MEDIA LITERACY ACCELERATOR

SKAITMENINIO SAUGUMO ABC

Atmintinė nevyriausybinėms organizacijoms

2021 m.

MEDIA LITERACY ACCELERATOR

Teigti, kad jums ***nerūpi privatumas****,*

nes neturite ***ką slėpti****,*

yra tas pats kaip pasakyti,

kad jums ***nerūpi žodžio laisvė****,*

nes neturite, ***ką pasakyti****.*

Atmintinę parengė Dalia Bankauskaitė, Aušrinė Diržinskaitė, Aidas Gedminas, Renata Matkevičenė, „Medijų raštingumo akseleratoriaus“ lektoriai

Šioje atmintinėje:

Prieš pradedant, kviečiame paskaityti kolegos Aido interviu.

Kodėl turėčiau skirti laiką savo skaitmeniniam saugumui ir kokie svarbiausi skaitmeninės higienos principai?

Atrodo pasaulį ištikus COVID-19 pandemijai ne tik darbą, bet ir gyvenimą kiekvienas perkėlėme į skaitmeninę erdvę. Mūsų organizacijų namais tapo nešiojami kompiuteriai ir išmanieji prietaisai, į internetą persikėlė ne tik bendravimas su tikslinėmis grupėmis, bet ir mūsų hobiai ar net šeimos šventės. Dar iki pandemijos, o greičiausiai ir po jos, vis daugiau mūsų pasaulio skaitmenėja. Kaip ir gyvame pasaulyje, taip ir virtualiame, egzistuoja pakankamai paprastos higienos taisyklės, kurios padeda apsisaugoti nuo kenkėjų. Pavyzdžiui įsilaužimo į kompiuterį ar mobilųjį telefoną, asmens duomenų vagysčių ir panaudojimo netinkamiems tikslams.

Pagrindiniai principai, kurių svarbu laikytis veikiant skaitmeninėje erdvėje:

- Mūsų saugumas stiprus tiek, kiek stipri yra mūsų silpniausia vieta.
- Jei paslauga ar produktas socialinėse medijose yra nemokamas, mes esame produktas arba prekė. Mūsų laikas ir dėmesys yra pati vertingiausia prekė.
- Skaitmeninis saugumas yra kelionė, kurią planuojame patys.
- Jos metu visada turime būti pasirengę įsilaužimui.

Cambridge Analytica ir duomenų rinkodara

Didžiosios Britanijos politinių konsultacijų ir technologijų įmonės „Cambridge Analytica“ atvejis 2016 m. JAV Prezidento rinkimų metu puikus pavyzdys, kodėl asmens duomenys yra tokie vertingi ir kaip jais gali būti piktnaudžiaujama. Įmonė surinko 87 mln. asmenų labai išsamios asmeninės informacijos apie JAV piliečius iš socialinio tinklo Facebook. Ir jiems net nereikėjo nieko vogti. Žmonės Facebook platformoje savanoriškai pildė pramoginio pobūdžio anketas ir taip patys atidavė savo asmeninę informaciją.

„Cambridge Analytica“ panaudodama duomenis sukūrė daugybę detalių psichologinių portretų, kuriuos naudojo formuluojant politines žinutes JAV rinkėjams ir jas reklamuojant. D. Trumpo prezidentinė rinkimų kampanija pasinaudojo šiais duomenimis, sukūrė labai konkrečias žinutes ir jas rodė tik tiems žmonėms, kuriems jos turėjo patikti, atsižvelgiant į gautus duomenis. Daugiau informacijos apie šį atvejį ir bylą anglų kalba. Jei dar nematėte

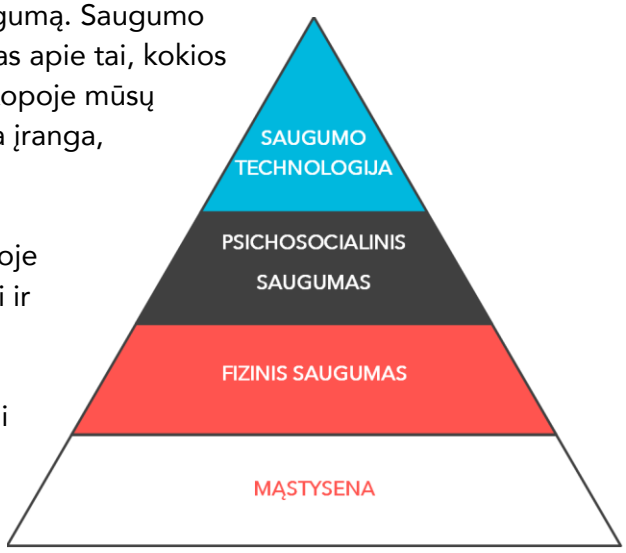
Suomija ir Lietuva – duomenų vagystės

2019 m. spalio mėn. Suomijos psichoterapijos klinika patyrė kibernetinę ataką, kilo pavojus dešimčiai tūkstančių pacientų, jų gydymo įrašams. Pacientai buvo šantažuojami, elektroniniu paštu jiems buvo siunčiami laiškai su reikalavimais sumokėti 200-500 eurų vertės bitkoinų mainais už tai, kad būtų ištrinti jų duomenys. Vadinamajame tamsiajame tinkle (dark web) buvo paskelbta 10 GB informacijos apie 300 pacientų, įskaitant diagnozes, kontaktų informaciją ir pacientų dienoraščius, buvo siūloma parduoti-pirkti duomenis. Daugiau apie šią istoriją skaitykite čia.

Panašus atvejis atsitiko ir Lietuvoje. Ne, kalbame ne apie „City Bee“, kurį daugelis ko gero girdėjote (daugiau apie šį atvejį ir duomenų apsaugą organizacijose klausykite tinklalaidėje „Kaip užtikrinti duomenų apsaugą organizacijoje“). Dar 2017 m. buvo įsilaužta į „Grožio chirurgijos“ duomenų bazę ir pavogti 22 tūkst. klinikos klientų duomenų. Iš „Grožio chirurgijos“ reikalauta 500 tūkst. eurų vertės bitkoinų kriptovaliutos, iš klinikos klientų – nuo 50 iki 800 eurų už tai, kad gauti duomenys, tarp kurių ir klientų nuotraukos, nebūtų paviešinti. Atliekant tyrimą paaiškėjo, kad įsilaužimas įvyko panaudojus buvusio klinikos darbuotojo prisijungimo duomenis.

Nesvarbu, kokia didelė ir pajėgi organizacija, įmonė ar net valstybė būsime, bet kada galime patirti kibernetinę ataką, mūsų duomenys gali būti nutekinti. Nesvarbu kaip gerai būsime pasiruošę, visada atsiras naujų virusų, naujų technologijų, kurios gali būti panaudotos piktavališkiems tikslams. Interneto pasaulio normatyvinė sistema vis dar yra reaktyvi, dar tik formuojama. Todėl skaitmeninio saugumo pagrindas turėtų būti asmens mąstysena, požiūris į saugumą interneto erdvėje, o tik tada formuojasi įpročiai, kuriems pasitelkiame technologijas.

Saugumo piramidė padeda suprasti holistinį požiūrį į saugumą. Saugumo piramidės pagrindas yra mūsų sąmoningumas ir supratimas apie tai, kokios grėsmės mums kyla ir kaip galime jų išvengti. Antroje pakopoje mūsų fizinis saugumas: kaip rūpinamės savo kompiuterine ir kita įranga, kur ją laikome, ar paliekame atrankintą ar užrakiname, kai nesinaudojame, ar duodame ja naudotis nepažįstamiems žmonėms, ar ją pametame. Trečioji pakopa - aplinka, kurioje naudojiesi internetu, kokie žmonės mus supa, kaip saugiai ir psichologiškai patogiai pats asmuo jaučiasi. Ir tik pačioje piramidės viršūnėje yra technologija, kuria naudojamės: mūsų slaptažodžiai, autentifikavimo protokolai, asmeniniai nustatymai ir pan.



Dažnai įsilaužimams technologiniai sprendimai nereikalingi. Pavyzdžiui, pažiūrėkite kaip atliekama socialinė inžinerija:

https://www.youtube.com/watch?v=fHhNWAKw0bY

Kaip susikurti tikrai saugų slaptažodį

Kuris iš dviejų slaptažodžių yra stipresnis?

sl4pt4zod1s! – ar tai stiprus ar silpnas slaptažodis?
antra.diena.lyja.siandien.valgiau.duona.su.sviestu.08.21! – ar tai stiprus ar silpnas slaptažodis?

Atsakymas - antrasis slaptažodis yra stipresnis. Jį nulaužti prireiks trilijonų šimtmečių. Ir jį lengviau įsiminti, nes toks slaptažodis yra prasminga frazė.

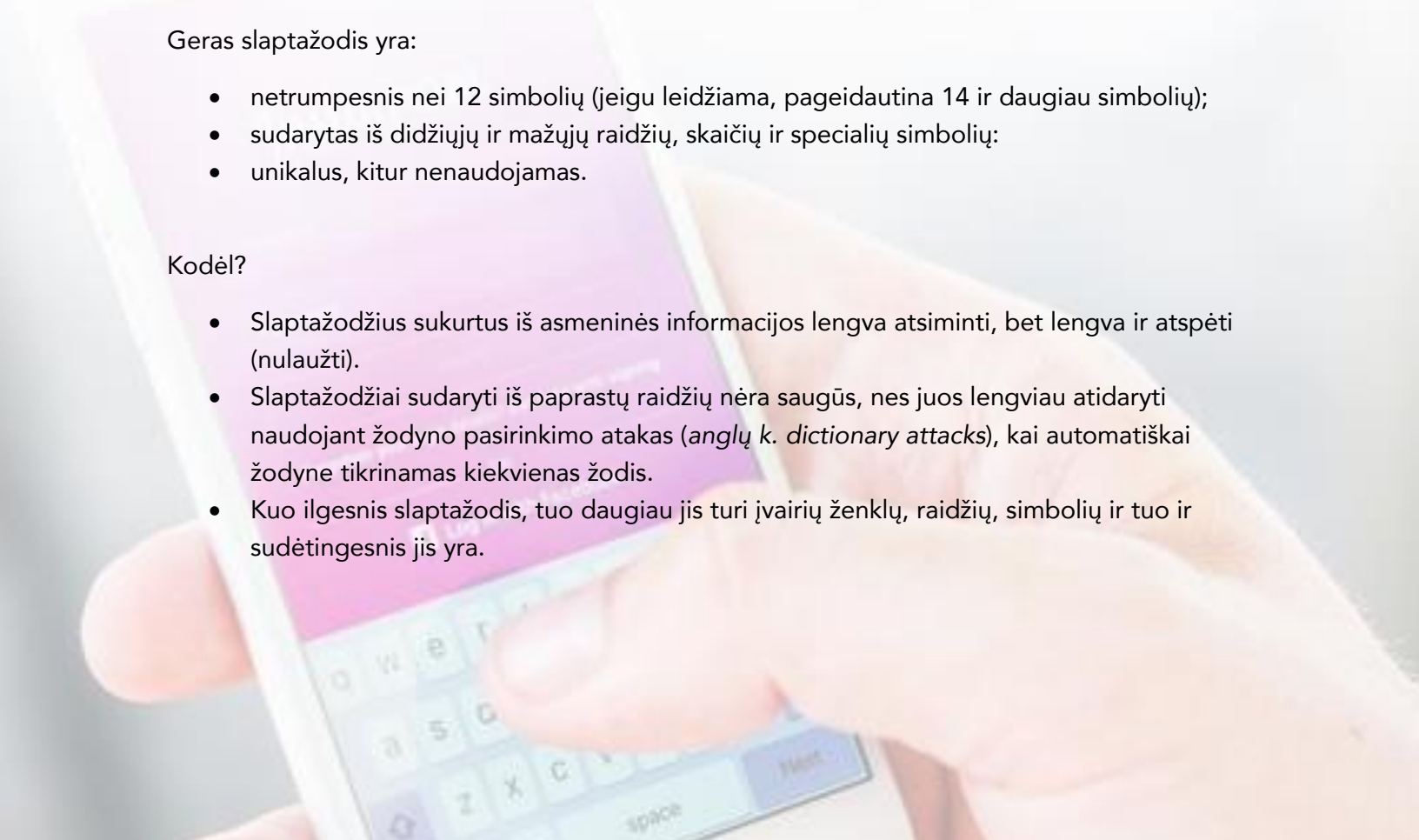
Todėl saugus slaptažodis nereiškia tokio, kurio neįmanoma prisiminti. Pagalvokite apie mėgstamą dainą, eilėraštį ar frazę. Ir panaudokite ją.

Geras slaptažodis yra:

- netrumpesnis nei 12 simbolių (jeigu leidžiama, pageidautina 14 ir daugiau simbolių);
- sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialių simbolių:
- unikalus, kitur nenaudojamas.

Kodėl?

- Slaptažodžius sukurtus iš asmeninės informacijos lengva atsiminti, bet lengva ir atspėti (nulaužti).
- Slaptažodžiai sudaryti iš paprastų raidžių nėra saugūs, nes juos lengviau atidaryti naudojant žodyno pasirinkimo atakas (*anglų k. dictionary attacks*), kai automatiškai žodyne tikrinamas kiekvienas žodis.
- Kuo ilgesnis slaptažodis, tuo daugiau jis turi įvairių ženklų, raidžių, simbolių ir tuo ir sudėtingesnis jis yra.



Asmens tapatybės patvirtinimas – dviejų faktorių autentifikavimas

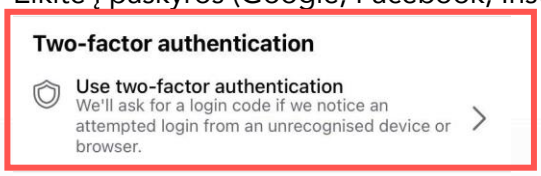
Net, jei jūsų slaptažodį kažkas ir atspėjo arba nulaužė, padėti gali paprasta priemonė – dviejų faktorių autentifikavimas. Tokiu principu veikia prisijungimas prie banko sąskaitos internetu, išmanioji aplikacija „Smart-ID“. Tokiu pats principu veikia ir banko generatoriai.

Ką tai reiškia? Autentiškumo patvirtinimo mechanizme pateikiami du ar daugiau įrodymų:

- **žinios** (slaptažodis, slaptas klausimas);
- **turėjimas** (mobiliojo telefono, duomenų rakto pvz. „YubiKey“);
- **įgimta savybė** (biometriniai duomenys).

Kaip nustatyti daugiafaktorinę autentifikaciją?

Eikite į paskyros (Google, Facebook, Instagram ir kt.) nustatymus ir ieškokite:



Slaptažodžių tvarkymas

- Naudokite skirtingus slaptažodžius skirtingose platformose ar sistemose;
- Daugelyje naršyklių galima išsaugoti slaptažodžius, tačiau to daryti nereikėtų, nes bet kas gavęs prieigą prie jūsų kompiuterio (pvz. paskolinote jį draugui) gaus prieigą ir prie visų išsaugotų slaptažodžių.
- Naudokite slaptažodžių saugojimo programines įrangas, kurios padės sekti jūsų slaptažodžius (pvz. Google);

Slaptažodis ne veltui taip vadinasi. Jis turi būti slaptas reikalas 😉 Todėl niekada niekam nesakykite savo slaptažodžio. Jei turite naudotis bendra paskyra su kažkuo (pvz. įmonės vardu), susikurkite bendrus slaptažodžius ir juos reguliariai keiskite.

Nepalikite užrašyto savo slaptažodžio vietose, kur lengva jį rasti, pvz. ant darbo stalo.

Keli slaptažodžių tvarkyklių pavyzdžiai (sąrašas tikrai ne tobulas ir ne baigtinis, tačiau nuo jo galima pradėti!).

Slaptažodžių tvarkyklės tipas	Privalumai	Trūkumai
Local (https://www.keepassx.org/)	Slaptažodžiai laikomi ten, kur jūs juos galite valdyti	Reikia reguliaraus atnaujinimo, sudėtinga sinchronizuoti su keliais prietaisais
Cloud (https://bitwarden.com/)	Sinchronizuojasi su keliais prietaisais (pvz. kompiuteris ir telefonas)	Slaptažodžiai laikomi trečiosios šalies valdomoje aplinkoje, paslaugos teikėjas gali rinkti metaduomenis tokius kaip IP, naršymo istorija
Stateless (https://lesspass.com/)	Slaptažodžiai nelaikomi debesyse ar vietiniame serveryje	Jautrus domenų pasikeitimui (pvz. keičiasi platformos adresas)

Renkantis sprendimą svarbu suprasti ir tai, kad dažniausiai turime rinktis iš saugumo vs. patogumo/universalumo. Kuo patogesnė ir universali įranga, tuo labiau tikėtinos saugumo spragos. Todėl kiekvienas turi įsivertinti, kiek turimi duomenys yra jautrūs ir kiek stiprios apsaugos reikia, o kiek svarbu galėti lengvai, lanksčiai ir greitai jais naudotis.

Domain name system – kas tai ir kodėl turėtų rūpėti???

Internetu naudojamės kasdien, o ar žinome kaip jis veikia? Siūlome skirti kelias minutes ir patiems suprasti, kur praleidžiame tokią didelę dalį savo gyvenimo:

https://www.youtube.com/watch?v=AYdF7b3nMto&feature=youtu.be

Taigi, mums naršyti internete padeda DNS (*domain name system)*, tačiau tai gali būti pirmoji mūsų fizinio saugumo spraga.

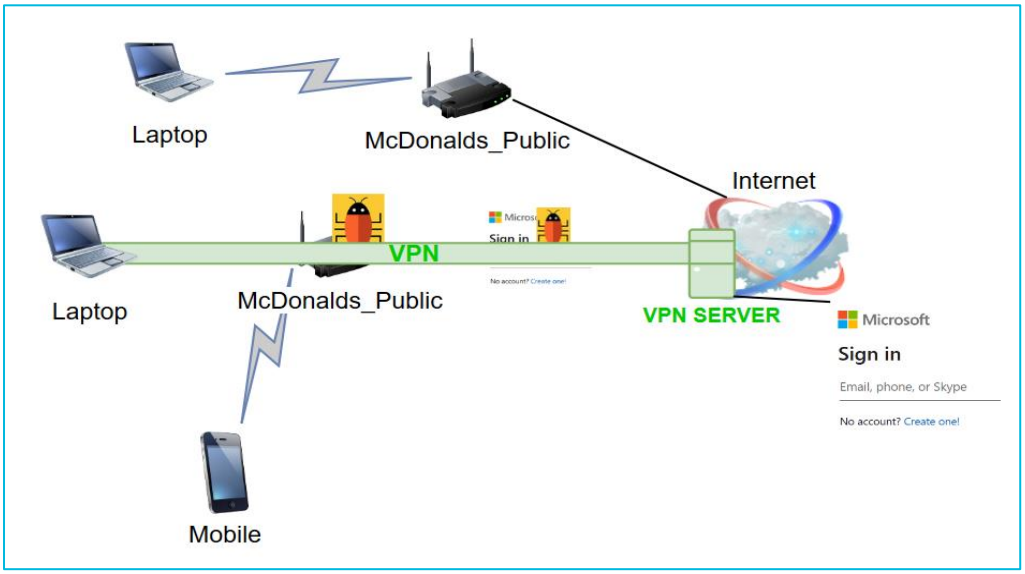
Pasitikrinkite ir nustatykite DNS:
1. IP adresą: https://www.nksc.lt/ip.html
2. Išsiaiškinkite ar jūsų DNS nustatymai tinkami: https://openresolver.com/ (reikės IP adreso, kurį patikrinote 1 žingsnyje)
3. Jei turite problemų, teks imtis kiek sudėtingesnių priemonių. Instrukcija ir šiek tiek daugiau informacijos anglų kalba čia: https://www.pcmag.com/how-to/how-and-why-to-change-your-dns-server

Dar viena santrumpa, kurią reikia žinoti – VPN!

Mėgstate dirbti kavinėse, o gal dažnai einate į svečius pas kitą organizaciją? Tikriausiai prisijungiate prie viešo WiFi tinklo – viešo interneto. Tačiau WiFi viešose vietose nėra saugus ir patikimas. Prie interneto nesijungiate tiesiogiai, šiame procese tarpininkauja įranga, kuri gali būti kenkėjiška ir perimti jūsų duomenis ar jūsų įrenginyje palikti užkratų.

Detaliau apie tai vaizdo įraše anglų kalba:
https://www.youtube.com/watch?v=SfFSxThtzhE&ab_channel=SimplyExplained

Kaip tai spręsti? Saugus būdas - naudoti VPN (virtual private entity). VPN šifruoja interneto srautą ir paslepia jūsų tapatybę internete.



Taip pat svarbu žinoti, kad laikyti savo mobiliojo telefono WiFi funkciją įjungtą, kai esate gatvėje ar kitoje viešose vietose, yra tas pats, kaip spausti ranką kiekvienam gatvėje sutiktam žmogui, t. y. mobiliojo telefono WiFi jungiasi su kiekvienu gatvėje esančiu interneto tiekėju. Įjungta WiFi funkcija leidžia sekti asmenį, t. y. gauti daugiau informacijos apie jį.

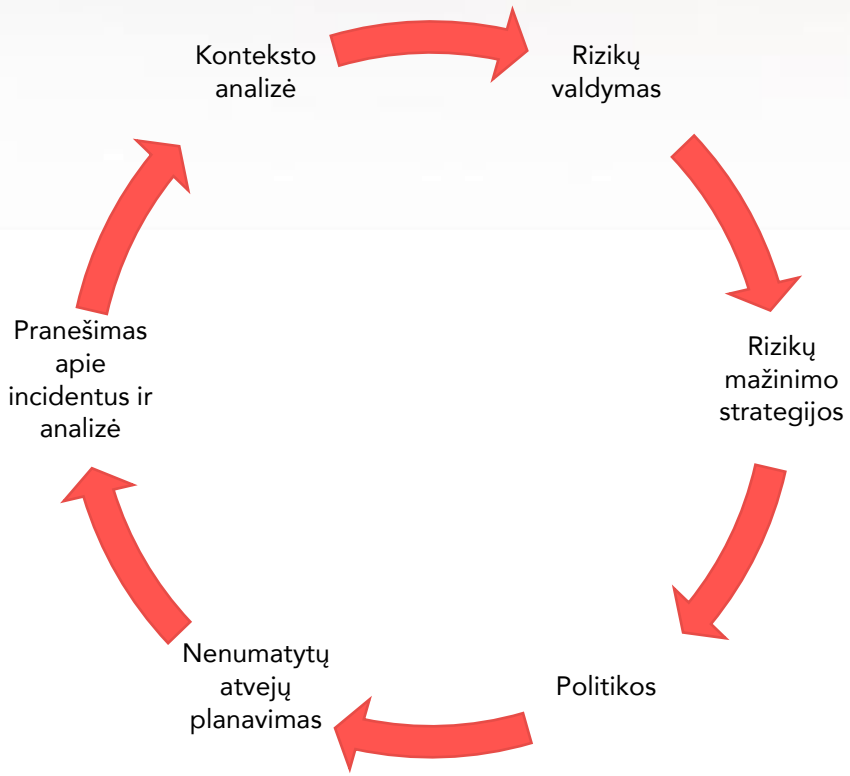
O čia daugiau patarimų organizacijoms savo WiFi nustatymams:
https://www.nksc.lt/doc/biuleteniai/2019-12-13__NKSC_Wi-fi_tinklo_apsauga.pdf

Šaltiniai, kur lietuvių kalba ieškoti praktinių patarimų, kaip užtikrinti elektroninį saugumą:
https://www.esaugumas.lt/
https://www.nksc.lt/rekomendacijos.html

Kaip suplanuoti savo organizacijos saugumą?

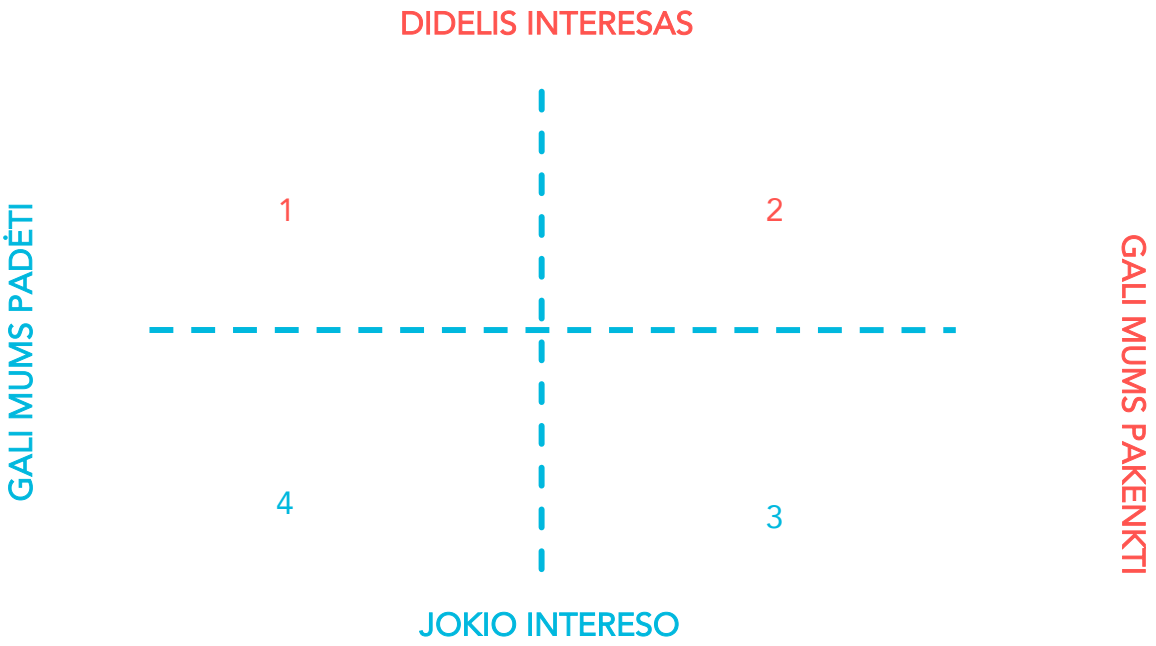
Organizacijos kibernetinio saugumo planavimas labai panašus į rizikų ir krizių valdymą ir apima:

1. Konteksto analizę (kas jūs, kas jums svarbu, kas jums kelia grėsmę ir gali padėti?)
2. Kokios rizikos kyla ir kaip jas valdyti?
3. Ką galima padaryti jau dabar, kad sumažintumėte rizikų tikimybę?
4. Konkrečios politikos – taisyklės, kuriomis vadovaujantis tvarkote duomenis, naudojate įrangą ir pan.
5. Suplanuojate kaip elgiatės, kai įvyksta nenumatytas atvejis,
6. Pasiruošiate šablonus pranešimams apie tokius atvejus savo organizacijoje ir su ja susijusiems asmenimis.
7. O tada viską pradedame vėl iš pradžių, nes saugumas – kelionė.



Pradedame nuo visiems puikiai pažįstamo pratimo: misijos, vizijos ir vertybių įsivardijimo. Kas jums svarbu? Kokie jūsų veikimo principai? Jei jau esate tai atlikę, tiesiog turėkite po ranka, nes būtent tai mums leidžia suprasti organizacijos saugumo poreikius.

Kas yra jūsų organizacijos suinteresuotieji? Ar jie gali padėti, ar pakenkti? Tai atlikti galite pasitelkdami žemiau pateiktą lentelę →



Ir, žinoma, kokios jūsų organizacijos stiprybės, silpnybės, grėsmės ir galimybės? Atrodo puikiai pažįstamas pratimas, bet be jo negalėsime pamatyti visų rizikų, tad nepraleiskite jo 😊

STIPRYBĖS	GALIMYBĖS
SILPNYBĖS	GRĖSMĖS

Rizikos planavimas ir apskaičiavimas (įvertinimas, kiek svarbu jai pasirengti). Pavyzdys, kuriuo galima vadovautis, bet kiekvienos organizacijos kelias ir planas bus vis kitoks!

Rizikos Nr.	**Rizikos aprašymas**	**Rizikos tipas** pagal *SSGG*	**Rizikos tipas** *Biuras/kelionės/ materialus ir nematerialus turtas/komunikacija/ žmogiškieji ištekliai/įsilaužimas*	**Tikimybė (1-5)**	**Poveikis (1-5)**	**Rizikos reitingas**	**Atsakas** *Pastangos sumažinti rizikas/ amortizuoti pasekmes arba didinti poveikio tikimybę*	**Tikimybė (1-5)**	**Poveikis (1-5)**	**Likusios rizikos įvertinimas**
R1	Įsilaužta į el paštą ir pavogta informacija	Grėsmė	Įsilaužimas	2	5	10	Stipresni slaptažodžiai; Reguliariai keisti slaptažodžius; Protonmail – pasikeitimu jautria informacija ar kitos užšifruojančios platformos...	3	4	2
R2	Stipri IT komanda	Stiprybė	Žmogiškieji ištekliai	5	3	20				
R3	Duomenų apie asmenis (politikus) nutekinimas	Grėsmė	Duomenų nutekinimas	2	5	10	Duomenys laikomi užšifruoti ir su slaptažodžiu; Keletas apsaugos lygių; Platformos reguliarus atnaujinimas;	2	2	6
R4	Motyvuoti darbuotojai ir savanoriai	Galimybė	Žmogiškieji ištekliai	3	5	15	Darbuotojai mokomi saugiai elgtis skaitmeninėje aplinkoje; Parengti kibernetinio saugumo planą ir jį integruoti į elgesio kodeksą; Reguliariai pakartoti kibernetinio saugumo principus integruoti ir aptarti, patikrinti ar laikomasi saugumo taisyklių	4	4	1