Funded by the Erasmus+ Programme of the European Union

KIbernetinis saugumas Europos Sąjungoje (ES)

Tendencijų ir Kibernetinio Saugumo Situacijos Apžvalga

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 apie naujausias kibernetinio saugumo tendencijas, kylančias grėsmes ir realijas bei pagrindinius kibernetinio saugumo incidentus.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Studento darbo krūvis

Paskaita	1,5 h
Audio ir video medžiaga	1 h
Atvejų analizė	1,5 h
Tolesni skaitiniai	2 h
Pasirengimas egzaminui	2 h

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

2019-2021

Kibernetinio saugumo grėsmių tendencijos

ENISA duomenimis du pagrindiniai faktai labai prisidėjo prie reikšmingų pokyčių ES kibernetinių grėsmių srityje.

1. *Unikali ir staigi transformacija, kurią sukėlė COVID-19 pandemija*
2. *Nuolatinė pažengusių grėsmių sukėlėjų pajėgumų didėjimo tendencija*

2019-2021

Kibernetinio saugumo grėsmių tendencijos

1. Kibernetinio saugumo srityje toliau plečiasi atakų sritys

2.Po COVID-19 pandemijos išpuoliai taps nauja socialine ir ekonomine norma

3. Rimta tendencija - socialinių tinklų naudojimas tikslinėms atakoms

4. Tikslingos ir nuolatinės atakos prieš didelės vertės duomenis

5. Milžiniškos paskirstytos atakos, trunkančios trumpai ir darančios didelį poveikį

Funded by the Erasmus+ Programme of the European Union

2019-2021

Kibernetinio saugumo grėsmių tendencijos

6. Daugumos kibernetinių atakų motyvacija - finansinė nauda

7. Išpirkos reikalavimas tebėra plačiai paplitęs ir brangiai kainuoja

8. Daugelis kibernetinio saugumo incidentų lieka nepastebėti arba nustatomi vėluojant

9. Organizacijos turi daugiau investuoti į pasirengimą apsisaugoti

10. Fišingo aukų skaičius tebeauga

Funded by the Erasmus+ Programme of the European Union

Top Threats 2018		Assessed Trends
1	Malware	-----
2	Web-based attacks	↗
3	Web application attacks	-----
4	Phishing	↗
5	Denial of service	↗
6	Spam	-----
7	Botnets	↗
8	Data Breaches	↗
9	Insider threat	↙
10	Physical manipulation, damage, theft	-----
11	Information leakage	↗
12	Identity theft	↗
13	Cryptojacking	↗
14	Ransomware	↙
15	Cyber espionage	↙

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	-----	-----
2	Web-based attacks	-----	↗
3	Phishing	↗	↗
4	Web application attacks	-----	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data Breaches	-----	-----
9	Insider threat	↗	-----
10	Botnets	↙	↙
11	Physical manipulation, damage, theft	-----	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyber espionage	↙	↗
15	Cryptojacking	↙	↙

Legend: **Trends:** ↙ Declining ----- Stable ↗ Increasing **Ranking:** ↗ Going up ----- Same ↙ Going down

Šaltinis: ENISA "Threat Landscape 2019 -2020" report

Penkios naujos kibernetinių grėsmių tendencijos

1. **Kenkėjiškos programos atnaujinamos**

   Kenkėjiškų programų šeimos atnaujinamos naujomis versijomis su papildomomis funkcijomis ir platinimo mechanizmais, pvz., Emotet

2. **Grėsmės taps visiškai mobilios**

   Vartotojai vis dažniau priklausomi nuo mobilių įrenginių, kad apsaugotų savo jautriausias paskyras.

Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Penkios naujos kibernetinių grėsmių tendencijos

Source: https://www.freepik.com/

3. **Naujų failų tipų naudojimas**

   Pvz.., disko veidrodiniai failai (ISO ir IMG) kenkėjiškos įrangos platinimui

   DOC, PDF, ZIP ir XLS failai yra vis dar tarp plačiausiai naudojamų

4. **Koordinuotų tikslinių išpirkos reikalaujančių atakų skaičiaus didėjimas**

   2019 buvo sudėtingų ir tikslinių išpirkos reikalaujančių atakų metais, pvz., sveikatos ir viešojo sektoriuose

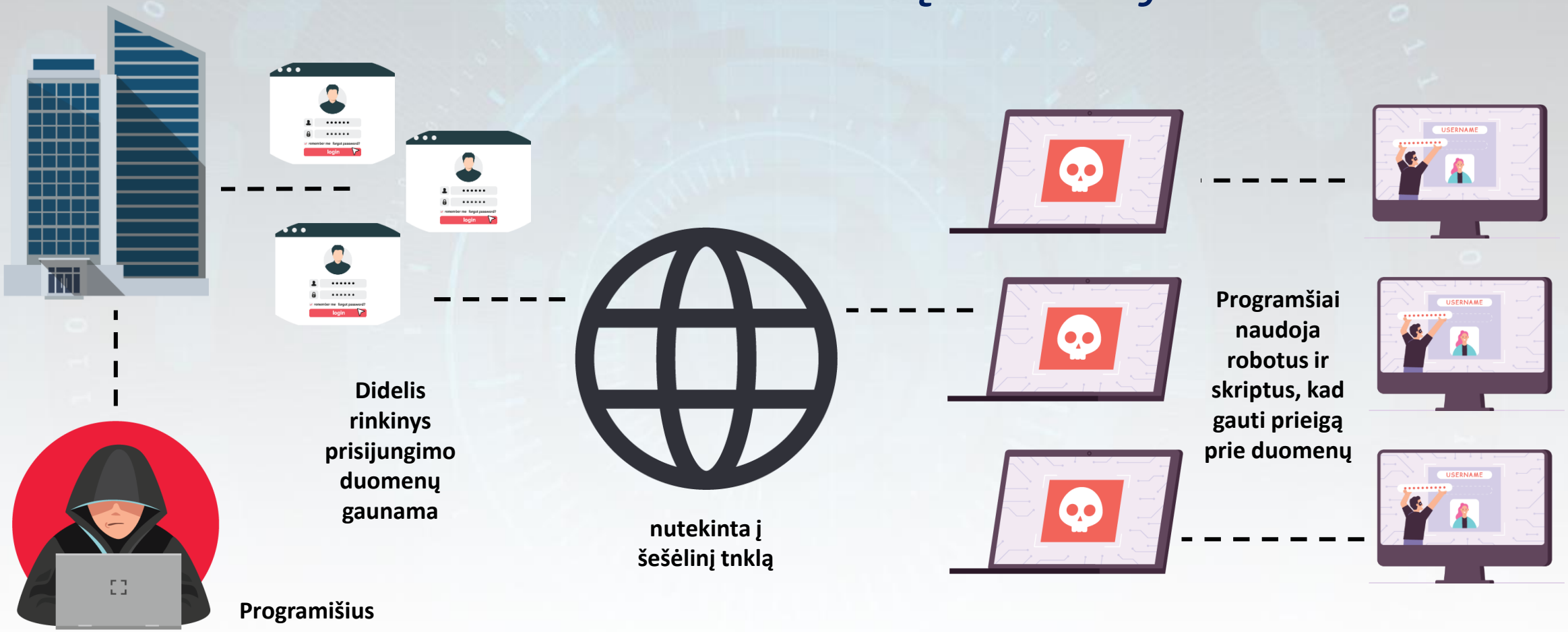
Penkios naujos kibernetinių grėsmių tendencijos

5. **Plačiai paplitusios kredencialų klastojimo atakos**

   Šių atakų skaičius augs, nes per dešimtmetį įvyko neįprastai daug duomenų saugumo pažeidimų ir pasisavinta trilijonai asmens duomenų įrašų.

Source: https://www.freepik.com/

Kredencialų klastojimo atakos



Adaptuota iš Compatech

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Dešimt naujų atakų vektorių krypčių

1. Atakos bus labiau paskirstytos, trumpos trukmės, bet didesnio poveikio
2. Tikslingos ir gerai parengtos atakos bus kruopščiai suplanuotos, siekiant aiškiai apibrėžtų ir ilgalaikių tikslų
3. Piktavaliai vis labiau naudos skaitmenines platformas tikslinėms atakoms

Source: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

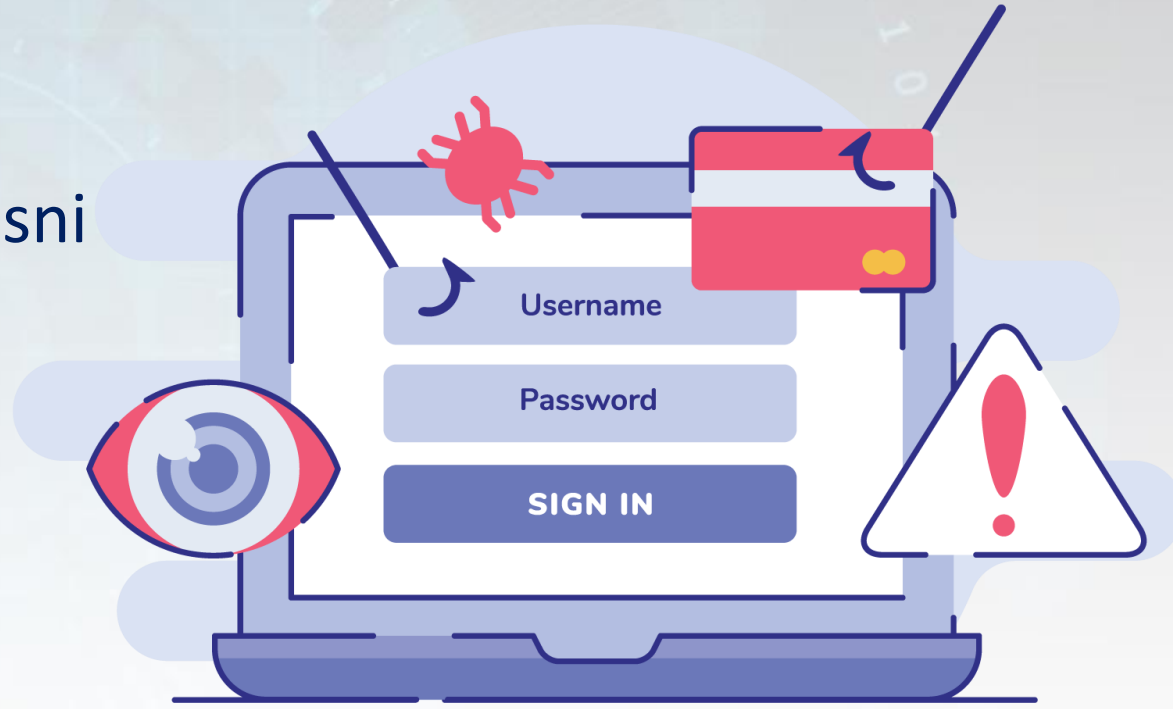
Dešimt naujų atakų vektorių krypčių

4. Padidės verslo procesų pažeidžiamumų išnaudojimas
5. Nutolusio darbo pažedžiamumai bus išnaudojami per asmeninius įrenginius namuose
6. Užpuolikai bus geriau pasirengę

Source: https://www.freepik.com/

Dešimt naujų atakų vektorių krypčių

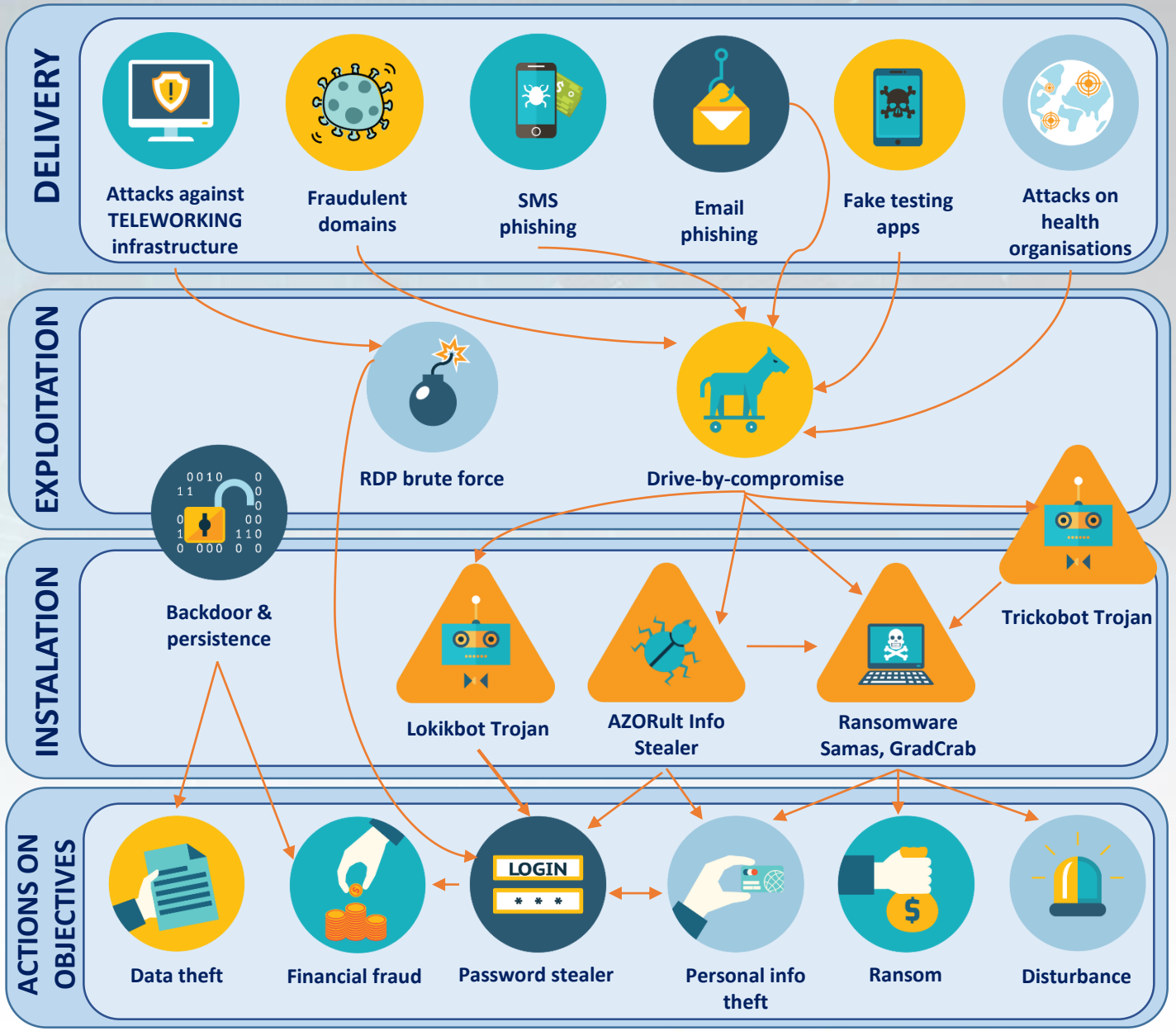
8. Fokusavimo metodai bus sudėtingesni
9. Automatizuotas nebeveikiančių programų ir neapsaugotų sistemų išnaudojimas didės
10. Kibernetinės grėsmės pasieks bet kuriuos taikymus



Šaltinis: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

COVID-19 Grėsmių Vaizdas pagal ENISA



Šaltinis: https://www.enisa.europa.eu/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kibernetinių grėsmių realybė: piliečiai

70 proc. interneto naudotojų kompiuterių ES patyrė bent vieną kenkėjiškos programinės įrangos klasės ataką

549 301 vartotojas ES patyrė išpirkos reikalaujančią ataką

1 523 148 vartotojas ES patyrėmkriptovaliutos kasėjų ataką

visame pasaulyje sukurta 6,95 mln. naujų sukčiavimo ir apgaulės puslapių, o didžiausias naujų sukčiavimo ir apgaulės puslapių skaičius per vieną mėnesį - 206 310 (73 proc. daugiau nei 2019 m.)

Kibernetinių grėsmių realybė: verslas

87 % organizacijų patyrė bandymą pasinaudoti jau žinomu esamu pažeidžiamumu.

46 % organizacijų bent vienas darbuotojas atsisiuntė kenkėjišką mobiliąją programėlę, kuri kelia grėsmę jų tinklams ir duomenims.

Vertnama, kad išpirkos reikalaujančios programos 2020 m. įmonėms visame pasaulyje kainavo 20 mlrd. dolerių, o 2019 m. - 11,5 mlrd. dolerių.

Tyrimai rodo, kad 2020 m. trečiąjį ketvirtį beveik pusė visų išpirkos reikalaujančių programų atvejų buvo susiję su pavogtų duomenų paviešinimo grėsme, o vidutinė išpirkos suma siekė 233 817 JAV dolerių - 30 % daugiau nei 2020 m. antrąjį ketvirtį.

Apskaičiuota, kad iki 2025 m. kibernetiniai nusikaltimai įmonėms visame pasaulyje kasmet kainuos po 10,5 trilijono JAV dolerių, palyginti su 3 trilijonais JAV dolerių 2015 m.

43 proc. kibernetinių atakų nukreiptos prieš mažąsias įmones, tačiau tik 14 proc. jų yra pasirengusios apsisaugoti.

Kibernetinio saugumo realijos ES

2019 m. ES užregistravo apie **450 atakų** prieš ypatingos svarbos infrastruktūros objektus energetikos ir vandens tiekimo sektoriuose, taip pat informacines ir ryšių technologijas sveikatos, transporto ir finansų sektoriuose.

Šaltimis: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

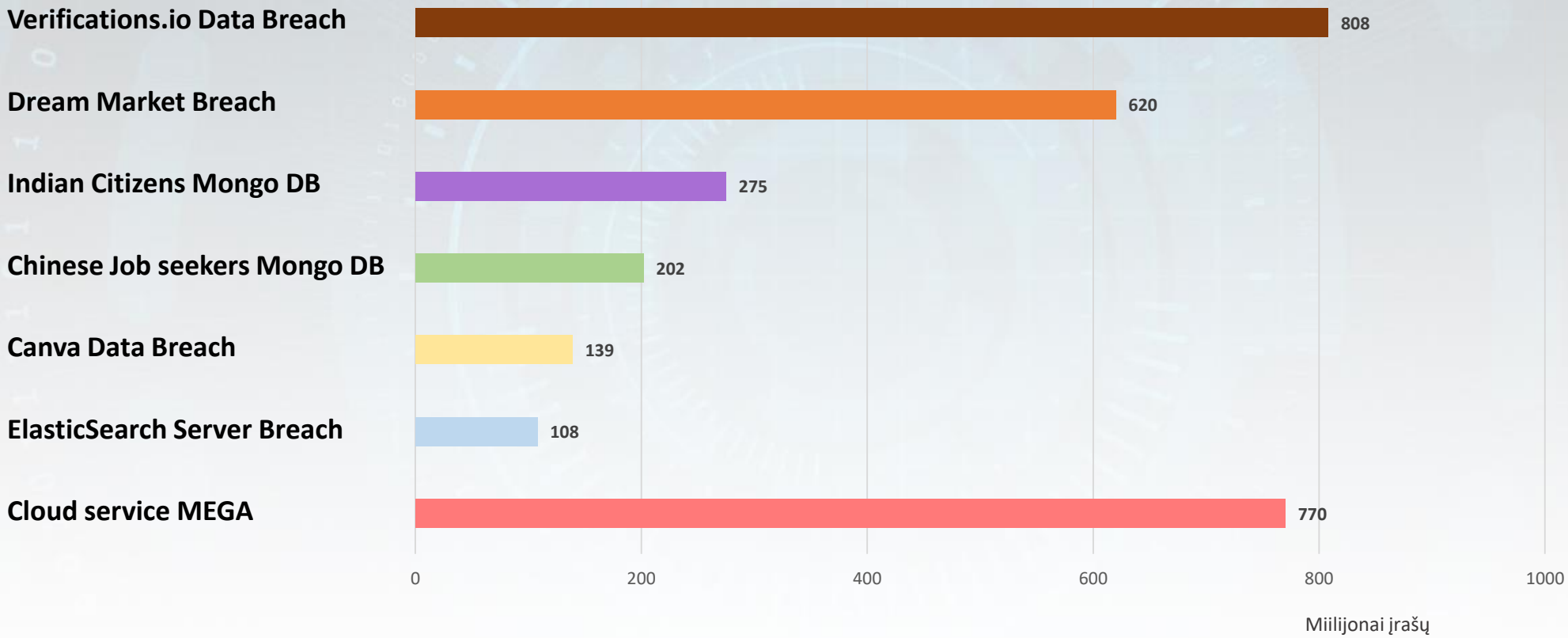
Pagrindiniai kibernetinio saugumo incidentai 2019 - 2021 metais

ENISA Threat Landscape 2020

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Svarbiausi duomenų saugumo pažeidimų incidentai



âltinis: ENISA "Threat Landscape 2020"

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Duomenų saugumo pažeidimai: pagrindinės pasekmės

Informacijos praradimas: Jei dėl duomenų saugumo pažeidimo prarandami neskelbtini asmens duomenys, pasekmės gali būti skaudžios.

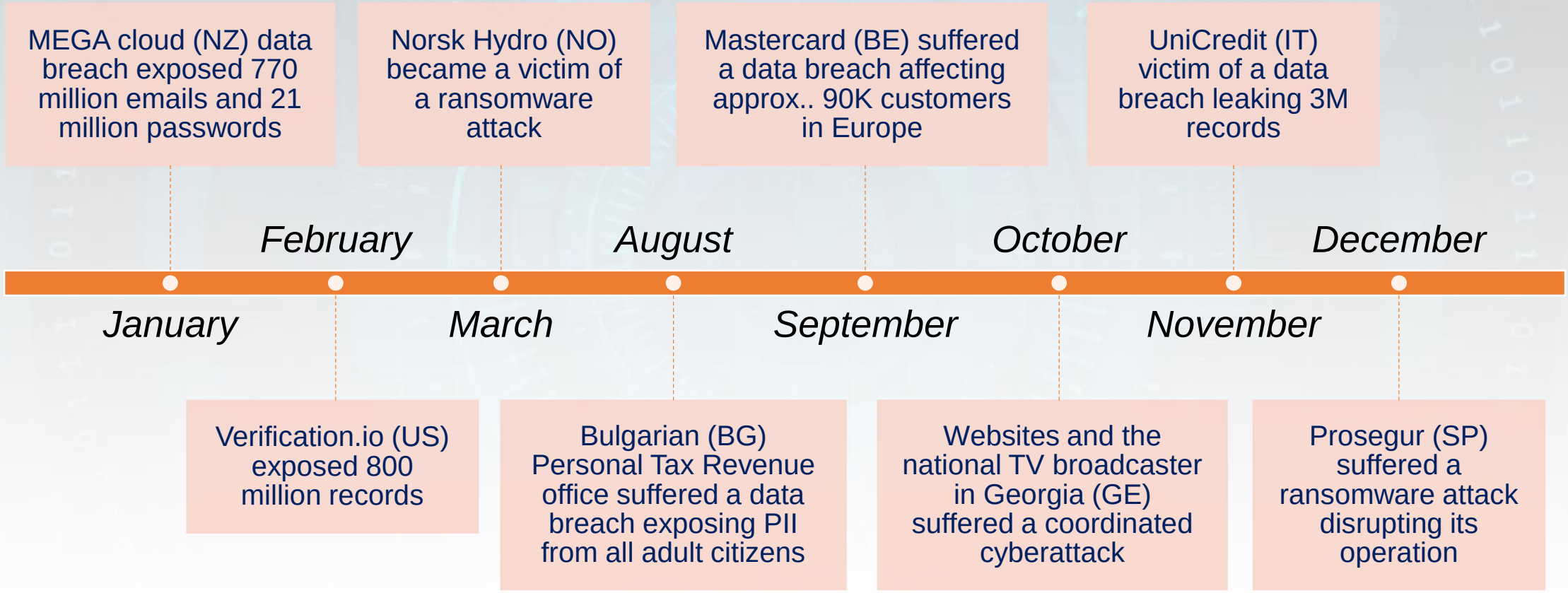
Ieškiniai ir baudos: Reguliavimo ir kolektyvinių ieškinių prieš įmones, kurios nesugeba apsaugoti duomenų, atsiradimas ir nauji įstatymai, pvz., ES Bendrasis duomenų apsaugos reglamentas (BDAR), gali būti naudojami skiriant itin griežtas baudas.

Papildomos investicijos: Organizacijoms gali tekti skirti lėšų sistemų remontui ir architektūros atnaujinimui, taip pat investuoti į naujas kibernetinio saugumo paslaugas ir kibernetinę kriminalistiką.

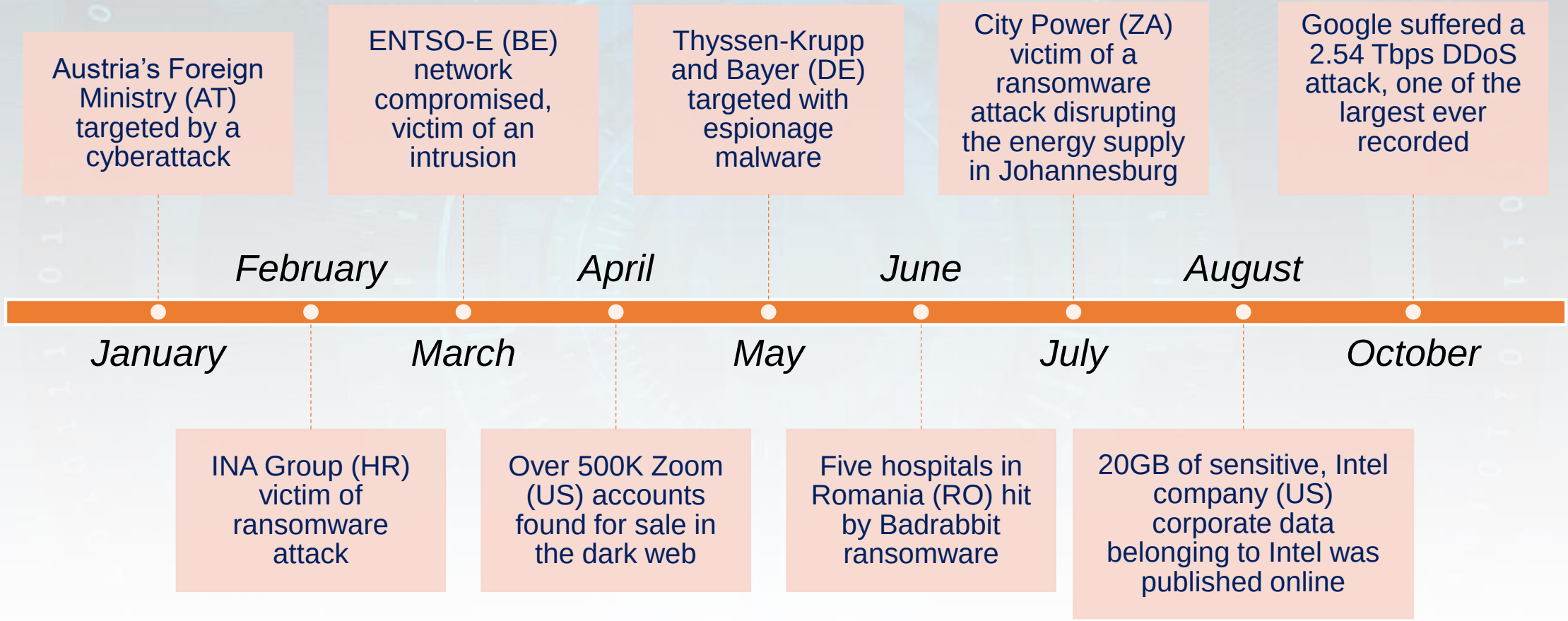
Reputacinė žala: "Forbes Insight" ataskaitoje nustatyta, kad 46 proc. organizacijų dėl duomenų saugumo pažeidimo patyrė reputacinę žalą.

Funded by the Erasmus+ Programme of the European Union

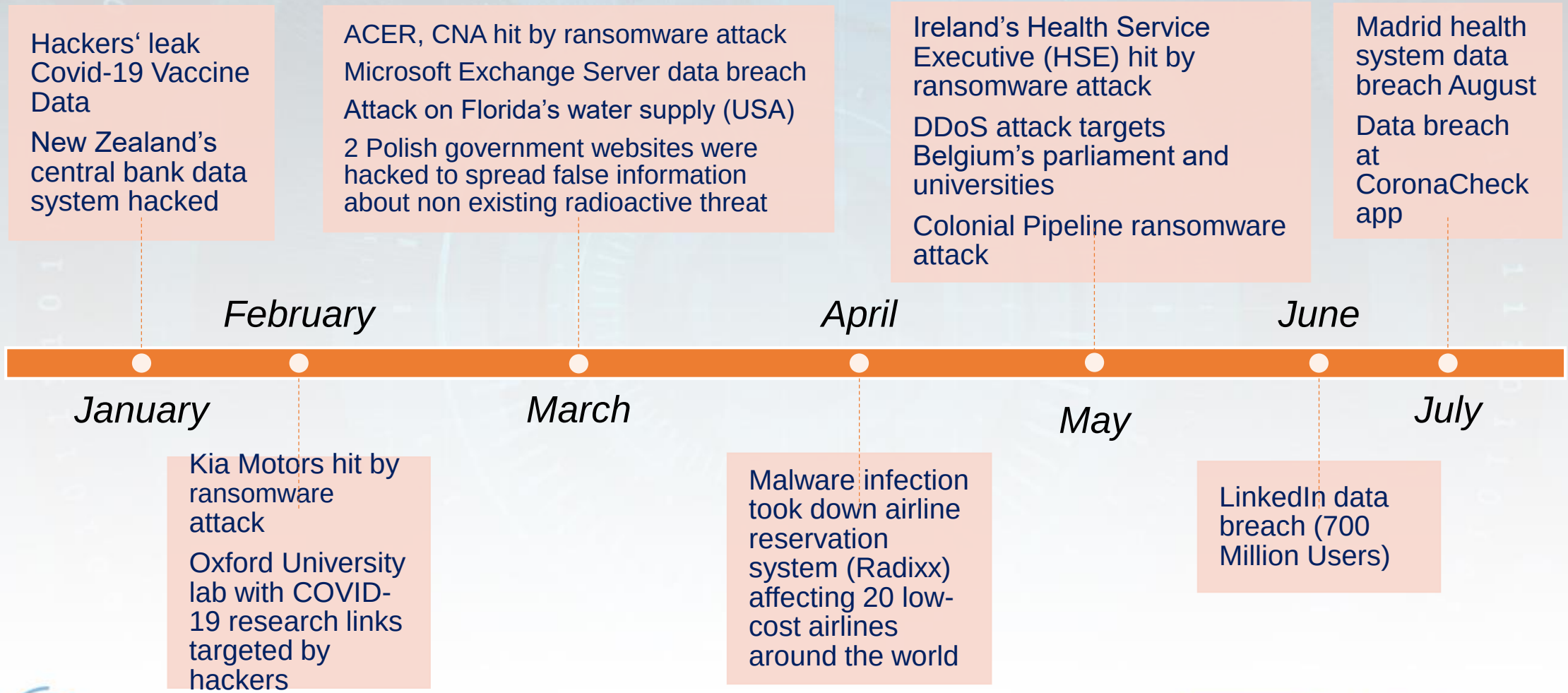
Pagrindiniai kibernetinio saugumo incidentai 2019 metais



Pagrindiniai kibernetinio saugumo incidentai 2020 metais



Kai kurie kibernetinio saugumo incidentai 2021 metais



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Šeši būdai kaip kibernetinis saugumas veikia verslą

Padidėjusios sąnaudos

Veikimo sutrikimai

Pakeista verslo praktika

Žala reputacijai

Lost Revenue

Pavogta intelektinė nuosavybė

Labiausiai atakuoti sektoriai 2019-2020

Skaitmeninės paslaugos

Vyriausybė Valdymas

Technologijos Pramonė

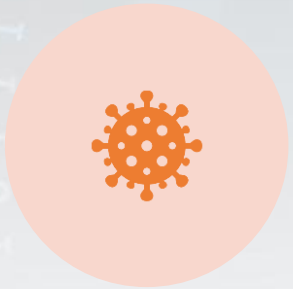
Finansų sektorius

Sveikatos apsauga

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Populiariausis fišingo atakos 2020



COVID-19

Nuotolinis darbas

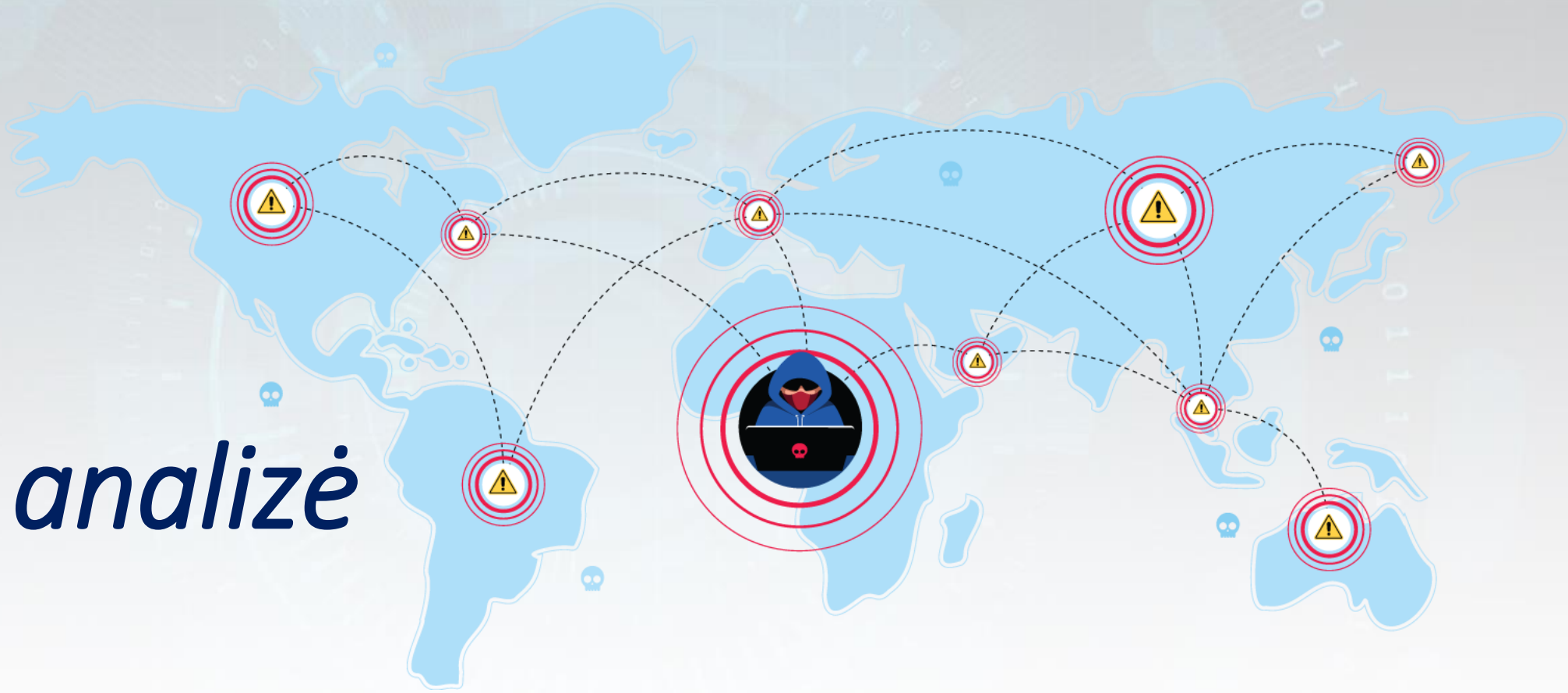
El. komercija

Mažmeninė prekyba

Žaidimai

Atvejų analizė

2020 metai



CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Twitter

Kai kurie iš labiausiai pripažintų ir vertinamų pasaulinių „Twitter“ paskyrų buvo užkrėsti ir panaudoti **melagingų pranešimų "Bitcoin" siuntimui**.

Šaltinis: https://www.freepik.com/

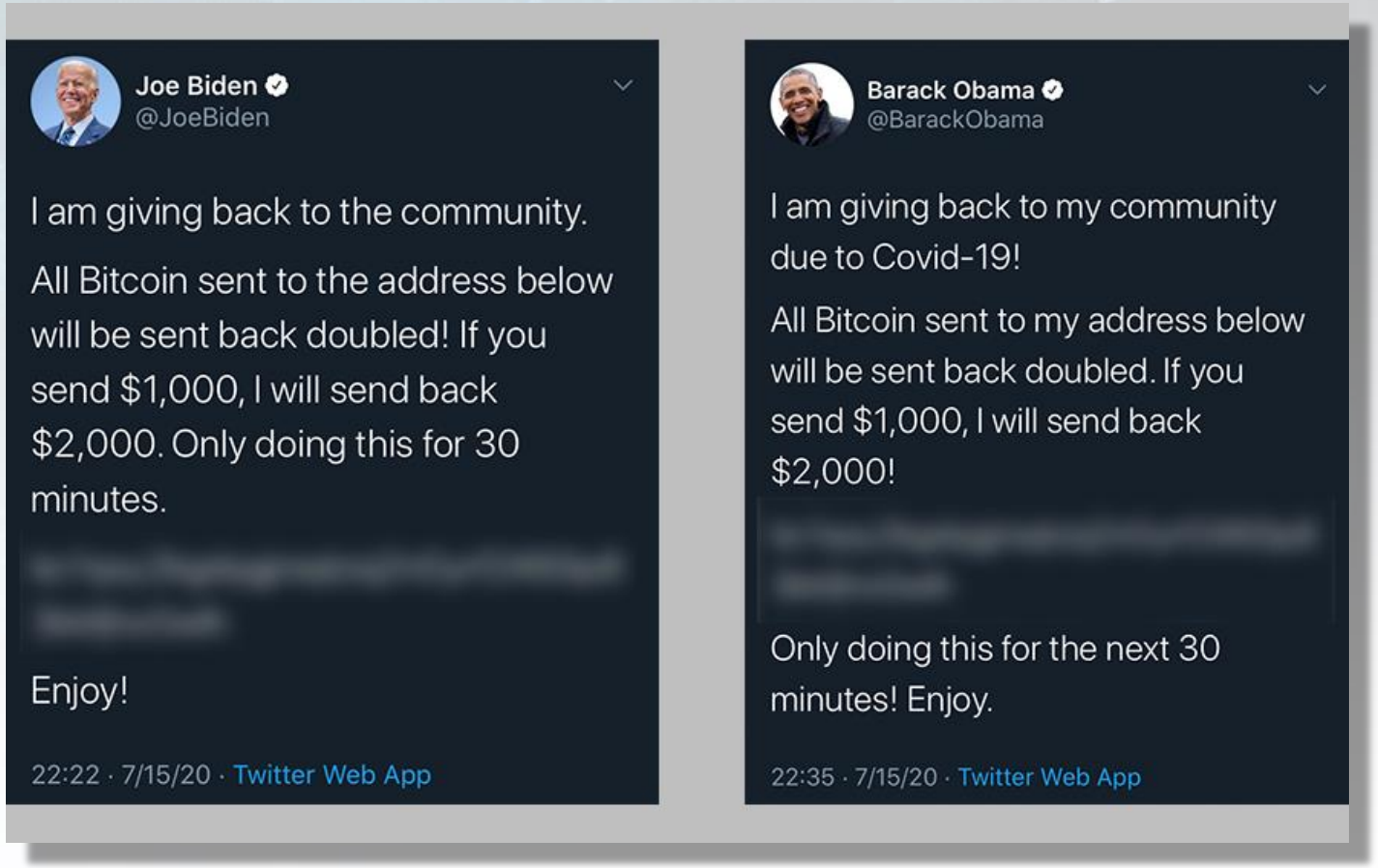
Kaip tai buvo padaryta ?

- Nusikaltėliai naudojo **fišingo** ataką, kad gautų „Twitter“ darbuotojų, kurie turėjo prieigą prie vidinių programinių priemonių, prisijungimo duomenis.
- Twitter išplatino sekantį pranešimą
  - *„Aptikome, kaip manome, koordinuotą socialinės inžinerijos ataką, kurią įvykdė asmenys, sėkmingai nusitaikę į kai kuriuos mūsų darbuotojus, turinčius prieigą prie vidaus sistemų ir įrankių.“*
- Keliems įtariamiesiems buvo pateikti kaltinimai dėl šios atakos

Funded by the Erasmus+ Programme of the European Union

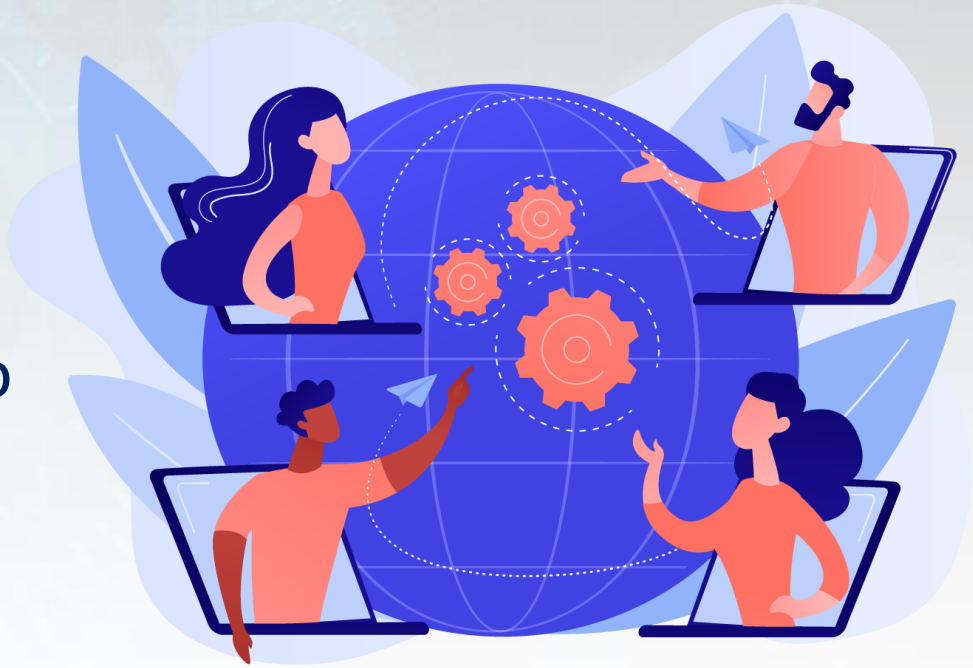
Atakuoti vartotojai

Apple ir Uber buvo tarp kompanijų kurios atakuotos,taip pat tokie asmenys kaip Bill Gates, Elon Musk, Jeff Bezos, Warren Buffett, Kanye West ir Floyd Mayweather



Šaltnis: BBC News

"Zoom" patyrė keletą saugumo incidentų, visų pirma buvo pavogti **apie 500 000 naudotojų paskyrų duomenys**, kurie buvo parduoti nelegalioje rinkoje.



Šaltinis: https://www.freepik.com/

Kaip tai buvo padaryta?

Pranešama, kad paskyrų duomenys buvo gauti naudojant naudotojo ID ir slaptažodžius, kurie tapo žinomi per ankstesnius įsilaužimus, tai kas vadinama kredencialų klastojimu.

Taip įsilaužėliai gavo prieigą prie svarbios asmeninės ir įmonės informacijos, kuri turėjo būti apsaugota. Be to, Zoom prisijungimo vardus buvo lengva atspėti, todėl naudotojai galėjo prisijungti prie susitikimų be kvietimo ir jį pertraukti arba dalytis netinkama medžiaga, taip pat vadinamu **Zoom bombardavimu**.

Funded by the Erasmus+ Programme of the European Union

Graikų bankai

Po to, kai buvo įsilaužta į Graikijos kelionių svetainę, keturi pagrindiniai Graikijos bankai turėjo anuliuoti ir pakeisti maždaug 15 000 klientų kredito ar debeto kortelių.

Šaltinis: https://www.freepik.com/

Kaip tai buvo padaryta ?

- Nėra aišku kaip tai buvo padaryta
- Pagrindinis tyrimo klausimas - ar turizmo svetainėje buvo laikomasi Mokėjimo kortelių duomenų saugumo standartų (PCI DSS)
- Tai ne pirmas kartas, kai buvo atakuojami Graikijos bankai: anksčiau jie patyrė DDoS ir išpirkos reikalaujančias atakas, dėl ko buvo sutrikdyta banko veikla (internetinė bankininkystė)

Funded by the Erasmus+ Programme of the European Union

Ligoninė Čekijoje

Brno Universiteto ligoninė Čekijoje patyrė kiberataką per patį COVID19 pandemijos įkarštį

Šaltinis: https://www.freepik.com/

Ligoninė turėjo:

- *atidėti skubias chirurgines intervencijas ir nukreipti skubius pacientus į netoliese esančią Šv. Onos universitetinę ligoninę*
- *išjungti vsą vidinį IT tiinklą incidento metu*

Santrauka

- 2019 m. padidėjo grėsmių sudėtingumas - daugelis kibernetinių nusikaltėlių naudoja specialias priemones, kredencialų vagystes ir daugiapakopes atakas.
- Duomenų saugumo pažeidimų skaičius išlieka labai didelis, o pavogtos jautrios inansinės informacijos ir naudotojų prisijungimo duomenų kiekis vis didėja.
- ENISA prognozuoja, kad ateinantį dešimtmetį kibernetinio saugumo riziką ir grėsmes bus vis sunkiau aptikti ir įvertinti, nes grėsmių apimtys tampa vis sudėtingesnės, o atakų mastas - vis didesnis.

Pratimai

Panagrinėkite pateiktas situacijas

- *Aptarkite, kokios galimos pasekmės gali būti tiek užpultoms įmonėms, tiek naudotojams?*
- *Aptarkite, kokias kibernetinio saugumo incidentų tendencijas matysime 2022 m.? Ko turėtume tikėtis ateinančiais metais?*
- *Aptarkite kvalifikacijos kėlimo svarbą atsižvelgiant į galimą kibernetinių atakų keliamą riziką.*

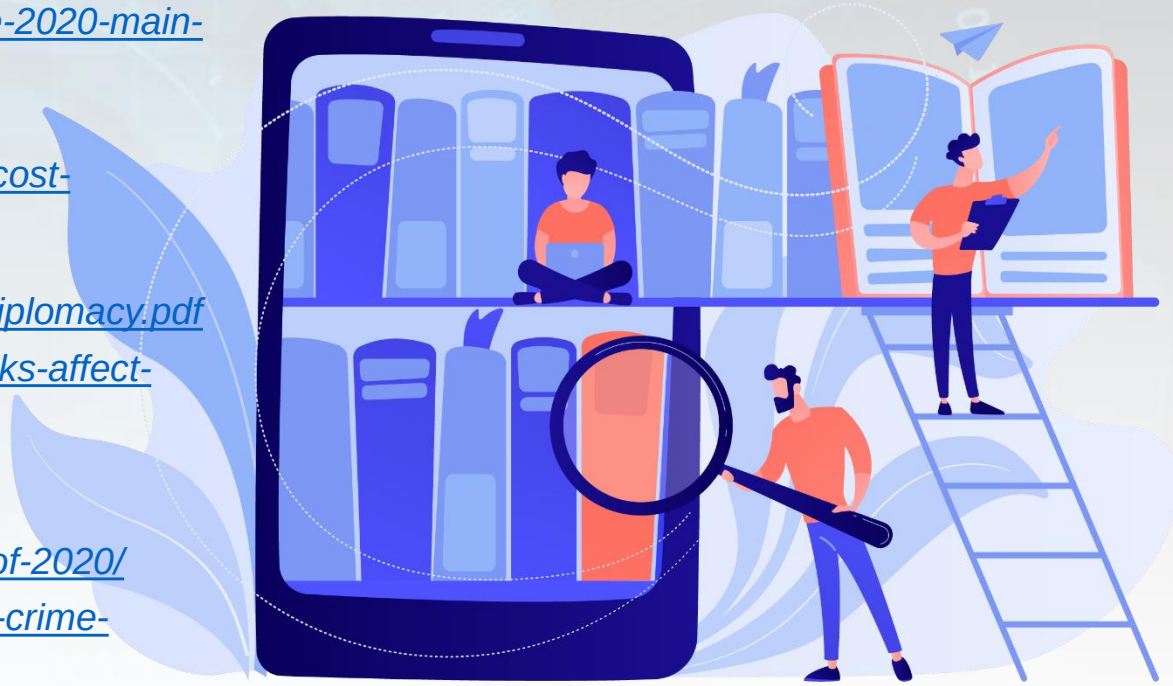
Funded by the Erasmus+ Programme of the European Union

Tolesni skaitiniai

Kibernetinio saugumo būklės tendecijų apžvalga

Medžiaga naudota ruošiant paskaitą

- https://www.enisa.europa.eu/publications/year-in-review
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents
- https://www.enisa.europa.eu/publications/emerging-trends
- https://www.zdnet.com/article/todays-mega-data-breaches-now-cost-companies-392-million-in-damages-lawsuits/
- https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf
- https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/
- https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF
- https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/
- https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
- https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency
- https://auth0.com/blog/what-is-credential-stuffing/



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Trumpi vaizdo įrašai

- Martin Casado apie naujas kiberatakas

  https://youtu.be/AQP0On85ZdQ

- 5 pavojingiausi atakų būdai ir kaip kovoti su jais

  https://youtu.be/xz7IFVJf3Lk

- 10 kibernetinio saugumo vystymosi krypčių

  https://youtu.be/kkP9URO8XJ8

Funded by the Erasmus+ Programme of the European Union

Dėkojame!