionaliniam saugumui vertinimo (2014 m.), Krašto apsaugos ministerijos bei kita medžiaga.

KIBERNETINIO SAUGUMO APLINKA LIETUVOJE

VALSTYBINIO AUDITO ATASKAITOS APŽVALGA

Romena ČIŪTIENĖ

www.flickr.com, Blue Coat nuotrauka

2015 metų gruodį Valstybinis auditas paskelbė ataskaitą apie Kibernetinio saugumo aplinką Lietuvoje. Skamba pakankamai paradoksaliai, bet tik 2015-aisiais metais valstybė iš esmės (pakankamai plačiai ir giliai) apžvelgė šalies kibernetinę aplinką. Tai iškalbingas faktas. Visgi straipsnio tikslas ne dramatizuoti, o trumpai apžvelgti 34 puslapių apimties atsakaitą, kuri, tiesą sakant, pati iš savęs yra pakankamai dramatiška. Bet apie viską – iš eilės.

APIE TYRIMĄ

Pasak ataskaitos, dar 2006 m. Lietuvos Respublikos Vyriausybė nustatė, kad galiojantis elektroninės informacijos saugos (kibernetinio saugumo) srities reglamentavimas nepakankamas, todėl nutarė parengti elektroninių ryšių tinklų ir informacijos saugumo įstatymą, o 2011 m. patvirtinto elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą. Tačiau programa realių rezultatų nedavė, o minėtas įstatymas taip ir nebuvo priimtas. Taigi, kibernetinio saugumo sritis iki 2015 m. rėmėsi teisės aktais, kuriuose nebuvo aiškiai nustatytų šios srities politiką formuojančių ir įgyvendinančių institucijų, kibernetinio saugumo dalyvių pareigų, atsakomybės, organizacinių ir techninių kibernetinio saugumo reikalavimų ir kibernetinio saugumo užtikrinimo priemonių.

Tiktai 2014 m. Lietuvoje pradedama kurti nuosekli kibernetinio saugumo sistema. Ir tai – tik *de jure*. 2014 metų pabaigoje priimtas Kibernetinio saugumo įstatymas, nustatantis kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžiantis kibernetinio saugumo ir kitas pagrindines šios srities sąvokas. Nuo 2015 metų, kuomet įsigaliojo įstatymas, Krašto apsaugos ministerijai suteikti įgaliojimai formuoti kibernetinio saugumo politiką, organizuoti, kontroliuoti ir koordinuoti jos įgyvendinimą. Įsteigtas Nacionalinis kibernetinio saugumo centras, sudaryta Kibernetinio saugumo taryba. Vidaus

reikalų ministerijai, kuri neteko formuotojos vaidmens, skirtos remiančios institucijos pareigos.

Lietuvos Respublikos Vyriausybės pavedimas atlikti Kibernetinio saugumo aplinkos Lietuvoje auditą duotas dar 2014 metų gale. Suburta auditorių grupė metus laiko analizavo 2011–2015 metų laikotarpį. Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas Lietuvoje. Tikslui pasiekti iškelti šie uždaviniai:

- įvertinti, ar sukurta kibernetinio saugumo sistema;
- įvertinti, ar užtikrinamas kibernetinis saugumas valstybinėse įmonėse.

Audito metu išanalizuotas esamas kibernetinio saugumo ir el. informacijos saugos teisinis reguliavimas, strateginis planavimas, valdymo praktika, šiai sričiai skirtos ir skiriamos bei naudojamos lėšos. Vertinta, ar pasiekti planavimo dokumentuose nustatyti kibernetinio saugumo ir el. informacijos saugos rezultatai ir kaip valstybės įstaigos užtikrina kibernetinį saugumą ar tinkamai taiko kibernetinio saugumo technines ir organizacines priemones. Auditas atliktas Vidaus reikalų ministerijoje ir Krašto apsaugos ministerijoje. Duomenys ir informacija surinkti iš šių ministerijų valdymo srities įstaigų, kitų ministerijų, Vyriausybės kanceliarijos, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Valstybės saugumo departamento, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) tarybos atstovų ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos. Audituojant bendradarbiauta ir su asociacijos „INFOBALT“ kibernetinio saugumo specialistais.

Siekiant gilesnės ir esminės analizės, auditoriai teigia analizavę užsienio šalių patirtį, gerąją praktiką, mokslinių tyrimų duomenis ir visuomenės informavimo priemonėse skelbiamą informaciją, susijusią su audituojama sritimi. Analizuojant pačią ataskaitą, iš tiesų susidaro įspūdis, jog į kibernetinį saugumą buvo bandyta pažvelgti plačiau, nei vien tik apibrėžta

Audito metu pastebėta, kad iki šiol valstybėje nepakankamai efektyviai sprendžiami kibernetinio saugumo ir jo atsparumo didinimo klausimai.

Kibernetinio saugumo įstatyme. Visgi bendram Lietuvos kibernetinio saugumo paveikslui susidaryti, jaučiamas didžiulis operatyvinių tarnybų įdirbio analizės trūkumas. Tikėkimės, kad egzistuoja ir klasifikuota apžvalginė medžiaga apie kibernetinį saugumą Lietuvoje ir su ja politikos formuotojai susipažinę, tačiau viešai apie tokį dokumentą jokios informacijos nesama.

AUDITO IŠVADOS

Audito metu pastebėta, kad iki šiol valstybėje nepakankamai efektyviai sprendžiami kibernetinio saugumo ir jo atsparumo didinimo klausimai. Akcentuojant tik reagavimą į incidentus ir jų užkardymą kibernetinėje erdvėje, pamirštami tradiciniai el. informacijos saugos valdymo klausimai (informacijos konfidencialumas, vientisumas, prieinamumas) ir nuo 2015 m. neskiriama pakankamai dėmesio šios srities plėtrai, teisės aktų rengimui, organizacinės struktūros tobulinimui ir panašiems aspektams.

Nustatyta, kad viešajame sektoriuje įgyvendinamos nepakankamos šios srities organizacinės ir techninės priemonės. Valstybinės įstaigos savo veikloje nepakankamai dėmesio skiria kibernetiniam saugumui užtikrinti, o naujai priimtas Kibernetinio saugumo įstatymas neišsprendžia visų su kibernetiniu saugumu susijusių grėsmių. Pasak Valstybės kontrolės, šis įstatymas gali būti veiksmingas tiek, kiek bus veiksmingi jį lydintieji teisės aktai, įstaigų praktinė patirtis ir gebėjimai valdyti kibernetinį saugumą ir el. informacijos saugą. Taip pat būtina parinkti efektyvias reikalavimų įgyvendinimo kontrolės priemones bei spręsti šios srities specialistų kompetencijos problemas. Nepašalinus šių trūkumų, gali nukentėti ne tik administracinės ir viešosios paslaugos, informacija, bet ir kiekvienas pilietis, šalies prestižas, pasitikėjimas naujomis technologijomis.

Siekiant tobulinti kibernetinio saugumo reglamentavimo kokybę, spręsti esamas planavimo ir finansavimo problemas, auditoriai pasiūlė Vyriausybei nustatyti bendras kibernetinio saugumo, el. informacijos saugos strateginės kryptis ir joms pasiekti būtinas priemones, konsoliduoti el. informacijos saugos valdymą. Taip pat rekomenduota skirti įstaigą, kuri koordinuotų šios srities reikalavimų rengimą, jų suvienijimą, ir nustatyti lėšų skyrimo, panaudojimo prioritetus ir kriterijus. Krašto apsaugos ir Vidaus reikalų ministerijoms rekomenduota peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti, patvirtinti šios srities trūkstamas nuostatas, metodinius dokumentus ir numatyti priemones, skirtas konsultuoti ir informuoti kibernetinį saugumą, el. informacijos saugą užtikrinančius subjektus aktualiais šios srities klausimais.

Auditas taip pat nustatė, jog kibernetinio saugumo ir el. informacijos saugos sritys Lietuvoje atskirtos įstatymų lygiu, tačiau juos įgyvendinti nėra lengva, o bendra valstybės saugumo būklė šiose srityse kol kas negerėja, nes:

- El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, kurioje planuota pasiekti daugiausia rezultatų šioje srityje, vykdoma nerezultatyviai. Nustatyti ne visi su kibernetinio saugumo ir el. informacijos sauga susijusių planavimo dokumentų tarpusavio ryšiai, vėluojama įgyvendinti planavimo dokumentuose numatytas priemones.
- Laiku neparengti teisės aktai, reglamentuojantys kibernetinį saugumą, nėra sprendimo dėl el. informacijos saugos, kibernetinio saugumo ir kitų su informacijos sauga susijusių sričių


www.flicr.com, Blogtrepreneur nuotrauka

reikalavimų peržiūrėjimo ir suderinimo.

- 2015 m. pradėjusi veikti kibernetinio saugumo valdymo sistema nesudaro visų su el. informacijos sauga susijusių sričių darnaus valdymo sąlygų: neišvengiama dalinio įstaigų veiklos dubliavimo, trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką.
- Kibernetiniam saugumui ir el. informacijos saugai reikalingų lėšų skyrimas ir panaudojimas (2015–2020 m. laikotarpiui yra suplanuota 15,6 mln. EUR) vykdomas nenustačius lėšų skyrimo prioritetų ir kriterijų, neturint duomenų apie faktinę įstaigų kibernetinio saugumo ir el. informacijos saugos būklę, panaudotas lėšas ir jų poveikį.

Įvertinta, jog kibernetinio saugumo ir el. informacijos saugos techninių ir organizacinių priemonių įgyvendinimas viešajame sektoriuje nepakankamas, netinkamai pasiruošta reaguoti į kibernetinėje erdvėje kylančias grėsmes, kadangi:

- Vidutiniškai taikoma 25 proc. šiai sričiai užtikrinti rekomenduojamų organizacinių priemonių. Pagrindiniai trūkumai susiję su saugumo valdymo sistemos kūrimu, incidentų valdymu, veiklos tęstinumo užtikrinimu, personalo kompetencijos tobulinimu ir išoriniu bendradarbiavimu.
- Tinkamai įgyvendinta tik 39 proc. rekomenduojamų techninių priemonių, kurios lieka pažeidžiamos dėl iš esmės netinkamo jų valdymo.

AUDITORIŲ REKOMENDACIJOS

Valstybės audito pateiktose rekomendacijose Lietuvos Respublikos Vyriausybei, siekiant užtikrinti kibernetinį saugumą ir jo atsparumo didinimą, siūloma:

- nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones;
- skirti įstaigą, kuri valstybės mastu koordinuotų kibernetinio saugumo, el. informacijos saugos reikalavimų rengimą, jų suvienijimą;
- konsoliduoti el. informacijos saugos valdymą;
- valstybės mastu nustatyti kibernetiniam saugumui, el. informacijos saugai reikalingų lėšų skyrimo ir panaudojimo prioritetus, kriterijus, stebėsenos ir kontrolės mechanizmą.

Lietuvos Respublikos krašto apsaugos ir vidaus reikalų ministerijoms, siekiant gerinti kibernetinio saugumo reglamentavimo kokybę ir efektyvumą, Valstybės auditas rekomendavo:

- peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti ir (arba) patvirtinti trūkstamas nuostatas ir metodinius dokumentus;
- užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo ir el. informacijos saugos (valdymo sistemos kūrimas, incidentų valdymas, veiklos tęstinumo užtikrinimas, personalo kompetencijos tobulinimas, išorinis bendradarbiavimas, saugios konfigūracijos nustatymas, tinklo saugumas, mobilių ir kitų technologijų valdymas) klausimais.

PABAIGAI, ARBA EPILOGAS

Taip, epilogas. Šis terminas vartojamas baigiant dramas ir šiame kontekste jis tikrai tinka. Lietuva jau eilę metų yra tarp pirmaujančių pasaulyje pagal interneto spartą ir plėtrą, ji taip pat kotiruojasi tarp imliausiųjų IT sektoriuje, o štai valstybiniame sektoriuje... viduramžiai? Koncentruota ir visa vertinanti šalies kibernetinio saugumo apžvalga atlikta tik 2015 viešpaties metais, praėjus daugiau nei pusei amžiaus (!) po interneto atsiradimo. Jos rezultatai – liūdni, nėra koordinavimo, nėra poįstatyminių aktų bazės, priemonės įgyvendinamos ne daugiau kaip 50 procentų to, kas buvo užsibrėžta. O ir užsibrėžta buvo, švelniai tariant, tikrai ne ambicingai.

Lietuvos ekonomikos vis didesnę dalį sudarant paslaugų sektoriui, kuris tiesiog šuoliuoja į kibernetinę erdvę, tokia šalies kibernetinio saugumo būklė yra ištis apverktina. Juolab kad aplinka veikti ištis dėkinga ir tą rodo pasauliniai reitingai. Ši ataskaita garsiai pasako, kad karalius nuogas – daug kartų valdžios naudotas argumentas apie plačiai išvystytą IT sektorių, deja, tėra privataus sektoriaus nuopelnas.

Baigiant telieka pasidžiaugti, kad sisteminio valdžios požiūrio į kibernetinį saugumą indikacijų esama. Įsteigtos insitucijos, pasidalinta atsakomybės sferomis, sukurti pagrindiniai teisės aktai. Belieka veikti. Veikti proveržio rėžimu, pamirštant trepsenimus ir blaškymusis. Veikti teikiant valstybinį prioritetą, paprastinant biurokratines procedūras, metant didžiulius resursus, įsigijant naujausią organizacinę techniką, priviliojant kompetetingą personalą, glaudžiai ir imliai bendradarbiaujant su privačiu sektoriumi, kuris mūsų valstybei šioje sferoje yra didysis brolis, pripažinkime. Tam reikalinga stipri politinė valia. Tikėkimės, artimos ateities vyriausybė jos nestokos. ■

KOVŲ ARENA – KIBERNETINĖ ERDVĖ

Aleksandras GRAŽELIS

Tik apie 1990 metus susijungė iki tol buvę lokalūs JAV ir kelių Europos valstybių interneto tinklai ir imta naudoti dabar visų puikiai pažįstamas interneto naršykles.

KIBERNETINIS SAUGUMAS – NACIONALINIO SAUGUMO DALIS

Kibernetine erdve vadiname aplinką, kurioje valstybinių institucijų, privačių įmonių bei vartotojų kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje elektroninė informacija yra sukuriama ir (arba) perduodama elektroninių ryšių tinklu. Kiekvienas asmuo, turintis kompiuterį ar mobilųjį telefoną, veikia šioje erdvėje, bendraudamas su kitais asmenimis, gaudamas įvairią informaciją, tvarkydamas buitinius ir finansinius reikalus ne tik savo šalyje, bet ir visame pasaulyje. Pasaulinis telefoninis ryšys atsirado apie 1930 metus, o interneto pasaulinio tinklo (*World Wide Web*) istorija dar visiškai „jauna“. Tik apie 1990 metus susijungė iki tol buvę lokalūs JAV ir kelių Europos valstybių interneto tinklai ir imta naudoti dabar visų puikiai pažįstamas interneto naršykles. Nuo 1994 metų Lietuvoje internetu galėjo naudotis mokslininkai, nuo 1995-ųjų šis tinklas tapo komercinis ir jo paslaugas galėjo įsigyti vartotojai. Interneto pasaulinis tinklas tapo erdve, kurioje savo interesus ėmė įgyvendinti visi: gerieji žmonės – bendrauti ir šviestis, verslininkai – reklamuoti ir parduoti savo prekes, blogieji žmonės – skleisti iškrypėliškus pomėgius, nusikaltėliai – vogti ir plėšti nesaugiuosius, kariškiai – ginti savo šalį (didelių valstybių – ir pulti).

Kenkėjai internetą užpuolė labai anksti, dar tada, kai jis veikė vien JAV teritorijoje, – 1988 metų lapkričio 1 dieną užkrato programa „Interneto kirminas“ (*Internet Worm*) sugadino 6 000 iš 60 000 tuometinių interneto centrų. Didėjant interneto vartotojų skaičiui bei plečiantis juo teikiamų paslaugų apimčiai, didėjo ir kibernetinių nusikaltimų skaičius. 2014 metais užregistruota 42,8 mln. kibernetinio saugumo pažeidimų, tai 48 procentais daugiau nei 2013 metais. 2015 metų statistika bus dar blogesnė – antivirusinė laboratorija „Panda Labs“ skelbia, kad ji 2015 metais aptiko ir nukenksmino 84 milijonus kenkėjiškų programų, 9 milijonais daugiau nei 2014 metais. Kiekvieną 2015 metų dieną atsirasdavo net 230000 kenkėjiškų programų, žymiai padidėjo kibernetinių atakų galia, iš bankų pavogta apie 1 mlrd. USD. JAV yra labiausiai kibernetinių nusikaltėlių atakuojama valstybė, pernai iš valstybės duomenų registrų buvo pavogta 20 milijonų valstybės tarnautojų asmeniniai duomenys, pažeisti sveikatos apsaugos, prekybos tinklai, taip pat filmų gamybos kompanija „Sony Pictures“.

Saugumas kibernetinėje erdvėje tapo kiekvienos valstybės nacionalinio saugumo dalimi. Kibernetiniam saugumui užtikrinti valstybės sukūrė struktūras, rengiančias strategijas, planus, standartus. Planų įgyvendinimui sukurtos kibernetinio saugumo tarnybos, stebinčios ir registruojančios incidentus kibernetinėje erdvėje, rengiančios pasiūlymus jų prevencijai. Parengtos ir veikia policijos ir kitos visuomenės saugos struktūros, persekiojančios ir užkardančios nusikaltimus kibernetinėje erdvėje. Valstybių teisėsaugos institucijos priėmė didžiulius kiekius įstatymų ir kitų teisės aktų, numatančių už tokio pobūdžio nusikaltimus griežtą baudžiamąją atsakomybę. Didesnis dėmesys skiriamas ir vartotojams – jie mokomi būti labiau atsakingi, geriau išmanyti apie elektroninių būdu teikiamas paslaugas, žinoti apie pavojus ir galimybes jų išvengti, apie kasdien tobulesnius nusikaltėlių būdus.

GYNYBOS LYGIAI IR JŲ STRUKTŪRA

Pirmosios kibernetinio saugumo struktūros buvo sukurtos JAV, nes šioje šalyje sparčiausiai plėtojosi elektroninės technologijos, joje buvo registruoti ir pirmieji nusikaltimai kibernetinėje erdvėje. Šios struktūros nuolat tobulinamos, o kitos valstybės JAV patirtį stebi, naudoja savos kibernetinės erdvės saugai

bei jungiasi į kolektyvinės gynybos sistemas. Pateiksime trumpą JAV, valstybės-lyderės kibernetinio saugumo veikloje, struktūrų ir veiksmų apžvalgą. Daugelio JAV struktūrų lietuviški pavadinimai gali būti išversti netiksliai, todėl šalia pateikiame jų originalų pavadinimą.

Su nusikaltimais kibernetinėje erdvėje JAV kovojama, visų pirma, teisinėmis priemonėmis, kaip ir su kitokio pobūdžio nusikaltimais. Jau nuo 1986 metų pradėta taikyti baudžiamoji atsakomybė už šiuos nusikaltimus pagal Kompiuterinių sukčiavimų ir piktnaudžiavimų įstatymą (*Computer Fraud and Abuse Act*). Vėliau buvo priimti reikalingi įstatymai dėl infrastruktūros kibernetinio saugumo, kibernetinės erdvės apsaugos ir kiti teisės aktai.

Jungtinės Amerikos Valstijos buvo pirmoji valstybė, ėmusi vertinti kibernetinį saugumą kaip nacionalinio saugumo sudėtinę dalį. Priežastys svarbios, pirma – informacinės technologijos ir elektroninė komercija tapo esmine ekonomikos, ypač finansų sektoriaus, dalimi. Antra – kibernetinis saugumas yra gyvybiškai svarbus energetikos (branduolinių jėgainių, dujų, elektros) infrastruktūroje bei transporto (metro, geležinkelių, oro) sistemose. 2003 metais JAV buvo paskelbta Nacionalinė kibernetinės erdvės saugumo strategija (*National Strategy to Secure Cyberspace*). Šis dokumentas buvo dalimi išsamesnio dokumento – Nacionalinės vidaus saugumo strategijos (*National Strategy for Homeland Security*), sukurtos atsakant į 2001 metų rugsėjo 11 d. teroristines atakas JAV teritorijoje. 2015 metais JAV priimtas Pasidalijimo kibernetinio saugumo informacija įstatymas (*Cybersecurity Information Sharing Act*).

Šioje kovoje sustoti negalima. 2016 m. vasario 9 d. JAV prezidentas Barackas Obama, pripažindamas 2015 metais įvykdytas kibernetines atakas prieš JAV valstybines institucijas ir verslo struktūras labai pavojingomis JAV nacionaliniam ir ekonomikos saugumui, paskelbė naują nacionalinį kibernetinio saugumo veiksmų planą. Plane numatyta įsteigti aukšto rango komisiją kibernetiniam saugumui stiprinti. Ji pateiks rekomendacijas dėl veiksmų, kurių reikia imtis per ateinantį dešimtmetį, stiprinant ekonominį ir nacionalinį saugumą bei naudojant naujausias kibernetinio saugumo technologijas. Šio plano vykdymui 2017 metų valstybės biudžete ketinama prašyti 19 milijardų USD.

Strategiją ir įstatymus įgyvendina JAV valstybės saugumo departamentas (*US Department of Homeland Security*), kuriame veikia Nacionalinės gynybos ir programų direktoratas (*National Protection & Programs Directorate*) ir Kibernetinio saugumo ir komunikacijų valdyba (*Office of Cybercecurity & Communications). Jai p*avaldus Nacionalinis kibernetinio saugumo skyrius (*National Cyber Security Division*), atsakingas už reagavimo į kibernetinius incidentus sistemą, kibernetinių rizikų valdymo programą ir JAV kibernetinio saugumo poreikius. Šiam skyriui pavaldūs keli padaliniai, iš kurių svarbiausiais galima laikyti Nacionalinį kibernetinio saugumo ir ryšių integracijos centrą (*National Cybersecurity and Communications Integration Center*), Nacionalinę kibernetinio perspėjimo sistemą (*National Cyber Alert System*) bei Kompiuterinių incidentų tyrimo komandą (*Computer Emergency Readiness Team,* sutr. US-CERT). US-CERT yra atsakingas už kompiuterių tinklų infrastruktūros apsaugą, kibernetinių incidentų šalinimo koordinavimą ir jų tyrimą bei analizę, nuolat teikia perspėjimo pranešimus apie pastebėtas ir galimas saugumo grėsmes ir spragas visų lygių tinklų vartotojams. US-CERT padalinys veikia visą parą ištisus metus, naudoja *Einstein 1, Einstein 2* ir *Einstein 3* ir *3A* sistemas, sugebančias aptikti įsibrovimą į kompiuterių tinklus realiu laiku, analizuoja informacijos srautų turinį, ieško duomenyse kenksmingų kodų.

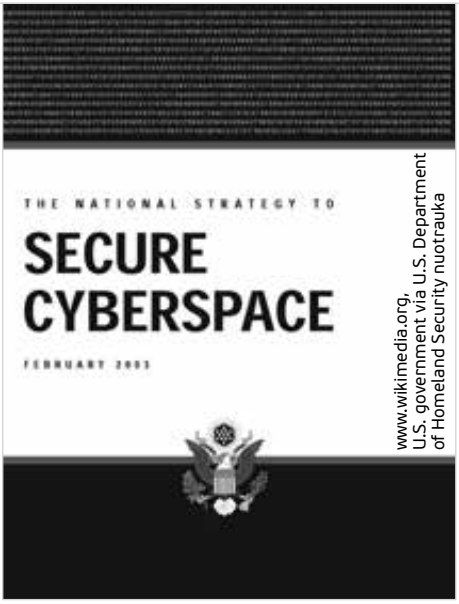
Kita JAV kibernetiniu saugumu besirūpinanti agentūra yra Federalinis tyrimų biuras (*Federal Bureau of Investigation,* sutr. FBI), veikiantis JAV Teisingumo departamento jurisdikcijoje. Vienas iš šio biuro veiklos prioritetų apibūdinamas taip: „ginti JAV nuo kibernetinių atakų ir nusikaltimų, susijusių su aukštosiomis technologijomis“. Biuras šią veiklą vykdo kartu su Nacionaliniu baltų apykaklių nusikaltimų centru (*National White Collar Crime Center*), kuris teisėsaugos organus apmoko kovoti su naujoviškais ekonominiais nusikaltimais kibernetinėje erdvėje. FBI taip pat bendradarbiauja su Skundų apie nusikaltimus internete centru (*Internet Crime Complaint Center*), teisėsaugos institucijoms teikiančiu nukentėjusių asmenų pranešimus, kuriais remiantis nusikaltėliams keliamos baudžiamosios ar civilinės atsakomybės bylos.

1988 metų lapkričio 1 dieną užkrato programa „Interneto kirminas“ *(Internet Worm)* sugadino 6 000 iš 60 000 tuometinių interneto centrų.

JAV Teisingumo departamente taip pat veikia ir Kompiuterinių nusikaltimų ir intelektualinės nuosavybės skyrius (*Computer Crime and Intellectual Property Section*), jis tiria kompiuterinius nusikaltimus (įsilaužimus, užkrėtimą virusais, „kirminais“), taip pat nusikaltimus intelektinės nuosavybės atžvilgiu, vykdo kratas bei skaitmeninių įrodymų poėmius iš kompiuterių ir tinklų.

JAV kibernetinė komanda (T*he United States Cyber Command*, sutr. USCYBERCOM) yra JAV gynybos departamento padalinys, centralizuotai vadovaujantis operacijoms kibernetinėje erdvėje ir sinchronizuojantis JAV karinių tinklų apsaugą. Civilinių tinklų šis padalinys nesaugo.

Aukščiau minėta Kompiuterinių incidentų tyrimo komanda US-CERT glaudžiai bendradarbiauja su kitų pasaulio šalių padaliniais, tiriančiais incidentus kibernetinėje erdvėje bei turinčiais savo pavadinimuose jau bendriniu tapusį žodį CERT (arba CIRT, CSIRT). 1990 metais buvo įkurtas Incidentų tyrimo ir saugumo komandų forumas (*Forum of Incident Response and Security Teams*, sutr. FIRST). Jo nariai yra 342 CERT komandos 74 valstybėse, atstovaujančios valstybinėms, akademinėms ir privačių kompanijų, tokių kaip *Adobe, AT&T, Apple, Cisco, McAfee, Microsoft, Oracle, Siemens, Symantec* ir daugybės kitų, CERT komandoms. Forumo dalyviai keičiasi informacija apie kibernetines atakas, saugumo sistemų spragas ir kitais pasauliniam interneto tinklui svarbiais klausimais. Šiame forume Lietuvą atstovauja penkios CERT komandos, trys – privačių kompanijų, dvi – valstybinių institucijų – Krašto apsaugos ministerijos Nacionalinio kibernetinio saugumo centro CERT bei Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinių elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT, kurio interneto svetainėje www.cert.lt kiekvienas vartotojas gali patikrinti savo kompiuterio „sveikatą“, pranešti apie „programišių“ atakas, rasti patarimų saugiam darbui kompiuteriu.



2003 metais JAV buvo paskelbta Nacionalinė kibernetinės erdvės saugumo strategija *(National Strategy to Secure Cyberspace).*

Pasaulinio interneto saugai 2004 metais buvo įkurta dar viena tarptautinė organizacija - Pranešimų ir kovos su kenkėjais darbo grupė (*Messaging, Malware and Mobile Anti-Abuse Working Group*), jungianti visame pasaulyje per 200 garsių kompanijų, veikiančių informacinių technologijų sektoriuje. Jos veikla nukreipta prieš kompiuterių „zombinimą“, elektroninį šlamštą, kenkėjiškas programas, virusų atakas. Veiklos principai – nuolatos keistis informacija apie interneto kenkėjus, mokyti ir šviesti interneto bendruomenę.

JAV kibernetinio saugumo struktūros glaudžiai bendradarbiauja su Europos Sąjungos kibernetinės saugos struktūromis - Europos Sąjungos tinklų ir informacijos apsaugos agentūra (*European Union Network and Information Security Agency,* sutr. ENISA) bei Transeuropinio mokslinių tyrimų ir švietimo tinklų asociacija (*Trans-European Research and Education Networking Association,* sutr. TERENA).

KAIP SAUGOME LIETUVOS KIBERNETINĘ ERDVĘ?

Ši trumpa apžvalga, kaip JAV rūpinasi valstybės kibernetiniu saugumu, nuteikia klausimui – ar tinkamai juo rūpinamasi mūsų valstybėje? Tai, kas aprašyta aukščiau, veikė JAV jau daugelį metų, ir jų patyrimu galima buvo naudotis. Reikia pripažinti, kad poslinkių labiau rūpintis Lietuvos kibernetiniu saugumu atsirado tik paskutiniaisiais metais. Iki tol gana ilgai buvo ramiai miegota – elektroninių paslaugų buvo mažai, įvairūs duomenų registrai – popieriuje. 2006 metais socdemų vyriausybė patvirtino elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepciją, tačiau parengti įstatymo neskubėjo ir nesugebėjo. Neskubėjo, nors 2007 metų balandį Estijos valstybė nukentėjo nuo pasaulinio masto kibernetinės atakos. Daugiau nei dvi savaites buvo atakuojami Estijos vyriausybės, parlamento, prezidento ir dviejų didžiausių šalies laikraščių – „Postimees“ ir „Eesti Paevaleht“ - tinklalapiai. Taip pat buvo atakuojami IT kompanijų ir komercinių bankų tinklalapiai, laikinai nutrauktas elektroninės bankininkystės ir interneto paslaugų teikimas. Ekspertai nustatė, kad kibernetinėje atakoje dalyvavo apie 1 mln. kompiuterių, buvo įtariama, kad ataką organizavo Rusija, tačiau tikslesnių įrodymų pritrūko, nes Rusijos kibernetinių karų specialistai sugeba slapstytis. Lietuva tokio masto atakų nepatyrė, nors įsilaužimai į kelias internetines svetaines parodė, kad kibernetinėje erdvėje nesame tokie stiprūs, kaip įsivaizdavome.

Andriaus Kubiliaus vyriausybė ėmėsi atsilikimą likviduoti ir 2011 metų birželį patvirtino Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programą. Šią programą Europos Komisija pripažino kaip Lietuvos kibernetinio saugumo strategiją, pagal ją dar ir šiuo metu veikia už šalies kibernetinį saugumą atsakingos institucijos. Ankstesnės kadencijos Seimas 2012 m. birželį priėmė naują Nacionalinio saugumo strategiją, kurioje kibernetinis saugumas apibūdintas kaip vienas svarbiausių nacionalinio saugumo aspektų.

2014 m. gruodį buvo priimtas Kibernetinio saugumo įstatymas, 2015 m. sausį prie Krašto apsaugos ministerijos įkurtas Nacionalinis kibernetinio saugumo centras. 2016 m. sausį patvirtintas

Nacionalinis kibernetinių incidentų valdymo planas. Skubėti privalome, nes Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT, apibendrinęs 2015 metų veiklos rezultatus paskelbė, kad per metus ištyrė 41 583 incidentus. Toks incidentų kiekis 15 procentų didesnis, nei buvo jų ištirta 2014 metais, o didėjimo tendencija tęsiasi jau kelerius metus. Kompiuterių vartotojams vertėtų susipažinti su šia ataskaita (*www.cert.lt/doc/2015.pdf*), joje išvardinti labiausiai paplitę nusikaltimai internete, patariama, kaip jų saugotis.

2015 metų gruodį išgirdome ir Lietuvos Respublikos valstybės kontrolės ataskaitą „Kibernetinio saugumo aplinka Lietuvoje“. Specialistai auditą atliko Vidaus reikalų ministerijoje ir Krašto apsaugos ministerijoje, joms pavaldžiose įstaigose, taip pat visose valstybinės valdžios institucijose ir įstaigose, susijusiose su kibernetinio saugumo plėtros programos įgyvendinimu nuo 2011 m. iki 2015 m. I pusm. Nustatyta, kad programa vykdoma nerezultatyviai, įgyvendinta tik 21 proc. numatytų tikslų, nors pagal grafiką reikėjo pasiekti apie 50 proc. Kibernetiniam saugumui ir elektroninės informacijos saugai reikalingos lėšos skiriamos ir panaudojamos Krašto apsaugos ir Vidaus reikalų ministerijoms nenustačius lėšų skyrimo prioritetų ir kriterijų. Dėl minėtų priežasčių nė viena institucija neturi tikslių duomenų, kiek skirta ir panaudota ES paramos lėšų valstybės institucijų kibernetiniam saugumui gerinti, nėra galimybės pamatuoti ir įvertinti, kaip pasikeitė valstybės įstaigų kibernetinio saugumo būklė, panaudojus šias lėšas. Neskiriama pakankamai dėmesio kibernetinio saugumo plėtrai, teisės aktų rengimui, organizacinės struktūros tobulinimui. Vertinant bendrus audito rezultatus teigiama, kad veiksminga kibernetinio saugumo sistema Lietuvoje nesukurta. Vyriausybei, Krašto apsaugos ministerijai ir Vidaus reikalų ministerijai pateiktas didelis kiekis rekomendacijų, jų įgyvendinimo priemonės ir terminai. ■

VIRTUALIOS ERDVĖS SAUGUMAS – IŠŠŪKIS IR JAV, IR EUROPAI

Linas KOJALA

Sėkmingą kanadiečių telekominkacijų bendrovę „NORTEL“ kibernetinė duomenų vagystė privedė prie bankroto.

Šiuolaikiniame pasaulyje technologijos yra sujungtos į tinklus, kurie leidžia sparčiai dalintis informacija bei teikti įvairias paslaugas. Tyrimų kompanijos „Gartner“ duomenimis, 2016 metais planetoje bus apie 6,8 milijardo į tinklą prisijungiančių prietaisų – 30 proc. daugiau nei praėjusiais metais. Iki 2020 metų šis rodiklis pasieks 20 milijardų ir reikš, kad, atsižvelgiant į globalias demografines tendencijas, kiekvienas žmogus žemėje turės du ar tris tokius prietaisus. Tad tai pažangos rodiklis, prie kurio jau esame įpratę.

Visgi virtualus pasaulis turi ir tamsiąją pusę, nes tampa piktavalių taikiniu: skaičiuojama, kad kasmet kibernetinėje erdvėje padaroma 90 milijonų nusikaltimų, kurie atsieina per 510 milijardų eurų. Ilgainiui augant tinkle veikiančių prietaisų skaičiui, o saugumo tobulėjimui atsiliekant nuo kiekybinės spartos, kibernetinių atakų skaičius bei nuostoliai tik augs.

Tad kas yra daroma, siekiant užtikrinti, kad virtualioje erdvėje jaustumėmės saugesni?

TAMSIOJI KIBERNETIKOS PUSĖ

Kaip teigia termino apibrėžimas, kibernetinės atakos – tai ekonominiu, socialiniu ar politiniu pagrindu motyvuoti veiksmai, kuomet, naudojantis internetu, yra siunčiamos kenksmingos programos, neteisėtai prisijungiama prie tinklų, naudojamasi neleistinomis prieigomis tam, kad būtų pavogta arba paviešinta informacija, priklausanti valstybės institucijoms, privačioms kompanijoms arba pavieniams asmenims.

Nestokojama konkrečių pavyzdžių, kai kibernetinėje erdvėje sukelti nusikaltimai pridaro gausybę problemų. Štai kadaise Kanados telekomunikacijų kompanija „Nortel“ klestėjo ir turėjo apie 100 tūkstančių darbuotojų. Ilgą laiką niekas nesuvokė, kad nuo 2000 metų į kompanijos serverius įsiveržę programišiai po truputį vogė jos vadovų ir klientų privačius duomenis. Nors įmonė keliskart tikrino prielaidą apie galimą įsilaužimą, ilgą laiką tai nebuvo pastebėta. Skandalas į viešumą iškilo tik 2009 metais, kai paaiškėjo, kad nusikaltėliai per beveik dešimtmetį užgrobė per 40 milijonų žmonių kreditinių kortelių numerius. Netrukus „Nortel“ susidūrė su šimtais nukentėjusių klientų bylų teismuose, jos akcijų kaina staigiai krito, o galiausiai privedė kompaniją prie bankroto.

Lietuva, kuri didžiuojasi sparčiausiu viešuoju internetu pasaulyje, taip pat nelieka nuošalyje. Užtenka prisiminti, kad 2015 metų vasarą trumpam buvo užgrobtas oficialus Lietuvos kariuomenės jungtinio štabo internetinis tinklalapis. Jame nusikaltėliai išplatino tikrovės neatitinkančią provokuojančią informaciją, esą Baltijos šalyse ir Lenkijoje

vyksiančios NATO pratybos yra pasirengimas Kaliningrado srities aneksijai. Nors lietuviškai išplatintame tekste buvo gausybė gramatinių ir stiliaus klaidų, tai privertė Aljansą reaguoti, išplatinti paneigiančią informaciją bei dar labiau susirūpinti strateginių institucijų pasirengimu atremti panašaus pobūdžio kibernetines atakas.

Ekspertų teigimu, didžiausi iššūkiai, su kuriais virtualioje erdvėje 2016 metais susidurs ir kasdieniai vartotojai, yra šie:
- dėl spartaus kiekybinio augimo ypač pažeidžiami išmanieji telefonai, kurie gali būti veikiami tiek per mobiliąsias aplikacijas, tiek per naršymą internete;
- augs virusai ir kenkėjiškos programos, kurios savarankiškai keliauja iš prietaiso į prietaisą. Didžiausia iki šiol fiksuota ataka apkrėtė 15 milijonų įtaisų;
- programišių taikinyje – „debesų“ technologija. Nors galimybė laikyti failus internetiniuose debesyse itin vilioja, būtent jie taps vis dažnesniu taikiniu.

Todėl visos pasaulio valstybės, taip pat ir didžiosios tarptautinės organizacijos, pradedant Jungtinėmis Tautomis ir baigiant Šiaurės Atlanto Sutarties Asociacija (NATO), kibernetines grėsmės laiko prioritetu.

LYDERĖ – JAV

Didžiausią dėmesį tam šiandien skiria inovacijomis garsėjančios Jungtinės Amerikos Valstijos. Tuo stebėtis neverta, mat per pastaruosius kelerius metus fiksuotos mažiausiai septynios plataus masto kibernetinės atakos, nukreiptos prieš įvairias stambias JAV įmones. Šių atakų kilmės šalis, spėjama, – Kinija. Teigiama, kad jomis siekta pasisavinti intelektinę nuosavybę, tokią kaip pažangios medicininės technologijos, taip pat valstybės paslaptys. Tad amerikiečiai yra laikomi tais, kurių pavyzdžiu seka Azijos bei Europos šalys.

2009 metais tapęs šalies prezidentu, Barrackas Obama išskyrė kibernetinį saugumą kaip vieną didžiausių ekonominių ir nacionalinio saugumo iššūkių. Nepaisant to, tiek jis pats, tiek garsiausi ekspertai pripažįsta, kad net ir JAV nėra pakankamai pasiruošusi deramai apsiginti. Siekdama keisti šią tendenciją, Obamos administracija išskyrė tris prioritetus, kuriems skirtas didžiausias dėmesys:
- sukurti priešakinę gynybos liniją, kuri būtų pajėgi identifikuoti bei atremti atakas, ypač nukreiptas prieš strateginės reikšmės objektus, infrastruktūrą, valstybės institucijas;
- tobulinti gynybą prieš platų grėsmių spektrą, stiprinant kontražvalgybos pajėgumus bei gerinant informacinių technologijų saugumo reikalavimus;
- kurti saugesnę kibernetinę erdvę ateičiai, daugiau dėmesio skiriant privataus ir valstybinio sektoriaus bendradarbiavimui, taip pat visuomenės edukacijai apie virtualų pasaulį bei jame kylančius iššūkius.

Siekiant didinti federalinės valdžios pasirengimą kibernetinėms grėsmėms, vien šiemet Obama pažadėjo skirti 19 milijardų JAV dolerių, taip pat dar 3 milijardus – informacinių sistemų, kurias prezidentas pavadino „archaiškomis ir pažeidžiamomis“, atnaujinimui.

Vis tik pripažįstama, kad net ir imantis šių priemonių, kibernetinis saugumas išlieka jautrus nacionalinio saugumo aspektas, ypač, jei kalbame apie privatų lygmenį. Tą lemia ir iš pirmo žvilgsnio elementarios aplinkybės: visų pirma, virtuali erdvė nėra suvokiama kaip ta, kurią įmanoma kontroliuoti, todėl didelė dalis kompanijų nėra linkusios bendradarbiauti su valstybinėmis institucijomis, įvykus atakai ar vykdant prevencines priemones. Antra, net jei nusikaltimas yra užfiksuojamas, globalūs tinklai yra dinamiški bei aprėpiantys gausybę informacijos, tad atsekti kaltuosius tampa sudėtinga, o atsekus – teisiškai sudėtinga nuteisti. Trečia, yra nelengva apibrėžti, ypač pinigine išraiška, kokią realią žalą išpuolis padarė.

Atsižvelgiant į tai, kai kurie analitikai ragina į kibernetinę erdvę žvelgti paprasčiau ir apsunkti priešų darbą, laikantis itin paprastų taisyklių. Pavyzdžiui, su svarbia informacija dirbančioms

Monika Hohlmeier

„Artimiausioje ateityje Europos komisija ir ES narės turės padvigubinti Europolo kibernetinių nusikaltimų centrą (EC3), taip Europolui suteikiant galimybes išlaikyti tempą kovoje prieš labai sudėtingus, didžiulės apimties kibernetinius nusikaltimus.“

institucijoms bei pareigūnams ypač rekomenduojama elektroninius laiškus rašyti tik tekstine forma, be pridedamų dokumentų ar internetinių nuorodų. Be to, primygtinai siūloma naudoti tik valstybinius sektorius – kaip žinoma, JAV prezidento rinkimų favorite laikyta Hillary Clinton įsivėlė į skandalą, kuomet paaiškėjo, kad eidama Valstybės sekretorės pareigas naudojo asmeninį serverį, o susirašinėdama nevengė galimai slaptos informacijos. Galiausiai amerikiečiai raginami nesiųsti rinkmenų į valstybes, kurios nėra laikomos iki galo draugiškomis – Kiniją, Rusiją, Iraną ar Šiaurės Korėją.

EUROPA KURIA BENDRAS TAISYKLES

Europos Sąjunga taip pat stengiasi neatsilikti, o ir priežasčių tam nestokoja – Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) duomenimis, dėl saugumo spragų žemynas kasmet patiria 260–340 milijardų eurų nuostolių. Dar 2013 metų vasarį Europos Komisija paskelbė Kibernetinio saugumo strategiją, kurioje numatyta 14 priemonių, turinčių pagerinti situaciją. Įgyvendinant strategijos nuostatas, 2015 metų pabaigoje


ELP nuotrauka

Algirdas Saudargas

2016 metų gruodžio 15 dienos „The New York Times“ laikraščio pirmojo puslapio didelėje nuotraukoje matome JAV demokratų partijos būstinėje stovinčius du baldus. Vienam jų gal jau pusšimtis metų. Tai masyvių stalčių spintelė, pergabenta iš ankstesnės būstinės „Votergeito“ viešbutyje. Ši spintelė – tai nebyli garsiojo skandalo, dėl kurio teko atsistatydinti prezidentui Richardui Nixonui, liudininkė. Antrasis baldas – paprastas stalelis, ant kurio padėtas šiuolaikinis kompiuteris. Istorija nutyli, ar respublikonų samdyti įsilaužėliai neužmiršo meškiuko Teddy kuriame nors stalčiuje, bet nuotraukoje pavaizduotame kompiuteryje tupi mažiausiai du meškiukai. Jie taip pat turi malonybinius vardus: „draugiškas meškiukas“ ir „įmantrus meškiukas“. Šie meškiukai – tikrai ne respublikonų palikimas. Vieną jų atsiuntė mums gerai pažįstama KGB (kaip ji dabar besivadintų), o kitą GRU – ne mažiau garsi Rusijos karinė žvalgyba. Žinia, meškiukas Teddy atsirado, kai prezidentas Theodore'as „Teddy“ Rooseveltas atsisakė medžioklėje nušauti mešką. Visgi prezidentas Obama (kuris taip pat laiku meškiukų nelikvidavo) pažadėjo meškiukus Rusijai grąžinti ir dar pridėti lauktuvių. Kažkaip nesiseka JAV prezidentams su meškiukais...

Laikai keičiasi. Visi daiktai dabar tampa „išmanūs“. Reiškia, kad juose yra kuriam nors tikslui suprogramuotas kompiuterio procesorius, prijungtas prie interneto. Kuriasi vadinamasis daiktų internetas. Smagu, kai gali sužinoti, ar šaldytuve pieno netrūksta. Bet štai šį rudenį JAV tūkstančiai daiktų – šaldytuvų, žaislų ar fotoaparatų – buvo užgrobti ir panaudoti užgrobėjų tikslams. Šiame leidinyje išsamiai aptariamos pačios įvairiausios kibernetinės grėsmės ir būdai kaip su jomis kovoti. Priminiau šią istoriją su meškiukais, norėdamas pabrėžti, kad tai, kas įvyko per JAV prezidento rinkimus, žymi kokybinį pasikeitimą. Niekas neabejoja karine ir technologine JAV galybe. Amerikiečiai didžiuojasi savo demokratine valdysena. Todėl tiesioginis užsienio valstybės įsikišimas į rinkimus pažeidžia pačias jautriausias visuomenės savigarbos stygas. Visiškai nebesvarbu, kokiu mastu bus duotas atsakas. Nėra skirtumo, ar išrinktasis prezidentas Donaldas Trumpas pripažins saugumo įstaigų išvadas, ar jas toliau neigs. Faktas, kad GRU ir KGB valdomos programišių grupės įsilaužė į Demokratų partijos vidinį kompiuterinį tinklą, išvogė vidinio susirašinėjimo laiškus, juos dozuotai ir pritaikytai rinkimų kampanijos eigai pateikinėjo Wikileaks, iš kur juos godžiai siurbė JAV žiniasklaida ir pateikė rinkėjams. Galima svarstyti, kiek tai nulėmė D. Tumpo pergalę. Viena aišku, kad akcija buvo skirta pakenkti Hilary Clinton, kurios Rusijos prezidentas Vladimiras Putinas neapkenčia asmeniškai. O meškiukas šypsosi kandžia *Anonymous* šypsenėle.


www.wikimedia.org, autorius - Shawn P. Eklund

Naujasis JAV gynybos sekretorius Jamesas Mattisas kibernetinę erdvę išskiria kaip naują karo dimensiją, šalia oro, žemės ir jūros.

Europos Parlamente ir Ministrų Taryboje sutarta dėl pirmųjų ES lygmens taisyklių, kurios turės užtikrinti minimalius kibernetinio saugumo reikalavimus bankams, energetikos, vandens įmonėms, taip pat įpareigos privačias kompanijas pranešti atitinkamoms institucijoms apie bandymus įsilaužti. Tikimasi, jog tai paskatins ES šalių bendradarbiavimą, paspartins keitimąsi informacija bei gerųjų praktikų įgyvendinimą.

Prie to prisidės ir valstybės narės, kurios direktyvos įgyvendinimui turės paskelbti nacionalinę Elektroninių ryšių tinklų ir informacijos saugumo strategiją, taip pat paskirti kompetentingą instituciją, kuri prižiūrės priimtų sprendimų įgyvendinimą. Galiausiai buvo išplėstos ir ENISA galios įmonėms užtikrins, kad šalys narės tam tikru lygiu privaloma tvarka keistųsi informacija.

ES taip pat didina bendradarbiavimą su NATO, ypač techniniame lygmenyje. Vasario pradžioje pasirašytas susitarimas tarp organizacijų, kuriuo siekiama užtikrinti informacijos dalijimąsi, nes tai, anot NATO Komunikacijų ir informacijos agentūros vadovo Koeno Gijsberso, yra „esminė kibernetinės gynybos stiprinimo detalė“. Nepaisant to, pripažįstama, kad nors kibernetinis saugumas įgyja vis didesnę svarbą, praktiniame lygmenyje valstybių bendradarbiavimas šiuo klausimu dėl skirtingų teisės aktų, o kartais – ir politinių interesų, išlieka komplikuotas. Todėl itin svarbu užtikrinti, kad kibernetinis saugumas pasiektų deramą lygmenį nacionaliniu, o kartais – ir privačiu mastu. ■

KIBERNETINIŲ ATAKŲ LIETUVOJE ATVEJAI IR KAIP Į JUOS REAGUOJAMA

Paulius SAUDARGAS

Sparčiai plėtojantis informacinėms technologijoms, vis didesnę svarbą įgauna kibernetinės erdvės apsauga. Šiandien kibernetinis saugumas jau yra viena aktualiausių šiuolaikinės saugumo darbotvarkės temų, nes internetiniais kanalais vykdomos atakos neturi sienų, jos plinta žaibišku greičiu ir gali pridaryti didelių nuostolių.

Pirmųjų kibernetinių atakų Baltijos šalyse pradžia siejama su Bronzinio kario skulptūros perkėlimo istorija 2007 m., kada buvo paralyžiuotas Estijos valdžios institucijų, politinių partijų, bankų, žiniasklaidos priemonių interneto svetainių veikimas, taip pat Bendrojo pagalbos centro darbas.

Pirmųjų kibernetinių atakų Baltijos šalyse pradžia siejama su Bronzinio kario skulptūros perkėlimo istorija 2007 m., kada buvo paralyžiuotas Estijos valdžios institucijų, politinių partijų, bankų, žiniasklaidos priemonių interneto svetainių veikimas, taip pat Bendrojo pagalbos centro darbas. Panašių, tik mažesnio masto atakų patyrė ir Lietuva. 2008 m. Seimui kriminalizavus sovietinių simbolių naudojimą, buvo įsilaužta į daugiau nei 300 interneto tinklalapių. Daugiausia tai buvo privačių kompanijų serveriai. Tuo tarpu valstybės institucijų informacinės sistemos atlaikė dėl geresnių apsaugos priemonių.

Kita ataka Lietuvoje įvykdyta prieš šalies pirmininkavimą ES Tarybai. Tuo metu, t. y. 2013 m. gegužę, buvo įvykdyta serija kibernetinių išpuolių prieš didžiausią naujienų portalą „Delfi“ po to, kai jame buvo paskelbta informacija apie tai, kaip per „Eurovizijos“ dainų konkursą buvo perkami balsai už Rusijos atstovę. Iš pradžių portalas kelias valandas veikė su dideliais sutrikimais, o vėliau buvo neprieinamas užsienio vartotojams. Tokie portalo veiklos trikdymai tęsėsi daugiau nei savaitę. Ataka, siunčiant didelius kiekius užklausų, buvo vykdoma daugiausia iš Rusijoje, Baltarusijoje ir Ukrainoje esančių užkrėstų kompiuterių.

Viena vertus, manoma, kad tai buvo tiesiog chuliganiškas programišių elgesys, tačiau tokios atakos dažnai turi politinę potekstę, todėl, kita vertus, pagrįstai svarstoma, kad tai galėjo būti tam tikra treniruotė prieš kokius nors įvykius. Tuo metu artėjo Lietuvos pirmininkavimas ES Tarybai, ES Rytų partnerystės viršūnių susitikimas Vilniuje. Tuo tarpu „Delfi“ yra didžiausias šalies naujienų portalas, turintis gan populiarią versiją rusų kalba. Turint omeny, kad Rusija nėra suinteresuota Rytų partnerystės šalių suartėjimu su ES, galbūt buvo ruošiamasi riboti objektyvios informacijos apie tam tikrus įvykius teikimą visuomenei. Arba galėjo būti ruošiamasi atakoms prieš oficialią Lietuvos pirmininkavimo ES Tarybai interneto svetainę. Laimei, tai, kas galėjo būti blogiausia, neįvyko, nes saugumo požiūriu tam buvo pasiruošta.

Estijos atveju tai taip pat galėjo būti kaip treniruotė, nes po metų, 2008-aisiais, tokios kibernetinės atakos, tik labiau koordinuotos ir didesnio masto, buvo panaudotos Rusijos ir Gruzijos karo metu. Gruzijoje buvo atakuojama visa informacinė infrastruktūra: serveriai, internetiniai puslapiai – tiek privačių įmonių, tiek valstybės institucijų. Viskas buvo išvesta iš rikiuotės. Taigi, vyko tiek konvencinis, tiek nekonvencinis karas, trikdant valstybės veikimą.

Todėl labai svarbu, kad būtų užtikrinta visapusiška valstybės informacinių išteklių apsauga, nes nuo stabilaus informacinių sistemų darbo priklauso valstybės gebėjimas veikti ir teikti būtinas viešąsias paslaugas piliečiams. Po minėtų kibernetinių atakų pieš Lietuvą paaiškėjo, kad plėtojant informacinę infrastruktūrą, nebuvo skirtas pakankamas dėmesys saugumui, ne visos valstybės institucijos pakankamai apsaugotos, nebuvo koordinuotos elektroninių ryšių ir informacijos saugumo strategijos.

Iki tol Lietuvos ryšių reguliavimo tarnybos Kibernetinių incidentų likvidavimo padalinys CERT-LT buvo vienintelė šalies kibernetinio saugumo

2013 m. gegužę buvo įvykdyta serija kibernetinių išpuolių prieš didžiausią naujienų portalą „Delfi“.

institucija, kuri rūpinasi namų vartotojų ir viešųjų paslaugų teikėjų saugumu, o tiksliau, reaguoja į jau įvykusius kibernetinės erdvės incidentus, juos ištiria ir pateikia rekomendacijas, kaip užkirsti kelią tam, kad jie nepasikartotų. Tuo tarpu valstybės institucijos pačios buvo atsakingos už savo kibernetinę saugą pagal Vidaus reikalų ministerijos nustatytus bendrus reikalavimus.

NORS PADĖTIS GERĖJA, BET SAUGUMO LYGIS VIDUTINIS

Stiprinant kibernetinį saugumą, buvo priimtas ir nuo praeitų metų įsigaliojo Kibernetinio saugumo įstatymas, kuriuo nustatytas kibernetinio saugumo organizavimas, valdymas ir kontrolė, taip pat įkurtas Nacionalinis kibernetinio saugumo centras, užtikrinantis kritinės informacinės infrastruktūros ir valstybės informacinių išteklių apsaugą. Krašto apsaugos ministerijai pavaldus centras atlieka daugybę uždavinių: vykdo stebėseną, analizuoja kibernetinio saugumo situaciją, keičiasi informacija su kitų šalių panašiomis institucijomis, reaguoja į įvykusias kibernetines atakas, rengia kibernetinės gynybos planus. Kitaip tariant, šio centro veikla apima ne tik reagavimą į jau įvykusias atakas, bet ir prevencinę veiklą. Taip pat buvo sustiprinti CERT-LT pajėgumai. Padalinyje pradėjo dirbti daugiau žmonių, o darbas vyksta 24 valandas per parą, 7 dienas per savaitę.

Taigi, nors kibernetinio saugumo situacija gerėja, tačiau praėjusių metų birželio mėnesį prieš Lietuvą įvykdyta dar viena kibernetinė ataka parodė, kad dar reikia pasitempti. Valstybės kontrolė 2015 m. audito ataskaitoje šalies kibernetinio saugumo lygį įvertino kaip vidutinį. Ataskaitoje teigiama, kad valstybinės įstaigos išlieka pažeidžiamos dėl nepakankamai įgyvendintų techninių priemonių, organizacinių trūkumų, susijusių su saugumo valdymo sistemos kūrimu, incidentų valdymu, veiklos tęstinumo užtikrinimu, personalo kompetencijos tobulinimu ir išoriniu bendradarbiavimu. Taip pat atkreipiamas dėmesys, kad neišvengiama kibernetiniu saugumu besirūpinančių įstaigų veiklos dubliavimo, o kibernetiniam saugumui reikalingų lėšų skyrimas ir panaudojimas vykdomas nenustačius skyrimo prioritetų ir kriterijų, neturint duomenų apie faktinę įstaigų kibernetinio saugumo ir elektroninės informacijos saugos būklę.

Šias išvadas pagrindžia ir nemažėjantis kibernetinių atakų skaičius prieš Lietuvą. Nacionalinio kibernetinio centro duomenimis, vien per 2015 metus užfiksuota apie dešimt atakų, per kurias įsilaužta į įvairių valstybės institucijų ar strateginių verslo įmonių internetines svetaines. Ryškiausia iš jų – įvykdyta birželio mėnesį. Baltijos šalyse ir Lenkijoje vykusių karinių pratybų „Kardo kirtis“ (angl. – „*Saber Strike*“) metu programišiai įsilaužė į Lietuvos kariuomenės Jungtinio štabo internetinę svetainę ir joje patalpino melagingą informaciją, neva Pentagonas kartu su JAV strateginio planavimo institutais parengė planą, kaip įvykdyti Kaliningrado srities aneksiją. Su klaidomis parašytame tekste buvo teigiama, jog tai yra vienas iš karinių pratybų tikslų.

Remiantis Antrojo operatyvinių tyrimų departamento prie Krašto apsaugos ministerijos informacija, daugiausia kibernetinius išpuolius vykdo užsienio valstybių, pirmiausia Rusijos, žvalgybos ir saugumo tarnybos, su šiomis tarnybomis susiję ar šių tarnybų remiami kibernetiniai įsibrovėliai. Tokios tarnybos, ypač Federalinė saugumo tarnyba bei Gynybos ministerijos struktūriniai padaliniai ir su jais susiję subjektai, turi didžiausius kibernetinius pajėgumus, nukreiptus rinkti informaciją, trikdyti Lietuvos informacinių sistemų ir tinklų funkcionavimą, juos užvaldyti, tikrinti Lietuvos atsakingų institucijų gebėjimą gintis. Tai susiję su Rusijos strateginiais

tikslais įgyti pranašumo gynybos, politikos, ekonomikos, technologijų ir kt. srityse.

REIKIA RUOŠTIS ATAKOMS

Prognozuojama, kad panašių atakų skaičius nemažės, o kibernetinė erdvė išliks viena pagrindinių veiklos erdvių, vykdant tiek įvairius išpuolius prieš nacionaliniam saugumui svarbius kritinės infrastruktūros objektus, tiek kibernetinį šnipinėjimą, siekiant rinkti įvairius duomenis, stebėti ir valdyti virusu užkrėstus kompiuterius. Todėl kibernetinio saugumo stiprinimas turi išlikti vienu svarbiausiu valstybės prioritetu.

Esama tolesnių žingsnių šia kryptimi – praėjusį mėnesį vyriausybė patvirtino Nacionalinį kibernetinių incidentų valdymo planą, kuriame aiškiai įvardintos už kibernetinių incidentų valdymą atsakingos institucijos, t. y. Nacionalinis kibernetinio saugumo centras ir Ryšių reguliavimo tarnyba, taip pat nustatytos keturios atakų kategorijos: pavojingos, didelės reikšmės, vidutinės reikšmės ir nereikšmingi kibernetiniai incidentai. Atsižvelgiant į Valstybės kontrolės rekomendacijas, labai svarbu iki galo sistemiškai sureguliuoti strategiškai svarbias kibernetinio saugumo ir informacijos apsaugos sritis, nes galiojantis kibernetinio saugumo įstatymas sudaro tik teisinį pagrindą valdyti situaciją, nustato atsakingas institucijas, jų funkcijas, teises ir atsakomybes. Taip pat turi būti numatyti lėšų kibernetiniam saugumui užtikrinti skyrimo prioritetai ir kriterijai.

Su kibernetinėmis grėsmėmis susiduria ne tik Lietuva, bet ir kitos Vakarų valstybės, todėl šiuo klausimu yra bendradarbiaujama ir NATO bei ES lygmenyse, tai pat privalu laikytis europinių kibernetinio saugumo reikalavimų. Visgi svarbiausia nepamišti, kad kibernetinis saugumas, kaip ir pasirengimas teritorinei gynybai, yra kiekvienos šalies individuali atsakomybė. O pačioje šalyje už informacinių sistemų saugumą pirmiausia yra atsakingi tų sistemų valdytojai. Kiekvienas tam turi skirti deramą dėmesį. ■

TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO DIREKTYVA – DIDŽIULĖS AMBICIJOS IR NEAPIBRĖŽTOS PRIEMONĖS

Albert KOMAR

Kibernetinės atakos gali prisidėti prie elektros tiekimo nutraukimo.

Reaguodama į padažnėjusias kibernetines atakas, gedimus, paralyžiuojančius kasdienę piliečių veiklą, ir su tuo susijusius nuostolius, Europos Sąjunga žengė dar vieną žingsnį link bendrų kibernetinės erdvės apsaugos taisyklių priėmimo. 2015 metų pabaigoje Taryba ir Europos Parlamentas po ilgų derybų sutarė dėl ES tinklų ir informacinių sistemų saugumo direktyvos priėmimo (NIS). Šia direktyva siekiama „nustatyti aukštą bendrą tinklų ir informacijos sistemų apsaugos standartą“ valstybėse narėse. Nors pirminis sutarimas jau yra, kad direktyva įsigaliotų, jai turi būti pritarta Europos Parlamento plenarinėje sesijoje bei Vadovų Taryboje, tuomet ES valstybės privalės per 21 mėnesį pakeisti savo kibernetinį saugumą reglamentuojančią teisinę bazę bei įgyvendinti tam tikrus institucinius pokyčius.

PAGRINDINĖS DIREKTYVOS NUOSTATOS

Nepaisant to, kad ES narės vis dažniau imasi iniciatyvų užtikrinti tinklų ir informacinių sistemų apsaugą, jų pasirengimas kovoti su kibernetinėm grėsmėm labai skiriasi, o bendrų saugumo standartų išvis nėra. Todėl glaudžiai tarpusavyje susiję tinklai ir sistemos tampa ypač pažeidžiami. Dažni informacinių sistemų, tinklų bei paslaugų, tokių kaip transporto, elektroninės bankininkystės, paieškos ir failų talpinimo sistemų valdymo pažeidimai yra sukeliami įvairaus mąsto kibernetinių atakų ar paprasčiausiai žmogiškųjų klaidų. Skaičiuojama, kad dėl minėtų priežasčių ES per metus praranda apie 260-340 mln. eurų. Į kaštus nėra įtraukiamos sunkiai įvertinamos, emocinės privačios informacijos praradimo pasekmės asmenims bei kiti

www.flickr.com, Perspecsys Photos nuotrauka

su kasdieniu žmonių gyvenimu susiję nepatogumai. Nepasitenkinimas taip pat skatina vartotojų nepasitikėjimą elektroninėmis paslaugomis. Toks nepasitikėjimas didėja kiekvienais metais.

Būtent dėl to tinklų ir informacinių sistemų saugumo klausimas vienas pirmųjų atsidūrė ES institucijų darbotvarkėje. Dokumente numatytas priemones, kuriomis siekiama užtikrinti patikimesnę apsaugą bei sumažinti nemalonias pasekmes, galima suskirstyti į 3 pagrindinius žingsnius:

Pirma – bus sustiprinti valstybių narių pajėgumai kovoti su kibernetinėmis grėsmėmis numatant, kad kiekviena Valstybė narė turi priimti tinklų ir informacinių sistemų apsaugos strategijas, kooperacijos planus bei atitinkamai pritaikyti nacionalinę teisę. Papildomai šalys narės privalės įsteigti specialias, už tinklų ir informacinių sistemų apsaugą atsakingas institucijas bei kompiuterinių incidentų tyrimų tarnybas („Computer Security Incident ResponseTeams“ – CSIRTs), kurios reaguos į pažeidimus ir bus atsakingos už incidentų ir rizikos valdymą. Tarnybos galės būti įsteigtos ir veikti prie esamų valstybės institucijų (pvz., Krašto apsaugos ministerijos).

Antra – ES šalys, kurdamos ir palaikydamos saugumo struktūrą, turės bendradarbiauti tarpusavyje. Taip bus siekiama dalintis geraja tarnybų kūrimo bei įstatyminės bazės reformavimo patirtimi bei keistis informacija apie pažeidimus ir jų prevenciją įvairiose valstybėse. Bendradarbiavimas tarp šalių bus vykdomas per valstybinių institucijų bendradarbiavo grupę, CSIRTs tinklą, padedant Europos tinklų ir informacijos apsaugos agentūrai (ENISA).

Trečia – valstybės turės skatinti viešojo ir privataus sektoriaus bendradarbiavimą, keičiantis informacija apie saugumą. Valstybės privalės apibrėžti saugumo grėsmes, įvertinti konkrečių sektorių pažeidžiamumą bei užtikrinti direktyvos reikalavimus, atitinkančius saugumo standartus. Iš kompanijų bus reikalaujama sustiprinti tinklų apsaugą bei pranešti apie patiriamus pažeidimus. Nustačius pažeidimą, valstybės institucijos, įvertinusios grėsmes, turės nuspręsti dėl tolesnių veiksmų siekiant apsaugoti viešųjų paslaugų teikimą. Šis reikalavimas bus taikomas kompanijoms, kurios teikia „būtiniausias paslaugas“ (transporto, sveikatos, energetikos, atsiskaitymų ir t.t.) ir kurių paslaugų nutraukimas lemtų didžiulius nuostolius. Svarbu pabrėžti, kad direktyva prie tokių kompanijų priskiria ir internetinių paslaugų teikėjus – internetines parduotuves, paieškos sistemas ir duomenų talpyklas.

SAUGUMAS AR PRIVATUMAS?

Nuo pat pradžių ES politikus neramino direktyvos nuostatos, kuriomis vadovaudamosi valstybės institucijos galėtų perimti interneto teikėjų turimus duomenis. Nors diskusijų Europos Parlamente metu šis punktas iš galutinio dokumento buvo išbrauktas, internetinių parduotuvių, paieškos sistemų ar duomenų talpyklų naudotojų asmeninė informacija galės patekti į valdžios rankas. Šių skaitmeninių paslaugų įtraukimas į direktyvos veikimo lauką kelia

www.flickr.com, Perspecsys Photos nuotrauka

Valstybės institucijos turės prieigą prie duomenų talpyklų vartotojų informacijos.

pagrįstą nerimą dėl vartotojų privatumo. Kompanijai pranešus apie sistemos saugumo pažeidimus, valstybės institucijos potencialiai turės prieigą prie gausybės asmeninių piliečių duomenų.

Direktyvos kritikus iš kitos pusės neramina ir tai, kad direktyvos nuostatų vykdymas yra nepakankamai reglamentuotas. Anot kritikų, tai gali lemti, kad ES valstybės skirtingai interpretuos ir vykdys direktyvą, o tinklų ir sistemų apsaugos sritis ir toliau stagnuos. Apibrėžtumo trūksta ir straipsniuose, kurie numato ES šalių bendradarbiavimą, ypač formuojant atsaką į kelias valstybes vienijančius saugumo pažeidimus bei taikant sankcijas už taisyklių nesilaikymą.

Apibendrinant, direktyvos nuostatos sprendimų priėmėjus verčia užduoti amžiną klausimą: saugumas ar privatumas? Lietuvai šie pokyčiai yra naudingi visų pirma dėl to, kad vyriausybė bus įpareigota imtis konkrečių veiksmų, įtvirtinant valstybės institucijų ir svarbiausių valstybėje veikiančių įmonių kibernetinį saugumą. Esamos saugumo programos bus atnaujintos ir pritaikytos naujiems iššūkiams, kas yra svarbu Rusijos agresijos ir padažnėjusių kibernetinių atakų kontekste. Dar vienas direktyvos privalumas yra tai, kad valstybės privalės dalintis informacija apie pažeidimus. Tai praplės Lietuvos ekspertų supratinimą apie informacines grėsmes ES. Vienintelis iššūkis, su kuriuo gali susidurti Lietuvos institucijos įgyvendinant direktyvą, yra patirties ir atitinkamos kvalifikacijos ekspertų stoka.

Vis dėlto, nors pagrindinis dokumento tikslas buvo nustatyti bendrą tinklų ir informacijos sistemų apsaugos standartą, svarbių straipsnių neapibrėžtumas ir didžiulė valstybių manevro laisvė gali ir vėl nulemti skirtingų taisyklių priėmimą ES šalyse. Straipsniai dėl tolesnio tarnybų bendradarbiavimo bei informacijos apsikeitimo galės būti koreguojami proceso metu, tačiau silpni direktyvos pamatai gali nulemti, kad prie bendradarbiavimo bus prieita tik po labai ilgo laiko. ■

IŠMANIEJI ELEKTROS TINKLAI: PROBLEMOS IR PERSPEKTYVOS. ENISA STUDIJOS APŽVALGA

Jonas Kazimieras ŠVAGŽLYS

www.wikimedia.org, wikicommons nuotrauka

Kibernetinės atakos gali prisidėti prie elektros tiekimo nutraukimo.

Aukštųjų technologijų pažanga apima vis įvairesnes gyvenimo sritis. Viena jų – elektros perdavimo tinklai bei jų modernizacija. Pastaruoju metu vienu energetikos sektoriaus prioritetų tampa išmaniųjų elektros tinklų (angl. *Smart grids*) diegimas bei tobulinimas.

Išmanieji tinklai apima įvairias naujas funkcijas. Pavyzdžiui, išmanieji elektros skaitikliai nuskaito suvartotos elektros sąnaudas nuotoliniu būdu. Dėl to elektros vartotojui nebereikia tikrinti elektros skaitliukų ir nurašinėti rodmenų. Tai nėra vienintelis tokių skaitliukų privalumas. Tokios technologijos leidžia geriau planuoti elektros sąnaudas, kadangi vartotojui pateikiama detali informacija, kokiu metu kiek konkrečiai elektros jis suvartoja.

Kitas itin svarbus išmaniųjų elektros tinklų ypatumas - galimybė nuotolinio stebėjimo įrenginiais nustatyti gedimus elektros tinkluose bei automatiškai juos suremontuoti.

Ši funkcija ypač svarbi tada, kai tinklų gedimai įvyksta dėl stichinių nelaimių kaimo vietovėse, nes tokiais atvejais tenka laukti nemažai laiko, kol tinklai yra suremontuojami ir gali vėl atlikti savo funkcijas.

Esama ir daugiau išmaniųjų elektros tinklų privalumų. Vartotojai

turi galimybę patys pasirinkti elektros tiekėją, ir, veikiant rinkos konkurencijai, mažėja elektros kainos. Vartotojai, turintys nuosavas nedideles elektrines (saulės baterijas arba vėjo jėgaines), įgyja galimybę jas prijungti prie bendro elektros tiekimo tinklo ir parduoti dalį savo pagaminamos produkcijos. Be to, išmanieji elektros skaitikliai turi galimybę įvertinti tiekiamos elektros energijos kokybę.

Išmaniųjų elektros tinklų plėtra tampa vienu ES energetikos politikos prioritetų. Pagal 2009 m. EP priimtą direktyvą iki 2020 m. ne mažiau kaip 80 proc. vartotojų turėtų būti įdiegtos išmaniosios matavimo technologijos, jeigu naudos ir kaštų santykis bus teigiamas. Ši nuostata įtraukta į ES Trečiąjį energetikos paketą.

Išmaniųjų elektros tinklų plėtros situacija ES šalyse analizuojama ES tinklų ir informacijos apsaugos agentūros (angl. *European Union Agency for Network and Information Security*; ENISA) paruoštoje studijoje. ENISA įkurta 2004 metais ir sudaryta iš informacinių technologijų industriją atstovaujančių ekspertų. ENISA užsiima tyrimais, kurių tikslas – pagerinti informacijos apsaugos kokybę ES šalyse. Neseniai publikuotoje studijoje išanalizuota šiandieninė išmaniųjų elektros tinklų situacija ES, esminiai jos trūkumai bei rizikos faktoriai ir pateikiamos rekomendacijos, kokių priemonių turėtų būti imtasi, siekiant pagerinti šiandieninę situaciją.

Daugiausia dėmesio studijoje skiriamas komunikacijos tinklams, koordinuojantiems išmaniųjų elektros tinklų veiklą, kylant kibernetinio saugumo grėsmėms. Jų pavyzdžiais galima išskirti kompiuterinių virusų poveikį tinklus koordinuojančioms sistemoms, svarbių duomenų vagystes, kibernetines atakas prieš interneto serverius, sistemas administruojančių darbuotojų netyčines klaidas arba sukčiavimą.

Viena didžiausių galimų grėsmių yra ataka prieš tinklo kontrolės centrus (šie centrai koordinuoja elektros

Išmaniųjų elektros tinklų plėtra tampa vienu ES energetikos politikos prioritetų.

gamybą bei perdavimą vartotojams), nes tokiu atveju gali būti sutrikdyta viso elektros tinklo veikla.

Šios atakos yra pavojingos įvairiais aspektais. Pirma, jos sutrikdo elektros tinklų veiklą, gali laikinai nutrūkti elektros tiekimas. Kitos potencialios grėsmės – gali būti pateikiami klaidinantys mokėjimo rodmenys, sutrikdyti finansiniai pervedimai ir t.t.

Apibendrinant, kibernetinės atakos pavojingos tiek techniniu, tiek finansiniu požiūriu. Minimi šie, atakų riziką didinantys, svarbūs veiksniai: per maža tinklų standartizacija (tinkluose naudojama pernelyg skirtingų rūšių įrenginių, kas didina tinklų pažeidžiamumą), taip pat juose naudojamos ryšio priemonės, tokios kaip Wi-Fi, kurių techniniai protokolai gerai pažįstami atakų organizatoriams.

Daug dėmesio studijoje skiriama gerų praktikų, kaip pagerinti tokių tinklų veiklą, analizei. Tokiomis laikomas tinklų įrangos paruošimas galimoms atakoms (kad sutrikus dalies prietaisų veiklai, nebūtų surikdyta likusių tinklo dalių veikla), saugi tinklo dalių segregacija (siekiant apsaugoti labiausiai pažeidžiamus tinklo komponentus), reguliarus techninis auditas, papildomi matavimo įrenginiai, tikrinantys grėsmių tinklo saugumui tikimybę.

Studijoje pateiktos rekomendacijos apima kelias skirtingas sritis – darbuotojų kvalifikacijos kėlimą, technikos bei veiklos organizavimo tobulinimą. Kaip vienas esminių prioritetų išskiriamas vieningos ES politikos sukūrimas. Teigiama, kad ES turėtų įvesti visoms šalims galiojančią bendrą išmaniųjų tinklų valdymo tvarką, kadangi šiuo metu įvairiose šalyse galioja skirtinga tvarka, – atsižvelgiant į tai, jog komunikacijos tinklai apima daugiau nei vieną šalį, tai trukdo imtis efektyvių saugumo priemonių.

Taip pat svarbu, kad būtų pasiekti susitarimai tarp skirtingų išmaniesiems tinklams reikalingos įrangos gamintojų bei prekybininkų dėl bendrų produkcijos standartų protokolų. Šiuo metu daugelis tinklų tuo pačiu metu naudoja skirtingų įmonių produkciją (taigi turinčią skirtingą techninę specifikaciją), kas taip pat kenkia tinklų veiklai ir didina veiklos sutrikimų tikimybę. Taip pat svarbu, jog išmaniųjų tinklų valdytojai bei akcininkai tarpusavyje dalintųsi informacija apie įvykusias atakas. Taip būtų užkertamas kelias tokioms atakoms pasikartoti.

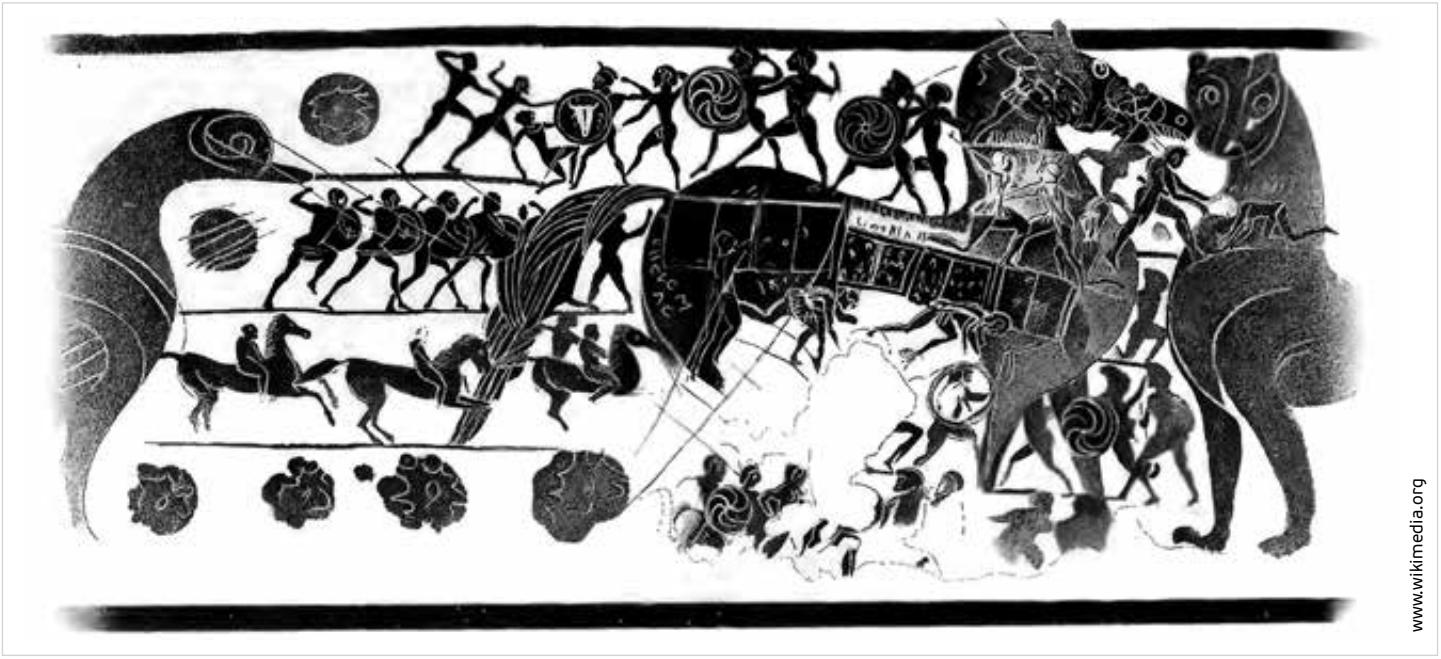
Studijoje teigiama, jog tiek EK, tiek privatūs tokių tinklų akcininkai turėtų dalyvauti rengiant specialius apmokymo kursus išmaniųjų tinklų operatoriams, kurie būtų supažindinami su galimomis grėsmėmis ir apmokomi, kaip jų išvengti. Kaip būdai mažinti atakų grėsmes taip pat minimi kompiuterinių technologijų tobulinimas bei apsaugos programų kūrimas, tinklų techninis auditas, griežtesni tinklų darbuotojų veiklos apribojimai (leidžiant jiems turėti priėjimą tik prie tų tinklo funkcijų, už kurias jie yra tiesiogiai atsakingi) ir t.t.

Apibendrinant, išmanieji elektros tinklai yra perspektyvi technikos naujovė, leidžianti pagerinti elektros tiekimo kokybę ir mažinti jos kaštus, tačiau, norint užtikrinti kokybišką jų funkcionavimą, būtina investuoti į naujų technologijų kūrimą bei plėsti ES institucijų ir paslaugas tiekiančių bendrovių bendradarbiavimą.

Vienas ES institucijų tikslų turėtų būti bendrų standartų, apimančių visas ES šalis, įtvirtinimas, taip sudarant geresnes sąlygas išmaniųjų elektros tinklų veiklos tobulinimui ir galimos rizikos mažinimui. ■

DERAMO ELGESIO ELEKTRONINĖJE ERDVĖJE TAISYKLĖS

Marius LAURINAITIS



www.wikimedia.org

Trojos Arklys. Šiuo principu sudaryti virusai *Trojan* tapo viena populiariausių kenkėjiškų programų.

Dėl elektroninės erdvės specifikos galima išskirti būdus, kuriais elektroniniai nusikaltimai ar teisės pažeidimai gali būti atliekama tik elektroninėje erdvėje, į pagalbą pasitelkiant informacines ir ryšio technologijas bei specialią programinę įrangą ar atitinkamus įrenginius.

Su elektroniniai nusikaltimais ar teisės pažeidimais dažniausiai susiduriama tada, kai elektroninės erdvės naudotojai dalyvauja autentifikavimo procese. Šiame procese vartotojai, norėdami gauti prieigą prie atitinkamų informacinių sistemų, turi patvirtinti savo tapatybę. Tada ir kyla grėsmė tapti nusikaltimo auka, nes ne visi asmenys laikosi būtinų asmens duomenų apsaugos principų ir taisyklių, dažnai elgiasi neapdairiai, neatidžiai ar nesuvokia, kokią žalą gali padaryti internetinis sukčius, pasinaudojęs vartotojo neatsargumu ir gavęs jo asmens duomenis ar kitą asmeninę informaciją. Be to, turi būti užtikrinamas atsiskaitymų, duomenų tvarkymo (t. y. bet kokio veiksmo, atliekamo su duomenimis) ir ryšio kanalų saugumas. Galima paminėti galimus tokių nusikaltimų ar pažeidimų įvykdymo būdus ir jų klasifikaciją:

Galimos tapatybės vagystės: Tiesioginė ryšio, siejančio asmenį ir autentifikavimo duomenis, ataka, atliekant vieną ar kelis tolesnius žingsnius:

naudojant kompiuterinius kirminus, kurie įdiegia kenkėjiškas programas (pavyzdžiui, *key logger*). Autentifikavimo duomenys yra tiesiogiai paimami iš asmens, manipuliuojant jo įvesties įrenginiais (dažniausiai vietiniu kompiuteriu). Tokia ataka vykdoma nesiremiant jokiais atrankos metodais ir yra nukreipta prieš daugelį įvesties įrenginių be tiesioginio kreipimosi į asmenį;

socialinė inžinerija: naudojantis ryšio priemonėmis (pavyzdžiui, telefonu, elektroniniu paštu), autentifikavimo duomenys iš vartotojo gaunami tiesiogiai, vartotojui pateikiant įtikinamą priežastį atskleisti prašomus duomenis, tarkim, nurodant, kad tokie duomenys reikalingi įmonės informacinių technologijų departamento administraciniam personalui tikrinimo tikslais. Tokia ataka yra nukreipta prieš konkretų asmenį;

Trojos arkliai ir kitos kenkėjiškos programos, siunčiamos elektroniniu paštu kaip priedai (angl. *attachments*): pirmiausia neapibrėžtam vartotojų skaičiui išsiunčiama nepageidaujama elektroninio pašto žinutė, kurios priede yra kenkėjiška programa. Vartotojui perskaičius minėtą laišką ir atidarius laiško priedą, kenkėjiška programa automatiškai įdiegiama į vartotojo kompiuterį ir pradeda rinkti autentifikavimo duomenis;

apgaulės taktika prieš (biometrinius) jutiklius (angl. *spoofing of (biometric) sensors*): veiksmai atliekami be asmens, su kuriuo tokie jutikliai susieti, žinios. Pirmiausia iš asmens gaunami reikalingi biometriniai duomenys, pavyzdžiui, akių nuotrauka, kuri po to atspausdinama ir neteisėtai panaudojama. Ataka yra nukreipta prieš konkretų asmenį.

netiesioginė ataka, nukreipta prieš duomenis: su asmeniu susijusių

identifikatorių, duomenų, suteikiančių asmeniui tam tikras teises atlikti kai kuriuos veiksmus duomenų apdorojimo sistemoje, nuorodų paieška: ataka gali būti nukreipta prieš visą duomenų bazę arba tik prieš tam tikrus duomenų įrašus;

manipuliavimas nuorodų duomenimis, susijusiais su asmeniu: autentifikavimo duomenų perdavimas peradresuojamas taip, kad juos gautų internetinis sukčius, o ne informacinių technologijų sistemos, prie kurių turi teisę prisijungti teisėtas vartotojas;

duomenų vagystė (angl. *phishing*): daugeliui vartotojų, pavyzdžiui, banko klientams, išsiunčiamos nepageidaujamos elektroninio pašto žinutės, kurios atrodo taip, tarsi būtų gautos iš patikimos (šiuo atveju – banko) institucijos. Dažniausiai žinutėje raginama paspausti ant pateiktos nuorodos, kuri nukreipia į suklastotą internetinį tinklalapį, iš pirmo žvilgsnio atrodantį lygiai taip pat kaip originalus institucijos tinklalapis. Tokia ataka yra nukreipta prieš ryšį tarp informacinės sistemos ir autentifikavimo duomenų (žr. 2 schemą, Ryšys 3). Suklastotame tinklalapyje vartotojas apgaulės būdu įtikinamas įrašyti savo autentifikavimo duomenis.

„Žmogus – viduryje" atakos: leidžia atlikti ir tiesiogines, ir netiesiogines atakas. Šios rūšies atakų metu perimami duomenys, kuriais keičiasi vartotojas ir sistema. Atakos yra labai veiksmingos ir, be kita ko (pavyzdžiui, duomenų pakeitimo galimybės), suteikia galimybę įvairiais būdais atlikti tapatybės vagystę:

tapatybės vagystė, atliekama ieškant autentifikavimo duomenų, kai asmuo komunikacijos procese dalyvauja nesilaikydamas saugumo reikalavimų;

atsakomosios atakos: manipuliuojama interneto protokolo paketu, kuriame yra autentifikavimo duomenys su siuntėjo adresu. Toks protokolas persiunčiamas gaunančiajai sistemai. Ataka nukreipta prieš specialių įvesties įrenginių naudotoją;

tapatybės vagystė, atliekama peradresuojant pranešimą į suklastotą interneto tinklalapį (pavyzdžiui, naudojant apgaulės taktiką domenų vardų sistemos atžvilgiu (angl. *DNS-spoofing*): suklastotame interneto tinklalapyje vartotojas apgaulės būdu įtikinamas įrašyti savo autentifikavimo duomenis;

Tapatybės perdavimas turint nesąžiningą tikslą arba apsikeitimas tapatybėmis nesąžiningu tikslu: šiuo atveju asmuo bendrininkauja su internetiniu sukčiumi, sąmoningai duoda jam savo autentifikavimo duomenis, suvokdamas, kad jie bus naudojami neteisėtai;

Tapatybės sukūrimas: internetinis sukčius paprastai pasinaudoja tam tikrais registracijos aspektais ir manipuliaciniais veiksmais tam, kad suardytų jo, kaip fizinio asmens, ir duomenų, suteikiančių asmeniui tam tikras teises atlikti kai kuriuos veiksmus duomenų apdorojimo sistemoje, veiksmų grandinę. Taip internetinis sukčius, neturėdamas tam teisės, kurį laiką gali naudotis informacine sistema.

Dažna vieta, kur bandoma pasisavinti mokėjimo duomenis, yra bankomatas.

Visi sutinkame, kad siekiant maksimaliai sumažinti elektroninių nusikaltimų elektroninėje erdvėje tikimybę, būtina apsaugoti savo asmeninę informaciją[1]. Atlikti moksloniai tyrimai rodo, kad patys vartotojai bene daugiausia prisideda prie elektroninių nusikaltimų prevencijos[2], todėl prevencija konkretaus asmens lygmeniu yra labai svarbi.

Prevencijos konkretaus asmens lygmeniu atveju paminėtina 21 taisyklė, kuri padėtų sumažinti elektroninių nusikaltimų grėsmę asmenims. Šias taisykles Martinas T. Biegelmanas savo kny*goje Identity Theft Handbook: Detection, Prevention and Security*[3] pristato kaip kiekvienam vartotojui žinoti privalomas taisykles, tačiau jos labiausiai pritaikomos yra JAV praktikoje. Šį taisyklių rinkinį galima adaptuoti taip, kad būtų galima pritaikyti ir Lietuvoje,

[1] *Higgins, G. E. 2010. Cybercrime: An Introduction to an Emerging Phenomenon. McGraw-Hill, p. 70.*

[2] *Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back. <http://www.prnewswire.com/news-releases/javelin-study-finds-identity-fraud-reached-new-high-in-2009-but-consumers-are-fighting-back-83987287.html>.*

[3] *Biegelman, M. T. 2009. Identity theft handbook : detection, prevention and security, p. 295.*

atsižvelgiant į naudojamas finansines paslaugas, teisinę sistemą ir kitus svarbius aspektus. Paminėtina, kad tokių taisyklių rinkinių pateikiama ir kitoje literatūroje.

Taigi, kiekvienas vartotojas Lietuvoje, norėdamas apsisaugoti nuo dalies galimų elektroninių nusikaltimų rizikos, turėtų atkreipti dėmesį į šias taisykles.

Reikia apsaugoti kitą asmeninę informaciją

Asmens identifikavimo numerių apsauga yra pirmas žingsnis asmeninės informacijos apsaugos link. Prie tokių apsaugos priemonių būtina priskirti elektroninių mokėjimo kortelių numerius, banko sąskaitų duomenis ir kt. Negalima pateikti kreditinės kortelės numerio ar kitos asmeninės informacijos asmenims, kurie skambina, net jei prisistato kaip oficialūs asmenys ir vilioja įvairiais pasiūlymais. Būtina maksimaliai susiaurinti ratą subjektų, kuriems suteikiame savo asmeninę informaciją, taip pat reikia maksimaliai sumažinti asmeninės informacijos kiekį, kurį nešiojamės su savimi. Rekomenduojama nesinešioti užsirašytų savo kortelių asmens identifikavimo numerių (PIN). Taip pat nesaugoti svarbios asmeninės informacijos, PIN kodų, slaptažodžių mobiliuosiuose įrenginiuose, jei tokia informacija nėra apsaugota kriptografiniu būdu. Reikia nuolatos tikrinti sąskaitų išrašus, ypač kredito kortelių, po kiekvieno naudojimo ir apsipirkimo tiek fizinėje, tiek elektroninėje erdvėje. Neduoti kortelių į rankas, jei atsiskaitinėjama lustinėmis kortelėmis. Perkant internetu iš mažmenininkų reikia pasidomėti, kas ir kiek laiko saugos finansinę informaciją – kuo mažiau informacijos leista laikyti, tuo mažesnė rizika, kad ji bus neteisėtai panaudota.

Pasirūpinti tinkama kompiuterio apsauga

Kompiuteryje turi būti įdiegta ugniasienė ir antivirusinė programa. Būtina imtis prevencinių priemonių dėl galimų kenkėjiškų programų ar virusų. Reikia laiku atnaujinti visą apsaugos programinę įrangą, įtariai vertinti neprašytus laiškus, kuriuose prašoma pateikti asmeninės ar finansinės informacijos. Teisėti prašymai pateikti asmeninę informaciją paprastai nėra siunčiami elektroniniu paštu. Negalima naudotis viešais kompiuteriais tokiose vietose, kaip viešbučiuose, kavinėse ar kt., ir atlikti finansinius sandorius ar tvarkyti kitą svarbią asmeninę informaciją. Minėtose vietose esantys kompiuteriai gali būti užkrėsti šnipinėjimo programomis arba virusais. Niekada neatidarinėkite nežinomų elektroninių laiškų priedų arba atsisiųstos abejotinos programinės įrangos. Nusikaltėliai gali siūlyti nemokama muziką, antivirusinę apsaugą ar kitas programas. Būtina apsaugoti ir koduoti namų bevielį kompiuterinį tinklą, taip nusikaltėliams bus sunkiau rasti neapsaugotą prieigą. Visada naudokite sunkius slaptažodžius, nenaudokite žodžių, pavadinimų, ar frazių, kurios gali būti lengvai atspėjamos. Kuo ilgesnis slaptažodis, tuo geriau. Dažnai rekomenduojama, kad slaptažodis turėtų būti bent aštuonių simbolių, raidės būtų atsitiktinės, o skaičiai yra stipriausi slaptažodžio elementai. Taip pat reikia nustatyti slaptažodžio keitimo tvarką ir jos laikytis.

Būtinas atsargumas naudojantis bankomatais

Dažna vieta, kur bandoma pasisavinti mokėjimo duomenis, yra bankomatas. Būtina atkreipti dėmesį į įtartinus prietaisus. Apžiūrėkite, ar bankomatas techniškai tvarkingas, ar nematyti atvirų laidų, jungčių, paslėptų kamerų, kurias nusikaltėliai naudoja PIN slaptažodžiams įrašyti. Jei bankomatas atrodo įtartinai, pavyzdžiui, per daug iškilusi klaviatūra, prie kortelės įkišimo lizdo primontuotas neaiškus įrenginys, rekomenduojama nesinaudoti ir, esant galimybei, pranešti apie tai atitinkamam bankui ir teisėsaugos institucijai. Būtina atkreipti dėmesį į žmones, kurie pernelyg ilgai atlieka paprastas operacijas ar įdėmiai stebi kitų žmonių veiksmus prie bankomatų. Tokie žmonės gali naudoti paprasčiausius žiūrėjimo per petį metodus tam, kad pamatytų PIN kodą, pinigų likutį sąskaitoje, o tai gali paskatinti juos įvykdyti apiplėšimą, o vėliau, gavus mokėjimo kortelę, ištuštinti sąskaitą. PIN kodą geriau įrašyti viena ranka, kitą naudojant kaip skydą PIN kodui apsaugoti nuo galimo pamatymo. Ypač reikia būti atsargiems naudojantis bankomatais užsienyje, nes jų modeliai atskirose šalyse skiriasi, tad nepažįstami bankomatai visada kelia didesnę riziką. Taip pat iki minimumo bankomatuose reikėtų naudotis kvitais ir iš karto juos sunaikinti, kad jais negalėtų pasinaudoti galimi nusikaltėliai, rinkdamiesi potencialią auką.

Uždrausti platinti asmeninę informaciją

Vartotojai gali rinktis, kiek ir kokią informaciją jie nori pateikti prekybos įmonėms, kitoms bendrovėms, tam tikroms vyriausybinėms organizacijoms elektroninėje erdvėje. Informacija apie asmenis dažnai dalijamasi, tai daro daugelis verslo atstovų, ypač siūlydami naujas paslaugas ir prekybines akcijas. Galima nesutikti, kad asmeninė informacija būtų atskleista tretiesiems asmenims, būtina reikalauti pašalinti asmeninius duomenis iš komercinės rinkodaros duomenų bazių, atsisakyti nepageidaujamų laiškų, įskaitant katalogus ir kt.

Reikia pasidaryti asmens duomenų atsarginę kopiją

Dažnai patys asmenys net nežino savo asmens dokumentų numerių, jų galiojimo laiko, išdavimo datos ir t. t. Rekomenduojama padaryti dokumentų, kuriuos nešiojamasi su savimi, aprašą. Užsirašyti arba padaryti kopijas sąskaitų numerių, kredito kortelių, užfiksuoti dokumentų galiojimo datas, emitentų pavadinimus ir reikiamus telefono numerius, kad pranešus būtų galima atšaukti prarastų dokumentų galiojimą. Toks sąrašas padės susiorientuoti, kokie dokumentai prarasti nelaimės atveju, sutikrinti, kokie buvo kartu ir kokių

jau nėra. Žinoma, negalima laikyti šio sąrašo piniginėje ar rankinėje, jį reikia paslėpti saugioje vietoje, kur pasiektų tik pats savininkas, tai galėtų būti namų seifas, kurį šiais laikais privalu turėti.

Kiekvieną mėnesį būtina peržiūrėti gaunamas sąskaitas

Reikia įsitikinti, kad visos gautos sąskaitos yra pagrįstos, paslaugų teikėjai žinomi ir pateikti jų sąskaitų duomenys taip pat. Dažnai pasitaiko, kad aptinkamos fiktyvios sąskaitos už paslaugas, vartotojai nieko neįtardami jas apmoka, vėliau paaiškėja, kad už jiems įprastas paslaugas jie sumokėjo sukčiams. Reikia tinkamai sekti mokėjimus, skirti keletą minučių jiems peržiūrėti, jei kyla įtarimas, kad pateiktos sąskaitos ir mokėjimo tvarka skiriasi nuo įprastos. Būtina atkreipti dėmesį, jeigu mokėjimo gavėjo pavadinimas pasikeitė arba pakeista pastovi mokėtina suma. Tokią grėsmę gerokai sumažintų elektroninės sąskaitos, gaunamos iš paslaugų teikėjų, ir tinkamai suformuoti atskaitymų šablonai elektroninės bankininkystės sistemoje – taip bet kokie pakeitimai būtų iškart pastebimi.

Rekomenduojama prieš išmetant ar keičiant sunaikinti duomenis seno kompiuterio[4] kietajame diske

Kai asmuo perka naują kompiuterį ar keičia senojo kietąjį diską, ką daro su senuoju? Daugelis žmonių tiesiog jį išmeta. Tačiau jau nebeveikiantis kietasis diskas dar gali būti nuskaitytas, iš jo įmanoma ištraukti visą ar dalį buvusios informacijos. Būtina ištrinti visą informaciją, jei planuojama keisti diską ar išmesti seną. Net jei diskas neveikia, reikia pasirūpinti, kad jo niekas nebandytų nuskaityti. Dažniausiai siūlomi sprendimai – tai diską fiziškai sunaikinti (smūgiu plaktuku, įrenginį pergręžti, neatstatomai pažeidžiant standžius diskus). Jei diskas geras ir ketinama jį parduoti ar kt., reikia pasirūpinti, kad visi ten esantys duomenys tikrai būtų pašalinti. Jį reikia paprasčiausiai suformatuoti, o jei diske buvo tikrai svarbios informacijos, galima atlikti vadinamąjį nulinį formatavimą (angl. *Zero-filling*), kai visa disko talpa užpildoma nuliais, neatstatomai panaikinant bet kokį buvusį įrašą. Tokie patys sunaikinimo veiksmai turėtų būti atliekami ir su kitomis laikmenomis (USB kištukinėmis atmintinėmis, optinėmis laikmenomis).

Galima naudoti privatumą saugančias priemones

Jei kompiuteris naudojamas keliaujant, kavinėse ir kitose viešose vietose ir būtinai tenka naudotis elektroninėmis finansinėmis paslaugomis, reikia pasirūpinti priemonėmis, kurios užtikrintų privatumą. Kaip vienas iš siūlymų – specialios ekrano apsaugos, klijuojamos plėvelės, kurios užtikrina ekrano duomenų privatumą, kai matoma tik sėdint tiesiai prieš ekraną. Tokie ekranai gali apsaugoti nuo smalsių akių, kai keliaujama ankštose erdvėse, tokiose kaip lėktuvas, traukinys, autobusas. Nors vadinamieji privatumo ekranai yra labai veiksmingi, tačiau jų nėra standartiniame komplekte, todėl tenka pirkti atskirai.

Negalima lengvai tikėti atsitiktine sėkme ir laimėjimais, taip pat nelaimėmis ir problemomis elektroninėje erdvėje

Sukčiai dažnai naudoja laiškus, telefonus, internetą, kad apgautų. Jie gali pranešti, kad asmuo laimėjo puikų prizą, ar siekti sukelti nerimą pranešdami apie menamą nelaimę, gali prisistatyti valstybės pareigūnu, banko atstovu, įmonių vadovu, taikyti tam tikrus psichologinius metodus. Rekomenduojama neatsakinėkite į laiškus, kuriuose prašoma mokesčių ar verslo susitarimų, į raginimus pateikti informaciją apie banko sąskaitą, siekiant perduoti didelę pinigų sumą. Dažnai sukčiai bando išvilioti pinigus pirkdami prekes, už kurias neva per daug sumoka, dažnai atsiunčia fiktyvius tarptautinių mokėjimo kvitus, taip pat bando išvilioti pinigų menamoms advokato išlaidoms, kurios atsiranda dėl didelio laimėjimo dokumentų tvarkymo ir t. t.

Reikia stengtis išvengti duomenų pažeidimų

Dėl galimų duomenų pažeidimų būtina imtis reikiamų priemonių:

- Riboti svarbių duomenų saugojimą kompiuteriuose. Per daug asmeniškos ir identifikuojančios informacijos nelaikyti nešiojamame kompiuteryje, nes jį galima prarasti.
- Įdiegti šifravimo programinę įrangą, jei yra naudojami svarbūs duomenys.
- Nuolatos atnaujinti informacinės sistemos elementus.
- Naudoti saugų interneto prisijungimą keliaujant.

Jei asmuo tapo auka

Jei asmuo tapo elektroninių nusiklatimų auka, būtina nedelsiant kreiptis į banką, jei vagys pasinaudojo asmens finansiniais instrumentais, – ir į policiją. Jei pastebėjote, kad kažkas naudoja asmens duomenis be asmens sutikimo, reikia kreiptis į Valstybinę duomenų apsaugos inspekciją. Atsiminkite svarbiausią taisyklę – pirmiausia pats asmuo turi saugoti savo duomenis ir tik pasirūpinęs tinkama apsauga, jis galės tikėtis tinkamos pagalbos, nes jei asmuo kontroliuos visus savo duomenis, žinos, kur ir kiek jų yra palikęs, labiau padės tyrėjams atskleisti įvykusią tapatybės vagystę.

Be šių taisyklių, būtina laikytis ir asmeninės informacijos valdymo kontrolės. Asmeninės informacijos skelbimas, pavyzdžiui, socialiniame tinkle, padidina elektroninių nusikaltimų tikimybę. Todėl asmenys turi kontroliuoti asmeninės informacijos apie save skelbimą viešai. ■

[4] Tokios pačios taisyklės taikomos ir išmaniųjų telefonų atveju bei pan.

APIE ELEKTRONINĮ BALSAVIMĄ PAPRASTAI

Konstantin AGAFONOV, Mykolo Romerio universiteto doktorantas

Lietuvoje prieš kiekvienus rinkimus ar referendumą viešoje erdvėje atsiranda straipsnių apie elektroninį balsavimą, Žurnalistai ir apžvalgininkai ir vėl mėgina svarstyti galimybę elektroninį balsavimą naudoti ir Lietuvoje.

www.flicr.com, LWVC nuotrauka

Jei paklausite manęs, ar man patinka elektroninio balsavimo naudojimo Lietuvoje idėja, tai aš, pridėjęs ranką prie širdies, atsakysiu Jums – taip, aš palaikau elektroninį balsavimą ir tai turi tapti Lietuvos rinkimų sistemos dalimi. Suprantu, kad daugeliui Lietuvos piliečių ir šio žurnalo skaitytojų toks mano teiginys sukels jausmų audrą ir jie pradės priekaištauti, kad eilinį kartą valdžia užsakė straipsnį ir sumokėjo autoriui už tai, kad jis įtikintų plačiąją visuomenę palaikyti elektroninį balsavimą, kad valdžia galėtų manipuliuoti rinkimais. Sutikite, kad tokių komentarų ir piliečių nuomonės apie elektroninį balsavimą tikrai teko išgirsti ir jums. Aš taip pat kažkada buvau prieš elektroninius rinkimus, bet, pradėjus skaityti ir domėtis šia tema, mano nuomonė pasikeitė.

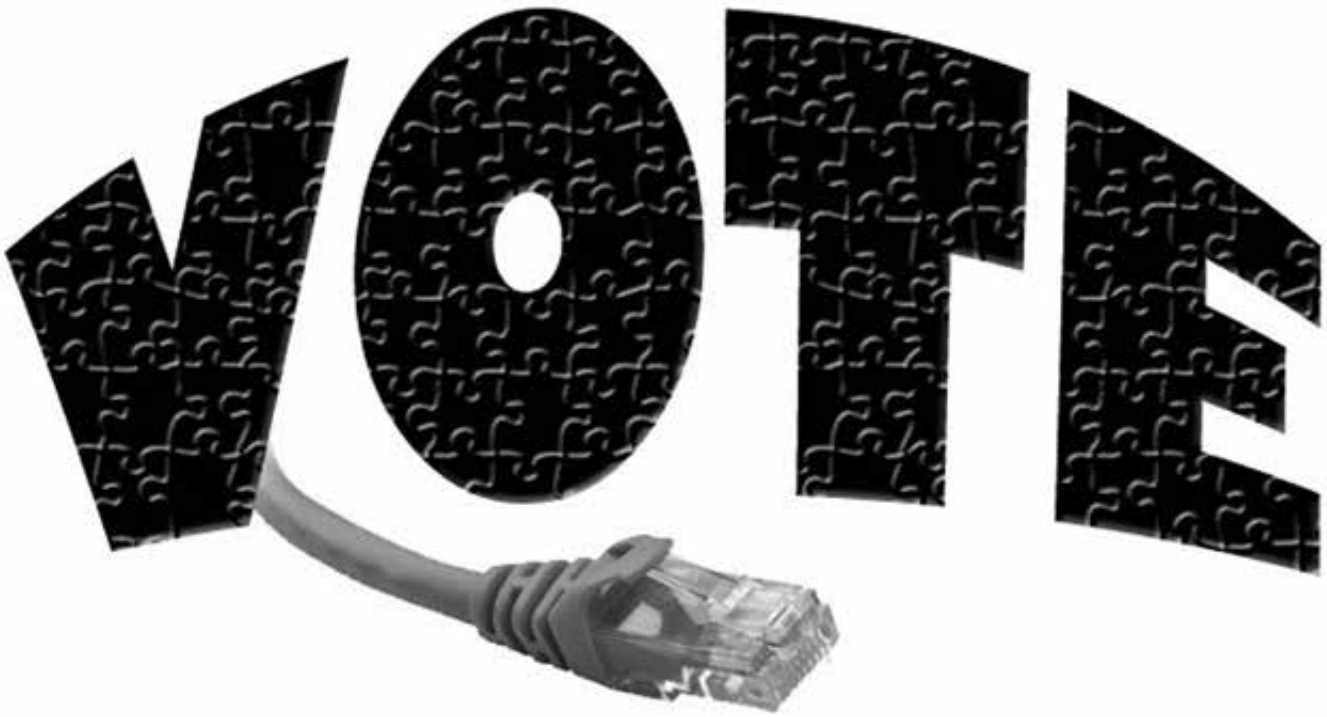
Šiame straipsnyje pabandysiu pateikti skaitytojui bendrą informaciją apie elektroninius rinkimus ir jų panaudojimo galimybes, apžvelgti Lietuvos patirtį žengiant elektroninių rinkimų link, o skaitytojas pats galės padaryti išvadas ir nuspręsti, ar tikrai elektroniniai rinkimai yra toks neigiamas ir nepriimtinas mūsų visuomenei dalykas.

ELEKTRONINIŲ RINKIMŲ SISTEMŲ NAUDOJIMAS

Elektroniniai balsavimai pasaulyje yra charakterizuojami kaip balsavimo proceso organizavimas rinkimuose ir referendumuose pasinaudojant naujausiomis informacinėmis ir telekomunikacinėmis technologijomis. Elektroninius rinkimus galima skirstyti į dvi dideles grupes: internetinis balsavimas ir elektroninis balsavimas.

Elektroninis balsavimas yra grindžiamas balsavimo sistemomis, kuriose yra naudojami tam tikri techniniai įrenginiai, kuriais balsavimo rezultatai yra surenkami ir apdorojami bei saugomi. Elektroniniam balsavimui naudojami įrenginiai yra patalpinami kontroliuojamoje aplinkoje (pvz., rinkimų apylinkėse, mobiliuose balsavimo kioskuose, konsulatuose) ir balsavimo proceso metu jie yra naudojami tam, kad fiksuotų rinkėjo pasirinkimą. Paprasčiausi įrenginiai yra optiniai balsavimo biuletenių skaitytuvai, kurie nuskaito rinkėjo užpildytą balsavimo biuletenį ir automatiškai suskaičiuoja rinkimų rezultatus (rinkimo biuletenis po nuskaitymo yra patalpinamas i specialų konteinerį). Taip pat gali būti naudojami balsavimo terminalai, kuriose biuletenis yra atspausdinamas ir, rinkėjui patvirtinus, kad biuletenis teisingas, yra automatiškai įmetamas į balsadėžę (rinkėjas biuletenį pildo naudodamasis terminalo liečiamu ekranu). Tokių įrenginių naudojimas gali smarkiai sumažinti balsų skaičiavimo klaidų, sumažinti netyčia sugadinamų biuletenių kiekį.

Internetinis balsavimas yra siejamas su balsavimo sistemomis, kurių pagrindą sudaro pasaulinis interneto tinklas. Internetas šiose sistemose panaudojamas kaip duomenų perdavimo terpė. Šių balsavimo sistemų panaudojimo pradininke laikoma Estija, kur taip balsuojama jau dešimtmetį. Pagrindinis šios sistemos privalumas yra galimybė integruoti į rinkimų procesą visus suinteresuotus piliečius, kadangi balsavimas tampa įmanomas iš bet kurios pasaulio vietos ir bet kuriuo paros metu, kai tai yra patogu pačiam rinkėjui. Estijoje apie trečdalis visų rinkėjų pasirenka internetinio balsavimo sistemą, o rinkėjų, dalyvaujančių balsavime, skaičiaus



www.flickr.com, Democracy Chronicles nuotrauka

mažėjimo problema, būdinga vakarų valstybėms, Estijoje nėra tokia jau ir aštri.

Elektroninės ir internetinės rinkimų sistemos pasaulyje pradėtos vystyti XX amžiaus paskutiniojo dešimtmečio viduryje, kai politinės partijos ir vyriausybės pradėjo aiškiai suvokti, kad pasaulyje atsiradęs visuotinis interneto tinklas yra reikšmingas visuomenei ir jį galima panaudoti politiniams rinkimams.

Aibė projektų buvo vykdoma Europos šalyse: Nyderlanduose, Vokietijoje, Prancūzijoje, Anglijoje. Taip pat elektroninio balsavimo technologijos buvo naudojamos ir JAV, Brazilijoje. Skaitytojas turbūt nustebs, bet pirmieji elektroniniai rinkimai buvo įvykdyti Brazilijoje net 1996 metais. Nors brazilų elektroninių rinkimų sistema ir yra kritikuojama brazilų opozicijos, nors ši sistema pripažįstama esanti netobula, ji vis vien yra naudojama. Nyderlandų elektroninių rinkimų sistema, nors ir vadinta tobulesne nei Brazilijos, vis dėlto neatlaikė saugumo išbandymo ir valdžia buvo priversta atsisakyti šios sistemos tobulinimo ir naudojimo.

Elektroniniai balsavimai yra labai specifinė sritis, ir, mano nuomone, kiekviena šalis turi išmėginti šią sritį, kad suprastų, ar ji yra tinkama naudoti šalies politiniams procesams. Sakyti, kad kitoms šalims nepasisekė, tai nepasiseks ir mums, yra mažų mažiausiai neteisinga.

LIETUVOS ŽINGSNIAI ELEKTRONINIŲ RINKIMŲ LINK

Lietuvoje, kaip ir visame pasaulyje, seniai yra pastebima rinkėjų aktyvumo mažėjimo problema. Rinkimai, vykdomi įprastiniu būdu, nepritraukia rinkėjų, kadangi rinkėjams ne visuomet yra patogu apsilankyti rinkimų apylinkėse dėl laiko stokos ar dėl didelio atstumo, kurį reikia įveikti, norint pasiekti rinkimų apylinkę.

Piliečiai, kurie yra išvykę ieškoti geresnio gyvenimo į kitas pasaulio šalis, galbūt ir norėtų pareikšti savo politinę poziciją, bet, deja, to nedaro, nes nemato tikslo eikvoti savo sunkiai uždirbtus pinigus kelionei iki konsulato, o dalis visuomenės tiesiog nemato, už ką galima būtų balsuoti. Ką gi daro šie piliečiai per rinkimus? Aš jums atsakysiu: jie tiesiog nedalyvauja rinkimuose ir tai daro sąmoningai taupydami savo pinigus ir laiką.

Lietuva, norėdama paskatinti piliečių aktyvumą bei bandydama įgyvendinti Europos Sąjungos skatinamus elektroninės valdžios ir elektroninės vyriausybės principus, taip pat siekdama aktyvinti piliečius dalyvauti šalyje organizuojamuose rinkimuose ir referendumuose, jau beveik 10 metų žingsniuoja elektroninių rinkimų sistemos įkūrimo link.

Pabandykime atsigręžti į praeitį ir papasakoti skaitytojui, kokie gi buvo tie žingsniai. Mėginsiu neįkyrėti skaitytojams, pateikdamas konkrečias datas ir detalizuodamas įvykius, bet pasistengsiu nupiešti bendrą paveikslą, kuriame atsispindės padėtis, susidariusi Lietuvoje ir susijusi su elektroninių rinkimų įgyvendinimu.

Lietuvoje 2006 metais buvo parengta ir Vyriausiosios rinkimų komisijos patvirtinta „Balsavimo internetu rinkimuose ir referendumuose koncepcija“. Vadovaujantis koncepcija, 2007 metais buvo priimtas Lietuvos Respublikos Vyriausybės nutarimas „Dėl balsavimo internetu diegimo

programos patvirtinimo“. Atrodytų, kad viskas, kas yra reikalinga internetiniams rinkimams įgyvendinti, jau yra atlikta, bet, deja. Aukščiau aprašyti teisės aktai yra tik rekomendacinio pobūdžio. Šie dokumentai yra tiesiog kelrodis, nurodantis tik pagrindines kryptis ir būtinus pakeitimus, kurie yra neišvengiami, norint Lietuvoje įdiegti internetinio balsavimo sistemą. Tie pakeitimai apima rinkimų ir referendumo įstatymų pakeitimus, kurie įteisintų balsavimo internetu galimybę, taip pat Administracinės teisės ir Baudžiamojo kodekso pakeitimus, kurie nustatytų juridinių ir fizinių asmenų atsakomybę už teisės pažeidimus, susijusius su elektroninių balsavimų kompromitavimu (sistemų saugumo pažeidimus, duomenų klastojimą, balsų pirkimą ir kt.).

2007-2014 metais Seime buvo registruojami įstatymų pakeitimo projektai, bet nė vienas iš šių projektų taip ir nebuvo baigtas svarstyti.

Apibendrinant galima teigti, kad dabartiniu laikotarpiu valdžios institucijos deklaruoja norą Lietuvoje įdiegti internetinio balsavimo sistemą, bet tiesioginių veiksmų, kurių imtųsi valdžia, nesimato. Pagrindinė priežastis, dėl kurios internetinis balsavimas nėra įdiegtas Lietuvoje, yra politinės valios trūkumas, taip pat kai kurių politinių partijų baimės jausmas. Dažniausiai politinės partijos yra orientuotos į juos pastoviai palaikančias rinkėjų grupes, o abejojančių ar valdžios politika nepatenkintų, ar tiesiog užsiėmusių rinkėjų balsai jiems yra nelabai aktualūs. Panaši situacija buvo susidariusi ir Estijoje, kur konservatyvių požiūrių, „senos“ politinės partijos nenorėjo internetinio balsavimo sistemos įdiegimo.

MITAI IR TIKROVĖ, PRIELAIDOS IR REALYBĖ

Dažniausias mūsų šalies politikų pasiteisinimas yra susijęs su internetinio balsavimo nesaugumo arba tiksliau su situacija, kai balsuojant internetu, balsavusio žmogaus pasirinkimas gali būti stebimas kito asmens ir tokiu būdu

Dabartiniu laikotarpiu valdžios institucijos deklaruoja norą Lietuvoje įdiegti internetinio balsavimo sistemą, bet tiesioginių veiksmų, kurių imtųsi valdžia, nesimato.

yra pažeidžiama nuostata dėl balsavimo slaptumo. Žinoma, tai yra svarus argumentas, bet nereikia pamiršti ir to, kad Lietuvos internetinio balsavimo sistemą siūloma organizuoti vadovaujantis jau veikiančiu Estijos internetinio balsavimo sistemos modeliu.

Trumpai papasakosiu skaitytojams apie Estijos internetinio rinkimo sistemą. Kadangi ne visi skaitytojai yra informacinių technologijų specialistai, tai šis pasakojimas neapims technologinių sprendimų, kurie yra panaudoti Estijos balsavimo sistemoje, bet atskleis pagrindinius sistemos veikimo principus.

Estijoje internetinis balsavimas yra vykdomas prieš balsavimą rinkiminėse apylinkėse ir šiam balsavimui yra numatytas tam tikras laikotarpis (dvi dienos), kuomet rinkėjas savo balsą gali atiduoti už jam patinkantį kandidatą. Kiekvienas, nusprendęs balsuoti internetu, prisijungia prie balsavimo internetu sistemos ir, naudodamasis techninėmis priemonėmis, patvirtina savo tapatybę. Po tapatybės patvirtinimo rinkėjas patenka į balsavimo sistemą, kurioje gali pareikšti savo apsisprendimą ir balsuoti už tam tikrą kandidatą. Po balsavimo rinkėjo balsavimo biuletenis yra užšifruojamas ir patenka į elektroninę balsadėžę (duomenų centrą), kuriame yra saugomas iki rinkimų pabaigos.

Jei rinkėjas dėl bet kokios priežasties persigalvoja dėl savo pareikštos nuomonės, tai laikotarpiu, kol dar nėra pasibaigęs internetinis balsavimas, jis gali iš naujo balsuoti. Balsavus antrą kartą, pirmasis rinkėjo balsavimo biuletenis yra panaikinamas, tokiu būdu paliekant galioti tik paskutinį rinkėjo pateiktą elektroninį biuletenį. Šis procesas gali būti tęsiamas tol, kol vyksta internetinis balsavimas, o tai suteikia rinkėjui galimybę pačiam nuspręsti, kada jis jausis saugiai balsuodamas, ar apsisprendimo momentu bus išsaugotas balsavimo slaptumas.

Panaudojant šią schemą ir Lietuvos internetinių rinkimų sistemoje, automatiškai bus išvengiama grėsmių, susijusių su nuogąstavimais dėl balsavimo slaptumo. Mano nuomone, tai yra tikrai priimtinas ir teigiamas sprendimas, bet dažnai tenka išgirsti nuomonių, kad tuomet bus nuskriausti rinkėjai, kurie nesinaudos internetinių rinkimų sistema. Susidarys situacija, kai rinkėjai turės nelygias teises: balsuojantys internetu galės keisti savo pasirinkimą, o balsuojantys tik rinkimų apylinkėje to padaryti jau nebegalės. Tai galėtų tapti svariu argumentu, bet nepamirškime to, kad internetiniai rinkimai bus prieinami kiekvienam rinkėjui ir tik kiekvieno rinkėjo apsisprendimas, naudoti technologijas ar ne, lemia šio „pranašumo“ (jei taip galima pavadinti) atsiradimą. Jeigu rinkėjas nemoka naudotis kompiuteriu arba nenori naudoti internetinio balsavimo sistemos, tai visiškai nereiškia, kad yra ribojamos jo teisės ar kad kitam rinkėjui, naudojančiam internetinio balsavimo sistemą, yra suteikiamas pranašumas.

Jei aš vis dar neįtikinau skaitytojo, kad galimybė pakeisti savo balsą internetinio balsavimo sistemoje nėra pranašumas, tai paprašysiu jūsų pagalvoti apie atstumą, kurį jums reikia nueiti iki rinkiminės apylinkės balsavimo diena. Pagalvojote? Puiku. Sakykim, tas atstumas sudaro 1,5 kilometro, o jūsų draugų šeima gyvena kiek tolėliau ir jiems reikia įveikti 2,5 kilometrų atstumą. Ar jums yra suteiktas pranašumas? Manau visi

atsakysite – ne. Taip pat ir su internetiniu balsavimu: jei jums suteikta galimybė juo naudotis, bet jūs to nenorit daryti, tai tie, kurie jį naudoja, tikrai neįgauna daugiau teisių nei jūs.

Dažnai Lietuvoje pasigirsta nuomonių, kad internetinis balsavimas dar labiau paskatins tokį neigiamą reiškinį, kaip balsų pirkimas. Visuomenė yra įtikinta, kad „balsų pirkliai“ pasiims nešiojamus kompiuterius ir važiuos pas tas rinkėjų grupes, kurios yra pažeidžiamos dėl savo socialinės ir materialinės padėties arba yra priklausomos nuo svaigalų. Tokie rinkėjai bus labai lengvai įtraukiami į balsų pirkimo procesą, o tas procesas bus nebekontroliuojamas. Galima sakyti, kad taip ir įvyks, bet internetinis balsavimas tuo pačiu momentu ir sudaro galimybę balsų pirkimui, ir šią galimybę panaikina. Galimybė pakeisti savo balsą internetinio balsavimo laikotarpiu sukuria situaciją, kuomet „balso pirklys“ nebus šimtu procentų garantuotas, kad balsas atiteko jam, nes jis gali būti parduotas vėl ir vėl, o balsą parduodantis rinkėjas jaučia sentimentus tik pinigams.

Taigi, kaip jau buvo minėta anksčiau, internetinis balsavimas gali ne tik sudaryti problemų ir sukelti komplikacijų, bet tuo pačiu metu ir spręsti tas pačias problemas. Iš esmės atsiranda paradoksali situacija: internetinio balsavimo sistema, turinti vieną veikimo mechanizmą, gali būti traktuojama dvejopai – gerai arba blogai, o požiūris į sistemą priklauso tik nuo to, kas apie ją pasakoja ir kokius aspektus kaip pateikia. Čia kaip ir su vandens stikline, kuri iki pusės pripilta vandens. Vienas žmogus pasakys, kad stiklinė yra pustuštė, kitas – artipilnė, bet jie abu bus teisūs.

Galima teigti, kad visus anksčiau aptartus internetinio balsavimo sistemos trūkumus galima kompensuoti vienu paprastu faktu – internetinio balsavimo sistema nebus sistema, kuri momentaliai pakeis jau egzistuojančias tradicines rinkimų technologijas. Tai tiesiog tradicinės rinkiminės sistemos

Dažnai Lietuvoje pasigirsta nuomonių, kad internetinis balsavimas dar labiau paskatins tokį neigiamą reiškinį, kaip balsų pirkimas.

patobulinimas, kuris padės taupyti gyventojų laiką ir gyventojų lėšas, kurias jie naudoja vykdami į rinkimų apylinkes.

Kiekvienas rinkėjas galės nuspręsti, kaip jam balsuoti: internetu ar apylinkėje, o suabejojus internetinės sistemos saugumu ar pasikeitus nuomonei, rinkimų dieną galima bus nuvykti į balsavimo apylinkę ir užpildyti balsavimo biuletenį. Tokia galimybė būtų užtikrinama.

Siūloma nustatyti balsavimo eiliškumą ir viršenybę pagal šias balsavimo formas: balsavimas paštu – internetinis balsavimas – balsavimas rinkimų apylinkėje. Taigi, kaip matome, balsavimas rinkimų apylinkėje rinkimų dieną vis vien išlieka svarbiausiu ir visi balsai, atiduoti prieš tai, gali būti pakeičiami rinkimų dieną.

Šiuo metu Lietuvoje yra mėginama pradėti naudoti elektroninio balsavimo technologijas išankstiniam balsavimui. Vyriausybės posėdyje buvo pritarta, kad per išankstinį balsavimą gali būti naudojami elektroniniai terminalai, kurie supaprastintų balsų skaičiavimą bei padėtų išvengti balsų falsifikavimo. Trūkstant politinės valios įteisinti internetinį balsavimą ir tą valios trūkumą pateisinant gyventojų nepasitikėjimu internetiniu balsavimu, šių terminalų naudojimas jau yra milžiniškas žingsnis į priekį. Tikėtina, kad pradėjus naudoti terminalus, gyventojai palankiau žiūrės ir į internetinį balsavimą. Beje, Teisingumo ministerijos užsakymu 2015 metais atlikta apklausa parodė, kad daugiau nei pusė Lietuvos gyventojų pritaria internetiniam balsavimui.

Rašydamas paskutinius šios apžvalgos žodžius, noriu dar kartą atsiprašyti skaitytojų, kad neapžvelgiau technologinių internetinių rinkimų organizavimo ypatumų, bet manau, kad tai nėra pagrindinis internetinių rinkimų įgyvendinimo klausimas, kadangi sparčiai plintant naujoms technologijoms, keičiasi ir rinkimų sistemų sandara, ir jų panaudojimo galimybės. Tai, kad šiame straipsnyje nebuvo skiriama dėmesio technologinėms saugumo priemonėms, kurios yra būtinos užtikrinant elektroninių rinkimo sistemų techninį saugumą, visiškai nereiškia, kad šių priemonių nereikia arba jos yra nesvarbios. Jos yra labai svarbios, o bet kokios elektroninio balsavimo sistemos sukūrimas ir naudojimas turi būti grindžiamas, visu pirma, aiškiais ir tiksliai suformuluotais reikalavimais – kaip organizaciniais, taip ir techniniais.

Privalu užtikrinti, kad balsavimo sistema bei jos veikimo principai būtų skaidrūs ir visiškai suprantami rinkėjams, o to galima pasiekti tik viešinant ir reklamuojant tas sistemas, vykdant visuomenės švietimą bei pasitelkiant bendradarbiavimui visuomenines organizacijas, kurios galėtų atstovauti visuomenę.

Dėl kompiuterinių žinių stokos internetinio balsavimo mechanizmai gali būti nesuprantami tam tikroms visuomenės grupėms, o tai reiškia, kad bent jau kol kas šios sistemos gali būti naudojamos tik kaip pagalbinis mechanizmas, įgyvendinant rinkimus.

Internetinio balsavimo naudojimas rinkimų procese yra ne kas kita, kaip žmogaus asmeninio pasitikėjimo internetinio balsavimo sistema klausimas. Pasitikėjimas balsavimo sistema reiškia pasitikėjimą valdžia. Pasitikėjimas, kuris yra sunkiai įgyjamas, bet labai lengvai prarandamas. ■

KAIP LIETUVOJE ĮGYVENDINAMA E. VALDŽIA?

Simonas KLIMANSKIS

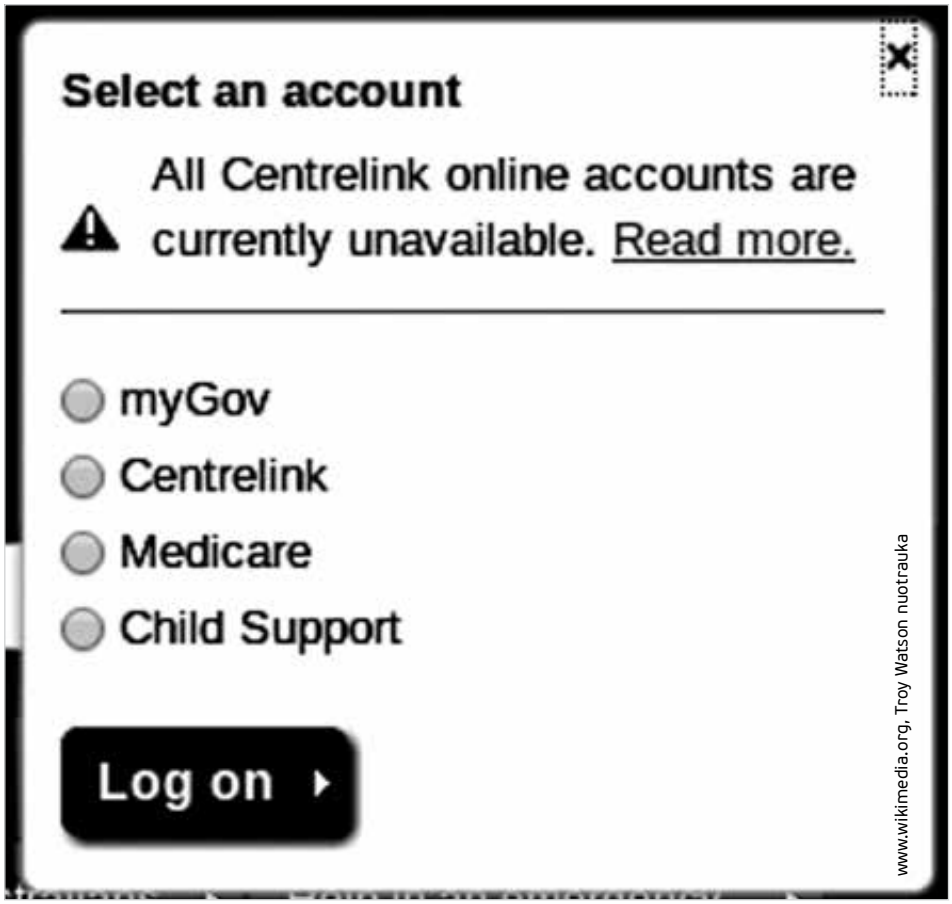
Sparčiai besivystančios informacinės technologijos visuomenei atvėrė naujas galimybes – sukūrė elektroninę erdvę, kur žmonės be jokių laiko ir atstumo suvaržymų gali tvarkyti savo kasdienius, darbo ar verslo reikalus. Būtent skaitmeninėje rinkoje glūdi didžiulis ekonominis potencialas – verslas gali lengviau ir greičiau įsisteigti, skaidriau ir efektyviau veikti, o vartotojai prekes ir paslaugas įsigyti iš kitų šalių ir už jas mokėti pigiau.

Visa tai iškėlė svarbų tikslą ir valstybei – pagal modernėjančios visuomenės lūkesčius modernizuoti viešąjį sektorių. Todėl 2002 m. pabaigoje Vyriausybė patvirtino Elektroninės valdžios koncepciją, kuria siekta padidinti vykdomosios valdžios sprendimų priėmimo skaidrumą, kokybiškiau ir efektyviau teikti visuomenei, verslui ir valstybės bei savivaldybių institucijoms viešąsias paslaugas ir informaciją, jas vieno langelio principu perkeliant į elektroninę erdvę. Maždaug po metų patvirtintas ir koncepcijos įgyvendinimo priemonių planas. Tai buvo elektroninės valdžios (e. valdžios) projekto pradžia.

Šioje koncepcijoje buvo užsibrėžtas svarbus uždavinys – pasiekti, kad iki 2005 m. visos viešojo administravimo institucijų paslaugos iki trečiojo lygio (t. y. galimybė vartotojui autentifikuotis, užpildyti ir pateikti paslaugai gauti reikalingas dokumentų formas) būtų perkeltos į internetą ar teikiamos kitais nuotoliniais būdais 24 valandas per parą, 7 dienas per savaitę (išskyrus tas, kurias teikiant privalo dalyvauti pats valstybės tarnautojas). Tai pavyko pasiekti tik iš dalies. 2005 m. buvo didelis atotrūkis tarp elektroninių paslaugų gyventojams pasiūlos, kuri siekė beveik 60 proc., ir jų vartojimo, kuris buvo įvertintas tik apie 15 proc. Visgi džiugina tai, kad nebuvo sustota, o e. valdžios projektai sparčiai vystomi iki šiol.

Kiti e. valdžios projekto elementai yra pateikti dar keliuose šiuo metu galiojančiuose programiniuose dokumentuose. Pirmiausia tai – Informacinės visuomenės plėtros 2014–2020 m. programa „Lietuvos Respublikos skaitmeninė darbotvarkė“, kuria numatomas tolesnis e. valdžios plėtojimas informacinės visuomenės kontekste, tam išnaudojant informacinių ir ryšių technologijų teikiamas galimybes. Kitas dokumentas – Viešojo valdymo tobulinimo 2012–2020 m. programa, kurioje yra vienas vienintelis punktas, susijęs su e. valdžia ir numatantis plėsti elektroninių paslaugų teikimą bei didinti jų prieinamumą.

Už visa tai yra atsakinga Vidaus reikalų ministerija. Būtent ši ministerija planuoja e. valdžios projektus ir koordinuoja jų įgyvendinimą, pagal kompetenciją dalyvauja koordinuojant informacinių ir ryšių technologijų naudojimą administracinėms ir viešosioms paslaugoms teikti. Tuo tarpu Susisiekimo ministerija formuoja valstybės politiką informacinės visuomenės plėtros srityje, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą. Šiame procese dalyvauja Informacinės



Sparčiai besivystančios informacinės technologijos visuomenei atvėrė naujas galimybes – sukūrė elektroninę erdvę, kur žmonės be jokių laiko ir atstumo suvaržymų gali tvarkyti savo kasdienius, darbo ar verslo reikalus.

www.wikimedia.org, Davidbravoortiz nuotrauka

E. valdžią galima apibūdinti kaip tinkamą skaitmeninių technologijų panaudojimą, siekiant kuo efektyviau teikti viešąsias paslaugas vartotojams.

visuomenės plėtros komitetas, kuris kaip institucija konkrečiai koordinuoja elektroninio turinio, informacinių ir ryšių technologijų infrastruktūros kūrimą, planuoja ir skirsto ES paramos lėšas šios srities projektams, atlieka projektų ekspertinį vertinimą, prižiūri projektų įgyvendinimą, renka statistinę informaciją tiek apie sukurtas e. paslaugas, tiek apie bendrą e. valdžios ir informacinės visuomenės statistiką. Kadangi informacinės visuomenės plėtra yra horizontali sritis, jos politikos planavime ir įgyvendinime dalyvauja ir kitos ministerijos (pavyzdžiui, e. sveikatos srityje – Sveikatos apsaugos ministerija, e. verslo srityje – Ūkio ministerija ir kt.).

Todėl išties pravartu apžvelgti, ką per tuos metus pavyko pasiekti, kas tebestringa, kokie tolesni planai. Taip pat įdomu palyginti, kokią vietą pagal e. valdžios išvystymo lygį užima Lietuva ES kontekste.

Pirmiausia reikėtų apsibrėžti, kas yra e. valdžia. Sąvokų yra įvairių – nuo siauros, susijusios su viešųjų paslaugų teikimų elektroniniais kanalais, iki plačios, apimančios įvairius informacinių ir ryšio technologijų diegimo aspektus. Tuo tarpu Europos Komisija e. valdžią apibrėžia kaip visumą viešajame administravime diegiamų informacinių ir telekomunikacinių technologijų, organizacinių pokyčių ir naujų įgūdžių, kurie naudojami tobulinant viešąsias paslaugas, demokratinius procesus ir viešąsias politikas. Taigi, e. valdžią galima apibūdinti kaip tinkamą skaitmeninių technologijų panaudojimą, siekiant kuo efektyviau teikti viešąsias paslaugas vartotojams.

Europos Komisija yra parengusi veiksmų planus, susijusius su informacinės visuomenės ir e. valdžios kūrimu bei modernizavimu, kuriais siekiama didinti viešųjų paslaugų efektyvumą ir prieinamumą ES vartotojams. Nuo 2001 iki 2011 m. Komisija, siekdama stebėti pažangą, kaip valstybės narės įgyvendina e. valdžios planus, koks yra e. valdžios išvystymo lygis ES ir dar keliose šalyse, atlikdavo tyrimus pagal metodiką, kuri paremta tuometinės Vidaus rinkos tarybos patvirtintu e. Europos 20 pagrindinių viešųjų paslaugų sąrašu (12 iš jų skirtos gyventojams, 8 – verslui). Tyrimo metu būdavo vertinama, koks yra kiekvienos iš 20 paslaugų perkėlimo į internetą lygis, saugumas (tapatybės nustatymas, abipusiškai pripažįstamas e. identifikavimas), patogumas (iš anksto užpildytų duomenų laukelių skaičius), skaidrumas, atskaitingumas (galimybė sekti proceso eigą), daugiakalbiškumas, integralumas (paslauga prieinama iš nacionalinio portalo), prieinamumas, pagalbos funkcija. Tam yra sukurta europinė interneto svetainių turinio brandos klasifikacija, kurioje išskirti penki viešųjų paslaugų perkėlimo į internetą lygiai:

Informacija – institucija savo interneto svetainėje pateikia paslaugai gauti reikiamą informaciją.

Vienpusė sąveika – institucija savo interneto svetainėje suteikia vartotojui galimybę gauti reikalingų dokumentų formas ir anketas, kurias užpildęs ir atsispausdinęs vartotojas gali pateikti į atitinkamas institucijas ne elektroniniu būdu.

Abipusė sąveika – nustačius vartotojo tapatybę, institucijos interneto svetainėje suteikiama galimybė užpildyti paslaugai gauti reikalingas dokumentų formas ir jas perduoti internetu, o institucija šio elektroninio dokumento pagrindu suteikia viešąją paslaugą, tačiau neelektronine forma.

Visiškas internetinis aptarnavimas – vartotojas gali internetu pateikti užklausą ir gauti galiojančią elektroninę viešąją paslaugą, nenaudojant jokių popierinių dokumentų formų procedūroms užbaigti.

Funkcionuojanti elektroninė

E. valdžią galima apibūdinti kaip tinkamą skaitmeninių technologijų panaudojima, siekiant kuo efektyviau teikti viešąsias paslaugas vartotojams.

procedūra arba personalizavimas – viešosios paslaugos teikiamos internetu automatiškai panaudojant buvusią vartotojo registraciją, duomenis apie vartotoją ir atsisakant pakartotinio duomenų įvedimo.

2010 m. buvo atlikta e. valdžios vertinimo metodikos peržiūra, atsižvelgiant į sparčią technologinę pažangą e. valdžios srityje, naujai nubrėžtas e. valdžios politikos įgyvendinimo ir vertinimo gaires. Esminis metodikos pakeitimas – atsisakyta 20 pagrindinių viešųjų paslaugų stebėsenos ir imta stebėti e. paslaugų teikimą pagal gyvenimo įvykius (pavyzdžiui, naujos įmonės steigimas, darbo netekimas, darbo paieška, automobilio registravimas ir kt.). Tyrime vertinami keturi kriterijai:

- *Orientacija į vartotoją* – parodo, kokiu mastu informacija apie paslaugą yra pateikta internete ir kaip ji suprantama.
- *Paslaugų aiškumas / skaidrumas* – parodo e. paslaugas teikiančių institucijų skaidrumą, kalbant apie jų pačių atsakomybę ir veiklos rezultatus, paslaugos suteikimo procesą ir asmeninių duomenų naudojimą, pavyzdžiui, ar yra paaiškinimai, ar vartotojas informuojamas apie e. prašymo gavima, jo būseną, apie sekančius proceso žingsnius ir pan.
- *Tarpvalstybinės paslaugos* – parodo, kokiu mastu Europos vartotojai gali naudotis e. paslaugomis kitoje šalyje.
- *Bendro naudojimo IT sprendimai* – leidžia nustatyti penkių techninių sprendimų, būtinų viešųjų e. paslaugų teikimui, prieinamumą (t. y. elektroninė identifikacija; elektroniniai dokumentai; autentiški šaltiniai; elektroninis seifas; prisijungimo mechanizmas, kai vienu vartotojo veiksmu vykdomas autentifikavimas ir autorizavimas (angl. – *Single Sign On* (SSO))).

PASIEKTA DIDELĖ PAŽANGA

Paskutinio Europos Komisijos užsakymu atlikto tyrimo pagal senąją metodiką duomenimis, 2010 m. bendras pagrindinių viešųjų paslaugų

PAGRINDINIŲ VIEŠŲJŲ IR ADMINISTRACINIŲ PASLAUGŲ GYVENTOJAMS IR VERSLUI PERKĖLIMO Į INTERNETĄ BRANDOS LYGIAI

Eil. Nr.	Paslauga	Aukščiausias galimas brandos lygis	2013 m. brandos lygis	2013 m. brandos proc.	Numatytas brandos lygis 2015 m.	Numatytas brandos proc. 2015 m.
Pagrindinės viešosios ir administracinės paslaugos gyventojams						
1	Pajamų mokesčio deklaravimas	5	5	100	5	100
2	Darbo vietų paieška	4	4	100	4	100
3	Socialinės apsaugos paslaugos			70		70
3.1	Nedarbo socialinio draudimo išmokos	4	2	50	2	50
3.2	Vaikų priežiūros išmokos	5	4	80	4	80
3.3	Stipendijos studentams	5	4	80	4	80
4	Asmens dokumentai			60		60
4.1	Pasas, asmens tapatybės kortelė	5	1	20	1	20
4.2	Vairuotojo pažymėjimas	5	5	100	5	100
5	Automobilių registravimas	4	4	100	4	100
6	Prašymai statybų leidimams gauti	4	3	75	4	100
7	Pranešimai policijai	3	3	100	3	100
8	Viešųjų bibliotekų paslaugos: katalogų prieinamumas	5	4	80	5	100
9	Pažymų (gimimo, santuokos liudijimų) užsakymas ir išdavimas	4	3	75	3	75
10	Priėmimas į aukštąsias mokyklas	4	3	75	3	75
11	Gyvenamosios vietos deklaravimas	4	4	100	4	100
12	Su sveikatos priežiūra susijusios paslaugos	4	4	100	4	100
Pagrindinės viešosios ir administracinės paslaugos verslui						
13	Socialinio draudimo įmokos	4	4	100	4	100
14	Pelno mokesčio deklaravimas	4	4	100	4	100
15	PVM deklaravimas	4	4	100	4	100
16	Naujo juridinio asmens įregistravimas	4	4	100	4	100
17	Duomenų teikimas statistikos biurams	5	5	100	5	100
18	Muitinės deklaracijos	4	4	100	4	100
19	Su aplinkosauga susiję leidimai	5	4	80	4	80
20	Viešieji pirkimai	4	4	100	4	100

perkėlimo į internetą brandos procentas Lietuvoje siekė 84 proc., iš kurio gyventojams skirtų paslaugų perkėlimas buvo 85 proc., verslui – 84 proc., ir buvo mažesnis už ES vidurkį (90 proc., iš kurio gyventojams skirtų paslaugų perkėlimas – 87 proc., verslui – 94 proc.). Pagal šį rodiklį Lietuva užėmė 23 vietą iš 32 Europos šalių (ES, Šveicarija, Islandija, Norvegija, Turkija). Visgi tokie rezultatai reiškia iš esmės pasiektą ketvirtą brandos lygį. Tuo tarpu tik keturios šalys – Airija, Malta, Austrija ir Portugalija – buvo visiškai perkėlusios viešąsias paslaugas į internetą – jų brandos procentas buvo lygus 100 proc. Kitaip tariant, ten, kur galima, pasiekusios penktą lygį.

Tiesa, Lietuvoje Informacinės visuomenės ir plėtros komitetas dar kurį laiką atliko e. paslaugų tyrimus pagal minėtą Europos Komisijos metodiką. Toks tyrimas paskutinį kartą buvo atliktas 2013 m. (1 lentelė).

Lyginant su 2010 m., 20-ties pagrindinių viešųjų paslaugų perkėlime į internetą yra matoma pažanga. 2013 m. bendras pagrindinių viešųjų paslaugų perkėlimo į internetą brandos procentas siekė 91 proc. 2015 metams numatyti paslaugų brandos lygiai yra pasiekti, ir šiuo metu brandos procentas sudaro 96 proc. Kaip matyti, labiausiai išvystytos verslui skirtos e. paslaugos. Tiesa, nuo 2017 m. įsigaliojus naujajam Civilinės būklės aktų registravimo įstatymui, visa informacija apie gyventojų gimimo, mirties ir santuokos faktus bus saugoma elektroninėje erdvėje, o popieriniai liudijimai bus išduodami tik asmenims pageidaujant. Tuomet brandos procentas padidės iki 97 proc.

Be abejo, e. valdžios išvystymo lygį padidintų elektroninio balsavimo projektas, dėl kurio šiuo metu diskutuojama. Tai užtikrintų didesnį rinkėjų aktyvumą, ypač tarp jaunimo ir užsienyje gyvenančių Lietuvos piliečių, sumažėtų balsavimo kaštai. Tačiau greta šio, bene vienintelio teigiamo argumento yra ir klausimų, susijusių su saugumo rizikomis, galimomis techninėmis problemomis, balsavimo privatumo užtikrinimu.

Pasauliniame kontekste pagal e. valdžios išvystymo lygį Lietuva tarp 193 šalių užima 29 vietą.

Kalbant apie e. valdžios išvystymo tyrimus pagal naująją metodiką, paskutinį kartą toks tyrimas 33 Europos šalyse (ES, Šveicarijoje, Norvegijoje, Islandijoje, Turkijoje ir Serbijoje) Europos Komisijos užsakymu buvo atliktas 2015 m. Rezultatai rodo, kad Europa nuosekliai žengia skaitmeninės brandos keliu – orientacijos į vartotoją požiūriu e. paslaugų pagal gyvenimo įvykius teikimo lygio vidurkis Europos šalyse, siekiantis 73 proc., yra vienas iš labiausiai pažengusių rodiklių. Per 2013–2014 m. jis paaugo 3 proc. Žvelgiant kitais pjūviais, taip pat matoma pažanga, tačiau nepakankama. Pavyzdžiui, informacijos apie teikiamas e. paslaugas (procesą, asmeninę informaciją ir kt.) teikimo lygio vidurkis per metus augo 3 proc., ir siekia tik 51 proc., o bendro naudojimo IT sprendimų taikymas išliko nepakitęs ir sudaro 50 proc. E. paslaugų tarpvalstybinis sąveikumas, nepaisant padarytos pažangos (4 proc. metinio padidėjimo), yra mažesnis nei vidutinis – tik 48 proc.

Konkrečiai daugelis Lietuvos rodiklių yra didesni už Europos vidurkius – e. paslaugų teikimo, aiškumo ir bendro naudojimo IT sprendimų taikymo lygiai siekia atitinkamai maždaug 55, 55 ir 60 proc. Tuo tarpu tarpvalstybinio sąveikumo teikiant e. paslaugas lygis tesiekia tik apie 35 proc.

Apibendrintai Lietuva yra priskiriama aukštą skaitmenizacijos lygį turinčių Europos šalių grupei kartu su Estija, Belgija, Kipru, Malta, Ispanija ir Portugalija ir lenkia kaimynes Latviją bei Lenkiją. O pasauliniame kontekste pagal e. valdžios išvystymo lygį Lietuva tarp 193 šalių užima 29 vietą. Taip pat tyrimo ataskaitoje atkreiptas dėmesys, kad inovacijų diegimas atliktas tinkamai ir efektyviai, viešojo administravimo institucijos pasižymi struktūruotu požiūriu diegiant inovatyvias technologijas bei procedūras.

VIS SVARBESNĖ KOKYBĖ, O NE VIEN KIEKYBĖ

Yra ir trūkumų. Pirmiausia tai vidutiniškas e. paslaugų naudojimas ir vartotojų pasitenkinimas e. paslaugomis. Šį faktą gerai iliustruoja tai, kad Lietuvoje yra išduota per milijoną kvalifikuotų elektroninio parašo sertifikatų, o jais naudojasi beveik penktadalis gyventojų. Tam įtakos turi žinių trūkumas, ypač tarp vyresnio amžiaus, turinčių žemesnį išsilavinimą, gaunančių mažesnes pajams, gyvenančių mažesniuose miestuose žmonių, nepakankamai greitas e. paslaugų teikimas, prastas pasirengimas tarpvalstybinėms paslaugoms / tarpvalstybiniam sąveikumui. Taip pat ne visų institucijų internetinės svetainės pritaikytos mobiliesiems įrenginiams. Skaičiuojama, kad Europoje vos 1 iš 4 viešojo sektoriaus portalų turi mobiliąją versiją, todėl prarandama dalis potencialių portalo naudotojų.

Taigi, Lietuvai reikia intensyviau vystyti tarpvalstybines e. paslaugas, pritaikyti institucijų portalus ir e. paslaugas mobiliesiems įrenginiams, aktyviau viešinti e. paslaugas ir skatinti gyventojus jomis naudotis bei toliau tobulinti teikiamas e. paslaugas, jas labiau pritaikant vartotojų poreikiams (pavyzdžiui, diegiant sąsajas su registrais, sudėtines paslaugas ir pan.), didinti gyventojų, ypač provincijoje gyvenančių, skaitmeninį raštingumą. Tai yra svarbiausi ateities darbai toliau vystant e. valdžią Lietuvoje. Yra pasiektas toks taškas, kada jau nebeužtenka viešąsias paslaugas perkelti į internetą. Vis daugiau dėmesio reikia skirti jų kokybei, efektyvumui ir saugumui. ■

SEMINARAS „VIENINGAI SKAITMENINEI EUROPOS RINKAI SAUGI SKAITMENINĖ TAPATYBĖ“.

Rita Vaitkevičienė, Valstybinės duomenų apsaugos inspekcijos (toliau VDAI) direktoriaus pavaduotoja

SANTRAUKA

Jeigu šiandien pažvelgsime į straipsnių laikračiuose antraštes ar mokslinių darbų temas, susidurime su naujais terminais, pvz., „skaitmeninė dienotvarkė,“ „skaitmeninė vieninga rinka,“ „skaitmeninė tapatybė,“ „duomenų saugumo pažeidimas,“ „kritinė infrastruktūra“ ir kt. Privačiame ir viešajame sektoriuose per pastaruosius penkerius metus tvarkomų duomenų kiekis išaugo 800 proc., net 71 proc. naudotojų turi prieigas prie duomenų, kurių jie neturėtų gauti[1]. Nei vienas privataus ar viešojo sektoriaus subjektas nėra apsaugotas nuo rizikos, kad nebus pažeidimo, tapatybės atskleidimo arba vagystės, asmens duomenų praradimo ar kitokių nemalonių aplinkybių.

Skaitmeninė tapatybė yra vienas iš labiausiai geidžiamų ir vertingų skaitmeninės aplinkos atributų, nuo skaitmeninės tapatybės (toliau – ID), skirtos pateikti prašymą ar registruotis, identifikavimo sprendimų iki griežtos skaitmeninės tapatybės nustatymo tvarkos sveikatos ir finansų sektoriuose. Ką iš tikrųjų reiškia sąvoka „skaitmeninė tapatybė,“ kaip užtikrinti skaitmeninės tapatybės saugumą, kaip padidinti Europos piliečių informuotumą, kad jie suprastų, jog tai ne tik technologijos ir kaip padrąsinti privatų sektorių ir valstybės institucijas bendradarbiauti su skaitmenine tapatybe susijusiais, ne tik su piliečių, bet ir su ekonomikos, politikos ir visuomenės interesais susijusiais klausimais. Šiais ir kitais klausimais buvo diskutuojama Lietuvos mokslų ir Europos Komisijos kartu su Aukšto lygio mokslinių konsultantų grupe organizuotame seminare „Vieningai skaitmeninei Europos rinkai saugi skaitmeninė tapatybė,“ kuris 2016 m. spalio 25–26 d. įvyko Vilniuje, Mokslų akademijoje. Rengiant šį straipsnelį buvo naudota seminaro metu gauta informacija.

2016 m. spalio 25–26 d. Vilniuje įvyko Lietuvos mokslų akademijos kartu su Europos Komisija organizuotas Kibernetinio saugumo seminaras „Vieningai skaitmeninei Europos rinkai saugi skaitmeninė tapatybė.“ Į Vilnių atvyko daugiau kaip dvidešimt įžymių Europos akademinėje visuomenėje žinomų mokslininkų, kibernetinio saugumo, technologijų, socialinių mokslų aukščiausio lygio ekspertų, į kuriuos kreipėsi Europos Komisijos viceprezidentas Andrus Ansip ir Komisijos narys Guenther Oettinger dėl nuomonės pateikimo. Daugiau kaip 75 seminaro dalyviai, Europos Komisijos Aukšto lygio mokslinių patarėjų grupės mokslininkai[2] (toliau tekste – Mokslininkų grupė), Europos Sąjungos šalių narių atstovai, dvi dienas diskutavo skaitmeninės tapatybės valdymo ir jos reikšmės vieningai skaitmeninei Europos rinkai klausimais.

Lietuvos mokslų akademijos didžiojoje salėje gausiai susirinkusius seminaro dalyvius pasveikino Lietuvos mokslų akademijos prezidentas prof. Valdemaras Razumas, pabrėžęs mokslininkų misiją, jos svarbą Europos Sąjungos plėtros politikai. Įvadinėje sesijoje kalbėję Aukšto lygio mokslinių patarėjų grupės nariai Pearl Dykstra, Orange įmonių grupės kibernetinio saugumo strategijos ir viešųjų ryšių direktorius Nicolas Arpagian, Seminaro pirmininkas, Europos branduolinių tyrimų organizacijos generalinis direktorius, keletos mokslų akademijų narys, Europos fizikų draugijos garbės narys, Vokietijos fizikų draugijos prezidentas, eksperimentinės fizikos (branduolio fizikos) profesorius Rolf-Dieter

Seminaro prezidiumas (iš kairės): prof. Dykstra Pearl, prof. Janusz Buinicki, prof. Pam Brigs ir prof. Michael Waidner.

[1] https://data.sailpoint.com/?gclid=COiyvt_kq80CFUgMcwodQSMKxw [žr. 2016-11-01].

[2] Aukšto lygio mokslinių konsultantų grupė pagal ES mokslinių konsultacijų mechanizmą teikia Europos Komisijai aukštos kokybės, aktualias ir nepriklausomas mokslines konsultacijas konkrečiais politikos klausimais. Šios konsultacijos yra ypač svarbios plėtojant ES politiką ir (arba) teisėkūros procese. Konsultacijos yra grindžiamos geriausiais, kokie yra galimi, moksliniais įrodymais. Grupę sudaro septyni aukščiausio kompetencijos lygio įvairių mokslo sričių atstovai, kurie teikia mokslines ekspertines konsultacijas įvairiais mokslo ir ES politikos klausimais. Tai Janusz M. Bujnicki, Pearl Dykstra, Elvira Fortunato, Rolf-Dieter Heuer, Julia Slingo, Cédric Villani, Henrik C. Wegener.

Heuer pabrėžė mokslininkų atsakomybę už skaitmeninės Seminaro tikslas buvo interaktyviu būdu motyvuoti ir diskusijose pasidalinti idėjomis rašant Europos Komisijai skirtą Mokslininkų grupės nuomonę dėl kibernetinio saugumo.

Seminaro dalyviai – teisininkai, informacinių sistemų, fizinių mokslų ir technologijų specialistai iš visų Europos Sąjungos šalių narių vadovaujami Aukšto lygio mokslinių patarėjų grupės mokslininkais R.-D. Heuer, P.Dykstra, N. Arpagian, Tarptautinio Varšuvos molekulinės ir ląstelių biologijos instituto Bioinformatikos ir proteinų inžinerijos laboratorijos (lenk., *Międzynarodowy Instytut Biologii Molekularnej i Komórkowej w Warszawie, Laboratorium Bioinformatyki i Inżynierii Bialka*) vadovu Janusz Bujnicki, Paryžiaus Henri Poincaré instituto direktoriumi Cédric Villani su grupe pranešėjų dvi dienas klausė pranešimų skaitmeninės tapatybės valdymo, pasitikėjimo temomis, diskutavo, kaip pasiekti pusiausvyrą tarp privatumo ir saugumo, saugumo ir pasitikėjimo skaitmeninėje erdvėje.

Tapatybės valdymas yra tarpdisciplininis dalykas. Sėkmingas asmens identifikavimas skaitmeninėje erdvėje turi didelę reikšmę ne tik įgyvendinant piliečių ir vartotojų teises naudotis skaitmeninėmis paslaugomis, bet ir verslui bei viešojo administravimo subjektams. Pranešėjai akcentavo tai, kad incidentai globaliame elektroninių ryšių tinkle sukelia realias grėsmes individų teisėms ir laisvėms. Asmens duomenų saugumas, saugus identifikavimas ir autentifikavimas elektroninėje erdvėje yra būtinos sąlygos siekiant skatinti verslo plėtrą, pritraukti investicijas, sudaryti sąlygas ekonomikos augimui, rūpintis socialinio teisingumo užtikrinimu. Tris – keturis pastaruosius metus grėsmingai didėjantis kibernetinių atakų bei kibernetinių incipentų skaičius elektroninių ryšių tinkluose taip pat turi reikšmės klientų pasitikėjimo e-vadžios, viešojo ir privataus sektorių teikiamomis paslaugomis lygiui.

Pirmojoje sesijoje kalbėję pranešėjai Roterdamo Erasmus Universiteto Erasmus socialinių mokslų ir žmogaus studijų aukštosios mokyklos dekanė prof. Liebest van Zoonen kalbėjo apie prieštaravimus tarp virtualaus ir fizinio identifikavimo, Talino technologijos universiteto prof. Ahto Buldas perskaitęs pranešimą tema „Reikalavimai skaitmeninei tapatybei vs dabartinei praktikai“ pakvietė diskutuoti skaitmeninės tapatybės tema. Pranešėjai ir diskusijų dalyviai pabrėžė, jog skaitmeninė tapatybė negali būti vertinama tik kaip technologinė kategorija, tai yra visas kompleksas skirtingų sprendinių. Iki naujos iniciatyvos „Vieninga Europos skaitmeninė rinka“ paskelbimo saugi skaitmeninė tapatybė buvo labiau reikalinga verslui, kuris skaitmeninę tapatybę vertina kaip minimalius reikalavimus, kuriuos turi įgyvendinti viešojo ir (arba) privataus sektoriaus subjektas vykdantis (vykdysiantis) veiklą elektroninėje erdvėje. Praktika patvirtina, jog skaitmeninė tapatybė yra daugialypė sąvoka ir priklauso nuo įvairių faktorių – pacientų, vartotojų ir (arba) kitų visuomenės grupių poreikių. Praktika patvirtina, jog tapatybei nustatyti kartais pakanka visai nedaug atributų, todėl nebūtina iš asmens reikalauti didelio duomenų rinkinio tapatybei patvirtinti.

Antroje dienos pusėje pirmininkaujant prof. Rolf-Dieter Heuer buvo atlikta skaitmeninės tapatybės SWOT analizė (Stiprybės, silpnybės, galimybės ir grėsmės). Saugi skaitmeninė tapatybė, užtikrinanti asmens teisę į privatų gyvenimą ir saugumą, yra šių dienų ekonomikos pagrindas, bet identiteto vagystės, profiliavimas, vartotojų sekimas internete bei neužtikrintas kibernetinis saugumas yra grėsmės, kurias būtina kiek galima sumažinti ir neutralizuoti. Įstatymų leidėjas privalo pasiūlyti sprendimą, kuris ne tik atitiktų ekonomikos poreikius, bet suteiktų piliečiams saugumo elektroninėje erdvėje jausmą, paskatintų juos naudotis viešojo ir privataus sektoriaus teikiamomis elektroninėmis paslaugomis.

Antrąją seminaro dieną buvo diskutuojama dviejose lygiagrečiose sesijose, 3-čiojoje sesijoje buvo kalbama tema „Privatumas ir saugumas“, 4-tojoje – „Saugumas ir pasitikėjimas“. Seminaro dalyviai kartu su informacinių technologijų saugumo ekspertu Frederic Jacobs, Liuveno katalikiško universiteto (pranc. *Katholieke Universiteit Leuven*) prof. Bart Preneel bei Veicmano (*Weizmann*) instituto prof. Adi Shamir aptarė būdus, kurie galėtų būti naudojami siekiant padidinti visuomenės pasitikėjimą technologijomis bei skaitmeninės tapatybės saugumu.

Pasitikėjimas yra pagrindinis faktorius. Nesant pasitikėjimo visuomenė nebendradarbiaus, vartotojai nesinaudos elektroninėje erdvėje teikiamomis paslaugomis, nebus ekonomikos augimo. Didinant duomenų saugumą kibernetinėje erdvėje, sudėtingesnė darosi ir vartotojo aplinka, sudėtingesnės prieigos galimybės. Nepakankamas duomenų saugumo užtikrinimas žmones atgrąso nuo technologijų. Kaip padidinti pasitikėjimą skaitmenine tapatybe, kaip rasti pusiausvyrą tarp duomenų saugumo ir draugiškos vartotojo aplinkos yra iššūkis ateičiai. Svarbiausias vaidmuo tenka gamintojui ir konkurencijai, tačiau reguliavimas nacionaliniame, o kai kuriais atvejais ir Europos Sąjungos lygmenyje yra reikalingas.

Seminaro pabaigoje buvo pateiktos pagal šio renginio dalyvių pasiūlymus suformuluotos išvados:

Transakcijos elektroninėje erdvėje taupo naudotojų laiką ir kitus išteklius. Pagrindinis faktorius turintis įtakos skaitmeninės ekonomikos vystymuisi – saugi asmens tapatybė elektroninėje erdvėje. Apsaugota skaitmeninė tapatybė būtina tam, kad individai pasitikėtų ir naudotųsi skaitmeninės ekonomikos produktais. Skaitmeninės tapatybės saugumo stiprinimas negalimas nedalyvaujant vartotojams. Vartotojai yra indikatorius. Tik jų elgesys parodo, yra pasitikėjimas elektroninėmis paslaugomis, arba jo nėra. Tapatybės valdymui labai svarbi savireguliacija, saugumo kriterijų nustatymas, atitikimo šiems kriterijams patvirtinimas, t.y. sertifikavimas. Ten, kur šios priemonės yra nepakankamos, reikalingas įstatymų leidėjo įsikišimas – t.y. teisėkūros priemonėmis turi būti nustatyti reikalavimai nacionaliniu, o kai kuriais atvejais ir Europos Sąjungos lygmenyje. ■