Funded by the
Erasmus+ Programme
of the European Union

Kibernetinio saugumo įvadas

Kibernetinio saugumo istorija

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

Mokymo tikslai

Sužinoti trumpą istoriją apie tai, kaip laikui bėgant keitėsi požiūriai į kibernetines atakas, dėl ko atsirado daugiau priemonių, o kartu atsirado priemonės kovai su kibernetinėmis atakomis.

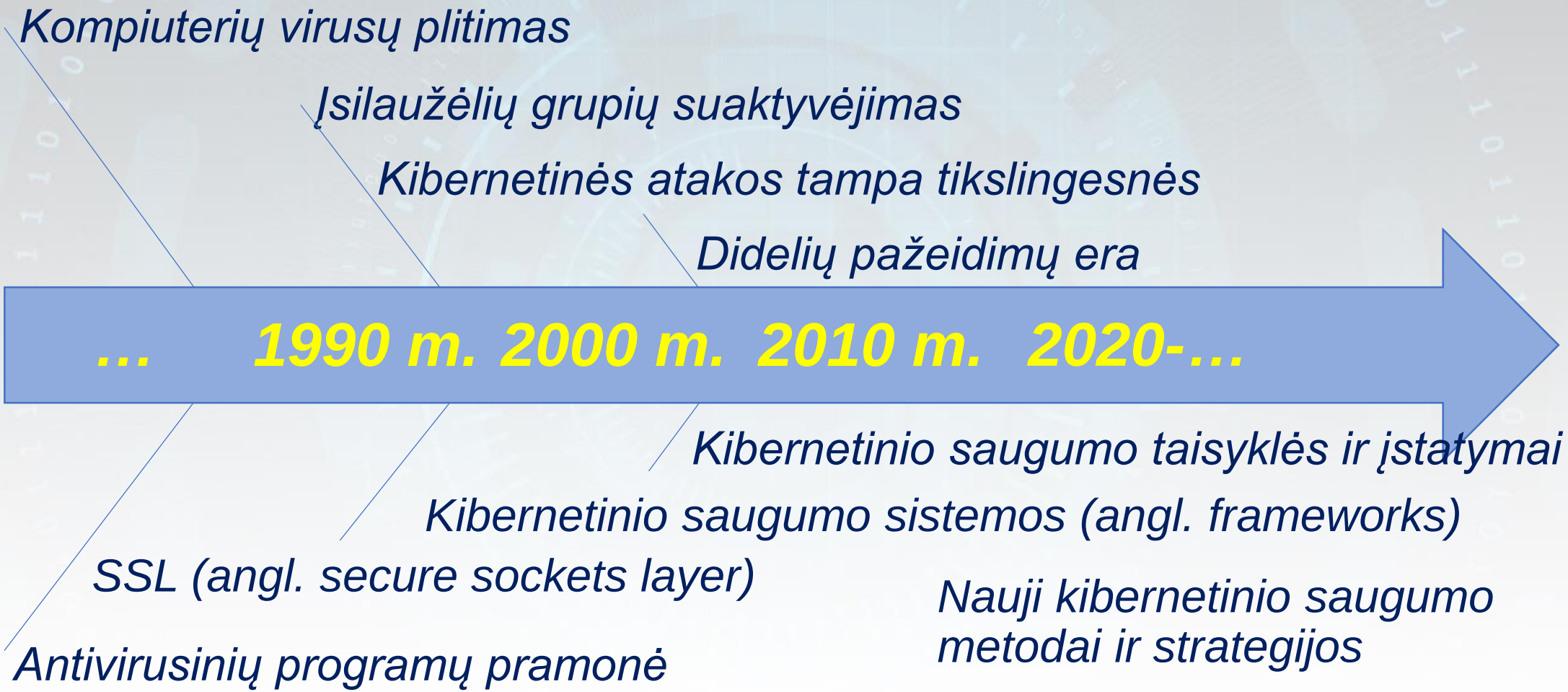
Studento darbo krūvis

Paskaitos	1 val.
Garso ir vaizdo medžiaga	1 val.
Panaudojimo atvejai	1 val.
Papildomi skaitiniai	2 val.
Pasiruošimas atsiskaitymui	1 val.

Turinys


Telefoniniai apgavikai
Pirmieji įsilaužimai
Atsiranda kompiuterinis saugumas
Kibernetinis saugumas tampa realus
… 1950 m. 1960 m. 1970 m. 1980 m. …
CERT atsiradimas
Pirmasis kibernetinio saugumo patentas

Turinys


Kompiuterių virusų plitimas
Įsilaužėlių grupių suaktyvėjimas
Kibernetinės atakos tampa tikslingesnės
Didelių pažeidimų era
… 1990 m. 2000 m. 2010 m. 2020-…
Kibernetinio saugumo taisyklės ir įstatymai
Kibernetinio saugumo sistemos (angl. frameworks)
SSL (angl. secure sockets layer)
Nauji kibernetinio saugumo metodai ir strategijos
Antivirusinių programų pramonė

Telefoniniai apgavikai

XX a. šeštajame dešimtmetyje telefonai buvo pažangiausia ryšio technologija

- **Telefoniniai apgavikai**
  - Išmoko valdyti telefono linijas klausydamiesi garsų, kai operatoriai sujungdavo skambučius.
  - Skaitė telefonų bendrovių techninius žurnalus
  - Įsilaužinėjo į biurus ir kūrė savo techninę įrangą

[*Lapsley, 2013*]

Telefoniniai įsilaužėliai pradėjo įsilaužimo mąstyseną dar prieš atsirandant kompiuteriui, į kurį būtų galima įsilaužti.

Pirmieji įsilaužimai

Septintajame dešimtmetyje kompiuteriai buvo milžiniški kambario dydžio įrenginiai

Įsilaužimas išsivystė kaip teigiama praktika, padedanti tobulinti kompiuterių sistemas.

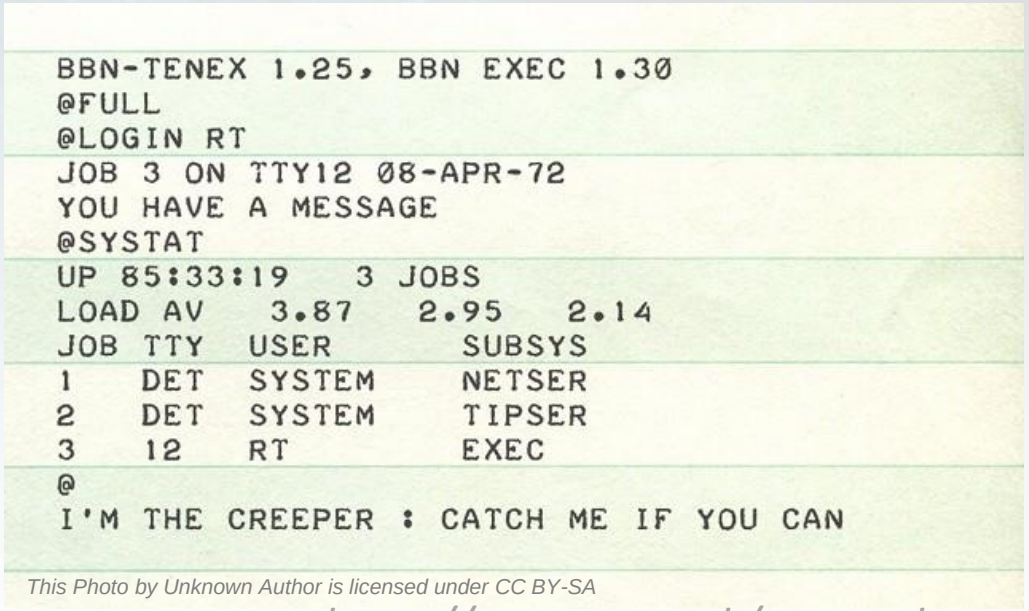
Taip atsirado keletas pirmųjų idėjų, kaip sukurti gynybines programas, kurios galėtų sustabdyti įsilaužėlius.

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

Atsiranda kompiuterinis saugumas

1971 m. **„I am the creeper: catch me if you can“**

- Tyrėjas **Bob Thomas** sukūrė **Creeper** kurie galėtų judėti ARPA tinkle.
- **Ray Tomlinson** parašė **Reaper**, kuris sekė ir šalino „Creeper“
  - „Reaper“ buvo pirmasis antivirusinės programinės įrangos pavyzdys
  - „Reaper“ taip pat buvo pirmoji save replikuojanti programa, todėl tai buvo pirmasis kompiuterinis kirminas



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

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

Pirmasis kibernetinio saugumo patentas

1983 m. Kriptografinių ryšių sistema ir metodas

RSA

- Suteiktas Masačusetso technologijos institutui (MIT)
  - **RSA** (Rivest-Shamir-Adleman) algoritmas, kuris buvo viena iš pirmųjų viešojo rakto kriptosistemų.

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

Funded by the Erasmus+ Programme of the European Union

Kibernetinis saugumas tampa realus

1980-aisiais įsilaužimas tapo nacionalinio saugumo klausimu

- 1986 m. Vokietijos pilietis **Marcus Hess** įsilaužė į **400 karinių kompiuterių**
  - Jis ketino parduoti paslaptis KGB
- Atakos metodas
  - Naudojosi Lawrence Berkeley laboratorija (LBL), norėdamas įsilaužti (“***piggyback***”) į ARPANET ir MILNET
- Astronomas **Clifford Stoll** pasinaudojo ***honeypot***, norėdamas aptikti įsilaužimą ir sužlugdyti sąmokslą.

CERT atsiradimas

1988 m. Moriso kirminas arba interneto kirminas – pirmasis tinklo virusas

- **Morris kirminas**
  - Programa „keliavo“ tinklais, įsiveržė į „Unix“ terminalus ir kopijavo pati save
  - Užkrėtė kompiuterį kelis kartus
  - Kiekvienas papildomas procesas sulėtindavo kompiuterį, galiausiai jis buvo sugadinamas

- R. Morris buvo apkaltintas pagal Kompiuterio sukčiavimo ir piktnaudžiavimo (angl. **Computer Fraud and Abuse Act**) įstatymą
  - Todėl buvo įkurta **Kompiuterinių incidentų reagavimo grupė** (angl. Computer Emergency Response Team, **CERT**)

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

1990'ieji : Kompiuterių virusų plitimas

- Dėl netinkamų saugumo sprendimų nukentėjo daugybė nenumatytų aukų.
- Dauguma virusų atakų pirmiausia buvo susijusios su finansine nauda arba strateginiais tikslais.

2000 m. gegužė. I LOVE YOU

- **El. pašto laiškas**
  - Laiško tema „ILOVEYOU“ ir
  - priedas „LOVE-LETTER-FOR-YOU.txt.vbs“
- **Atveriant laiško priedą**
  - aktyvavo Visual Basic skriptą
    - Perrašydamas įvairius (vaizdo, muzikos) failus,
    - išsiuntė savo kopiją į pirmuosius 50 „Microsoft Outlook“ naudojamos „Windows“ adresų knygos kontaktus

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

2000 m. gegužė. ***I LOVE YOU***

Poveikis

- Per 10 dienų
  - pranešta apie 50 mln. (10% prie interneto prijungtų kompiuterių) užkrėtimų
  - Pentagonas, CŽV, Didžiosios Britanijos parlamentas visiškai išjungė savo pašto sistemas
- 5,5-8,7 mlrd. dolerių žala
- 15 mlrd. dolerių kirmino pašalinimui

Kodėl sėkmingas?

- Leidžiama paleisti scenarijus
- „Microsoft“ failų plėtinių slėpimas
- Socialinė inžinerija
- „Microsoft“ projektavimo trūkumas
  - Prieiga prie operacinių sistemų
  - Antrinė saugykla

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Antivirusinių programų pramonė

Devintojo dešimtmečio pradžia: staigus antivirusinių produktų augimas

Kenkėjiškų programų skaičiaus augimas nuo
kelių tūkstančių dešimtame dešimtmetyje **iki mažiausiai 5 mln.** 2007 m.

- Pirmosios komercinės antivirusinės programos 1987 m:
  - Antivirusinė programa Atari ST
  - NOD antivirusinė programa
  - McAfee VirusScan
- Antivirusinės programos **skenavo** ir **tikrino** IT sistemas, naudodamos duomenų bazėje įrašytus ***parašus***
  - Intensyvus išteklių naudojimas
  - Didelis klaidingų teigiamų rezultatų skaičius

- **„Endpoint protection“ platformos**
  - nustatyti ***kenkėjiškų programų šeimas***
  - Prielaida: kenkėjiškų programų pavyzdžiai skiriasi nuo esamų pavyzdžių
  - Galima aptikti ir sustabdyti nežinomą kenkėjišką programinę įrangą, nes reikėjo tik kitų esamų kenkėjiškų programų parašo

CyberPhish
Safeguarding your digital future

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

Funded by the Erasmus+ Programme of the European Union

SSL – saugaus sujungimo lygmuo

1995 m. SSL išpopuliarėja

- **SSL**
  - Sukurta „Netscape“ netrukus po to, kai buvo išleista pirmoji interneto naršyklė
  - Pagrindas kuriant tokias kalbas kaip HTTPS (HyperText Transfer Protocol Secure)
  - Naudotojams suteikia galimybę saugiai naudotis internetu ir atlikti tokius veiksmus, kaip pirkimas internetu

Įsilaužėlių grupių suaktyvėjimas

2003: Anonymous – pirmoji programišių grupė

Anonymous – 2003 m. spalio 1 d.

- Pirma: įsilaužta į Scientologijos bažnyčiai priklausančią svetainę naudojant **DDoS**
- Neturi konkretaus lyderio
- Nariai iš įvairių neprisijungusių ir prisijungusių internetinių bendruomenių
- Iki šiol – susijęs su daugeliu garsių atakų incidentų
- Pagrindinė priežastis – piliečių privatumo apsauga
- Motyvavo kitas grupes vykdyti plataus masto kibernetines atakas
  - *Lazarus* ir *Apt38 ir kiti*

Kredito kortelių įsilaužimai

2005-2007 m. Kibernetinės atakos tikslingesnės

- **Albert Gonzales**:
  - Sukūrė kibernetinių nusikaltėlių grupuotę
  - Kompromituoti kredito kortelių sistemas
  - Konfidenciali informacija iš mažiausiai ***45,7*** mln. kortelių
  - ***256*** milijonų JAV dolerių nuostoliai
  - Lėšos nukentėjusiųjų patirtoms žaloms atlyginti

Kai įvyko pažeidimas, „TJX“ buvo neapsaugota, o kitos organizacijos tai suprato kaip signalą apsisaugoti naudojant sudėtingą kibernetinio saugumo programą.

2010 m. Didelių pažeidimų era

- **Snowden ir NSA, 2013 m.**
  - buvęs CŽV darbuotojas ir JAV vyriausybės rangovas – nukopijavo ir nutekino slaptą Nacionalinės saugumo agentūros (NSA) informaciją
  - atkreipė dėmesį į tai, kad vyriausybė „šnipinėjo“ visuomenę
- **Yahoo, 2013 – 2014 m.**
  - įsilaužėliai, naudodamiesi personalizuoto sukčiavimo (angl. spear-phishing) metodais, „Yahoo“ serveriuose įdiegė kenkėjišką programinę įrangą, suteikiančią jiems neribotą prieigą prie „užpakalinių durų“
  - sukėlė pavojų trijų milijardų naudotojų paskyroms ir asmeninei informacijai
  - „Yahoo“ buvo nubausta ***35 mln. dolerių*** bauda už tai, kad neatskleidė informacijos apie pažeidimą
  - Dėl to pardavimo kaina sumažėjo ***350 mln. dolerių***
- **Išpirkos reikalaujanti WannaCry, 2017 m.**
  - Taikinys – kompiuteriai, kuriuose įdiegta „Microsoft Windows“ operacinė sistema
  - Reikalavo sumokėti išpirką kriptovaliuta „Bitcoin“
  - Vos per vieną dieną kirminas užkrėtė daugiau kaip ***230 000*** įrenginių ***150*** šalių

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

Funded by the Erasmus+ Programme of the European Union

2017 m. gegužės 12-15 d. WannaCry

- „Microsoft“ projektavimo trūkumas
  - Platinama per „EternalBlue“
  - Atveria prieigą prie užkrėstų sistemų per „užpakalines duris“ (angl. backdoors)
- Nors „Microsoft“ išleido atnaujinimus
  - Organizacijos jų netaikė arba naudojo senesnes „Windows“ sistemas.

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

Kibernetinio saugumo sistemos (angl. frameworks)

- **Standartai**
  - ISO/IEC 2700x serija
  - NIST specialusis leidinys
  - BSI 100 informacijos saugumo standartas
  - Bendrieji kriterijai
  - …
- **Technikos**
  - Piktnaudžiavimo atvejai
  - Neteisingos veiklos diagramos
  - SecureUML
  - UMLsec
  - Aktyvi saugumo reikalavimų inžinerija
- **Sistemos (angl. Frameworks)**
  - Saugumo reikalavimų inžinerijos sistema: vaizdavimas ir analizė
  - Saugumas pagal ontologiją: į žinias orientuotas požiūris
  - …
- **Procesai**
  - CC pagrįstas saugumo inžinerijos procesas
  - Saugumo reikalavimai programinės įrangos produktų linijoms
  - Reikalavimų pakartotinis panaudojimas siekiant pagerinti sistemos saugumą
  - …
- **Metodai**
  - Secure Tropos
  - SQUARE
  - SREBP
  - …

Funded by the Erasmus+ Programme of the European Union

Kibernetinio saugumo taisyklės ir įstatymai

1996 m. HIPPA – sveikatos draudimo perkeliamumo ir apskaitos įstatymas (anlg. Health Insurance Portability and Account Act)

1999 m. GLBA – Gramm-Leach-Bliley aktas

2003 m. FISMA – Federalinis informacijos saugumo valdymo įstatymas (angl. Federal Information Security Management Act)

2018 m. GDPR – Bendrasis duomenų apsaugos reglamentas (angl. General Data Protection Regulation)

2020 m. CCPA – Kalifornijos vartotojų privatumo įstatymas (angl. California Consumer Privacy Act)

Nauji kibernetinio saugumo metodai ir strategijos

- **MFA** – daugiapakopis (angl. multi-factor autentifikavimas
- **NBA** – tinklo elgsenos analizė
  - nustatyti kenkėjiškus failus pagal elgsenos nukrypimus ar anomalijas
- **Grėsmių žvalgyba** ir atnaujinimų automatizavimas
- **Apsauga realiu laiku**
  - Prieigos metu atliekamas skenavimas, foninė apsauga, apsauga realiu laiku (angl. resident shield) ir automatinė apsauga
- **Testinė aplinka (angl. Sandboxing)**
  - izoliuota bandymų aplinka, kurioje galima paleisti įtartiną failą arba URL adresą.
- **Teismo analizė (angl. Forensics)**
  - atakų atkūrimas, padedantis saugumo komandoms geriau sušvelninti būsimus pažeidimus
- **Atsarginės kopijos** ir dubliavimas (angl. Mirroring)
- **WAF** – žiniatinklio programų ugniasienės
  - nuo kryžminio svetainės klastojimo (angl. cross-site forgery), kryžminio svetainės scenarijų rašymo (angl. ross-site-scriptingXSS), failų įtraukimo ir SQL injekcijos.

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

Funded by the Erasmus+ Programme of the European Union

Santrauka

- Telefoniniai apgavikai
- Pirmieji įsilaužimai
- Atsiranda kompiuterinis saugumas
- Kompiuterinis virusas
- Įsilaužėlių grupės
- Didžiausi pažeidimai
- Kibernetinio saugumo patentas
- CERT
- Antivirusinių programų pramonė
- SSL
- Saugumo sistemos
- Reglamentai ir įstatymai

Užduotys

Aptarkite, ko reikėtų pasimokyti iš telefoninių apgavikų atvejų.

Palyginkite ***I LOVE YOU*** ir ***WannaCry*** atakas

Kokias kibernetinio saugumo sistemas (angl. famewroks) studijavote arba apie kurias skaitėte?

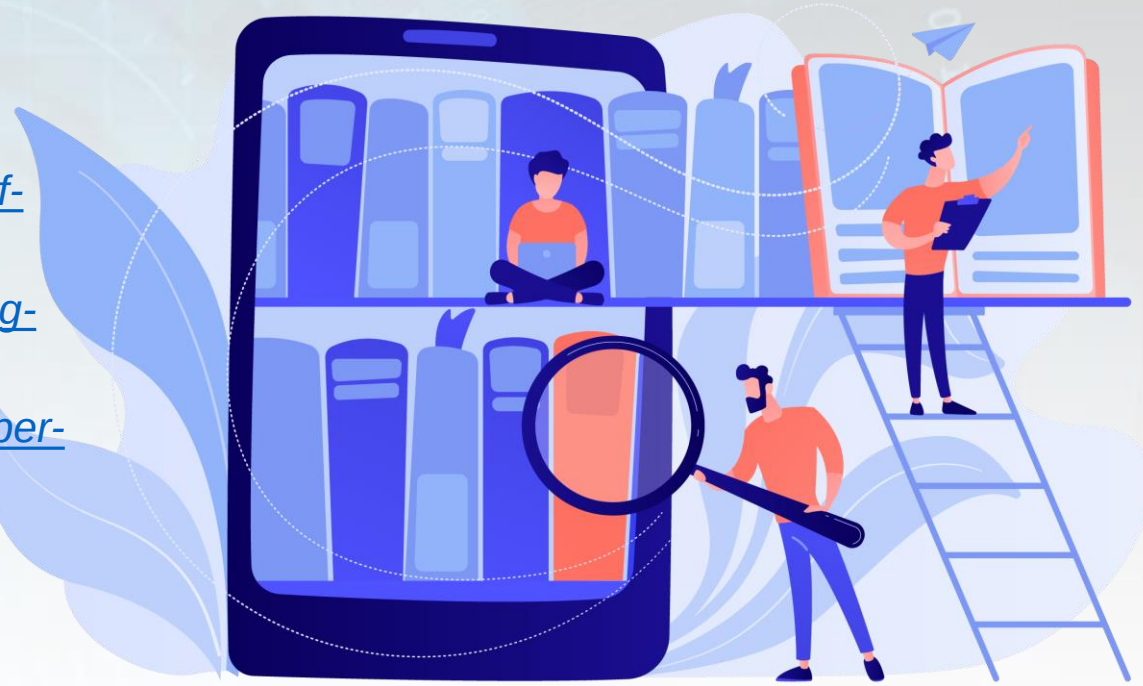
Funded by the Erasmus+ Programme of the European Union

Papildomi skaitiniai

Kibernetinio saugumo istorija

Medžiaga, naudota rengiant šią pateiktį

- 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



Trumpi vaizdo įrašai

- Trumpa kibernetinio saugumo ir įsilaužimo istorija (EN)

  https://youtu.be/V6p7lFsokXo

- Kibernetinio saugumo istorija (EN)

  https://youtu.be/CFwmTzCVuFQ

- Kibernetinio saugumo raida nuo 80-ųjų iki šių dienų (EN)

  https://youtu.be/wKaRdugeAPs

- Didžiausios kibernetinės atakos istorijoje (EN)

  https://youtu.be/fUeJtM1bgGo

  https://youtu.be/lJc3viPKXk4

Dėkojame!