Funded by the
Erasmus+ Programme
of the European Union

Kibernetinių atakų atpažinimas ir apsauga

Žalos sumažinimas pasinaudojant incidento valdymo planu

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

Mokymo tikslai

Paaiškinti reagavimo į incidentus planų kūrimą, rengimą ir įgyvendinimą.

Funded by the
Erasmus+ Programme
of the European Union

Studento darbo krūvis

Paskaitos	1.5 val.
Papildomi skaitiniai	4 val.
Pasiruošimas atsiskaitymui	0.5 val.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

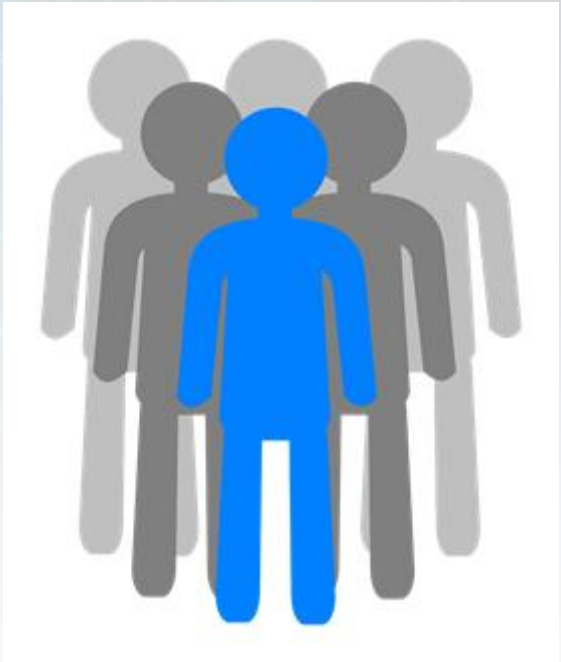
Turinys

- **Veiksmai žalai sumažinti**
- Veiksmai įvykus kibernetinei atakai
- Saugumo pažeidimo įvertinimas
- Kibernetinės atakos padarinių valdymas
- Reagavimas po incidento

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinio saugumo kultūros diegimas ir laikymasis organizacijoje

- Kibernetinio saugumo kultūros plėtojimo aspektai, kaip nustatyta EISP (Įmonės informacijos saugumo politikoje) ir atitinkamose papildomose politikose.
- Vadovai savo veiksmais turi aiškiai parodyti, kad kibernetinis saugumas yra itin svarbus organizacijos misijai.



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Sukurti oficialius komunikacijos kanalus

- Pranešimų apie problemas teikimo komunikacijos strategija
- Komunikavimo procedūros pranešant apie problemas
- Skubių pranešimų apie klaidas arba anomalijų aptikimo eskalavimo politika
- Bent du oficialūs kanalai kiekvienam iš pirmiau nurodytų atvejų
- Bendravimo su vidaus ir išorės suinteresuotomis šalimis ir atitinkamomis nacionalinėmis ar reguliavimo institucijomis strategija

Source: Cyber Security Incident Management Guide (2017)

Verslui svarbių aktyvų identifikavimas Vertinimas

Svarbu identifikuoti (inventorizuoti) turtą, kuris yra labai svarbus organizacijos gebėjimui vykdyti savo misiją.

- PAGRINDINĖS INFORMACINĖS SISTEMOS
  - kokios naudojamos informacinės sistemos ir kokie duomenys renkami
  - nustatyti galimus pažeidžiamumus ir grėsmes
- ĮMONĖS TINKLAI
  - Įmonėje naudojami tinklai
  - galimi tinklų pažeidžiamumai
- ĮMONĖS INFORMACIJA
  - kokie duomenys saugomi (t. y. privatūs duomenys, finansiniai duomenys, prisijungimo duomenys...)
  - su įmonės saugoma informacija susiję galimi pažeidžiamumai

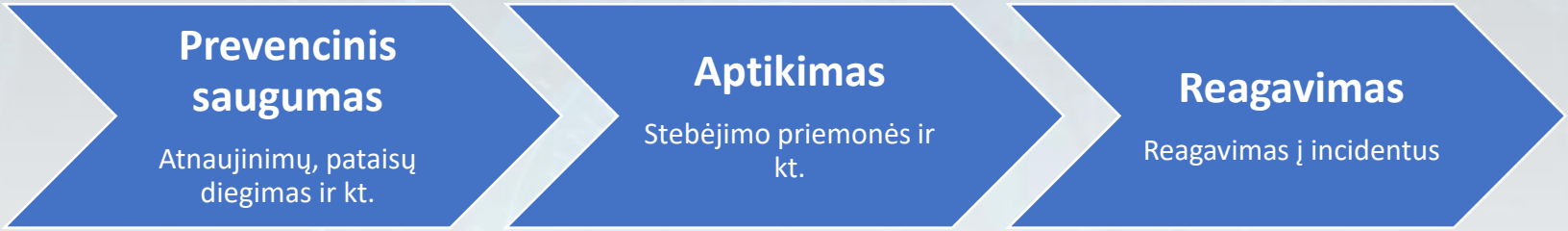
Metrikos ir veiksmingumo matavimas

- Atsakingas asmuo turi nustatyti reguliarių ataskaitų teikimo tvarkaraštį apie kibernetinio saugumo pažangą, rizikos švelninimą ir įvykdytus pokyčius.
- Politikoje turėtų būti apibrėžti atitinkami rodikliai, pagal kuriuos būtų vertinama kibernetinė situacija įmonėje.

Funded by the
Erasmus+ Programme
of the European Union

Saugumo tipai

- Skirtingi kibernetinio saugumo veiksmų lygiai:



Šaltinis: Japonijos ekonomikos, prekybos ir pramonės ministerijos kibernetinio saugumo gairės

- Aukščiausias saugumas bus pasiektas taikant aktyvias saugumo priemones, pavyzdžiui, didinant bendrą informuotumą apie kenkėjišką veiklą
- Visada turite žinoti, ką daryti kibernetinės atakos atveju
- Atminkite: net ir griežčiausios priemonės negali užtikrinti 100 proc. kibernetinio saugumo

Veiksmai žalai sumažinti

Pirmasis ir svarbiausias patarimas – mokymai, kurie užtikrins, kad visi darbuotojai pagal užimamas pareigas sugebėtų susidoroti su kibernetiniu incidentu.

- *1 žingsnis: nustatyti atakos tipą*
- *2 žingsnis: suvaldyti žalą*
- *3 žingsnis: informuoti nukentėjusias šalis*
- *4 žingsnis: analizuoti situaciją ir viską fiksuoti*
- *5 veiksmas: apsisaugoti nuo būsimų išpuolių*

Funded by the
Erasmus+ Programme
of the European Union

Turinys

- Veiksmai žalai sumažinti
- **Veiksmai įvykus kibernetinei atakai**
- Saugumo pažeidimo įvertinimas
- Kibernetinės atakos padarinių valdymas
- Reagavimas po incidento

Funded by the
Erasmus+ Programme
of the European Union

Veiksmai įvykus kibernetinei atakai

Čia bus pateikti pagrindiniai žingsniai, kuriuos reikia atlikti įvykus kibernetinei atakai

Funded by the
Erasmus+ Programme
of the European Union

Ką daryti, jei įvyksta kibernetinė ataka

- Jei jūs arba jūsų įmonė tapote duomenų pažeidimo auka, rekomenduojama atlikti žemiau nurodytus veiksmus, siekiant sumažinti žalą.

- Sustabdykite vykstančio/įvykusio kibernetinio saugumo pažeidimą
- Įvertinkite saugumo pažeidimo apimtį
- Valdykite vykstančią/įvykusią kibernetinę ataką
- Praneškite apie kibernetinį nusikaltimą

Funded by the Erasmus+ Programme of the European Union

Kibernetinio saugumo pažeidimo apribojimas

- Nepanikuokite!
- Pasistenkite išsiaiškinti situaciją: veikite greitai, bet ne skubotai!

- Atminkite:

  Nors įvykus duomenų saugumo pažeidimui gali kilti pagunda viską ištrinti, labai svarbu išsaugoti visus įrodymus siekiant įvertinti, kaip pažeidimas įvyko ir kas už jį atsakingas.

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinio saugumo pažeidimo apribojimas

- Štai keletas neatidėliotinų veiksmų, kuriuos galite ir privalote atlikti, kad užkirstumėte kelią duomenų saugumo pažeidimui:

- Atjunkite internetą
- Išjungti nuotolinę prieigą
- Išsaugokite ugniasienės nustatymus
- Įdiekite visus saugumo atnaujinimus ar pataisas
- Pakeiskite slaptažodžius

Funded by the Erasmus+ Programme of the European Union

Kibernetinio saugumo pažeidimo apribojimas

- *Jei dirbate komandoje, pateikiame keletą praktiko patarimų:*

- Pirmiausia suburkite veiklos tęstinumo komandą, į kurią įeitų IT ir duomenų ekspertai, ir paprašykite jų nustatyti pažeidžiamumo dydį ir apimtį.
- Tada apsaugokite fizines prieigas, kurios gali būti susijusios su pažeidimu.
- Nedelsiant pakeiskite visus prieigos leidimus.
- Užkirskite kelią bet kokiam papildomam duomenų praradimui, išjungdami visas paveiktas sistemas.

Funded by the Erasmus+ Programme of the European Union

Turinys

- Veiksmai žalai sumažinti
- Veiksmai įvykus kibernetinei atakai
- **Saugumo pažeidimo įvertinimas**
- Kibernetinės atakos padarinių valdymas
- Reagavimas po incidento

Funded by the
Erasmus+ Programme
of the European Union

Saugumo pažeidimo įvertinimas

Veiksniai, į kuriuos reikia atsižvelgti vertinant saugumo pažeidimą:

- Saugumas (priemonės, kurios turėjo būti įdiegtos),
- Ar tai liečia asmeninius duomenis,
- Pasekmės duomenų subjektams,
- Pažeidimo aplinkybės,
- Duomenų valdytojo tipas.

Funded by the Erasmus+ Programme of the European Union

Saugumo pažeidimo įvertinimas

Pabandykite atsakyti į kitus klausimus:

- Kaip prasidėjo ataka?
- Kas turėjo prieigą prie užkrėstų serverių?
- Kurie kompiuteriai buvo aktyvūs, kai įvyko pažeidimas?

Pavyzdžiui, galite nustatyti, kaip buvo pradėtas pažeidimas, patikrinę savo saugumo duomenų žurnalus per ugniasienę ar el. pašto paslaugų teikėjus, antivirusinę programą ar kitais būdais.

Gali tekti prašyti kibernetinio saugumo specialistų pagalbos.

Funded by the Erasmus+ Programme of the European Union

Saugumo pažeidimo įvertinimas

Identifikuokite 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 pažeidimas, nustatydami, prie kokios informacijos nusikaltėliai gavo prieigą, pavyzdžiui, gimtadieniai, el. pašto adresai, el. pašto paskyrų duomenys ir kredito kortelių numeriai.

Saugumo pažeidimo įvertinimas

Inicijuokite kibernetinės atakos protokolą:

- Darbuotojai turėtų žinoti jūsų įmonės politiką dėl duomenų saugumo pažeidimų.

- Nustatę pažeidimo priežastį, pakoreguokite savo saugumo protokolus ir praneškite apie juos, kad imkitės reikiamų priemonių, kad tokio pobūdžio incidentas nepasikartotų.

Funded by the
Erasmus+ Programme
of the European Union

Saugumo pažeidimo įvertinimas

Pildykite kibernetinės atakos protokolą:

- Nepamirškite ne tik skaitmeninių, bet ir fizinių saugumo priemonių, kad išvengtumėte naujų duomenų pažeidimų (fizinės prieigos prie įrenginio ar darbo vietos).

Funded by the
Erasmus+ Programme
of the European Union

Turinys

- Veiksmai žalai sumažinti
- Veiksmai įvykus kibernetinei atakai
- Saugumo pažeidimo įvertinimas
- **Kibernetinės atakos padarinių valdymas**
- Reagavimas po incidento

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinės atakos padarinių valdymas

Pateikiame pagrindines gaires, kaip išvengti kibernetinės atakos su mažiausiais nuostoliais

Funded by the
Erasmus+ Programme
of the European Union

Kibernetinės atakos padarinių valdymas

Jei ataka buvo įvykdyta prieš įmonę: praneškite apie pažeidimą vadovams ir darbuotojams, taip pat visiems kitiems asmenims, kuriems ataka gali turėti įtakos.

- Bendraukite su kolegomis ir praneškite jiems, kas nutiko.

- Apibrėžkite aiškius komandos narių įgaliojimus šiuo klausimu tiek viduje, tiek išorėje.

- Atsigaunant po duomenų saugumo pažeidimo labai svarbu palaikyti glaudų ryšį su komanda.

- Jums gali prireikti teisinės konsultacijos dėl teisinių incidento aspektų.

Kibernetinės atakos padarinių valdymas

Jei ataka buvo įvykdyta prieš įmonę: praneškite apie pažeidimą vadovams ir darbuotojams bei visiems kitiems asmenims, kuriems gali turėti įtakos ataka prieš jus.

- Jei esate apsidraudę atsakomybę už kibernetinius nusikaltimus, praneškite apie tai savo draudėjui.

- Kibernetinės atsakomybės draudimas skirtas padėti jums atsigauti po duomenų saugumo pažeidimo ar kibernetinio saugumo atakos.

- Kuo greičiau susisiekite su savo draudėjui ir sužinokite, kaip jis gali padėti jums, ką daryti po kibernetinės atakos.

Funded by the Erasmus+ Programme of the European Union

Kibernetinės atakos padarinių valdymas

Jei ataka buvo įvykdyta prieš įmonę: praneškite klientams

- Parodykite, kad žinote apie situaciją ir nieko neslepiate.

- Bendravimas gali būti raktas į teigiamų, profesionalių santykių su klientais palaikymą ir padėti sumažinti galimus nuostolius.

Funded by the
Erasmus+ Programme
of the European Union

Turinys

- Veiksmai žalai sumažinti
- Veiksmai įvykus kibernetinei atakai
- Saugumo pažeidimo įvertinimas
- Kibernetinės atakos padarinių valdymas
- **Reagavimas po incidento**

Funded by the
Erasmus+ Programme
of the European Union

Reagavimas po incidento

- Pasibaigus atakai, reikėtų išanalizuoti ir į veiksmų planą įtraukti per šį procesą įgytą patirtį.
- Jei įgyta patirtis nebus įtraukta į veiksmų planą, tai gali pasimiršti ir kitą kartą įvykus tokiai ar panašiai atakai, gali būti daromos tos pačios klaidos.
- Atminkite: laikas, sugaištas kaupiant įgytą patirtį ir koreguojant planus bei scenarijus, yra investicija, kuri atsipirks kitos krizės metu.

Funded by the Erasmus+ Programme of the European Union

Reagavimas po incidento

Išmoktų pamokų žurnalas:

- Kad nekartotumėte tų pačių klaidų, pildykite išmoktų pamokų žurnalą.
- Tai gali būti naudinga medžiaga naujiems darbuotojams ir sprendimus priimantiems asmenims dėl papildomo kibernetinio saugumo biudžeto.

Funded by the Erasmus+ Programme of the European Union

Santrauka

- Geriausias būdas sumažinti žalą – didinti bendrą informuotumą apie sukčiavimą.
- Reikia turėti planą, ką daryti kibernetinės atakos atveju.
- Įvertinkite saugumo pažeidimą.
- Veikite pagal vertinimo rezultatus.
- Pasimokykite iš atakos.

Funded by the Erasmus+ Programme of the European Union

Užduotys

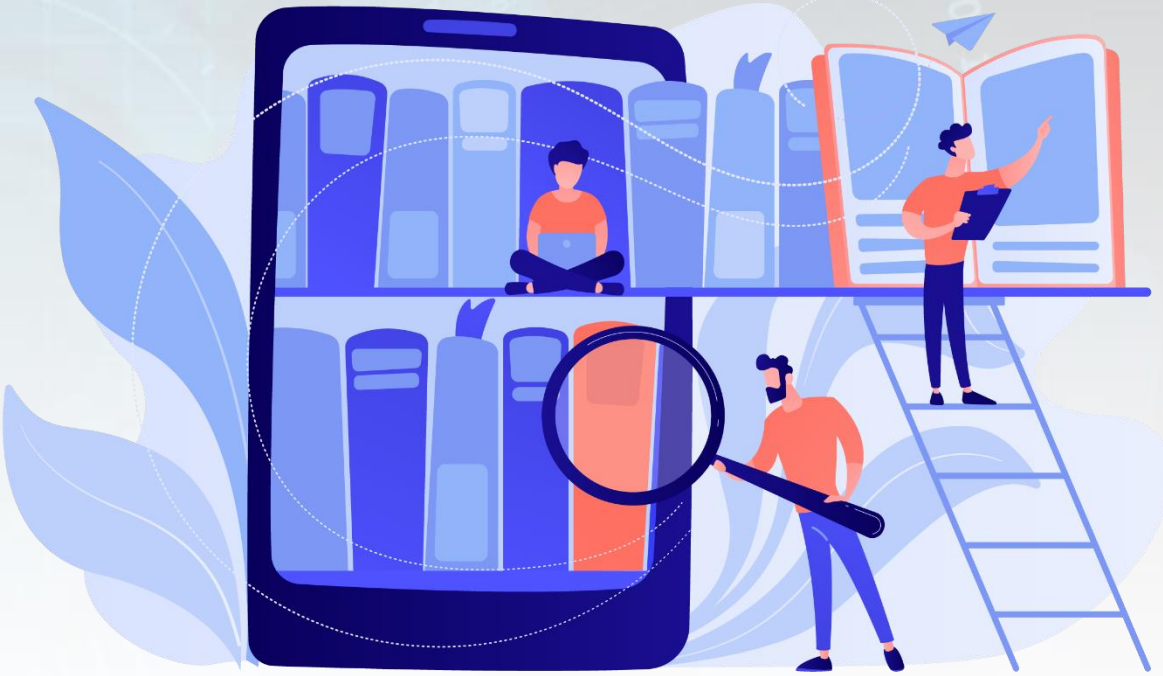
- *Tarkime, esate 10 darbuotojų komandos vadovas. Jūsų sistemų administratorius pastebėjo neįprastą serverio veiklą.*

- *Aprašykite savo neatidėliotinus veiksmus šioje situacijoje.*

Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

- Oguchi Kyohei, Yamazaki Teru, Yamane Masato. Incident Response Solution to Minimize Attack Damage. NEC Tech Reports, 2018
- George Grispos. On The Enhancement of Data Quality in Security Incident Response Investigations. Ph. D. Thesis, University of Glasgow, 2016



This Photo by Unknown Author is licensed under CC BY-NC

Dėkojame!