Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų supratimo ir suvaldymo apžvalga

Kibernetinių atakų valdymas

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Mokymosi tikslai

Paaiškinti ir suprasti būdus, kaip suvaldyti kibernetines atakas.

Suprasti, kaip išvengti kibernetinių atakų arba sumažinti žalą.

Studento darbo krūvis

Paskaita	5 h
Garso ir vaizdo medžiaga	2 h
Panaudojimo atvejai	2 h
Papildomi skaitiniai	4 h
Pasiruošimas atsiskaitymui	2 h

Turinys


2
Kibernetinių atakų stabdymo technikos
1
Kaip išvengti kibernetinių atakų
Kibernetinių atakų suvaldymas
3
Saugumo pažeidimo įvertinimas
4
Tolesnių veiksmų žingsniai

Kibernetinių atakų vengimas

- Veiksmingiausias būdas kovoti su kibernetinėmis atakomis - naudoti tinkamas prevencines priemones.
- *Nėra sėkmingos atakos - nėra nuostolių*.

- Norint išvengti atakos arba ją sušvelninti, reikia išsiugdyti tam tikrus įpročius, kurie dažnai vadinami **saugumo higiena** arba **kibernetine higiena**.

- Jei jūs ir jūsų darbuotojai laikysis saugumo higienos, **tikimybė** tapti kibernetinės atakos auka gali sumažėti **bent 90 procentų** !

Funded by the Erasmus+ Programme of the European Union

Sąmoningumo ugdymas

- Pirmasis ir vienas svarbiausių patarimų, kaip kovoti su kibernetinėmis atakomis, yra **sąmoningumo ugdymas**.
- Tai užtikrins, kad visi darbuotojai pagal savo pareigas arba piliečiai gebėtų atremti kibernetinį incidentą.

- Mokymas taip pat yra viena iš pagrindinių rizikos mažinimo priemonių.
- *Tai negali užtikrinti 100 proc. saugumo, tačiau gali sumažinti riziką.*

Funded by the Erasmus+ Programme of the European Union

Geriausia praktika siekiant išvengti kibernetinių atakų

1. Politika nukreipta „Iš viršaus į apačią“, skirta saugumo padėties gerinimui.

Geriausia praktika visada turi būti paremta tinkama politika. Tai reiškia, kad kibernetinis saugumas turėtų būti neatsiejama įmonės valdymo dalis.

2. Kibernetinio saugumo komandų praktika turi būti nukreipta „Iš apačios į viršų“.

Remiantis gerai parengta politika, galima taikyti tam tikrą praktiką, kuri padėtų užkirsti kelią kibernetinėms atakoms, jas apriboti ar sušvelninti.

3. Imtis prevencinių priemonių pažangių kibernetinių grėsmių aptikimui ir atsakui į jas.

Bene svarbiausia geroji praktika - laikytis prevencinio požiūrio į kibernetinį saugumą.

Funded by the Erasmus+ Programme of the European Union

Veiksmai, kaip elgtis galimos atakos atveju

1 žingsnis: žinoti dažniausias kibernetinės grėsmes;

2 žingsnis: pereiti į kibernetinio saugumo veiksmų režimą;

3 žingsnis: įvertinti rizikos poveikį;

4 žingsnis: sukurti apsaugos ir aptikimo priemones;

5 žingsnis: parengti nenumatytų atvejų veiksmų planą;

6 žingsnis: atstatymas.

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

1. Apmokyti savo darbuotojus.

- Vienas veiksmingiausių būdų kovoti su kibernetinėmis atakomis ir visų rūšių duomenų saugumo pažeidimais - apmokyti savo darbuotojus;

- Siekiant išvengti sukčiavimo, jie turi:
  - *patikrinti nuorodas prieš paspausdami jas;*
  - *patikrinti gauto el. pašto adresą;*
  - *Vadovautis sveiku protu prieš išsiunčiant jautrią informaciją. Prieš vykdant "prašymą", geriau paskambinti tam asmeniui telefonu ir pasitikrinti.*

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

2. Pilnai atnaujinti savo programinę įrangą ir sistemas.

- dažnai įsilaužėliai išnaudoja programinės įrangos spragas, žinomas įsilaužėlių bendruomenei;

- protinga investuoti į pataisymų valdymo sistemą (Patch Management System);

- pataisymų valdymas (Leaf Offer Patch Management) yra jo saugumo sprendimo valdymo dalis.

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

3. Užtikrinti galutinio kompiuterio apsaugą.

- *Galutinio taško apsauga apsaugo tinklus, kurie nuotoliniu būdu sujungia įrenginius. Mobilieji įrenginiai, planšetiniai ir nešiojamieji kompiuteriai, kurie yra prijungti prie įmonės tinklų, suteikia galimybę platinti grėsmes.*

4. Įdiegti ugniasienę.

- tinklo užkardymas ugniasiene yra vienas veiksmingiausių būdų apsisaugoti nuo bet kokios kibernetinės atakos.

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

5. Daryti atsargines duomenų kopijas.

- *įvykus nelaimei (kurią gali sukelti kibernetinė ataka), privalote turėti savo duomenų kopiją.*

6. Kontroliuoti prieigą prie savo sistemų.

- *atakos gali būti ir fizinės.*
- *svarbu kontroliuoti, kas gali prisijungti prie jūsų tinklo.*

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

7. Wi-Fi saugumas.

- *Nepamirškite įvesti slaptažodžio kiekvienam naudojamam "Wi-Fi" ryšiui.*

8. Asmeninės darbuotojų paskyros.

- *kiekvienas darbuotojas turi naudoti asmeninę paskyrą;*
- *turi būti uždrausta dalytis paskyromis.*

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų vengimas

Siekiant išvengti kibernetinės atakos, primygtinai rekomenduojama atlikti sekančius veiksmus:

9. Prieigos valdymas.

- darbuotojams turi būti įdiegta tik autorizuota programinė įranga;

- neautorizuota programinė įranga turi būti uždrausta naudoti.

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų vengimas

Patarimai, kaip padidinti savo saugumą:

1. Sumažinti duomenų perdavimą ir nereikalingą komunikaciją;

2. Sekti kibernetinio saugumo situaciją;

3. Tirti duomenų nutekinimą;

4. Parengti ir įgyvendinti reagavimo į incidentus planą.

Nelengva visų jų laikytis kiekvieną dieną, tačiau reikia apie juos galvoti.

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų vengimas

Jei laikysitės šių rekomendacijų, gerokai sumažinsite kibernetinių atakų riziką.

Tačiau nepamirškite, kad:

- *gali būti sunku sužinoti, kur yra silpniausios vietos.*
- *yra daug informacijos, kuri kartais net prieštarauja viena kitai.*
- *reikalingas tik jums pritaikytas sprendimas.*

Funded by the
Erasmus+ Programme
of the European Union

Saugus naršymas internete

- *Naršydami internete galite prisirinkti šnipinėjimo programų, atsisiųsti kenkėjiškų programų ar net apsilankyti sukčių svetainėse.*
- *Dažnai galite net neįtarti, kad darote kažką nesaugaus.*
- *Tai nereiškia, kad turite bijoti kiekvieną kartą spustelėdami bet kokią nuorodą.*
- *Kai kurios paprastos atsargumo priemonės gali padėti jums būti gerokai saugesniems naršant*.

Co-funded by the Erasmus+ Programme of the European Union

Saugus naršymas internete

- **Apsaugokite kompiuterį nuo kenkėjiškų svetainių:** kiekviena naršyklė turi saugumo funkcijas, kurios apsaugo jus nuo apsilankymo kenkėjiškose svetainėse. Įjunkite šias funkcijas!

- **Nuolat atnaujinkite naršyklę**: *naujos kenkėjiškos programos ir sukčiavimo grėsmės kuriamos reguliariai, todėl svarbu nuolat atnaujinti naršyklę.*

  - Įsitikinkite, kad turite naujausią naršyklės versiją.

  - Įsitikinkite, kad įdiegti visi naujausi atnaujinimai.

Funded by the Erasmus+ Programme of the European Union

Saugus naršymas internete

- **Tikrinkite domenus**: kenkėjiškos svetainės dažnai naudoja apgaulingus domenus, tam kad įtikintų naudotojus, jog jie yra teisėtame tinklalapyje. Dauguma naršyklių turi funkcijas, leidžiančias patikrinti domeną, arba galima naudoti specialias interneto svetaines domeno patikrinimui (tai mažiau patogu).
- **Siųskitės tik iš patikimų svetainių**: vienas lengviausių būdų kenkėjiškoms, šnipinėjimo ir reklamą siūlančioms programos patekti į jūsų kompiuterį, yra atsisiuntimai:

  - Būkite atsargūs su nemokama programine įranga;

  - Venkite neteisėtų atsisiuntimų;

  - Būkite atsargūs P2P failų dalijimosi atveju.

Funded by the Erasmus+ Programme of the European Union

Saugus naršymas internete

- **Reguliariai valykite podėlį (*Cache*)**
  - Naršyklė gali paspartinti prieigą įkeldama puslapius iš podėlio.
  - Naudodami spartųjį interneto ryšį, skirtumo galite nepastebėti.
  - Laikui bėgant podėlis prisipildo ir todėl naršyklė gali sulėtėti.

Pravartu reguliariai išvalyti podėlį, tam kad atlaisvinti vietos kompiuteryje ir ... pašalinti galimus kenkėjiškus failus.

Funded by the Erasmus+ Programme of the European Union

Saugus naršymas internete

Blokuoti iššokančius langus

- Iššokantys langai - tai maži naršyklės langai, kurie automatiškai pasirodo, kai lankotės tam tikrose svetainėse.
- Iššokantys langai gali būti teisėtos svetainės veikimo dalis.
- Kai kuriuose iššokančiuose languose gali būti kenkėjiškų programų.

Pravartu blokuoti iššokančius langus

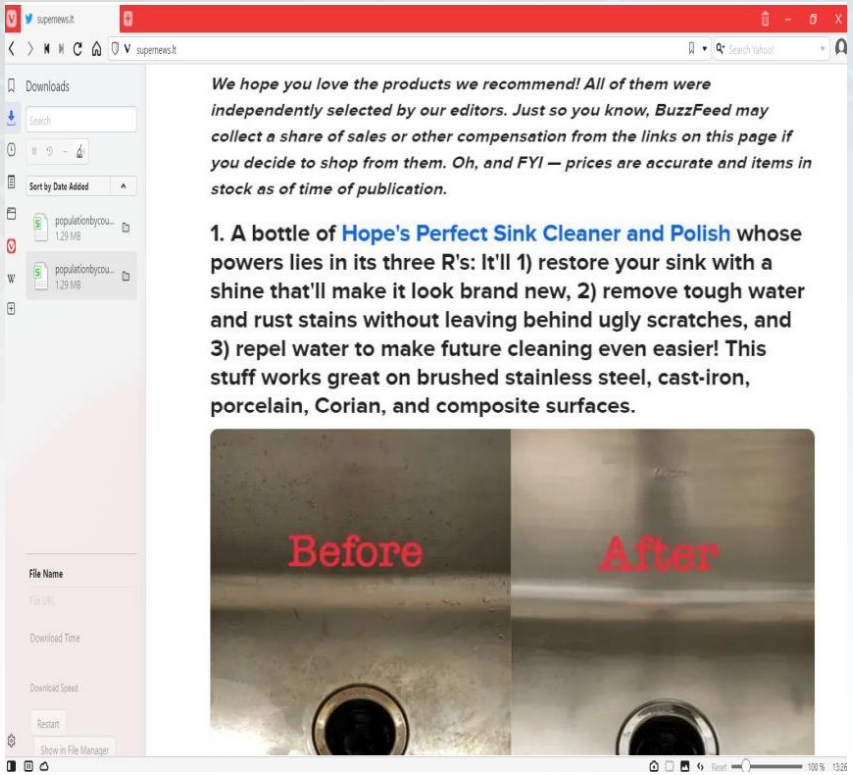
Dauguma naršyklių turi specialius iššokančiųjų langų blokatorius.

Funded by the Erasmus+ Programme of the European Union

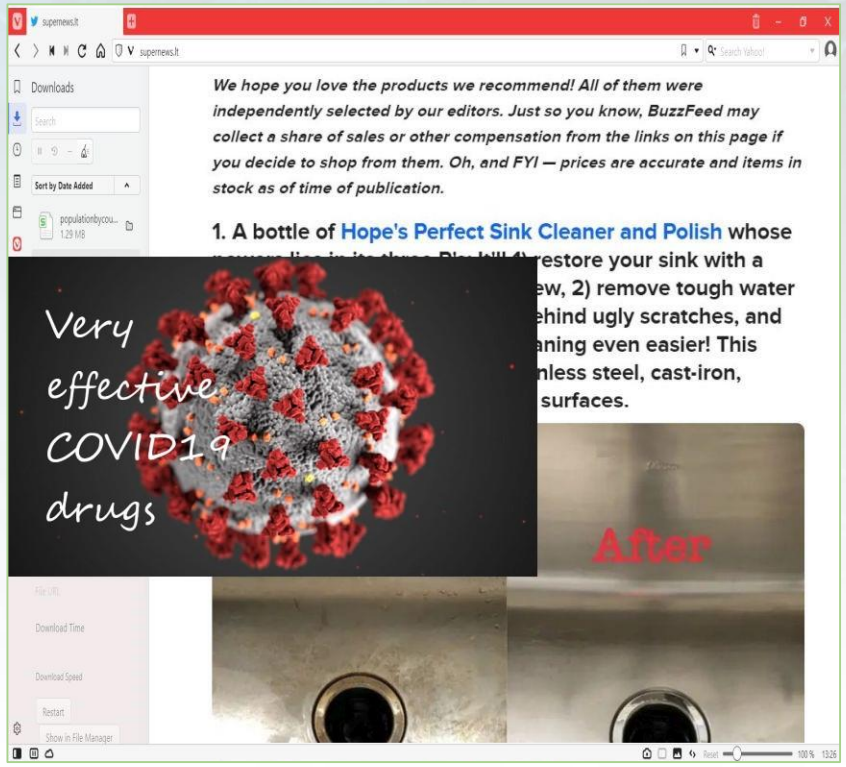
Saugus naršymas internete:

Pavyzdžiai su iššokančiais langais ir be jų

Marija užblokavo iššokančius langus



Jonas neužblokavo iššokančių langų



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saugumo programinės įrangos diegimas

Saugumo programinė įranga yra esminis saugaus darbo kibernetinėje erdvėje elementas.

Nepamirškite:

1. *Įdiegti interneto saugumo programinės įrangos;*
2. *Įdiegti ugniasienę;*
3. *Sukurti pakrovimo diską (Boot Disk);*
4. *Sukonfigūruoti griežtus žiniatinklio naršyklės ir el. pašto saugumo nustatymus;*
5. *Vengti nežinomų programų diegimo/ paleidimo;*
6. *Išjungti paslėptų failų vardų plėtinius.*

Funded by the Erasmus+ Programme of the European Union

Kaip sekama jūsų naršymo veikla

- Kai kuriose svetainėse (*Amazon*, *eBay*, *Netflix* ir daugelyje kitų) renkami duomenys apie jūsų pageidavimus: jos nori pasiūlyti jums patinkančių produktų.
- *Google* seka ir analizuoja jūsų veiklą, kad pateiktų statistinius duomenis įmonėms.
- Kai kurios vyriausybės renka duomenis apie jūsų veiklą internete, jei jų prireiktų kriminaliniams tyrimams arba nacionalinio saugumo tikslais.
- **Kai kurie nusikaltėliai taip pat gali bandyti sekti jūsų veiklą**.

- Svarbu žinoti apie tokį sekimą, ir išsiugdyti saugaus naršymo įpročius.

Funded by the
Erasmus+ Programme
of the European Union

Stiprių slaptažodžių kūrimas

- Slaptažodis - paprastai pagrindinė priemonė, užtikrinanti jūsų saugumą šiuolaikinėse IT sistemose.
- Slaptažodis turi būti stiprus, tam kad būtų užtikrintas aukštas saugumo lygis.

Koks yra stiprus slaptažodis ?

Stiprus slaptažodis yra toks, kurį lengva įsiminti, bet sunku atspėti kitiems.

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip sukurti stiprius slaptažodžius

Bloga praktika: kiekvienai paskyrai naudoti tą patį slaptažodį.

Priežastis: jei kas nors sužinos jūsų vienos paskyros slaptažodį, visos kitos paskyros gali tapti pažeidžiamos.

Patarimas: slaptažodyje naudoti skaičius, simbolius ir didžiąsias bei mažąsias raides. Taip bus sunkiau nulaužti slaptažodį naudojant brutalios jėgos ataką (*Brute Force Attack*).

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip sukurti stiprius slaptažodžius

Bloga praktika: naudoti asmeninę informaciją, pvz., savo vardą, pavardę, gimimo datą, naudotojo vardą ar el. pašto adresą.

Priežastis: tokia informacija dažnai yra viešai prieinama, todėl kas nors galėtų lengvai atspėti jūsų slaptažodį.

Naudokite ilgesnį slaptažodį

Nykščio taisyklė: kuo ilgesnis slaptažodis, tuo geriau (jį taip pat sunkiau įsiminti). Nors dėl papildomo saugumo jis turėtų būti dar ilgesnis.

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip sukurti stiprius slaptažodžius

Bloga praktika: naudoti žodžius, kuriuos galima rasti žodyne.

Priežastis: daugelis įsilaužimo įrankių atlieka vadinamąsias žodynu grįstas atakas (*vocabulary-based attacks)*. Pirmiausia bandoma patikrinti žinomus žodžius žodyne.

Pvz. **žaidėjas2002** būtų silpnas slaptažodis (žodis iš žodyno ir gimimo metai).

Atsitiktiniai slaptažodžiai yra stipriausi. Pagalvokite apie galimybę naudoti slaptažodžių generatorių.

Funded by the Erasmus+ Programme of the European Union

Dažniausiai pasitaikančios slaptažodžių problemos

Dažniausiai slaptažodžiuose naudojami šeimos narių vardai, pomėgiai, ar tiesiog paprastas šablonas. Tokius slaptažodžius lengva įsiminti, bet taip pat ir lengva atspėti.

Silpno slaptažodžio pavyzdys

Slaptažodis: *nick1995katie1997*

Problema: atrodo ilgas, bet lengvai atspėjamas, nes naudojami du vardai (vaikino ir merginos) ir jų gimimo metais Lengva atspėti, jei turite/ žinote informaciją apie juos.

Sprendimas: įterpti atsitiktinius simbolius, naudoti didžiųjų ir mažųjų raidžių derinius, pvz. ***ni%k199oK$tie199x***

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip sukurti stiprius slaptažodžius

Dažniausiai pasitaikančios slaptažodžių problemos

Slaptažodis: *w@kLx*

Problema: atrodo kaip atsitiktinis ir sunkiai atspėjamas, tačiau jame yra tik 5 simboliai. Per trumpas...

Sprendimas: stipresnis slaptažodis turėtų būti ilgesnis, pageidautina, bent 10 simbolių ilgio.

Slaptažodis: *123abc456cba789*

Problema: lengva įsiminti, bet naudojamas simbolių derinys bus vienas pirmųjų, kurį bus galima patikrinti.

Sprendimas: naudoti atsitiktinių slaptažodžių generatorių, pvz., #eV$pIg&qf

Funded by the Erasmus+ Programme of the European Union

Dažniausiai pasitaikančios slaptažodžių problemos

Vienodas slaptažodis keliose paskyrose

Gmail: Bd458$%Kl!df;
eBay: Bd458$%Kl!df;
Amazon: Bd458$%Kl!df

Problema: slaptažodis tinkamas, tačiau jį naudoti skirtingose svetainėse yra bloga praktika.

Sprendimas: kiekvienoje svetainėje naudokite skirtingus slaptažodžius.

Užuot rašę slaptažodžius ant popieriaus, naudokite **slaptažodžių tvarkyklę**. Slaptažodžių tvarkyklės gali įsiminti ir įvesti jūsų slaptažodį skirtingose svetainėse, todėl jums nereikės prisiminti ilgesnių slaptažodžių.

Funded by the Erasmus+ Programme of the European Union

Daugiapakopis autentifikavimas

Daugiapakopis autentifikavimas - tai dar geresnis būdas apsaugoti jautrius duomenis.

Kas yra daugiapakopis autentifikavimas?

Daugiapakopis autentifikavimas - tai tikrinimo metodas, kai reikalaujama **bent dviejų skirtingų įrodymų veiksnių**.

Daugiapakopis autentifikavimas kartais vadinamas 2FA (dviejų veiksnių autentifikavimu).

Iš esmės jis suteikia papildomą saugumo lygį.

Funded by the Erasmus+ Programme of the European Union

Daugiapakopio autentifikavimo tipai

Egzistuoja trys autentifikavimo veiksnių tipai:

1 tipas: kažkas, ką žinote – jis apima slaptažodžius, PIN kodus, kodinius žodžius ir pan.

2 tipas: kažkas, ką turite - apima visus daiktus, kurie yra fiziniai objektai (raktai, išmanieji telefonai, išmaniosios kortelės, USB atmintinės).

3 tipas: kažkas, kas esate - apima biometrinius duomenis (pirštų atspaudus, delno nuskaitymą, veido atpažinimą, akies tinklainės nuskaitymą, akies rainelės nuskaitymą, balso patikrinimą).

Funded by the Erasmus+ Programme of the European Union

Daugiapakopis autentifikavimas

Apjungus bent du veiksnius iš šių trijų kategorijų, gaunamas daugiapakopis autentifikavimas.

Daugiapakopį autentifikavimą įsilaužėliui įveikti daug sunkiau.

Jei naudojamas daugiapakopis autentifikavimas, reikalinga aukštesnė užpuoliko kvalifikacija (gebėti vienu metu vykdyti kelias atakas).

Paprastai tai yra sunku.

Gerai žinomas daugiapakopio autentiškumo patvirtinimo pavyzdys yra *PayPal*.

Funded by the
Erasmus+ Programme
of the European Union

Populiariausi daugiapakopio autentifikavimo įrankiai

Yra daug daugiapakopio autentiškumo patvirtinimo įrankių.

Dažniausiai naudojamas autentifikavimo programėles rasite savo mobiliojo įrenginio programėlių parduotuvėje (*app store*):

- *Google Authenticator*;
- *LastPass Authenticator*;
- *Microsoft Authenticator*;
- *Authy*;
- ir daugelį kitų.

Funded by the Erasmus+ Programme of the European Union

Failų šifravimas

Kas yra failų šifravimas?

Failų šifravimas - tai duomenų kodavimo metodas, skirtas saugiam failų perdavimui.

Ką daro failų šifravimas?

Failų užšifravimas padeda išvengti klastojimo ar neautorizuotos prieigos.

Kaip veikia failų šifravimas?

Jis veikia naudodamas sudėtingus algoritmus siunčiamiems duomenims išmaišyti.

Funded by the Erasmus+ Programme of the European Union

Failų šifravimas

Svarbu:

norint gauti prieigą prie faile esančios informacijos, reikia turėti raktą!

Funded by the
Erasmus+ Programme
of the European Union

Kaip šifruojami failai

Yra du populiariausi šifravimo standartai:

Atvirasis PGP (*Pretty Good Privacy*) - leidžia šifruoti ir iššifruoti failus naudojant viešąjį ir privatųjį raktus.

ZIP su AES (*Advanced Encryption Standard*) - suspaudžia ir užšifruoja failus AES šifravimu, naudodami ZIP ir GZIP (GNU zip) standartus.

Funded by the Erasmus+ Programme of the European Union

Kodėl verta naudoti failų šifravimo programinę įrangą

- Daugiasluoksnė duomenų apsauga;

- Saugumas daugelyje įrenginių;

- Saugus duomenų perdavimas;

- Išlaikomas vientisumas;

- Užtikrintas atitikimas teisės aktų reikalavimams.

Funded by the
Erasmus+ Programme
of the European Union

Kaip pasirinkti kodavimo programinę įrangą

-Kokius kodavimo standartus reikia palaikyti?

- Kiek duomenys yra jautrūs?

- Ar keičiamasi dideliais failais?

- Ar failai turėtų būti šifruojami, ar kanalas kuriuo jie perduodami?

- Kaip bus perduodami duomenys?

Funded by the
Erasmus+ Programme
of the European Union

Kodavimo programinė įranga

- *AxCrypt Premium*
- *Folder Lock*
- *CryptoForge*
- *NordLocker*
- *Steganos Safe*

Patarimai, kaip atpažinti kibernetinę ataką

Jei jau atidarėte įtartiną el. laišką ar nuorodą, patikrinkite šiuos dalykus:

- *neįprastą veiklą savo prietaise ar tinkle.*
- *įtartiną bandymą prisijungti prie jūsų paskyros .*
- *Identifikuokite įtartinus iššokančius langus.*
- *Stebėkite lėtesnį nei įprasta tinkle veikimą.*
- *Atnaujinkite programinę įrangą.*
- *Netikėtus ar staigius disko vietos ar atminties pokyčius.*

Funded by the
Erasmus+ Programme
of the European Union

Keletas saugaus apsipirkimo internetu patarimų

Apsipirkimas internetu yra labai patogus ir dažnai ekonomiškas būdas ką nors nusipirkti.

Tačiau taip pat labai pavojingas: FTB Nusikaltimų internete skundų centras (IC3) nustatė, kad 2019 m. **pusė elektroninių nusikaltimų** buvo susiję su apsipirkimu internete. Situacija panaši visur.

Įvairūs netinkamo elgesio šaltiniai:

- negautos prekės;
- *nesumokėta už prekes;*
- *pavogti konfidencialūs duomenys, ypač finansiniai duomenys, pvz. kredito kortelių duomenys*.

Funded by the Erasmus+ Programme of the European Union

Keletas saugaus apsipirkimo internetu patarimų

1 patarimas: naudokitės tik pažįstamomis arba patikimomis internetinėmis parduotuvėmis

- Tai yra pirmoji saugumo priemonė;

- Pasidomėkite klientų nuomone apie internetinę parduotuvę;

- Pasidomėkite, kiek laiko parduotuvė veikia (paprastai kuo ilgiau veikia, tuo patikimesnė);

- Stenkitės nesinaudoti parduotuvėmis, apie kurias sužinojote iš iššokančių reklamų ar elektroninio pašto reklamų;

- Praneškite apie elektroninius nusikaltimus, jei pasijutote nukentėję!

Funded by the Erasmus+ Programme of the European Union

Keletas saugaus apsipirkimo internetu patarimų

2 patarimas: niekada nieko nepirkite internetu naudodami kredito kortelę svetainėje, kurioje nėra įdiegtas SSL (*Secure Sockets Layer*) šifravimas.

- *Svetainėje įdiegtas SSL, kai jos URL prasideda HTTPS, vietoje HTTP;*
- *URL adreso kairėje, arba ekrano apačioje, būsenos juostoje, atsiras užrakintos pakabinamos spynos piktograma;*
- *HTTPS dabar yra tapęs beveik standartu ir naudojamas praktiškai visur.*

Funded by the Erasmus+ Programme of the European Union

Keletas saugaus apsipirkimo internetu patarimų

3 patarimas: nesidalykite asmenine informacija

- *Jokia internetinė apsipirkimo svetainė (internetinė parduotuvė) nereikalauja jūsų asmens kodo, paso duomenų ir pan.;*
- *Jūsų kredito kortelės duomenis turi patvirtinti jūsų internetinis bankas;*
- *Įjunkite saugaus apsipirkimo nustatymą savo el. bankininkystėje;*
- *Būti neregistruotu pirkėju dažnai yra privalumas saugumo požiūriu.*

Atminkite: kuo mažiau sukčiai apie jus žino, tuo sunkiau nulaužti jūsų paskyrą.

Keletas saugaus apsipirkimo internetu patarimų

4 patarimas: tinkamai apsaugokite savo paskyrą

- *Naudokite stiprius slaptažodžius (žr. pirmiau);*
- *Reguliariai keiskite slaptažodžius (tai daro tik 25 % žmonių, jei to iš jų nereikalaujama);*
- *Skirtingose apsipirkimo platformose naudokite skirtingus slaptažodžius;*
- *Jei įmanoma, naudokite daugiapakopį autentifikavimą;*
- *Naudokite antivirusinę programinę įrangą;*
- *Perkant internetu naudokite tik savo skaitmeninį įranginį.*

Keletas saugaus apsipirkimo internetu patarimų

5 patarimas: mąstykite iš mobiliojo įrenginio vartotojo perspektyvos

- *nebijokite pirkti naudodami mobiliąsias programėles: jos nemažiau saugios nei įprasta programinė įranga;*
- *tačiau naudokite tik mažmenininko arba kitos internetinės prekybos platformos pateiktas programėles;*
- *slėpkite įrenginio ekraną, kai atliekate mokėjimą viešoje vietoje;*
- *tinkamai apsaugokite savo mobilųjį įrenginį.*

Atminkite: saugiai apsipirkdami ar atlikdami mokėjimą viešoje vietoje turite mąstyti šiek tiek kaip gangsteris.

Keletas saugaus apsipirkimo internetu patarimų

6 patarimas: nevenkite atsiskaitinėti mobiliuoju telefonu

- *atsiskaityti už prekes išmaniuoju telefonu yra įprasta;*
- *iš tiesų tai yra netgi saugiau nei naudoti kredito kortelę;*
- *mobiliųjų mokėjimų programėlės, pvz., Apple Pay, sugeneruoja vienkartinį pirkinio autentifikavimo kodą, kurio niekas kitas negalėtų pavogti ir panaudoti;*
- *su savimi nereikia turėti kredito kortelės: tai taip pat yra atsargumo priemonė!*

Funded by the Erasmus+ Programme of the European Union

Darbas su slapukais

- Slapukai yra esminis šiuolaikinio interneto elementas, tačiau jie pažeidžia jūsų privatumą.
- Slapukai padeda žiniatinklio kūrėjams suteikti jums personalizuotą ir patogesnį apsilankymą svetainėje.
- Slapukai leidžia svetainėms įsiminti jus, jūsų prisijungimus prie svetainės, pirkinių krepšelius ir kt.
- Tačiau jie taip pat gali būti privačios informacijos lobis, kurį nusikaltėliai gali šnipinėti.
- Net ir elementarus supratimas apie slapukus gali padėti išvengti nepageidaujamų žvilgsnių į jūsų veiklą internete.

Funded by the Erasmus+ Programme of the European Union

Kas yra slapukai ?

- Pagrindinis apibrėžimas: slapukai - tai tekstiniai failai, kuriuose yra duomenų fragmentų (pvz., vartotojo vardas ir slaptažodis).
- Jie naudojami jūsų, kaip besinaudojančio internetu identifikavimui.
- HTTP slapukai naudojami konkretiems naudotojams identifikuoti ir naršymui suteikti daugiau patogumo.

- Slapukuose saugomus duomenis serveris sukuria jums prisijungus. Šie duomenys pažymėti unikaliu jūsų ir jūsų kompiuterio ID.
- Serveris nuskaito ID ir žino, kokią konkrečiai informaciją pateikti jums.

Funded by the Erasmus+ Programme of the European Union

Slapukų tipai

Du pagrindiniai tipai:

- Magic slapukai
- HTTP slapukai

***Magic* slapukai** (*Magic cookies*) - tai terminas, reiškiantis informacijos paketus, kurie siunčiami ir gaunami be pakeitimų.

Dažniausiai naudojami prisijungiant prie kompiuterinių duomenų bazių sistemų, pvz. verslo vidinis tinklas.

Funded by the Erasmus+ Programme of the European Union

Slapukų tipai

Du pagrindiniai tipai:

- Magic slapukai
- HTTP slapukai

HTTP slapukai - tai modifikuota *Magic cookie* versija, sukurta naršymui internete.

HTTP slapukas naudojamas mūsų prioritetams internete valdyti.

Piktavaliai gali juos išnaudoti šnipinėdami jūsų veiklą internete ir net vogdami jūsų asmeninę informaciją.

Funded by the Erasmus+ Programme of the European Union

Kam naudojami slapukai?

- **Sesijos valdymui:** slapukai leidžia svetainėms atpažinti naudotojus ir prisiminti jų individualią prisijungimo informaciją ir pageidavimus,
  pvz., sporto naujienos, politika, ar kt.

- **Personalizavimas:** pritaikyta reklama yra pagrindinis būdas, kuriuo slapukai naudojami sesijoms personalizuoti.

- **Stebėjimas:** apsipirkimo svetainės naudoja slapukus, kad galėtų sekti naudotojų anksčiau peržiūrėtas prekes, todėl svetainės gali pasiūlyti kitų prekių, kurios jiems gali patikti, ir išlaikyti prekes pirkinių krepšeliuose, kol jie tęsia apsipirkimą.

Funded by the
Erasmus+ Programme
of the European Union

Skirtingi HTTP slapukų tipai

Sesijos slapukai naudojami tik naršant svetainėje. Jie saugomi operatyviojoje atmintyje (RAM) niekada neįrašomi į kietąjį diską.
Pasibaigus sesijai, sesijos slapukai automatiškai ištrinami.

Nuolatiniai slapukai kompiuteryje išlieka neribotą laiką, tačiau dažnai daugelyje jų nurodoma galiojimo pabaigos data ir jie ištrinami praėjus iš anksto nustatytam laikotarpiui.

Funded by the Erasmus+ Programme of the European Union

Nuolatiniai slapukai

Nuolatiniai slapukai naudojami dviem pagrindiniais tikslais:

Autentifikavimas: stebima, ar naudotojas yra prisijungęs ir kokiu vardu.
Jie taip pat supaprastina prisijungimo informaciją, todėl naudotojams nereikia prisiminti svetainės slaptažodžių.

Stebėjimas: stebi daugkartinius apsilankymus toje pačioje svetainėje per tam tikrą laiką.

Funded by the
Erasmus+ Programme
of the European Union

Kaip slapukai gali būti pavojingi

- Kadangi slapukuose esantys duomenys nesikeičia, patys slapukai nėra kenksmingi.
- Tačiau kai kurios kibernetinės atakos gali perimti prieigą prie jūsų naršymo įpročių.
- Pavojų kelia jų galimybė sekti asmenų naršymo istoriją.
- Kartais jie gali būti naudojami kompiuterio užkrėtimui kenkėjiškomis programomis.

Funded by the Erasmus+ Programme of the European Union

Pirmosios ir trečiosios šalies slapukai

- Pirmosios šalies slapukus tiesiogiai sukuria jūsų naudojama svetainė. Jie paprastai yra saugesni, jei naršote patikimas svetaines arba svetaines, kurios nebuvo pažeistos.
- Trečiųjų šalių slapukai sukuriami svetainių, kurios skiriasi nuo tinklalapių, kuriuose vartotojai tuo metu naršo, paprastai dėl to, kad jie susiję su tame puslapyje esančiais skelbimais.
- Apsilankius svetainėje, kurioje yra 10 skelbimų, gali būti sukurta 10 slapukų, net jei naudotojai niekada nespaudžia tų skelbimų.
- Trečiųjų šalių slapukai leidžia reklamuotojams arba analitikos bendrovėms sekti asmens naršymo internete istoriją visose svetainėse, kuriose yra jų skelbimų.

Funded by the Erasmus+ Programme of the European Union

Pirmosios šalies ir trečiosios šalies slapukai

Zombie cookies - šie slapukai yra trečiosios šalies slapukai, kurie nuolat įdiegiami naudotojų kompiuteriuose, net jei jie pasirenka neįdiegti slapukų.

Jie paprastai vėl atsiranda po to, kai buvo ištrinti.

Kaip ir kitus trečiųjų šalių slapukus, *Zombie cookies* gali naudoti žiniatinklio analitikos kompanijos, kad galėtų sekti konkrečių asmenų naršymo įpročius.

Svetainės taip pat gali naudoti tokius slapukus, kad uždraustų tam tikrus naudotojus.

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip elgtis su slapukais

- ES teisės aktai reikalauja gauti naudotojo sutikimą naudoti slapukus.
- Norėdami laikytis slapukus reglamentuojančių nuostatų pagal BDAR ir E-privatumo direktyvą, privalote:
  - *Prieš naudodami bet kokius slapukus, išskyrus griežtai būtinus slapukus, turite gauti naudotojų sutikimą.*
  - *Siekdami gauti vartotojo sutikimą, pateikite tikslią ir konkrečią informaciją apie kiekvieno slapuko sekamus duomenis ir jų paskirtį, vartotojui suprantama kalba.*
  - *Dokumentuokite ir saugokite iš naudotojų gautus sutikimus. Leiskite naudotojams naudotis jūsų paslauga, net jei jie atsisako leisti naudoti tam tikrus slapukus.*
  - *Užtikrinkite, kad naudotojams būtų taip pat lengva atšaukti savo sutikimą, kaip ir duoti sutikimą*

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip elgtis su slapukais

- Dauguma šiuolaikinių naršyklių leidžia valdyti kompiuteryje išsaugotus slapukus.
- Pvz., galite norėti priimti visus slapukus, ištrinti tam tikros svetainės slapukus arba atmesti visus slapukus.
- Norėdami rasti naršyklės teikiamas slapukų valdymo galimybes, turite ieškoti naršyklės vadove arba pagalbos sistemoje.

Funded by the
Erasmus+ Programme
of the European Union

Kenkėjiškų programų tvarkymas

- Kenkėjiškos programos - tai kenkėjiška programinė įranga, kuri, patekusi į sistemą, leidžia užpuolikui visiškai arba dalinai ją kontroliuoti.
- Jos gali sugadinti arba pakeisti sistemoje esančią informaciją, ar net ją pavogti.
- Yra įvairių tipų kenkėjiškų programų, pvz., virusai, Trojos arkliai, kirminai, „rutkitai“ (*Rootkits*), šnipinėjimo programos (*Spyware)* ir išpirkos reikalaujančios programos (*Ransomware)*.
- Kenkėjiška programinė įranga gali patekti į sistemą per el. laiškus, failų perdavimą, atsitiktinės trečiųjų šalių programinės įrangos diegimą, nenaudojant kokybiškos antivirusinės programinės įrangos.

Funded by the Erasmus+ Programme of the European Union

Skirtumas tarp ***viruso*** *ir* ***kirmino***

Virus

- prisitvirtina prie programos arba failo ir plinta iš vienos sistemos į kitą.
- plinta kopijuodamas ir vykdydamas save.
- atlieka pakeitimus sistemose be naudotojo žinios.
- plinta tokiu pat greičiu, kaip ir suprogramuotas.

Kirminas

- panašių virusų poklasis, kurie plinta iš vieno kompiuterio į kitą.
- išnaudoja operacinę sistemą, turinčią silpną apsaugą.
- sukelia sistemos ar tinklo veikimo sutrikimus.
- plinta greičiau nei virusas.

Funded by the Erasmus+ Programme of the European Union

Antivirusinė programinė įranga

- Antivirusinė programinė įranga naudojama siekiant nustatyti, užkardyti arba pašalinti sistemoje esančią kenkėjišką programinę įrangą.
- Gali reguliariai tikrinti sistemą ir atnaujinti sistemos saugumą.
- Rinkoje galima įsigyti įvairios mokamos arba nemokamos antivirusinės programinės įrangos.
- Antivirusinės programinės įrangos nenaudojimas yra “kibernetinio nusikaltimo rūšis”!
  Galite ne tik tapti atakos auka, bet ir jūsų kompiuteris gali būti panaudotas kaip kibernetinės atakos įrankis.

Funded by the Erasmus+ Programme of the European Union

Patarimai, kaip apsisaugoti nuo kenkėjiškų programų

Nors tai aptarta anksčiau, bet vis tiek reikia prisiminti:

- *Nuolat atnaujinkite savo kompiuterinę ir programinę įrangą.*
- *Jei įmanoma, naudokite ne administratoriaus paskyrą.*
- *Du kartus pagalvokite prieš spustelėdami nuorodas arba ką nors atsisiųsdami.*
- *Būkite atsargūs atidarydami el. laiškų priedus ar paveikslėlius.*
- *Nepasitikėkite iššokančiais langais, kuriuose reklamuojama programinė įranga.*
- *Apribokite failų dalijimąsi.*

Funded by the
Erasmus+ Programme
of the European Union

Įvertinkite saugumo pažeidimą

Du svarbūs klausimai:

- **Pasitikrinkite ar šaltinis yra patikimas**: jei tapote viena iš platesnio masto atakos, nuo kurios nukentėjo kelios įmonės ar asmenys, aukų, sekite patikimų šaltinių, kuriems pavesta stebėti situaciją, naujienas.

- **Nustatykite pažeidimo priežastį**: nepriklausomai nuo to, ar esate platesnės atakos dalis, ar vienintelė auka, jums taip pat reikės nustatyti pažeidimo priežastį konkrečioje jūsų įstaigoje, kad galėtumėte padėti užkirsti kelią tokiai pačiai atakai pasikartoti.

Funded by the
Erasmus+ Programme
of the European Union

Įvertinkite saugumo pažeidimą

Pabandykite rasti atsakymus į kitus klausimus:

- Kaip buvo pradėta ataka?
- Kas turi prieigą prie užkrėstų serverių?
- Kurie tinklo ryšiai buvo aktyvūs, kai įvyko pažeidimas?

Funded by the
Erasmus+ Programme
of the European Union

Įvertinkite saugumo pažeidimą

- Pavyzdžiui, jums gali pasisekti padėti nustatyti, kaip įvyko įsilaužimas, patikrinus visus saugumo duomenų žurnalus.
- Gali tekti prašyti kibernetinio saugumo specialistų pagalbos.
- Nedvejodami kreipkitės patarimo, jei jaučiate, kad jums trūksta žinių.

Funded by the Erasmus+ Programme of the European Union

Įvertinkite saugumo pažeidimą

Nustatykite asmenis, kuriems pažeidimas turėjo įtakos:

- Labai svarbu išsiaiškinti, kas galėjo nukentėti nuo pažeidimo, įskaitant darbuotojus, klientus ir trečiųjų šalių tiekėjus.

- Įvertinkite, kiek rimtas buvo duomenų saugumo pažeidimas, nustatydami, kuri informacija galėjo būti pasiekta arba į ką buvo nukreipta, pvz., gimtadieniai, pašto adresai, el. pašto paskyros ir kredito kortelių numeriai.

Funded by the Erasmus+ Programme of the European Union

Įvertinkite saugumo pažeidimą

Inicijuokite kibernetinės atakos protokolą:

- Darbuotojai turėtų žinoti jūsų politiką dėl duomenų saugumo pažeidimų.
- Nustatę pažeidimo priežastį, pakoreguokite savo saugumo protokolus ir iškomunikuokite apie juos, kad užtikrintumėte, jog tokio pobūdžio incidentas nepasikartos.
- Apsvarstykite galimybę apriboti darbuotojų prieigą prie duomenų pagal jų darbo funkcijas.

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų padarinių valdymas

Jei ataka buvo įvykdyta prieš įmonę: informuokite vadovus ir darbuotojus apie įsilaužimą bei praneškite visiems kitiems asmenims, kuriuos gali paveikti ataka prieš jus.

Tai apima:

- *komunikuokite su kolegomis ir praneškite jiems, kas nutiko.*
- *Nustatykite aiškius komandos narių įgaliojimus komunikuoti šiuo klausimu tiek įmonės viduje, tiek išorėje.*
- *Atsistatant po duomenų saugumo pažeidimo labai svarbu palaikyti glaudų ryšį su komanda.*
- *Jums gali prireikti teisinės konsultacijos dėl teisinių incidento aspektų.*

Kibernetinių atakų padarinių valdymas

Jei ataka buvo įvykdyta prieš įmonę: informuokite vadovus ir darbuotojus apie įsilaužimą bei praneškite visiems kitiems asmenims, kuriuos gali paveikti ataka prieš jus.

Tai apima:

- *Jei turite kibernetinės atsakomybės draudimą (Cyber Liability Insurance), praneškite apie tai atsakingam asmeniui.*
- *Kibernetinės atsakomybės draudimas skirtas padėti atsigauti po duomenų saugumo pažeidimo ar kibernetinio saugumo atakos.*
- *Kuo greičiau susisiekite su savo atsakingam asmeniui ir sužinokite, kaip jis gali padėti jums, ką daryti po kibernetinės atakos.*

Funded by the Erasmus+ Programme of the European Union

Kibernetinių atakų padarinių valdymas

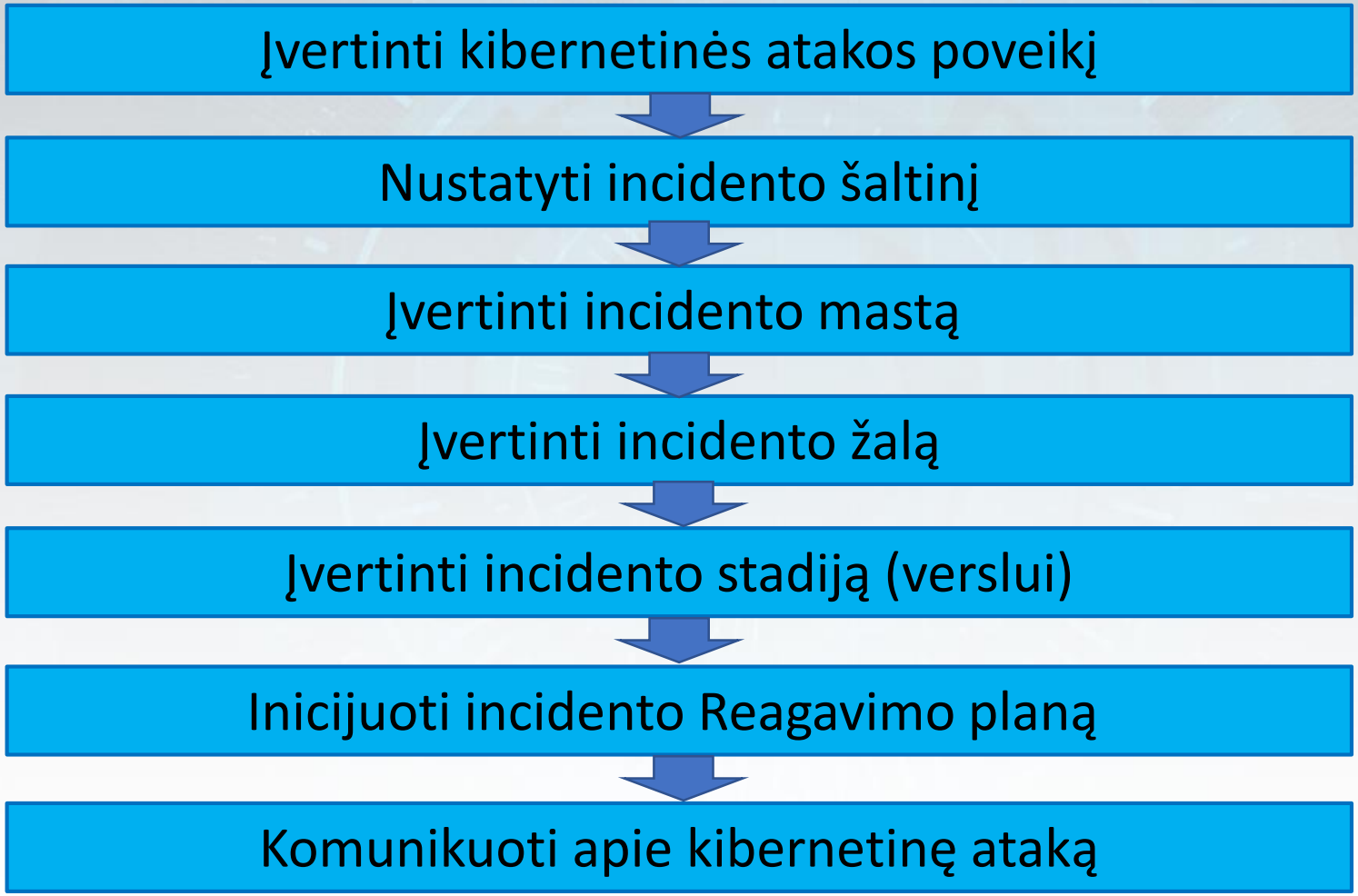
Jei ataka buvo nukreipta prieš įmonę: praneškite klientams

Tai apima:

- *Pabrėžkite savo norą skaidriai bendrauti su klientais, apsvarstydami galimybę įsteigti specialią veiksmų karštąją liniją, skirtą specialiai nukentėjusių asmenų klausimams spręsti.*

- *Bendravimas gali būti labai svarbus siekiant palaikyti teigiamus, profesionalius santykius su savo klientais ir sumažinti galimus nuostolius.*

Kibernetinių atakų vertinimas



Praneškite apie kibernetinius nusikaltimus

- Praneškite apie išpuolį atsakingai institucijai:

  - Kiekviena šalis turi atsakingą instituciją, pvz., CERT.

- Priklausomai nuo kibernetinės atakos tipo ir nacionalinio arba tarptautinio reguliavimo, apie įvykį gali tekti informuoti teisėsaugos institucijas.
- Jei baiminatės, kad gali būti pažeisti slapti finansiniai duomenys, gali tekti susisiekti su kredito kortelės bendrove.
- Praneškite finansinei organizacijai, kad ginčijate sukčių atliktus neautorizuotus nurašymus nuo jūsų kortelės arba jei įtariate, kad buvo pažeistas jūsų kortelės numeris.
- Aptarkite tolesnius veiksmus su finansine organizacija.

Funded by the Erasmus+ Programme of the European Union

Praneškite apie kibernetinius nusikaltimus

Tai ypač svarbu, jei pastebėjote veiksmus susijusius su nusikalstama veikla:

- pvz., jaunas įsilaužėlis siekė išbandyti save.

Jei pastebėjote, kad tapote sukčiavimo incidento auka:

- kreipkitės į IT/ saugumo skyrių, jei tokį turite;
- Nedelsdami susisiekite su finansų įstaiga ir paprašykite atšaukti lėšas;
- Kreipkitės į darbdavį ir praneškite apie darbo užmokesčio pervedimo pažeidimus.

Pašalinus tiesioginę grėsmę

- Atnaujinkite programinę įrangą. Įdiekite reikiamus pataisymus (*patches*).
- Pakeiskite slaptažodžius sistemoje.
- Saugumo tikslais pakeiskite slaptažodžius kitose sistemose.
- Įdiekite dviejų žingsnių verifikavimo metodus, kad galėtumėte prisijungti prie pažeidžiamų paskyrų.

- Įdiekite žiniatinklio programų ugniasienę *(web application firewall*), kad apsaugotumėte savo svetainę, jei esate svetainės administratorius arba turite savo svetainę.
- Užtikrinkite, kad jūsų e. prekybos platforma atitinka PCI-DSS (*Payment Card Industry Data Security Standards*) pirmojo lygio reikalavimus.

Ką daryti toliau

„60% per pastaruosius trejus metus įvykusių smulkaus verslo ir asmeninių duomenų saugumo pažeidimų įvyko dėl išorinių veiksnių. Todėl reguliariai turėtų vykti darbuotojų išsamūs mokymai.

Užtikrinkite, kad darbuotojai gebėtų atpažinti įspėjamuosius įtartinų el. laiškų ir jų priedų požymius ir žinotų, kaip pranešti apie visus gautus laiškus. Taip pat apmokykite juos, kaip šifruoti asmeninę ar neskelbtiną informaciją“

Mike'as Tanenbaumas,
"Chubb North America"
vykdomasis viceprezidentas
ir kibernetinio padalinio vadovas.

Funded by the
Erasmus+ Programme
of the European Union

Jei buvo įsilaužta į jūsų Gmail arba Youtube paskyrą

Jei pastebėjote įtartiną veiklą savo *Google* paskyroje, *Gmail* ar kituose *Google* produktuose, gali būti, kad kažkas kitas jais naudojasi be jūsų leidimo.

1 žingsnis: prisijunkite prie savo *Google* paskyros;

2 veiksmas: peržiūrėkite veiklą ir padėkite apsaugoti „nulaužtą“ *Google* paskyrą;

3 veiksmas: imkitės daugiau saugumo priemonių.

Daugiau informacijos rasite adresu: https://support.google.com/accounts/answer/6294825?hl=en

Jei buvo įsilaužta į jūsų Facebook paskyrą

Remiantis *Facebook* rekomendacijomis, į jūsų paskyrą galėjo būti įsilaužta, jei pastebėjote, kad:

- buvo pakeistas jūsų el. pašto adresas arba slaptažodis.
- buvo pakeistas jūsų vardas arba gimtadienis.
- prašymai priimti į draugų ratą buvo išsiųsti nepažįstamiems žmonėms.
- Buvo išsiųstos žinutės, kurių jūs nerašėte.
- Paskelbtos žinutės, kurių jūs nesukūrėte.

Jei manote, kad į jūsų paskyrą buvo įsilaužta arba ji buvo perimta, apsilankykite puslapyje: https://www.facebook.com/hacked

Funded by the Erasmus+ Programme of the European Union

Ką daryti, jei buvo įsilaužta į kitą jūsų paskyrą

- Yra labai daug įvairių sistemų, į kurias gali būti įsilaužta;
- Neįmanoma pateikti išsamios informacijos apie visas sistemas.

Bendrieji pasiūlymai yra šie:

- ieškokite patarimų pagalbos sistemoje;

- pabandykite susisiekti su įmone, kuri yra atsakinga už šį produktą.

Funded by the
Erasmus+ Programme
of the European Union

Apibendrinimas

Išvengti kibernetinių atakų įmanoma.

- Mokykitės ir ugdykite sąmoningumą;
- Ugdykite reikiamus įpročius;
- Naudokite tinkamas priemones;
- Turėkite planą, kaip elgtis kibernetinės atakos atveju.

Funded by the Erasmus+ Programme of the European Union

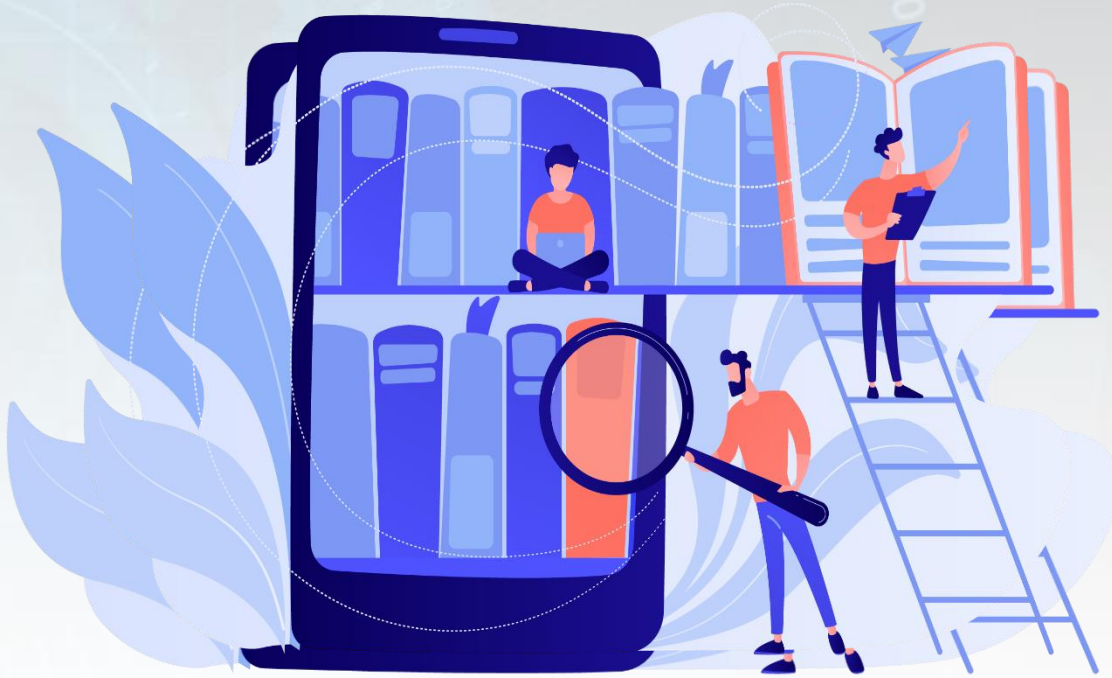
Užduotys

Įvertinkite kibernetinio saugumo būklę įmonėse

- Parengties būsena;
- Naudojamų priemonių kokybė;
- Slaptažodžių kokybė;
- Reakcijos;
- Pokyčiai po atakos.

Papildomi skaitiniai

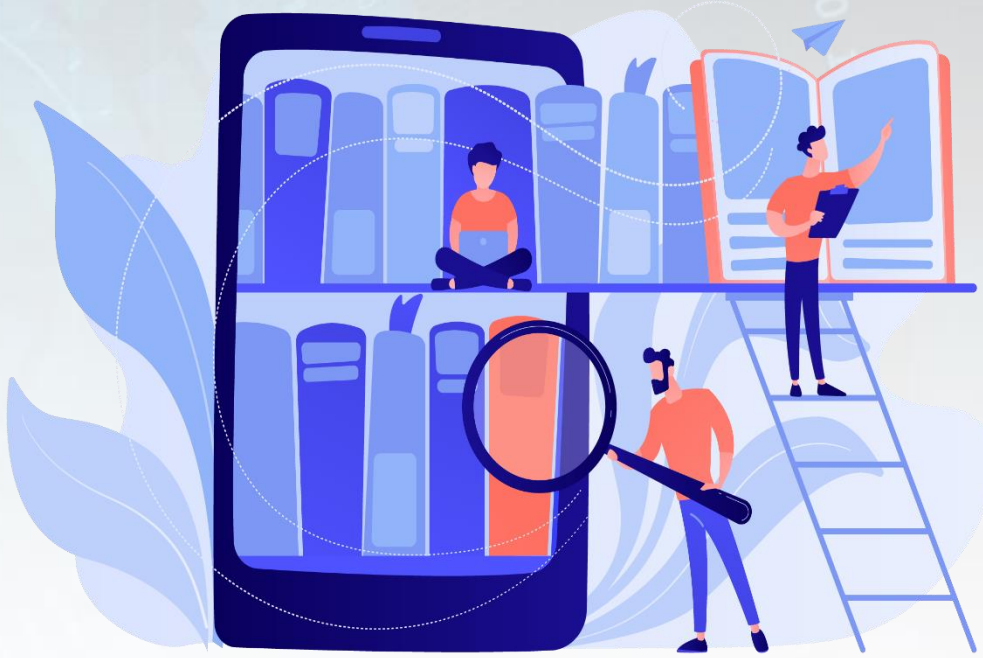
- Protect your business from cyber threats. Australian Government Guidelines. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats
- Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, September 2021*
- Atul S Choudhary; Pankaj P Choudhary; Shrikant Salve. A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. *In Proc. of IEEE 2018 3rd International Conference on Inventive Computation Technologies*



Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

- Federal Communications Commission. Cybersecurity for Small Business. https://www.fcc.gov/general/cybersecurity-small-business
- State of Cybersecurity in Local, State & Federal Government. *Ponemon Institute Research Paper.* https://www.ponemon.org/local/upload/file/State%20of%20Cybersecurity%20in%20Government%20FINAL2.pdf
- NCSS Good Practice Guide. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/ncss-good-practice-guide



Dėkojame!