KRAŠTO APSAUGOS MINISTERIJA

Finansuoja Europos Sąjunga
NextGenerationEU

NAUJOS KARTOS LIETUVA

2026

Kibernetinis saugumas ir verslas

Ką turėtų žinoti kiekvienas įmonės vadovas

Turinys

Įvadas

Per pastaruosius metus skaitmeninė transformacija iš esmės pakeitė verslo įmonių veikimo principus – informacija tapo viena svarbiausių verslo vertybių, o informacinės technologijos – neatsiejama ir kritiškai svarbia infrastruktūra, užtikrinančia sklandų kasdienės veiklos vykdymą. Tokios skaitmeninės paslaugos ir informacinių technologijų sprendimai kaip elektroninis paštas, elektroninė bankininkystė, debesija, finansų ir klientų duomenų valdymo sistemos suteikia verslo įmonėms galimybę veikti efektyviau, sparčiau ir lanksčiau. Vis dėlto, kartu su naujomis technologinėmis galimybėmis neišvengiamai atsiranda ir naujos grėsmės.

Šiandien kibernetinis saugumas nebėra vien tik informacinių technologijų padalinio rūpestis, tai strateginė verslo sudedamoji dalis, tiesiogiai susijusi su veiklos tęstinumu, klientų ir darbuotojų pasitikėjimu bei verslo įmonės reputacija. Kibernetiniai incidentai gali lemti ne tik duomenų praradimą, konfidencialios informacijos atskleidimą ar finansinius nuostolius, bet ir pasitikėjimo verslo įmonėmis mažėjimą, trumpalaikius ar ilgalaikius veiklos sutrikimus bei teisines pasekmes. Net ir trumpalaikiai verslo įmonių sistemų veiklos sutrikimai gali reikšmingai paveikti įmonės konkurencingumą. Be to, vis daugiau organizacijų privalo prisitaikyti prie griežtėjančių teisinių ir reguliacinių reikalavimų, tokių kaip Bendrasis duomenų apsaugos reglamentas[1] (toliau – BDAR) ar Lietuvos Respublikos kibernetinio saugumo įstatymas[2], į kurį buvo perkelta TIS 2 direktyva[3], kurie įpareigoja ne tik užtikrinti duomenų apsaugą, bet ir gebėti pagrįsti taikomų saugumo priemonių veiksmingumą.

Smulkioms ir vidutinėms verslo (toliau – SVV) įmonėms verta skirti ypatingą dėmesį, nes praktika rodo, kad būtent šios įmonės dažnai tampa kibernetinių atakų taikiniais. SVV įmonės yra patrauklios piktavaliams dėl dažnai ribotų investicijų į kibernetinį saugumą, nepakankamo darbuotojų pasirengimo bei neišplėtotų saugumo procesų.

Pažymėtina, kad kibernetinio saugumo srityje vis didesnę reikšmę įgauna žmogiškasis faktorius. Darbuotojų neatsargumas, silpni slaptažodžiai, nepakankamos bazinės kibernetinio saugumo žinios sudaro palankias sąlygas socialinės inžinerijos metodais vykdomoms atakoms. Kibernetinis saugumas kuria vertę, jei įmonės darbuotojai yra sąmoningi, kritiški, suvokia savo veiksmų vertę bei laikosi kibernetinės higienos principų. Kibernetinis saugumas turėtų būti suvokiamas kaip kiekvieno darbuotojo atsakomybė, o tam būtinas ne tik įmonės vadovų, bet ir visų darbuotojų įsitraukimas, edukacija, žinių atnaujinimas.

Pagrindinis vadovo „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas?“ (toliau – Vadovas) tikslas – aptarti SVV įmonėms kylančias grėsmes bei pateikti praktines rekomendacijas, padedančias stiprinti įmonės kibernetinį atsparumą. Pirmasis Vadovas buvo paskelbtas 2020 m. Jame pristatyti apklausos rezultatai, atskleidę SVV įmonių kibernetinio saugumo sąmoningumo lygį. Siekiant įvertinti, kaip per laikotarpį nuo 2020 m. iki 2025 m. pasikeitė verslo įmonių požiūris ir vertinimas kibernetinio saugumo srityje, buvo atlikta nauja apklausa, o jos rezultatai pateikiami atnaujintoje Vadovo versijoje.

---

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Nuoroda: https://eur-lex.europa.eu/eli/reg/2016/679/oj/lit

[2] Lietuvos Respublikos kibernetinio saugumo įstatymas. Nuoroda: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

[3] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva). Nuoroda: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32022L2555

/01/

Kas yra kibernetinis saugumas?

Kas yra kibernetinis saugumas?

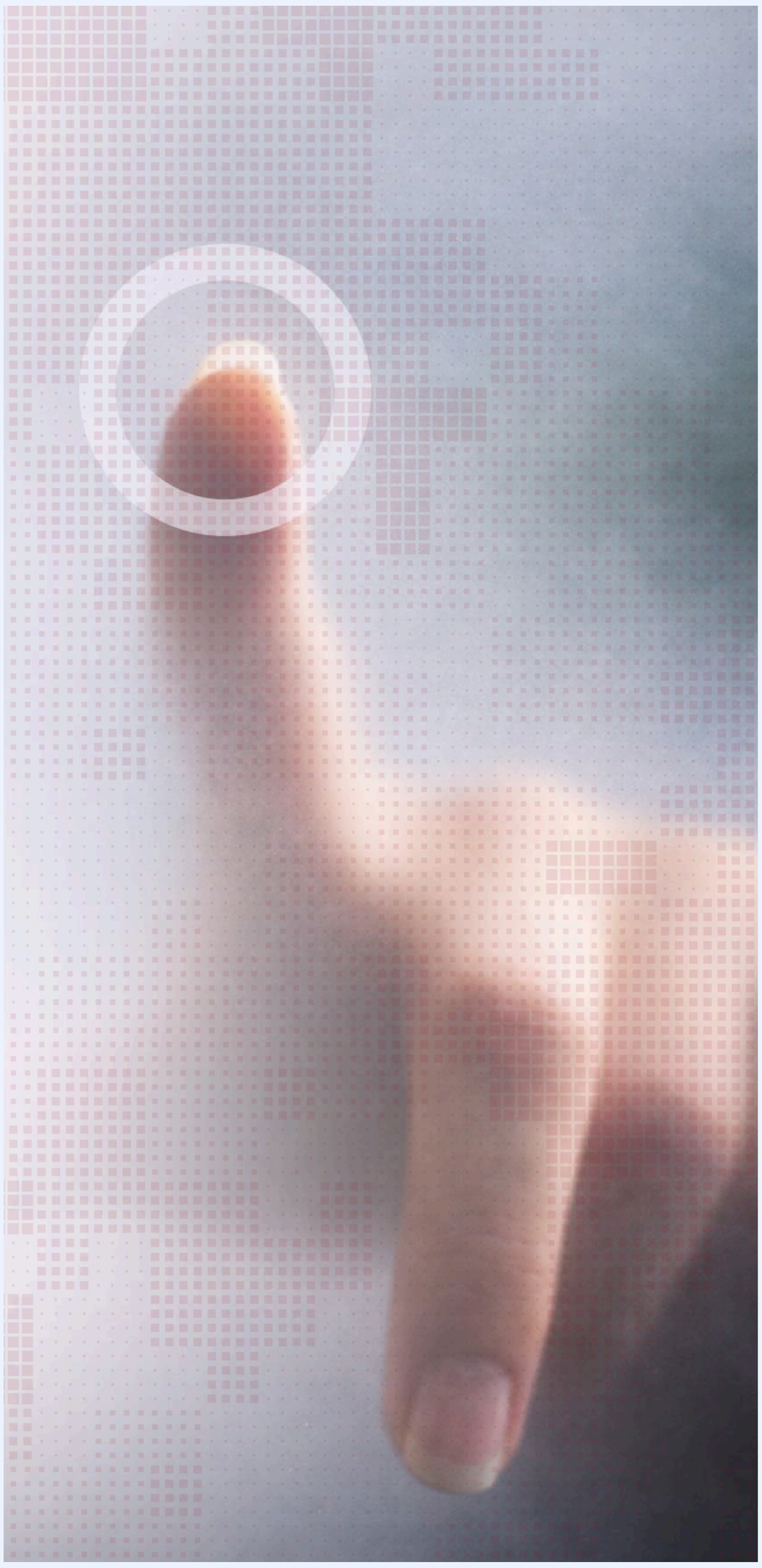
Kibernetinis saugumas – tai taisyklių, priemonių ir veiksmų visuma, skirta apsaugoti skaitmeninę informaciją, tinklus, informacines sistemas bei teikiamas paslaugas. Paprastai tai reiškia, kad turime užtikrinti:

- **Konfidencialumą** (angl. *Confidentiality*) užtikrinimas, kad visi jautrūs vidiniai įmonės ar verslo partnerių duomenys yra pasiekiami tik asmenims, kurie tiesiogiai dirba su šiais duomenimis.
- **Vientisumą** (angl. *Integrity*) užtikrinimas, kad visi vidiniai įmonės duomenys išlieka patikimi, nepakeisti, nesugadinti ar nėra ištrinti.
- **Pasiekiamumą** (angl. *Availability*) užtikrinimas, kad įgalioti vartotojai bei sistemos gali pasiekti duomenis ir juos naudoti.

Kibernetinio saugumo politikos dokumentai nustato pagrindines taisykles darbuotojams, pvz. kaip saugoti slaptažodžius, naudoti įrenginius, dalintis duomenimis ir pan. Antra, procedūros nustato aiškią veiksmų seką, pvz. kaip pranešti apie kibernetinį incidentą. Trečia, technologiniai sprendimai padeda automatizuoti ir įgyvendinti dokumentuose aprašytas taisykles, pvz. realizuoja prieigos prie duomenų kontrolę, šifruota duomenis.

Kuriant saugią verslo aplinką būtina suprasti, kad kibernetinio atsparumo stiprinimas nėra baigtinis veiksmas. Tai nuolatinis procesas, kurio metu, pasitelkiant žmogiškuosius išteklius, technologijas bei organizacinius procesus, išvystomas reikalingas kibernetinio saugumo lygis.

- **Žmonės – svarbiausia gynybos linija**. Piktavaliai dažniau taikosi į įmonės darbuotojus nei į sistemas – tai patvirtina statistika, rodanti, kad socialinės inžinerijos atakos yra vienos populiariausių. Kiekvienas darbuotojas atlieka svarbų vaidmenį užtikrinant kibernetinį saugumą. Siekiant paruošti darbuotojus galimoms kibernetinėms atakoms, būtina organizuoti reguliarius mokymus, didinančius sąmoningumą, skatinti pranešti apie įtartinus laiškus ar jų priedus, skambučius iš nežinomų numerių bei kitas įtartinas situacijas.
- **Dokumentuota kibernetinio saugumo politika**. Parengta ir dokumentuota kibernetinio saugumo politika suteikia įmonei aiškumo ir nuoseklumo, nes apibrėžia veiksmų seką ir atsakingus asmenis. Joje nustatoma, kaip elgtis kibernetinio incidento atveju, kaip užtikrinti veiklos tęstinumą ir kokių saugumo taisyklių laikytis kasdienėje veikloje. Dokumentuota kibernetinio saugumo politika padeda užtikrinti, kad darbuotojai žinotų, kaip elgtis kasdienėse ir kritinėse situacijose.
- **Technologijos**. Technologijos yra neatsiejamai susijusios su kiekvienos įmonės veikla, todėl svarbu užtikrinti, kad jos būtų tinkamai valdomos, prižiūrimos ir naudojamos, laikantis saugumo principų. Tai užtikrinama reguliariai atnaujinant programinę įrangą, naudojant patikimas ir licencijuotas programas, taikant prieigos prie duomenų ir sistemų kontrolę, saugiai konfigūruojant įrenginius, vykdant veiklos stebėseną bei pasenusios įrangos ar laikmenų saugų sunaikinimą. Šie veiksmai padeda užtikrinti, kad kasdien naudojami įrankiai nesukeltų papildomų kibernetinio saugumo rizikų.



Kodėl svarbu užtikrinti kibernetinį saugumą?

Remiantis draudimo bendrovės „Hiscox“ ataskaita[4], 2024 m. net ir pačios mažiausios įmonės (iki 10 darbuotojų) vidutiniškai patyrė 35 kibernetines atakas, o vidutinio dydžio organizacijos (nuo 50 iki 249 darbuotojų) – 53. Nors 2025 m. statistika yra pozityvesnė, visgi įmonės saugumui skiria 11–20 % nuo IT biudžeto, o 94 % vadovų planuoja šias investicijas didinti.

Nusikaltėliai vis rečiau taikosi į konkrečias įmones. Šiandien dominuoja automatizuoti dirbtinio intelekto (toliau – DI) įrankiai, kurie leidžia piktavaliams vienu metu skenuoti ir atakuoti tūkstančius taikinių visame pasaulyje. Dėl šios priežasties bet kuri įmonė, turinti interneto puslapį, duomenų bazę ar bet kokią prie tinklo prijungtą įrangą, automatiškai tampa potencialiu kibernetinės atakos taikiniu, nepriklausomai nuo jos dydžio ar veiklos sektoriaus. 2025 m. Europos Sąjungos (toliau – ES) teisėsaugos bendradarbiavimo agentūros (toliau – EUROPOL) ataskaitoje[5], pateikiama informacija apie DI įrankių naudojimo proveržį, kuomet atakos vis dažniau kuriamos naudojant specializuotus DI sprendimus, gebančius savarankiškai analizuoti tinklus ir vykdyti tūkstančius įsilaužimų be tiesioginio žmogaus dalyvavimo. Be to, neteisėtai gauti duomenys vis dažniau tampa preke, kuri siūloma tiek nukentėjusioms įmonėms, tiek konkurentams.

Svarbu pabrėžti, kad kibernetinis saugumas neapsiriboja tik įmonės duomenų apsauga. Įmonės skaitmeninė infrastruktūra gali tapti tiltu, per kurį piktavaliai pasiekia verslo partnerių sistemas. Kuo platesnis partnerių tinklas, tuo didesnė atsakomybė tenka įmonei – viena spraga įmonės sistemoje gali sukelti grandininę reakciją visoje tiekimo grandinėje. Atsakingas požiūris į duomenų apsaugą ir sistemingas rizikų valdymas ne tik saugo įmonės turtą, bet ir stiprina jos reputaciją kaip patikimos įmonės. Ignoravus šias rizikas, kyla pavojus prarasti esminį verslo kapitalą – klientų ir partnerių pasitikėjimą, be kurio tvari plėtra ir tolimesnis įmonės veiklos gyvavimas skaitmeninėje erdvėje tampa sudėtingi arba neįmanomi.

Teisinis reguliavimas taip pat daro įtaką įmonės kibernetinio saugumo politikos nustatymui. Įmonės, siekiančios bendradarbiauti su kitomis įmonėmis, kurioms taikomas Kibernetinio saugumo įstatymas, privalo pačios atitikti aukštesnius, nei įprasta, kibernetinio saugumo standartus. Tai reiškia, kad kibernetinis saugumas tampa ne tik vidiniu pasirinkimu, bet ir būtina sąlyga norint sėkmingai veikti rinkoje bei palaikyti strategines partnerystes.

Taigi, kibernetinis saugumas turėtų būti nuosekliai integruojamas į įmonės procesus ir kasdienę veiklą, nes užtikrina verslo tęstinumą, sukuria saugią aplinką įmonės veiklai bei įgalina patikimą paslaugų teikimą. Saugus verslas prasideda nuo požiūrio, kad saugumas yra ne kaina, o investicija į ateitį.

Vidutiniškai

35

kibernetines atakas patyrė mažiausios įmonės (iki 10 darbuotojų) 2024 metais

53

kibernetines atakas patyrė vidutinio dydžio įmonės (nuo 50 iki 249 darbuotojų) 2024 metais

Skaitmeninėje erdvėje daugėja ne tik kibernetinių grėsmių, bet ir sėkmingų kovos su jomis pavyzdžių. 2025 m. EUROPOL, bendradarbiaudamas su „Microsoft“, įgyvendino tarptautinę operaciją, skirtą suardyti nusikalstamą infrastruktūrą. Taikiniu tapo „Lumma“ – viena plačiausiai naudojamų duomenų vagystėms skirtų kenkėjiškų programų. „Lumma“ kenkėjiška programa iš užkrėstų įrenginių rinkdavo prisijungimo ir finansinius duomenis, kurie vėliau buvo parduodami specializuotose platformose. Nustatyta, kad „Lumma“ buvo užkrėsta daugiau kaip 394 tūkst. kompiuterių visame pasaulyje.

[4] „Businesses Report Increase in Cyberattacks in 2024“. Nuoroda: https://riskandinsurance.com/businesses-report-increase-in-cyberattacks-in-2024/

[5] EUROPOL. „Internet Organised Crime Threat Assessment 2025“. Nuoroda: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

/02/

Kibernetinių grėsmių analizė

Smulkaus ir vidutinio verslo kibernetinio saugumo būklės apžvalga

SVV įmonės sudaro didžiąją dalį įmonių Lietuvoje ir visoje ES. 2024 m. Valstybės duomenų agentūros duomenimis[6], Lietuvoje veikia daugiau kaip 116 tūkst. labai mažų, mažų ir vidutinių įmonių – tai sudaro net 99,8 % visų šalies įmonių. Šiose įmonėse dirba daugiau nei 700 tūkst. žmonių, arba apie 68 % visų dirbančiųjų. SVV įmonės yra Lietuvos ekonomikos pagrindas, todėl jų kibernetinio saugumo stiprinimas tiesiogiai veikia šalies ekonomiką – saugesnės įmonės patiria mažesnius finansinius nuostolius, užtikrina stabilų verslo veiklos tęstinumą ir skatina pasitikėjimą rinkoje, o tai prisideda prie darbo vietų išlaikymo, investicijų pritraukimo ir bendro ekonomikos augimo.

Kibernetiniam saugumui skiriama biudžeto dalis nuo viso IT numatyto biudžeto.

4-10 %
Smulkios ir vidutinės verslo įmonės

8-20 %
Didelės verslo įmonės

Tarptautinė praktika rodo, jog SVV įmonės dažniau patiria kibernetinius incidentus,o dauguma jų pripažįsta esą nepakankamai pasirengusios tinkamai į juos reaguoti. Šios įmonės dažnai turi ribotus resursus, mažiau specializuotų žinių ir kuklesnį biudžetą. ES kibernetinio saugumo agentūra (angl. *European Union Agency for Cybersecurity*, toliau – ENISA) 2024 m. kibernetinių grėsmių vertinimo ataskaitoje[7] pažymi, kad mažų įmonių pažeidžiamumas per pastaruosius metus padidėjo keturis kartus.

- 2023 m. „Sophos X-Ops“[8] nustatė, kad daugiau nei 75 % jų tirtų incidentų įvyko įmonėse, kuriose dirbo mažiau nei 500 darbuotojų.
- „Microsoft“ tyrimas[9], parodė, kad 9 iš 10 SVV įmonių pripažįsta – kibernetinės grėsmės kasmet didėja, tačiau įmonės vis dar jaučiasi nepakankamai pasirengusios jas atremti.
- „ConnectWise“ tyrimas[10] atskleidė, kad 61 % organizacijų baiminasi, jog rimta kibernetinė ataka galėtų visiškai sustabdyti jų veiklą.
- 2024 m. „Sophos X-Ops“ duomenimis[11] 58 % SVV įmonių pritarė, kad kibernetiniam saugumui teko skirti daugiau lėšų nei buvo planuota.

„Cymulate“ parengta analizė[12] rodo, kad kibernetiniam saugumui skiriama biudžeto dalis tiesiogiai priklauso nuo verslo įmonės dydžio – kibernetiniam saugumui SVV įmonės skiria 4–10 %, o didelės įmonės 8–20 % nuo informacinių technologijų (toliau – IT) plėtrai ir priežiūrai skirto biudžeto. Mažesnės investicijos rodo, kad kasdienių procesų skaitmeninimas vyksta sparčiau, nei saugumo stiprinimas. Nepakankamas dėmesys saugumui lemia, kad piktavaliai pasinaudoja tuo, kad SVV įmonės neturi reagavimo į kibernetinius incidentus plano, ekspertinių žinių turinčių darbuotojų ar įmonės, teikiančios kibernetinio saugumo paslaugas. Dėl to, į kibernetines atakas dažniausiai reaguojama lėčiau, o būtent reagavimo laikas yra vienas pagrindinių veiksnių, lemiantis patirtos žalos mastą.

SVV įmonės blogiausiai vertina savo atsparumą grėsmėms šiose srityse[13]:

- nuotolinio darbo sukeliamos rizikos – 60 % įmonių mano, kad šioje srityje jų saugumas yra nepakankamas,
- duomenų pažeidimų rizikos – 55 % įmonių nepasitiki sistemų apsauga,
- klientų duomenų neleistino atskleidimo rizikos – 53 % įmonių mano, kad jų apsauga šioje srityje yra nepakankama.

---

[6] „Valstybės duomenų agentūra“. Veikiančių įmonių skaičius. https://osp.stat.gov.lt/statistiniu-rodikliu-analize?indicator=S8R732#/

[7] „ENISA Threat Landscape 2025”. Nuoroda: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf

[8] „Sophos 2024 Threat Report: Cybercrime on Main Street“. Nuoroda: https://www.sophos.com/en-us/blog/2024-sophos-threat-report

[9] „SMB Cybersecurity Report“. Nuoroda: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/SMBCybersecurity-Report-Final.pdf

[10] „The state of SMB cybersecurity: racing against AI-driven cyberthreats“. Nuoroda: https://www.connectwise.com/globalassets/media/asset-docs/executive-briefs/the-state-of-smb-cybersecurity-in-2025.pdf

[11] „Sophos 2024 Threat Report: Cybercrime on Main Street“. Nuoroda: https://www.ccsmedia.com/wp-content/uploads/sophos-2024-threat-report-2.pdf

[12] „How cybersecurity leaders are optimizing their budgets in 2025“. Nuoroda: https://cymulate.com/blog/cybersecurity-budget-optimization/

[13] „The state of SMB cybersecurity: racing against AI-driven cyberthreats“. Nuoroda: https://www.connectwise.com/globalassets/media/asset-docs/executive-briefs/the-state-of-smb-cybersecurity-in-2025.pdf

Remiantis 2024 m. ENISA ataskaita[14], ES kibernetinės atakos dažniausiai buvo vykdomos pasitelkiant socialinės inžinerijos metodus, iš kurių pirmoje vietoje buvo duomenų viliojimas (angl. *phishing*), sudaręs 60 % visų registruotų kibernetinių incidentų. Antroje vietoje – pažeidžiamumų išnaudojimas (angl. *exploitation of vulnerabilities*), sudaręs 21 % visų registruotų kibernetinių incidentų. Trečioje vietoje buvo botnetai, kurie sudarė 10 % visų registruotų kibernetinių incidentų.

Panaši tendencija pastebima ir Lietuvoje – 2024 m. NKSC duomenimis[15], iš viso buvo užregistruoti 3 874 kibernetiniai incidentai. Iš jų 2 288 (59 %) buvo paremti socialinės inžinerijos metodais.

Toliau seka incidentai, susiję su neteisėta įtaka ryšių ir informacinių sistemų (RIS) veiklai – iš viso 444 (11 %), bei nepageidaujamų laiškų ir klaidinančios informacijos platinimas – 318 (8 %).

Šią tendenciją patvirtina ir Lietuvos Policijos duomenys[16]: sukčiavimas, glaudžiai susijęs su socialine inžinerija, išlieka pagrindine problema elektroninėje erdvėje. 2024 m. sukčiavimo elektroninėje erdvėje atvejai sudarė 53 % visų tokio pobūdžio nusikalstamų veikų.

Kaip 2024 m. keitėsi sukčiavimo būdai?

Telefoniniai sukčiai dažniausiai apsimetinėjo

+98 %
Informacinių sistemų specialistais

+66 %
Bankų darbuotojais

+21 %
Policijos pareigūnais

Sukčiavimas vis sparčiau pereina į skaitmeninę erdvę:

+20 %
apgaulingų žinučių bendravimo internete programose (pvz., „Messenger“)[17]

+27 %
socialiniame tinkle „Facebook” 2024 m. paskelbtų apgaulingų skelbimų skaičius, palyginus su 2023 m.[18]

-50 %
apgaulingų SMS žinučių sumažėjo 50 %

„+“/„-“ reiškia procentinį padidėjimą arba pamažėjimą, lyginant su ankstesniais metais

[14] „ENISA Threat Landscape 2025”. Nuoroda: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf

[15, 16, 17, 18] „Nacionalinė kibernetinio saugumo ataskaita 2024”. Nuoroda: https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

Svarbiausios kibernetinio saugumo grėsmės

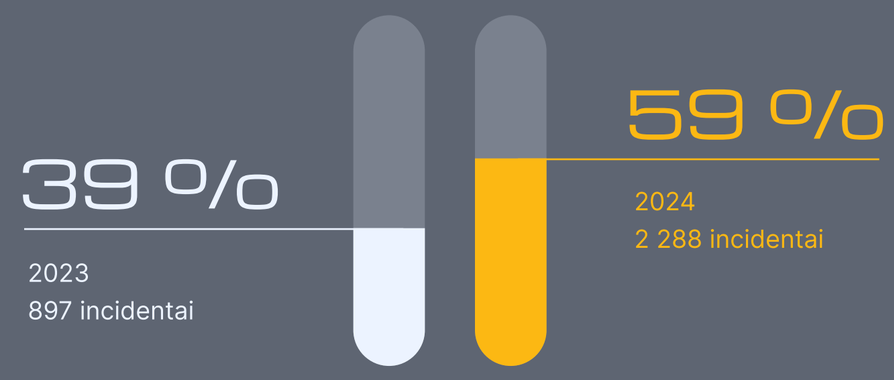
/ 1 / Atakos, vykdomos pasitelkiant socialinės inžinerijos metodus

Socialinė inžinerija (angl. *social engineering*) – vienas dažniausiai pasitaikančių kibernetinių atakų metodų tiek ES, tiek Lietuvoje. Šiuo atveju pagrindinis taikinys yra ne technologijos, o žmogus. Nusikaltėliai manipuliuoja emocijomis – skubos, baimės, smalsumo ar pasitikėjimo jausmais – siekdami sudaryti įspūdį, kad teikia pagalbą ar perduoda svarbią informaciją. Paprastai išskiriami keturi pagrindiniai socialinės inžinerijos atakų tipai: duomenų viliojimas (angl. *phishing*), tikslinis duomenų viliojimas (angl. *spear phishing*), vadovo apgavystė (angl. *whaling*) ir verslo el. pašto kompromitavimas (angl. *business email compromise*)[19]. Toliau pateikiamas išsamesnis šių kibernetinių atakų tipų aprašymas:

Duomenų viliojimas arba duomenų vagystės (angl. *phishing*)	Tai viena iš socialinės inžinerijos formų, kai apgaulės būdu siekiama išgauti vartotojo vardus bei slaptažodžius, banko sąskaitų numerius ar mokėjimo kortelių informaciją. Šių atakų metu piktavaliai dažnai apsimeta patikimais fiziniais arba juridiniais asmenimis, siekdami sukurti pasitikėjimą.

Atakos paprastai vykdomos siunčiant el. laiškus su nuorodomis į puslapius, imituojančius tikras svetaines – socialinius tinklus, elektroninių mokėjimų sistemas ar el. pašto paslaugas teikiančius tinklapius. Pagrindinis šių atakų tikslas – išvilioti prisijungimo duomenis prie elektroninės bankininkystės, vidinių įmonių sistemų, asmeninių paskyrų ar debesijos paslaugų.

NKSC duomenimis[20], vien 2024 m. užregistruoti 2 288 incidentai, susiję su duomenų viliojimų, sudarė 59 % visų registruotų incidentų (2023 m. tokių incidentų buvo 897 bei sudarė 39 % visų incidentų). Šią tendenciją patvirtina 2023 m. „Microsoft“ atliktas tyrimas, parodęs, kad net 43 % prieš SVV įmones nukreiptos kenkėjiškos programinės įrangos sudarė duomenų vagystės įrankiai.



Kaip gali pasireikšti tokia ataka? Teorinis pavyzdys

Langų ir durų montavimo įmonė gauna el. laišką iš tariamo kliento, kuriame teigiama, kad prisegtos sugadintų langų nuotraukos. Iš tiesų priedas yra kenkėjiškas failas. Administratorei jį atidarius, į kompiuterį įdiegiama kenkėjiška programa su paslėpta prieiga (angl. *backdoor*).

Piktavaliai įgyja prieigą prie įmonės el. pašto ir klientų valdymo sistemos (angl. *Customer Relationship Management*, CRM), kur saugomi klientų kontaktai ir sąmatos. Pasinaudodami neteisėtai įgyta prieiga, piktavaliai klientams išsiunčia netikras sąskaitas ir išvilioja pinigus.

Įmonė patiria:

- finansinę žalą
- reputacijos ir klientų pasitikėjimo praradimą
- užsakymų atšaukimus ir papildomą darbo krūvį tvarkant incidentą

Pastaraisiais metais duomenų viliojimo atakos tapo sudėtingesnės, nes piktavaliai pradėjo pasitelkti DI. Naudodami DI, jie gali kurti laiškus be rašybos klaidų, greitai generuoti netikras, bet itin tikroviškas svetaines, kurios beveik nesiskiria nuo originalių, nekelia įtarimų, o aiški ir skubi žinutė paskatina veikti impulsyviai. Įmonės darbuotojams tampa kur kas sunkiau atpažinti apgaulę. Dažniausios piktavalių naudojamos taktikos:

- → įspėjimas apie nepatvirtintą sąskaitą-faktūrą,
- → informacija apie gautą mokėjimą iš nežinomo siuntėjo,
- → „saugumo patikrinimas“, reikalaujantis prisijungti prie paskyros.

[19] „Rekomendacijos socialinės inžinerijos atakų atpažinimui el. laiškuose ir jų tyrimams“. Nuoroda: https://www.nksc.lt/doc/biuleteniai/Rekomendacija_9-leidinys.pdf

[20] „Nacionalinė kibernetinio saugumo ataskaita 2024”. Nuoroda: https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

Incidentų pavyzdžiai

2024 m. „Pepco Group“, Vengrija[21]: drabužių ir namų apyvokos prekių parduotuvė patyrė kibernetinę ataką, kurioje piktavaliai, pasitelkę socialinės inžinerijos metodus, bandė išvilioti pinigus. Buvo naudojami DI sugeneruoti el. laiškai, gramatiškai taisyklingi, primenantys tikrą vidinį susirašinėjimą ir paremti ankstesnių darbuotojų žinutėmis, todėl nesukėlė įtarimų. Preliminariais duomenimis, galimai padaryta finansinė žala galėjo siekti iki 16 mln. Eur. Klientų duomenys nenutekėjo, atakos tikslas buvo finansinė nauda.

- DI sugeneruoti el. laiškai, paremti darbuotojų žinučių turiniu
- Pervesta iki 16 mln. Eur

2024 m., Lietuva[22]: įmonė gavo elektroninį laišką, tariamai iš savo paslaugų teikėjo, su pranešimu apie pasikeitusią banko sąskaitą. Laiškas atrodė įprastas ir buvo panašus į ankstesnę komunikaciją, todėl finansininkas, neįtaręs apgaulės, atliko pavedimą. Vėliau išaiškėjo apgavystė: į tiekėjo el. pašto paskyrą buvo įsilaužta, o nurodyta banko sąskaita priklausė asmenims, vykdantiems sukčiavimą. Dėl šios apgaulės 390 tūkst. Eur buvo pervestos į asmenų, vykdančių sukčiavimą, valdomą sąskaitą.

- Pranešimas apie pasikeitusią banko sąskaitą
- Pervesta 390 tūkst. Eur

Tikslinis duomenų viliojimas

(angl. *Spear phishing*)

Šios socialinės inžinerijos atakos skiriasi nuo įprasto duomenų viliojimo tuo, kad laiškai siunčiami konkretiems įmonių darbuotojams, turintiems prieigą prie jautrios informacijos. Piktavaliai naudoja viešai prieinamą asmeninę informaciją iš socialinių tinklų, žiniasklaidos ar kitų šaltinių, kad sukurtų kuo asmeniškesnį laišką, kuris nepastebimai įsilietų į darbuotojo kasdienę korespondenciją.

Vadovo apgavystė

(angl. *Whaling*)

Tai socialinės inžinerijos atakos forma, panaši į duomenų viliojimą, tačiau jos metu piktavaliai apsimeta aukšto lygio vadovu ar akcininku. Tikslas – įgyti įmonės vadovo pasitikėjimą ir juo manipuliuojant paskatinti atskleisti jautrią informaciją arba atlikti skubų finansinį pavedimą.

Tokio tipo atakos ypač pavojingos SVV įmonėms, kur atsakomybė dažnai sutelkta vieno asmens, dažniausiai vadovo, rankose. Jei vienas žmogus turi prieigą prie komercinės informacijos ir priima daug finansinių sprendimų, rizika ženkliai padidėja. Be to, DI leidžia itin tiksliai atkartoti bendravimo stilių, balsą ar net vaizdą, todėl tokias atakas sunku atpažinti.

Incidento pavyzdys

2024 m. Didžiojoje Britanijoje įsikūrusioje inžinerijos įmonėje „Arup“ įvyko viena didžiausių žinomų vadovo apgavystės atakų. Įmonės darbuotoja, turėjusi prieigą prie banko sąskaitų, pervedė sukčiams daugiau nei 20 mln. svarų. Piktavaliai panaudojo DI, kad sukurtų vaizdo skambutį su tariamais aukšto lygmens vadovais. Visi dalyviai – jų veidai, balsai ir elgesys – buvo sugeneruoti DI. Skambučio metu darbuotojai gavo skubias finansines užduotis, todėl buvo atlikta 15 pervedimų į 5 skirtingas sąskaitas.

Atakos sėkmę lėmė keli veiksniai:

- didelis dalyvių skaičius susitikime sumažino darbuotojos budrumą,
- DI sugeneruoti vaizdai ir balsai atrodė itin tikroviškai,
- aukštos vadovų pareigos ir skubos reikalavimas sukėlė spaudimą veikti nedelsiant.

Incidentas parodė, kad apgaulė tampa itin tikroviška, kai naudojamos kelios socialinės inžinerijos priemonės kartu.[23]

- DI sugeneruoti aukštų vadovų vaizdai ir balsai
- Skubios finansinės užduotys
- Pervesta 20 mln. svarų sukčiams

---

[21] „The 5 Biggest Phishing Attacks of 2024“. Nuoroda: https://www.memcyco.com/the-5-biggest-phishing-attacks-of-2024/#:~:text=In%20February%202024%2C%20Pepco%20Group,funds%20may%20never%20be%20recovered

[22] „Vienas didžiausių sukčių grobių šiemet – iš įmonės išviliojo beveik 400 tūkst. Eurų“. Nuoroda: https://www.lrt.lt/naujienos/verslas/4/2262106/vienas-didziausiu-sukciu-grobiu-siemet-is-imones-isviliojo-beveik-400-tukst-euru

[23] „Arup’s $25M Deepfake Loss: Anatomy of an AI-Powered Scam“. Nuoroda: https://www.adaptivesecurity.com/blog/arup-deepfake-scam-attack

Verslo elektroninio pašto kompromitavimas

(angl. *Business email compromise*)

Šios atakos metu piktavaliai suklastoja organizacijos ar vieno iš jos darbuotojų el. pašto paskyrą ir ją naudoja el. laiškų siuntimui. Dažnai tokiuose laiškuose prašoma apmokėti sąskaitas, atlikti vėluojančius mokėjimus ar atnaujinti prisijungimo prie bankinės sistemos duomenis. Šios atakos gali sukelti reikšmingų finansinių nuostolių ir ypač pavojingos SVV įmonėms, kur vienas darbuotojas atsakingas už bankinių pavedimų atlikimą ir gali laisvai disponuoti įmonės lėšomis be papildomo patvirtinimo.

/ 2 / Išpirkos reikalavimo programinės įrangos atakos

Išpirkos reikalavimo programinė įranga (angl. *Ransomware*) – tai kenkėjiškos programinės įrangos rūšis, kuri užšifruoja įmonės duomenis ir padaro juos nepasiekiamus. Norint atgauti prieigą piktavaliai dažniausiai reikalauja išpirkos. Tai viena labiausiai paplitusių kibernetinių grėsmių pasaulyje[24].

Išpirkos reikalavimo programinė įranga gali būti skirstoma į šiuos tipus:

- **Šifruojanti**

  (angl. *Encrypting ransomware*)

  Dažniausia rūšis, užšifruojanti kompiuterio ar tinklo duomenis, kurie tampa nepasiekiami. Už iššifravimo raktą reikalaujama išpirkos, dažniausiai kriptovaliuta.

- **Šantažuojanti**

  (angl. *Doxware arba Leakware*)

  Grasinama paviešinti neteisėtai perimtus duomenis, siekiant pakenkti reputacijai. Dažnai derinama su šifravimu, kad duomenys būtų visiškai neprieinami.

- **Nešifruojanti**

  (angl. *Non-encrypting ransomware*)

  Neužšifruoja duomenų, bet blokuoja prieigą prie jų ar visos sistemos. Ekrane rodomas reikalavimas sumokėti išpirką.

- **Naikintanti**

  (angl. *Wiper ransomware*)

  Tikslas – ne pinigai, o maksimali žala: duomenys tyčia ištrinami ar sugadinami, net jei išpirka sumokėta. Žinomiausias pavyzdys – 2017 m. „NotPetya“ virusas, padaręs žalos už ~10 mlrd. JAV dolerių.

Atkreiptinas dėmesys, kad skaitmeninėje erdvėje egzistuoja išpirkos reikalavimo programinės įrangos paslauga (angl. *Ransomware-as-a-Service*, RaaS), kurios kūrėjai nuomoja savo sukurtus šifruojančius įrankius kitiems piktavaliams. Tai leidžia net techninių žinių neturintiems asmenims surengti ataką prieš pasirinktą taikinį.

Dažniausiai išpirkos reikalavimo programinės įrangos atakos vykdomos:

- per elektroninių laiškų priedus ir žalingas nuorodas,
- per kenksmingas svetaines ar failų atsisiuntimus.

2024 m. Lietuvoje užregistruoti 4 išpirkos reikalavimo programinės įrangos atakos atvejai, šis incidentų tipas buvo penktoje vietoje ir tai yra 5 kartus mažiau nei 2023 m[25]. Reikalautos išpirkos dydis svyravo nuo 10 iki 112 tūkst. Eur (2023 m. didžiausia reikalauta suma – 832 tūkst. Eur)[26].

Piktavaliai vis dažniau taiko dvigubo šantažo metodus: ne tik užšifruoja duomenis, bet ir grasina juos paviešinti, taip siekdami išgauti dar didesnes sumas.

Kokiu būdu gali pasireikšti tokia ataka? Teorinis pavyzdys

Rajono centre veikiantis darbuotojų apskaitos paslaugų biuras aptarnauja daugiau kaip 40 SVV įmonių. Viena darbuotoja atidaro tariamą „Sodros“ pranešimą su prisegtu „PDF“ dokumentu – iš tikrųjų tai kenkėjiškas failas. Dokumentui atsidarius, į kompiuterį patenka išpirkos reikalavimo programinis kodas ir užkrečia bendrą biuro bevielį tinklą.

Pasekmės:

- užšifruojami penkerių metų klientų archyvai
- 14 klientų vėluoja pateikti deklaracijas ir jiems gresia baudos
- įmonė sulaukia daug neigiamų reakcijų ir skundų
- 2 klientai nutraukia bendradarbiavimą dėl prasto kibernetinio incidento valdymo

[25, 26] „Nacionalinė kibernetinio saugumo ataskaita 2024”. Nuoroda: https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

Incidentų pavyzdžiai

2025 m. „Comcast Corporation“[27] patyrė kibernetinę ataką, kurią įvykdė grupuotė „Medusa“, pavogusi daugiau nei 830 GB klientų ir galimai vidinių įmonės duomenų. Po atakos grupuotė tamsiajame internete (angl. *dark web*) siūlė parduoti neteisėtai perimtus duomenis už 1,2 mln. JAV dolerių arba reikalavo tos pačios sumos iš „Comcast Corporation“ už jų ištrynimą. Nesumokėjus išpirkos, informacija galėjo būti paviešinta arba parduota tretiesiems asmenims.

- Pavogė daugiau kaip 830 GB duomenų
- Pavogti duomenys už 1,2 mln. JAV dolerių

2025 m. kibernetinė grupuotė „Payoutsking“[28] įvykdė didelio masto išpirkos programinės įrangos ataką prieš tarptautinę kredito informacijos bendrovę „Creditinfo Group“, pavogdama daugiau nei 2,3 TB duomenų, įskaitant klientų sąrašus, partnerių informaciją, finansines ataskaitas ir kainodaros failus. Grupuotė nustatė šešių dienų terminą sumokėti išpirką, kitu atveju duomenys būtų paviešinti. Buvo patvirtinta, kad prarasta apie 29 tūkst. Lietuvos vartotojų asmens duomenų. Įmonė izoliavo paveiktą infrastruktūros dalį, atliko vidinį tyrimą ir nustatė galimus išorinius kibernetinės atakos vektorius. Incidentas sulaukė tarptautinio dėmesio, o tyrimas dėl duomenų pažeidimo vis dar vyksta.

- Didelio masto išpirkos reikalavimo programinės įrangos ataka prieš „Creditinfo Group“
- Pavogta daugiau nei 2,3 TB duomenų
- Prarasta apie 29 tūkst. Lietuvos vartotojų asmens duomenų
- Tyrimas dėl duomenų pažeidimo vis dar vyksta

/ 3 / Tiekimo grandinės pažeidžiamumas

SVV įmonės dažnai yra didesnių tiekimo grandinių dalis – jos bendradarbiauja su įvairiais tiekėjais ar įrangos gamintojais. Naudojama programinė ar techninė įranga taip pat yra sukurta integruojant kelių skirtingų tiekėjų ar gamintojų sprendimus. Dėl šios priežasties kibernetinė ataka gali pasiekti įmonę per tiekimo grandinę, pasinaudojant vieno iš jos partnerių ar tiekėjų sistemų pažeidžiamumu (angl. *Supply chain vulnerability*). Kadangi tiekimo grandinės tampa vis sudėtingesnės ir dažnai apima kelias valstybes, svarbu užtikrinti ne tik savo organizacijos, bet ir partnerių bei tiekėjų kibernetinį saugumą.

Kas gali nutikti pažeidus tiekimo grandinę?

- **Duomenų vagystė.**
  Gali būti nutekinta ar paviešinta jautri informacija apie klientus, tiekėjus arba įmonės veiklą.
- **Veiklos sutrikimai.**
  Kibernetinė ataka gali sustabdyti įmonės veiklą kelioms valandoms ar net dienoms, o jos poveikis gali išplisti ir visoje tiekimo grandinėje.
- **Reputacinė žala.**
  Paslaugų teikimo vėlavimai ar nekokybiški produktai gali sumažinti klientų pasitikėjimą įmonės gebėjimu vykdyti įsipareigojimus ateityje. Dėl to gali būti prarasti esami ir potencialūs klientai. Net ir laikinas elektroninės svetainės neveikimas gali paskatinti klientus kreiptis į kitus tiekėjus ar konkurentus.
- **Finansiniai nuostoliai.**
  Kibernetinės atakos gali sukelti tiesioginių išlaidų, pvz. susijusių su išpirkos reikalavimais ar teisinių paslaugų įsigijimu. Be to, jei kibernetinis incidentas buvo netinkamai suvaldytas, SVV įmonės gali patirti ir netiesioginių nuostolių, pvz. dėl atšauktų ar neįvykusių sandorių.

„SecurityScorecard“ atliktas tyrimas[29] rodo, kad daugiau nei 70 % organizacijų 2024 m. patyrė bent vieną reikšmingą kibernetinį incidentą, susijusį su trečiąja šalimi – tiekimo grandinės partneriu, kuris turėjo apčiuopiamą poveikį jų veiklai. Be to, 62 % organizacijų nurodo, kad mažiau nei pusė jų tiekėjų atitinka nustatytus kibernetinio saugumo reikalavimus. Šie duomenys rodo, kad vien vidinių sistemų apsauga nėra pakankama siekiant sumažinti kibernetinių atakų riziką. Saugumas turi būti užtikrinamas visoje tiekimo grandinėje, nes būtent silpniausia jos dalis dažnai tampa ta vieta, per kurią piktavaliai patenka į platesnę verslo ekosistemą.

Didžiausia rizika dažniausiai tenka IT paslaugų tiekėjams, debesijos paslaugų teikėjams ir programinės įrangos kūrėjams. Jei jų sistemose išlieka saugumo spragų, pažeidžiamos tampa ir jų klientų – įskaitant SVV įmones – informacinės sistemos. Neatnaujinamos ar netinkamai prižiūrimos sistemos didina pažeidžiamumą kibernetinėms atakoms.

---

[27] „8 of the biggest ransomware attacks of 2025“. Nuoroda: https://nordlayer.com/blog/ransomware-attacks-2025/

[28] „Creditinfo“ patyrė milžinišką kibernetinę ataką, klientų Lietuvoje duomenys – saugūs“. Nuoroda: https://www.lrt.lt/naujienos/mokslas-ir-it/11/2623297/creditinfo-patyre-milziniska-kibernetine-ataka-klientu-lietuvoje-duomenys-saugus

[29] „2025 Supply chain cybersecurity trends“. Nuoroda: https://securityscorecard.com/wp-content/uploads/2025/06/2025-Supply-Chain-Cybersecurity-Trends.pdf

Kokiu būdu gali pasireikšti tokia ataka? Teorinis pavyzdys

Privatus odontologijos kabinetų tinklas neturi vidinio IT padalinio. IT paslaugos teikiamos samdomo specialisto. Prisijungdamas prie klientų informacinių sistemų ir debesijos platformų, kuriose saugomi rentgeno vaizdai bei pacientų medicininiai duomenys, specialistas nenaudoja dviejų veiksnių autentifikavimo. Piktavaliai perima šio paslaugų teikėjo paskyrą ir per ją gauna prieigą prie jautrios pacientų informacijos.

Pasekmės:

- klinika tris dienas negali naudotis pacientų registracijos sistema
- kyla rizika gauti baudą už Bendrojo duomenų apsaugos reglamento (BDAR) pažeidimus
- įmonė patiria papildomų išlaidų, susijusių su IT sistemų atkūrimu
- prarandamos pajamos, nes dalis pacientų negali užsiregistruoti vizitams

Incidento pavyzdys

2022 m. „Kojima Industries“, vienas pagrindinių „Toyota“ tiekėjų, patyrė kibernetinę ataką, sutrikdžiusią jos IT sistemas. Dėl šio incidento buvo sustabdytas komponentų tiekimas „Toyota“ gamykloms. Įmonė savo gamyboje taiko vadinamąjį „just-in-time“ principą – reikalingos dalys pristatomos tik tuo metu, kai jų reikia gamybos procese. Todėl net ir trumpalaikis tiekimo sutrikimas iš karto paveikia visą tolesnę gamybos grandinę. Dėl vieno tiekėjo veiklos sustabdymo „Toyota“ buvo priversta vienai dienai sustabdyti darbą 14 automobilių surinkimo gamyklų Japonijoje. Skaičiuojama, kad dėl šio sutrikimo buvo pagaminta apie 13 tūkst. automobilių mažiau.

- „Kojima Industries“ patyrė kibernetinę ataką
- Sustojo visų komponentų tiekimas „Toyota“ gamykloms
- Buvo pagaminta 13 tūkst. automobilių mažiau

/ 4 / Vidinės grėsmės

Nė viena įmonė nėra visiškai apsaugota nuo vidinių grėsmių (angl. *insider threat*), kurias gali sukelti tiek darbuotojų aplaidumas, tiek tyčiniai veiksmai. Vidinės grėsmės apima sabotažą, duomenų vagystę ar sunaikinimą, sukčiavimą, kenkėjišką informacijos rinkimą ir kitą veiklą, galinčią sukelti duomenų nutekėjimą, veiklos sutrikimus arba finansinę žalą.

Norint įvertinti vidinių grėsmių lygį, būtina atkreipti dėmesį į pagrindines darbuotojų grupes:

- **Aplaidūs arba neįsitraukę darbuotojai** – jų veikla gali reikšmingai pakenkti įmonės saugumui. Neatsargumas, saugumo procesų neišmanymas ir rekomenduojamų priemonių nepaisymas didina visos įmonės pažeidžiamumą. Tokie darbuotojai dažniau:
  - patenka į sukčiavimo spąstus,
  - naudoja silpnus slaptažodžius,
  - nesilaiko rekomendacijų dėl duomenų kopijų kūrimo ar saugaus failų tvarkymo.

Valstybinės duomenų apsaugos inspekcijos duomenimis[30], beveik pusė registruotų pranešimų apie asmens duomenų saugumo pažeidimus susiję su netyčinėmis žmogiškomis klaidomis. Ši rizika dar labiau išauga dirbant nuotoliniu būdu. Nuotolinis darbas didina kibernetinės atakos galimybes, o prisijungimas prie sistemų naudojant asmeninius ir neapsaugotus įrenginius gali atskleisti konfidencialią informaciją. Tyrimas[31] parodė, kad net 60 % SVV įmonių nesijaučia pakankamai apsaugotos nuo su nuotoliniu darbu susijusių kibernetinių grėsmių.

- **Darbuotojai, kurie sąmoningai siekia pakenkti įmonei** – dėl asmeninės naudos, keršto ar išorės įtakos. Veikdami įmonės viduje jie gali:
  - neteisėtai pasisavinti arba naikinti duomenis,
  - trikdyti įmonės veiklą,
  - viešinti ar perduoti tretiesiems asmenims komercines paslaptis.
- **Trečiųjų šalių (išorės) darbuotojai** – šios grupės asmenys kelia grėsmę įmonės saugumui, jei turėdami prieigą prie vidinių sistemų ar dokumentų nesilaiko nustatytų saugumo procedūrų. Papildoma rizika kyla, kai trečiųjų šalių tiekėjai savo įmonėje netaiko tinkamų saugumo priemonių.

[30] „Nacionalinė kibernetinio saugumo ataskaita 2024”. Nuoroda: https://kam.lt/wp-content/uploads/2025/07/Nacionaline-kibernetinio-saugumo-bukles-ataskaita-2024.pdf

[31] „The state of SMB cybersecurity: racing against AI-driven cyberthreats“. Nuoroda: https://www.connectwise.com/globalassets/media/asset-docs/executive-briefs/the-state-of-smb-cybersecurity-in-2025.pdf

Kaip gali pasireikšti tokia ataka? Teorinis pavyzdys

Aplaidumo atvejis

Veterinarijos klinikos administratorė naudoja tą patį slaptažodį asmeninei „Facebook“ paskyrai, įmonės el. paštui ir klientų registracijos sistemai. Gavę prieigą prie administratorės asmeninės paskyros, piktavaliai gauna prieigą ir prie klinikos registracijos sistemos.

Pasekmės:

- ištrinamas dviejų savaičių vizitų grafikas
- duomenų bazės atkūrimas užtrunka iki 48 valandų
- klinika turi atšaukti apie 60 vizitų per dvi dienas
- prarandamos kelių tūkstančių eurų pajamos

Incidentų pavyzdžiai

2022–2023 m., sporto klubas „Impuls“[32] . Sporto klube „Impuls“ nustatytas vidinis sukčiavimas: administratorė, pasinaudojusi buvusios kolegės prisijungimo duomenimis, manipuliavo elektroninės apskaitos sistema ir neteisėtai pasisavino 24 abonementus (virš 12 tūkst. Eur), dalį jų perduodama tretiesiems asmenims, keisdama tikrąsias kainas į nulines, fiksuodama fiktyvius pardavimus ir neparduotus abonementus žymėdama kaip suteiktus nemokamai.

- Neteisėtai pasisavinti 24 abonementai
- Abonementų vertė didesnė nei 12 tūkst. Eur

2023 m., „Tesla“[33]. 2023 m. du buvę „Tesla“ darbuotojai neteisėtai perėmė ir Vokietijos žiniasklaidai perdavė slaptus įmonės duomenis. Nutekinta daugiau nei 75 tūkst. buvusių ir esamų darbuotojų asmens duomenų, taip pat klientų informacija, įskaitant banko duomenis, skundus dėl savaeigių automobilių funkcijų ir gamybos procesų komercines paslaptis.

- Du buvę darbuotojai perdavė slaptus duomenis
- Nutekinti darbuotojų asmens duomenys ir klientų informacija

/ 5 / Botnetas

Botnetas (angl. *Botnet*) – tai piktavalių kontroliuojamas užvaldytų kompiuterių, vaizdo kamerų ar kitų interneto prieigą turinčių įrenginių tinklas, kurį piktavaliai gali panaudoti plataus masto kenkėjiškai veiklai.

Dažniausiai pasitaikančios botneto atakų rūšys:

- **Paskirstyta paslaugos trikdymo ataka** (angl. *Distributed Denial of Service, DDoS*) – tokios atakos tikslas yra sutrikdyti svetainių ar paslaugų veikimą, kad jos taptų neprieinamos vartotojams arba veiktų netinkamai. Remiantis 2024 m. ENISA ataskaita[34], net 77 % užregistruotų kibernetinių incidentų priklausė šiai kiberentinių atakų kategorijai.
- **Prisijungimo duomenų klastojimas** (angl. *Credential stuffing*) – šios atakos nukreiptos į vartotojus, kurie skirtingose svetainėse naudoja tą patį vartotojo vardo ir slaptažodžio derinį. Piktavaliai, naudodami automatizuotas priemones ir neteisėtai perimtus prisijungimo duomenis, prisijungia prie kitų paskyrų ir iš jų pasisavina informaciją.
- **Didelių kiekių nepageidaujamų el. laiškų siuntimas** (angl. *Spam*) – siunčiant didelius kiekius nepageidaujamų laiškų su kenkėjiškomis nuorodomis arba reklama, piktavaliai perkrauna el. laiškų aplankus, el. pašto serverius.

Kenkėjiška programinė įranga, priklausanti botnetui, dažniausiai patenka į įrenginius per:

- kenkėjiškas svetaines,
- apgaulingus el. laiškus,
- programų spragas, kurios nėra laiku pašalinamos.

[32] „Klaipėdietė iš bendrovės „Impuls LTU“ pasisavino abonementų už 12 tūkst. eurų“. Nuoroda: https://www.lrt.lt/naujienos/verslas/4/2047160/klaipediete-is-bendroves-impuls-ltu-pasisavino-abonementu-uz-12-tukst-euru?srsltid=AfmBOoqf83wi_2NNeBBcRtHv7SGa5EFrP0vbcbprB0MxxaZ9-fGxNGDb

[33] „Former employees behind Tesla data breach“. Nuoroda: - https://cyfor.co.uk/former-employees-behind-tesla-data-breach/

[34] „ENISA Threat Landscape 2025”. Nuoroda: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

Kaip gali pasireikšti tokia ataka? Teorinis pavyzdys

Rajono centro senamiestyje veikia populiari kavinė, kurioje įdiegta IP kamera su nepakeistu gamintojo slaptažodžiu. Kamera prijungta prie to paties belaidžio interneto ryšio tinklo, kurį naudoja kavinė. Piktavaliai, pasitelkdami botnetą ir naudodami gamintojo numatytus (angl. *default*) slaptažodžius, lengvai užvaldo kamerą ir ją panaudoja kitoms paskirstytos paslaugos trikdymo atakoms.

Pasekmės:

- interneto ryšys sulėtėja iki minimumo, todėl darbuotojai negali naudotis socialiniais tinklais ar vykdyti įprastos komunikacijos
- kortelių mokėjimai neveikia apie 4 valandas, nes bankas laikinai sustabdo kortelių terminalo veikimą dėl saugumo. Kavinė gali priimti tik klientus, atsiskaitančius grynaisiais
- pietų metu prarandama daugiau nei 60 potencialių klientų

Incidentų pavyzdžiai

2024 m., „Gorilla Botnet“[35]. 2024 m. rugsėjį identifikuota nauja botnetų grupė „Gorilla Botnet“, per mažiau nei mėnesį pardavusi daugiau nei 300 tūkst. paskirstytos paslaugos trikdymo atakų komandų „Telegram“ kanale už kelis dolerius. Kibernetinės atakos nukreiptos į daugiau nei 100 šalių, daugiausia Kiniją (20 %), JAV (19 %), Kanadą (16 %) ir Vokietiją (6 %), taikiniai – universitetai, bankai, vyriausybinės svetainės, telekomunikacijos ir azartinių žaidimų sektorius.

- Parduota daugiau nei 300 tūkst. paskirstytos trikdymo atakos komandų
- Atakos nukreiptos į daugiau nei 100 šalių

2022 m., „Ignitis“[36]. 2022 m. valstybinė energetikos įmonė „Ignitis“ patyrė vieną didžiausių per pastarąjį dešimtmetį paskirstytos paslaugos trikdymo atakų, dėl kurios įvykdymo atsakomybę prisiėmė prorusiška grupuotė „Killnet“. Kibernetinė ataka sutrikdė ne tik „Ignitis“ išorinį interneto srautą, dėl ko laikinai neveikė įmonės interneto svetainė, savitarnos sistema ir dalis IT paslaugų, bet sutrikdė ir dalį Lietuvos interneto tinklo, paveikdamas kitas įmones bei organizacijas.

- Prorusiška grupuotė įvykdė ataką prieš „Ignitis“
- Sutriko interneto srautas, neveikė dalis paslaugų ir sistemų

/ 6 / Dirbinio Intelekto keliamos rizikos

DI įrankiai gali padidinti veiklos efektyvumą, automatizuoti užduotis ir sumažinti žmogiškųjų klaidų riziką, tačiau jie kelia ir naujų kibernetinio saugumo iššūkių, tokių kaip duomenų nutekėjimas, neteisėta prieiga ir klaidingų sprendimų priėmimas. 2025 m. „Eurostat“ duomenimis[37], apie 21 % Lietuvos įmonių (2024 m., – 9 % įmonių) naudojo DI įrankius įvairioms užduotims atlikti. Praktikoje DI dažniausiai taikomas kaip kasdienis įrankis: klientų aptarnavimui (atsakymai, pokalbių sistemos), rinkodarai ir pardavimams (reklamų tekstų kūrimui), dokumentų rengimui (pasiūlymams, sutartims, santraukoms), duomenų analizei (ataskaitų aiškinimui, anomalijų nustatymui) bei IT darbams (kodo fragmentams, testavimui, automatizavimui).

21 %

įmonių Lietuvoje naudojo DI įrankius įvairioms užduotims atlikti

„Eurostat“ duomenimis, 2025 m.
2024 m. - 9 %

---

[35] „Gorilla botnet launched 300K DDoS attacks on banks, governments, and more“. Nuoroda: https://moonlock.com/gorilla-botnet-ddos-attacks

[36] „Vienas „Ignitis grupės“ vadovų rimtą „DDoS“ ataką linki patirti ir kitiems“. Nuoroda: https://www.vz.lt/inovacijos/2022/09/12/vienas-ignitis-grupes-vadovu-rimta-ddos-ataka-linki-patirti-ir-kitiems

Nors vis daugiau darbuotojų kasdienėse užduotyse pasitelkia DI įrankius, tačiau daugelyje įmonių trūksta aiškių jų naudojimo taisyklių. Tokiais atvejais kyla rizika, kad konfidencialūs įmonės ar klientų duomenys pateks trečiosioms šalims. Tokia informacija vėliau gali būti naudojama DI modelių mokymui, pasitelkiama sukčiavimui ar tapatybės vagystėms. Šiuo atveju svarbiausia:

- **Patikimi tiekėjai** – naudoti tik žinomų ir patikrintų tiekėjų DI įrankius, kurie aiškiai nurodo duomenų saugojimo vietą, laiką ir naudojimą modelių tobulinimui.
- **Žmogaus patvirtinimas** – neleisti DI priimti galutinių sprendimų finansiniuose ar administraciniuose procesuose; visada reikalauti žmogaus patvirtinimo prieš sąskaitų tvirtinimą, mokėjimų atlikimą, paskyrų kūrimą ar naikinimą.
- **Darbuotojų mokymai** – reguliariai šviesti darbuotojus apie DI naudojimo rizikas, pvz., apgaulingų el. laiškų atpažinimą, suklastotų garso ar vaizdo įrašų identifikavimą bei įmonės dokumentų įkėlimo į viešai prieinamus DI įrankius pavojus.

SVV įmonėms svarbu naudoti DI priemones atsakingai, užtikrinant, kad sprendimų kontrolė liktų žmogaus rankose ir kad duomenys būtų saugomi bei tvarkomi saugiai.

DI vis dažniau naudojamas ne tik versle, bet ir piktavalių. Piktavaliai pasitelkia DI kurdami įtikinamesnius duomenų viliojimo el. laiškus – įrankis gali atkartoti įmonės ar konkretaus asmens rašymo stilių, išvengti gramatinių klaidų ir sukurti itin tikrovišką turinį. 2024 m. duomenimis[38], net 82,6 % duomenų viliojimo el. laiškų buvo sukurti arba patobulinti pasitelkiant DI.

Taip pat DI suteikia piktavaliams galimybę rengti sudėtingas kibernetines atakas net neturint didelės techninės patirties. DI naudojamas automatizuotai ieškant sistemų pažeidžiamumų ir parenkant efektyviausius atakų metodus, taip didinant jų mastą ir greitį. 2025 m. „Anthropic“ ataskaitos duomenimis[39], DI gali automatizuoti daugelį veiksmų, kuriems anksčiau reikėjo specifinių technologinių įgūdžių.

Kaip gali pasireikšti tokia ataka? Teorinis pavyzdys

Baldų gamybos įmonė neturi vidinių DI naudojimo taisyklių, todėl darbuotojai savarankiškai naudoja viešus generatyvinio DI įrankius. Projekto vadovas įkelia į sistemą visą su projektu susijusią informaciją ir prašo DI paruošti pasiūlymą klientui. Jis neįvertina, kad duomenys perduodami trečiajai šaliai, o įmonė neturi tam teisinio pagrindo. Po kelių mėn. konkurentas pateikia panašų pasiūlymą, o vidinis tyrimas rodo, kad duomenų nutekėjimo šaltinis buvo viešas DI įrankis.

Pasekmės:

- konfidencialios informacijos nutekėjimas – kainodara, tiekėjų sąlygos ir individualūs sprendimai tampa prieinami trečiosioms šalims
- teisinė ir reputacinė rizika – klientas kelia klausimus dėl BDAR pažeidimų, įmonė priversta aiškintis duomenų perdavimo teisėtumą
- prarastas konkurencinis pranašumas – unikalūs sprendimai praranda išskirtinumą, o klientas gali pasirinkti kitą tiekėją
- incidentas įvyksta be įsilaužimo – nebuvo piktavalių ar virusų; žalą sukėlė kasdienis, iš pažiūros „nekaltas“ siekis pagreitinti užduoties vykdymą

[37] „Use of artificial intelligence in enterprises“. Nuoroda: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises

[38] „Phishing Threat Trends Report“. Nuoroda: https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf

[39] „Threat Intelligence Report: August 2025“. Nuoroda: https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf

/03/

Smulkių ir vidutinių įmonių kibernetinio saugumo būklės vertinimas: apklausos rezultatai

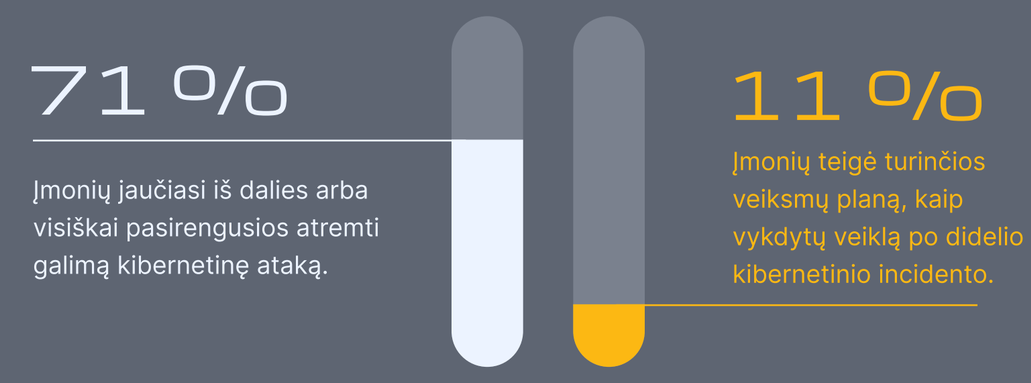
Šioje dalyje pateikiama atliktos kibernetinio saugumo būklės vertinimo apklausos apžvalga. 2025 m. apklausos tikslas buvo įvertinti, kaip SVV įmonės suvokia kibernetinį saugumą ir atlikus lyginamąją 2020 m. ir 2025 m. analizę nustatyti, ar pasikeitė SVV įmonių požiūris į kibernetinį saugumą, su kokiais iššūkiais susiduria įmonės šiuo metu ir kokias priemones jos savarankiškai taiko saugumui stiprinti. Apklausos klausimynas buvo paruoštas „Google Forms“ platformoje ir platinamas socialiniuose tinkluose, savivaldybių svetainėse bei siunčiant elektroniniu paštu individualius kvietimus dalyvauti apklausoje. Apklausos laikotarpis – nuo 2025 m. lapkričio 25 d. iki 2026 m. vasario 10 d., o bendras respondentų skaičius siekė 134.

Apklausos rezultatai leidžia pateikti įvairiapusių įžvalgų, tačiau pagrindinė išvada yra ta, kad SVV įmonių kibernetinio saugumo sąmoningumo lygis Lietuvoje vis dar nėra aukštas. Nors pastebimos teigiamos tendencijos naudojamų elektroninių paslaugų ir kibernetinio saugumo priemonių srityje, įmonės vis dar skiria per mažai dėmesio kibernetinio saugumo stiprinimui, įskaitant darbuotojų švietimą. Įmonėms trūksta žinių, kaip pasirinkti tinkamas kibernetinio saugumo priemones ir įvertinti galimas rizikas. Tai mažina įmonių atsparumą piktavalių atakoms, kurių skaičius pastaraisiais metais ženkliai išaugo.

Svarbiausios išvados:

- Vis daugiau įmonių turi dokumentuotą vidinę kibernetinio saugumo politiką, kuri leidžia operatyviau reaguoti į kibernetines atakas.
- Reikšmingai padaugėjo įmonių, kurios jautėsi pasirengusios iš dalies ar visiškai atremti galimą kibernetinę ataką ar suvaldyti kibernetinį incidentą.
- Vis daugiau įmonių teigia gebančios tinkamai įvertinti kibernetinio saugumo rizikas.
- Dauguma įmonių pasirenka turėti vidinį darbuotoją, atsakingą už kibernetinį saugumą, tačiau dalis jų neturi parengtos kibernetinio saugumo politikos, nustatančios tokio darbuotojo funkcijas.
- Dauguma įmonių jautėsi iš dalies priklausomos nuo tiekėjų ir pabrėžė, kad joms svarbu, kad verslo partneriai laikytųsi kibernetinio saugumo standartų.
- Sumažėjo įmonių, pasirengusių investuoti į kibernetinio saugumo priemones. Tikėtina tam įtakos galėjo turėti besiformuojantis supratimas, kad kibernetinio saugumo baziniam užtikrinimui pakanka viešai skelbiamų rekomendacijų laikymosi.
- Nuotoliniai mokymai tapo patraukliausia žinių gilinimo forma.
- Darbuotojai nuotolinio darbo galimybes išnaudoja skirtingai, o su tuo susijusias grėsmes kibernetiniam saugumui vertina kaip vidutines arba dideles.

Svarbu pažymėti, kad siekiant užtikrinti bazinį įmonės kibernetinio saugumo lygį, daugelis rekomendacijų nereikalauja didelių investicijų. Viena veiksmingiausių priemonių – nuolatinis darbuotojų švietimas bei įmonės kibernetinio saugumo politikos sukūrimas ir taikymas praktikoje.



Išsamesni apklausos rezultatai pateikiami šio dokumento Priede 2

/04/

Rekomendacijos, padėsiančios sukurti stipresnę kibernetinio saugumo aplinką įmonėje

Bazinių kibernetinio saugumo praktikų įgyvendinimas reikalauja integruoto požiūrio: taisyklių nustatymo politikos dokumentuose, procedūrų laikymosi ir techninių priemonių diegimo. Žemiau pateikiamos rekomenduojamos priemonės, sudarančios galimybes pasiekti bazinį kibernetinio saugumo lygį SVV įmonėse. Vis dėlto, kiekviena SVV įmonė turėtų, atlikusi rizikų vertinimą, pasirinkti ir taikyti tas priemones, kurios geriausiai užtikrins jos vykdomos veiklos saugumą.

Prieigos kontrolė:

- Slaptažodžių politika,
- Mažiausių privilegijų principas,
- Prieigos teisių peržiūra.

Operacijų saugumas:

- Automatiniai programinės įrangos atnaujinimai,
- Įvykių registravimas,
- Pažeidžiamumų valdymas (aukštesnio lygio),
- Kontroliuojamas įsilaužimo bandymas (aukštesnio lygio).

Tinklo saugumas:

- Belaidžio interneto ryšio saugumas.

Turto valdymas:

- IT turto inventorizacija,
- Duomenų klasifikavimas.

Kibernetinio saugumo incidentų valdymas:

- Kibernetinio saugumo incidentų valdymo planas.

Kriptografija:

- Duomenų šifravimas.

Veiklos atkūrimo valdymas:

- Atsarginės duomenų kopijos,
- Veiklos tęstinumo planas.

Žmogiškųjų išteklių saugumas:

- Nuolatinis darbuotojų švietimas ir mokymas.

Tiekėjų ir trečiųjų šalių saugumas:

- Saugumo reikalavimai sutartyse,
- Tiekėjų saugumo vertinimas (aukštesnio lygio).

/ 1 / Prieigos kontrolė

/ 1.1. / Slaptažodžių politika

Slaptažodis yra pagrindinė priemonė, užtikrinanti, kad prie sistemos prisijungtų tik įgalioti vartotojai. Siekiant užtikrinti slaptažodžių saugumą, taikomos šios rekomendacijos:

- **1. Slaptažodžių sudarymas**: naudoti ilgus, sudėtingus slaptažodžius arba slaptažodžių frazes, įtraukiant didžiąsias ir mažąsias raides, skaičius bei specialiuosius simbolius (pvz., „ŽaliaKavaMėlynasDebesis2026“). Administratorių paskyroms rekomenduojama naudoti ne mažiau kaip 15 simbolių.
- **2. Slaptažodžių keitimas**: reguliariai keisti slaptažodžius – ne rečiau nei kas 6 mėn. (administratorių paskyroms – kas 3–6 mėn.), užtikrinant, kad naujas slaptažodis nesutaptų su paskutiniais 6–8 buvusiais. Slaptažodį reikia pakeisti, jei kyla įtarimas dėl jo saugumo pažeidimo.
- **3. Unikalumas ir slaptažodžių tvarkyklės**: kiekvienai paskyrai naudoti unikalius slaptažodžius. Rekomenduojama naudoti slaptažodžių tvarkykles, kurios sugeneruoja sudėtingus slaptažodžius ir leidžia vartotojui įsiminti tik pagrindinį prisijungimo slaptažodį.

/ 1.2. / Mažiausių privilegijų principas

Mažiausių privilegijų principas yra viena esminių prieigos kontrolės priemonių, užtikrinanti, kad kiekvienas darbuotojas turėtų prieigą tik prie tos informacijos ir sistemų, kurios būtinos jo tiesioginėms užduotims atlikti. Praktika suteikti visiems darbuotojams administratoriaus lygio prieigos teises prilygsta sprendimui kiekvienam komandos nariui įteikti po raktą nuo visų įmonės durų – tai kelia didelę saugumo riziką.

Prieigos kontrolės lygiai, išdėstyti nuo mažiausiai iki labiausiai apribojančio yra šie:

- Rolėmis pagrįstos prieigos teisės (angl. RBAC *Role Based Access Control*) – bazinis, kiekvienam vartotojui suteikiamos tik reikalingos teisės.
- Kontekstinė prieiga ir privilegijuotų teisių valdymas – naudojama papildomoms saugumo sąlygoms tikrinti.
- Nulinis pasitikėjimas (angl. *Zero Trust*) – nuolatinė vartotojo ir įrenginio patikra.

Svarbu atkreipti dėmesį, kad griežtesnis prieigos teisių valdymas dažnai reikalauja papildomų išteklių ir technologijų, užtikrinančių tinkamą sistemų veikimą ir administravimą. SVV įmonėms reikėtų pradėti nuo lengviausiai įgyvendinamo, rolėmis pagrįsto prieigos teisių modelio, kurio pagrindiniai įgyvendinimo žingsniai yra:

- Nustatyti vaidmenis organizacijoje – identifikuoti pagrindines funkcijas (pvz., finansininkas, IT administratorius, pardavimų vadybininkas) ir kokią informaciją bei sistemas kiekvienas vaidmuo turi pasiekti.
- Priskirti teises pagal vaidmenis – kiekvienam vaidmeniui suteikti tik tas prieigos teises, kurios būtinos jo funkcijoms atlikti.
- Sukurti paskyras pagal vaidmenis – vartotojams priskirti vaidmenis ir unikalius prisijungimo vardus.
- Įgyvendinti technologinėje sistemoje – nustatyti leidimus programinėje įrangoje, IT sistemose ar duomenų bazėse, kad vartotojai galėtų atlikti tik savo funkcijas.
- Reguliariai peržiūrėti ir atnaujinti teises – kartą per nustatytą laikotarpį patikrinti, ar vartotojų prieigos atitinka jų dabartines funkcijas, ypač kai keičiasi pareigos ar atsakomybės.

/ 1.3. / Prieigos teisių peržiūra

Reguliari prieigos teisių peržiūra ir jų panaikinimas taip pat yra svarbi priemonė užtikrinant įmonės informacijos saugumą. Šis procesas turėtų būti aiškiai apibrėžtas vidaus tvarkose, koordinuojant veiksmus tarp žmogiškųjų išteklių padalinio ir IT padalinio. Prieigos panaikinimas turi būti vykdomas paskutinę darbuotojo darbo dieną arba nedelsiant, jei nustatoma galimų saugumo rizikų.

Įgyvendinimo rekomendacijos:

- Naudoti standartizuotą šabloną, kuriame būtų išvardintos darbuotojui suteiktos priemonės (kompiuteris, telefonas, planšetė ir kt.) bei prieigos prie programų ir paslaugų (debesijos paslaugos, nuotolinės prieigos įrankiai ir pan.).
- Užtikrinti, kad prisijungimo teisės būtų visiškai panaikintos pasibaigus darbo santykiams ar pasikeitus pozicijai.
- Apsibrėžti procedūras prieigos teisių peržiūrai darbuotojams, keičiantiems pareigas, kad būtų ribojama prieiga prie ankstesnėje pozicijoje naudotos informacijos bei prieigos prie programų ir paslaugų.

/ 1.4. / Kelių veiksnių tapatumo priemonių naudojimas (aukštesnio lygio)

Kelių veiksnių tapatumo priemonių naudojimas užtikrina, kad vartotojas turi įrodyti savo tapatybę bent dviem skirtingais autentifikacijos veiksniais. Tokiu būdu paskyros ir sistemos apsaugomos net ir tuo atveju, jei slaptažodis buvo pasisavintas.

Naudotojas turi įrodyti savo tapatybę bent dviem skirtingais autentifikacijos veiksnių tipais:

Žinojimo faktorius („Ką žinote?“): slaptažodis, PIN kodas arba atsakymas į saugumo klausimą.

Turėjimo faktorius („Ką turite?“): išmanusis telefonas, fizinis saugumo raktas (pvz., FIDO2, „YubiKey“), ID kortelė.

Buvimo faktorius („Kas esate?“): biometriniai duomenys, pvz., piršto antspaudas arba veido atpažinimas (Apple FaceID).

Įgyvendinimo rekomendacijos:

- Vengti SMS kaip antrojo veiksnio; pirmenybę teikti autentifikavimo programėlėms arba fiziniams saugumo raktams.
- Administratoriams ir darbuotojams, dirbantiems su jautriais finansiniais ar klientų duomenimis, naudoti fizinius saugumo raktus (FIDO2 standartas).
- Naudoti biometrinius duomenis (veido atpažinimą ar piršto antspaudą) greitai ir patogiai autentifikacijai.
- Papildomas autentifikacijos patvirtinimas taikomas tik pasikeitus aplinkybėms (pvz., prisijungimas iš neįprastos vietos ar naujo įrenginio), užtikrinant balansą tarp saugumo ir naudotojo patogumo.

/ 2 / Operacijų saugumas

/ 2.1. / Automatiniai programinės įrangos atnaujinimai

Automatiniai programinės įrangos atnaujinimai yra priemonė užtikrinanti įmonės informacijos saugumą ir verslo tęstinumą. Jie ne tik leidžia naudotis naujomis funkcijomis, bet ir pašalina kritines saugumo spragas, kurias galėtų išnaudoti piktavaliai. SVV įmonėms, neturinčioms nuolatinės kibernetinio saugumo komandos, automatiniai atnaujinimai veikia kaip efektyvi apsaugos sistema, mažinanti žmogiškosios klaidos ir užmaršumo riziką.

Įgyvendinimo rekomendacijos:

- Įjungti automatinį programinės įrangos atnaujinimą visuose įrenginiuose.
- Reguliariai atlikti pažeidžiamumų skenavimą, siekiant identifikuoti neatnaujintas sistemas ar programas.
- Nesuteikti vartotojams teisių išjungti ar neribotai atidėti atnaujinimų.
- Paruošti atsargines duomenų kopijas prieš atnaujinimus, kad būtų apsaugoti svarbūs duomenys.
- Formuoti atliktų atnaujinimų ataskaitas ir identifikuoti neatitikimus, kad būtų galima greitai reaguoti į kylančias rizikas.

/ 2.2. / Įvykių registravimas

Įvykių registravimas yra automatinis procesas, kurio metu sistemos fiksuoja veiksmus chronologine tvarka. Kiekvienas įrašas nurodo, kas, kada, kur ir kokį veiksmą atliko. Viena iš įvykių registravimo naudų – galimybė atkurti kibernetinių incidentų eigą ir nustatyti jų priežastis.

Įgyvendinimo rekomendacijos:

- **Prieigos valdymas ir autentifikacija:** fiksuoti visus sėkmingus ir nesėkmingus prisijungimo bandymus, paskyrų blokavimus bei slaptažodžių keitimus, siekiant anksti identifikuoti galimas kibernetines atakas.
- **Veiksmai su jautriais duomenimis:** registruoti, kas skaitė, keitė, kopijavo ar trynė informaciją, susijusią su finansais, klientų asmens duomenimis ar intelektine nuosavybe.
- **Sistemos nustatymų ir teisių pakeitimai:** fiksuoti naujus administratoriaus teisių ar saugumo nustatymų pakeitimus, kad būtų galima anksti aptikti galimus neteisėtus veiksmus.
- **Tinklo srautas ir išorinės jungtys:** stebėti ryšius tarp vidinių sistemų ir išorinius prisijungimo bandymus (pvz., VPN), atkreipiant dėmesį į neįprastą srautą ar prisijungimus iš neįprastų vietų.

/ 2.3. / Pažeidžiamumų valdymas (aukštesnio lygio)

Pažeidžiamumų valdymas apima nuolatinę sistemų peržiūrą, siekiant identifikuoti spragas, kurios leistų atlikti neautorizuotus veiksmus. Tai nėra tik sistemų skenavimas – tai visapusiškas procesas, apimantis identifikavimą, vertinimą ir šalinimą.

Įgyvendinimo rekomendacijos:

- Sudaryti visų serverių, tinklo įrangos, darbo vietų, naudojamų sistemų ir paslaugų sąrašus, kad būtų galima identifikuoti neatpažintus įrenginius ar sistemas.
- Vykdyti automatizuotus pažeidžiamumų skenavimus, atsižvelgiant į gamintojų saugumo pranešimus, bet ne rečiau nei kas ketvirtį arba po reikšmingų atnaujinimų.
- Nustatyti aiškius terminus pažeidžiamumų šalinimui.
- Užtikrinti reguliarius sistemų atnaujinimus; jei įmanoma, aktyvuoti automatinius atnaujinimus.
- Paskirstyti atsakomybes darbuotojams, užtikrinant aiškią kiekvieno darbuotojo atsakomybės sritį.
- Naudoti pažeidžiamumų registrą, kuriame dokumentuojami visi aptikti pažeidžiamumai ir jų šalinimo veiksmai.

/ 2.4. / Kontroliuojamas įsilaužimo bandymas (aukštesnio lygio)

Kontroliuojamas įsilaužimo bandymas leidžia identifikuoti saugumo spragas IT infrastruktūroje, kurias galėtų išnaudoti tikrieji piktavaliai. Šiuos bandymus atlieka etiniai įsilaužėliai (angl. *White Hat Hackers* arba angl. *Ethical Hackers*), naudojantys tas pačias technikas kaip ir tikrieji įsilaužėliai (angl. *Black Hat*), tačiau šiuos bandymus atlieka tik įmonei leidus.

Įgyvendinimo rekomendacijos:

- Atlikti reguliarias kontroliuojamas įsilaužimų simuliacijas, kad būtų patikrintos esamos apsaugos priemonės (EDR (angl. *Endpoint Detection and Response*), ugniasienės (angl. *Firewall*) ir kt.).
- Gautas ataskaitas naudoti nustatytų spragų rizikos vertinimui, identifikuojant realias ir teorines grėsmes bei prioritetizuojant jų šalinimą.
- Įtraukti darbuotojus į simuliacijas, kad jie įgytų praktinių įgūdžių tinkamai reaguoti į realias kibernetines atakas.

/ 3 / Tinklo saugumas

/ 3.1. / Belaidžio interneto ryšio saugumas

Prieiga prie belaidžio tinklo sukuria papildomų saugumo rizikų, kurias galima valdyti įgyvendinant atitinkamas procedūras ir diegiant technologinius sprendimus. Įmonės turi pasirinkti saugumo priemones, atsižvelgdamos į reikalingą saugumo lygį ir turimus išteklius.

SVV įmonėms rekomenduojama įgyvendinti bazines priemones (1 lygis), o kitos priemonės gali būti įgyvendinamos nustačius tokį poreikį po atlikto rizikos vertinimo.

- **Bazinė apsauga (1 lygis)**
  yra būtina visoms įmonėms – tai minimalus saugumo standartas, lengvai įgyvendinamas ir užtikrinantis esminę apsaugą nuo daugumos grėsmių.
- **Papildoma apsauga (2 lygis)**
  rekomenduojama, jei įmonėje yra svečių įrenginių arba norima sumažinti riziką vidiniam įmonės tinklui. Tai ne visada būtina mažoms SVV įmonėms, jei svečių įrenginių kiekis minimalus.
- **Aukštas saugumo lygis (3 lygis)**
  skirtas organizacijoms, kurios tvarko jautrius duomenis arba turi didelę IT infrastruktūrą. Mažoms įmonėms tai dažniausiai nėra būtina dėl resursų trūkumo ir įgyvendinimo sudėtingumo.

Pirmojo lygio įgyvendinimo rekomendacijos:

- **WPA3** *(angl. Wi-Fi Protected Access 3)* **šifravimas:**
  naudoti WPA3 protokolą, jei maršrutizatorius jį palaiko; vengti pasenusių TKIP (angl. *Temporal Key Integrity Protocol*) arba WEP (angl. *Wired Equivalent Privacy*) protokolų.
- **Sudėtingas slaptažodis:**
  nustatyti ilgą (ne trumpesnę nei 10 simbolių) slaptažodžio frazę, kuri neturi būti susijusi su įmonės pavadinimu ar adresu.
- **WPS išjungimas:**
  WPS (Wi-Fi Protected Setup) funkcija turi būti išjungta, kad sumažėtų neteisėtos prieigos prie tinklo rizika.

/ 4 / Turto valdymas

/ 4.1. / IT turto inventorizacija

IT turto valdymas – tai procesas, kurio metu identifikuojami, inventorizuojami ir prižiūrimi visi įmonės turimi IT įrenginiai bei sistemos. IT turto valdymas leidžia kontroliuoti jo naudojimą, sumažinti riziką ir užtikrinti tinkamą apsaugą.

Įgyvendinimo rekomendacijos:

- Sudaryti ir reguliariai atnaujinti visų IT įrenginių bei sistemų sąrašą.
- Priskirti atsakingus asmenis kiekvienam IT ištekliui.
- Dokumentuoti turto judėjimą – priskyrimą, perdavimą ar sunaikinimą.

/ 4.2. / Duomenų klasifikavimas

Duomenų klasifikavimas – tai procesas, kurio metu įmonės informacija priskiriama tam tikrai saugumo kategorijai pagal jos jautrumo lygį. Tinkamas klasifikavimas leidžia taikyti atitinkamas apsaugos priemones ir sumažinti neteisėtos prieigos ar duomenų praradimo riziką.

Įgyvendinimo rekomendacijos:

- Nustatyti pagrindines duomenų kategorijas, pvz., „vieši“, „vidiniai“, „konfidencialūs“.
- Priskirti atsakingus asmenis už duomenų klasifikavimą ir peržiūrą.
- Užtikrinti, kad prieiga prie duomenų būtų ribojama pagal jų klasifikaciją.
- Periodiškai peržiūrėti ir atnaujinti klasifikaciją, ypač kai keičiasi duomenų naudojimo ar saugumo aplinkybės.

/ 5 / Kibernetinio saugumo incidentų valdymas

/ 5.1. / Kibernetinio saugumo incidentų valdymo planas

Kibernetinio saugumo incidentų valdymas – tai procesas, skirtas identifikuoti, registruoti, vertinti ir reaguoti į IT infrastruktūros bei informacinių sistemų ar duomenų saugumo įvykius.

Įgyvendinimo rekomendacijos:

- **Incidentų apibrėžimas ir registravimas.**
  Aiškiai nustatyti, kas laikoma kibernetiniu incidentu (pvz., neteisėta prieiga, duomenų nutekėjimas, IT sistemos trikdžiai). Apibrėžti registracijos formą ir kriterijus, kaip vertinti incidento svarbą ir prioritetą.
- **Atsakomybės ir veiksmų planas.**
  Paskirti atsakingus darbuotojus ir aprašyti jų atsakomybės sritis kiekviename incidento valdymo etape. Nustatyti veiksmų seką nuo incidento aptikimo iki jo uždarymo.
- **Pranešimo procesas.**
  Sukurti aiškų ir paprastą kanalą, kaip darbuotojai praneša apie incidentus. Užtikrinti, kad visi darbuotojai žinotų apie pranešimo procedūrą ir kontaktinius asmenis.
- **Dokumentacija ir analizė.**
  Fiksuoti visus incidentus, jų aplinkybes, priimtus sprendimus ir veiksmus. Periodiškai peržiūrėti incidentų istoriją, kad būtų galima identifikuoti tendencijas, rizikas ir tobulinti prevencines priemones.

/ 6 / Kriptografija

/ 6.1. / Duomenų šifravimas

Duomenų šifravimas – tai priemonė, skirta apsaugoti įmonės informaciją tiek saugojimo, tiek perdavimo metu. Net jei kompiuteris ar telefonas prarandamas, šifruoti duomenys lieka saugūs. Kai duomenys siunčiami internetu, šifravimas apsaugo juos nuo perėmimo ar pakeitimo. Tai užtikrina, kad informacija liktų konfidenciali ir nepakitusi.

Įgyvendinimo rekomendacijos:

- Šifruoti duomenis tiek saugojimo, tiek perdavimo metu.
- Naudoti stiprius ir pripažintus šifravimo algoritmus, tokius kaip AES-256, RSA ar TLS.
- Užtikrinti, kad nešiojamieji kompiuteriai, telefonai ir kitos laikmenos būtų apsaugotos pilno disko šifravimu (pvz., BitLocker).
- Šifravimo raktus suteikti tik įgaliotiems asmenims, atsakingiems už duomenų atkūrimą.

/ 7 / Veiklos atkūrimo valdymas

/ 7.1. / Atsarginės duomenų kopijos

Reguliarus atsarginių duomenų kopijų kūrimas yra būtinas informacijos saugumui užtikrinti. Klientų sąrašų, sąskaitų ar darbo archyvų praradimas gali sukelti reikšmingą žalą, ypač SVV įmonėms. Atsarginių duomenų kopijų tvarkymas priklauso nuo įmonės poreikių – kaip greitai reikia atstatyti duomenis.

SVV įmonėms rekomenduojama įgyvendinti bazines priemones (1 arba 2 lygiai), o kitos priemonės gali būti įgyvendinamos nustačius tokį poreikį po atlikto rizikos vertinimo.

- **Rankinis kopijavimas (1 lygis)**
  paprasčiausias metodas, kai duomenys periodiškai kopijuojami į išorinę laikmeną ir laikomi saugioje vietoje.
- **Automatinis sinchronizavimas į debesiją (2 lygis)**
  duomenys automatiškai kopijuojami į debesijos saugyklą ar duomenų centrą; patogu, bet reikalaujama turėti interneto ryšį ir daugiau technologinių priemonių.
- **3-2-1 principas (3 lygis)**
  sukuriamos trys atsarginės duomenų kopijos: dvi skirtingose laikmenose ir viena kopija laikoma kitoje vietoje (pvz., debesyje).
- **Fizinės atskirties (angl. *Air-Gap*) ir nepriklausomų kopijų (angl. *Immutable backups*) principas (4 lygis)**
  viena laikmena fiziškai atjungta nuo tinklo, kopijos negalima ištrinti ar pakeisti nustatytą laikotarpį; skirti aukščiausio lygio duomenų saugumui.

Pirmojo lygio įgyvendinimo rekomendacijos:

- Periodiškai (pvz., kartą per mėnesį) nukopijuoti informaciją į išorinį USB diską arba kitą laikmeną.
- Laikyti laikmeną saugioje vietoje.
- Periodiškai patikrinti, ar duomenų kopijos nesugadintos.

Antro lygio įgyvendinimo rekomendacijos:

- Užtikrinti saugų prisijungimą, naudojant stiprius slaptažodžius ar dviejų veiksnių autentifikavimą.
- Įgalinti duomenų automatinį kopijavimą į debesijos saugyklą ar duomenų centrą.

/ 7.2. / Veiklos tęstinumo planas

Veiklos tęstinumo planas skirtas užtikrinti kritinių verslo funkcijų tęstinumą ir greitą atstatymą po incidentų ar trikdžių, įskaitant IT infrastruktūros sutrikimus, duomenų praradimą ar kibernetinius incidentus.

Įgyvendinimo rekomendacijos:

- **Kritinių funkcijų identifikavimas.** Nustatyti verslo procesus, be kurių įmonė negali veikti. Įvertinti, kiek laiko kiekvienas procesas gali nevykti.
- **Rizikų ir grėsmių analizė.** Įvertinti galimas grėsmes: gaisrus, IT trikdžius, kibernetines atakas, gamtines katastrofas. Įvertinti grėsmių poveikį kritinėms funkcijoms.
- **Ištekliai ir priemonės.** Užtikrinti atsarginių duomenų kopijų ir tinkamos infrastruktūros atsarginių elementų prieinamumą.
- **Dokumentavimas ir komunikacija.** Planas turi būti prieinamas atsakingiems asmenims. Įmonės darbuotojai turi žinoti, kaip elgtis ekstremalių situacijų atveju.
- **Testavimas ir priežiūra.** Reguliariai testuoti planą. Atnaujinti planą po pokyčių organizacijoje arba pasikeitus grėsmėms.
- **Atsakomybės ir vaidmenų nustatymas.** Paskirti atsakingus darbuotojus už kritinių procesų atkūrimą. Apibrėžti jų veiksmus ekstremalių situacijų metu.
- **Atkūrimo procedūrų parengimas.** Sukurti veiksmų planus kritinių funkcijų atstatymui. Įtraukti duomenų atkūrimą, IT infrastruktūros atstatymą.

/ 8 / Žmogiškųjų išteklių saugumas

/ 8.1. / Nuolatinis darbuotojų švietimas ir mokymas

Reguliarus darbuotojų švietimas ir mokymai kibernetinio saugumo srityje mažina žmogiškosios klaidos riziką, kuri dažnai yra pagrindinė sėkmingų kibernetinių atakų priežastis. Jie suteikia darbuotojams žinių ir praktinius įgūdžius atpažinti įtartinus elgesio modelius, pavojingus el. laiškus ar nuorodas. Tinkamai paruošta komanda geba greičiau ir tiksliau reaguoti į incidentus. Mokymai skatina saugų kasdienį darbo elgesį ir didina darbuotojų atsakomybę už informacijos apsaugą. Ilgalaikėje perspektyvoje švietimas stiprina įmonės bendrą kibernetinio saugumo kultūrą ir mažina galimą finansinę bei reputacinę žalą.

Įgyvendinimo rekomendacijos:

- Vykdyti reguliarius kibernetinio saugumo mokymus visiems darbuotojams.
- Pritaikyti mokymų turinį pagal darbuotojų pareigybes.
- Naudoti praktinius pavyzdžius ir situacijų simuliacijas, kurie iliustruoja tikras atakas ir galimas pasekmes.
- Parengti aiškią ir suprantamą mokymų medžiagą.
- Tikrinti mokymų efektyvumą, imituojant atakas ir vertinant darbuotojų reakciją.

/ 9 / Tiekėjų ir trečiųjų šalių saugumas

/ 9.1. / Saugumo reikalavimai sutartyse

Tiekėjų ir trečiųjų šalių saugumo valdymas užtikrina, kad partneriai laikytųsi įmonės saugumo reikalavimų. Saugumo reikalavimai turi būti įtraukti į sutartis, apibrėžiant atsakomybes, saugumo standartus ir atitikties tikrinimo mechanizmus. Tinkamai valdomi tiekėjai mažina informacijos nutekėjimo, neteisėtos prieigos ir kibernetinių incidentų riziką.

Įgyvendinimo rekomendacijos:

- **Saugumo reikalavimų nustatymas sutartyse.**
  Saugumo reikalavimai turi būti nustatyti sutartyse su naujais tiekėjais, įskaitant duomenų apsaugos standartus, pranešimų apie kibernetinius incidentus procedūras ir atsakomybės ribas.
- **Tiekėjų vertinimas.**
  Esami tiekėjai turėtų būti vertinami pagal atitiktį saugumo standartams, pvz., per periodines ataskaitas, auditus.
- **Atsakomybių apibrėžimas.**
  Atsakomybės tiekėjams ir įmonės darbuotojams turi būti aiškiai apibrėžtos, įtraukiant veiksmus kibernetinio saugumo incidento atveju bei įsipareigojimus laikytis nustatytų procedūrų.
- **Periodinis saugumo tikrinimas.**
  Periodiškai tikrinti tiekėjų saugumą, įvertinant fizinę ir skaitmeninę infrastruktūrą, prieigos teisių valdymą ir duomenų apsaugos priemones.
- **Sutarties atnaujinimas.**
  Atnaujinti sutartis pagal nustatytų saugumo standartų pasikeitimus arba po pastebėtų neatitikimų, kad partnerių atsakomybės ir įsipareigojimai visuomet atitiktų organizacijos reikalavimus.

/ 9.2. / Tiekėjų saugumo vertinimas (aukštesnio lygio)

Tiekėjų saugumo vertinimas yra procesas, skirtas patikrinti, ar tiekėjai laikosi įmonės nustatytų saugumo standartų ir procedūrų. Vertinimo tikslas – identifikuoti rizikas, susijusias su duomenų apsauga, prieigos kontrolės laikymusi bei atsakomybės vykdymu. Šis procesas padeda sumažinti tiekėjų keliamą grėsmę įmonės IT ir informacijos saugumui.

Įgyvendinimo rekomendacijos:

- **Tiekėjų sąrašas ir kontaktai.**
  Sudaryti visų esamų tiekėjų bei jų teikiamų paslaugų sąrašą.
- **Periodinės ataskaitos.**
  Reikalauti iš tiekėjų periodinių saugumo ataskaitų, apimančių fizinės ir skaitmeninės infrastruktūros būklę, prieigos teisių ir kibernetinių incidentų valdymą.
- **Vertinimo kriterijai.**
  Nustatyti aiškius vertinimo kriterijus, kaip sertifikato (pvz. ISO 27001) turėjimą, pranešimo apie kibernetinius incidentus laikus.
- **Rizikų vertinimas.**
  Įvertinti tiekėjo teikiamų paslaugų poveikį įmonės saugumui ir nustatyti, kurie tiekėjai kelia didžiausią riziką.

/ PRIEDAS 1 /

Nuorodos į užsienio šalių kibernetinio saugumo informacijos šaltinius ir priemones

Naudinga informacija, susijusi su žinių apie kibernetinį saugumą, stiprinimu:

- **TIS2 direktyva (Europos Sąjunga) -**
  https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32022L2555
- **NIST kibernetinio saugumo sistema (JAV) -**
  https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
- **Žinomų išnaudotų pažeidžiamumų katalogas (JAV) -**
  https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Saugių debesijos verslo programų projektas (JAV) -**
  https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
- **Pilnas SVV siūlomų priemonių sąrašas (JAV) -**
  https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/smb-resources
- **Internetinė mokymų programa (Estija) -**
  https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest
- **Analizės ir tyrimai, kuriais siekiama stiprinti kibernetinį saugumą (Estija) -**
  https://www.ria.ee/en/cyber-security/national-coordination-centre-ncc-ee/cybersecurity-future-technologies
- **Mėnesinės ir metinės ataskaitos apie kibernetinį saugumą (Estija) -**
  https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/situation-cyberspace
- **Kibernetinio saugumo vadovas SVV (Kipras) -**
  https://ncc.cy/images/educational-material/pwc/Cyber-Guide-SMEs%20-FINAL-EN.pdf
- **Kibernetinio saugumo pagrindai SVV (Kipras) -**
  https://ncc.cy/images/ENGLISH_HYGIENE.pdf
- **Mokomoji medžiaga apie kibernetinį saugumą (Kipras) -**
  https://ncc.cy/en/educational-material
- **Kibernetinio saugumo pagrindų sistema (Belgija) -**
  https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Praktinės priemonės kibernetinio saugumo vertinimui:

- **Kibernetinio saugumo higienos paslauga (JAV) -**
  https://www.cisa.gov/cyber-hygiene-services
- **Kenkėjiškų programų analizė (JAV) -**
  https://www.cisa.gov/resources-tools/services/malware-analysis
- **Atvirojo kodo tinklo srauto analizės priemonė Malcolm (JAV) -**
  https://www.cisa.gov/resources-tools/services/malcolm
- **Internetinių nuorodų patikrinimo įrankis (Kipras) -**
  https://getsafeonline.dsa.ee.cy/en/home
- **Kibernetinio saugumo brandos vertinimo forma (Belgija) -**
  https://atwork.safeonweb.be/tools-resources/self-assessment
- **SVV gidas: atsakas ir atsigavimas (Jungtinė Karalystė) -**
  https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery
- **Personalo saugumo mokymų programa (Jungtinė Karalystė) -**
  https://www.ncsc.gov.uk/information/top-tips-for-staff
- **Kibernetinio saugumo patikrinimo įrankis (Jungtinė Karalystė) -**
  https://checkcybersecurity.service.ncsc.gov.uk/
- **Kibernetinių veiksmų įrankių rinkinys (Jungtinė Karalystė) -**
  https://cybertoolkit.service.ncsc.gov.uk/

/ PRIEDAS 2 /

Smulkių ir vidutinių įmonių kibernetinio saugumo būklės vertinimas: apklausos rezultatai

SVV įmonių kibernetinio saugumo būklės vertinimo apklausa

Apklausoje buvo siekiama įvertinti, kaip SVV įmonės suvokia kibernetinį saugumą bei ar pasikeitė jų požiūris į kibernetinį saugumą.

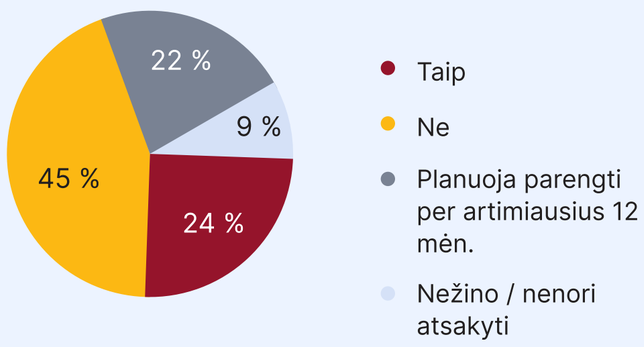
134 įmonės dalyvavo apklausoje

- labai mažos įmonės: 49
- mažos įmonės: 38
- vidutinės įmonės: 47

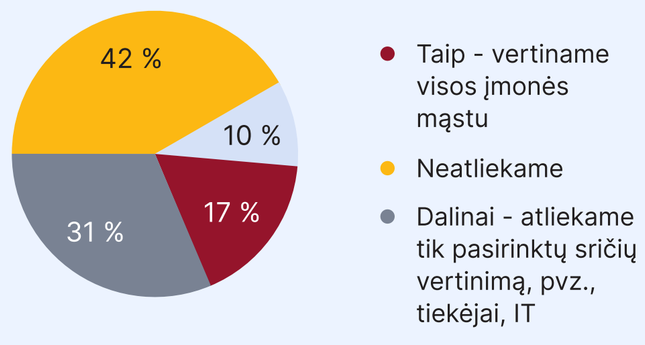
71 % Įmonių jaučiasi iš dalies arba visiškai pasirengusios atremti galimą kibernetinę ataką.

11 % Įmonių teigė turinčios veiksmų planą, kaip vykdytų veiklą po didelio kibernetinio incidento ar kito įvykio, jei netektų prieigos prie duomenų, juos prarastų, sutriktų techninės priemonės ar nutrūktų ryšio paslaugos.

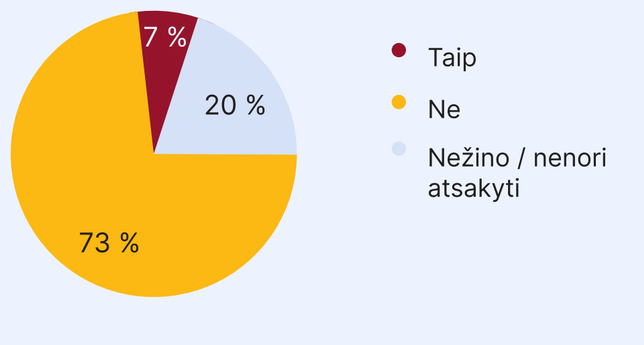
Ar Jūsų įmonė turi dokumentuotą vidinę kibernetinio saugumo politiką?



Ar Jūsų įmonė vykdo kibernetinio saugumo vertinimą?



Ar Jūsų įmonė mato kibernetinio saugumo priemonių naudą?



29 % Įmonių nurodė per pastaruosius finansinius metus neinvestavusios į kibernetinio saugumo priemones, susijusias su kibernetinio saugumo stiprinimu.

75 % Įmonių teigė nesusidūrusios su bet kokios formos kibernetine ataka, kurios rezultate būtų fiksuotas kibernetinis incidentas.

62 % Įmonių nurodė, kad joms svarbu, kad jų verslo partneriai turėtų kibernetinio saugumo standartą ir jo laikytųsi.

Apklausoje dalyvavusių įmonių profilis

Apklausoje buvo kviečiamos dalyvauti smulkios ir vidutinės įmonės, kuriose dirba iki 250 darbuotojų ir metinės pajamos neviršija 50 mln. Eur arba įmonės balanse nurodyto turto vertė neviršija 43 mln. Eur. Dalyvavusios apklausoje įmonės pasiskirstė žemiau nurodyta proporcija:

- **Labai mažos įmonės** - 49 respondentai;
- **Mažos įmonės** - 38 respondentai;
- **Vidutinės įmonės** - 47 respondentai.

Daugiausiai apklausoje dalyvavusių įmonių buvo registruotos Vilniaus apskrityje (35 %), Kauno apskrityje (19 %) ir Klaipėdos apskrityje (10 %). Įmonės nurodė savo veiklos sektorius, įskaitant ypatingos svarbos ir itin svarbius sektorius, kaip numatyta Lietuvos Respublikos kibernetinio saugumo įstatyme (KSĮ). Daugiausiai respondentų atstovavo sveikatos priežiūros (15 %), viešojo administravimo (9 %) bei gamybos ir švietimo (po 8 %) sektorius. Pažymėtina, kad švietimas nebuvo priskirtas nei ypatingos svarbos, nei itin svarbiems sektoriams.

Iš apklausoje dalyvavusių įmonių 28 % nurodė, kad jos buvo įtrauktos į kibernetinio saugumo registrą pagal KSĮ, 38 % teigė, kad nebuvo įtrauktos, o 34 % nesugebėjo atsakyti arba nenorėjo pateikti informacijos apie savo įtraukimo statusą.

Papildomai įmonių buvo teiraujamasi, ar jos seka naujausią informaciją iš Krašto apsaugos ministerijos (KAM) arba Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (NKSC) socialiniuose tinkluose. 46 % respondentų nurodė, kad neseka KAM, o 50 % neseka NKSC skelbiamų naujienų socialiniuose tinkluose. Likusi dalis respondentų informaciją daugiausiai stebi „Facebook“ platformoje bei KAM ir NKSC oficialiuose interneto puslapiuose.

Beveik 40 % apklaustų respondentų nebuvo susipažinę su 2020 m. KAM ir NKSC paruoštu leidiniu „Kibernetinio saugumo vadovas verslui“[40], o 36 % apie jį nieko nebuvo girdėję. Šiuos rezultatus galėjo lemti tai, kad dauguma dalyvių neseka informacijos socialiniuose tinkluose ar oficialiuose tinklapiuose. Dauguma respondentų nurodė, kad informacijos apie kibernetinį saugumą ieškotų NKSC puslapyje, naudotų paieškos sistemas (pvz., „Google“) arba pasitelktų DI įrankius, tokius kaip „Gemini“ ar „ChatGPT“.

Kibernetinio saugumo brandos vertinimas

Beveik visi apklausoje dalyvavę respondentai naudoja elektroninį paštą (99 %). Kitos dažniausiai naudojamos elektroninės paslaugos yra elektroninė bankininkystė (95 %), interneto svetainės (92 %), socialiniai tinklai (82 %) ir Elektroninių valdžios vartų portalas (66 %). 2020 m. naudojamų paslaugų struktūra buvo panaši, tačiau reikšmingiausias pokytis pastebėtas elektroninės bankininkystės ir interneto svetainių paslaugų naudojime – naudotojų skaičius padidėjo daugiau nei 15 %. Šiuos pokyčius galima sieti su vis didėjančiu elektroninių paslaugų pasiūlos skaičiumi.

Kibernetinio saugumo politika

Apklausos duomenimis, apie 45 % įmonių neturi dokumentuotos vidinės kibernetinio saugumo politikos. Tuo tarpu 24 % įmonių ją jau turi, o 22 % planuoja parengti per artimiausius 12 mėn. Likę 9 % respondentų nežinojo arba nenorėjo atsakyti į šį klausimą. Palyginus su 2020 m., kai 68 % įmonių teigė neturėjusios ar nežinojusios, ar turi vidinę politiką. Matoma teigiama tendencija – vis daugiau įmonių proaktyviai rengia kibernetinio saugumo politikos dokumentus. Tokia politika apibrėžia organizacijos kibernetinio saugumo reikalavimus, padeda greičiau reaguoti į incidentus, priimti tinkamus sprendimus ir informuoti atsakingus asmenis.

Tarp įmonių, kurios yra dokumentavę vidinę kibernetinio saugumo politiką, pirmauja vidutinės įmonės (37 % visų dalyvavusių vidutinių įmonių). Tuo tarpu 68 % labai mažų ir 55 % mažų įmonių kibernetinio saugumo politikos nėra dokumentavusios.

[40] „Kibernetinis saugumas ir verslas. Ką turi žinoti kiekvienas įmonės vadovas“. Nuoroda: https://www.nksc.lt/doc/Kibernetinio_saugumo_vadovas_verslui_2020.pdf

Atsakingi asmenys

Šių metų apklausoje pastebimas neigiamas pokytis dėl kibernetinio saugumo atsakomybės priskyrimo: 46 % įmonių neturėjo darbuotojo, padalinio ar išorės paslaugų tiekėjo, atsakingo už kibernetinį saugumą, palyginti su 32 % 2020 m. Tuo pačiu metu išaugo įmonių, turinčių vidinį darbuotoją, atsakingą už kibernetinį saugumą – nuo 3 % 2020 m. iki 14 % 2026 m. Taigi, įmonės yra labiau linkusios turėti darbuotoją, atsakingą už kibernetinį saugumą, įmonės viduje.

15 % įmonių, turėjusių vidinį darbuotoją, atsakingą už kibernetinį saugumą, neturėjo dokumentuotos vidinės kibernetinio saugumo politikos. Tai kelia klausimų, ar paskirtas asmuo aiškiai supranta savo atsakomybės ribas ir remiasi nustatytomis procedūromis vykdydamas kibernetinio saugumo funkcijas įmonėje.

Kas penkta (21 %) įmonė turėjo atsakingą asmenį įmonės viduje, dažniausiai tai buvo vidutinio dydžio įmonės. Šios įmonės taip pat dominavo tarp tų, kurios pasitelkė išorės paslaugų tiekėjus (56 %).

Daugiau nei pusė (68 %) apklausoje dalyvavusių įmonių nurodė, kad kibernetinis saugumas jų įmonėje yra svarbus arba labai svarbus. Pagal 2020 m. apklausos duomenis, tokių įmonių buvo 74 % Šie duomenys rodo, kad kibernetinio saugumo svarba įmonėse išliko panaši.

Kibernetinio saugumo rizikos

14 % apklaustų įmonių nurodė, kad visiškai įvertino kylančias kibernetinio saugumo rizikas. Dauguma (69 %) savo gebėjimą vertinti rizikas įvertino kaip vidutinį arba gerą, o 7 % teigė visiškai nesugebantys įvertinti kibernetinio saugumo rizikų. 2020 m. duomenis, 72 % įmonių nurodė, kad nesugeba arba nežino, ar geba įvertinti rizikas. Šie pokyčiai rodo, kad vis daugiau įmonių skiria dėmesio rizikų vertinimui ir darbuotojų žinių gilinimui.

71 % įmonių nurodė, kad jaučiasi iš dalies arba visiškai pasirengusios atremti galimą kibernetinę ataką arba suvaldyti kibernetinį incidentą, tuo tarpu 29 % jautėsi silpnai pasirengusios arba visiškai nepasirengusios. 2020 m. duomenimis net 74 % įmonių teigė nesančios pasiruošę arba nežinančios, ar yra pasiruošę atremti kibernetines atakas. Šiam pokyčiui, lyginant su 2020 m. duomenimis, daugiausiai įtakos galėjo turėti vis didėjantis informacijos apie kibernetinį saugumą prieinamumas, organizuojami mokymai bei didėjantis įmonių sąmoningumas.

68 % įmonių, kurios nurodė visiškai įvertinusios kylančias kibernetinio saugumo rizikas, taip pat pažymėjo, kad kibernetinis saugumas jų įmonėje yra labai svarbus.

Pusė apklaustų įmonių (51 %) nurodė, kad neatliko arba nežino apie kibernetinio saugumo rizikų vertinimą įmonės viduje. 31 % įmonių atliko pasirinktų sričių vertinimus (pvz., tiekėjų ar IT), o 17 % nurodė vykdantys visos įmonės mastu rizikų vertinimą. 2020 m. tokių įmonių, kurios neatliko arba nežinojo apie rizikų vertinimą, buvo 79 % Duomenys rodo teigiamą tendenciją – mažėja įmonių, nevykdančių rizikų vertinimo, kas leidžia daryti prielaidą, kad įmonės geriau suvokia kibernetinio saugumo svarbą.

Tarp įmonių, kurios jautėsi iš dalies arba visiškai pasirengusios atremti galimą kibernetinę ataką ar suvaldyti kibernetinį incidentą, didžiąją dalį sudarė vidutinės įmonės (43 %). Tuo tarpu tarp įmonių, kurios jautėsi visiškai nepasirengusios arba silpnai pasirengusios, didžiąją dalį sudarė mažos ir labai mažos įmonės (84 %). Ši statistika leidžia daryti prielaidą, kad vidutinės įmonės skiria daugiau dėmesio kibernetiniam saugumui nei mažos ar labai mažos įmonės.

Kibernetinio saugumo mokymai

46 % įmonių nurodė, kad jų darbuotojams nėra organizuojami arba įsigyjami kibernetinio saugumo mokymai. 2020 m. kibernetinio saugumo mokymų neorganizavo net 72 % apklausoje dalyvavusių įmonių. Šis pokytis rodo, kad vis daugiau įmonių skiria dėmesio darbuotojų apmokymui kibernetinio saugumo srityje.

Daugiau nei pusė įmonių nurodė, kad patraukliausi kibernetinio saugumo mokymų formatai yra nuotoliniai mokymai (60 %) ir internetiniai kursai, seminarai bei vaizdo įrašai (51 %). 40 % įmonių mato poreikį mokymams įmonės viduje, o 38 % – informacijai internetiniuose puslapiuose. 2020 m. dauguma įmonių kaip patraukliausią būdą nurodė konsultacijas su ekspertais (57 %), informaciją internetiniuose puslapiuose (50 %) ir mokymus įmonės viduje (43 %). Pokyčiui daugiausia įtakos turėjo COVID-19 pandemija, po kurios daug veiklų tapo prieinamos nuotoliniu būdu, o įvykusių renginių įrašai yra pasiekiami patogiu metu.

Beveik kas penkta įmonė (18 %) suteikė prieigą prie kibernetinio saugumo mokymų visiems darbuotojams, daugiausia vidutinės įmonės (44 %).
16 % įmonių planuoja organizuoti mokymus per artimiausius 12 mėn., iš jų daugumą sudaro vidutinės įmonės (52 %).
Mažiausiai dėmesio mokymams skiria labai mažos ir mažos įmonės (85 %).

Kibernetinio saugumo priemonių suteikiama nauda

Net 73 % apklaustųjų pripažino kibernetinio saugumo priemonių naudą, 20 % nebuvo tikri arba nenorėjo atsakyti, o 7 % nematė šių priemonių naudos. 2020 m. tokią naudą nurodė 67 % įmonių. Šie duomenys leidžia daryti prielaidą, kad vis daugiau įmonių, didindamos dėmesį kibernetinio saugumo stiprinimui, geriau supranta priemonių teikiamą naudą.

Tarp įmonių, pripažįstančių kibernetinio saugumo priemonių naudą, 57 % sudaro įmonės, vertinančios kibernetinį saugumą kaip svarbų arba labai svarbų savo veiklai. Teigiamam priemonių naudos vertinimui galėjo turėti įtakos didėjantis prieinamos informacijos kiekis bei praktiškai pritaikomos rekomendacijos, skelbiamos tiek Lietuvos, tiek užsienio kibernetinio saugumo centruose.

Kibernetinio saugumo priemonių pasirinkimas

60 % įmonių nurodė, kad neturi pakankamų žinių arba nežino, ar turi pakankamai kompetencijos pasirinkti tinkamas saugumo priemones įmonės apsaugai užtikrinti. Iš jų 40 % pripažino kibernetinio saugumo priemonių naudą. Tai rodo, kad dalis įmonių vis dar abejoja savo gebėjimu pasirinkti tinkamas priemones.

35 % įmonių nurodė, kad kibernetinio saugumo priemonės yra per brangios, 30 % teigė neturintys vidinių kompetencijų tinkamų priemonių pasirinkimui, o dar 30 % – kad nėra susipažinę su siūlomomis priemonėmis. 2020 m. beveik pusė įmonių (48 %) manė, kad priemonės yra per brangios. Tai rodo, kad per pastaruosius metus sumažėjo įmonių, vertinančių kibernetinio saugumo priemones kaip neįperkamas, galimai dėl didesnio susipažinimo su priemonių nauda ir kibernetinio saugumo svarbos įmonės veiklai pripažinimo.

Kas penkta (20 %) labai maža įmonė teigė turinti pakankamas kibernetinio saugumo priemones, tuo tarpu kas trečia (38 %) vidutinė įmonė nurodė, kad priemonės yra per brangios.

Kibernetinio saugumo priemonės

Dažniausiai įmonės savo veikloje naudojo šias kibernetinio saugumo technines priemones: antivirusines programas (78 %), atsarginių kopijų kūrimą arba debesijos saugumo sprendimus (65 %) ir ugniasienes (58 %).

44 % apklaustų įmonių nurodė, kad yra pasirengusios investuoti į kibernetinio saugumo priemones siekdamos užtikrinti veiklos tęstinumą ir įmonės reputaciją, tuo tarpu 43 % nežinojo arba nenorėjo atsakyti. 2020 m. duomenimis, 74 % įmonių teigė, kad investuotų į kibernetinį saugumą dėl įmonės veiklos tęstinumo ir klientų apsaugos. Tai rodo, kad ankstesniais metais įmonės buvo labiau linkusios investuoti į kibernetinį saugumą, o šiuo metu vis daugiau kibernetinio saugumo stiprinimui skirtų priemonių nereikalauja investicijų.

Iš įmonių, pasirengusių investuoti į kibernetinio saugumo priemones, 51 % nurodė turinčios pakankamai žinių apie galimas kibernetinio saugumo priemones.
Tuo tarpu tarp įmonių, kurios nežinojo arba nenorėjo atsakyti dėl savo pasirengimo investuoti, 29 % teigė turinčios reikiamas žinias apie priemonių pasirinkimą.

Investicijos į kibernetinio saugumo priemones

Beveik trečdalis (30 %) įmonių per pastaruosius finansinius metus neinvestavo į kibernetinio saugumo stiprinimą. Kiek mažiau nei kas penkta įmonė (21 %) skyrė tam mažiau nei 1 000 Eur, 18 % – nuo 1 000 iki 10 000 Eur, o 7 % – daugiau nei 10 000 Eur.

Tarp neinvestavusių daugiausiai buvo labai mažos įmonės (53 %), o tarp didžiausias investicijas atlikusių įmonių lyderiavo vidutinės įmonės (63 %), iš kurių pusė (50 %) nurodė turinčios pakankamai žinių kibernetinio saugumo priemonių pasirinkimui.

Įmonių priklausomumas nuo elektroninių paslaugų

33 % apklaustųjų nurodė, kad jų įmonės veikla visiškai priklauso nuo elektroninių paslaugų, o 53 % jautėsi iš dalies arba labai priklausomi nuo šių paslaugų. Tarp įmonių, kurios savo veiklą įvardijo kaip visiškai priklausančią nuo elektroninių paslaugų, 39 % turėjo dokumentuotą vidinę kibernetinio saugumo politiką, o 36 % neturėjo ir neplanuoja jos parengti per artimiausius 12 mėn. Ši statistika rodo, kad nors įmonės vertina elektronines paslaugas kaip svarbų veiklos komponentą, nemaža dalis nėra tinkamai pasirengusios reaguoti į galimas grėsmes.

Incidentų patirtys ir pasirengimas

60 % įmonių nurodė, kad įvykusi kibernetinė ataka turėtų didelės arba labai didelės įtakos jų veiklai. 2020 m. apklausoje panašus skaičius įmonių (58 %) taip pat pripažino, kad kibernetinis incidentas turėtų didelės įtakos įmonės veiklai. Tai rodo, kad įmonės tiek anksčiau, tiek dabar vertina galimą kibernetinių incidentų riziką savo veiklai.

Vidutinės įmonės dažniau įvertina kibernetinių atakų poveikį kaip reikšmingą (68 %), palyginti su mažomis (61 %) ir labai mažomis įmonėmis (51 %).

Kibernetiniu incidentu pasibaigusios kibernetinės atakos

75 % įmonių teigė, kad per pastaruosius 12 mėn. nepatyrė jokios kibernetinės atakos, sukėlusios kibernetinį incidentą. Tai ženkliai skiriasi nuo 2020 m. apklausos, kai apie trečdalis įmonių (30 %) nurodė nesusidūrę su kibernetiniu incidentu. Tokį pokytį galėjo lemti didesnis dėmesys tiek technologiniams sprendimams, tiek darbuotojų mokymui.

16 % įmonių per pastaruosius metus patyrė kibernetinį incidentą po kibernetinės atakos. Iš jų 52 % nurodė, kad tokių atakų buvo nuo vienos iki trijų. Dažniausiai atakos buvo susijusios su nepageidaujamų laiškų platinimu (81 %), neteisėta veikla ar sukčiavimu (39 %) bei mėginimais įsilaužti (29 %). Statistika išlieka panaši 2020 m. statistikai, kai taip pat daugiausiai atakų buvo susijusios su nepageidaujamais laiškais (46 %). Kibernetinių atakų metodai iš esmės nepasikeitė.

39 %

įmonių, kurios savo veiklą įvardijo kaip visiškai priklausančią nuo elektroninių paslaugų, turėjo dokumentuotą vidinę kibernetinio saugumo politiką

75 %

įmonių teigė nesusidūrusios su bet kokios formos kibernetine ataka, kurios rezultate būtų fiksuotas kibernetinis incidentas

16 %

įmonių per pastaruosius metus patyrė kibernetinį incidentą po kibernetinės atakos

Kibernetinių incidentų sukelti nuostoliai

48 % įmonių, patyrusių kibernetinį incidentą, nurodė, kad negali tiksliai įvardinti, kokio tipo nuostolius sukėlė incidentas. Panaši situacija buvo ir 2020 m., kai 53 % įmonių teigė nežinančios galimų nuostolių masto. Tai rodo, kad daugelis įmonių vis dar neturi aiškių metodų vertinti nuostolius, ypač susijusius su duomenų vientisumo, konfidencialumo ar prieinamumo pažeidimais.

43 % įmonių, patyrusių incidentą, patyrė veiklos sutrikimų.

Daugiau nei pusė (57 %) įmonių įvertino, kad kibernetinių incidentų padaryta žala nesiekė 1 000 Eur, o trečdalis (33 %) nenorėjo arba negalėjo atsakyti. 2020 m. žalą, nesiekiančią 1 000 Eur, įvardijo 40 % įmonių, patyrusių incidentus. Tai leidžia manyti, kad įmonės, neturėdamos aiškių metodų nuostoliams įvertinti, linkusios juos vertinti kaip nedidelius – neviršijančius 1 000 Eur.

Informavimas apie kibernetinius incidentus

Apie įvykusį kibernetinį incidentą 52 % įmonių praneštų NKSC, 48 % – interneto ar tinklo paslaugų tiekėjui, o 44 % – policijai. 2020 m. dauguma įmonių nurodė, kad kreiptųsi į interneto ar tinklo paslaugų tiekėją (41 %), policiją (35 %) ir bankus ar kredito įstaigas (28 %).

78 % įmonių teigė, kad veiksmingiausia valstybės pagalbos forma kibernetinio saugumo stiprinimui būtų paruošti šablonai ir įrankiai, 66 % nurodė subsidijuojamus mokymus, o 45 % – finansinę paramą projektų vykdymui. Reikėtų pažymėti, kad NKSC šiuo metu siūlo įvairius įrankius kibernetinio saugumo stiprinimui, taip pat yra prieinami užsienio šalių siūlomi įrankiai anglų kalba.

Naujos grėsmės ir jų poveikis

Šioje dalyje pateikti duomenys nėra lyginami su 2020 m. apklausa, nes tuo metu grėsmės ir jų poveikis kibernetiniam saugumui nebuvo nagrinėjami.

Įmonių naudojamos DI ir debesijos paslaugos bei jų rizikų vertinimas

73 % įmonių nurodė, kad jų darbuotojai naudoja DI priemones. Tarp populiariausių – teksto redagavimo ir pokalbių įrankiai (pvz., „ChatGPT“, „Google Gemini“ – 95 %), kalbos ir darbo automatizavimo sprendimai (pvz., „Microsoft Copilot“ – 38 %) bei vaizdo generavimo įrankiai (pvz., „Midjourney“, „DALL·E“ – 26 %). Tik 10 % apklaustųjų vertina DI poveikį kibernetiniam saugumui kaip labai didelę riziką, 36 % mano, kad DI kelia didelę papildomą riziką, o 41 % – vidutinę riziką.

66 % įmonių naudojosi debesijos paslaugomis. Populiariausia forma buvo programinė įranga kaip paslauga (angl. Software as a Service, SaaS) – ją naudojo 75 % įmonių (pvz., „Google Workspace“, „Salesforce“, „Microsoft 365“). 43 % apklaustųjų debesijos paslaugų keliamą kibernetinio saugumo riziką įvertino kaip vidutinę, o 12 % – kaip labai didelę papildomą riziką.

Nuotolinio darbo galimybės įmonėse ir jo keliamų rizikų kibernetiniam saugumui vertinimas

Daugumoje apklaustų įmonių (59 %) darbuotojai turėjo galimybę dirbti nuotoliniu būdu. Ketvirtadalyje įmonių (25 %) nuotolinio darbo dienų skaičius buvo ribojamas, o 16 % įmonių tokios galimybės neturėjo. Nuotolinis darbas įmonėse buvo įdiegtas po COVID 19 pandemijos, tačiau net ir pasibaigus pandemijai daug įmonių išlaikė šią galimybę.

Paprašius įmonių įvertinti, kiek darbuotojų, turinčių galimybę, renkasi darbą nuotoliniu būdu, 41 % respondentų nurodė, kad šia galimybe naudojasi mažiau nei 10 % darbuotojų. 26 % teigė, kad daugiau nei pusė darbuotojų dirba nuotoliniu būdu, o 25 % – kad 10–50 % darbuotojų pasirenka tokį darbo modelį. Šie duomenys rodo, kad darbuotojų noras dirbti nuotoliu sumažėjęs, nes mažesnė dalis darbuotojų renkasi šią galimybę.

Kas penkta įmonė (20 %) nurodė, kad nuotolinis darbas kelia labai didelę kibernetinio saugumo riziką, tuo tarpu 30 % vertina rizikas kaip vidutines, o dar 30 % – kaip dideles. Tai rodo, kad darbuotojai nesureikšmina nuotolinio darbo keliamo pavojaus kibernetiniam saugumui, o tokį požiūrį gali lemti tai, kad daugelis įmonių, siūlančių nuotolinį darbą, užtikrina tinkamas saugumo priemones.

Įmonių priklausomybė nuo tiekėjų

43 % apklaustųjų nurodė, kad jų esminių paslaugų teikimas dalinai priklauso nuo tiekėjų, 34 % jautėsi visiškai nepriklausomi, o 19 % – visiškai priklausomi nuo tiekėjų. Priklausomybė nuo tiekėjų didina riziką, kad kibernetinio incidento atveju tiekėjo problemos gali paveikti ir įmonės veiklą.

Dauguma įmonių (47 %), kurių esminių paslaugų teikimas dalinai priklauso nuo tiekėjų, buvo vidutinio dydžio, o visiškai nepriklausomos nuo tiekėjų dažniausiai buvo labai mažos įmonės (46 %).

62 % įmonių nurodė, kad joms svarbu, jog verslo partneriai turėtų kibernetinio saugumo standartą ir jo laikytųsi, o 27 % nežinojo arba nenorėjo atsakyti.

Iš įmonių, kurioms tai svarbu, net 74 % jau turi arba per artimiausius 12 mėn. planuoja turėti dokumentuotą kibernetinio saugumo politiką.

Įmonių tiekėjų patirtis, susijusi su kibernetiniais incidentais

Dauguma įmonių (60 %) nežinojo arba neatsakė, ar per pastaruosius metus jų tiekėjai buvo susidūrę su kibernetiniais incidentais, galėjusiais paveikti teikiamas paslaugas. Trečdalis įmonių (33 %) teigė manančios, kad jų tiekėjai su tokiomis situacijomis nesusidūrė. Viena įmonė, kurios tiekėjas patyrė kibernetinį incidentą, nurodė, kad dėl jo buvo prarasti įmonės duomenys, o jų atkūrimas vyko rankiniu būdu, nes tiekėjas atsisakė sumokėti piktavalių reikalautą išpirką.

Kibernetinių incidentų valdymo plano parengimas

Beveik trečdalis įmonių (30 %) nurodė neturinčios parengto veiksmų plano kibernetinio incidento atveju. 26 % įmonių buvo parengusios planą tik daliai galimų situacijų, o 19 % planuoja tokį planą parengti ateityje. Šie duomenys rodo, kad įmonėms vis dar yra kur tobulėti kibernetinio saugumo srityje. Iš anksto parengtas veiksmų planas ir darbuotojų supažindinimas su juo galėtų padėti sumažinti kibernetinių atakų padarinių riziką.

Vadove vartojamų sąvokų sąrašas

Sąvokos:

Botnetas (angl. *Botnet*)	tai piktavalių kontroliuojamas užvaldytų kompiuterių, vaizdo kamerų ar kitų interneto prieigą turinčių įrenginių tinklas, kurį piktavaliai gali panaudoti plataus masto kenkėjiškai veiklai.
Dirbtinis intelektas	sistemos, kurios demonstruoja protingą ir sumanų elgesį, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti.
Duomenų viliojimas (angl. *Phishing*)	socialinės inžinerijos forma, kai apgaulės būdu siekiama išgauti vartotojo vardus bei slaptažodžius, banko sąskaitų numerius ar mokėjimo kortelių informaciją.
Išpirkos reikalavimo programinė įranga (angl. *Ransomware*)	kenkėjiškos programinės įrangos rūšis, kuri užšifruoja įmonės duomenis ir padaro juos nepasiekiamus.
Konfidencialumas (angl. *Confidentiality*)	užtikrinimas, kad visi jautrūs vidiniai įmonės ar verslo partnerių duomenys yra pasiekiami tik asmenims, kurie tiesiogiai dirba su šiais duomenimis.
Pasiekiamumas (angl. *Availability*)	užtikrinimas, kad įgalioti vartotojai bei sistemos gali pasiekti duomenis ir juos naudoti.
Paskirstyta paslaugos trikdymo ataka (angl. *Distributed Denial ofService, DDoS*)	atakos tikslas yra sutrikdyti svetainių ar paslaugų veikimą, kad jos taptų neprieinamos vartotojams arba veiktų netinkamai.
Pažeidžiamumų išnaudojimas (angl. *Exploitation of vulnerabilities*)	procesas, kurio metu piktavaliai pasinaudoja spragomis ir neteisėtai pasiekia sistemas, pavogia duomenis ar sutrikdo įmonės veiklą.
Socialinė inžinerija (angl. *Social engineering*)	piktavalių taikoma strategija, kurios tikslas manipuliuojant žmonėmis gauti prieigą prie jautrių duomenų.
Tiekimo grandinės pažeidžiamumas (angl. *Supply chain vulnerability*)	rizika, kad tiekimo grandinė (prekių, paslaugų) gali būti sutrikdyta, sulėtinta arba visiškai sustabdyta dėl vidinių ar išorinių veiksnių.
Vientisumas (angl. *Integrity*)	užtikrinimas, kad visi vidiniai įmonės duomenys išlieka patikimi, nepakeisti, nesugadinti ar nėra ištrinti.

Išlyga

Informacija, pateikta šiame dokumente, yra rekomendacinio pobūdžio. Informacijos platintojas neprisiima jokios atsakomybės, susijusios su jos naudojimu. Pateikta informacija nėra laikoma baigtine ir nesuteikia saugumo garantijos. Naudotojai turi savarankiškai nuspręsti, ar pateikta informacija yra tinkama siekiant užtikrinti įmonės kibernetinį saugumą. Naudotojai dėl šių ir papildomų kibernetinio saugumo rekomendacijų įgyvendinimo turėtų konsultuotis su IT ir kibernetinio saugumo ekspertais.

Trumpiniai:

BDAR	Bendrasis duomenų apsaugos reglamentas
DI	Dirbtinis intelektas
ES	Europos Sąjunga
EUROPOL	Europos Sąjungos teisėsaugos bendradarbiavimo agentūra
ENISA	Europos Sąjungos kibernetinio saugumo agentūra
IT	informacinės technologijos
KAM	Krašto apsaugos ministerija
NKSC	Nacionalinis kibernetinio saugumo centras prie krašto apsaugos ministerijos
SVV	Smulkus ir vidutinis verslas