Funded by the
Erasmus+ Programme
of the European Union

Ievads kiberdrošībā

Kiberdrošības vēsture

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

Apgūt īsu vēsturi par to, kā laika gaitā ir mainījusies pieeja kiberuzbrukumiem, kā rezultātā ir veikti pastiprināti pasākumi un līdz ar to – arī pretpasākumi pret kiberuzbrukumiem.

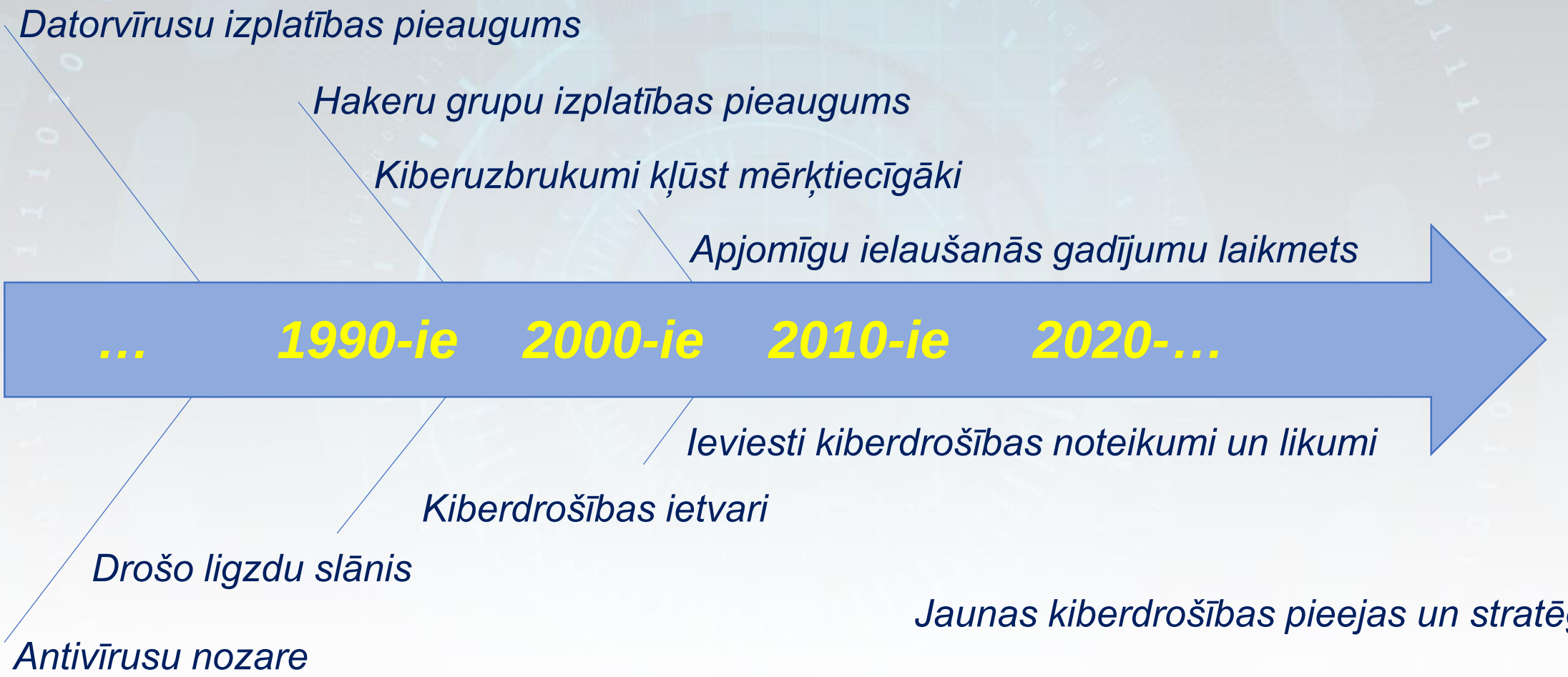
Kursantu darba slodze

Lekcija	1 st.
Audio un video materiāli	1 st.
Pētījumi	1 st.
Papildu lasīšana	2 st.
Sagatavošanās eksāmenam	1 st.

Saturs

Funded by the Erasmus+ Programme of the European Union

Saturs


Datorvīrusu izplatības pieaugums
Hakeru grupu izplatības pieaugums
Kiberuzbrukumi kļūst mērķtiecīgāki
Apjomīgu ielaušanās gadījumu laikmets
…
1990-ie
2000-ie
2010-ie
2020-…
Ieviesti kiberdrošības noteikumi un likumi
Kiberdrošības ietvari
Drošo ligzdu slānis
Jaunas kiberdrošības pieejas un stratēģijas
Antivīrusu nozare

Tālruņu un centrāļu manipuluācijas

1950. gados tālruņi bija vismodernākās tehnoloģijas

- **Tālruņu/centrāļu manipulācijas**
  - Cilvēki iemācījās kontrolēt tālruņa līnijas, klausoties skaņas, kad operatori savienoja zvanus
  - Telefonkompāniju tehnisko žurnālu lasīšana
  - Ielaušanās birojos, lai izstrādātu savu aparatūru

[*Lepslijs [Lapsley], 2013. gads*]

Tālruņu uzbrukumi uzsāka hakerisma domāšanas veidu, pirms bija pieejams datori, ko uzlauzt

Agrīnie hakeri

1960. gados datori bija milzīgi lieldatori, kas bija ieslēgti telpās

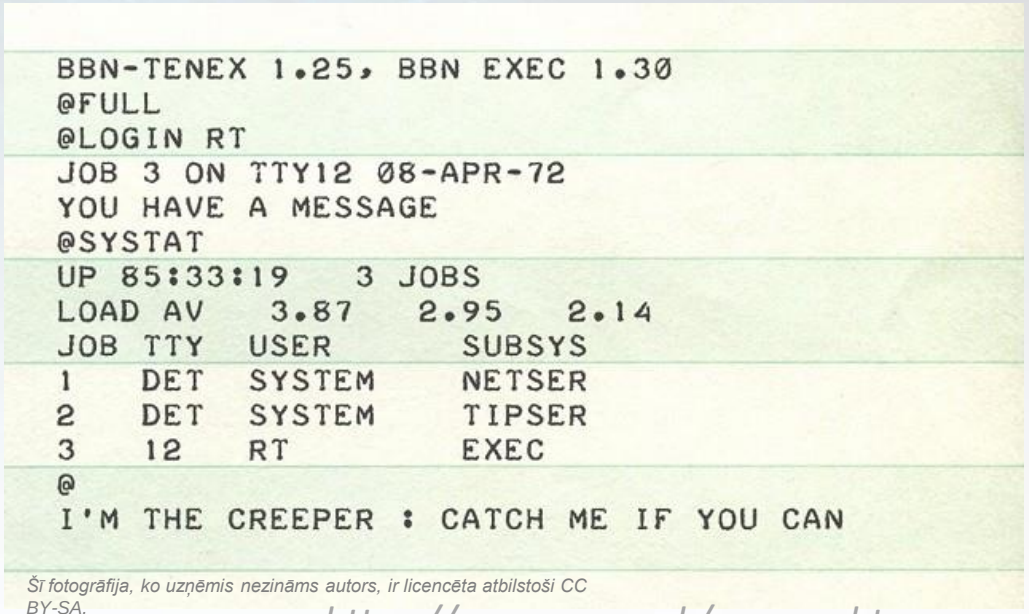
Datorurķēšana (hakerisms) tika izstrādāta kā pozitīva prakse, kas paredzēta, lai palīdzētu uzlabot datorsistēmas

Tā rezultātā radās dažas no pirmajām idejām par aizsardzības programmām, kas varētu apturēt hakerus.

Parādās pirmie datoru drošības iedīgļi

1971. gads: **Šeit urķis, noķer mani, ja vari**

- Pētnieks **Bobs Tomass** *[Bob Thomas]* radīja **urķa skriptu** (*angl. Creeper*), kas varēja pārvietoties brīvi visā ARPA tīklā.
- **Rejs Tomlinsons** *[Ray Tomlinson]* uzrakstīja **novācēja** (*angl. Reaper*) skriptu, kas noķēra un izdzēsa urķa skriptu.
  - Novācējs bija pirmais antivīrusu programmatūras piemērs.
  - Novācējs bija arī pirmā pašreplicējošā programma, padarot to par pirmo datoru tārpu.



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

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

Pirmie kiberdrošības patenti

1983. gads: *Kriptogrāfisko sakaru sistēma un metode*

- Pirmais patents tika piešķirts Masačūsetsas Tehnoloģiju institūtam (MIT)
  - **RSA** (Rivesta – Šamira – Eidlmana *[Rivest-Shamir-Adleman]* algoritms), kas bija viena no pirmajām publiskajām atslēgas kriptosistēmām.

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kiberdrošība kļūst reālāka

Hakerisms kļuva par nacionālās drošības jautājumu 80. gados

- 1986. gadā Vācijas pilsonis **Markuss Hess** *[Marcus Hess]* ielauzās **400 militārajos datoros.**
  - Viņš plānoja pārdot noslēpumus VDK.
- Uzbrukumu metode
  - Izmantoja Lorensa Berkelija laboratoriju (LBL), lai ar ***parazitēšanas*** palīdzību pārvietotos uz ARPANET un MILNET.

- Astronoms **Klifords Stols** *[Clifford Stoll]*, pateicoties ***ēsmas izlikšanai*** noteica ielaušanās mēģinājumu un padarīja plānu par nefunkcionējošu.

Šī fotogrāfija, ko uzņēmis nezināms autors, ir licencēta atbilstoši

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

CERT dibināšana

1988. gads: Morisa tārps jeb interneta tārps – pirmais tīkla vīruss

- **Morisa tārps**
  - Programma šķērsoja tīklus, iebruka Unix terminālos un kopēja pati sevi.
  - Tā vairākas reizes inficēja vienu datoru.
  - Katrs papildu process palēnināja iekārtas darbību, galu galā līdz pat bojājumu izraisīšanai.

- R. Morisu *[R. Morris]* tika apsūdzēts saskaņā ar **Likumu par krāpšanos un nelikumīgām darbībām datorsistēmās**
  - Likums noveda pie organizācijas **Datoru ārkārtas reaģēšanas komanda** *nodibināšanas, kas pazīstama kā* **CERT**

Šī fotogrāfija, ko uzņēmis nezināms autors, ir licencēta atbilstoši CC BY-SA-NC

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

1990-tie gadi: *Datorvīrusu izplatības pieaugums*

Šī fotogrāfija, ko uzņēmis nezināms autors, ir licencēta atbilstoši CC BY-SA.

- Neatbilstoši drošības risinājumi izraisīja milzīgu skaitu netīšu upuru
- Lielākā daļa vīrusu uzbrukumu galvenokārt bija saistīti ar finansiāliem ieguvumiem vai stratēģiskiem mērķiem

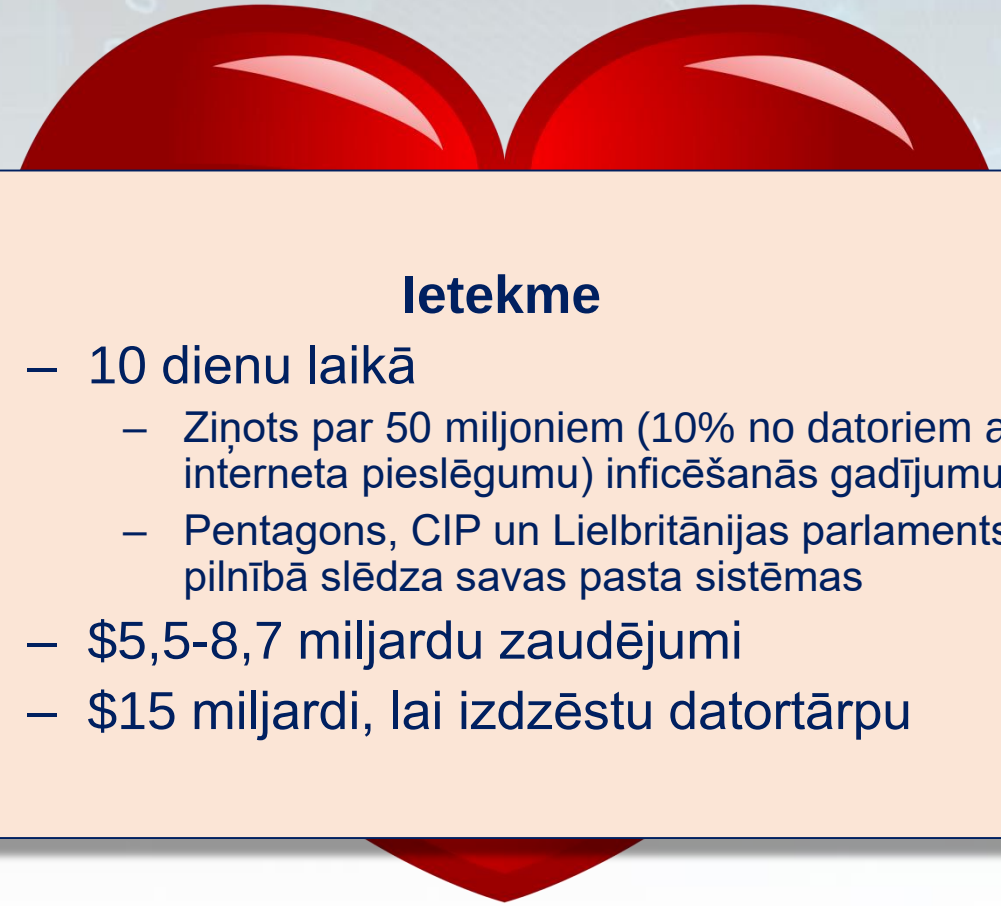
2000. gada maijs: *Vīruss "I LOVE YOU"*

- **E-pasta ziņojums**
  - Teksts, kas ietverts tēmas līnijā – "ILOVEYOU" un
  - pielikumā fails "LOVE-LETTER-FOR-YOU.txt.vbs"

- **Pēc pielikuma atvēršanas**
  - tiek aktivizēts Visual Basic skripts
    - Notiek attēlu failu pārrakstīšana,
    - savukārt vīruss nosūta savu kopiju uz pirmajām 50 adresēm Windows adrešu grāmatā, ko izmanto Microsoft Outlook

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

2000. gada maijs: *Vīruss "I LOVE YOU"*



Ietekme

- 10 dienu laikā
  - Ziņots par 50 miljoniem (10% no datoriem ar interneta pieslēgumu) inficēšanās gadījumu
  - Pentagons, CIP un Lielbritānijas parlaments pilnībā slēdza savas pasta sistēmas
- $5,5-8,7 miljardu zaudējumi
- $15 miljardi, lai izdzēstu datortārpu

Sekmes

- Skriptu programma ir iespējota
- Microsoft algoritma priekšrocība failu paplašinājumu slēpšanai
- Sociālā inženierija
- Microsoft uzbūves vājums
  - Piekļuve operētājsistēmām
  - Sekundārā krātuve

Grupas "Pet Shop Boys" e-pasts
https://youtu.be/AEF8hAAm_sg

Funded by the Erasmus+ Programme of the European Union

Antivīrusu industrija

Deviņdesmito gadu sākums: straujš pretvīrusu produktu pieaugums

Ļaunprātīgo programmu pieaugums
no dažiem tūkstošiem deviņdesmitajos gados līdz vismaz 5 miljoniem līdz 2007. gadam

- Pirmās komerciālās pretvīrusu programmas 1987. gadā:
  - Antivīruss datoriem Atari ST
  - Antivīruss "NOD"
  - Antivīruss "McAfee VirusScan"
- Antivīrusu programmas skenēja un testēja IT sistēmas uz parakstu klātbūtni, kas bija ierakstīti to datu bāzēs.
  - Intensīva resursu izmantošana
  - Liels skaits viltus pozitīvu

- **Galapunktu aizsardzības platformas**
  - Ļaunprātīgu programmatūras saimju identificēšana
  - Priekšnoteikums: ļaunprātīgas programmatūras paraugi atšķiras no esošajiem paraugiem
  - Iespējams atklāt un apturēt nezināmu ļaunprogrammatūru, jo bija nepieciešams tikai citas esošas ļaunprogrammatūras paraksts

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

Funded by the Erasmus+ Programme of the European Union

Drošo ligzdu slānis

1995. gads: SSL sāk attīstīties

- **SSL**
  - To izstrādāja Netscape neilgi pēc pirmās interneta pārlūkprogrammas izlaišanas
  - Kodols komunikācijas valodu izstrādei, piemēram, HyperText Transfer Protocol Secure (HTTPS)
  - Ļauj lietotājiem droši piekļūt tīmeklim un veikt tādas darbības kā pirkumi tiešsaistē

Hakeru grupu izplatības pieaugums

2003. gads: Anonymous – pirmā hakeru grupa

Anonymous – 2003. gada 1. oktobris:

- Pirmkārt: uzlauza vietni, kas pieder Scientoloģijas baznīcai, izmantojot DDoS
- Grupai nav konkrēta vadītāja
- Dalībnieki no dažādām bezsaistes un tiešsaistes kopienām
- Līdz pat šodienai – grupa saistīta ar daudziem augsta līmeņa uzbrukumu incidentiem
- Galvenais iemesls ir pilsoņu privātuma aizsardzība
- Motivēja citas grupas veikt liela mēroga kiberuzbrukumus
  - *Lazarus* un *Apt38*, u. tml.

Kredītkaršu uzlaušana

No 2005. līdz 2007. gadam: kiberuzbrukumi kļūst mērķtiecīgāki

- **Alberts Gonzaless** *[Albert Gonzales]*:
  - Izveidoja kibernoziedznieku loku
  - Tie apdraud kredītkaršu sistēmas
  - Konfidenciāla informācija no vismaz 45,7 miljoniem karšu
  - Zaudējumu, kuru apmērs sniedzas līdz ***$256*** miljoniem
  - Līdzekļi kompensācijām cietušajiem

Mazumtirgotājs TJX nebija pienācīgi aizsargāts, kad notika uzlaušana, un citas organizācijas to uzskatīja par signālu sevis aizsardzībai ar augsta līmeņa sarežģītu kiberdrošības programmu.

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

Funded by the Erasmus+ Programme of the European Union

2010-ie gadi: *Apjomīgu ielaušanās gadījumu laikmets*

- **Snoudens un NSA, 2013. gads**:
  - bijušais CIP darbinieks un ASV valdības līgumdarbu strādnieks – nokopēja un nopludināja klasificētu informāciju no Nacionālās drošības aģentūras (NSA)
  - Viņš uzsvēra faktu, ka valdība "izspiego" sabiedrību.
- **Yahoo, 2013. – 2014. gads**:
  - Hakeri izmantoja pikšķerēšanas paņēmienus, lai Yahoo serveros instalētu ļaunprātīgu programmatūru, nodrošinot viņiem neierobežotu piekļuvi aizmugures durvīm.
  - Tie apdraud trīs miljardu lietotāju kontus un personisko informāciju
  - Yahoo tika uzlikts naudas sods 35 miljonu dolāru apmērā par ziņu neizpaušanu par pārkāpumu
  - Tā rezultātā pārdošanas cena samazinājās par 350 miljoniem dolāru
- **Izspiedējvīrusa kriptotārps WannaCry, 2017. gads**:
  - Mērķa datori, kuros darbojas operētājsistēma Microsoft Windows
  - Pieprasīja izpirkuma maksājumus Bitcoin kriptovalūtā
  - Tikai vienas dienas laikā tārps inficēja ***230 000*** sistēmas ***150*** valstīs

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

Funded by the Erasmus+ Programme of the European Union

2017. gada 12.-15. maijs: WannaCry

- Microsoft uzbūves vājums
  - Izplatījās caur eksploitu EternalBlue
  - Izmantoja aizmugures durvju instalēšanas priekšrocības inficētajās sistēmās
- Neņemot vērā, ka Microsoft bija izlaidis drošības ielāpus
  - organizācijas tos nebija izmantojušas vai izmantoja vecākas Windows sistēmas

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

Kiberdrošības ietvari

- **Standarti**
  - ISO/IEC 2700x sērija
  - NIST speciālās publikācijas
  - BSI standarts 100 informācijas drošībai
  - Kopīgie kritēriji
  - …
- **Paņēmieni**
  - Ļaunprātīgas lietošanas gadījumi
  - Nepareizas darbības diagrammas
  - SecureUML
  - UMLsec
  - Pielāgotiesspējīga drošības prasību inženierija

- **Ietvari**
  - Drošības prasību inženierijas ietvars: attēlojums un analīze
  - Drošība pēc ontoloģijas: uz zināšanām orientēta pieeja
  - …
- **Procesi**
  - Uz CC balstīts drošības inženierijas process
  - Drošības prasības programmatūras produktu līnijām
  - Prasības atkārtotai izmantošanai sistēmas drošības uzlabošanai
  - …
- **Metodes**
  - Secure Tropos
  - SQUARE
  - SREBP
  - …

Funded by the Erasmus+ Programme of the European Union

Kiberdrošības noteikumi un likumi

1996. gads: **HIPPA** – Veselības apdrošināšanas pārnesamības un kontu likums

1999. gads: **GLBA** – Grema – Līča – Blailija *[Gramm – Leach – Bliley]* likums

2003. gads: **FISMA** – Federālais informācijas drošības pārvaldības likums

2018. gads: **GDPR** – Vispārējā datu aizsardzības regula

2020. gads: **CCPA** – Kalifornijas Patērētāju privātuma likums

Jaunas kiberdrošības pieejas un stratēģijas

- **MFA** – daudzfaktoru autentifikācija
- **NBA** – tīkla uzvedības analīze
  - identificē ļaunprātīgus failus, pamatojoties uz uzvedības novirzēm vai anomālijām
- **Draudu izlūkošanas** un atjaunināšanas automatizācija
- **Reāllaika aizsardzība**
  - piekļuves skenēšana, fona aizsargs, pastāvīgais vairogs un automātiskā aizsardzība

- **Smilšu kastes metode**
  - Izolēta testa vide, lai palaistu aizdomīgu failu vai URL
- **Kriminālistika**
  - Uzbrukumu atkārtošana, lai palīdzētu drošības komandām labāk mazināt turpmākos pārkāpumus
- **Rezerves kopiju** un spoguļsistēmu veidošana
- **WAF** – tīkla lietotņu ugunsmūri
  - pret starpvietņu viltošanu, starpvietņu skriptēšanu (XSS), failu iekļaušanu un SQL ievadīšanu.

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

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums

- Tālruņu/centrāļu manipulācijas
- Agrīnās hakeru aktivitātes
- Pirmie kiberdrošības iedīgļi
- Datorvīrusi
- Hakeru grupas
- Lielapjoma ielaušanās
- Kiberdrošības patents
- CERT
- Antivīrusu nozare
- SSL
- Drošības ietvari
- Noteikumi un likumi

Uzdevumi

Pārrunājiet, kādas mācības būtu jāgūst no tālruņu un centrāļu manipulāciju gadījumiem

Salīdziniet uzbrukumus, ko izraisīja vīrusi ***I LOVE YOU*** un ***WannaCry***

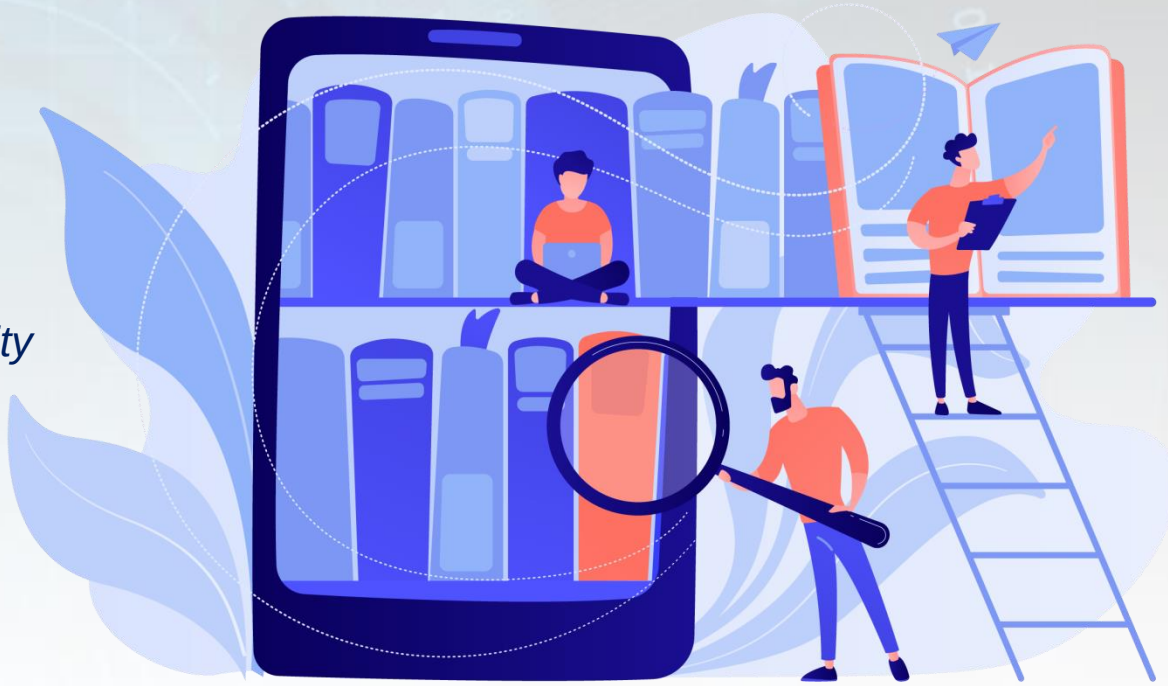
Par kuriem kiberdrošības ietvariem esat pētījis vai lasījis?

Papildu lasīšana

Kiberdrošības vēsture

Šīs lekcijas sagatavošanā izmantotie materiāli

- *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/*



Īsi video

- Īsa kiberdrošības un hakeru vēsture
  https://youtu.be/V6p7lFsokXo
- Kiberdrošības vēsture
  https://youtu.be/CFwmTzCVuFQ
- Kiberdrošības evolūcija no 80. gadiem līdz mūsdienām
  https://youtu.be/wKaRdugeAPs
- Populārākie kiberuzbrukumi vēsturē
  https://youtu.be/fUeJtM1bgGo
  https://youtu.be/lJc3viPKXk4

Funded by the Erasmus+ Programme of the European Union

Pateicamies!