KIBERNETINIO SAUGUMO RIZIKŲ VALDYMAS

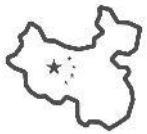
NKSC prie KAM

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

KIBERNETINIO SAUGUMO RIZIKŲ TENDENCIJOS

Pagrindiniai vektoriai iš kur kyla atakos – „Didysis 4”

Rusija – pagrinde matomas DDoS modelis, ypač nukreiptas į kaimynines valstybes, valstybes remiančias Ukrainą.

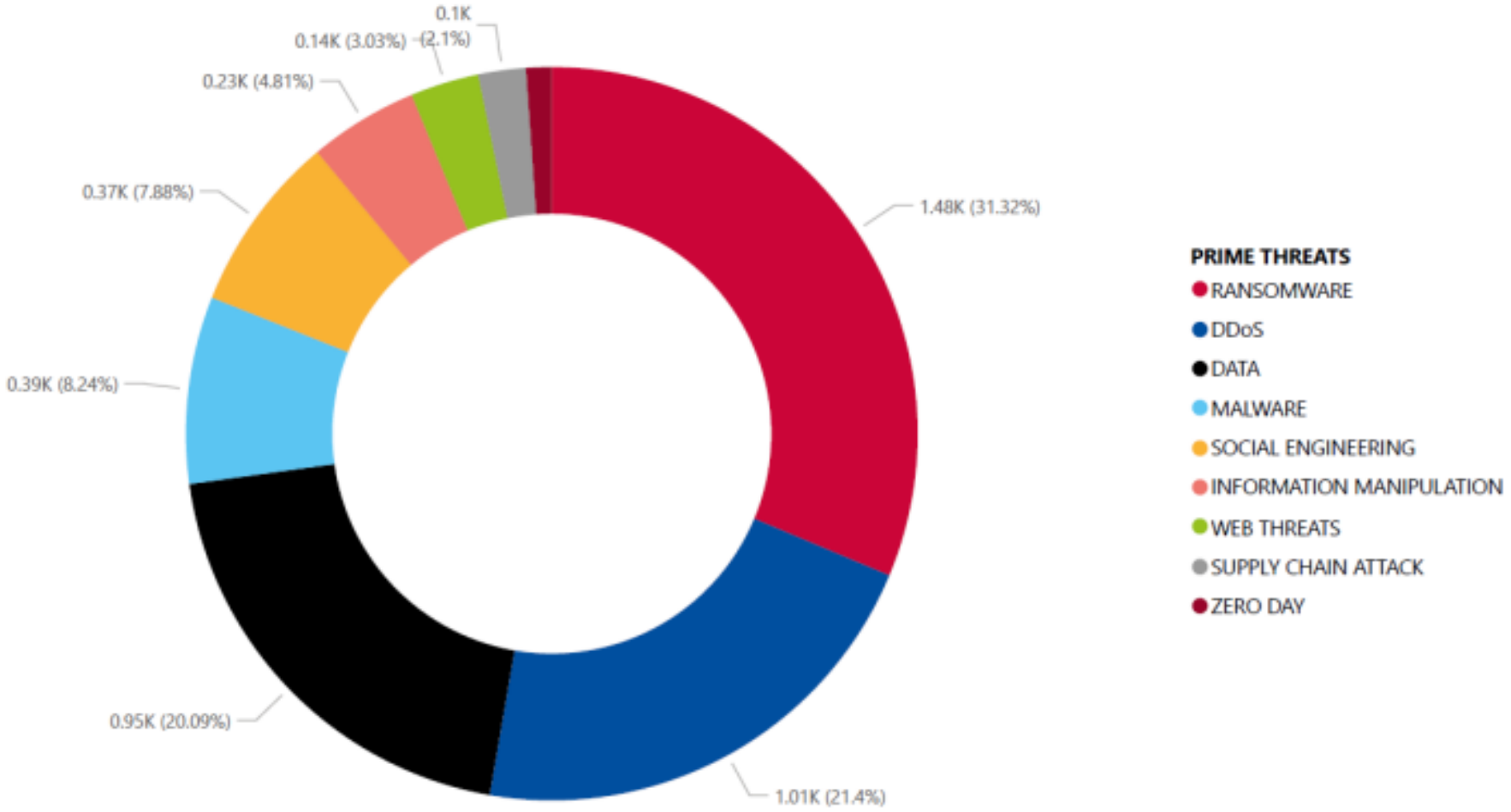


Kinija – kompleksiškos kibernetinės atakos, dažniausiai infiltruojantis į aukos sistemas ir išlaikant buvimą jose ilgą laiką iki tinkamo momento. Pagrindinės aukos – šalys kaimynės, Okeanijos regionas, Taivanas.

***Š. Korėja** – grupuotės, motyvuotos finansine nauda, karinių paslapčių vogimu.*

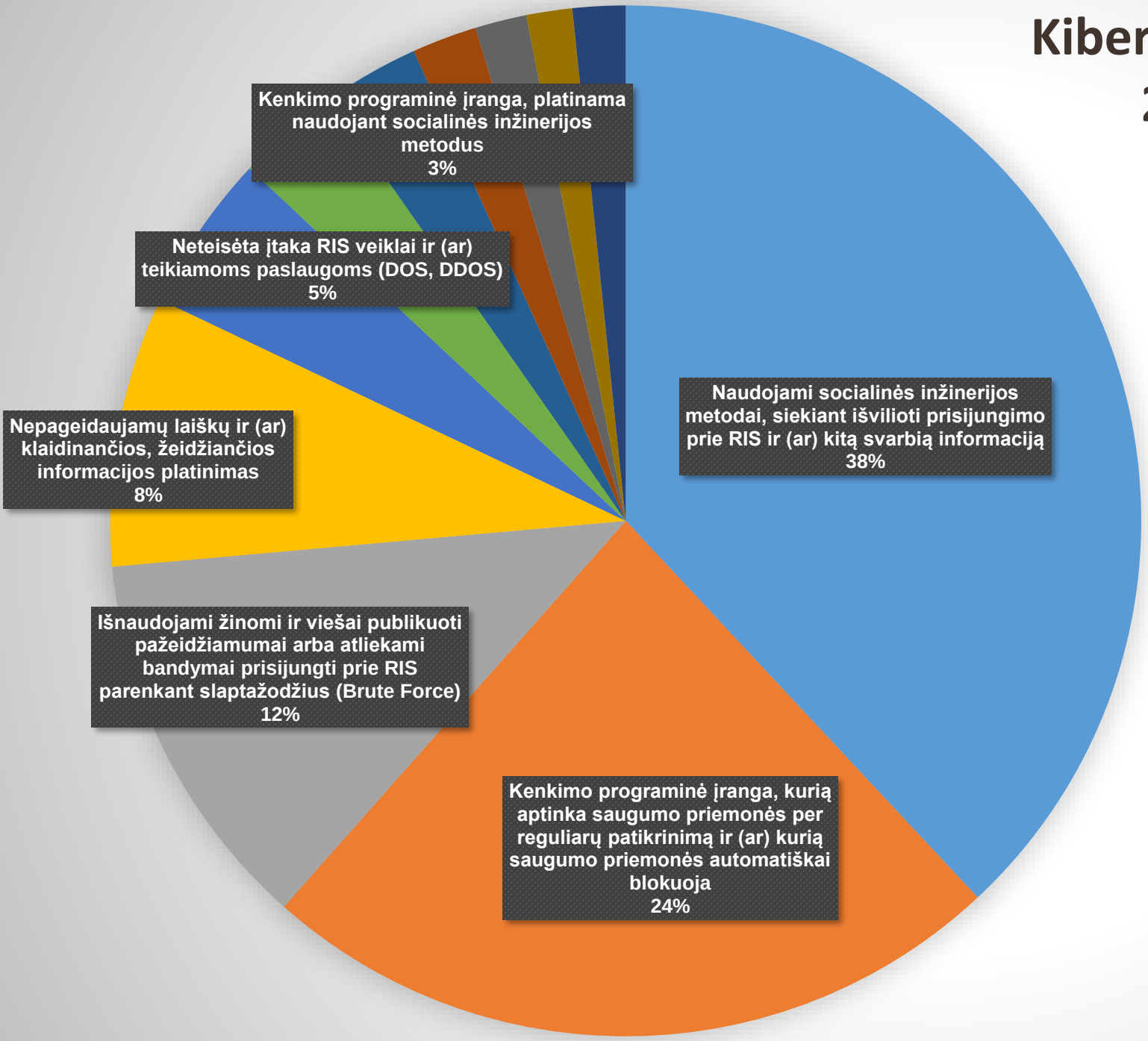
***Iranas** – užpuolikai žinomi dėl savo atkaklios ir tobulėjančios taktikos, nukreiptos prieš įvairias pramonės šakas ir valstybes. Grupės vykdo strategines kibernetines operacijas, siekdamos politinių, karinių ir ideologinių tikslų.*

ENISA incidentų pobūdis 2023



Šaltinis: ENISA Threat Landscape 2023

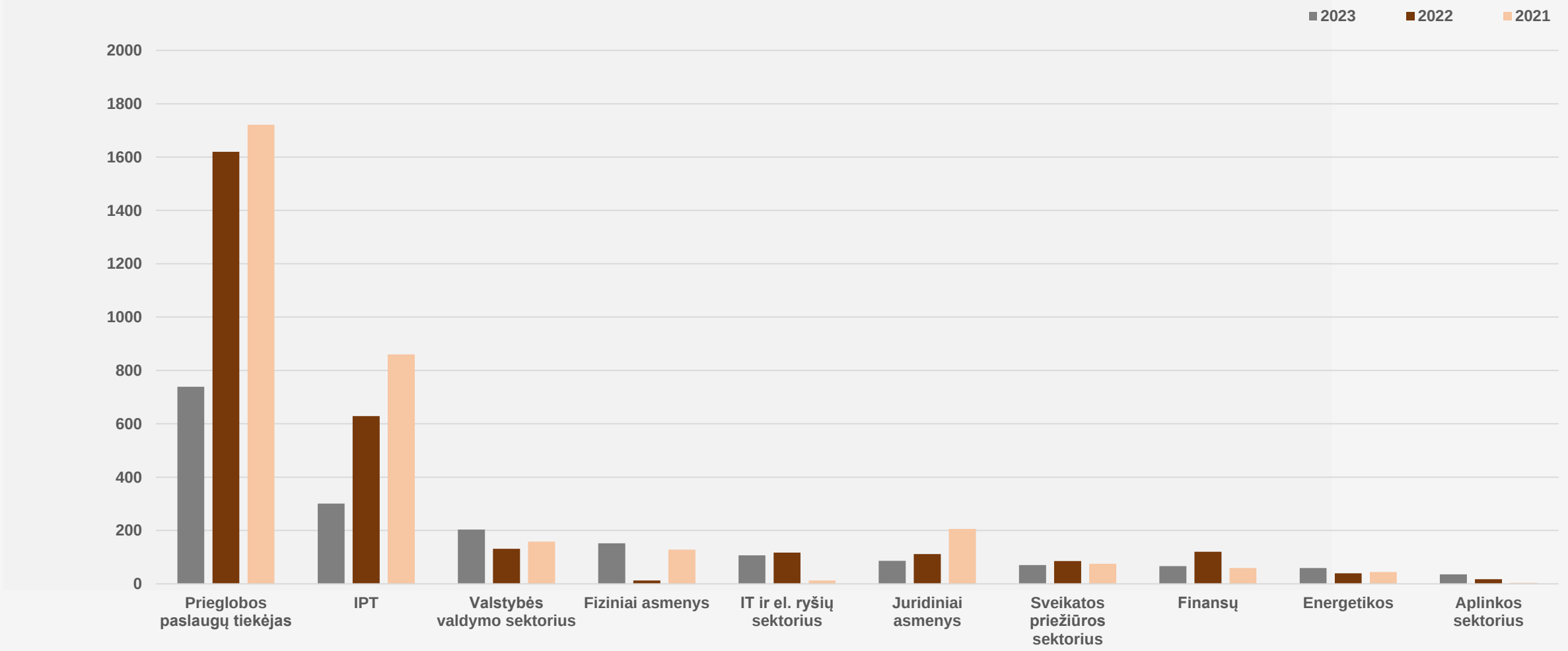
Kibernetinių incidentų pobūdis 2023 metais Lietuvoje



- Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją
- Kenkimo programinė įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja
- Išnaudojami žinomi ir viešai publikuoti pažeidžiamumai arba atliekami bandymai prisijungti prie RIS parenkant slaptažodžius
- Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas
- Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms
- Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus
- Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas
- Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui
- Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui
- Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)
- Incidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų

Šaltinis: NKSC duomenys

Kibernetiniai incidentai pagal sektorius 2021 - 2023



Šaltinis: NKSC duomenys

Kibernetinių grėsmių kryptys

Išpirkos motyvuotos atakos (angl. ransomware)

Tiekimo grandinės atakos (angl. supply chain attacks)

ChatGPT / Genaratyvusis dirbtinis intelektas

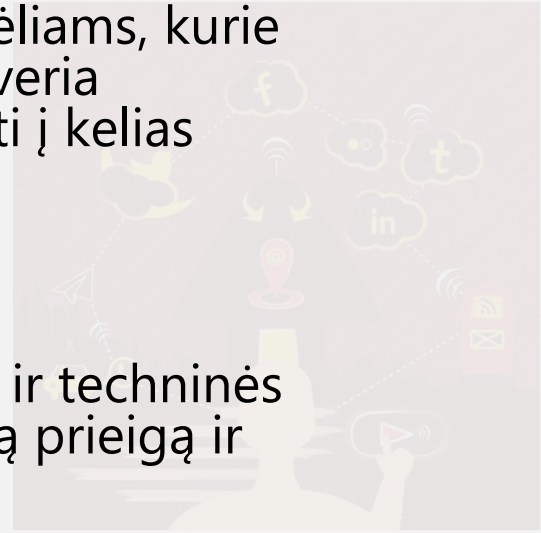
DDoS atakos

Šaltinis: ENISA Threat Landscape 2023 - Prime threats

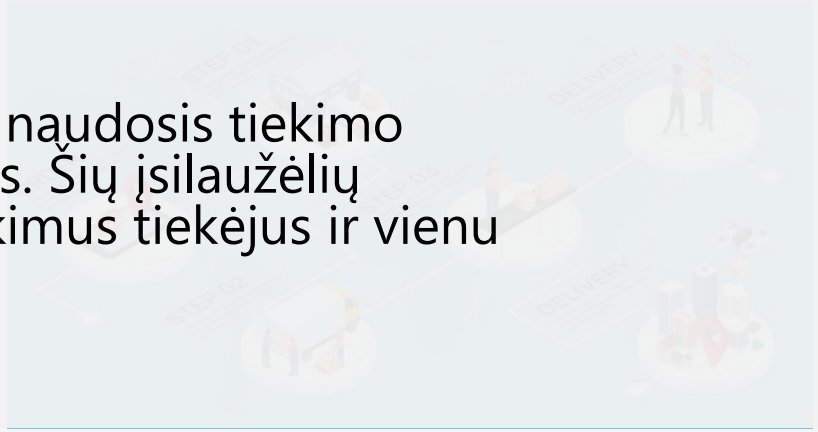
Tiekimo grandinės atakos (angl. Supply chain attacks)

Atakų pagausėjimas
Tikimasi, kad tiekimo grandinės atakos ateityje daugės, nes nusikaltėliams, kurie taikosi į pardavėjus, rangovus ir trečiųjų šalių paslaugų teikėjus, atsiveria platesnis atakos laukas, nes per vieną pažeidimo tašką jie gali patekti į kelias organizacijas.

Programinės įrangos pažeidžiamumų išnaudojimas
Užpuolikai pasinaudos tiekimo grandinėse naudojamų programinės ir techninės įrangos komponentų pažeidžiamumais, taip siekdami gauti neteisėtą prieigą ir vykdyti kenkėjišką veiką.



Valstybės remiami įsilaužėliai
Tikėtina, kad valstybės remiami grėsmių aktoriai ir toliau naudosis tiekimo grandinės pažeidžiamumu šnipinėjimo ir sabotažo tikslais. Šių įsilaužėlių pažangumas ir ištekliai leidžia jiems kompromituoti patikimus tiekėjus ir vienu metu paveikti kelis taikinius.

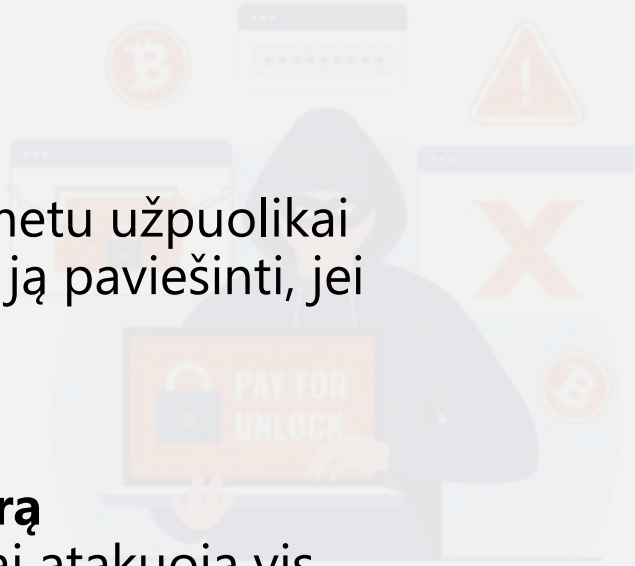


Išpirkos reikalaujančios atakos (angl. Ransomware)

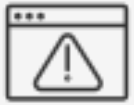
Daugėja "RaaS" (Ransomware-as-a-Service) naudojimo atvejų
Naudodamiesi RaaS modeliu nusikaltėliai gali išsinuomoti išpirkos reikalaujančią programinę įrangą, kad galėtų atakuoti kitas įmones.

Padaugėjo dvigubos išpirkos atvejų
Dvigubu išpirkos reikalaujančios programinės įrangos išpuolio metu užpuolikai užšifruoja aukos duomenis ir kartu pavagia jų kopiją bei grasina ją paviešinti, jei nebus sumokėta išpirka.

Daugėja tikslinių atakų prieš ypatingos svarbos infrastruktūrą
Išpirkos reikalaujančią programinę įrangą naudojantys užpuolikai atakuoja vis daugiau ypatingos svarbos infrastruktūros objektų, įskaitant ligonines, elektros tinklus ir transporto sistemas. Kadangi šios organizacijos negali sau leisti, kad jų sistemos būtų išjungtos, neatmestina, kad jos dažniau moka išpirką.



ChatGPT / dirbtinis intelektas



Automatinės atakos
Piktavaliai gali pasitelkti dirbtinio intelekto įrankius, kad automatizuotų įvairius kibernetinių atakų etapus, įskaitant žvalgybą, pažeidžiamumo išnaudojimą ir net sprendimų priėmimą atakų metu, ir taip pasiekti, kad atakos būtų veiksmingesnės.

Kenkėjiškų programų kūrimas ir vengimas
Dirbtinio intelekto algoritmai gali būti naudojami polimorfinėms kenkėjiškoms programoms, kurios keičia savo kodą, kad išvengtų tradicinių parašais pagrįstų aptikimo metodų, todėl kenkėjiškų programų aptikimas tampa sudėtingesnis.

Grėsmių žvalgyba ir analizė
Dirbtinio intelekto įrankiai gali pagreitinti ir padėti tiksliau kaupti, analizuoti ir koreliuoti didžiulius grėsmių žvalgybos duomenų kiekius, padėdami organizacijoms užkirsti kelią kylančioms grėsmėms.

DDOS atakos

Didesnės ir sudėtingesnės atakos
Tikėtina, kad užpuolikai rengs didesnes ir sudėtingesnes DDoS atakas, naudodami botnetus, sudarytus iš užkrėstų įrenginių, įskaitant daiktų interneto įrenginius, kad generuotų didžiulius duomenų srautus.

5G ir daiktų interneto poveikis
Vis labiau plintant 5G tinklams ir daiktų interneto įrenginiams, įsilaužėliai gali pasinaudoti padidėjusiu duomenų srauto pralaidumu ir dideliu prijungtų įrenginių skaičiumi, kad įvykdytų didesnio masto atakas.

Nedidelės ir lėtos atakos
Užpuolikai gali pereiti prie nedidelių ir lėtų atakų, kurios nepastebimos tradicinių DDoS aptikimo mechanizmų, todėl jas sunkiau identifikuoti ir sušvelninti.

ATITIKTIS KIBERNETINIO SAUGUMO REIKALAVIMAMS – BAZINIS RIZIKŲ VALDYMAS

Kas yra kibernetinio saugumo atitiktis

Atitiktis kibernetinio saugumo standartams reiškia tam tikrų agentūrų, įstatymų ar valdžios institucijų nustatytų standartų ir reguliavimo reikalavimų laikymąsi

Organizacijos privalo laikytis reikalavimų nustatydamos rizika pagrįstas kontrolės priemones, kurios apsaugotų informacijos konfidencialumą, vientisumą ir prieinamumą (KVP). Informacija turi būti apsaugota, nesvarbu, ar ji tvarkoma, integruota ar perduodama.

Organizacijos, dirbančios su informacinėmis sistemomis ir teikiančios viešai prieinamą bei naudojamą informaciją neišvengiamai susiduria kibernetine sauga

Prieiga prie duomenų ir dalinimasis jais daro organizacijas pažeidžiamas galimoms kibernetinėms atakoms

Atitiktis nėra tik varnelės užsidėjimas,

tai yra būdas apsaugoti jūsų organizaciją nuo kibernetinių atakų:

tokių kaip DDoS atakos, sukčiavimas, kenkėjiškos programos, išpirkos reikalaujančios programos ir kt.

Kodėl reikalinga atitikti kibernetinio saugumo reikalavimus

Kibernetinio saugumo standartų ir taisyklių laikymasis yra lemiamas veiksnys įgalinant organizacijas taikyti saugumo praktikas ir sklandžiai veikti

Kibernetinio saugumo standartų laikymasis yra prevencinė ir efektyvi priemonė, leidžianti minimizuoti kibernetinio saugumo rizikas ir apsisaugoti nuo daugumos nesudėtingų kibernetinių atakų

Techniniai sistemų pažeidimai gali tapti veiklos sustabdymo priežastimi, todėl iškart pakenks organizacijos reputacijai, teisinei, finansinei būklei ir veiklos tęstinumui

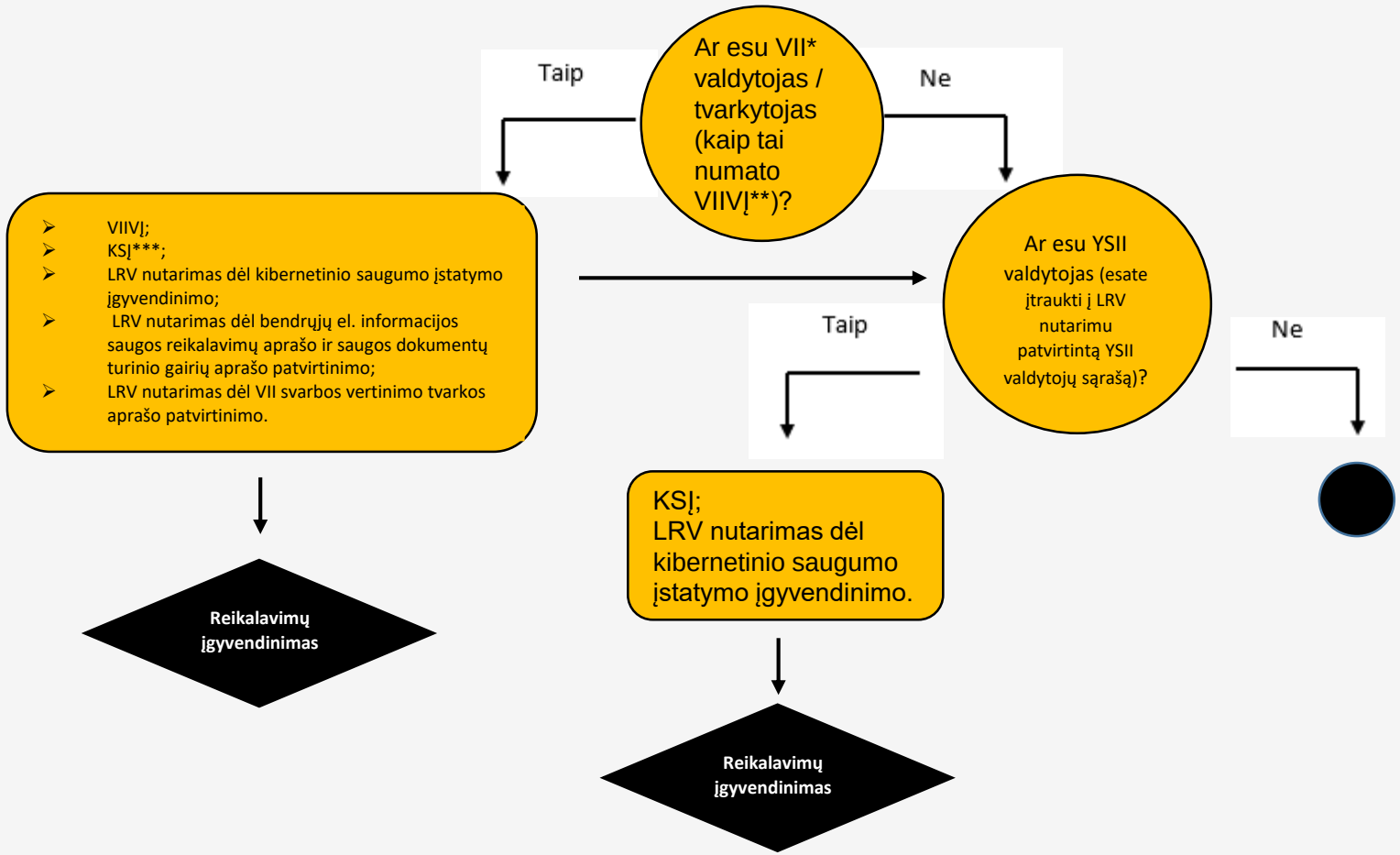
Įsilaužėliams - lengviau išnaudoti žinomus pažeidžiamumus ir vykdyti kibernetines atakas, jei nesilaikoma geriausių saugumo praktikų

Atitiktis OTR – organizaciniams techniniams reikalavimams ir kitiems TA

YSII ir VII atitiktis

- LRV nutarimas „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“
- LRV nutarimas Nr. 716 „Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir saugos dokumentų turinio gairių aprašo patvirtinimo”.
- Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymas
- LRV nutarimas „Dėl VII svarbos vertinimo tvarkos aprašo patvirtinimo“

YSII atitiktis



Šaltinis: * VII - Valstybės informaciniai ištekliai; ** VIIVĮ - Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatymas, XI-1807 Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (lrs.lt)
*** KSĮ – Lietuvos Respublikos kibernetinio saugumo įstatymas, XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas (lrs.lt)

KAIP VALDYTI RIZIKAS – PRAKTINIAI PATARIMAI

Informacija yra turtas

Asmenį identifikuojanti informacija:

- Gimimo data
- Vardai/pavardės
- Adresas
- Socialinio draudimo numeris

Kita įvairių tipų neskelbtina informacija:

- Rasė
- Religija
- Šeimyninė padėtis
- IP adresai
- Pašto adresai, vartotojo vardai ir slaptažodžiai
- Biometriniai duomenys (pirštų atspaudai, veido atpažinimas ir balso atspaudai)

Saugoma sveikatos informacija:

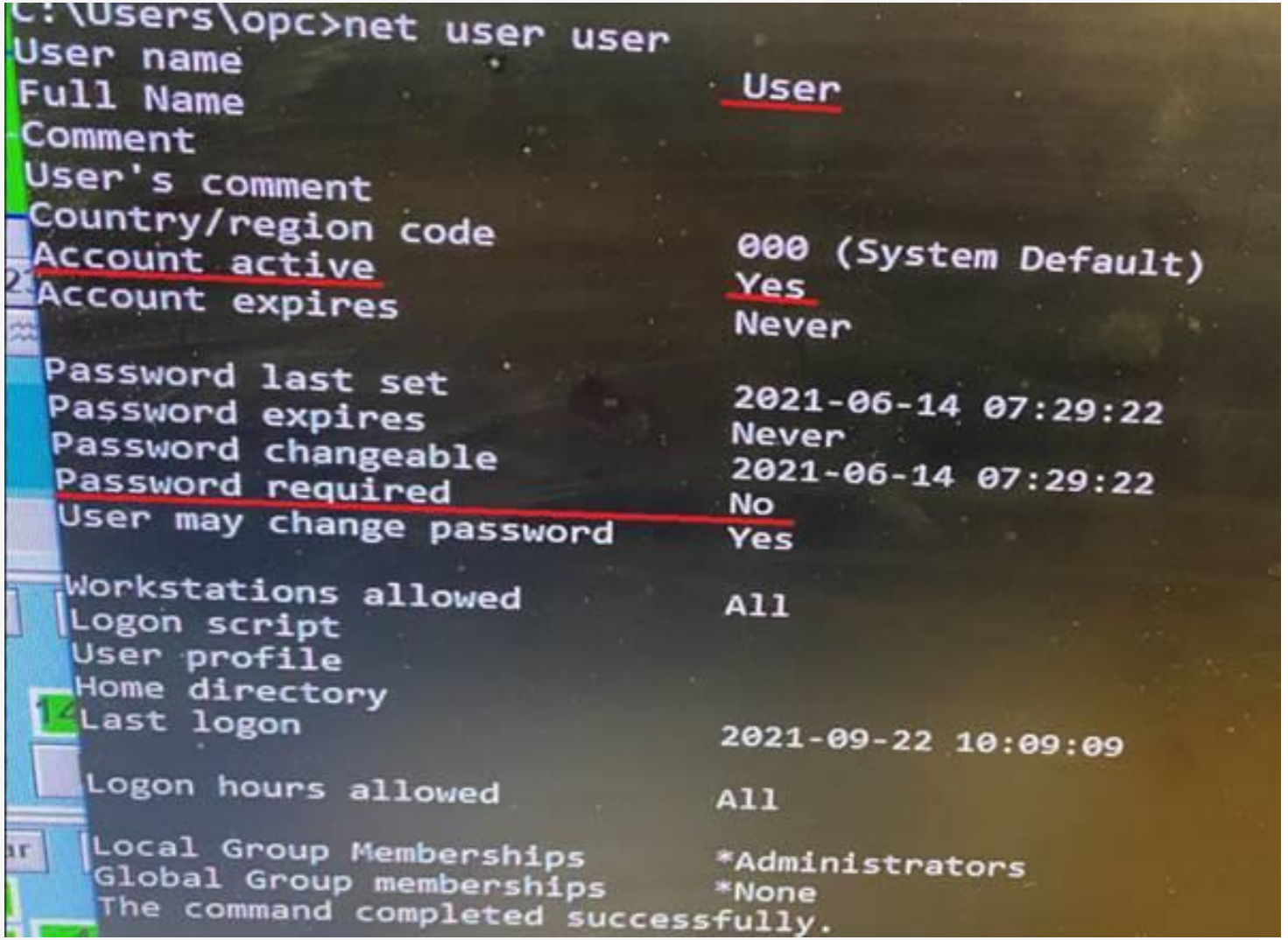
- Medicinos istorija
- Draudimo įrašai
- Paslaugų paskyrimų istorija
- Receptų įrašai
- Priėmimo į ligoninę įrašai

Finansinė informacija:

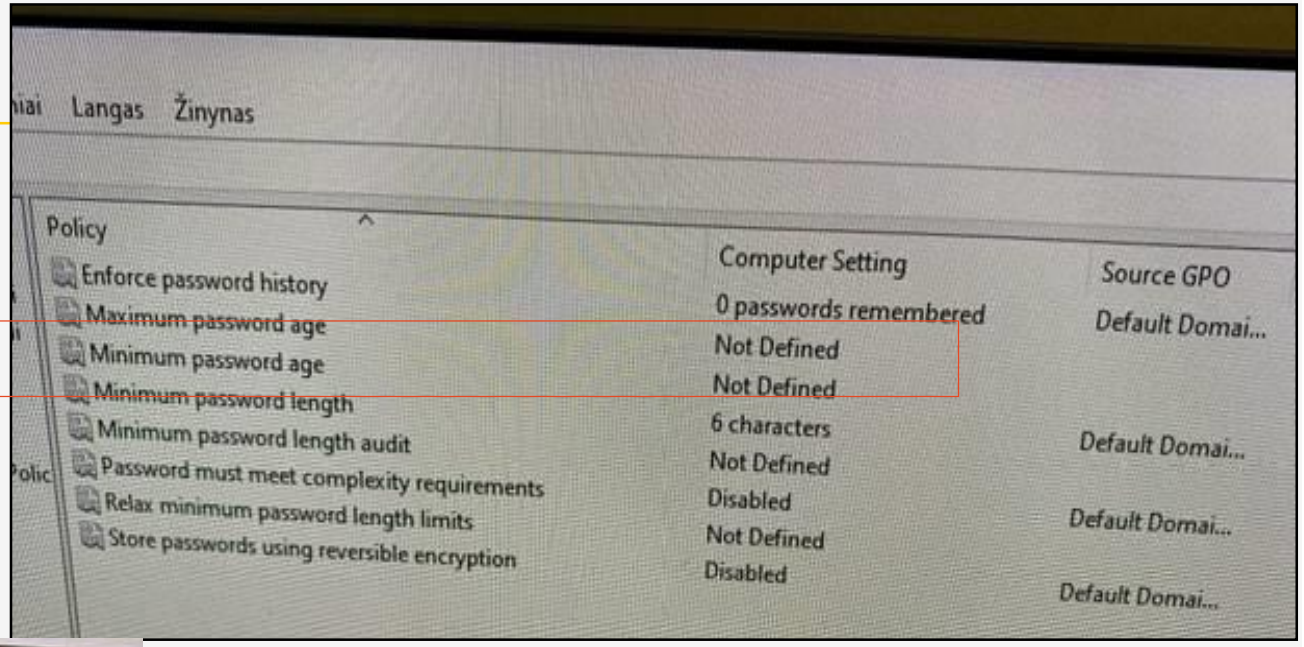
- Kredito kortelių numeriai, galiojimo datos ir kortelės patvirtinimo vertės (CVV)
- Banko sąskaitos informacija
- Debeto arba kredito kortelių asmens identifikavimo numeriai (PIN)
- Kredito istorija arba kredito reitingai

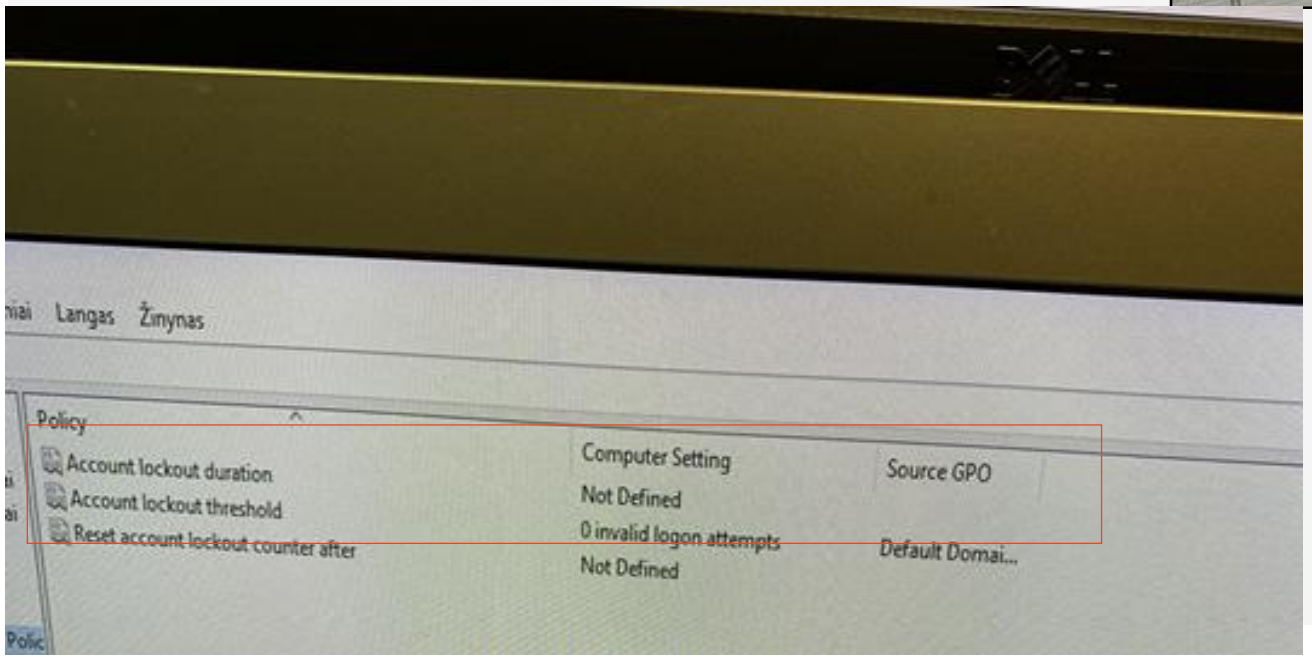
Ką reiškia atitiktis praktiškai – vartotojo paskyros valdymas

- Paskyros savininkas turi būti aiškiai identifikuojamas
- Paskyra privalo turėti galiojimą datą
- Privalome prie paskyros prisijungti naudojant slaptažodį



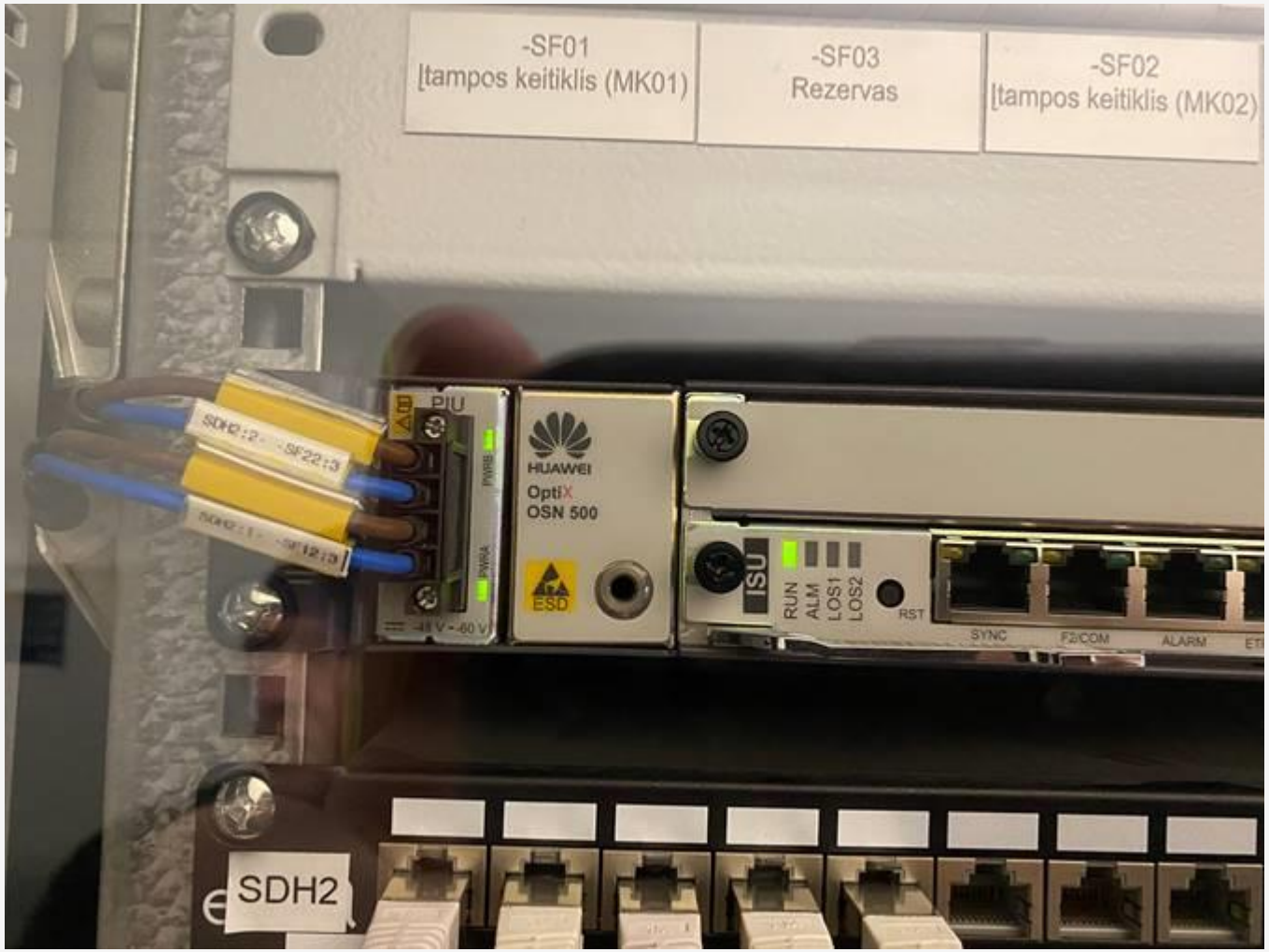
Ydinga slaptažodžių valdymo politika





Atitiktis VPĮ

Iki 2025 sausio 1 d. privaloma atsisakyti savo infrastruktūroje naudoti techninę, programinę įrangą iš nedraugiškų šalių



Atitikties gerosios praktikos - incidentų valdymo priemonės

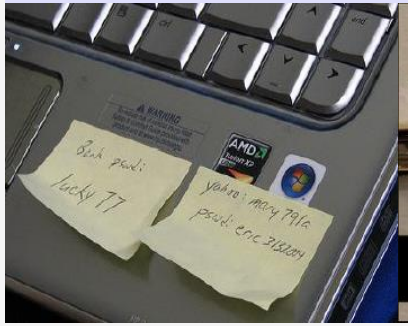
- **Administracinės:** efektyvi ir veikianti kibernetinio saugumo politika, procesai ir procedūros pagal Kibernetinio saugumo įstatymo reikalavimus – privaloma visiems organizacijos darbuotojams

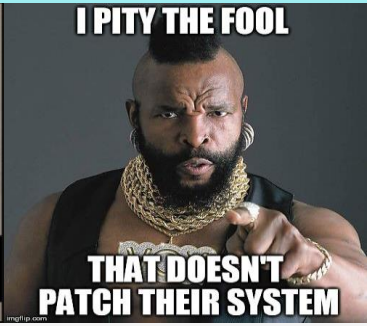
- **Operacinės/techninės:** techninės priemonės, apimančios: naudotojų/paslaugos teikėjų prisijungimus autentifikuojantis keliais faktoriais, užtikrinant informacijos šifravimą, laiku identifikuojant anomalijas ir kibernetinius incidentus (pvz., SIEM)

- **Fizinės:** rakinamos durys, serverinės, kabinetai, tikrinami darbuotojai

Kritinis mąstymas padeda valdyti rizikas – atitiktis įgyvendinama ne tik „ant popieriaus“

- Sudėtingų slaptažodžių naudojimas ir jų periodiškas keitimas;
- Niekada niekam neduokite savo slaptažodžių (administratoriai niekada to jūsų neklaus, nes jie turi aukštesnio lygmens teises);
- Neteikite perteklinės asmeninės informacijos internete ar socialiniuose tinkluose;
- Jei kolega staiga atsiuntė netikėtą prašymą ar prašo veiksmų, kurie gali būti lemtingi (pvz.: pervesti pinigų) – pasitikslinkite paklausdami jį telefonu;
- Atsiminkite, kad išmanieji telefonai – maži kompiuteriai, jie „paveldi“ visas kompiuterių kibernetines grėsmes
- Naudotojai visada turėtų būti atsargūs ir truputį paranojiški (bet kuris gautas laiškas, dokumentas ar nuoroda gali būti kenksmingas);
- Svarbių duomenų ir dokumentų kopijos turi būti saugomos atskirai nuo sistemos;





Kas organizacijoje atsakingas už kibernetinį saugumą?

- **Įstaigos vadovas:** užduočių ir resursų skyrimas, atskaitomybės reikalavimas iš pavaldžių asmenų (pagal KSĮ neša administracinę atsakomybę)
- **IT specialistai:** saugių prieigų valdymas, tinklo segmentavimas, atnaujinimų diegimas, veiklos tęstinumo užtikrinimas
- **Informacijos bei kibernetinio saugumo specialistai:** rizikos vertinimas, darbuotojų mokymai, pažeidžiamumų paieška, anomalijų sistemose stebėjimas, vadovybės informavimas apie problemas/kibernetinio saugumo rezultatus
- **Darbuotojai:** informavimas apie kibernetinius incidentus, informacijos bei kibernetinio saugumo reikalavimų laikymasis

NKSC VAIDMUO

Kuo gali padėti NKSC?

NKSC dalinasi – teikia konsultacijas OTR klausimais**,** specialistai ruošia rekomendacijas, dažniausiai skirtas paprastiems naudotojams, kaip galima pagerinti savo kibernetinį atsparumą ir padidinti budrumą

Organizuoja - vadovų, IT administratorių ir kitų specialistų edukacija ir mokymai

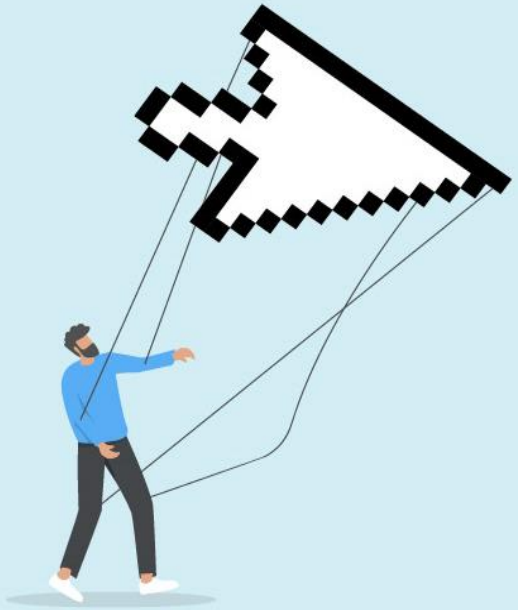
Rengia pratybas – pvz. „Kibernetinis Skydas“ (Stratex, Opex, PhishEx)

Teikia įrankius - skirtus tikrinti svetainių pažeidžiamumą, apsaugoti įrenginį nuo kenkėjiško turinio, pasitikrinti dėl saugumo spragų

DNS užkarda
Apsaugoti savo įrenginį nuo kenkėjiško turinio

CYBER SHIELD
OpEx 2023

Kaip apsisaugoti nuo kibernetinių nusikaltėlių



Nekalbėkite su nepažįstamaisiais.

Prisiminkite, ką išmokote dar vaikystėje. Venkite kalbėtis ir dalintis informacija su kažkuo, ko nepažįstate realiame gyvenime.

Būkite atsargūs sulaukę netikėto prašymo.

Nesidalinkite jokiais savo duomenimis ir atsiminkite – jūsų bankas ar kitas paslaugų teikėjas žinutėmis niekada neprašys jūsų slaptažodžių.

Gyvenime nieko nėra nemokamo.

Nemokamas sūris – tik pelėkautuose. Tas pats galioja ir internete. Neapsigaukite sulaukę pasiūlymo, kuris per geras, kad būtų tiesa.

Būkite budrūs, kai prašoma imtis veiksmų greitai.

Nepasiduokite spaudimui veikti „čia ir dabar“. Giliai įkvėpkite ir pagalvokite prieš imantis bet kokių veiksmų.

Saugokite savo duomenis.

Slaptažodžiai, kredito kortelių numeriai, asmens tapatybės duomenys – labai vertingi. Vertinkite juos kaip savo turtą.

Pagalvokite prieš paspausdami.

Prieš spustelėdami nuorodą įvertinkite jos autentiškumą. Užvedus pelytės kursorių ant nuorodos reikėtų patikrinti, kur iš tikrųjų nuoroda veda.

Geriau būti atsargiems, nei vėliau gailėtis.

Visada naudokite skirtingus ir stiprius slaptažodžius. Savo paskyrose įgalinkite dviejų arba kelių veiksnių prisijungimo autentifikavimą.

Apsunkinkite nusikaltėlių gyvenimą.

Nuolat tikrinkite galimus savo įrenginių atnaujinimus, turėkite atsargines svarbios informacijos kopijas, nenaudokite darbinio elektroninio pašto adreso asmeniniams reikalams.

Be smarter than a hacker

EUROPEAN CYBER SECURITY MONTH

KRAŠTO APSAUGOS MINISTERIJA

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

DĖKOJU UŽ DĖMESĮ

www.nksc.lt

info@nksc.lt