Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Kahjude minimeerimine juhtumitele reageerimise kaudu

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

Õppe-eesmärgid

Selgitada intsidentidele reageerimise plaanide koostamise, väljatöötamise ja rakendamise põhimõtteid.

Funded by the Erasmus+ Programme of the European Union

Õpilase töökoormus

Loengud	1.5 h
Lisalugemine	4 h
Eksamiks valmistumine	0.5 h

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

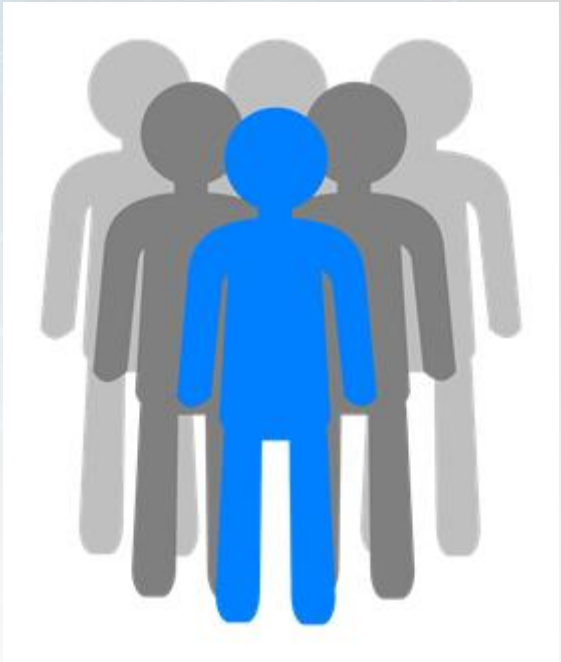
Loenguteemad

- **Meetmed kahju minimeerimiseks**
- Toimingud pärast küberrünnakut
- Turvarikkumise mõju hindamine
- Küberrünnaku tagajärgede likvideerimine
- Juhtumijärgne analüüs

Funded by the
Erasmus+ Programme
of the European Union

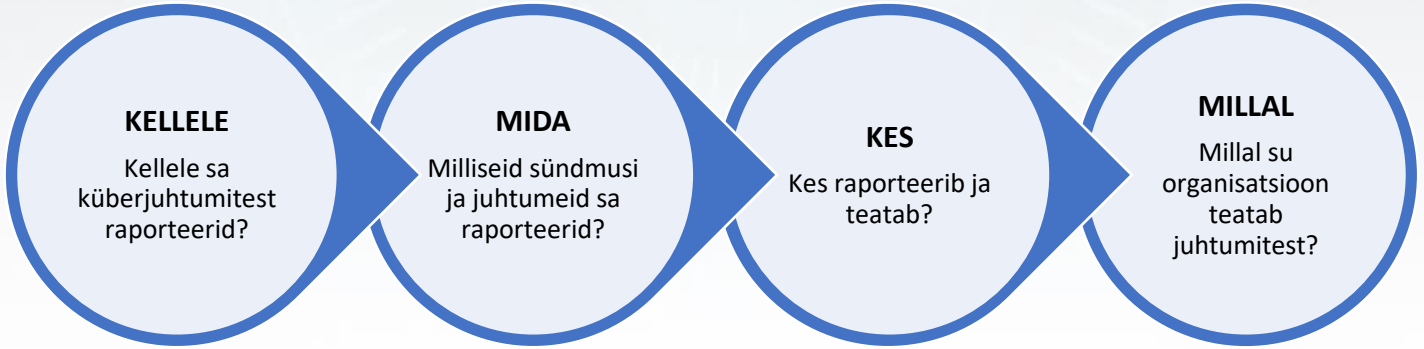
Rakendage ja järgige organisatsioonis küberjulgeolekukultuuri

- Küberturbekultuuri arendamise aspektid, nagu on sätestatud EISP-s (Ettevõtte teabeturbepoliitika) ja asjakohastes täiendavates poliitikates.
- Juhid peavad oma tegevusega selgelt näitama, et küberturvalisus on organisatsiooni missiooni jaoks ülioluline.



Looge ametlikud suhtluskanalid

- Suhtlusstrateegia probleemidest teatamiseks
- Probleemidest teatamise eskalatsiooniprotseduurid
- Eskalatsioonipoliitika kiireloomuliseks veateavitamiseks või anomaaliate tuvastamiseks
- Vähemalt kaks ametlikku kanalit iga ülaltoodud juhtumi jaoks
- Sisemiste ja väliste sidusrühmade ning asjakohaste riiklike või reguleerivate asutustega suhtlemise taktika.



Source: Cyber Security Incident Management Guide (2017)

Tehke kindlaks ärikriitilised varad

Tehke kindlaks varad, mis on organisatsiooni võime jaoks oma missiooni täitmiseks hädavajalikud

- PEAMISED INFOSÜSTEEMID
  - süsteemid ja klientide (kaupade) andmed
  - seotud infosüsteemide haavatavused
- ETTEVÕTTE SIDEVÕRK
  - ettevõtete võrgud
  - LAN-ide seotud haavatavused
- ETTEVÕTTE TOIMISE INFORMATSIOON
  - milliseid andmeid salvestatakse (nt isikut tõendavad andmed, finantsandmed, mandaadid jne)
  - ettevõtte teabega seotud haavatavused

Funded by the Erasmus+ Programme of the European Union

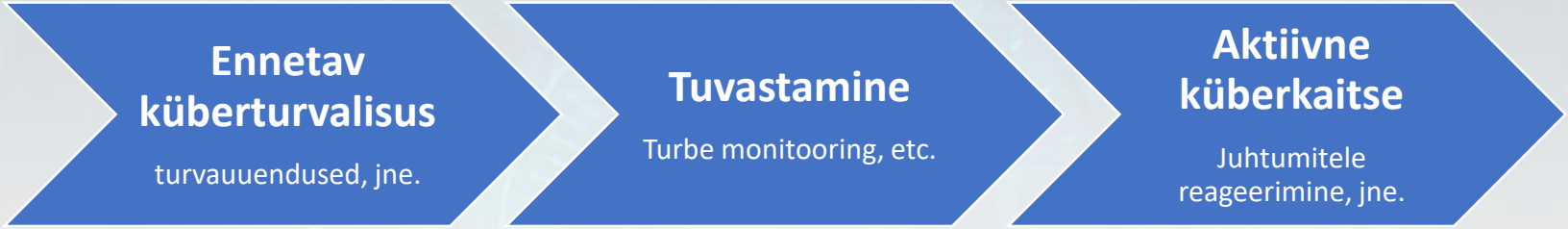
Mõõdikud ja mõõdetav tõhusus

- Vastutav isik peab koostama ajakava küberturvalisuse edenemise, maandatud riskide ja muudatuste kohta regulaarse tagasiside andmiseks.
- Poliitika peaks määratlema asjakohased näitajad, mille alusel paranemist mõõta.

Funded by the
Erasmus+ Programme
of the European Union

Security Types

- Erinevad küberturvalisuse toimingud:



Joonis pärineb: Japanese Ministry of Economy, Trade and Industry Cybersecurity Guidelines

- Pidage meeles: kõrgeim turvalisus saavutatakse ennetavate turvameetmetega, nagu üldise andmepüügiteadlikkuse tõstmine.
- Kuid rünnaku ja eriti eduka rünnaku korral peate alati teadma, mida teha.
- Pidage meeles: isegi kõige karmimad meetmed ei taga 100% turvalisust.

Funded by the Erasmus+ Programme of the European Union

Sammud kahju minimeerimiseks

Esimene ja kõige olulisem näpunäide on koolitus, mis tagab, et kõik töötajad saavad vastavalt oma ametikohtadele sellise juhtumiga hakkama.

- *1. samm: tuvastage rünnaku tüüp*
- *2. samm: piirake kahjustusi*
- *3. samm: teavitage mõjutatud pooli*
- *4. samm: uurige ja teatage*
- *5. samm: kaitske tulevaste rünnakute eest*

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

- Meetmed kahju minimeerimiseks
- **Toimingud pärast küberrünnakut**
- Turvarikkumise mõju hindamine
- Küberrünnaku tagajärgede likvideerimine
- Juhtumijärgne analüüs

Funded by the
Erasmus+ Programme
of the European Union

Tegevused pärast küberrünnakut

Järgnevalt on toodud peamised sammud, mida peate tegema pärast küberrünnaku ohvriks sattumist.

Funded by the
Erasmus+ Programme
of the European Union

Mida teha pärast küberrünnakut

- Kui teie või teie ettevõte langeb andmetega seotud rikkumise ohvriks, järgige kahju minimeerimiseks järgmisi samme.

- Piirake küberturründe mõjusid
- Hinnake turvarikkumise mõjusid
- Hallake oma küberrünnakust tulenevat äri (käibe) langust
- Raporteerige küberkuritegevusest (juhtumitest)

Funded by the Erasmus+ Programme of the European Union

Piirake küberturründe mõjusid

- Ära paanitse !
- Proovige olukorda selgitada: tegutsege ruttu, kuid mitte kiiresti!

- Pidage meeles:

Ehkki teil võib tekkida kiusatus pärast andmetega seotud rikkumise toimumist kõik kustutada, on tõendite säilitamine ülioluline, et hinnata, kuidas rikkumine juhtus ja kes vastutas.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumise mõjusid

- Siin on mõned kohesed toimingud, mida saate ja peate tegema, et püüda piirata andmetega seotud rikkumist.

- Katkestage Interneti-ühendus
- Keela kaugjuurdepääs
- Säilitage oma tulemüüri sätted
- Installige kõik ootel olevad turvavärskendused või paigad
- Muutke paroole

Funded by the Erasmus+ Programme of the European Union

Hallake oma küberrünnakust tulenevat äri (käibe) langust

- Kui töötate meeskonnas, mõned praktiku soovitused:
- Esiteks pange kokku talitluspidevuse meeskond, kuhu kuuluvad IT- ja andmeekspertiisi eksperdid, ning laske neil määrata haavatavuse suurus ja ulatus.
- Seejärel kaitske füüsilised alad, mis võivad olla rikkumisega seotud.
- Muutke kohe kõiki juurdepääsuõigusi.
- Peatage igasugune täiendav andmete kadu, lülitades kõik mõjutatud süsteemid võrguühenduseta.

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

- Meetmed kahju minimeerimiseks
- Toimingud pärast küberrünnakut
- **Turvarikkumise mõju hindamine**
- Küberrünnaku tagajärgede likvideerimine
- Juhtumijärgne analüüs

Funded by the
Erasmus+ Programme
of the European Union

Hinnake turvarikkumist

Tegurid, mida turvarikkumise hindamisel arvesse võtta:

- Turvalisus (meetmed, mis pidid olema paigas),
- Asjaomased isikuandmed,
- Tagajärjed andmesubjektidele,
- Rikkumise asjaolud,
- Kontrolleri tüüp.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

Proovige vastata järgmistele küsimustele:

- Kuidas rünnak algas?
- Kellel oli juurdepääs nakatunud serveritele?
- Millised arvutid olid rikkumise toimumise ajal aktiivsed?

Näiteks võite olla võimeline tuvastama, kuidas rikkumine algatati, kontrollides oma turvaandmete logisid tulemüüri või meiliteenuse pakkujate, viirusetõrjeprogrammi või muul viisil.

Võimalik, et peate küsima abi küberturvalisuse spetsialistidelt.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

Tehke kindlaks need, keda rikkumine mõjutab:

- Väga oluline on välja selgitada, keda rikkumine võis mõjutada, sealhulgas teie töötajaid, kliente ja kolmandatest osapooltest tarnijaid.

- Hinnake andmete rikkumise tõsidust, leides, millist teavet kasutati või millist teavet sihiti (nt sünnipäevad, postiaadressid, e-posti kontod ja krediitkaardinumbrid).

Hinnake turvarikkumist

Käivitage oma küberrünnaku protokoll:

- Teie töötajad peaksid olema teadlikud teie andmetega seotud rikkumiste eeskirjadest.

- Pärast rikkumise põhjuse avastamist kohandage ja edastage oma turvaprotokolle, et tagada sama tüüpi intsidentide kordumine.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

Käivitage oma küberrünnaku protokoll:

- Pidage meeles mitte ainult digitaalseid, vaid ka füüsilisi turvameetmeid, et vältida uut andme lekkimist (füüsiline juurdepääs seadmele või töökohale).

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

- Meetmed kahju minimeerimiseks
- Toimingud pärast küberrünnakut
- Turvarikkumise mõju hindamine
- **Küberrünnaku tagajärgede likvideerimine**
- Juhtumijärgne analüüs

Funded by the
Erasmus+ Programme
of the European Union

Küberrünnaku tagajärgede likvideerimine

Siin on peamised juhised, kuidas küberrünnakust minimaalsete kaotustega väljuda.

Funded by the Erasmus+ Programme of the European Union

Küberrünnaku tagajärgede likvideerimine

Kui rünnak oli ettevõtte vastu: teavitage rikkumisest juhte ja töötajaid ning kõiki teisi, keda rünnak mõjutada võis

- Suhelge oma kolleegidega, et anda neile juhtunust teada.

- Määrake meeskonnaliikmetele selged volitused selles küsimuses nii sisemiselt kui ka väliselt.

- Andmerikkumisest taastumisel on meeskonnaga tihedas kontaktis püsimine ülioluline.

- Võimalik, et vajate õigusnõu intsidendi õiguslike aspektide kohta

Funded by the Erasmus+ Programme of the European Union

Küberrünnaku tagajärgede likvideerimine

Kui rünnak oli ettevõtte vastu: teavitage rikkumisest juhte ja töötajaid ning kõiki teisi, keda teie vastu suunatud rünnak mõjutada võib.

- Kui teil on kübervastutuskindlustus, teavitage sellest oma partnerit.

- Kübervastutuskindlustus on loodud selleks, et aidata teil taastuda andmete rikkumisest või küberturvalisuse rünnakust.

- Võtke esimesel võimalusel ühendust oma operaatoriga, et näha, kuidas ta saab teid aidata küberrünnaku järel tegutsemisel.

Küberrünnaku tagajärgede likvideerimine

Kui rünnak oli ettevõtte vastu: teavitage kliente

- Rõhutage oma valmisolekut olla läbipaistev

- Suhtlemine võib olla võti klientidega positiivsete ja professionaalsete suhete hoidmisel ja võimalike kahjude minimeerimisel.

Funded by the Erasmus+ Programme of the European Union

Loenguteemad

- Meetmed kahju minimeerimiseks
- Toimingud pärast küberrünnakut
- Turvarikkumise mõju hindamine
- Küberrünnaku tagajärgede likvideerimine
- **Juhtumijärgne analüüs**

Funded by the
Erasmus+ Programme
of the European Union

Juhtumijärgne analüüs

- Kui rünnak on lõppenud, tuleks protsessi käigus tuvastatud õppetunde analüüsida ja tegevuskavasse lisada.
- See on väga oluline ja seda ei tohiks unustada, kuna kipub juhtum kiiresti unustama.
- Pidage meeles: õppetundide kogumisele ning plaanide ja stsenaariumide kohandamisele kulutatud aeg on investeering, mis tasub end ära järgmises kriisis.

Funded by the Erasmus+ Programme of the European Union

Juhtumijärgne analüüs

Õppetundide logi:

Pidage oma õppetundidest dokumentatsiooni, et mitte korrata samu vigu.

See võib olla kasulik materjal uutele töötajatele ja otsustajatele täiendava küberturvalisuse eelarve jaoks.

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

- Parim viis kahju minimeerimiseks on tõsta üldist teadlikkust andmepüügist.
- Sul peab olema plaan, mida küberrünnaku korral teha.
- Hinnake turvarikkumise mõju.
- Toimige vastavalt hindamistulemustele.
- Õppige rünnakust.

Funded by the Erasmus+ Programme of the European Union

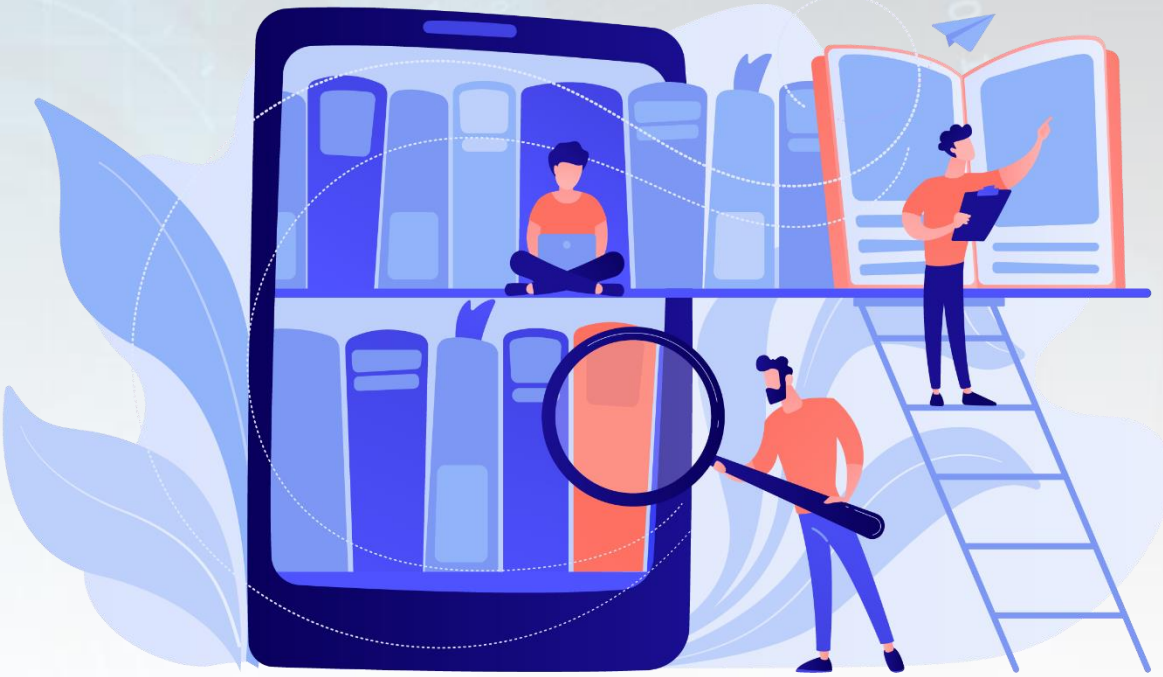
Ülesanne

- *Oled 10 töötajaga meeskonna juht. Teie süsteemiadministraator täheldas serveris ebatavalisi tegevusi.*

- *Kirjeldage oma viivitamatuid tegevusi olukorras.*

Lisalugemine

- 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



Tänan kuulamast!