KIBERNETINIS SAUGUMAS IR DARBUOTOJŲ SAUGA IR SVEIKATA (DSS)

Reziumė

Šiame dokumente aptariamas naujas aspektas nagrinėjant kibernetinių grėsmių ir darbuotojų saugos ir sveikatos ryšį. Tai darant reikia atsiriboti nuo tradicinio požiūrio į kibernetinį saugumą, kuris yra orientuotas tik į techninius aspektus, ir diskusiją praplėsti, kad ji apimtų kibernetinių išpuolių sukeliamas žmogiškąsias ir socialines pasekmes.

Atsižvelgiant į tai, kad visose organizacijose vis dažniau diegiamos skaitmeninės technologijos, ir į didėjantį išpuolių prieš jų kompiuterines sistemas ir tinklus skaičių, reikia išnagrinėti darbuotojų saugai ir sveikatai kylančią naują riziką. Darbuotojų saugos ir sveikatos (DSS) srityje artimiausiais metais būtina n naujus poreikius ir spręsti naujus uždavinius.

Kibernetinio saugumo scenarijus

Per pastaruosius keletą metų kibernetinis saugumas tapo aktualia tema visų sektorių įmonėms. Kibernetiniai nusikaltimai tampa vis sudėtingesni, o kibernetiniai nusikaltėliai vykdydami išpuolius išnaudoja visų rūšių spragas, tiek fizines, tiek technines ar žmogiškąsias.

Kembridžo žodyne kibernetinis išpuolis apibrėžiamas kaip „neteisėtas bandymas pakenkti kieno nors kompiuterinei sistemai arba joje esančiai informacijai naudojantis internetu“[1]. Konkrečiau, pasak Nacionalinio standartų ir technologijų instituto (NIST), kibernetinis išpuolis – tai „išpuolis kibernetinėje erdvėje, nukreiptas į įmonės naudojamą kibernetinę erdvę, siekiant sutrikdyti, išjungti, sunaikinti arba kenkėjiškai kontroliuoti kompiuterinę aplinką / infrastruktūrą, arba sunaikinti duomenų vientisumą arba pavogti kontroliuojamą informaciją“[2].

Pasaulyje, kuris vis labiau skaitmeninamas, kibernetinio išpuolio rizika kyla kiekvienai įmonei. 2020 m. buvo kaip niekad ryški skaitmeninimo ir kibernetinio saugumo problema. Įmonės savo nustatytus organizacinius metodus vis labiau grindė lankstumu ir technologijomis, kad dirbtų nuotoliniu būdu, taip iš esmės buvo dėl COVID-19 pandemijos, tačiau ši situacija taip pat buvo palanki kibernetiniams nusikaltėliams ir buvo pasiektas toks lygis, kai 78 proc. organizacijų dėl perėjimo prie nuotolinio darbo patyrė daugiau kibernetinių išpuolių[3].

Viso pasaulio mastu 87 proc. organizacijų susidūrė su bandymu išnaudoti esamą spragą, o 71 proc. saugumo specialistų pranešė, kad nuo koronaviruso protrūkio pradžios padaugėjo kibernetinių grėsmių skaičius (duomenų viliojimas, kenkimo programinė įranga, išpirkos reikalavimo programinė įranga)[4].

Apskritai didėja ne tik išpuolių prieš kibernetinį saugumą skaičius, bet ir jų poveikis (ENISA, 2021a), o šalys kibernetinio saugumo problemas sprendžia naudodamos skirtingus išteklius ir priemones. Pavyzdžiui, remiantis konkrečiais veiksniais, tokiais kaip įsipareigojimas kibernetinio saugumo ir teisės aktų srityje, trys Europos šalys (Portugalija, Lietuva ir Slovakija) klasifikuojamos kaip turinčios didžiausią kibernetinio saugumo indeksą[5].

Besiplečiantis grėsmių spektras lėmė poreikį Europos Komisijai skubiai įgyvendinti veiksmingą ES skaitmeninio dešimtmečio kibernetinio saugumo strategiją[6], siekiant garantuoti saugų skaitmeninimą, šiuo tikslu didinant atsparumą, kuriant gebėjimus užkirsti kelią kibernetiniams incidentams ir į juos reaguoti, ir nustatant nuoseklią tarptautinę kibernetinę politiką. Be to, šioje strategijoje atkreipiamas

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/
[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/
[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

dėmesys į kibernetinio sąmoningumo programos svarbą visoms ES institucijoms, įstaigoms ir agentūroms kuriant veiksmingą kibernetinio saugumo kultūrą.

Dabartinės ir būsimos grėsmės

Tikimasi, kad kibernetinių nusikaltimų kaina pasauliniu mastu iki 2025 m. pasieks 10,5 trln. JAV dolerių per metus[7]. Iš tiesų kibernetinę erdvę kenkėjiškais tikslais ir skirtingais motyvais naudoja įvairūs subjektai – pradedant kibernetiniais nusikaltėliais, kurių pagrindinis motyvas yra finansinė nauda, baigiant kibernetiniais teroristais, kurie veikia vedini politinių ir ideologinių tikslų. Nusikaltimų internete sritis yra labai plati ir apima daugybę neteisėtų veiksmų, kurie jau žinomi fiziniame pasaulyje, pvz., tapatybės vagystė, sukčiavimas, šnipinėjimas, nusikaltimai intelektinei nuosavybei, taip pat kelios smurto internete formos (pvz., persekiojimas arba patyčios). Šie veiksmai gali būti grindžiami galingomis skaitmeninės srities priemonėmis, o dėl vis labiau tarpusavy susijusio pasaulio kibernetiniai nusikaltimai yra vienas iš pagrindinių rizikos veiksnių per artimiausius du dešimtmečius[8].

Kibernetinės grėsmės yra svarbus kiekvienos organizacijos ir šalies prioritetas atsižvelgiant į pasekmių įvairovę ir rimtumą: pradedant vertingos informacijos praradimu, baigiant kompiuterinių sistemų ir susijusių paslaugų paralyžiumi, taip pat didele rizika žmonių saugai ir sveikatai.

Kai kurių rūšių kibernetinių grėsmių (1 lentelė), nepaisant to, kad jos žinomos daugybę metų, pvz., duomenų viliojimas ir išpirkos reikalavimo programinė įranga, skaičius toliau didėja[9]. Iš tiesų, kibernetiniams nusikaltėliams šie nusikaltimai yra labai pelningi, o jų įvykdymo išlaidos yra labai mažos, palyginti su rizika, kad įsilaužėliai bus pagauti (Hernandez-Castro ir kt., 2020). Duomenų viliojimas išlieka vienas pagrindinių saugumo pažeidimų taktikos būdų (Verizon, 2021), tačiau iš kibernetinių išpuolių formų įvairovės matyti, kad padėtis kibernetinių grėsmių srityje yra labai sudėtinga. Pavyzdžiui, daugėja išpuolių prieš tiekimo grandines ir jos ateityje organizacijoms kels didelį susirūpinimą (ENISA, 2021b)[10].

1 lentelė. Kai kurios dažniausiai pasitaikančios kibernetinės grėsmės[11]

Rūšis	Aprašymas
Duomenų viliojimas ir tikslinis duomenų viliojimas	Duomenų viliojimas – tai apgaulingų pranešimų, kurie yra panašūs į pranešimus, paprastai e. paštu gaunamus iš patikimo šaltinio, siuntimo praktika. Taip siekiama pavogti neskelbtinus duomenis, pvz., informaciją apie kredito kortelę ir prisijungimo duomenis, arba aukos įrenginyje įdiegti kenkimo programinę įrangą. Duomenys gali būti viliojami įvairiomis formomis, pvz., naudojant tikslinį duomenų viliojimą, t. y. sudėtingesnę duomenų viliojimo versiją, kurios taikinys yra konkretus asmuo ar organizacija.
Kenkimo programinė programos ir išpirkos reikalaujančios programos	Kenkimo programos yra platus terminas, kuris vartojamas kenkimo programinei įrangai, pvz., šnipinėjimo programai, išpirkos reikalavimo programinei įrangai, virusams ir kirminams, apibūdinti. Išpirkos reikalaujančios programos, pvz., yra kenkėjiškos programinės įrangos forma, kuri užšifruoja aukos informaciją ir reikalauja sumokėti mokestį už iššifravimo raktą. Tai viena pelningiausių kibernetinio išpuolio rūšių.

[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/
[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] Tiekimo grandinė – tai „išteklių, reikalingų produktui sukurti, pagaminti ir paskirstyti, ekosistemos derinys“. Kibernetinio saugumo srityje tiekimo grandinė apima aparatinę įrangą ir programinę įrangą, debesiją arba saugojimą vietoje ir paskirstymo mechanizmus, https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Tai yra keletas dažniausiai pasitaikančių kibernetinių grėsmių, apie kurias pranešė ENISA (2020; 2021). Grėsmių aprašymą taip pat žr. https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Rūšis	Aprašymas
Socialinė inžinerija	Socialinė inžinerija – tai metodas, naudojamas žmonėms apgauti ir jais manipuliuoti siekiant gauti konfidencialią informaciją arba prieigą prie jų kompiuterio. Duomenų viliojimas (vagystė) yra socialinės inžinerijos pavyzdys
Paslaugos trikdymas (DoS)	Šios rūšies išpuoliai naudojami sistemoms, serveriams arba tinklams perpildyti tokiu intensyviu srautu, kad sistema negalėtų įvykdyti teisėtų užklausų. Įsilaužėliai taip pat gali naudoti įvairius pažeistus prietaisus šiai atakai pradėti (DDos, paskirstytojo paslaugos trikdymo ataka).
Duomenų saugumo pažeidimas	Duomenų saugumo pažeidimas yra saugumo incidentas, kurio metu informacija pavagiama, išimama iš sistemos arba panaudojama be leidimo.
Kibernetinis šnipinėjimas	Kibernetinio šnipinėjimo veiklos tikslas – pavogti neskelbtinus arba slaptus duomenis arba intelektinę nuosavybę, siekiant įgyti pranašumą prieš konkuruojančią įmonę arba vyriausybės subjektą.
Dezinformacijos ir klaidingos informacijos kampanijos	Dezinformacija – tai klaidingos informacijos kūrimas ir dalijimasis ja, siekiant sąmoningai sukelti žalą. Klaidingą informavimą sudaro netikros arba netikslios informacijos skleidimas atsitiktiniu būdu. Dezinformacija ir klaidinga informacija gali būti parengiamoji veikla kitiems išpuoliams, pvz., susijusiems su socialine inžinerija ir duomenų viliojimu, vykdyti ir naudojamos kartu su kitomis kibernetinėmis grėsmėmis.

Paradoksalu yra tai, kad, viena vertus, inovatyvios technologijos gali būti naudojamos naujiems kibernetinio saugumo sprendimams kurti; kita vertus, tos pačios technologijos suteikia papildomas galimybes patiems kibernetiniams nusikaltėliams. Taigi, greta teigiamo dirbtinio intelekto (DI) naudojimo, pvz., nustatant įsibrovimą ir kenkimo programinę įrangą (Truong ir kt., 2020), atsiranda naujos grėsmės, o tradicinės grėsmės dar labiau sustiprėja (Brundage ir kt., 2018). Pavyzdžiui, DI technologijos gali būti naudojamos automatizuotiems socialinės inžinerijos išpuoliams vykdyti, taip pat kenkimo programinės įrangos veiksmingumui didinti. Be to, plintant daiktų interneto prietaisams atsiranda papildomų pažeidžiamumų, nes jie turi silpnesnes duomenų apdorojimo ir saugojimo galimybes, todėl jų apsaugai skirtos saugumo programos yra ribotos[12].

Dėl konkrečios darbo aplinkos padidėjo galimybės kibernetiniams nusikaltėliams. Pavyzdžiui, nuotolinis darbas, kuris plačiu mastu pradėtas naudoti 2020 m. dėl COVID-19 pandemijos, sukėlė įmonėms naujų saugumo problemų, pvz., sukuriama daugiau galutinių taškų, kurie gali būti paveikūs saugumo pažeidimams, ir naudojami asmeniniai prietaisai, skirti su darbu susijusiai veiklai („BYOD – Bring Your Own Device“, liet. „atsineškite savo įrenginį“)[13]. Iš tiesų, viename prietaise labai patogu laikyti visus duomenis, tačiau dėl to kyla didelė rizika saugumui, kai, pvz., neapdairus elgesys, susijęs su privačiu skaitmeninių prietaisų naudojimu, tampa įpročiu verslo srityje (Disterer ir Kleiner, 2013). Jau nekalbant apie tai, kad skaitmeninio prietaiso praradimas reiškia riziką ne tik asmeninei, bet ir įmonės informacijai. Todėl dėl nuotolinio darbo kyla saugumo problemų įmonėms, kurios raginamos peržiūrėti savo organizacinę politiką ir investuoti į patikimą nuotolinių darbuotojų mokymą (Borkovich ir Skovira, 2020).

Taip pat įdomu pastebėti, kad patys darbuotojai, naudojantys dėvimuosius prietaisus (pvz., belaides ausines arba išmaniuosius laikrodžius), gali tapti lengvais kibernetinių nusikaltėlių taikiniais. Iš tiesų, dėvimosios technologijos kelia tam tikrą riziką kibernetiniam saugumui, pvz., su įmonės nešiojamuoju

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/
[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/

kompiuteriu sujungtų prietaisų atveju, per kuriuos į įmonės sistemą gali patekti virusai, taip pat riziką privatumui, kurią sukelia neteisėta prieiga (Heembrock, 2015).

Kitos naujos kibernetinės grėsmės kelia papildomą pavojų asmenims ir įmonėms, ir taip yra dėl didesnio poveikio, kurį lemia socialiniai tinklai. Pavyzdžiui, sintetinę vaizdakaitą sudaro skaitmeniniu būdu pakeista asmenų (dažnai įžymybių arba politikų) vaizdo ar garso rinkmena, siekiant kenkėjiškų tikslų, pvz., skleisti klaidingą informaciją ir pakenkti jų reputacijai. Tačiau nerimas dėl šių grėsmių neapima vien propagandos ir politinių rinkimų, nes jos taip pat gali daryti poveikį įmonėms dėl manipuliavimo rinka, prekių ženklo sabotažo, šantažo ir vykdomojo direktoriaus skaitmeninio tapatybės pasisavinimo (Westerlund, 2019).

Galiausiai atsižvelgiant į įspūdingą pažangą technologinių inovacijų srityje, manoma, kad kvantinė kompiuterija, kuri gali apdoroti informaciją daug veiksmingiau, palyginti su įprastais metodais, galėtų būti pradėta naudoti iki 2025 m.[14] Teoriškai šie kompiuteriai galėtų padėti įveikti daugumą dabartinių užšifravimo schemų, tačiau tam, kad šią technologiją būtų galima panaudoti praktiškai, reikalinga reikšminga technologinė pažanga[15].

Iš ką tik aprašyto scenarijaus aiškiai matyti, kodėl kibernetiniam saugumui kylanti rizika yra tarp pagrindinių kitų pasaulinio lygmens rizikos rūšių (WEF, 2021).

Kibernetinių išpuolių poveikis DSS

Kibernetiniai išpuoliai prieš įmones ir institucijas visada analizuojami technologiniu požiūriu, net jeigu žmogiškasis veiksnys yra vienodai svarbi kibernetinio saugumo problemos dalis (Corradini ir kt., 2020). Be to, nagrinėjant kibernetinių išpuolių poveikį, dėmesys visų pirma skiriamas ekonominiams aspektams (Cashell ir kt., 2004; Anderson ir kt., 2013) ir retai – darbuotojų saugai ir sveikatai. Iš tiesų, poveikis iš esmės vertinamas atsižvelgiant į materialias sąnaudas, pvz., duomenų praradimą ir verslo operacijų sutrikdymą, ir nematerialias išlaidas, pvz., konkurencinio pranašumo, susijusio su prarasta intelektine nuosavybe, praradimą ir žalą prekių ženklo reputacijai[16].

Kibernetiniai išpuoliai iš tiesų gali sukelti sužalojimus, psichologines problemas arba prarastas žmonių gyvybes, todėl akivaizdu, kad kibernetiniam saugumui kylančios rizikos vertinimas ir DSS rizikos vertinimas darbo vietoje turi būti laikomi ne atskira, bet kartu vykdoma veikla (Izuakor, 2016). Todėl įmonės turėtų atsižvelgti į įvairias pasekmes, susijusias su kibernetinėmis grėsmėmis, ir patvirtinti išsamesnį požiūrį į kibernetiniam saugumui kylančios rizikos valdymo optimizavimą (Couce-Vieira ir kt., 2020) kaip, pvz., aprašyta 2 lentelėje.

2 lentelė. Kibernetinio saugumo rizikos valdymo poveikio įvairovė

Kategorijos	Poveikis
Organizacija	Ekonominiai nuostoliai (pvz., mažesni gamybos mastai dėl neprieinamos paslaugos, rinkos dalies praradimo arba konkurencinio pranašumo praradimo)
	Žala reputacijai (pakenkta suinteresuotųjų subjektų pasitikėjimui)
	Kiti ekonominiai aspektai (pvz., kibernetinis draudimas)
Darbuotojai	Fiziniai sužalojimai (pvz., gyvybės praradimas dėl kibernetinės fizinės sistemos neveikimo)
	Psichikos sveikatos pažeidimai (pvz., nerimas arba susierzinimas)
	Poveikis asmens teisėms (privatumo pažeidimas, kurį lemia duomenų saugumo pažeidimas)
	Asmeninė ekonominė žala

[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution
[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html

Kategorijos	Poveikis
Kitos susijusios organizacijos	Žala dėl sutrikdytų pasaulinio tiekimo grandinės jungčių
Aplinka	Poveikis gamtos aplinkai (pvz., dėl kibernetinio incidento užteršta žemė)

Pritaikyta pagal Couce-Vieira ir kt. 2020.

Šios pasekmės gali būti susietos su pinigine išraiška išmatuojamomis išlaidomis, pvz., rinkos dalies praradimas, ir nepiniginėmis išlaidomis, pvz., fiziniai arba psichikos sveikatos sužeidimai.

Kitame skirsnyje bus aptarta galimų fizinių ir psichologinių pasekmių darbuotojų saugai ir sveikatai svarba.

Kibernetinio saugumo saugos aspektai

Prastas kibernetinio saugumo saugos aspektų įvertinimas galėtų būti susijęs su tuo, kad kibernetiniam saugumui kylanti rizika suvokiama kaip išorės grėsmė, o darbuotojų saugos ir sveikatos klausimai sprendžiami organizacijų viduje[17]. Tačiau, atsižvelgiant į kibernetinių grėsmių raidą ir didėjantį kibernetinių išpuolių poveikį organizacijoms, reikia parengti išsamų požiūrį į veiksmingą šių grėsmių ir poveikio valdymą, be kita ko, įskaitant darbuotojų saugos ir sveikatos užtikrinimą.

Dėl kibernetinių išpuolių rizika gali kilti ne tik organizacijos informaciniam turtui, grėsmė taip pat gali kilti darbuotojų fizinei ir psichikos sveikatai, kai įsilaužėliai vykdo išpuolius prieš ypatingos svarbos infrastruktūros objektus[18] arba perima jų technologinių prietaisų kontrolę. Pavyzdžiui, manipuliavimas įrenginiu gali sukelti fizinę žalą asmenims ir pakenkti asmens duomenims (Loukas, 2019).

Šį klausimą galima paaiškinti pateikiant keletą pavyzdžių. 2014 m. į Vokietijos plieno gamyklą įsilaužusiems įsilaužėliams pavyko išjungti krosnį[19]. Rizika, kad kibernetinis išpuolis virs kritiniu įvykiu, susijusiu su darbuotojų sauga ir sveikata, buvo labai didelė dėl naudojamų medžiagų pobūdžio.

2017 m. JAV maisto ir vaistų administracija (FDA) dėl saugumo spragų atšaukė apytiksliai 465 000 širdies stimuliatorių. Prietaisai turėjo spragų, dėl kurių į juos buvo galima įsilaužti, todėl pacientų gyvybėms kilo pavojus[20].

Kibernetiniai išpuoliai prieš pramonės kontrolės sistemas (PKS), kurias sudaro kibernetiniai ir fiziniai komponentai, kelia pavojų žmonių gyvybei. Pavyzdžiui, „Stuxnet“[21] – 2010 m. sukurtas kompiuterinis kirminas, siekiant perimti Irano centrifugų, naudojamų urano sodrinimui, kontrolę arba kenkimo programinė įranga „Triton“[22], kuri 2017 m. buvo susijusi su naftos chemijos infrastruktūra Artimuosiuose Rytuose, tačiau, laimei, nesuveikė. Šios rūšies išpuoliai taip pat gali sukelti rimtų pasekmių aplinkai.

Pavojingose situacijose naudojant nuotolinę įrangą, darbuotojų saugai ir sveikatai gali kilti pavojus, pvz., kai dėl sutrikusio belaidžio ryšio signalo arba įsilaužėlių išpuolių transporto priemonės arba mašinos gali tapti nekontroliuojamos (Steijn ir kt., 2016).

Gamybos sektoriuje, kai žmonės ir robotai kartu dirba gamybos linijose, dėl kibernetinių išpuolių galėtų sutrikti fiziniai pramoniniai procesai ir sužaloti darbuotojus (Perales Gómez ir kt., 2020).

Pasak Gartner, kibernetiniai įsilaužėliai iki 2025 m. operacines technologijas (OT) ir kitas kibernetines fizines sistemas gali pradėti sėkmingai naudoti kaip ginklus žmonėms kenkti ar žudyti[23].

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/
[18] Ypatingos svarbos infrastruktūros objektai yra gyvybiškai svarbūs šalies veikimui, atsižvelgiant į tai, kad šie objektai naudojami tokiuose sektoriuose kaip energetika, visuomenės sveikata, telekomunikacijos, bankai ir finansai.
[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362
[21] https://spectrum.ieee.org/the-real-story-of-stuxnet
[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/
[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece

Vykdydami kibernetinius išpuolius prieš ligonines, įsilaužėliai gali gauti prieigą prie visų pacientų ir darbuotojų neskelbtinos informacijos; tačiau, iš tiesų, didelė žala gali būti padaryta pacientų gebėjimui gauti tinkamą priežiūrą ir būtinas medicinines operacijas (Argaw ir kt., 2020)[24]. Pasaulinės išpirkos reikalavimo programinės įrangos „WannaCry“ išpuolio 2017 m. gegužės mėn. analizė parodė, kad jis sukėlė rimtų neigiamų pasekmių Didžiosios Britanijos nacionalinei sveikatos tarnybai (Ghafur ir kt., 2019).

Per COVID-19 pandemiją prieš JAV ligonines įvykdyta daugybė išpirkos reikalavimo programinės įrangos išpuolių, dėl kurių sutriko sveikatos priežiūra keliose ligoninėse, įskaitant didelį pavojų pacientų gyvybėms[25]. Iš mokslinių tyrimų, kuriuose daugiausia dėmesio skiriama išpirkos reikalavimo programinės įrangos naudojimui prieš sveikatos priežiūros organizacijas, matyti, kaip šios kibernetinės grėsmės gali sukelti su gyvybe ar mirtimi susijusių pasekmių (Ponemon, 2021).

Socialinis ir psichologinis poveikis

Kibernetiniai išpuoliai gali būti siejami su socialiniu poveikiu, pvz., pasitikėjimo skaitmeninėmis technologijomis praradimu, ir psichologiniu poveikiu, pvz., nerimu, pykčiu ir depresija (Bada ir Nurse, 2020). Nuo kibernetinių išpuolių nukentėję darbuotojai taip pat gali jausti gėdą, kaltę, sumišimą arba nusivylimą, ypač nutekėjus skaitmeninei informacijai, o šio poveikio mastas priklauso nuo to, kokioje aplinkoje buvo įvykdytas kibernetinis išpuolis (Agrafiotis ir kt., 2018). Pavyzdžiui, finansų įstaigoje, kurioje duomenų saugumo pažeidimo pasekmės, tikėtina, bus rimtesnės nei kitas paslaugas teikiančioje įstaigoje, psichologinė žala darbuotojams gali būti didesnė. Kraštutiniais atvejais duomenų nutekėjimo pasekmė gali būti susijusi su nukentėjusių asmenų savižudybėmis, nes viešai atskleidus informaciją apie juos jaučiama didelė gėda[26] – darbuotojams gali būti labai sunku pakelti psichologinę naštą.

Taigi privatumas ir saugumas tampa vis labiau tarpusavyje susiję: privatumas reiškia asmens duomenų rinkimą ir naudojimą, o saugumu siekiama garantuoti tų duomenų apsaugą[27]. Pagal 2018 m. gegužės 25 d. įsigaliojusį Bendrąjį duomenų apsaugos reglamentą (BDAR) organizacijos įpareigojamos Europos Sąjungoje užtikrinti duomenų apsaugą ir privatumą[28], o duomenų saugumo pažeidimų, kurie kelia riziką naudotojų teisėms ir laisvėms, atveju įmonės per 72 valandas privalo informuoti bent jau nuo pažeidimo nukentėjusius asmenis.

Įdomu stebėti, kaip privatumo pažeidimas gali sukelti neigiamas pasekmes asmenų psichikos sveikatai. Privatumas iš tiesų reiškia psichologinį poreikį, kuris yra griežtai susijęs su asmens tapatybės raida (Aboujaoude, 2019).

Iš kibernetinių nusikaltimų viktimizacijos tyrimų matyti neigiama įmonių ir asmenų patirtis (pvz., Augustina, 2015, ir McGuire ir Dowling, 2013). Organizacijoms nukentėjus nuo išpuolio, susijusio su išpirkos reikalavimo programine įranga, visų pirma nukenčia IT grupės dėl patirtos žalos profesiniam pasitikėjimui ir aukštam kvalifikuotų darbuotojų vertinimui[29]. Be to, tikėtina, kad išpirkos reikalavimo programinė įranga turės didesnį psichologinį poveikį darbuotojų emocijoms nei kiti saugumo incidentai, nes tuo atveju, kai įmonės sumoka išpirką, jos „apdovanoja“ įsilaužėlius, užuot investavusios pinigus į savo darbuotojus[30].

[24] 2020 m. Vokietijos ligoninė tapo kibernetinio išpuolio, dėl kurio ji negalėjo priimti atvykusių pacientų, auka. Moteris, kuri buvo vežama į šią ligoninę priežiūros paslaugoms suteikti, mirė pakeliui į artimiausią ligoninę, esančią už daugiau nei 30 km. Po tyrimo prokurorai priėjo prie išvados, kad įrodymų nepakako, tačiau žinoma, kad ligoninės skubiosios pagalbos skyrius buvo uždarytas būtent dėl su išpirkos reikalavimo programine įranga susijusio išpuolio. https://www.wired.co.uk/article/ransomware-hospital-death-germany

25 https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

[26] Pasimatymų svetainės „Ashley Madison“, į kurią buvo įsilaužta 2015 m. liepos mėn., yra dramatiškas pasekmes sukėlusio atvejo pavyzdys. Įsilaužėlių atskleisti duomenys apėmė vardus ir pavardes, slaptažodžius, adresus, taip pat informaciją apie klientų seksualinius troškimus. Dėl šio duomenų saugumo pažeidimo nemažai žmonių išėjo iš darbo, nutraukė santuoką ir nusižudė, https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

[28] https://gdpr.eu/tag/gdpr/

[29] https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

[30] https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

Papildomų pastabų galima pateikti dėl žmogiškosios klaidos, kuri laikoma pagrindine 90 proc. kibernetinių saugumo pažeidimų atvejų priežastimi[31]. Šios klaidos, kaip ir duomenų viliojimo e. laiškų atidarymas arba slaptažodžio valdymo taisyklių nepaisymas organizacijoms gali sukelti rimtų pasekmių, pvz., atsitiktinis kenkimo programinės įrangos įdiegimas įmonės tinkle. Galima lengvai įsivaizduoti nesėkmės jausmą, kurį patiria už atsitikusį įvykį atsakingi darbuotojai ir dėl kurio jie taip pat gali baimintis pranešti savo organizacijai apie padarytą klaidą.

Kalbant apie žmogiškąsias klaidas, pažymėtina, kad svarbu įvertinti psichologinius veiksnius, susijusius su kibernetinio saugumo incidentais: 52 proc. darbuotojų dažniau daro klaidas, kai patiria stresą, 43 proc. – kai yra pavargę ir 26 proc. – kai jaučiasi perdegę[32]. Jau nekalbant apie tai, kad kibernetinio saugumo specialistai jaučia didelį stresą arba perdegimą dirbdami tam, kad užkirstų kelią kibernetiniams išpuoliams arba sumažintų jų poveikį[33].

Galiausiai, taip pat pažymėtina, kad svarbu stebėti, kokį poveikį kibernetinis aspektas turi ir smurto reiškiniui. Pavyzdžiui, patyčios kibernetinėje erdvėje yra geriausiai žinoma priekabiavimo internete forma (Notar ir kt., 2013), siekiant pažeminti, persekioti ir kontroliuoti asmenį naudojant skaitmenines priemones. Net jei šis reiškinys nėra griežtai susijęs su kibernetinio saugumo sritimi, tokie išpuoliai kaip antai kenkimo programinė įranga ir tapatybės vagystė gali būti naudojami žmonėms pakenkti. Patyčios kibernetinėje erdvėje gali sukelti rimtų psichosomatinių, socialinių ir psichikos pasekmių (Dressing ir kt., 2014; Betts, 2016). Todėl, atsižvelgiant į tai, kad patyčios kibernetinėje erdvėje (Corradini, 2019; Farley ir kt., 2021) gali kelti pavojų darbuotojų saugai ir sveikatai, šį klausimą reikėtų tinkamai spręsti.

Kibernetinių išpuolių taikinys

Kiekviename darbo sektoriuje galime rasti inovatyvių technologijų. Visos organizacijos – labai mažos, mažosios ir vidutinės įmonės (MVĮ), taip pat didelės įmonės – gali tapti kibernetinių nusikaltėlių taikiniais, todėl joms gali grėsti kibernetiniai išpuoliai. Dauguma labai mažų ir mažųjų įmonių neturi apsisaugojimui būtinų išteklių, kaip matyti iš to, kad 43 proc. visų duomenų saugumo pažeidimų padaromi labai mažose ir mažosiose įmonėse (Verizon, 2019).

Akivaizdu, kad pasaulio skaitmeninimo mastas didėja, todėl įmonės tampa vis labiau susietos tarpusavyje, ir tai yra didesnių galimybių vykdyti išpuolius priežastis.

Nagrinėjant sektorius, kuriems gresia didžiausia kibernetinių išpuolių grėsmė, ir remiantis 2021 m. IBM saugumo ataskaita, finansų ir draudimo sektoriai 2020 m. patyrė daugiausia išpuolių, t. y. 23 proc. išpuolių, po jų ėjo gamybos (17,7 proc.), energetikos (11,1 proc.), mažmeninės prekybos (10,2 proc.), profesinių paslaugų (8,7 proc.), vyriausybės (7,9 proc.), sveikatos priežiūros (6,6 proc.), žiniasklaidos (5,7 proc.), transporto (5,1 proc.), švietimo (4,0 proc.) sektoriai.

Iš sektorių, kuriuose vykdomi kibernetiniai išpuoliai, raidos stebėsenos tyrimų matyti, kad sveikatos priežiūros sektorius tampa vis patrauklesniu taikiniu kibernetiniams nusikaltėliams[34], ypač dėl medicinos dokumentuose saugomos neskelbtinos informacijos (Martin ir kt., 2017). COVID-19 pandemija dar labiau apsunkino padėtį, todėl kibernetiniai nusikaltėliai savo dėmesį nukreipė į intelektinę nuosavybę, susijusią su vakcinų kūrimu (Muthuppalaniappan ir Stevenson, 2021) ir pradėjo siuntinėti su COVID-19 susijusius duomenų viliojimo e. laiškus[35]. Tačiau sveikatos priežiūros sektorius dėl kovos su pandemija iš esmės transformavosi ir, remiantis ateities įžvalgomis, jis privalo didinti savo atsparumą saugumo srityje[36].

Net ir švietimo įstaigos tampa patraukliu taikiniu kibernetiniams nusikaltėliams, atsižvelgiant į tai, kad 2020 m. 44 proc. įstaigų tapo išpirkos reikalavimo programinės įrangos taikiniais, o 35 proc. šių įstaigų sumokėjo išpirką, kad susigrąžintų savo duomenis[37]. Priežastys iš esmės yra susijusios su ribotais kibernetinio saugumo biudžetais ir didele naudotojų, pvz., studentų ir darbuotojų, baze, todėl išpuolių grėsmė gali padidėti. Be to, dėl mažo mokytojų ir studentų sąmoningumo mokymo programas reikia

[31] https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/
[32] https://www.tessian.com/research/the-psychology-of-human-error/
[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021
[34] https://cybersecurityguide.org/industries/healthcare/
[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home
[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective
[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/

pritaikyti daugiau dėmesio skiriant atsakingam skaitmeninių technologijų naudojimui (Corradini ir Nardelli, 2020).

Dabartinė padėtis, susijusi su kibernetiniais išpuoliais, nuolat kinta, todėl labai svarbu kasmet stebėti atnaujinimus. Kartu aiškėja dar didesnį susirūpinimą keliančios aplinkybės. Iš tiesų, išpirkos reikalavimo programinę įrangą kuriantys subjektai išbando naujus prievartavimo metodus, dėl kurių organizacijos bendradarbiauja ir dalijasi informacija, kad reaguotų į grėsmingą veiklą[38].

Viktimizacijos rizikos veiksniai

Kibernetiniai nusikaltėliai yra labiau suinteresuoti vykdyti išpuolius prieš įmones naudodami pavogtus slaptažodžius, o ne imtis masinių įsilaužimų siekiant gauti informacijos apie vartotojus[39]. Vis dėlto, 330 mln. suaugusiųjų 10 šalių 2020 m. susidūrė su kibernetiniais nusikaltimais[40], jau nekalbant apie tai, kad išpuoliai prieš konkrečius darbuotojus, pvz., naudojant tikslinį duomenų viliojimą, gali būti veiksminga strategija prieigai prie organizacijos gauti.

Rizika tapti įvairių formų kibernetinių nusikaltimų auka priklauso nuo asmeninių ir aplinkos veiksnių (Jansen ir kt., 2017), o aukų profilių tyrimas gali padėti geriausiai suprasti kibernetinių išpuolių ir aukų kilmės ryšį.

Pavyzdžiui, analizuojant kibernetinių nusikaltimų aukų kartas, atrodo, kad jaunimui (jaunesniam nei 25 metų) ir vyresnio amžiaus asmenims (75 metų ir vyresniems) kyla didesnė kibernetinių išpuolių grėsmė[41]. Lytis yra svarbus veiksnys, darantis įtaką su kibernetiniu saugumu susijusiam elgesiui (Anwar ir kt., 2017), nors tolesni tyrimai šioje srityje, įskaitant tyrimus dėl demografinių ypatumų, gali duoti labai įdomių rezultatų, susijusių su prevencine veikla. Iš kai kurių tyrimų matyti, kad moterys dažniau susiduria su duomenų viliojimo išpuoliais (Darwish ir kt., 2012), o kiti tyrimai atskleidžia, kad moterys, kitaip nei vyrai, labiau nerimauja dėl privatumo socialiniuose tinkluose (Tifferet, 2019).

Galiausiai, atsižvelgiant į poreikį didinti darbo vietų aplinkos atsparumą kibernetinėms grėsmėms, būtų įdomu išanalizuoti, kokį poveikį organizaciniai veiksniai, pvz., taisyklės ir procedūros, daro tikimybei, kad darbuotojai taps duomenų viliojimo ar tikslinio duomenų viliojimo aukomis (Williams ir kt., 2018). Tokia plataus masto analizė gali suteikti naudingų įžvalgų, susijusių su sąsajos dizaino tobulinimu ir darbuotojų sąmoningumo programomis.

Siekiant išsamaus požiūrio į kibernetinį saugumą: sąmoningumo vaidmuo

Kibernetinių grėsmių ir darbuotojų saugos ir sveikatos ryšys kelia ypač dinamiškų iššūkių organizacijai, todėl jos raginamos integruoti kiekvieną būtiną priemonę į bendrą įmonės požiūrį į kibernetinį saugumą[42].

Šiuo požiūriu reikia derinti darbuotojų saugos ir sveikatos aspektus, kurie dėl teisės aktuose nustatytų ribų, interesų ir praktinių klausimų paprastai laikomi atskiromis koncepcijomis (Boustras ir Waring, 2020).

Siekiant šio tikslo, svarbų vaidmenį atlieka įvairių suinteresuotųjų subjektų sąmoningumas ir jo reikėtų siekti atsižvelgiant į kibernetinį saugumą ir DSS, kurie tarpusavyje yra glaudžiai susiję.

Iš tyrimų, susijusių su kibernetinio saugumo klausimais, matyti, kaip dėl prastos atitikties saugumo ir kitiems organizaciniams veiksniams, pvz., nepakankamų atsako priemonių, organizacijoms kyla kibernetinių išpuolių pavojus (Hart, 2019). Be to, nepaisant darbo sektorių įvairovės, prastas darbuotojų sąmoningumas kibernetinio saugumo klausimais yra pagrindinė daugybės kibernetinio saugumo incidentų priežastis[43]. Taigi, sąmoningumo kibernetinio saugumo klausimais programos gali atlikti

[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021
[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport
[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report
[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511
[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

svarbų vaidmenį organizacijose kuriant veiksmingą kibernetinio saugumo kultūrą (Corradini, 2020) ir užkertant kelią kibernetiniams išpuoliams (Aldawood ir Skinner, 2018).

Didinant sąmoningumą apie galimas kibernetinių išpuolių pasekmes DSS srityje, daugiau dėmesio reikia skirti rizikos šaltiniams, į kuriuos paprastai neatsižvelgiama darbuotojų saugos ir sveikatos srityje. Teigiama DSS rizikos valdymo patirtis taip pat gali būti puikus įkvėpimo šaltinis, nes, palyginti su kibernetinio saugumo sritimi, sveikatos ir saugos organizacijoje tema remiasi ilgamete patirtimi, o daugelis taikomųjų programėlių ir programų, skirtų saugesnei darbo aplinkai kurti, ir toliau sėkmingai įgyvendinamos. Žmogaus klaidų valdymas taip pat laikomas gyvybiškai svarbiu siekiant užkirsti kelią nelaimingiems atsitikimams DSS srityje.

Be to, atsižvelgiant į tai, kad IT saugumo tarnybos / departamentai / specialistai paprastai nėra susipažinę su DSS, o DSS bendruomenė nėra susipažinusi su kibernetinėmis grėsmėmis, labai svarbu užtikrinti bendradarbiavimą šiose dviejose srityse. Pavyzdžiui, DSS, žmogiškųjų išteklių ir IT saugumo padalinių bendradarbiavimas organizacijoje, kai tai įmanoma, gali sudaryti sąlygas kibernetinės grėsmės klausimą vertinti įvairiais požiūriais ir įgyvendinti veiksmingesnius, inovatyvesnius prevencinius sprendimus.

Suinteresuotųjų subjektų sąmoningumo didinimas

Atsižvelgiant į tai, kas aptarta pirmiau, pirmas žingsnis yra informuoti įvairius suinteresuotuosius subjektus apie DSS riziką, susijusią su kibernetinėmis grėsmėmis, kad jie pradėtų veikti atsakingai.

Sąmoningumo didinimo programos gali būti ypač naudingos, tačiau tam, kad jos būtų veiksmingos, jos turi būti gerai parengtos ir tinkamai pritaikytos prie konkrečių situacijų, kad būtų tinkamos įvairiems suinteresuotiesiems subjektams. Jose taip pat turėtų būti nustatytas priemonių ir metodikos, pvz., kampanijų, praktinių seminarų, konferencijų, švietimo medžiagos ir kitos komunikacinės veiklos, rinkinys. Be to, atsižvelgiant į labai mažų įmonių ir MVĮ ypatumus ir jų ribotus išteklius, siekiant joms padėti, reikėtų nustatyti konkrečias iniciatyvas.

Sąmoningumo didinimo programose turėtų dalyvauti bent šie vidaus ir išorės suinteresuotieji subjektai:

- **Darbdaviai**, kurie teisiškai atsako už savo darbuotojų saugą ir sveikatą, taip pat **vadovai** yra pagrindiniai subjektai, prisiimantys lyderių vaidmenį organizacijose. Pagal darbuotojų saugą ir sveikatą reglamentuojančius teisės aktus darbdaviai turi plataus masto pareigas apsaugoti savo darbuotojus nuo visų darbe kylančių rizikos veiksnių ir veiksmingai juos valdyti. Kadangi kibernetinės grėsmės gali daryti poveikį darbuotojų saugai ir sveikatai, į jas reikėtų aiškiai atsižvelgti vykdant DSS rizikos prevencijos ir valdymo veiklą.
- **Darbuotojus** būtina informuoti apie bet kokią riziką jų saugai ir sveikatai, su kuria darbuotojai gali susidurti savo profesinėje veikloje, ir šiai rizikai turėtų būti priskirti kibernetinės rizikos veiksniai, todėl akivaizdu, kad informacijos teikimas ir darbuotojų mokymas šiuo konkrečiu klausimu yra esminė prevencijos priemonė.
- **DSS specialistai** turėtų būti įtraukti į sąmoningumo iniciatyvas, nes jiems paprastai trūksta žinių apie kibernetinį saugumą. Jie galėtų atlikti svarbų vaidmenį užkertant kelią kibernetinių išpuolių poveikiui darbuotojų saugai ir sveikatai, ir jiems reikėtų pateikti naujausią informaciją apie su organizacija susijusių aplinkybių raidą ir atitinkamą kibernetiniam saugumui kylančią riziką.
- **Darbo inspekcijos**. Atsižvelgiant į naujus kibernetinių grėsmių iššūkius, susijusius su DSS, tikriausiai reikės naujų metodų ir priemonių, kad darbo inspekcijos galėtų vykdyti savo funkcijas. Todėl tikrinimo ir prevenciniais tikslais labai svarbu turėti žinių apie DSS rizikos, susijusios su kibernetinėmis grėsmėmis, veiksnius.
- **IT saugumo valdytojai**. Jie dažnai nėra susipažinę su kibernetinio saugumo aspektais atsižvelgiant į tai, kad dėl savo darbo pobūdžio jie daugiausia dėmesio skiria tinklo ir duomenų saugumui ir veiksmingos savo organizacijos IT politikos kūrimui ir valdymui. Didesnis jų sąmoningumas šiuo klausimu galėtų padėti paskatinti bendradarbiavimą su DSS specialistais ir integruoti papildomą požiūrį į saugumo taisyklių ir praktikos apibrėžimą organizacijose.

Atsižvelgiant į tai, kad su kibernetiniu saugumu susijusi rizika apima darbuotojų saugą ir sveikatą, kitų rūšių suinteresuotieji subjektai turėtų būti informuoti apie kibernetinio saugumo pasekmes DSS ir jie

taip pat turėtų prisidėti rengiant prevencijos strategijas. Tarp jų, pvz., žmonių ir kompiuterių sąveikos (HCI) specialistai ir programinės įrangos kūrėjai.

Žmonių ir kompiuterių sąveika yra tarpdalykinė tyrimų sritis, kuri visų pirma buvo orientuota į naudotojų ir kompiuterių sąveiką, o dabar apima daugybę informacinių technologijų kūrimo formų[44]. Atsižvelgiant į tai, kad darbo įranga vis dažniau bus sujungta į tinklą, šios srities specialistų tinkamai suprojektuota žmonių ir kompiuterių sąsaja bus labai svarbi siekiant kuo labiau sumažinti poveikį kibernetiniam saugumui ir DSS (Korfmacher, 2019).

Be to, **programinės įrangos kūrėjai** gali atlikti svarbų vaidmenį atsižvelgiant į tai, kad vis didesnė darbingo amžiaus gyventojų dalis, nesvarbu, jie dirba namuose ar nuotoliniu būdu, savo veiklą vykdo naudodami programinės įrangos sistemas. Todėl svarbu didinti programinės įrangos kūrėjų sąmoningumą apie kibernetinių išpuolių poveikį darbuotojų saugai ir sveikatai, siekiant užtikrinti atidų šių sistemų projektavimą ir įgyvendinimą atsižvelgiant į jų pajėgumus apsisaugoti nuo kibernetiniam saugumui kylančios rizikos, nes tai turės teigiamą poveikį darbuotojų gerovei ir padės jiems jaustis apsaugotais nuo išpuolių.

Apibendrinant galima teigti, kad pagrindinė rekomendacija yra įtraukti **žmogaus elgsenos specialistus** į kibernetinio saugumo sąmoningumo didinimo programų kūrimą ir įgyvendinimą. Iš tiesų, tokių iniciatyvų sėkmė priklauso nuo dalyvių motyvacijos, taip pat nuo įgyvendinimui naudojamų metodų ir priemonių. Todėl reikalingi tinkami įgūdžiai ir žinios, susijusios su žmogaus elgsena.

Galiausiai kibernetinis saugumas visų pirma yra žmogaus problema. Todėl veiksmingam jo valdymui bus vis labiau reikalingesnės tarpdalykinės komandos, kuriose derinami techniniai, žmogiškieji ir socialiniai įgūdžiai.

Tolesni veiksmai

Būsimi tyrimai turėtų būti orientuoti į abiejų aptartų sričių, t. y. kibernetinio saugumo ir DSS, tarpusavio sąsajas. Poreikių ir spragų nustatymas padės nustatyti galimą kibernetinių išpuolių riziką darbuotojams, taip pat apibrėžti tinkamas politikos ir prevencijos strategijas organizacijose. Literatūroje jau aptarti susidomėjimą keliantys saugos ir sveikatos ryšiai, pvz., teigiamas saugumo kultūros, pasitenkinimo darbu ir saugumo reikalavimus atitinkančios elgsenos ryšys (Green ir D'Arcy, 2010).

Dabartiniai moksliniai tyrimai, kuriuose nagrinėjamas kibernetinio saugumo ir saugos rizikos ryšys, iš esmės orientuoti į sveikatos priežiūros sektorių (pvz., Martin ir kt., 2017) ir į autonomines transporto priemones (pvz., Taeihagh ir Lim, 2019), o reikia atlikti daugiau tyrimų, siekiant išsiaiškinti visas įmanomas kibernetinių išpuolių pasekmes darbuotojų saugai ir sveikatai kiekviename darbo sektoriuje.

Be to, atsižvelgiant į tai, kad įterptosios kompiuterinės sistemos ateityje bus naudojamos vis plačiau, būtinai reikės užtikrinti tinkamą saugos ir sveikatos integraciją. Iš tiesų šios sistemos galėtų būti suprojektuotos taip, kad padėtų siekti saugumo tikslų (pvz., apsisaugoti nuo įsilaužėlių išpuolių) ir garantuotų saugos funkcijas, išvengiant žalos naudotojams (darbuotojams). Saugos ir sveikatos integracija yra aktuali tema rengiant ypatingos svarbos misijų sistemas[45], o tarptautiniai standartai gali būti naudingas pagalbos šaltinis organizacijoms[46].

Galiausiai galima daryti prielaidą, kad mišrios darbo formos, kurias taikant derinamas darbas namuose ir biure, ateityje bus naudojamos vis platesniu mastu. Tą patį galima pasakyti apie daiktų interneto technologijomis ir kibernetinėmis fizinėmis sistemomis pagrįstą darbo aplinką (Podgórski ir kt., 2017). Todėl organizacijoms reikės atnaujinti savo rizikos vertinimą siekiant nustatyti bet kokį potencialų pavojų savo darbuotojams, kad būtų galima imtis tinkamų priemonių. Siekiant šio tikslo reikės įgyvendinti naujus metodus ir priemones.

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction
[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/
[46] Žr., pvz., ISO/TR 22100-4, Mašinų sauga, ryšys su ISO 12100 – 4 dalis Gairės mašinų gamintojams nagrinėjant su IT saugumu (kibernetinis saugumas) susijusius aspektus; IEC TR 63074:2019 „Mašinų sauga – saugumo aspektai, susiję su veikiančiomis darbuotojų saugos ir sveikatos kontrolės sistemomis".

Baigiamosios išvados

Skaitmeninė transformacija yra nesustabdomas procesas, neatsiejamas nuo kelių uždavinių, kuriuos turi spręsti kiekviena šalis. Dabar kibernetinis saugumas kelia didelį susirūpinimą visų dydžių ir sektorių įmonėms bei institucijoms ir šis susirūpinimas ateityje tik didės.

Tačiau kibernetinio saugumo valdymo negalima apriboti vien technologine sistemų ir informacijos apsauga. Kadangi kibernetiniai išpuoliai taip pat gali daryti poveikį darbuotojų saugai ir sveikatai, organizacijos turėtų įgyvendinti visapusišką požiūrį į kibernetinį saugumą. Siekiant šio tikslo, **reikia patvirtinti tarpdalykinę viziją, kurioje**, siekiant valdyti įvairias kibernetines grėsmes, **integruojami techniniai ir socialiniai įgūdžiai**.

Kalbant apie dideles organizacijas, ypač rekomenduojama bendradarbiauti IT saugumo ir DSS funkcijas vykdantiems pareigūnams apibrėžiant inovatyvų rizikos vertinimo procesą, siekiant apsaugoti materialųjį ir nematerialųjį turtą ir, svarbiausia, žmones. Kartu reikia spręsti svarbų klausimą – kaip labai mažoms įmonėms ir MVĮ, kurios dažnai neturi specialių vidinių išteklių[47], tačiau nuolat susiduria su kibernetinės grėsmės pasekmėmis, įgyvendinti veiksmingas strategijas.

Ateityje reikės spręsti labai sudėtingus uždavinius. Visų pirma reikia parengti patikimą ir plataus masto sąmoningumo didinimo šiais klausimais programą, siekiant parengti darbdavius, darbuotojus ir DSS bendruomenę, taip pat IT saugumo valdytojus ir kitus susijusius subjektus, pvz., žmonių ir kompiuterių sąveikos specialistus, programinės įrangos kūrėjus ir žmogaus elgsenos specialistus, vis labiau skaitmeninamai visuomenei ir kibernetinių grėsmių didėjimui.

Autoriai: Isabella Corradini, „Themis“ mokslinių tyrimų centro (Italija) mokslinė direktorė,

Projektą administravo: Emmanuelle Brun, Annick Starren, padedant Ana Cayuela, Europos darbuotojų saugos ir sveikatos agentūra (EU-OSHA).

Šį diskusijoms skirtą dokumentą užsakė Europos darbuotojų saugos ir sveikatos agentūra (EU-OSHA). Jo turinys, įskaitant visas pateiktas nuomones ir (arba) išvadas, yra tik autorių ir nebūtinai atspindi EU-OSHA nuomonę.

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

Literatūros sąrašas

E. Aboujaoude (2019), „Protecting privacy to protect mental health: The new ethical imperative“, *Journal of Medical Ethics*. *45*(9), p. 604–607.

I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese ir D. Upton (2018), „A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate“, *Journal of Cybersecurity*, *4*(1).

H. Aldawood ir G. Skinner (2018), „Educating and raising awareness on cyber security social engineering: A literature review“, skelbiama *IEEE International Conference on Teaching, Assessment, and Learning for Engineering* (TALE), IEEE, p. 62–68.

R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore ir S. Savage (2013), „Measuring the cost of cybercrime“, skelbiama R. Böhme (red.) *The economics of information security and privacy* (p. 265–300). Springer-Verlag.

M. Anwar, W. He, I. Ash, X. Yuan, L. Li ir L. Xu (2017), „Gender difference and employees' cybersecurity behaviors“, *Computers in Human Behavior*, 69, p. 437–443.

S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacey, M. V. Florin, F. Calcavecchia, D. Anderson, W. Burleson, J. M. Vogel, C. O'Leary, B. Eshaya-Chauvin ir A. Flahault (2020), „Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks“, *BMC Medical Informatics and Decision Making, 20*(146).

J. R. Augustina (2015), „Understanding cyber victimization: Digital architectures and the disinhibition effect“, *International Journal of Cyber Criminology*. *9*(1), p. 35–54.

M. Bada ir J. R. C. Nurse (2020), „The social and psychological impact of cyber-attacks, psychology“, skelbiama V. Benson ir J. Mcalaney (red.), *Emerging cyber threats and cognitive vulnerabilities* (p. 73–92), *Academic Press*.

L. R. Betts (2016), „Cyberbullying: Approaches, consequences, and interventions“, skelbiama J. Binder (red.), *Palgrave studies in Cyberpsychology*, *Palgrave Macmillan*.

D. J. Borkovich ir R. J. Skovira (2020), „Working from home: Cybersecurity in the age of covid-19“, *Issues in Information Systems*. *21*(4), p. 234–236.

G. Boustras ir A. Waring (2020), „Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context“, *Safety Science*, 132.

M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel ir kt. (2018), *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.* https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

B. Cashell, W. D. Jackson, M. Jickling ir B. Webel (2004), „The Economic Impact of Cyber-Attacks“, *CRS Report for Congress*.

I. Corradini (2020), *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology, Springer*.

I. Corradini (2019), *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking, Themis*.

I. Corradini, E. Nardelli ir T. Ahram (red.) (2020), *Advances in human factors in cybersecurity*, AHFE 2020, „Advances in Intelligent Systems and Computing“, 1 219 tomas, *Springer*.

I. Corradini ir E. Nardelli (2020), „Developing digital awareness at school: A fundamental step for cybersecurity education“, skelbiama I. Corradini, E. Nardelli ir T. Ahram (red.) *Advances in human factors in cybersecurity*, AHFE 2020, „Advances in intelligent systems and computing“, 1 219 tomas, *Springer*.

A. Couce-Vieira, D. R. Insua ir A. Kosgodagan (2020), „Assessing and forecasting cybersecurity impacts“, *Decision Analysis, 17*(4), p. 356–374.

A. Darwish, A. El Zarka ir F. Aloul (2012), „Towards understanding phishing victims' profile“, *International Conference on Computer Systems and Industrial Informatics*, p. 1–5.

G. Disterer ir C. Kleiner (2013), „BYOD - Bring Your Own Device“, *HMD*, 50, p. 92–100.

H. Dressing, J. Bailer, A. Anders, A. Wagner ir C. Gallas (2014), „Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims“, *Cyberpsychology, Behavior, and Social Networking,* 17: p. 61–67.

ENISA. (2020), *Grėsmių padėtis 2020 m.* https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2021a), Grėsmių padėtis 2021 m., 2021 m. spalio 27 d. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b), Išpuolių prieš tiekimo grandines grėsmių padėtis, 2021 m. liepos 29 d. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

S. Farley, I. Coyne ir P. D'Cruz (2021), „Cyberbullying at Work: Understanding the influence of technology“, skelbiama P. D'Cruz, E. Noronha, G. Notelaers ir C. Rayner (red.), *Handbooks of workplace bullying, emotional abuse and harassment*, 1 tomas, *Springer*.

S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi ir P. Aylin (2019), „A retrospective impact analysis of the WannaCry cyberattack on the NHS“, *NPJ Digital Medicine*, *2*(98).

J. H. Hamlyn-Harris (2017), *Three reasons why pacemakers are vulnerable to hacking.* The Conversation. http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

D. V. Hart (2019), „Factors influencing the adoption of cybersecurity situational awareness programs“, *Isaca Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

M. Heembrock (2015), „The risks of wearable tech in the workplace“, *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

J. Hernandez-Castro, A. Cartwright ir E. Cartwright (2020), „An economic analysis of ransomware and its welfare consequences. Royal Society Open Science“, 7(3), 190023.

C. Izuakor (2016), „Understanding the impact of cyber security risks on safety. ICISSP 2016 - 2nd International Conference on Information Systems Security and Privacy“.

J. Jansen, M. Junger, J. Kort, R. Leukfeldt, S. Veenstra, J. van Wilsem, ir S. van der Zee (2017), „Victims“, skelbiama R. Leukfeldt (red.), *Research agenda. The human factor in cybercrime and cybersecurity*, *Eleven International Publishing*.

G. Kavallieratos, S. Katsikas ir V. Gkioulos (2020), „Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey“, *Future Internet*, *12*(4), p. 65.

S. Korfmacher (2019), „The relevance of cybersecurity for functional safety and HCI“, skelbiama V. Duffy (red.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science*, 11581, *Springer.*

G. Loukas (2019 m. lapkričio mėn.), „Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0“, https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

G. Martin, P. Martin, C. Hankin, A. Darzi ir J. Kinross (2017), „Cybersecurity and healthcare: How safe are we?“, *British Medical Journal* (*Clinical research ed.*), 358, j3179.

M. McGuire ir S. Dowling (2013), „Cybercrime: A review of the evidence. Summary of key findings and implications (Home Office Research Report, 75)“, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

M. Muthuppalaniappan ir K. Stevenson (2021), „Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health“, *International Journal for Quality in Health Care*, *33*(1).

C. E. Notar, S. Padgett ir J. Roden (2013), „Cyberbullying: A review of the literature“, *Universal Journal of Educational Research, 1*(1), p. 1–9.

Á. L. Perales Gómez, L. Fernández Maimó, A. Huertas Celdrán, F. J. García Clemente, M. Gil Pérez ir G. Martínez Pérez (2020), „SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry“, *Software: Practice and Experience 51(3),* p. 607–627.

D. Podgórski, K. Majchrzycka, A. Dąbrowska, G. Gralewicz ir M. Okrasa (2017), „Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies“, *International Journal of Occupational Safety and Ergonomics*, *23*(1), p. 1–20.

Ponemon (2021), „The impact of ransomware on healthcare during covid-19 and beyond“, https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

N. Stacey, P. Ellwood, S. Bradbrook, J. Reynolds, H. Williams ir L. David (2018), *Key trends and drivers of change in information and communication technologies and work location. Foresight on new and emerging risks in OSH.* Europos darbuotojų saugos ir sveikatos agentūra https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

W. Steijn, J. van der Vorm, E. Luiijf, R. Gallis ir D. van der Beek (2016 m. rugsėjo 6 d.), „Emergent risks to workplace safety as a result of IT connections of and between work equipment“, *TNO report*.

A. Taeihagh ir H. S. M.Lim (2019), „Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks“, *Transport Reviews*, 39, p. 103–128.

S. Tifferet (2019), „Gender differences in privacy tendencies on social network sites: A meta-analysis“, *Computers in Human Behavior*, 93: p. 1–12.

T. C. Truong Q. B. Diep ir I. Zelinka (2020), „Artificial Intelligence in the Cyber Domain: Offense and Defense“, *Symmetry, 12*(3), 410.

Verizon (2019), 2019 m. duomenų saugumo pažeidimų tyrimo ataskaita, https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon (2021), 2021 m. duomenų saugumo pažeidimų tyrimo ataskaita, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

WEF (2021), „These are the top cybersecurity challenges of 2021“, https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

M. Westerlund (2019), „The emergence of deepfake technology: A review“, *Technology Innovation Management Review, 9*(11), p. 40–53.

E. J. Williams, J. Hinds ir A. N. Joinson (2018), „Exploring susceptibility to phishing in the workplace“, *International Journal of Human-Computer Studies*, 120, p. 1–13.