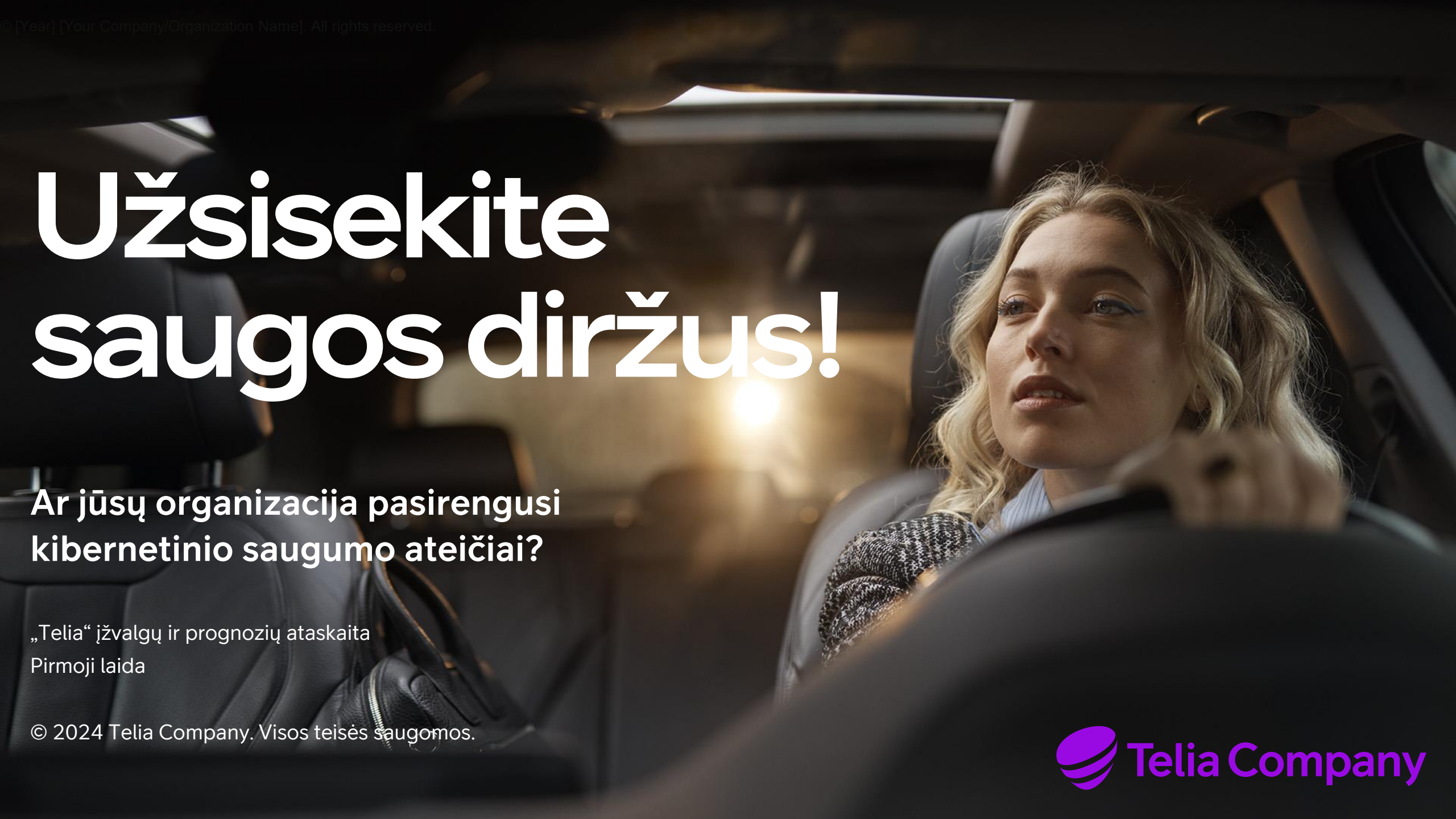


Užsisekite saugos diržus!

Ar jūsų organizacija pasirengusi kibernetinio saugumo ateičiai?

„Telia“ įžvalgų ir prognozių ataskaita
Pirmoji laida

Telia Company

Turinys

1-oji laida. 2024 m. spalio mėn.

„Niekada nebuvo taip svarbu turėti tvirtas saugumo priemones.“

Patrik Hofbauer
„Telia Company“ prezidentas ir vykdomasis direktorius

Vykdomojo direktoriaus žodis

Kadangi mūsų visuomenė vis daugiau naudojasi ryšio technologijomis, tuo pačiu metu ji tampa prasčiau apsaugota nuo skaitmeninių grėsmių. Nors programišių atakų ir kibernetinių nusikaltimų skaičius auga kiekvieną minutę, daugelis organizacijų labai atsilieka kibernetinio saugumo srityje.

Nors kai kam gal ir atrodo, kad saugumas yra sudėtingas ir brangus dalykas, tačiau kibernetinis atsparumas tikrai sudaro geresnes sąlygas verslui. Jis padeda išvengti brangių prastovų, kurios atsiranda dėl sudėtingų kibernetinių atakų, ir sumažina duomenų saugumo pažeidimų, galinčių pakenkti ir įmonei, ir jos darbuotojams, riziką. Asmens duomenų ir privatumo apsauga iš tiesų didina pasitikėjimą, kas ypač svarbu šiais laikais, kai duomenų apsauga yra mūsų dėmesio centre. Patikimos saugumo priemonės sukuria didelį pranašumą kiekviename sektoriuje ir kiekvienoje vietoje. O kadangi kibernetinio saugumo svarba auga, jis neabejotinai nusipelno ir mūsų dėmesio.

Būdama kibernetinio saugumo lydere „Telia“ žino, ko reikia tam, kad taptume atsparūs.

Nors technologijos ir procesai turi svarbią reikšmę, mūsų patirtis rodo, kad labai svarbu ir žmonės. Žmones labai lengva apgauti. Jei jų neįtrauksite į saugumo stiprinimą, kiek beinvestuotumėte į priemones ir technologijas, niekas nepadės.

Šioje ataskaitoje nagrinėjama, kaip žmonių elgesys ir emocijos lemia kibernetinio atsparumo būklę. Bendradarbiaudami su saugumo ekspertais, klientais ir sektoriaus lyderiais, mes išgirdome svarbių įžvalgų apie kai kuriuos iššūkius, su kuriais šiandien susiduria organizacijos, ir parengėme praktinių patarimų, kaip juos įveikti, paketą. Siekdami sustiprinti supratimą, paskatinti kalbėtis ir prisidėti prie nuolatinių pastangų drauge užtikrinti, kad ryšį turėtumėte visur ir visada, mes norėtume pasidalyti šiomis įžvalgomis. Tikimės, kad pavyks įkvėpti organizacijas imtis veiksmų.

02

Pradžios taškas

Mūsų laikų saugos diržai

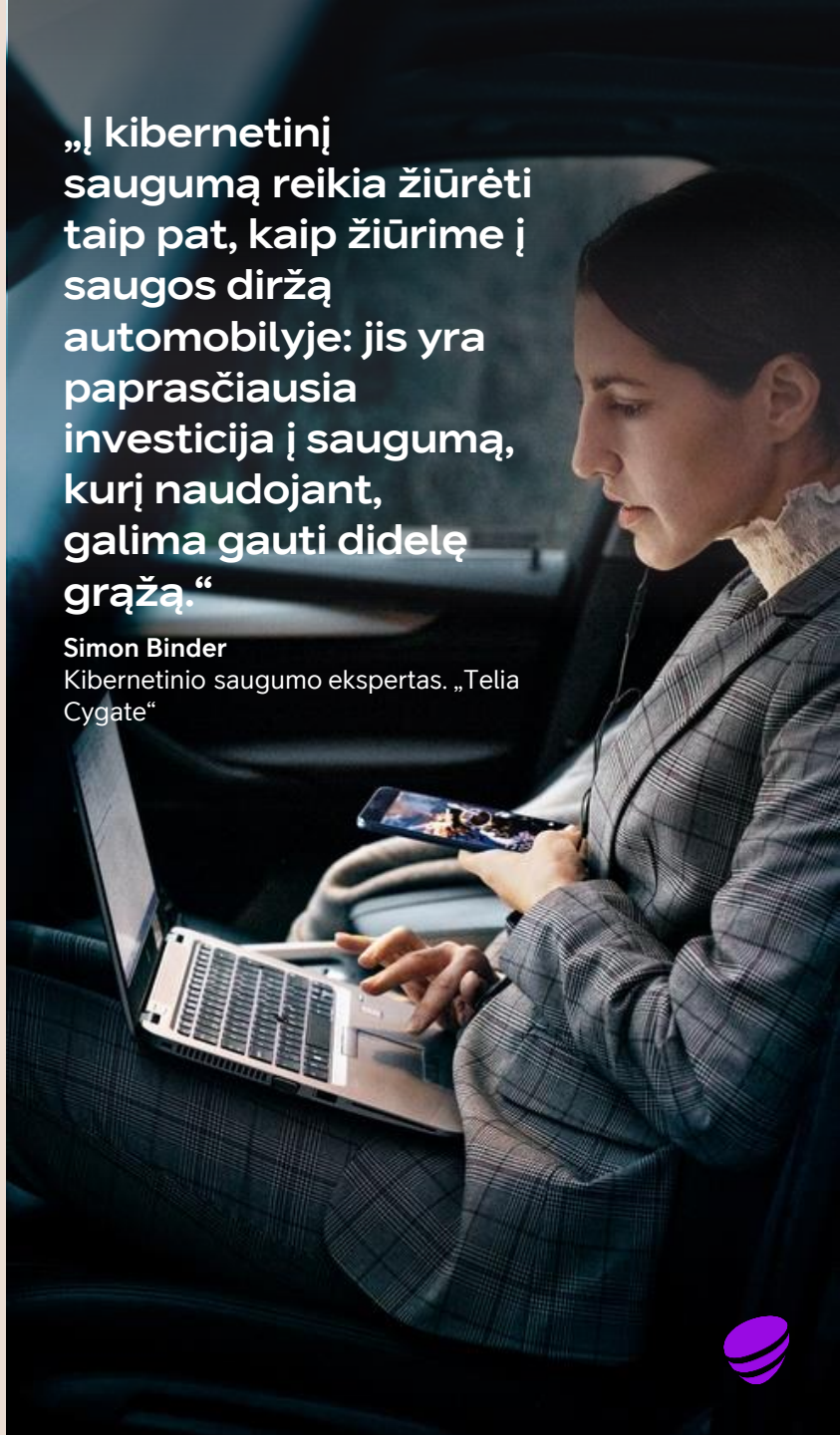
1959 m. pradėti naudoti trijų taškų saugos diržai, kurie teikė vilčių, kad įvykus automobilio avarijai, tikimybė išgyventi žymiai padidės. Nepaisant informacinių kampanijų ir fakto, kad automobilių gamybos pramonė juos įdiegė labai greitai, visuomenė juos pradėjo naudoti vėliau. Kodėl? Keisti įpročius yra sudėtinga, net jei jų keitimas susijęs su mūsų pačių galimybe išgyventi.

Mūsų visiškai skaitmeniniame pasaulyje susiduriame su daug sudėtingesnėmis ir abstraktesnėmis grėsmėmis nei eismo įvykiai. Tačiau, kaip ir automobilių bei saugos diržų atveju, kibernetinis saugumas dažniausiai tėra antraeilis dalykas. Skaitmeniniais greitkeliais lakstome dideliu greičiu, naiviai nepaisydami rizikos.

Tas faktas, kad nors saugos diržus visuomenė pripažino lėtai, tačiau galiausiai vis tiek juos ėmė plačiai naudoti, yra puikus pavyzdys, padedantis priminti keletą elementarių tiesų apie inovacijas, žmones ir saugumą:

- Kai aršios konkurencijos sąlygomis kuriama ir platinama nauja, aktuali ir dažnai menkai suprantama technologija, saugumas (jei apskritai yra) retai kada tampa svarbiausiu rūpesčiu. Tik palaipsniui, kai išryškėja technologijos trūkumai, saugumui irgi pradedama skirti pelnytą dėmesį.
- Net jei saugumo priemonės yra, jokių garantijų, kad mes jas lengvai pritaikysime proporcingai technologijos keliamai rizikai, nėra.
- Saugumas, kaip sąvoka ir praktika, dažnai yra neapčiuopiamas dalykas, todėl tam, kad į jį atkreiptume dėmesį, suprastume, juo rūpintumėmės ir veiktume, saugumą būtina supaprastinti ir sukonkretinti.

Skirtingai nei eisme, skaitmeninė grėsmė yra iš anksto apgalvotas dalykas: kibernetiniai nusikaltėliai aktyviai ir vis veiksmingiau taikosi į aukas, kurias pasiekia vis lengviau. O žengdami į naują ir dar neištirtą dirbtinio intelekto sritį, mes privalome turėti ne tik tinkamus saugumo sprendimus, bet ir vėl iš naujo išmokti prisisegti diržus.



03

Metodika

Metodika

Šios ataskaitos tikslas – apibūdinti organizacijų skaitmeninio saugumo ateitį. Ji parengta pagal mišraus tyrimo metodiką, kurią taikant, derinami iš įvairių šaltinių gauti pirminiai, kiekybiniai ir kokybiniai duomenys. Tyrimas atliktas 2024 m. pavasarį.

- **- 13 išsamių interviu** su sprendimų saugumo srityje priėmėjais (pvz., informacinio saugumo direktorius, veiklos operacijų direktorius) didelėse įmonėse ir organizacijose, veikiančiose pagrindinių „Telia“ rinkų Šiaurės ir Baltijos šalyse įvairiuose ūkio sektoriuose.
- **9 išsamūs interviu** su žinomais kibernetinio ir skaitmeninio saugumo ekspertais, taip pat atitinkamo profilio „Telia“ ekspertais (žr. dešinėje →).
- **Ekspertų apskritojo stalo diskusijos,** kuriose dalyvavo daugiau kaip 15 įvairių sričių specialistų iš visos „Telia“ organizacijos, įskaitant rizikos, strategijos, žmogiškųjų išteklių, inovacijų, komunikacijos ir kibernetinio saugumo sritis (žr. priedą).
- **Duomenys ir** įžvalgos iš svarbiausių sektoriaus ataskaitų bei straipsnių.
- **2024 m. „Telia Company“ skaitmeninio indekso duomenys,** gauti iš 1 152 įvairaus dydžio organizacijų. „Telia“ skaitmeninis indeksas – tai kasmetinė apklausa, skirta stebėti Švedijos įmonių skaitmeninę plėtrą.

Ekspertai-konsultantai

Ypatingai dėkojame šiems ekspertams, kurie rengiant ataskaitą pateikė vertingų ir išsamių nuomonių bei įžvalgų.

Anne Marie Eklund Löwinder

„Amelsec“ generalinė direktorė ir kibernetinio saugumo ekspertė

Mehis Hakkaja

„Clarified Security OÛ“ steigėjas, generalinis direktorius ir savininkas

Åke Holmgren

Švedijos civilinės saugos agentūra, MSB Kibernetinio saugumo ir saugių ryšių vadovas

Pontus Johnson

KTH profesorius, Kibernetinės apsaugos ir informacijos saugumo centro direktorius

Niclas Jalvinger

Informacinio saugumo ir kitų sričių saugumo direktorius, „Telia Company“

Michael Mothander

Kibernetinio saugumo ekspertas, „Telia Cygate“

Malin Fransén Kronberg

„Telia Company“ saugumo vadovė

Simon Binder

Kibernetinio saugumo ekspertas, „Telia Cygate“

Mats Mägiste

„Telia Company“ saugumo infrastruktūros ekspertas

04

Dabartinė kibernetinio saugumo būklė

Saugumo formavimas – tai tarsi bėgimo takelis, kuris vis greitėja

91%

organizacijų per 2022 m. pranešė apie bent vieną kibernetinį incidentą ar pažeidimą. *Šaltinis: Deloitte, Global Future Cyber Security 2023*

+466%

Tiek išaugo DDoS atakų skaičius Švedijoje 2024 m. I ketvirtį, jei palygintume su 2023 m. I ketvirčiu. *Šaltinis: Cloudflare DDoS threat report, 2024*

Kova ne vien tik konkurencijos prasme

Gamtoje rūšys dalyvauja nesibaigiančiose evoliucinėse ginklavimosi varžybose su konkuruojančiomis rūšimis. Prisitaikyk arba mirk. Įmonių atveju šias ginklavimosi varžybas istoriškai nulėmė tinkamumas rinkai. Tačiau palaipsniui atsirado egzistencinė grėsmė, kuri peržengė įprastos konkurencijos ribas ir taisykles.

Šiandien skaitmeninės grėsmės veikėjai (ne taip, kaip invazinės rūšys ekosistemose) kelia grėsmę viso pasaulio didelių ir mažų įmonių išlikimui, nepriklausomai nuo jų konkurencingumo rinkoje. O jei prie to pridėsime spartėjančius pokyčius, taps aišku, kad bėgti nuo išnykimo ateinantį dešimtmetį teks dar intensyviau.

Ginklavimosi varžybų analogija suteikia mums svarbią įžvalgą: saugumas, kaip ir fizinis pasirengimas, nėra absoliutus tikslas. Saugumo mes nepasieksime, tik nuolat tobulėsime ir prisitaikysime. Tai, kad vakar važiuodami automobiliu prisisegėme saugos diržą, dar nereiškia, kad šiandien jis mus pilnai apsaugos.

„Tiesiog manykite, kad jus užpuls.“

Informacijos saugos vadovas

$101,5 milijardo – tokios prognozuojamos pasaulinio masto išlaidos, susijusios su kibernetiniais nusikaltimais 2025 m.
Šaltinis: McKinsey; Cyber Security Trends, 2022

70% organizacijų nurodė, kad geopolitika turėjo įtakos kibernetinio saugumo strategijai.
Šaltinis: World Economic Forum, Global Cyber Security Outlook, 2024

Saugumo spragos Šiaurės ir Baltijos šalyse

Per pastaruosius dešimtmečius skaitmeninė transformacija iš esmės pakeitė daugumą organizacijų.

Didesnėse, labiau tradicinėse organizacijose reikia laiko, kad atsisakytume senų įpročių ir išsiugdytume naują saugumu grindžiamą mąstyseną.

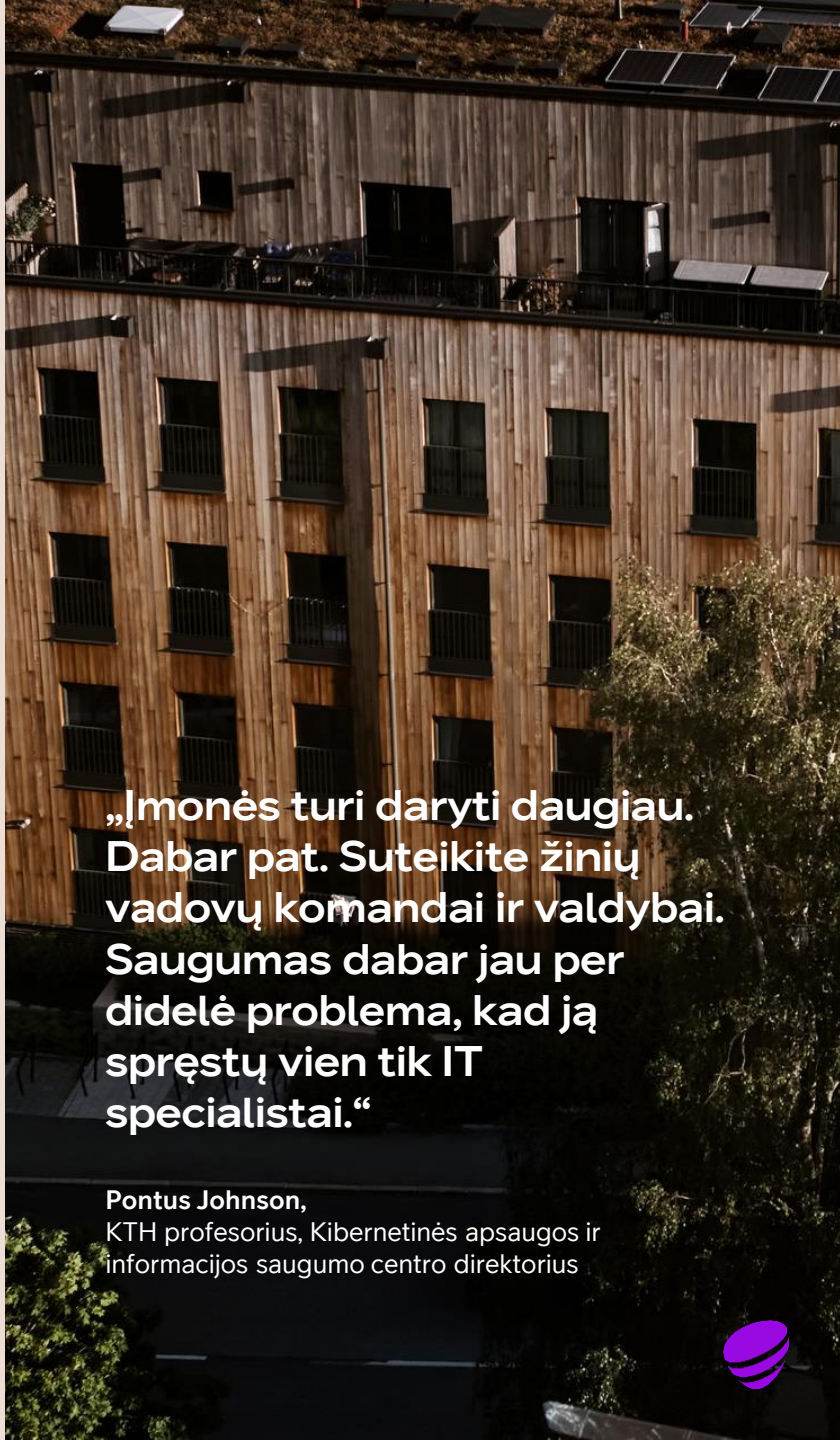
Saugumo spragos kelia didelių iššūkių organizacijoms, kurios pasikeitusiame pasaulyje neturi pakankamo pasirengimo ir apsaugos, kad galėtų įveikti kylančias grėsmes.

Buvusio FTB direktoriaus Roberto Muellerio žodžiais tariant, *„yra tik dviejų tipų įmonės: tos, į kurias buvo įsilaužta, ir tos, į kurias bus įsilaužta“.*

Šiandien organizacijų saugumo būklė labai fragmentiška. Pasirengimas įveikti grėsmes labai priklauso nuo kibernetinio saugumo brandos lygio.

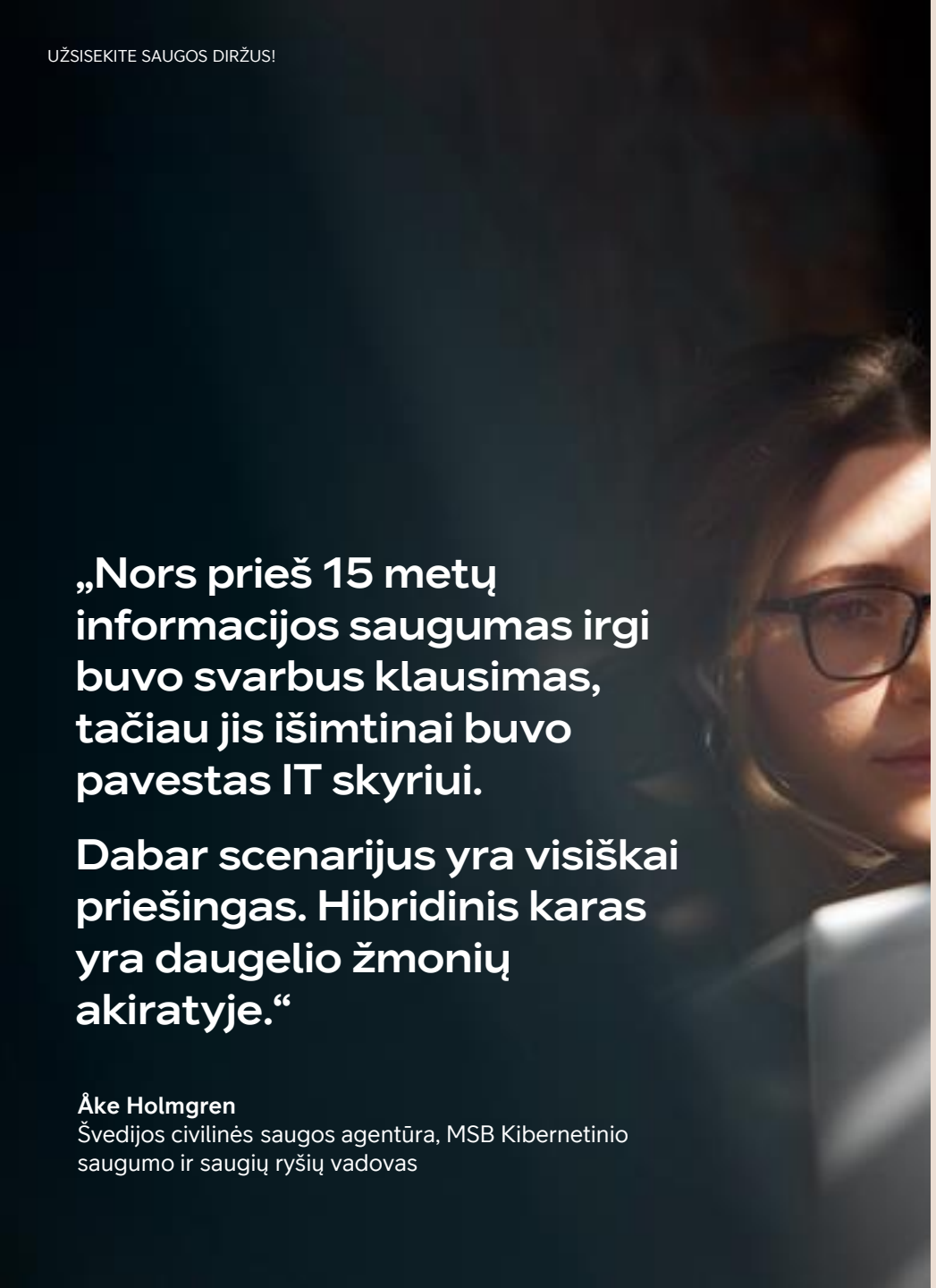
Tik 3%

Švedijos valdžios institucijų 2024 m. laikėsi kibernetinio saugumo reikalavimų.
Šaltinis: MSB



„Įmonės turi daryti daugiau. Dabar pat. Suteikite žinių vadovų komandai ir valdybai. Saugumas dabar jau per didelė problema, kad ją spręstų vien tik IT specialistai.“

Pontus Johnson,
KTH profesorius, Kibernetinės apsaugos ir informacijos saugumo centro direktorius



„Nors prieš 15 metų informacijos saugumas irgi buvo svarbus klausimas, tačiau jis išimtinai buvo pavestas IT skyriui.

Dabar scenarijus yra visiškai priešingas. Hibridinis karas yra daugelio žmonių akiratyje.“

Åke Holmgren
Švedijos civilinės saugos agentūra, MSB Kibernetinio saugumo ir saugių ryšių vadovas

Didėjantis nerimas

2/3

įmonių saugumo specialistų nerimauja dėl kibernetinių išpuolių.
Šaltinis: Telia Digital Index 2024

Atsiradus samdomiems programišiams ir valstybių valdžios remiamiems kibernetiniams teroristams, nusikaltimų skaičius virtualioje erdvėje neregėtai išaugo. Didėjantis mastas ir apimtis reiškia, kad išpuolių padaryta žala gali būti daug didesnė nei kada nors anksčiau. Gali atsitikti, kad nuo kibernetinių išpuolių nukentėjusioms organizacijoms teks kelias savaites ar net mėnesius tvarkytis be svarbiausių sistemų.

Tokia nauja realybė kelia didelį nerimą saugumo specialistams: dvi iš trijų didelių įmonių nerimauja dėl galimų išpuolių. 2024 m. „Telia Digital Index“ duomenimis, tai yra 10 proc. daugiau nei 2023 m.

„Telia Cygate“ kibernetinio saugumo ekspertas Simonas Binderis pastebi, kad keičiasi įmonių požiūris: *„Įmonių klientai šiandien yra daug sąmoningesni ir beveik paranojiški dėl saugumo virtualioje erdvėje“.*

Panašu, kad organizacijos pripažįsta, jog reikia skubėti, ir siekdamos sumažinti sistemų pažeidžiamumą, investuoja į patikimus technologinius sprendimus. Tačiau žengiant pirmyn, reikia imtis spręsti ir keletą svarbiausių iššūkių.

„Kol yra galimybė daug pinigų uždirbti greit ir beveik nerizikuojant, tol padėtis nesikeis.“

Michael Mothander
Kibernetinio saugumo ekspertas, „Telia Cygate“

Saugumo iššūkiai, su kuriais organizacijos susiduria šiandien

01. Surasti pusiausvyrą tarp saugumo ir investicijų į technologijas

51%

Pastebima, kad ieškoma kompromiso tarp technologijų diegimo ir skaitmeninio saugumo. Technologijų diegimas turi aiškų, pamatuojamą poveikį ūkinei veiklai, o kibernetinio saugumo nauda gali atrodyti abstrakti, jei organizacija nebuvo tiesiogiai paveikta. Jei saugumo biudžetas yra IT biudžeto dalis, kyla rizika, kad lėšos bus nukreiptos į dirbtinio intelekto diegimą, o ne į kibernetinio saugumo stiprinimą. „Telia“ saugumo strategijos ir pertvarkos vadovas Conor McGlynn kibernetinį saugumą palygina su draudimu: *„Investicijos į saugumą nebus suvokiamos kaip vertingos, kol neatsitiks koks nors įvykis“.*

Tiek informacinio saugumo vadovų prognozuoja, kad jų bendras IT saugumo biudžetas 2024 m. nesikeis arba mažės. *Šaltinis: Pentera, The State of Pentesting, 2024*

02. Pasirengti blogiausiam: tik prevencijos nebepakanka

71%

Daugelis organizacijų pirmenybę teikia incidentų prevencijai ir aptikimui, o ne pasiruošimui blogiausiam scenarijui. 2024 m. „Telia Digital Index“ duomenys rodo, kad įmonės turi daugiau sprendimų, skirtų grėsmėms nustatyti, nuo jų apsaugoti ir jas aptikti, negu priemonių veiklai atkurti ir pataisyti po išpuolio. Naujausi „Cisco“ apklausos, kurioje dalyvavo 4700 saugumo specialistų, duomenys rodo, kad daugiau dėmesio nuostolių mažinimui ir veiklos tęstinumo palaikymui skiria organizacijos, turinčios incidentų patirties.

Tiek organizacijų mano, kad neturi sprendimų, kaip atkurti paslaugas po išpuolio *Šaltinis: Telia Digital Index 2024*

03. Pritraukti gabių saugumo srities specialistų ir formuoti savo praktinį patyrimą

3,4 mln.

Įgūdžių trūkumas yra realus: įmonėms sunku pritraukti ir išlaikyti IT specialistus, ypač saugumo ekspertus. Mažosios ir vidutinės įmonės dažnai visiškai neturi saugumo srities žinių ir pasikliauja pardavėjais trečiosiomis šalimis bei partneriais. Šis specialistų trūkumas tampa dideliu iššūkiu, ypač trumpalaikiu periodu.

Dabartinis kibernetinio saugumo įgūdžių (žmonėmis) trūkumas pasauliniu mastu. *Šaltinis: Allianz, Cyber security trends, 2023*

04. Pastangos saugumo srityje tik šen bei ten, o bendro vaizdo nėra

15%

Skaitmeninių technologijų diegimas dažnai vyksta atskirose organizacijos komandose, todėl pastangos užtikrinti kibernetinį saugumą yra išsklaidytos. Nesant holistinės vieningos strategijos, kibernetinis saugumas dažnai tampa ne ūkinės veiklos varikliu, o tik pavėluotai atėjusia mintimi.

Tiek organizacijų yra pasiekę aukščiausią brandos lygį (4), kai kibernetiniam saugumui teikiama pirmenybė visose operacijose. *Šaltinis: Radar Cyber Maturity Index 2024.*

Minutėlę!

Jūs turbūt pastebėjote, kad šiame grupavime kažko trūksta. Taip, trūksta žmonių. Kol kas juos turėkite omenyje. Pirmiausia trumpai apžvelkime, ką organizacijos siekia padaryti gerindamos saugumą. Kaip minėta bėgimo takelio metaforoje, išgyvens tik ištvermingieji. Taigi, kaip tiksliai apibrėžtume kibernetinį atsparumą?

„Nepanašu, kad nebus keliami didesni saugos reikalavimai, ypač atsižvelgiant į naujus ES reglamentus.

Rimtos organizacijos stengsis bendradarbiauti su tais, kurie jau yra užsitikrinę pakankamai gerą saugumą.“

Åke Holmgren
Švedijos civilinės saugos agentūra, MSB Kibernetinio saugumo ir saugių ryšių vadovas

05

Kibernetinio atsparumo formavimas

96%

Tiek aukščiausiojo lygmens vadovų mano, kad kibernetinis atsparumas yra labai svarbus jų verslui.
Šaltinis: Cisco, Security Outcomes Report, 2024

„Jei ataka atsitiktinai pavyksta, mes galime reaguoti, identifikuoti įsilaužėlį ir atkurti veiklą patirdami minimalų poveikį.“

Informacijos saugos vadovas
Šiaurės šalių pieno perdirbimo įmonė

Formuodami atsparumą, vadovaukitės NIST gairėmis

1/5

Tokia dalis organizacijų yra priskirta „aukštos kibernetinės brandos“ segmentams. *Šaltinis: Deloitte, Global Future of Cyber Survey 2023*

37%

Tiek organizacijų yra įsitikinusios, kad gali išlikti atsparios blogiausio kibernetinio išpuolio atveju. *Šaltinis: Cisco, Security Outcomes Report, 2024*

Nuolat diegti patobulinimus – labai lengva

Kibernetinio atsparumo didinimas reikalauja struktūriškai apibrėžtų darbų ir tam skirtų išteklių. Laimei, esama nusistovėjusių būdų, kaip pradėti.

Plačiai pripažintose NIST kibernetinio saugumo gairėse kibernetinis atsparumas apibrėžiamas kaip „gebėjimas numatyti, atlaikyti nepalankias sąlygas, sunkumus, išpuolius ar sistemų pažeidimus, po jų atsigauti ir prie jų prisitaikyti, kuris naudoja kibernetinius išteklius arba pradeda veikti šiems esant.“

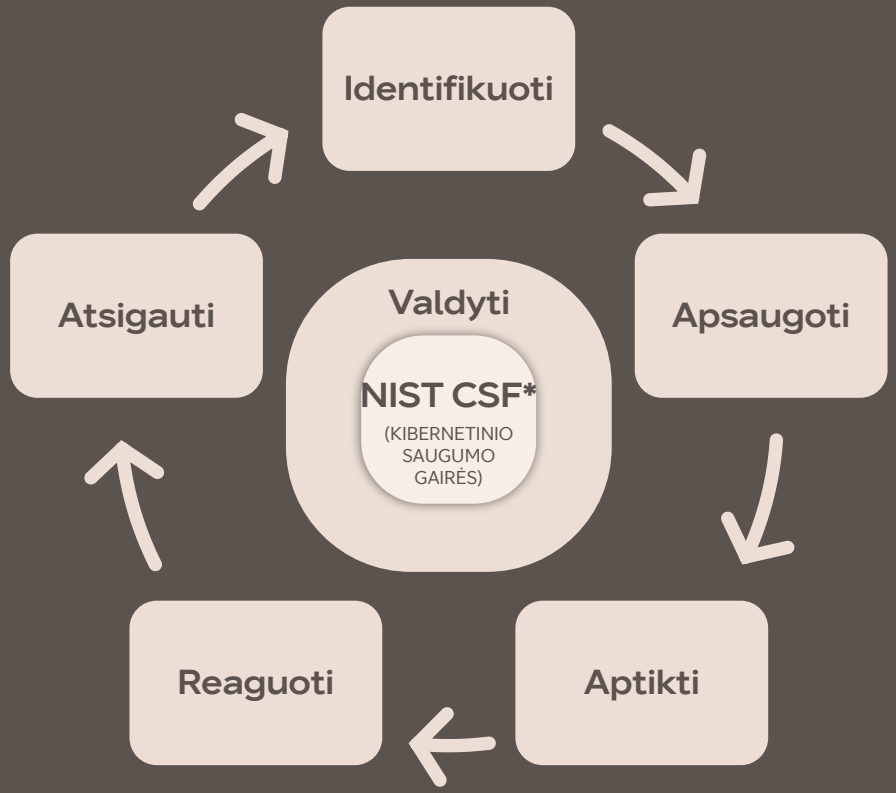
Pirma, ši apibrėžtis reiškia, kad organizacijos turi sutelkti savo pastangas saugumo srityje ne tik į apsaugą ir išpuolių skaičiaus mažinimą, bet ir į gebėjimą atsigauti, mokytis ir prisitaikyti prie įvykių, kurie nutiko ne tik joms, bet ir kitiems.

Antra, tai reiškia, kad atsparumo formavimo ir palaikymo procesas yra nuolat vykstantis – jis niekada nesibaigia.

Veiksmų imkitės palaipsniui

„Telia Cygate“ kibernetinio saugumo ekspertas Simon Binder:

„Į atsparumo stiprinimą aš žiūriu kaip į bet kokį sportą – juk nepradedame nuo sudėtingiausių dalykų. Pradedame nuo stipraus kūno, stipraus proto, tvirto pagrindo, ant kurio galėtumėte stovėti. Jei susikursite geriausią pagrindą, vėliau gebėsite paspartinti veiksmus ir varžytis“.



* 2024 m. Komponentas „valdyti“ bus įtrauktas kaip šeštasis sistemos komponentas. Daugiau informacijos rasite *nist.gov/cyberframework*

„Mes turime labai daug naudotojų. Tai reiškia, jog yra labai didelė rizika, kad kas nors atidarys el. pašto pranešimą arba paspaus nuorodą.

Anksčiau būdavo gėda prisipažinti, kad gavai virusą. Tačiau gerai, kad iš to mokomės.“

IT ir saugumo vadovas (viešasis sektorius)

Galia kuriama bendradarbiavimu ir skaidrumu

Partnerystė – geriausias pasirinkimas

Organizacijos nuolat susiduria su artėjančiomis grėsmėmis. Mūsų tyrimų rezultatai rodo vieną aiškią tendenciją: ateityje nė viena organizacija nebus pajėgi tik savo jėgomis išspręsti saugumo problemas. Pažeidžiamumas atsiranda dėl kvalifikuotų saugumo specialistų trūkumo bei dėl vis labiau tarpusavyje susijusių partnerių ekosistemų ir tiekimo grandinių, kuriose veikia organizacijos. Todėl, siekiant sėkmės, partnerystė ir bendradarbiavimas turės labai svarbią reikšmę. Ir nesvarbu, ar reikės stiprinti saugumą kartu su tiekėjais, ar užsakyti saugumo užtikrinimo darbus, ar dalintis patirtimi ir informacija su sektoriuje dirbančiais kolegomis.

Skaidrumas kuria pasitikėjimą

Visi žino apie didžiules diskusijas dėl duomenų privatumo apsaugos. Kuriant pasitikėjimą, duomenų apsauga būna ypač svarbi. Įsigaliojančio ES reglamento dinamika ir didėjantys visuomenės bei klientų reikalavimai rodo, kad ateityje reikės daugiau skaidrumo ir atvirumo. Ekspertai sutinka: skaidrumas ir atskaitomybė gali turėti didelę reikšmę, ypač formuojant klientų, žiniasklaidos ir kitų pagrindinių suinteresuotųjų šalių pasitikėjimą.

Subalansuoto saugumo beieškant

Gali būti, kad vertėtų į atsparumą žvelgti kaip į žmonių, procesų ir technologijų dinamikos pusiausvyrą. Taip prieiname prie didžiausio iššūkio ir galimybės kuriant atsparią organizaciją – prie žmonių.

94%

Tiek vartotojų būtų lojalesni tiems prekių ženklams, kurie praktikuoja skaidrumą.
Šaltinis: Forbes

06

Žmogus, kurį lengva „nulaužti“

#2

Žemas darbuotojų išprusimo saugumo srityje lygis yra antra pagal dydį (po ribotų biudžetų ir išteklių) kliūtis, trukdanti išlaikyti pakankamą saugumo lygį.
Source: Radar, Cybersäkerhet 2024

„Kibernetinėms grėsmėms dirbtinis intelektas yra tas pats, kas karo atveju – branduolinis ginklas.“

Håkan Kvarnström,
„Telia Company“ valdymo, rizikos ir atitikties vadovas

Pagrindinis būsimų išpuolių taikinys – žmonės

Paprasta, tačiau naudinga sistema „žmonės, procesai, technologijos“ (ŽPT) leidžia išnagrinėti, kaip sąveikauja trys pagrindinės bet kurios organizacijos sudedamosios dalys, kaip joms sąveikaujant atsiranda ir kokie būna mikromodeliai bei makromodeliai.

Istoriškai investicijos į kibernetinį saugumą daugiausia buvo skiriamos dviem iš minėtų trijų komponentų – technologijoms ir procesams. Viena akivaizdžių priežasčių – jų materialumas: daiktai ir darbo metodai yra paprasti, o žmonės ir kultūra – sudėtingi dalykai.

Gali būti, jog vadovai tikėjosi, kad komponentas „žmonės“ savaime atsistos į savo vietą, kai tik bus sutvarkyti kiti elementai. Deja, taip neįvyko.

Didžioji dauguma išpuolių būna nukreipti prieš žmones. Net pažangiausios technologijos negali apsaugoti žmonių nuo to, kad šie taps išpuolio auka. Atkreipti dėmesį į šį faktą privalo kiekviena organizacija, kuri siekia maksimaliai išnaudoti savo investicijas į kibernetinį saugumą. Panagrinėkime, kodėl būsimų išpuolių atvejais pagrindiniais taikiniais bus žmonės.

98%

Tiek kibernetinių išpuolių būna pagrįsta socialine inžinerija. *Šaltinis: Splunk, State of Security 2024*

52%

Tiek vadovų mano, kad jų darbuotojams trūksta būtinų kibernetinio saugumo žinių. *Šaltinis: Fortinet, Cybersecurity skills gap 2022*

„Nulaužti“ žmogų yra lengviau negu kompiuterį.“

Anne-Marie Eklund Löwinder (Amel), generalinė direktorė ir saugumo ekspertė

Trys veiksniai, keliantys pavojų žmonėms

01.
Spartus dirbtinio intelekto diegimas yra ir palaima, ir prakeiksmas

Esame dar vieno didelio technologijų naudojimo pokyčio liudininkai, nes siekdamos padidinti našumą, eliminuoti nuobodžias užduotis ir paskatinti kūrybiškumą, organizacijos tyrinėja dirbtinio intelekto įrankius. Kol kas viskas gerai. Tačiau yra vienas kabliukas: dažnai dirbtinio intelekto įrankius žmogus naudoja nebrandžiai, o tai kelia didelį pavojų saugumui ir sukuria terpę kibernetiniams nusikaltėliams.

Paprastais veiksmais, pavyzdžiui, kopijuodami tekstą ir jį įklijuodami į viešą dirbtinio intelekto modelį, galime atskleisti neskelbtiną informaciją. Konfidencialių duomenų teikimas šiems modeliams yra negrįžtamas procesas, tačiau vidutiniam statistiniam darbuotojui ši rizika atrodo tolima. Kai kurios įmonės elgiasi itin atsargiai, tačiau kitos neturi jokių taisyklių ir leidžia darbuotojams patiems naudoti dirbtinį intelektą.

34%

Tiek organizacijų neturi išbaigtos generatyvinio dirbtinio intelekto strategijos.
Šaltinis: Splunk, Cybersecurity skills gap 2022

43%

Tiek saugumo specialistų mano, kad dirbtinis intelektas gali būti naudingesnis besiginantiems, o ne užpuolikams (per 8 mėnesius tokių buvo 17 proc.).
Šaltinis: Splunk, Cybersecurity skills gap 2022

02.
Išpuoliai tampa hiperautomatizuoti (kaip ir mūsų atsakas)

Didelę dalį duomenų saugumo pažeidimų vis dar sudaro fišingas. Pasitelkęs dirbtinį intelektą bet kas gali vienu metu atakuoti tūkstančius įmonių ir net individualiai pritaikyti atakas darbuotojams. Kadangi giluminės klastotės (angl. *deep fake*) tampa vis sudėtingesnės, atskirti tikrą ir suklastotą el. laišką darosi beveik neįmanoma.

Pasitelkę „tamsiąją psichologiją“, nusikaltėliai naudojasi mūsų emocijomis ir įjungia mūsų autopiloto režimą, arba „1-ąją sistemą“ (kaip apibrėžė Nobelio premijos laureatas Daniel Kahneman). Priešingai sąmoningesnei „2-ajai sistemai“, kuriai reikia kognityvinių pastangų, 1-oji sistema yra refleksyvi ir emocionali. Iš darbuotojų tikimės daug: lankstumo, technologijų pritaikymo, darbo ir asmeninio gyvenimo pusiausvyros, todėl streso ar skubos sąlygomis beveik neišvengiamai galima paslysti.

4,8 mln. $

Tokius vidutinius nuostolius patyrė organizacijos, į kurias buvo įsilaužta dėl fišingo
Šaltinis: IBM, https://www.ibm.com/topics/phishing, 2024

03.
Į mūsų gyvenimus skverbiamasi kaip niekada anksčiau

Hibridinis darbas ištrynė ribą tarp asmeninio ir profesinio gyvenimo, todėl atsirado naujų skaitmeninio saugumo pavojų. Darbuotojai kasdien dalijasi asmenine ir slapta informacija. Vadovai skatinami būti atviri. Tai – puiki žinia nusikaltėliams. Turint prieigą prie mūsų pomėgių, to, ką mėgstame, ir buvimo vietos, „socialinė inžinerija“ dirbtinio intelekto amžiuje baugina kaip niekad anksčiau. Giluminės klastotės tampa tokios įtikinamos, kad netrukus gali mesti iššūkį mūsų realybės suvokimui.

Taigi, ką daryti?

Nė vienas žmogus nėra atskira sala. Darbuotojai niekada neveikia pavieniui. Organizacijoms tenka didžiulė užduotis sudaryti tinkamas sąlygas saugumui klestėti. Todėl dabar turime pereiti prie svarbiausio mūsų argumento: kultūros kaip atsparumo veiksnio.

46%

Tiek IT specialistų praneša apie padažnėjusias socialinės inžinerijos atakas, tiesiogiai nukreiptas į konkrečius asmenis.
Šaltinis: LastPass, Combating Social Engineering in 2024.

„Kaip organizacija, jūs turėtumėte būti labai atsargūs ir nekaltinti tų, kurie pasielgė neteisingai.

Tai klausimas vadovybei, nes ji nesudarė žmonėms tinkamų sąlygų.“

Åke Holmgren
Švedijos civilinės saugos agentūra, MSB Kibernetinio saugumo ir saugių ryšių vadovas

ATVEJO ANALIZĖ

Laurynas Prikockis
Pirmiausia – pagalba darbuotojams

„Labai svarbu, kad incidentą suvaldanti komanda būtų pasirengusi psichologiškai. Mes turime suprasti, kad darbuotojai yra pažeidžiami.“

Laurynas Prikockis buvęs „Vakarų laivų gamykla“ įmonių grupės informacinių technologijų direktorius. Šių metų pradžioje įmonė patyrė didelį kibernetinio saugumo incidentą – fišingo ataką, per kurią pažeidus darbuotojų prisijungimo duomenis, įvyko neteisėta prieiga prie neskelbtinos informacijos.

Atlikus tyrimą paaiškėjo, kad fišingo el. laiške buvo pasinaudota įmonės įdiegtos kelių veiksnių autentifikacijos (MFA) silpnosiomis vietomis ir kad ataką buvo galima sušvelninti geriau išmokius ir informavus darbuotojus.

Laurynas, kuris turi Verslo administravimo magistro (MBA) laipsnį, apimantį ir psichologijos studijas, dalijasi patirtimi, kaip jam su savo komanda pavyko susidoroti su incidentu pirmenybę teikiant žmonėms.

Į darbuotojus orientuotas reagavimas į incidentus

Įvykus pažeidimui, „Vakarų laivų gamykla“ įmonių grupės saugumo komanda sugebėjo greitai reaguoti. Pirminės priemonės – slaptažodžių atkūrimas ir paveiktų paskyrų apsauga.

Dar svarbiau yra tai, kad daug dėmesio skirta nukentėjusio darbuotojo, su kuriuo buvo nedelsiant susisiekta ir kuriam pranešta apie pažeidimą, gerai savijautai. „Vakarų laivų gamykla“ įmonių grupė suteikė psichologinę pagalbą, kad padėtų suvaldyti su incidentu susijusį stresą.

Visose platformose buvo sustiprintas kelių veiksnių autentifikacijos patvirtinimas. Siekdama nustatyti bet kokias kitas pažeidžiamas vietas, saugumo komanda atliko išsamų tyrimą ir ėmėsi veiksmų, skirtų sustiprinti sistemų apsaugą nuo panašių atakų.

Visiškas skaidrumas

Siekiant užtikrinti, kad darbuotojas suprastų situaciją ir veiksmus, kurių imtasi poveikiui sušvelninti, su paveiktu darbuotoju buvo skaidriai bendraujama.

Laurynas ir saugumo komanda glaudžiai bendradarbiavo su darbuotoju, siekdami atkurti jo pasitikėjimą ir surengti reikiamus mokymus, kad būtų išvengta incidentų ateityje.

Apie incidentą pranešta Nacionaliniam kibernetinio saugumo centrui ir kitoms atitinkamoms valstybės institucijoms taip, kaip nustatyta duomenų apsaugos taisyklėse. Įmonės reagavimo plane numatyta informuoti suinteresuotąsias šalis ir visuomenę, užtikrinti skaidrumą apie incidentą ir taikomas priemones.

Išvada

Incidentas parodė, kaip svarbu laikytis holistinio požiūrio, pagal kurį techninės priemonės derinamos su pagalba darbuotojams. Sutelkusi dėmesį į už pažeidimą atsakingo asmens gerą savijautą, bendrovė ne tik sugebėjo veiksmingai suvaldyti incidentą, bet ir puoselėjo pasitikėjimo ir atsparumo kultūrą. Visiems darbuotojams buvo surengti papildomi kibernetinio saugumo mokymai, kad jie galėtų geriau atpažinti bandymus sukčiauti ir į juos reaguoti.

Šis atvejis rodo, kad į žmogų orientuota kibernetinio saugumo praktika yra gyvybiškai svarbi suvaldant saugumo incidentus ir atkuriant įprastą padėtį.

Incidento data: 2024 m. vasario mėnuo
Išpuolio rūšis: Fišingas
Išpuolio vektorius: juodasis programišius, apgaule priverčiantis darbuotoją atskleisti prisijungimo prie socialinių tinklų paskyrų ir įmonės el. pašto duomenis

Nepraleiskite Lauryno išmoktų pamokų!

Lauryno kontrolinis sąrašas: išmoktos pamokos

Trys pagrindinės pamokos, kurias reikia išmokti formuojant į žmones orientuotą požiūrį į saugumą

01 Darbuotojo gera savijauta

Labai svarbu, kad pirmiausia pasirūpinta nukentėjusio darbuotojo psichikos sveikata ir pasitikėjimu savimi. Tai užtikrino, kad darbuotojas išliks vertinga komandos dalimi, ir padėjo atkurti pasitikėjimą organizacijoje.

02 Patobulinti mokymai

Parengtos nuolatinio švietimo ir mokymo programos, kad darbuotojai būtų nuolat informuojami apie naujausias kibernetinio saugumo grėsmes ir geriausią praktiką.

03 Sustiprinti protokolai

Šis incidentas paskatino peržiūrėti ir patobulinti esamus saugumo protokolus, įskaitant patikimesnių kelių faktorių autentifikacijos sprendimų diegimą ir periodiškai atliekamus saugumo auditus.

07

Kultūra kaip saugumo veiksnys

„Kultūra – tai kolektyvinė ir apibendrinta žmonių elgsena. Mums reikia pasakojimų, mokymų, informacijos ir diskusijų.“

Håkan Kvarnström
„Telia“ valdymo, rizikos ir atitikties vadovas

„Svarbiausia – mūsų žmonės ir patirtis. Juk ingredientų „Carbonara“ makaronams gali nusipirkti kiekvienas, tačiau įgūdžių pagaminti gerą patiekalą turi ne kiekvienas. Tas pats pasakytina ir apie kibernetinį saugumą.“

Sam Rabar
Kibernetinio saugumo ekspertas, „Telia Company“

Kaip kultūra galėtų būti saugumo veiksniu

73%

Tiek darbuotojų teigia, kad įtraukimas į įmonės kultūrą padeda jiems išlaikyti susidomėjimą. *Šaltinis: Seenit, The State of Employee Engagement, 2023*

72%

Tiek vadovų teigia, kultūra padeda įgyvendinti sėkmingų pokyčių iniciatyvas. *Šaltinis: PWC, Global Culture Survey 2021*

Fišingo el. laiškai, slaptažodžių atnaujinimas ir žmonių įleidimas į biuro pastatą. Tai – tiesiog kasdienybė. Tačiau kaip sukurti tvirtą saugumo kultūrą?

Prieš pradėdami gilintis, apibrėžkime kultūrą kaip bendras grupės vertybes, požiūrį, įsitikinimus ir elgseną. Trumpai tariant, kultūra gyvena jos narių širdyse, protuose ir rankose.

Keičiant širdis ir protus, svarbiausia – lyderystė

Keisti kultūrą yra sudėtinga. Daugelis vadovų natūraliai bando pakeisti tai, ką darbuotojai vertina ir kuo tiki. Skamba paprastai: apibrėžkime norimą kultūrą, praneškime apie ją ir laukime pokyčių.

Tačiau mokslas rodo, kad toks metodas retai kada pasiteisina. Kodėl? Todėl, kad vertybės keičiasi lėtai ir būna giliai įsišaknijusios. Net jei mums pavyksta pakeisti požiūrį ir įsitikinimus, vis tiek lieka liūdnai pagarsėjęs atotrūkis tarp žinojimo ir darymo. Kaip pavyzdį paimkime sveikatą: juk žinome, kad mankštintis naudinga, tačiau dažnai to net nedarome. Keičiant tik mintis, retai kada keičiasi ir veiksmai.

Veiksmai kalba garsiau nei žodžiai

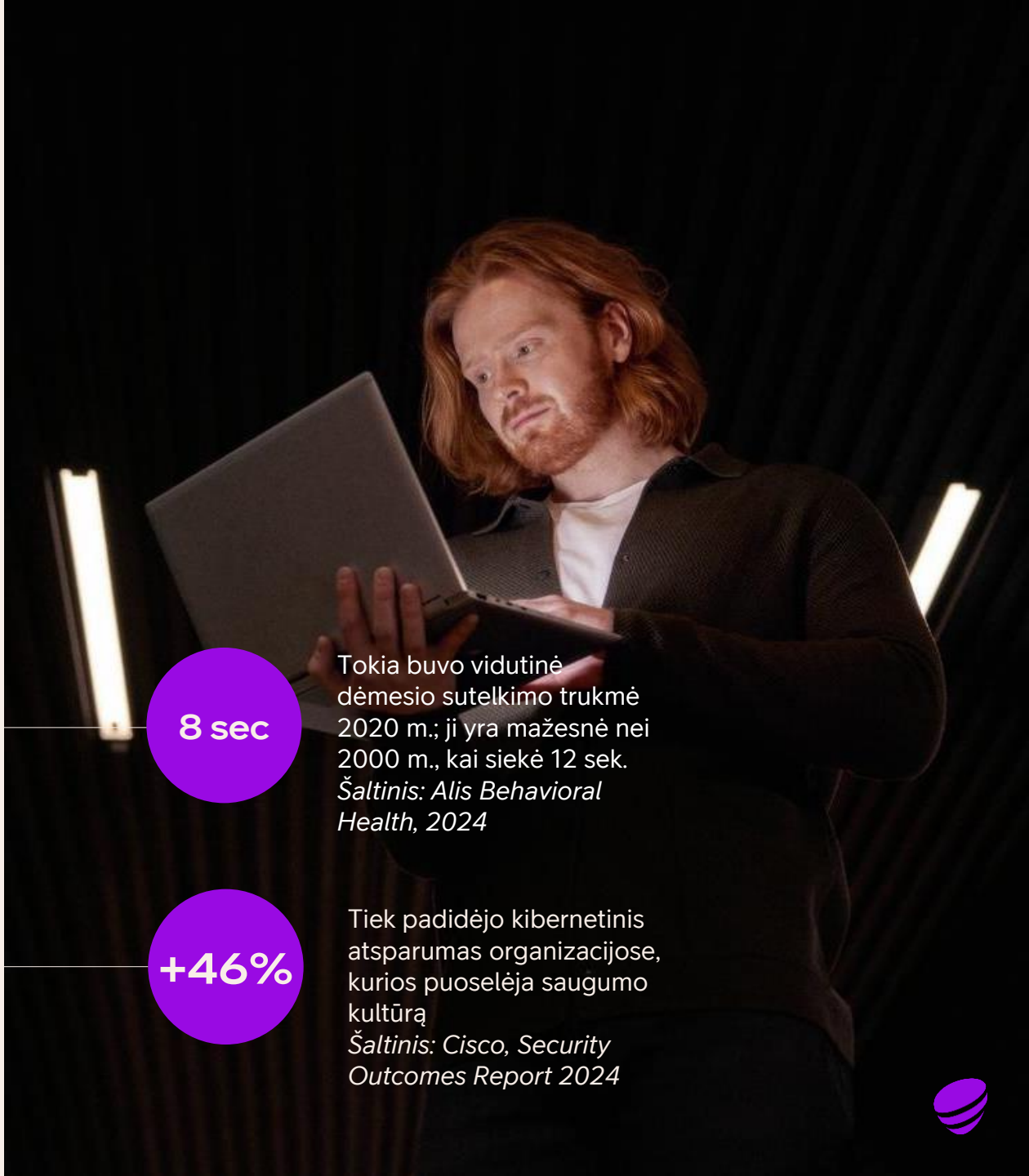
Gera žinia yra ta, kad veiksmingiausias būdas keisti kultūrą – taikytis į elgseną ir sprendimus. Žymūs moksliniai tyrimai aiškiai nurodo, kad vadovai pirmiausia turėtų skirti didžiulį dėmesį tam, kad darbuotojai elgtųsi kitaip. Laikui bėgant, perimta nauja elgsena suformuos naujas nuostatas, įsitikinimus ir vertybes. Taip atsiranda nauja kultūra, kurią skatina praktika, o ne pamokslavimas.

Vadovavimas rodant pavyzdį

Svarbiausia komponentas, kuris turi įtakos kitokiam darbuotojų elgesiui, yra vadovavimas. Kai vadovai sako, kad saugumas yra svarbiausias prioritetas, tačiau nesielgia atitinkamai, visiškai natūraliai darbuotojai seks jų pavyzdžiu.

„Saugumo kultūrai būdingi du dalykai: supratimas ir kaip tas supratimas kasdien veikia mane – nesvarbu, ar eičiau pro duris, ar atidaryčiau el. pašto pranešimą.“

Technologijų bendrovės IT ir saugumo vadovas



8 sec

Tokia buvo vidutinė dėmesio sutelkimo trukmė 2020 m.; ji yra mažesnė nei 2000 m., kai siekė 12 sek.
Šaltinis: Alis Behavioral Health, 2024

+46%

Tiek padidėjo kibernetinis atsparumas organizacijose, kurios puoselėja saugumo kultūrą
Šaltinis: Cisco, Security Outcomes Report 2024

„Prieš 10 metų saugumo klausimų su vadovybe neaptarinėjau – daugiau kalbėjau apie IT paslaugas ir stabilumą. „Saugumu turi pasirūpinti IT, jis tiesiog turi veikti“. Dabar saugumas – kur kas labiau lyderių lygmens tema. Saugumas – tai verslo ramstis. Mes kalbame apie saugumo kultūrą ir sąmoningumą.“

Finansinių paslaugų bendrovės IT ir saugumo vadovas

ATVEJO ANALIZĖ

Thomas Zuliani, „Arla Foods“ Saugumo kultūros svarba

„Jūs turite technologijas, žmones ir procesus. Tačiau jei visoje organizacijoje nebus įdiegta saugumo kultūra, nė vienas komponentas neveiks.“

Pieno sektoriaus milžinė „Arla Foods“, kurioje dirba apie 21 000 darbuotojų, iki Thomo Zuliani paskyrimo net dešimt metų neturėjo nei specialaus informacijos saugumo vadovo, nei tinkamo kibernetinio saugumo skyriaus. Dėl to susikaupė daug saugumo problemų, kurios vilkosi iš paskos ir kurias reikėjo spręsti.

Vadovaujant T. Zuliani, kibernetinio saugumo komanda greitai išaugo – vietoje 2 atsirado 12 darbuotojų. Taip atsirado galimybė spręsti minėtas problemas ir laikytis naujų ES reikalavimų.

Vienas svarbiausių iššūkių buvo tas, kad reikėjo pakeisti organizacijos, kuriai daugelį metų kibernetinis saugumas nelabai rūpėjo, mąstyseną. O tam reikėjo atkakliai visus lavinti, įtraukti ir parodyti aktyvių saugumo priemonių naudą.

Kultūros vaidmuo užtikrinant kibernetinį saugumą

T. Zuliani pabrėžia, kad bet kokios kibernetinio saugumo programos sėkmė labai priklauso nuo organizacijos kultūros, ir išskiria tris pagrindines sritis:

1. Aukščiausios vadovybės dalyvavimas

Aukščiausiosios vadovybės dalyvavimas labai svarbus. T. Zuliani nurodo, kad generalinis direktorius, kuriam kibernetinis saugumas yra prioritetas, gali paskatinti organizaciją siekti aukštesnio saugumo praktikos brandos lygio. Ir atvirkščiai, jei aukščiausioji vadovybė tam abejinga, pasiekti tą patį brandos lygį bus gerokai sunkiau.

2. Proaktyvi mąstysena

Labai svarbią reikšmę turi ir proaktyvus požiūris į kibernetinį saugumą. T. Zuliani teigia, kad daugelis organizacijų į kibernetinį saugumą reaguoja tik po didelio incidento. Tačiau bendrovėje „Arla“ buvo sąmoningai stengiamasi saugumo klausimus spręsti proaktyviai, Tai padeda sumažinti riziką iki to laiko, kol ji netapo didele problema.

3. Žmogiškasis veiksnys

Žmonės yra ir silpniausia kibernetinio saugumo grandis, ir didžiausias turtas. Nepaisant milijoninių investicijų į technologijas, didžiosios dalies sėkmingų kibernetinių išpuolių atvejais buvo naudojamasi žmogaus pažeidžiamomis vietomis, pavyzdžiui, imamasi sukčiavimo ir pasitelkiama socialinė inžinerija. Todėl labai svarbu, kad patys darbuotojai taptų budriais organizacijos gynėjais.

Išvada

T. Zuliani vadovavimas rodo, kad atspari kibernetinio saugumo strategija apima ne tik technologijas ir procesus. Norint ją įgyvendinti, reikia, kad būtų diegiama visuotinė saugumo suvokimo kultūra, ir kad aktyviai įsitrauktų visi organizacijos lygmenys, ypač aukščiausioji vadovybė. Skatindamos kultūrą, kurioje kiekvienas darbuotojas supranta savo vaidmenį užtikrinant skaitmeninį saugumą, organizacijos gali gerokai sustiprinti savo atsparumą.

Toks požiūris ne tik sumažina riziką, bet ir paverčia potencialias silpnąsias vietas stipriosiomis, sukurdamas žmogiškąją užkardą, kuri papildo techninėmis priemonėmis užtikrinamą apsaugą.

10

Tiek naujų darbuotojų į kibernetinio saugumo komandą Thomas priėmė per pirmuosius metus, kai tapo „Arla Foods“ informacinio saugumo vadovu. Komanda padidėjo nuo 2 iki 12 narių.

Nepraleiskite Tomo siūlomo kultūros puoselėjimo veiksmų sąrašo!

„Arla Foods“ ir Thomo sąrašas: kaip puoselėti saugumą

Keturi būdai, kaip organizacijos gali sudaryti palankesnes sąlygas atspariai saugumo kultūrai augti ir klestėti.

„Jei generalinis direktorius nepropaguoja mūsų norimos kultūros, pasiekti kibernetinio saugumo brandą bus daug sunkiau.“

01 Supratimas ir mokymai

„Arla“ rengia sukčiavimo atvejų imitacijas ir privalomus mokymus, kad darbuotojai būtų informuoti ir įspėti apie galimas grėsmes. Užsiėmimai rengiami taip, kad būtų patrauklūs ir susiję su darbuotojų kasdienėmis užduotimis.

02 Įtraukimas

T. Zuliani yra kūrybiškų dalyvavimo strategijų šalininkas. Pavyzdžiui, organizuoja kibernetinio saugumo mėnesį, kviečia iš kitur pranešėjus, organizuoja visuotinius darbuotojų susitikimus. Tokia veikla yra ne tik švietėjiška – ji motyvuoja darbuotojus rimtai žiūrėti į kibernetinį saugumą.

03 Meduolis, o ne rimbas

Užuot baudęs, T. Zuliani pirmenybę teikia švelniam stiliui, skatinančiam bendradarbiavimą ir bendrą atsakomybę. Tai reiškia, kad atsakomybė už saugumą perduodama darbuotojams, skatinamas jų atsakomybės ir budrumo jausmas.

04 Strateginė integracija

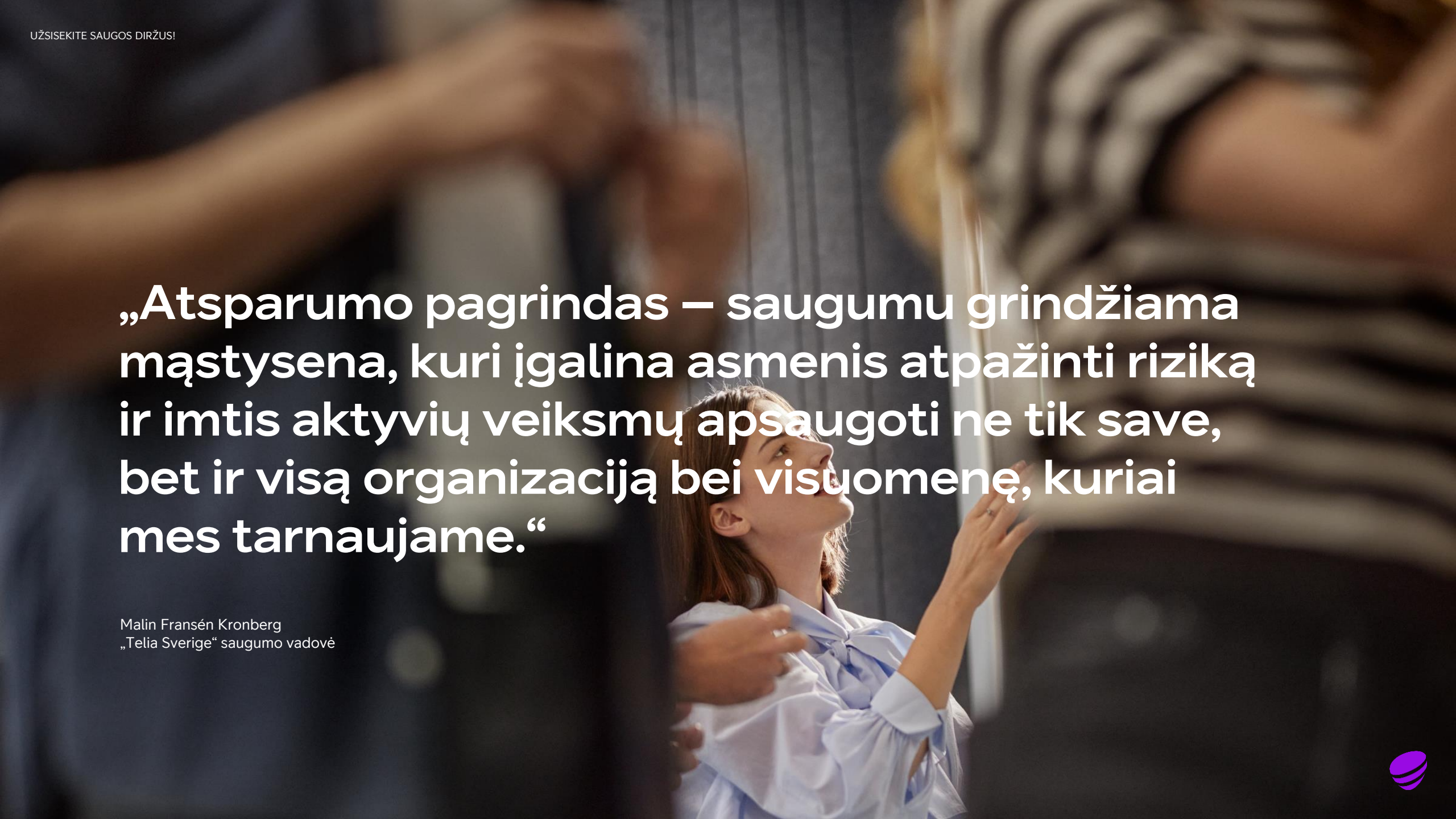
Kibernetinio saugumo tikslai integruoti į bendrą įmonės misiją ir viziją. Pavyzdžiui, duomenų patikimumo ir vientisumo užtikrinimas atitinka bendrovės misiją užtikrinti tvarumą ir kokybę pieno produktų gamyboje.

„Kadangi vis dažniau savo veiklą grindžiame duomenimis ir dirbtiniu intelektu, mes tampame labiau pažeidžiami. Saugumo ir patikimumo poreikis didės. Itin svarbu didinti atsparumą. Atsparumas reiškia, kad atlikdami savo darbą žmonės jaustųsi saugūs.“

Magnus Leonhardt
„Telia Company“ saugumo ir strategijos ekspertas

08

Kaip formuoti saugumo kultūrą: penki svarbiausi dalykai



„Atsparumo pagrindas – saugumu grindžiama mąstysena, kuri įgalina asmenis atpažinti riziką ir imtis aktyvių veiksmų apsaugoti ne tik save, bet ir visą organizaciją bei visuomenę, kuriai mes tarnaujame.“

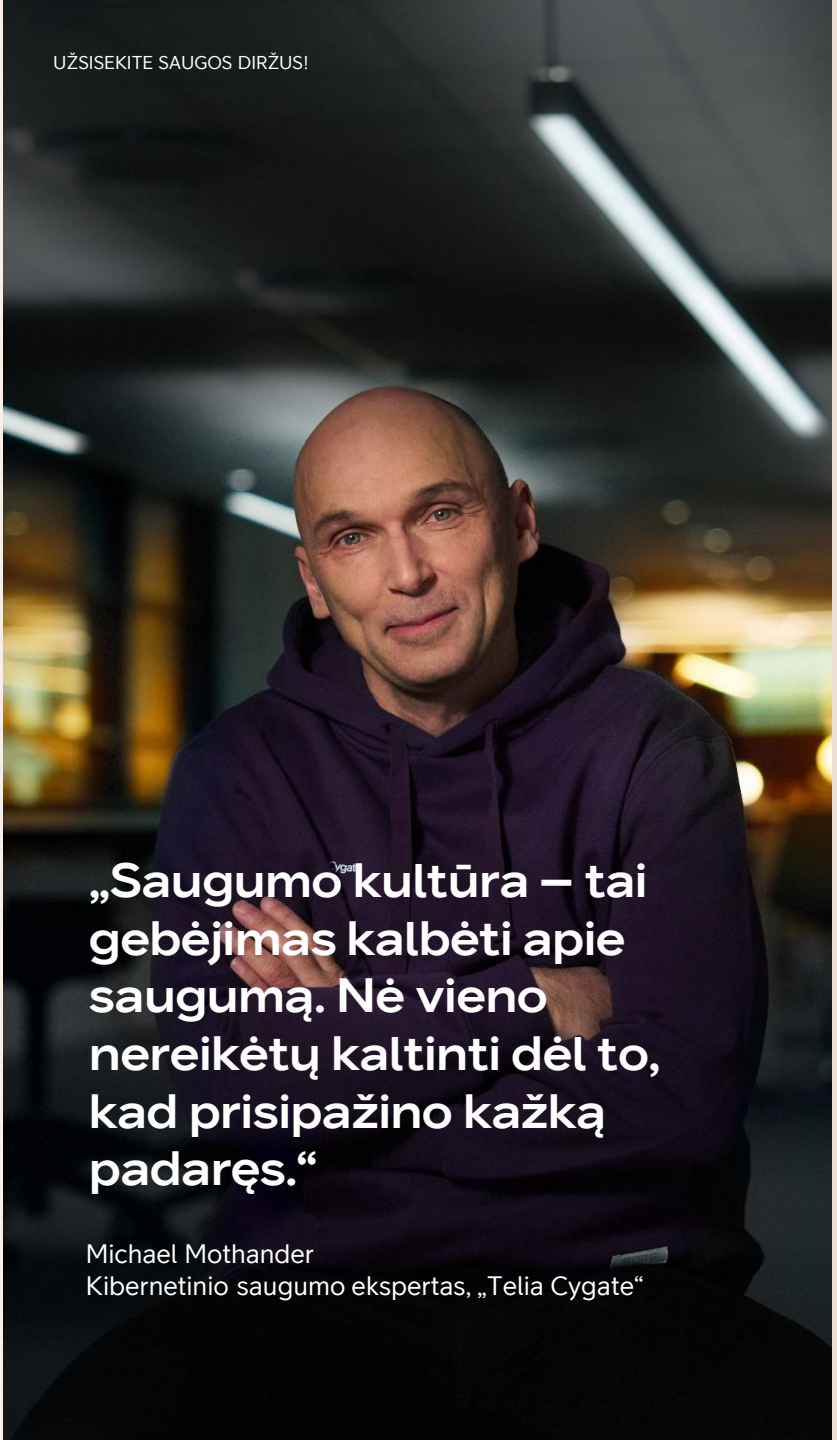
Malin Fransén Kronberg
„Telia Sverige“ saugumo vadovė

Kibernetinio atsparumo gidas: penkių svarbiausių saugumo kultūros elementų formavimas

Mes nustatėme penkis bendrus saugumo aspektu brandžių organizacijų elementus.

Visi minėti ypatumai padeda kurti atsparią saugumo kultūrą, suteikdami žmonėms galimybę aktyviai dalyvauti, mokytis ir tobulėti.

01	02	03	04	05
Ps	Lp	Jt	Sp	Nm
Psichologinis saugumas	Lengva paranoja	Jokios trinties	Skirtingos perspektyvos	Nuolatinis mokymasis



„Saugumo kultūra – tai gebėjimas kalbėti apie saugumą. Nė vieno nereikėtų kaltinti dėl to, kad prisipažino kažką padaręs.“

Michael Mothander
Kibernetinio saugumo ekspertas, „Telia Cygate“

01. Psichologinis saugumas

Tradiciškai daugelyje organizacijų kibernetinio saugumo sritį supdavo tylos ir gėdos kultūra. Žmonės bijodavo klysti ir pripažinti klaidas, o patyrusios išpuolį organizacijos stengdavosi apie jį nutylėti.

Atspariose organizacijose laikomasi nekaltinimo ir nesigėdinimo politikos: darbuotojai nebijo klysti ir žino, kad gali nesibaimindami apie savo klaidas pranešti. Padarius klaidą jokie atsakomieji veiksmai jų atžvilgiu jiems negresia.

Pirmieji reaguoja ir pagalbą pažeidžiamiems darbuotojams, kurie tapo grėsmių sukėlėjų taikiniu ir kuriais buvo pasinaudota nusikaltimo tikslu, teikia specialiai parengti ekspertai.

Pagrindinis psichologinio saugumo komponentas – skaidrumas. Įvykus incidentams ekspertai sąžiningai bendrauja su darbuotojais ir suinteresuotosiomis šalimis, kas savo ruožtu stiprina abipusį pasitikėjimą, nes darbuotojai nesibaimina „prisiduoti“.

Darbuotojų psichologinio saugumo vertinimas

*Klausimyną parengė Harvardo universiteto profesorė Amy Edmondson**

1	2	3	4	5	6	7
Jei šioje komandoje padarysite klaidą, jus dėl jos nekaltins.	Komandos nariai gali iškelti problemas ir sudėtingus klausimus.	Komandos nariai sutinka su tuo, kad kiti nariai yra kitokie.	Šioje komandoje saugu rizikuoti.	Paprašyti kitų komandos narių pagalbos nėra sunku.	Niekas nesiekia tyčia pakenkti mano pastangoms.	Mano unikalūs įgūdžiai ir gabumai yra vertinami bei panaudojami.

**Atlikite savo komandos testą fearlessorganizationscan.com*

02. Lengva paranoja

Galbūt dėl abstraktaus ir dažnai netiesioginio kibernetinių išpuolių pobūdžio žmonės apskritai yra pernelyg patiklūs. Šis budrumo trūkumas paskatino grėsmių sukėlėjus tuo pasinaudoti.

Tam, kad būtų galima užtikrinti visos įmonės budrumą, atsparios organizacijos sugebėjo sukonkretinti ir išryškinti riziką. Visa tai jos padarė pernelyg nepanikuodamos. Pasak „Telia Company“ informacijos saugos vadovo Niclaso Jalvingerio, šiuo atveju itin svarbu lengva paranoja – labiau suvokiama rizika neprarandant sveiko proto.

Visada geriau pranešti daugiau, nei pranešti nepakankamai. Vienintelė grėsmė, kurios galima išvengti, yra grėsmė, kuri yra aptikta. Tai du teiginiai, kurie susiję su psichologiniu saugumu.

Trys svarbiausios Niclaso Jalvingerio taisyklės

Kaip formuoti saugumą įkvepiančią kultūrą

1

Veikti pagal įsitikinimus
Nieko nebus, jei vadovai stovės tribūnoje ir kalbės apie saugumą, tačiau patys juo nesirūpins. Viskas prasideda nuo viršaus.

2

Daugiau klausytis, mažiau kalbėti
Niekada nemanykite, kad žinote daugiau nei darbuotojai. Daug ką galima sužinoti tiesiog klausantis, o ne patiems kalbant.

3

Mąstyti taip, kaip mąsto nusikaltėlis
Norėdami sustiprinti supratimą, skatinkite darbuotojus sugalvoti, kaip nusikaltėliai galėtų užpulti įmonę.

„Jūs nenorite statyti Fortnokso, nes tuomet negalėsite veikti. Reikia rasti tinkamą pusiausvyrą. Ne viską pavyks apsaugoti 100 proc.“

Niclas Jalvinger
„Telia Company“ informacijos saugos vadovas

„Jei padarysime taip, kad dėl saugumo priemonių dirbti bus sunkiau arba darbas vyks lėčiau, o sprendimus priimsime nedalyvaujant darbuotojams, skaitmeninės technologijos bus įdiegtos beprasmiai.“

Simon Binder
Kibernetinio saugumo ekspertas, „Telia Cygate“

03. Jokios trinties

Pastebėta, kad organizacijos, kurioms atlikti savo darbą reikalingas didelis kognityvinis krūvis darbuotojams, yra pasmerktos nesėkmei.

Atsparios organizacijos nedirba prieš žmogaus prigimtį. Veiksmus saugumo srityje jos pritaiko prie žmogaus prigimties. Užuot primetusios darbuotojams naujus darbo būdus, įmanomu laipsniu jos įtraukia saugumo technologijas ir procesus į esamą elgseną bei darbo eigą. Svarbiausia – atkreipti dėmesį į tai, kas žmonėms svarbu. Reikia rasti būdų, kaip suderinti individualias ir organizacines paskatas.

Dėl daugybės akronimų ir santrumpų, kurios naudojamos kibernetinio saugumo srityje, ši tema yra ir neaiški, ir atstumianti. Atsparios organizacijos mažina trintį naudodamos paprastą ir nedviprasmišką saugumo kalbą taip, kad sumažintų protinę įtampą ir išvengtų nesusipratimų rizikos. Svarbu ir tai, kad jos supranta, jog saugumo srityje nėra vienintelio universalaus sprendimo. Siekiant, kad padidėtų įtraukimas ir išlaikymas atmintyje, žinia turi būti pritaikyta skirtingoms auditorijoms.

Kitas trinties taškas – neaiški komunikacija: nežinojimas, ką daryti ir į ką kreiptis iškilus grėsmei. Tam, kad supaprastintų komunikaciją ir paskatintų teikti pranešimus, atsparios organizacijos sukuria aiškius protokolus.

3 būdai sumažinti trintį

Trys būdai, kaip atsparios organizacijos dirba su žmogaus prigimtimi, o ne prieš ją

1

Kreipkitės į ekspertus
Norėdami nustatyti, kaip būtų geriausia pasiekti ilgalaikių pokyčių, bendradarbiaukite su žmonių elgsenos ir psichologijos ekspertais.

2

Supaprastinkite kalbą
Siekdami rasti visiems suprantamą bendrą kalbą kibernetinio saugumo klausimais, bendradarbiaukite su komunikacijos skyriumi.

3

Apeliuokite į asmeninius interesus
Žmonės palaiko tai, ką sukuria patys. Siekdami nuleisti kartelę žemiau, sutelkite dėmesį į tai, kas motyvuoja žmones kasdieniame darbe

04. Skirtingos perspektyvos

Kibernetinis saugumas tradiciškai yra vienalytė sritis, kurioje dominuoja vyrai: daugelis specialistų turi panašią patirtį, išsilavinimą, žinias ir kultūrines nuostatas. Tai kelia labai realią nesuvokimo grėsmę dėl dėmesingumo stokos, kuri pasireiškia tuomet, kai asmenys nepastebi netikėtų, tačiau jiems matomoje vietoje esančių dirgiklių.

Atliekant vieną garsų eksperimentą, 24 radiologai tyrė plaučių rentgeno nuotraukų seriją, ieškodami auglių. Paskutinėje rentgeno nuotraukoje buvo įdėta gorila – 48 kartus didesnė už vidutinį auglį. 83 % radiologų gorilos nepastebėjo.

Atsparios organizacijos įtraukia darbuotojus į saugumo užtikrinimo procesą, pasinaudodamos tuo, kad **skirtingos perspektyvos didina tikimybę, jog grėsmės bus aptiktos ir jų pavyks išvengti**. Jos pasitelkia nestandartinį požiūrį ir panaudoja naujus įgūdžius: elgsenos mokslininkai, buvę programišiai ir kariškiai puikiai gali prisidėti formuojant ateities saugumo kompetenciją.

3 patarimai dėl naujo požiūrio

Keli patarimai ir gudrybės, kaip praplėsti akiratį

1

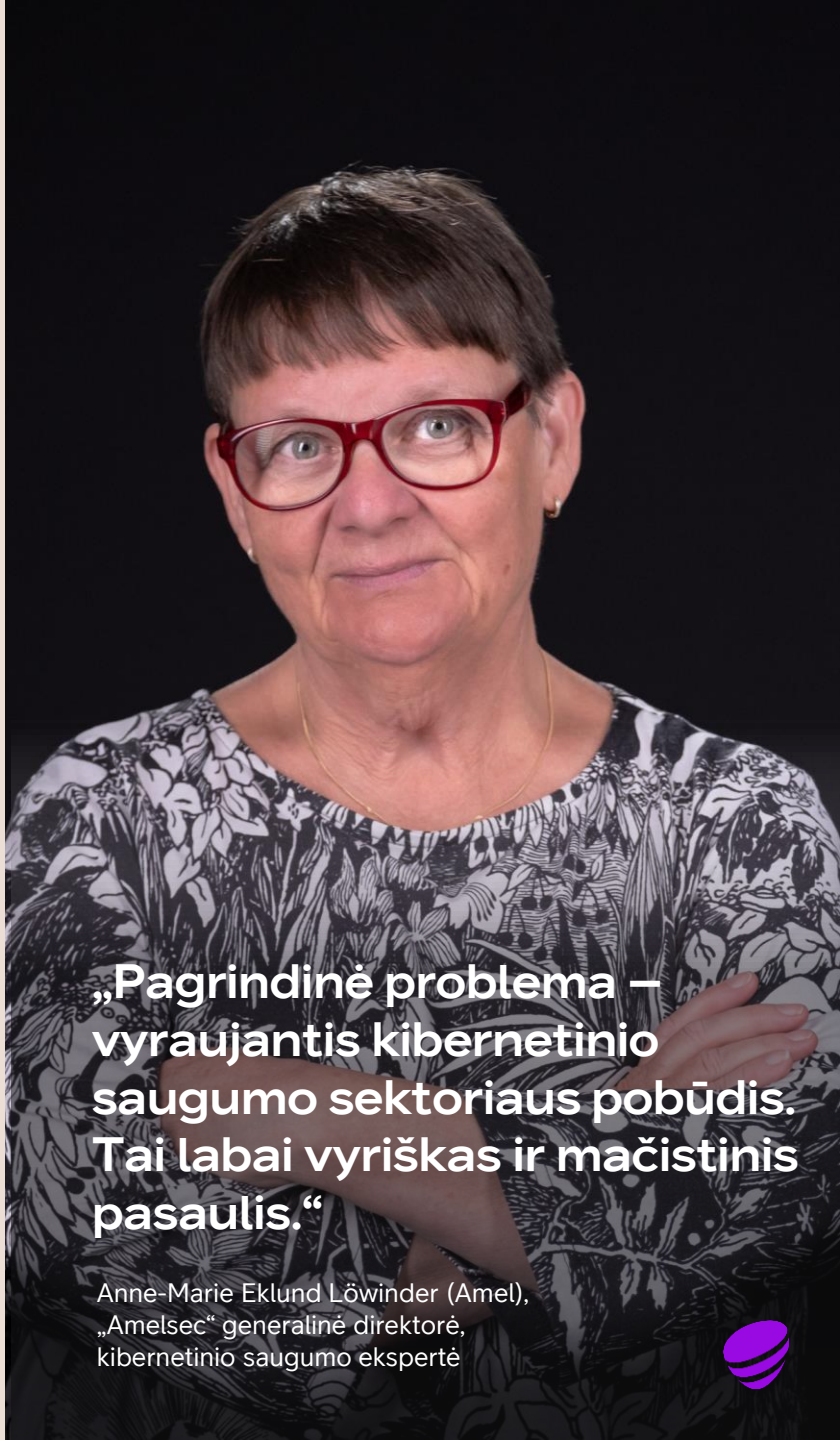
Pripažinkite savo tendencingumą
Komandos, kurių narių patirtis ir įgūdžiai panašūs, gali nepastebėti svarbių saugumo veiksnių. Nustatykite galimus tendencingumus ir įneškite naujų perspektyvų.

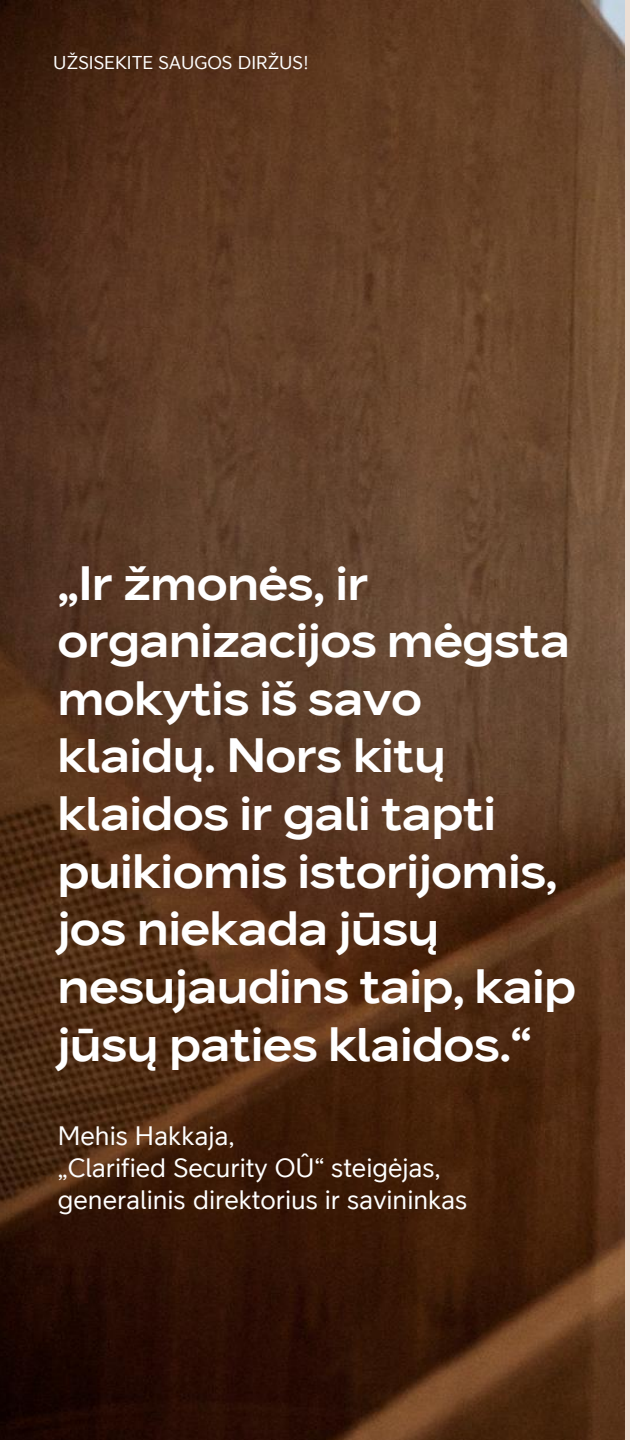
2

Diversifikuokite saugumo srities įgūdžius
Nusikaltėliai sparčiai tobulėja. Meskite iššūkį tradicijoms ir pasitelkite naujus įgūdžius. Geriausi įgūdžių šaltiniai, kurie padės jūsų komandai pasirūpinti ateitimi, yra elgsenos ekspertai, analitikai ir procesų vadovai.

3

Susiraskite naujų draugų
Suformuokite struktūriškai apibrėžtą pagrindinių suinteresuotųjų šalių ir skyrių bendradarbiavimą kibernetinio saugumo srityje – pradedant Personalo, Komunikacijos bei Teisės skyriais ir baigiant aukščiausiąja vadovybe.





„Ir žmonės, ir organizacijos mėgsta mokytis iš savo klaidų. Nors kitų klaidos ir gali tapti puikiomis istorijomis, jos niekada jūsų nesujaudins taip, kaip jūsų paties klaidos.“

Mehis Hakkaja,
„Clarified Security OÛ“ steigėjas,
generalinis direktorius ir savininkas

05. Nuolatinis mokymasis

Daugelis organizacijų nesupranta, kad labai svarbu leisti darbuotojams skirti laiko ir išteklių kvalifikacijos kėlimui. Jei to nėra, greitų pokyčių akivaizdoje darbuotojai tampa bejėgiai.

Atsparios organizacijos aprūpina darbuotojus žiniomis ir priemonėmis, skatina smalsumą ir nuolatinį tyrinėjimą. Siekdamos, kad nebūtų trinties, jos kruopščiai rengia ir vykdo mokymus taip, kad žinios būtų lengvai priimamos, įsimenamos ir įgyvendinamos.

Siekdamos sumažinti energijos sąnaudas ir padidinti poveikį, organizacijos taiko ir elgsenos mokslo metodus, pavyzdžiui, mažų įpročių formavimą. Darbuotojams neužkraunama daugiau informacijos ar instrukcijų, nei jų reikia saugiai veikti konkrečiame organizacijos kontekste.

Įvykę incidentai vertinami kaip galimybė mokytis ir tobulėti. Nuolatinis mokymasis veikiant ir prisitaikymas yra ne tik pagrindinis atsparumo bruožas, bet ir apčiuopiamas būdas kurti organizacijos žinių kapitalą.

Galiausiai, nors atsparios organizacijos konkuruoja verslo srityje, jos bendradarbiauja saugumo srityje. Keitimasis įgyta patirtimi įvairiuose ūkio sektoriuose didina bendrą sistemos atsparumą ir prisideda prie saugesnės organizacijos aplinkos.

3 mokymosi stimulai

Trys patarimai, kaip patraukti darbuotojų dėmesį ir juos įtraukti

1

Pranešimų teikimas
Įsitikinkite, kad darbuotojai turi tinkamas mokymosi ir pranešimų teikimo priemones bei procesus, kuriuos lengva suprasti ir naudoti.

2

Mokykitės kartu su kitais
Į realius incidentus žiūrėkite kaip į galimybę diskutuoti, bendradarbiauti, dalytis įgyta patirtimi ir prisitaikyti. Apsvarstykite galimybę bendradarbiauti su išorės organizacijomis ir partneriais.

3

Padarykite taip, kad mokymasis taptų įtraukus
Naudokite atvejus ir pavyzdžius iš tikrovės, kad įkvėptumėte (ir išgąsdintumėte). Eksperimentuokite su naujais ir patraukliais formatais, pavyzdžiui, naudokite žaidimus, tinklalaides, kvieskite pranešėjus iš kitur.

Kibernetinio atsparumo gidas: penki veiksmai, kurių reikia imtis

Norint pakeisti įpročius reikia laiko, net jei tie pokyčiai būtų susiję su mūsų pačių išlikimu.

Akivaizdu, kad nepakanka vien tik sukurti tinkamas saugumo priemones bei procesus – reikia, kad žmonės juos priimtų ir naudotų.

5 veiksmai, kurių reikėtų imtis norint sukurti atsparią saugumo kultūrą.

01	02	03	04	05
Ps	Lp	Jt	Sp	Nm
Psichologinis saugumas	Lengva paranoja	Jokios trinties	Skirtingos perspektyvos	Nuolatinis mokymasis
Paversti įmonę saugia erdve	Saugumą padaryti vadovybės prioritetu	Saugumą paversti paprastu dalyku	Saugumą paversti įtraukiu dalyku	Saugumą paversti viliojančiu dalyku

09

Išvados

Drauge – stipresni

Bandant susiorientuoti šiame skaitmeniniame amžiuje, kuris kinta vis sparčiau, **svarbiausias mūsų turtas yra atsparumas**. Kaip saugos diržas pakeitė automobilio saugumą, taip ir gyva kibernetinio saugumo kultūra gali apsaugoti mūsų organizacijas nuo nuolat kylančių grėsmių. Aktyviai apsvarstydami riziką ir puoselėdami nuolatinio mokymosi bei prisitaikymo kultūrą, pažeidžiamumą mes galime paversti stiprybe.

Ateitis priklauso tiems, kurie jai bus pasirengę. Priimkime šiuos principus tam, kad sukurtume saugų pagrindą, grindžiamą partneryste ir skaidrumu. Tik tada galėsime drąsiai žengti į saugesnį ir išmanesnį rytojų.

Niekas negali visko išspręsti vienas, todėl suvienykime jėgas! Drauge mes galime iššūkius paversti galimybėmis ir užtikrinti, kad mūsų skaitmeniniai greitkeliai būtų tiek pat saugūs, kiek yra greiti.

Jei norite tęsti diskusiją arba sužinoti daugiau, kreipkitės į „Telia“!

09

Priedas

Ataskaitos bendraautoriai

„Teli‘ atstovai	Pareigos	Organizacija
Aurimas Žlibinas	Verslo padalinio vadovas	Telia Lietuva
Kristjan Kukk	Verslo klientų padalinio vadovas	Telia Estonia
Conor McGlynn	Saugumo strategijos ir pertvarkos vadovas	Telia Company
Håkan Kvarnström	Valdymo, rizikos ir atitikties vadovas	Telia Company
Ida La Spisa	Informacinių technologijų direktorius	Telia Sweden
Jon Christian Hillestad	Įmonės vadovas	Telia Norway
Kristofer Ågren	Division X padalinio produkto vadovas	Telia Company
Magnus Leonhardt	Strategijos ir inovacijų vadovas	Telia Sweden
Malin Fransén Kronberg	Saugumo vadovas	Telia Sweden
Mats Mägiste	Saugumo infrastruktūros ekspertas	Telia Sweden
Michael Mothander	Kibernetinio saugumo ekspertas	Telia Cygate
Minna Vyyrylainen	Verslo ryšių formavimo vadovas	Telia Company
Nicholas Rundbom	Komunikacijos verslo klientams vadovas	Telia Sweden
Nicklas Olofsson	Kultūros ir augimo sritis	Telia Company
Niclas Jalvinger	Įmonių grupės informacinio saugumo ir kitų sričių saugumo direktorius	Telia Company
Ola Rembe	Prekės ženklo, komunikacijos ir tvarumo srities vadovas	Telia Company
Olli Pirttijärvi	Verslo klientų padalinio vadovas	Telia Finland
Patrik Holmqvist	Veiklos operacijų vadovas	Telia Cygate
Pontus Eklöf	Vyresnysis pardavimų specialistas	Telia Company
Sam Rabar	Kibernetinio saugumo ekspertas	Telia Company
Sigrid Reijnst	Darbdavio prekės ženklo vadovas	Telia Company
Simon Binder	Kibernetinio saugumo ekspertas	Telia Cygate
Thomas Johansson	Pasaulinio verslo strategijos sritis	Telia Company
Tobias Larsson	Verslo klientų padalinio Švedijoje vadovas	Telia Sweden
Tomas Eklind	Portfelio vadybininkas	Telia Company
Vinicius Joaquim Camargo	Division X padalinys	Telia Company

Ataskaitos rengimo projekto grupė	Pareigos	Organizacija
Emelie Aidehag	Įžvalgų ir prognozių vadovas	Telia Company
Magnus Fahlgren	Prekės ženklo įžvalgų vadovas	Telia Company
Suzanne Tellström	Prekės ženklo valdymas	Telia Company

Kviestiniai ekspertai	Pareigos
Anne Marie Eklund Löwinder	„Amelsec“ generalinis direktorius ir steigėjas, žinomas kibernetinio saugumo ekspertas ir buvęs „Crypto“ aukščiausiojo lygmens vadovas
Mehis Hakkaja	„Clarified Security OÛ“ steigėjas, generalinis direktorius ir savininkas
Pontus Johnson	KTH profesorius, Kibernetinės apsaugos ir informacijos saugumo centro direktorius
Åke Holmgren	Švedijos civilinės saugos agentūra, MSB Kibernetinio saugumo ir saugių ryšių vadovas

Tyrimų agentūros komanda	Pareigos
Alexis Bolonassos	„Augur“ tyrimų strategas
Jenny Franzén Lycke	„Augur“ prognozavimo direktorius

Šaltiniai

Albarracin, D. et. al. (2024). Determinants of behavior and their efficacy as targets of behavioral change interventions

Alis Behavioral Health (2024) https://www.alisbh.com/blog/ average-human-attention-span-statistics-and-facts

Allianz Commercial. (2023). *Cyber security trends 2023.*

Barreto, H. (2024). *The secret to creating brand loyalty. Forbes*

Brooks, C. (2023). *Cybersecurity Trends & Statistics for 2023; What You Need To Know. Forbes*.

Cisco. (2024). *Security Outcomes Report Vol. 3. Achieving Security Resilience.*

Click. (2024). *A no bullshit paper: A manifesto for Effortless Culture Change.*

Deloitte. (2022). *Global Future of Cyber Survey 2023. Building long-term value by putting cyber at the heart of the business.*

European Parliamentary Research Service. (2023). *The NIS2 Directive. A high common level of cybersecurity in the EU*

Farnam Street (2021) *The Great Mental Models Volume 2: Physics, Chemistry, and Biology*

Fortanix. (2023). *Preparing for post-quantum cryptography. Mapping your organization's data security strategy to the effects of quantum computing*

Fortinet (2022). *Cybersecurity skills gap.*

Gartner. (2023). *Gartner Identifies the Top Cybersecurity Trends for 2023.* [press release]

Heino, M et. al. (2024) *From a false sense of safety to resilience under uncertainty.*

IBM (2024) https://www.ibm.com/topics/phishing

LastPass (2024). *Combating Social Engineering in 2024.*

International Telecommunication Union. (2021).

McKinsey & Company. (2022). *Cybersecurity trends: Looking over the horizon.*

Pentera (2024) *The State of Pentesting 2024*

PWC (2021), *Global Culture Survey.*

Radar. (2024). *Cybersäkerhet 2024. Från verksamhet till ekosystem.*

Seenit (2023). *The State of Employee Engagement.*

Sentor. (2021). *ISO 27001. En introduktion till standarden.*

Snowflake. (2024). *Data + AI predictions 2024..*

Splunk (2024). *State of Security 2024: The Race to Harness AI*

SVT (2024), *Allvarliga brister i svenska myndigheters cybersäkerhet*

Telenor. (2024). *Digital Security 2023. It gets serious.*

Telia (2024) *Telia Digital Index (2024).*

World Economic Forum. (2024). *The Global Risks Report 2024.*

World Economic Forum. (2024). *Global Cybersecurity Oulook 2024.*