Funded by the
Erasmus+ Programme
of the European Union

Sissejuhatus küberturvalisusesse

Küberturvalisuse ajalugu

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

Anda lühike ülevaade selle kohta, kuidas küberrünnakute lähenemisviisid on aja jooksul muutunud, mis on suurendanud ohtusid ja seega ka küberrünnakute vastaseid vastumeetmeid.

Õpilase töökoormus

Loengud	1 h
Audio- ja videomaterjal	1 h
Juhtumiuuringud	1 h
Lisalugemine	2 h
Eksamiks valmistumine	1 h

Funded by the Erasmus+ Programme of the European Union

Areng

Funded by the Erasmus+ Programme of the European Union

Areng

Funded by the Erasmus+ Programme of the European Union

Telefoni ründed

1950. aastatel olid telefonid tehnoloogia tipptase

- **Telefoni ründed**
  - Õpiti juhtima telefoniliine, kuulates helisid, kui operaatorid kõnesid ühendasid
  - Loeti telefonifirmade tehnilisi ajakirju
  - Sissemurdmine kontoritesse oma riistvara arendamiseks

[*Lapsley, 2013*]

Telefoni ründed tekitasid häkkimise mõtteviisi enne, kui häkkimiseks oli arvuti leiutatud

Esimesed häkkimised

1960. aastatel olid arvutid ruumisuurused hiiglaslikud seadmed

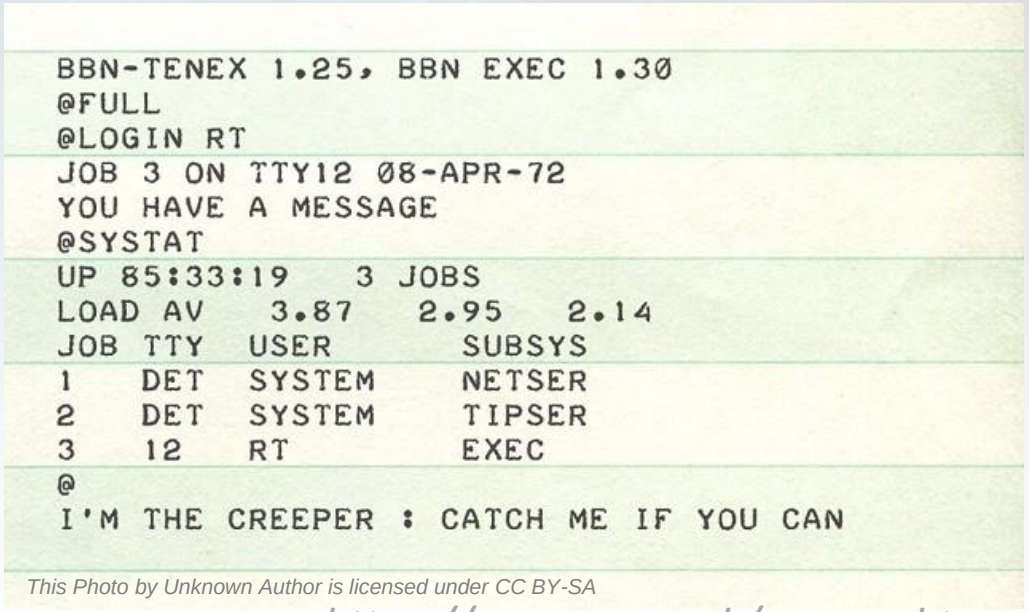
Häkkimine arenes välja positiivse praktikana, mille eesmärk on aidata arvutisüsteeme täiustada

Selle tulemusel tekkisid mõned esimesed ideed kaitseprogrammide kohta, mis võiksid häkkereid peatada

Küberturvalisuse sünd

1971: **I am the creeper: catch me if you can**

- Teadlane Bob Thomas lõi **Creeperi**, mis võis liikuda üle ARPA võrgu
- Ray Tomlinson kirjutas **Reaperi**, mis jälitas ja kustutas Creeperi
- Reaper oli viirusetõrjetarkvara esimene näide
- Reaper oli ka esimene isepaljunev programm, muutes selle kõigi aegade esimeseks arvutiussiks



https://corewar.co.uk/creeper.htm

https://www.javatpoint.com/history-of-cyber-security

Esimene küberturvalisuse patent

1983: krüptograafiline sidesüsteem ja meetod

- Patendi taotlejaks oli Massachusetts Institute of Technology (MIT)
  - **RSA** (Rivest-Shamir-Adleman) algoritm, mis oli üks esimesi avaliku võtmega krüptosüsteeme

https://www.secureworld.io/industry-news/historic-hacking-brief-history-cybersecurity

Küberrünnakud muutuvad sihipärasemaks

Häkkimisest sai 1980. aastatel riikliku julgeoleku probleem

- 1986. aastal tungis Saksamaa kodanik Marcus Hess sisse 400 sõjaväe arvutisse.
  - Ta kavatses KGB-le saladusi müüa
- Rünnaku meetod
  - Kasutas Lawrence Berkeley laboratooriumi (LBL) ARPANETi ja MILNETi “sisenemiseks"
- Astronoom Clifford Stoll kasutas meepotti sissetungi tuvastamiseks ja süžee nurjamiseks

https://www.javatpoint.com/history-of-cyber-security

CERT loomine

1988: Morrise uss või Interneti-uss – esimene võrguviirus

- **Morrise uss**
  - Programm läbis võrke, tungis Unixi terminalidesse ja kopeeris ennast
  - Nakatas arvuti mitu korda
  - Iga täiendav protsess aeglustab masina tööd ja lõpuks masin kahjustus
- R. Morrisele esitati süüdistus arvutipettuse ja kuritarvitamise seaduse alusel.
  - Akt ise sundis looma **Computer Emergency Response Team**, *a.k.a.*, **CERT**

https://www.javatpoint.com/history-of-cyber-security

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

1990. aastad: arvutiviiruste tõus

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

- Ebapiisavad turvalahendused mõjutasid tohutul hulgal kõrvalisi ohvreid
- Enamik viiruserünnakuid oli peamiselt seotud rahalise kasu või strateegiliste eesmärkidega

https://cyberexperts.com/history-of-cybersecurity/

CyberPhish
Safeguarding your digital future

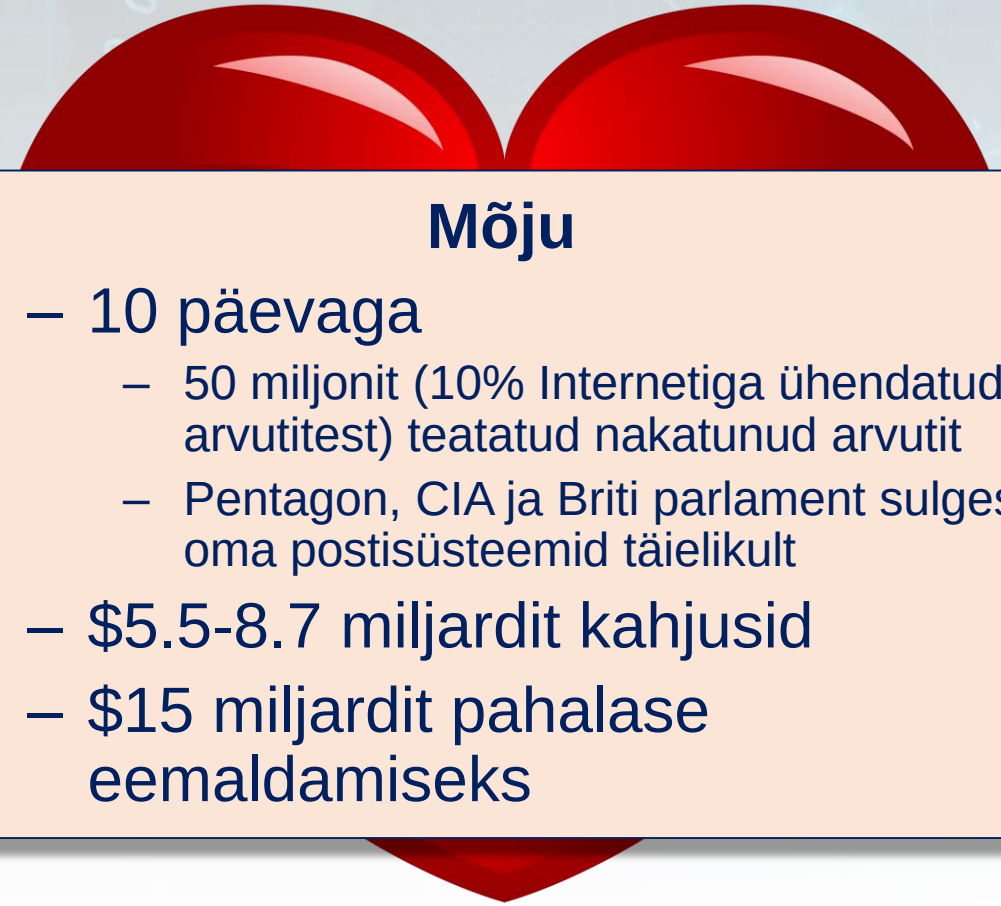
Funded by the Erasmus+ Programme of the European Union

Mai 2000: *I LOVE YOU*

- **E-mail sõnum**
  - pealkirjaga "ILOVEYOU" ja
  - manusega "LOVE-LETTER-FOR-YOU.txt.vbs"
- **Manuse avamine**
  - aktiveeris Visual Basic skripti
    - Kirjutades üle erinevaid (pildi, muusika jne) faile,
    - Saatis endast koopia Microsoft Outlooki kasutatavas Windowsi aadressiraamatu 50 esimesele aadressile

https://en.wikipedia.org/wiki/ILOVEYOU

Mai 2000: *I LOVE YOU*



Mõju

- 10 päevaga
  - 50 miljonit (10% Internetiga ühendatud arvutitest) teatatud nakatunud arvutit
  - Pentagon, CIA ja Briti parlament sulgesid oma postisüsteemid täielikult
- $5.5-8.7 miljardit kahjusid
- $15 miljardit pahalase eemaldamiseks

Võimalikkus

- Skriptide käivitamine on lubatud
- Microsofti peitis faililaiendeid
- Sotsiaalselt aktuallne teema
- Microsofti disaini nõrkus
  - Pahalese juurdepääs operatsioonisüsteemi tuumale
  - Sekundaarne salvestusruum

Pet Shop Boy's "E-mail"
https://youtu.be/AEF8hAAm_sg

Funded by the Erasmus+ Programme of the European Union

Antiviiruse tööstuse tõus

1990. aastate algus: viirusetõrjetoodete järsk kasv

Pahavaraprogrammide kasv mõnelt tuhandelt 1990. aastatel
vähemalt 5 miljonini aastaks 2007 aastaks

- Esimesed antiviiruse programmid 1987:
  - Antivirus for the Atari ST
  - The NOD antivirus
  - McAfee VirusScan
- Viirusetõrjeprogrammid skannisid ja testisid IT-süsteeme andmebaasi kirjutatud räsidega
  - Ressursi intensiivne kasutamine
  - Suur hulk valepositiivseid

- **Lõpp-punkti kaitseplatvormid**
  - Tuvastavad pahavara perekonnad
  - Eeldus: pahavara näidised erinevad olemasolevatest näidistest
  - Võimalik tuvastada ja peatada tundmatu pahavara, kuna vaja oli ainult muu olemasoleva pahavara signatuuri

https://cyberexperts.com/history-of-cybersecurity/

Funded by the Erasmus+ Programme of the European Union

SSL turvasoklite kiht

1995: SSL tõuseb esile

- **SSL**
  - Netscape töötas välja vahetult pärast esimese Interneti-brauseri väljaandmist
  - Tuum selliste keelte arendamiseks nagu HyperText Transfer Protocol Secure (HTTPS)
  - Võimaldab kasutajatel turvaliselt veebile juurde pääseda ja sooritada selliseid toiminguid nagu veebiostud

Häkkerigruppide tõus

2003: Anonymous – esimene tuntud häkkerite rühmitus

Anonymous – 1 oktoober 2003:

- Esiteks: häkkis saientoloogia kirikule kuuluvale veebisaidile DDoS-i abil
- Tal pole kindlat juhti
- Liikmed erinevatest võrguühenduseta ja võrguühendusega kogukondadest
- Praeguseks – seotud paljude kõrgetasemeliste rünnakujuhtumitega
- Peamine põhjus on kodanike privaatsuse kaitsmine
- Motiveeris teisi rühmitusi suuremahulisi küberrünnakuid korraldama
  - *Lazarus* and *Apt38*, etc

Krediitkaardi häkkimine

Aastatel 2005–2007: küberrünnakud on sihipärasemad

- **Albert Gonzales**:
  - Lõi küberkurjategijate ringi
  - Krediitkaardisüsteemide rünnakud
  - Konfidentsiaalne teave vähemalt 45,7 miljonilt kaardilt
  - Kahjum ulatub 256 miljoni dollarini
  - Vahendid kannatanutele kahju hüvitamiseks

TJX oli rikkumise toimumise ajal kaitsmata ja teised organisatsioonid nägid seda vihjena enda kaitsmiseks keeruka küberjulgeolekuprogrammiga

2010 ja edasi: Suurte rikkumiste ajastu

- **Snowden & NSA, 2013**:
  - endine CIA töötaja ja USA valitsuse töövõtja – kopeeris ja lekitas salastatud teavet riiklikust julgeolekuagentuurist (NSA)
  - rõhutas tõsiasja, et valitsus "luurab" avalikkust
- **Yahoo, 2013 – 2014**:
  - Häkkerid kasutasid Yahoo serveritesse pahavara installimiseks andmepüügi tehnikaid, võimaldades neile piiramatut juurdepääsu tagauksele
  - Seati ohtu kolme miljardi kasutaja kontod ja isiklik teave
  - Yahoo'le määrati 35 miljoni dollari suurune trahv, kuna ta ei avaldanud uudiseid rikkumise kohta
  - Müügihind langes selle tulemusel 350 miljoni dollari võrra
- **WannaCry lunavara krüptouss , 2017**:
  - Sihtarvutid, mis töötavad Microsoft Windowsi operatsioonisüsteemiga
  - Nõudis lunaraha maksmist Bitcoini krüptovaluutas
  - Vaid ühe päevaga nakatas uss üle 230 000 inimese 150 riigis

https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Funded by the Erasmus+ Programme of the European Union

May 12-15, 2017: *WannaCry*

- Microsofti disaini nõrkus
  - Paljundatud läbi EternalBlue
  - Kasutas ära tagauste installimis5 nakatunud süsteemidele
- Kuigi Microsoft oli välja andnud turvaaugu parandus
  - Organisatsioonid ei olnud neid rakendanud või kasutasid vanemaid Windowsi süsteeme

https://www.avast.com/c-wannacry

Küberturvalisuse raamistikud

- **Standardid**
  - ISO/IEC 2700x seeria
  - NIST küberturve standard
  - BSI standard 100 küberturvalisus
  - Ühised tunnusjooned
  - …
- **Tehnikad**
  - Väärkasutuse juhtumid
  - Halva aktiivsuse diagrammid
  - TurvalineUML
  - UMLsec
  - Agiilne turvanõuete projekteerimine
- **Raamistikud**
  - Turvanõuete kavandamise raamistik: esitus ja analüüs
  - Turvalisus ontoloogia järgi: teadmistekeskne lähenemine …
- **Protsessid**
  - CC-põhine turbetehnoloogia protsess
  - Turvanõuded tarkvara tootesarjadele
  - Nõuded taaskasutamiseks süsteemi turvalisuse parandamiseks
  - …
- **Meetodid**
  - Secure Tropos
  - SQUARE
  - SREBP
  - …

Funded by the Erasmus+ Programme of the European Union

Küberturvalisuse eeskirjad ja seadused

1996: **HIPPA** – Health Insurance Portability and Account Act

1999: **GLBA** – Gramm-Leach-Bliley Act

2003: **FISMA** – Federal Information Security Management Act

2018: **GDPR** – General Data Protection Regulation

2020: **CCPA** – California Consumer Privacy Act

2021: **E-ITS** – Eesti infoturbe Standard

https://eits.ria.ee/

https://cyberexperts.com/history-of-cybersecurity/

Uued küberturvalisuse lähenemisviisid ja strateegiad

- **MFA** – mitmefaktoriline autentimine
- **NBA** – võrgukäitumise analüüs
  - tuvastab pahatahtlikud failid käitumishälvete või anomaaliate põhjal
- **Ohu tuvastamine** ja uuenduste automitiseerimine
- **Reaalaja kaitse**
  - juurdepääsul skaneerimine, taustavalve, residentide kaitse ja automaatne kaitse

- **Liivakast / *Sandboxing***
  - isoleeritud testkeskkond kahtlase faili või URL-i käivitamiseks
- **Jälgede ajamine / *Forensics***
  - rünnakute analüüs ja kordamine, et aidata turvameeskondadel tulevasi rikkumisi paremini ette valmistuda
- **Tagavarakoopiad / *Back-up*** ja andmete peegeldamine
- **WAF** – veebirakenduste tulemüürid
  - saidiülese võltsimise, saidiülese skriptimise (XSS), failide kaasamise ja SQL-i sisestamise vastu.

CyberPhish
Safeguarding your digital future

https://blog.avast.com/history-of-cybersecurity-avast

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

- Telefoni ründed
- Esimesed häkkimised
- Küberturvalisuse sünd
- Arvutiviirused
- Häkkerirühmitused
- Ohvrite lood

- Küberturvalisuse patent
- CERT
- Antiviiruste tööstus
- SSL
- Küberturvalisuse raamistikud
- Seadused ja standardid

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Ülesanded

Arutage, milliseid õppetunde tuleks Phone Phreaksi juhtumitest õppida

Võrrelge I LOVE YOU ja WannaCry rünnakuid

Milliseid küberturvalisuse raamistikke olete uurinud või lugenud nende kohta?

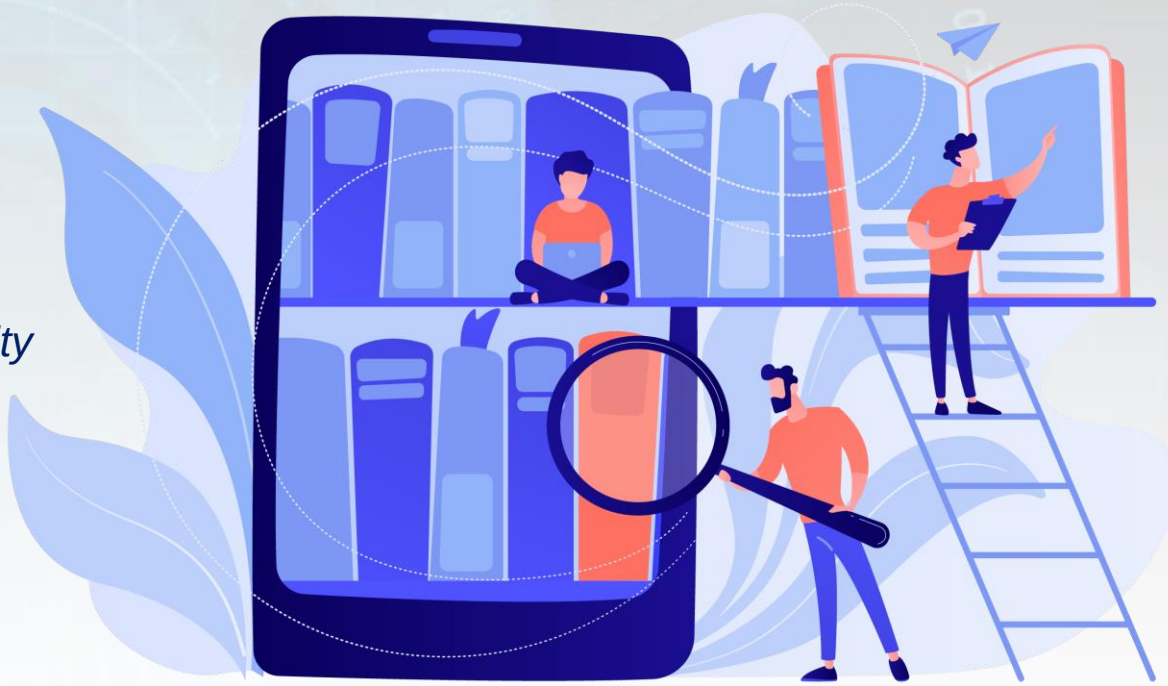
Funded by the Erasmus+ Programme of the European Union

Lisalugemine

History of Cybersecurity

Material used in preparation of this lecture

- *https://cyberexperts.com/history-of-cybersecurity/*
- *https://elevenfifty.org/blog/a-decade-by-decade-history-of-cybersecurity/*
- *https://www.secureworld.io/industry-news/historic-hacking-brief-history-cybersecurity*
- *https://www.jigsawacademy.com/blogs/cyber-security/cyber-security-history*
- *https://www.javatpoint.com/history-of-cyber-security*
- *https://blog.avast.com/history-of-cybersecurity-avast*
- *https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/*



Funded by the Erasmus+ Programme of the European Union

Lühivideod

- A Brief History of Cybersecurity and Hacking
  https://youtu.be/V6p7lFsokXo
- History of Cybersecurity
  https://youtu.be/CFwmTzCVuFQ
- Evolution of Cybersecurity from 80s to Today
  https://youtu.be/wKaRdugeAPs
- Top Cyber Attacks In History
  https://youtu.be/fUeJtM1bgGo
  https://youtu.be/lJc3viPKXk4

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tänan kuulamast!