Funded by the
Erasmus+ Programme
of the European Union

Pārskats par kiberuzbrukumu izpratni un apiešanos ar tiem

Bojājumu mazināšana reaģēšanas uz incidentiem ietvaros

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

Apmācību mērķis

Izskaidrot incidentu reaģēšanas plānu izstrādi, attīstību un ieviešanu.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kursantu darba slodze

Lekcija	1,5 st.
Papildu lasīšana	4 st.
Sagatavošanās eksāmenam	0,5 st.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

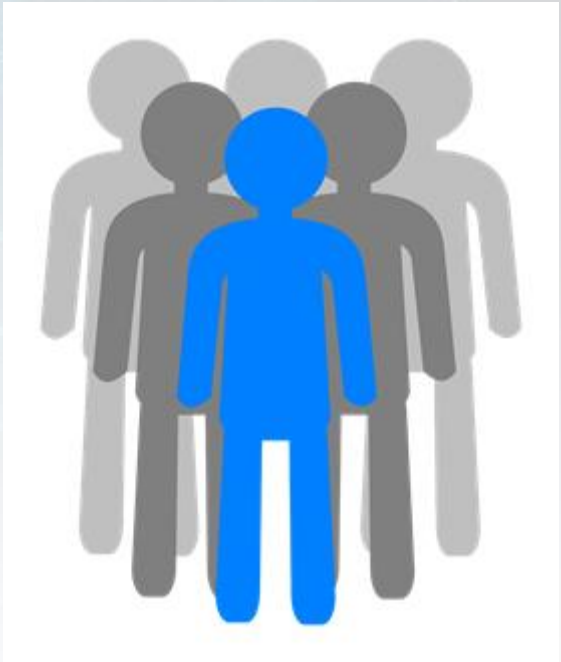
Saturs

- **Pasākumi, lai samazinātu bojājumus**
- Darbības pēc kiberuzbrukuma
- Novērtēt drošības pārkāpumu
- Pārvaldīt kiberuzbrukuma sekas
- Pēcnotikuma reakcija

Funded by the
Erasmus+ Programme
of the European Union

Ieviesiet un ievērojiet kiberdrošības kultūru organizācijā

- Kiberdrošības kultūras attīstības aspekti, kā noteikts EISP (uzņēmuma informācijas drošības politikā) un attiecīgajās papildu politikās.
- Līderiem ar savām darbībām ir skaidri jāparāda, ka kiberdrošība ir būtiska organizācijas misijai.



Funded by the Erasmus+ Programme of the European Union

Izveidojiet oficiālus saziņas kanālus

- Komunikācijas stratēģija problēmu ziņošanai
- Problēmu ziņošanas eskalācijas procedūras
- Eskalācijas politika steidzamai kļūdu ziņošanai vai anomāliju noteikšanai
- Vismaz divi formāli kanāli katram no iepriekš minētajiem gadījumiem
- Saziņas taktika ar iekšējām un ārējām ieinteresētajām personām/pusēm un visām attiecīgajām valsts vai regulatīvajām iestādēm

Avots: Kiberdrošības incidentu pārvaldības rokasgrāmata (2017)

Nosakiet uzņēmumam kritisko aktīvu novērtējumu

Nosakiet aktīvus, kas ir būtiski organizācijas spējai izpildīt savu misiju

- GALVENĀS INFORMĀCIJAS SISTĒMAS
  - sistēmas un savāktie dati
  - saistītās informācijas sistēmu ievainojamības
- UZŅĒMUMA TĪKLI
  - uzņēmumu tīkli
  - saistītās LAN ievainojamības
- INFORMĀCIJA UZŅĒMUMĀ
  - kādi dati tiek glabāti (t.i., PII, finanšu dati, akreditācijas dati utt.)
  - saistītās ievainojamības, kas saistītas ar informāciju uzņēmumā

Funded by the Erasmus+ Programme of the European Union

Metrika un izmērāmā efektivitāte

- Atbildīgajai personai ir jāizveido grafiks regulāras atgriezeniskās saites sniegšanai par kiberdrošības progresu, mazinātajiem riskiem un izmaiņām.
- Politikā būtu jādefinē atbilstoši rādītāji, pēc kuriem novērtēt uzlabojumus.

Drošības veidi

- Dažādi darbību līmeņi kiberdrošībā:

Attēls no Japānas Ekonomikas, tirdzniecības un rūpniecības ministrijas kiberdrošības vadlīnijām

- Atcerieties: augstākā drošība tiks sasniegta, izmantojot proaktīvus drošības pasākumus, piemēram, palielinot izpratni par pikšķerēšanu
- Taču vienmēr ir jāzina, kā rīkoties uzbrukuma un īpaši veiksmīga uzbrukuma gadījumā
- Atcerieties: pat visstingrākie pasākumi nevar garantēt 100% drošību

Funded by the Erasmus+ Programme of the European Union

Pasākumi, lai samazinātu bojājumus

Pirmais un svarīgākais padoms ir apmācība, kas nodrošinās, ka visi darbinieki atbilstoši ieņemamajam amatam spēs tikt galā ar šādu incidentu.

- *1. solis: Nosakiet uzbrukuma veidu*
- *2. solis: Nodrošiniet bojājumu neizplatību*
- *3. solis: Informējiet skartās puses*
- *4. solis: Izpētiet un ziņojiet*
- *5. solis: Aizsardzība pret turpmākiem uzbrukumiem*

Funded by the
Erasmus+ Programme
of the European Union

Saturs

- Pasākumi, lai samazinātu bojājumus
- **Darbības pēc kiberuzbrukuma**
- Novērtēt drošības pārkāpumu
- Pārvaldīt kiberuzbrukuma sekas
- Pēcnotikuma reakcija

Funded by the
Erasmus+ Programme
of the European Union

Darbības pēc kiberuzbrukuma

Šeit tiks parādīti galvenie soļi, kas jums jādara pēc kiberuzbrukuma (potenciāli veiksmīga)

Funded by the Erasmus+ Programme of the European Union

Ko darīt pēc kiberuzbrukuma

- Ja jūs vai jūsu uzņēmums esat cietis no datu pārkāpuma, incidenta vai uzbrukuma, veiciet tālāk norādītās darbības, lai palīdzētu samazināt kaitējumu:

- Ierobežojiet ciestā kiberdrošības pārkāpuma seku izplatību

- Novērtējiet drošības pārkāpumu

- Pārvaldiet kiberuzbrukuma sekas

- Ziņojiet par kibernoziegumu

Funded by the Erasmus+ Programme of the European Union

Ierobežojiet ciestā kiberdrošības pārkāpuma seku izplatību

- Neļaujieties panikai!
- Mēģiniet noskaidrot situāciju: rīkojieties ātri, bet ne drudžaini!

- Ievērojiet:

Lai gan jums var rasties kārdinājums dzēst visu pēc datu pārkāpuma, pierādījumu saglabāšana ir ļoti svarīga, lai novērtētu, kā noticis pārkāpums, un kurš ir bijis atbildīgs.

Funded by the Erasmus+ Programme of the European Union

Ierobežojiet ciestā kiberdrošības pārkāpuma seku izplatību

- Tālāk ir norādītas dažas tūlītējas darbības, kuras varat un kas jādara, lai mēģinātu ierobežot datu pārkāpumu un tā sekas.

- Atvienojiet internetu

- Atspējojiet attālo piekļuvi

- Saglabājiet savus ugunsmūra iestatījumus

- Instalējiet visus gaidošos drošības atjauninājumus vai ielāpus

- Nomainiet paroles

Funded by the Erasmus+ Programme of the European Union

Ierobežojiet ciestā kiberdrošības pārkāpuma seku izplatību

- *Ja strādājat komandā, daži praktiķa ieteikumi:*

- Pirmkārt, izveidojiet darbības nepārtrauktības komandu, tostarp IT un datu kriminālistikas ekspertus, un lieciet viņiem noteikt ievainojamības lielumu un apjomu,
- Pēc tam nodrošiniet fiziskās zonas, kas varētu būt saistītas ar pārkāpumu
- Nekavējoties nomainiet visas piekļuves atļaujas.
- Apturiet jebkādu papildu datu zudumu, pārslēdzot visas ietekmētās sistēmas bezsaistē

Funded by the Erasmus+ Programme of the European Union

Saturs

- Pasākumi, lai samazinātu bojājumus
- Darbības pēc kiberuzbrukuma
- ***Novērtēt drošības pārkāpumu***
- Pārvaldīt kiberuzbrukuma sekas
- Pēcnotikuma reakcija

Funded by the
Erasmus+ Programme
of the European Union

Novērtējiet drošības pārkāpumu

Faktori, kas jāņem vērā, novērtējot drošības pārkāpumu:

- Drošība (pasākumi, kuriem bija jābūt ieviestiem),
- Iesaistītie personas dati,
- Izrietošās sekas datu subjektiem,
- Pārkāpuma apstākļi,
- Kontroliera tips.

Funded by the
Erasmus+ Programme
of the European Union

Novērtējiet drošības pārkāpumu

Mēģiniet atbildēt uz šādiem jautājumiem:

- Kā tika uzsākts uzbrukums?
- Kam bija piekļuve inficētajiem serveriem?
- Kuri datori bija aktīvi, kad notika pārkāpums?

- Piemēram, jūs varat precīzi noteikt, kā tika uzsākts pārkāpums vai uzbrukums, pārbaudot drošības datu žurnālus (reģistrācijas failus), izmantojot ugunsmūri vai e-pasta pakalpojumu sniedzējus, pretvīrusu programmu vai citā veidā.
- Iespējams, jums būs jālūdz kiberdrošības speciālistu atbalsts.

Funded by the Erasmus+ Programme of the European Union

Novērtējiet drošības pārkāpumu

Nosakiet personas, kuras ietekmējis pārkāpums:

- Ir ļoti svarīgi noskaidrot, kuras personas, iespējams, ir ietekmējis pārkāpums, tostarp jūsu darbiniekus, klientus un trešo pušu pārdevējus/piegādātājus.

- Novērtējiet, cik nopietns bija datu pārkāpums, nosakot, kādai informācijai tika piekļūts vai kāda informācija tika izvēlēta (atlasīta), piemēram, dzimšanas dienas, pasta adreses, e-pasta konti un kredītkaršu numuri.

Funded by the Erasmus+ Programme of the European Union

Novērtējiet drošības pārkāpumu

Uzsāciet savu kiberuzbrukuma protokolu:

- Jūsu darbiniekiem ir jāzina jūsu politika attiecībā uz datu pārkāpumiem.
- Pēc pārkāpuma iemesla noteikšanas pielāgojiet un paziņojiet savus drošības protokolus, lai nodrošinātu, ka neatkārtojas tāda paša veida incidenti..

Funded by the Erasmus+ Programme of the European Union

Novērtējiet drošības pārkāpumu

Uzsāciet savu kiberuzbrukuma protokolu:

- Paturiet prātā ne tikai digitālos, bet arī fiziskos drošības pasākumus, lai izvairītos no jauniem datu pārkāpumiem (fiziska piekļuve ierīcēm vai darba vietai).

Funded by the Erasmus+ Programme of the European Union

Saturs

- Pasākumi, lai samazinātu bojājumus
- Darbības pēc kiberuzbrukuma
- *Novērtēt drošības pārkāpumu*
- **Pārvaldīt kiberuzbrukuma sekas**
- Pēcnotikuma reakcija

Funded by the
Erasmus+ Programme
of the European Union

Kiberuzbrukuma radīto zaudējumu un seku pārvaldīšana

Šeit ir sniegtas galvenās vadlīnijas, kā izkļūt no kiberuzbrukuma ar minimāliem zaudējumiem

Funded by the Erasmus+ Programme of the European Union

Kiberuzbrukuma radīto zaudējumu un seku pārvaldīšana

Ja uzbrukums bija uzņēmumam: paziņojiet par pārkāpumu vadītājiem un darbiniekiem, kā arī visiem citiem, kurus var ietekmēt uzbrukums.

- *Sazinieties ar saviem kolēģiem, lai viņi zinātu, kas noticis.*
- *Definējiet komandas locekļiem skaidras pilnvaras par šo problēmu gan iekšēji, gan ārēji.*
- *Atkopjoties no datu pārkāpuma, ir ļoti svarīgi uzturēt ciešu kontaktu ar savu komandu.*
- *Jums var būt nepieciešama juridiska konsultācija par incidenta juridiskiem aspektiem.*

Funded by the Erasmus+ Programme of the European Union

Kiberuzbrukuma radīto zaudējumu un seku pārvaldīšana

Ja uzbrukums bija uzņēmumam: paziņojiet par pārkāpumu vadītājiem un darbiniekiem, kā arī visiem citiem, kurus var ietekmēt uzbrukums jums.

- Ja jums ir kiberatbildības apdrošināšana, informējiet savu apdrošināšanu.

- Kiberatbildības apdrošināšana ir paredzēta, lai palīdzētu jums atgūties pēc datu pārkāpuma vai kiberdrošības uzbrukuma.

- Sazinieties ar savu mobilo sakaru operatoru, cik drīz vien iespējams, lai uzzinātu, kā viņš var jums palīdzēt noteikt, kā rīkoties pēc kiberuzbrukuma.

Funded by the Erasmus+ Programme of the European Union

Kiberuzbrukuma radīto zaudējumu un seku pārvaldīšana

Ja uzbrukums bija uzņēmumam: Informējiet klientus

- Uzsveriet savu vēlmi būt caurspīdīgam

- Saziņa var būt galvenais faktors, lai uzturētu pozitīvas, profesionālas attiecības ar saviem klientiem un var samazināt iespējamos zaudējumus.

Funded by the Erasmus+ Programme of the European Union

Pēcnotikuma reakcija

- Pasākumi, lai samazinātu bojājumus
- Darbības pēc kiberuzbrukuma
- Novērtēt drošības pārkāpumu
- Pārvaldīt kiberuzbrukuma sekas
- **Pēcnotikuma reakcija**

Funded by the
Erasmus+ Programme
of the European Union

Pēcnotikuma reakcija

- Kad uzbrukums ir beidzies, procesa gaitā gūtās mācības ir jāanalizē un jāiekļauj rīcības plānā.
- Tas ir ļoti svarīgi, un to nevajadzētu aizmirst, jo ir tendence ātri aizmirst incidentu.
- Atcerieties: laiks, kas pavadīts gūto mācību apkopošanai un plānu un scenāriju koriģēšanai, ir ieguldījums, kas atmaksāsies nākamajā krīzē.

Funded by the Erasmus+ Programme of the European Union

Pēcnotikuma reakcija

Apgūto mācību uzskaites žurnāls:

- Pierakstiet gūto pieredzi, lai neatkārtotu tās pašas kļūdas.
- Tas varētu būt noderīgs materiāls jaunajiem darbiniekiem un lēmumu pieņēmējiem papildu kiberdrošības budžetam.

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums

- Labākais veids, kā samazināt kaitējumu, ir palielināt vispārējo izpratni par pikšķerēšanu.
- Jums ir jāizstrādā plāns, kā rīkoties kiberuzbrukuma gadījumā.
- Novērtējiet drošības pārkāpumu
- Rīkojieties saskaņā ar novērtējuma rezultātiem.
- Gūstiet mācību no uzbrukuma.

Uzdevums

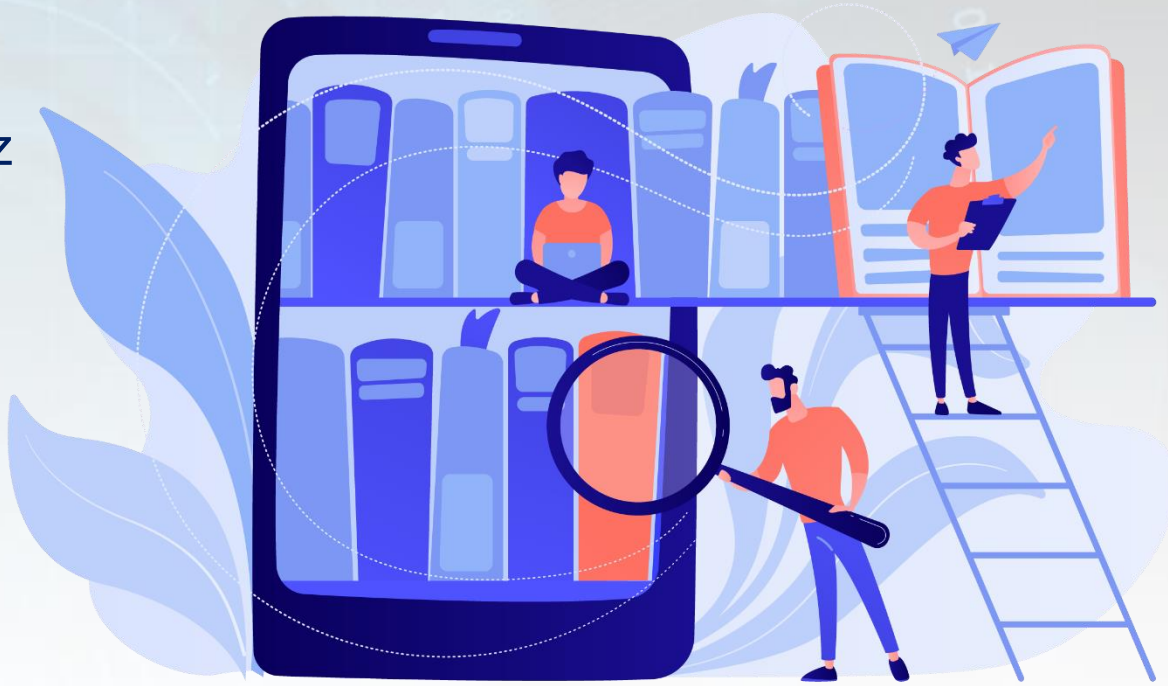
- *Jūs esat 10 darbinieku komandas vadītājs. Jūsu sistēmas administrators novēroja neparastas darbības serverī.*

- *Aprakstiet savas tūlītējās darbības attiecīgajā situācijā.*

Funded by the Erasmus+ Programme of the European Union

Papildu lasīšana

- Oguči Kjohejs *[Oguchi Kyohei]*, Jamazaki Teru *[Yamazaki Teru]*, Jamane Masato *[Yamane Masato]*. Risinājums reaģēšanai uz incidentiem, lai samazinātu uzbrukuma radītos bojājumus. NEC Tehniskie ziņojumi, 2018. gads
- Džordžs Grisposs *[George Grispos]*. Par datu kvalitātes uzlabošanu drošības incidentu reaģēšanas izmeklēšanā. Ph. D. tēzes, University of Glasgow, 2016. gads



Funded by the Erasmus+ Programme of the European Union

Pateicamies!