Funded by the
Erasmus+ Programme
of the European Union

Küberturvalisuse sissejuhatus

Küberturvalisuse mõisted

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

Saada tuttavaks küberturvalisuse mõistega

Mis on küberturvalisus

Mis on küberrünnak

Õpilase töökoormus

Loengud	0.5 h
Lisalugemine	4 h
Eksamiks valmistumine	1 h

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Cyberspace
Küberruumi määratlus

- Kõigepealt peame määratlema, mis on küberruum.
- Populaarse määratluse pakub NIST:

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers

Source: https://csrc.nist.gov/glossary/term/cyberspace

- *Sõna pärineb William Gibsoni romaanist "Neuromancer" (1984) ja seda kasutatakse praegu kogu selle informatsiooni tähistamiseks, mis on saadaval arvutivõrkude kaudu (vallaste.ee)*

Funded by the Erasmus+ Programme of the European Union

Cybersecurity
Küberturvalisus ehk Infoturve?

- Viimastel aastatel on „küberturvalisus” muutunud laialdaselt kasutatavaks terminiks, mida nii praktikud kui ka avalikkus on laialdasemalt kasutusele võtnud.
- Kuid nagu paljude moes nähtuste puhul, pole küberturvalisuse täpne määratlus nii selge.
- Nt. 2000. aastate alguses kasutati selles kontekstis regulaarselt termineid "arvutiturve", "IT-turvalisus" või "teabeturve".

- Mõiste küberturvalisus sai nii populaarseks alles 2010. aastatel.

Funded by the Erasmus+ Programme of the European Union

Cybersecurity
Küberturvalisus ehk Infoturve?

- Küberjulgeoleku mõiste kasvavat populaarsust seostatakse sageli USA presidendi **Barack Obamaga**.
- 2009. aastal kuulutas Barack Obama: "Kutsun Ameerika Ühendriikide elanikke üles tunnistama küberjulgeoleku tähtsust ja jälgima seda kuud asjakohaste tegevuste, sündmuste ja koolitustega, et suurendada meie rahvuslikku julgeolekut ja vastupidavust" (https://obamawhitehouse. archives.gov/the-press-office/presidentential-proclamation-national-cybersecurity-awareness-month).

- "Küberturvalisus" on palju enamat kui "arvutiturve"

Funded by the Erasmus+ Programme of the European Union

Küberturvalisuse definitsioon

Tööstuse definitsioon inglese keeles:

Cyber security is set of security practices related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems.

Cyber security is superset of security practices such as information security, IT security and other related practices.

Source: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

Küberturvalisus on turvapraktikate kogum, mis on seotud ründavate ja kaitsvate tegevuste kombinatsiooniga, mis hõlmavad või toetuvad infotehnoloogia- ja/või käitlustehnoloogia keskkonda ja süsteeme.

Küberturve on turbepraktikate, nagu infoturve, IT-turvalisus ja muud sellega seotud praktikad, üldistav komplekt.

Funded by the Erasmus+ Programme of the European Union

Küberturvalisuse definitsioon

Akadeemiline definitsioon inglese keeles

Cybersecurity is the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection in cyber space.

Source: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

infoturve, andmeturve, turvalisus - andmete kaitstus käideldavuse, tervikluse või konfidentsiaalsuse rikkumise eest arvutites, arvutivõrkudes ja sidesüsteemides. Tavaliselt eeldab turvalisuse tagamine andmete krüpteerimist ja paroolide kasutamist (vallaste.ee)

Funded by the Erasmus+ Programme of the European Union

Mis on küberrünnak / *Cyber Attack?*

- Küberturvalisus on tihedalt seotud küberohtudega.
- NISTi populaarne määratlus:

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Source: https://csrc.nist.gov/glossary/term/cyber_attack

Rünnak küberruumi kaudu, mis kasutab ära ettevõtte küberruumis tegutsemist, et häirida, keelata, hävitada või pahatahtlikult juhtida arvutikeskkonda/taristut; või andmete terviklikkuse hävitamine või kontrollitud teabe varastamine

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute näited

- **Malware -** Pahavara kirjeldab pahatahtlikku tarkvara, sealhulgas nuhkvara, lunavara, viiruseid ja usse. See rikub võrku teatud tüüpi haavatavuse kaudu. Kõige sagedamini klõpsates ohtlikul lingil või meilimanusel riskantse tarkvaraga.
- **Phishing** - Andmepüük tähendab petturliku teabe saatmist. Eesmärk on simuleerida usaldusväärsest allikast tulemist. Tavaliselt saadetakse meili teel. Eesmärk on varastada tundlikke andmeid, nagu sisselogimisandmed, või installida ohvri masinasse pahavara.
- **Man-in-the-middle (MitM)** rünnakud ehk pealtkuulamisrünnakud või vahendusründed toimuvad siis, kui ründajad sisestavad end kahe osapoole tehingusse.

Küberrünnakute näited

- **A denial-of-service attack -** Teenuse keelamise rünnaku eesmärk on arvuti- ja võrguressursid tarbetu liiklusega üle koormata. Selle tulemusena ei suuda süsteem õigeid taotlusi täita ja teenust pakkuda.
- **A Structured Query Language (SQL) injection -** Struktureeritud päringukeele (SQL) rünne toimub pahatahtliku koodi sisestamisel serverisse SQL-i abil. Eesmärk on avaldada teavet, mida tavaliselt ei avaldata.
- **DNS tunneling** DNS-tunneldamine DNS-protokolli abil mitte-DNS-liikluse edastamiseks
- **A zero-day exploit** Nullpäeva turvaaugu ärakasutamine on haavatavuse ärakasutamine, kui see leiti ja sellest teatati, kuid seda siiski ei parandatud. Ründajad, kes kasutavad selle ajavahemiku haavatavuse kohta teavet.

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute näited

- Erinevat tüüpi küberrünnakud võivad nõuda erinevaid toiminguid.

- Mõned küberrünnakud võivad vajada sügavaid tehnilisi teadmisi.
- Osa küberrünnakutest võib ära kasutada inimese psühholoogiat ja manipuleerimisi.

- **Pidage meeles**: küberahela nõrgim element on inimene.

Funded by the Erasmus+ Programme of the European Union

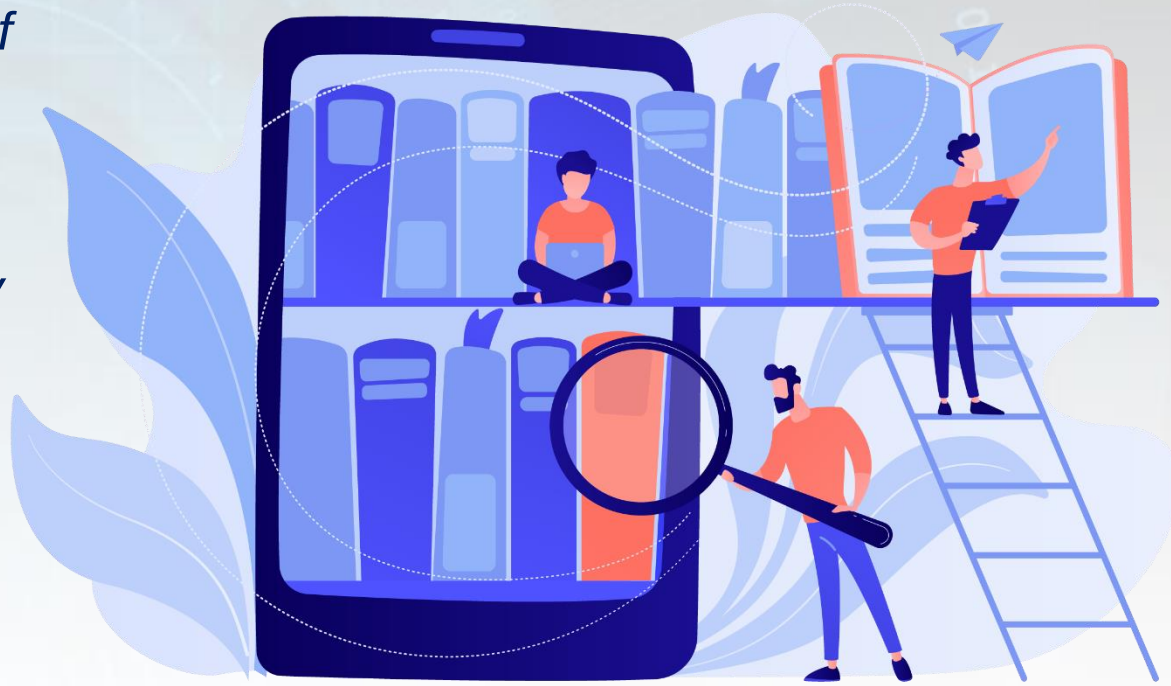
Küberrünnakute näited

- ***Email phishing***: Andmepüük e-posti teel: kõige populaarsem andmepüügi viis. Pettur kasutab võltsdomeeni, mis sarnaneb olemasoleva ja usaldusväärse organisatsiooni omaga, mis jäljendab ehtsat organisatsiooni ja saadab palju taotlusi.
- ***Spear phishing***: Andmepüük: konkreetsele inimesele saadetud pahatahtlikud meilid, mis on tavaliselt suure väärtusega sihtmärgiks. Ründajad koguvad tavaliselt ohvri kohta teavet.
- ***Whaling attacks*** Vaalapüügi rünnakud on veelgi sihipärasemad, võttes sihikule tippjuhid.
- ***Smishing and vishing***: telefone kasutatakse e-posti asemel peamise ründeviisina. Smishing hõlmab tekstisõnumeid, näiteks SMS-i, samas kui vishing toimub suulise vestluse kaudu.
- ***Angler phishing:*** Andmepüügi õngitseja: sotsiaalmeedia võimalusi kasutatakse inimeste veenmiseks tundlikku teavet avaldama või pahavara alla laadima. Kasutada võib ka andmeid, mida inimesed sotsiaalmeediasse postitavad täpselt sihitud rünnakute loomiseks.

Funded by the Erasmus+ Programme of the European Union

Lisalugemine

- *Daniel Schatz, Rabih Bashroush, Julie Wall. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law. Number 2, volume 12, 2017*
- *Dan Craigen, Nadia Diakun-Thibault, Randy Purse. Defining Cybersecurity. Technology Innovation Management Review. Number 4, volume 10, 2014*
- *Defining Cybersecurity. Emerging technologies and problem definition uncertainty: The case of cybersecurity. Regulation @ Governance, July 2020*



Tänan kuulamast!