Funded by the Erasmus+ Programme of the European Union

Kiberdrošība Eiropas Savienībā (ES)

Pārskats par kiberdrošības reljefa tendencēm

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

Uzzināt vairāk par jaunākajām kiberdrošības tendencēm, jauniem draudiem un realitāti, kā arī par galvenajiem kiberdrošības incidentiem.

Kursantu darba slodze

Lekcija	1,5 st.
Audio un video materiāli	1 st.
Pētījumi	1,5 st.
Papildu lasīšana	2 st.
Sagatavošanās eksāmenam	2 st.

2019. – 2021. gads

Kiberdrošības draudu tendences

Saskaņā ar ENISA datiem divi galvenie fakti ir būtiski veicinājuši būtiskas izmaiņas ES kiberdraudu vidē

1. *Unikāli, pēkšņas transformācijas spēki, ko izraisījusi COVID-19 pandēmija*
2. *Pastāvīgi pieaugoša tendence draudu dalībnieku progresīvās pretinieka spējās*

Funded by the Erasmus+ Programme of the European Union

2019. – 2021. gads

Kiberdrošības draudu tendences

1. Kiberdrošības uzbrukumu placdarms turpina paplašināties

2. Uzbrukumi būs jauna sociālā un ekonomiskā norma pēc Covid-19 pandēmijas

3. Nopietna tendence – sociālo mediju platformu izmantošana mērķtiecīgos uzbrukumos

4. Precīzi mērķēti un pastāvīgi uzbrukumi augstvērtīgiem datiem

5. Masīvi izplatīti uzbrukumi ar īsu laika periodu, bet plašu ietekmi

Funded by the Erasmus+ Programme of the European Union

2019. – 2021. gads

Kiberdrošības draudu tendences

6. Vairuma kiberuzbrukumu motivācija ir finansiāla

7. Izspiedējprogrammatūra (*angl. ransomware*) joprojām ir plaši izplatīta un izraisa apjomīgus zaudējumus

8. Daudzi kiberdrošības incidenti paliek nepamanīti vai paiet ilgs laiks, lai tos atklātu.

9. Organizācijas vairāk ieguldīs gatavībā sevi aizsargāt

10. Pikšķerēšanas upuru skaits turpina pieaugt

Funded by the Erasmus+ Programme of the European Union

2018. gada lielākie draudi		Novērtētās tendences
1	Ļaunprātīga programmatūra	-----
2	Tīmekļa uzbrukumi	↗
3	Tīmekļa lietojumprogrammu uzbrukumi	-----
4	Pikšķerēšana	↗
5	Pakalpojuma atteikums	↗
6	Mēstules	-----
7	Botu tīkli	↗
8	Datu pārkāpumi	↗
9	Iekšienes draudi	↙
10	Fiziskas manipulācijas, bojāšana, zādzība	-----
11	Informācijas noplūdes	↗
12	Identitātes zādzības	↗
13	Kriptolaupīšana	↗
14	Izspiedējprogrammatūra	↙
15	Kiberspiegošana	↙

2019. -2020. gada lielākie draudi		Novērtētās tendences	Izmaiņas rangā
1	Ļaunprātīga programmatūra	-----	-----
2	Tīmekļa uzbrukumi	-----	↗
3	Pikšķerēšana	↗	↗
4	Tīmekļa lietojumprogrammu uzbrukumi	-----	↙
5	Mēstules	↙	↗
6	Pakalpojuma atteikums	↙	↙
7	Identitātes zādzības	↗	↗
8	Datu pārkāpumi	-----	-----
9	Iekšienes draudi	↗	-----
10	Botu tīkli	↙	↙
11	Fiziskas manipulācijas, bojāšana, zādzība	-----	↙
12	Informācijas noplūdes	↗	↙
13	Izspiedējprogrammatūra	↗	↗
14	Kiberspiegošana	↙	↗
15	Kriptolaupīšana	↙	↙

Skaidrojums: **Tendences:** ↙ Samazinās ----- Nemainās ↗ Palielinās **Rangs:** ↗ Pieaug ----- Nemainīgs ↙ Samazinās

CyberPhish
Safeguarding your digital future

Avots: ENISA 2019. - 2020. gada Apdraudējumu reljefa pārskats

Funded by the Erasmus+ Programme of the European Union

Piecas jaunas tendences saistībā ar kiberdraudiem

1. **Ļaunprātīgā programmatūra tiek būtiski jaunināta**

   Ļaunprātīgo programmu saimes celmi tiek jaunināti jaunās versijās ar papildu funkcijām, izplatīšanas un izplatīšanas mehānismiem, piemēram, Emotet

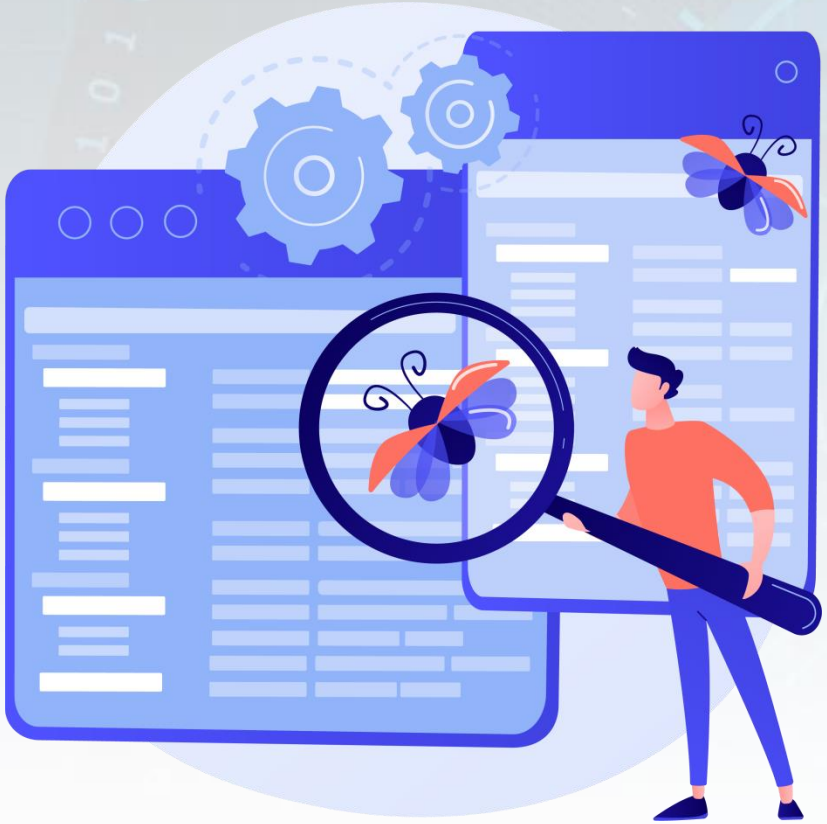
2. **Draudi kļūs pilnībā mobili**

   Lai aizsargātu savus sensitīvākos kontus, lietotāji arvien vairāk ir atkarīgi no mobilajām ierīcēm

Avots: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

Piecas jaunas tendences saistībā ar kiberdraudiem



Avots: https://www.freepik.com/

3. **Jaunu failu tipu izmantošana**

   Piemēram, diska attēlu faili (ISO un IMG) ļaunprātīgas programmatūras izplatīšanai

   Joprojām visbiežāk tiek izmantoti DOC, PDF, ZIP un XLS faili

4. **Koordinētu un mērķtiecīgu izspiedējvīrusu uzbrukumu pieaugums**

   2019. gadā tas bija sarežģītu un mērķtiecīgu izspiedējvīrusu ļaunprātīgas izmantošanas eskalācija, piemēram, veselības un valsts sektorā.

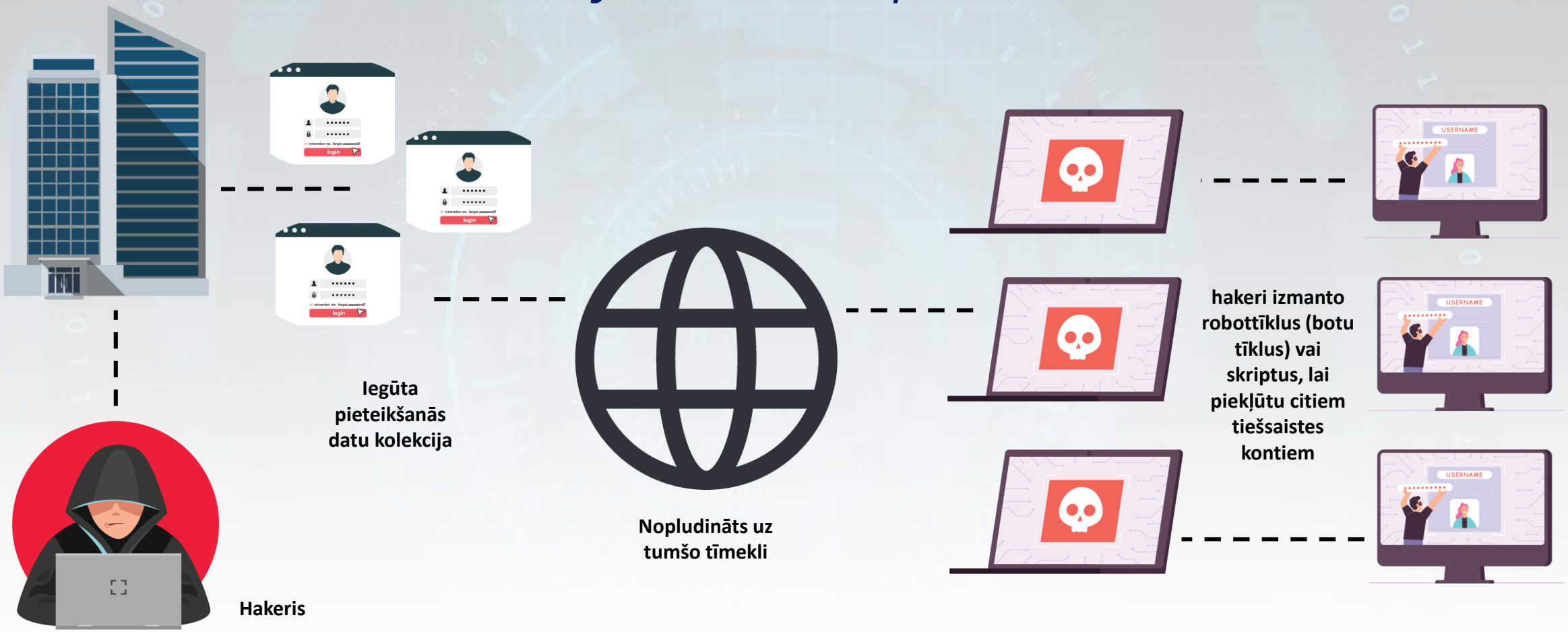
Piecas jaunas tendences saistībā ar kiberdraudiem

5. **Plaši izplatīti akreditācijas datu iepildīšanas uzbrukumi**

   Šie uzbrukumi izplatīsies veselas desmitgades rezultātā, kuras laikā tika nozagts neparasti daudz datu un triljoniem personu datu ierakstu.

Avots: https://www.freepik.com/

Akreditācijas datu iepildīšanas uzbrukums



Adaptēts no Comparitech

Desmit jaunas tendences uzbrukuma vektoros

1. Uzbrukumi tiks plaši izplatīti ar īsu laiku periodu, bet plašāku ietekmi
2. Precīzi mērķēti un pastāvīgi uzbrukumi tiks rūpīgi plānoti ar labi definētiem un ilgtermiņa mērķiem
3. Ļaunprātīgi dalībnieki mērķtiecīgiem uzbrukumiem izmantos digitālās platformas

Avots: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

Desmit jaunas tendences uzbrukuma vektoros

4. Palielināsies biznesa procesu nelabvēlīga izmantošana
5. Uzbrukuma placdarms turpinās paplašināties
6. Tāldarbs tiks nelabvēlīgi izmantots caur mājas ierīcēm
7. Uzbrucēji būs labāk sagatavoti

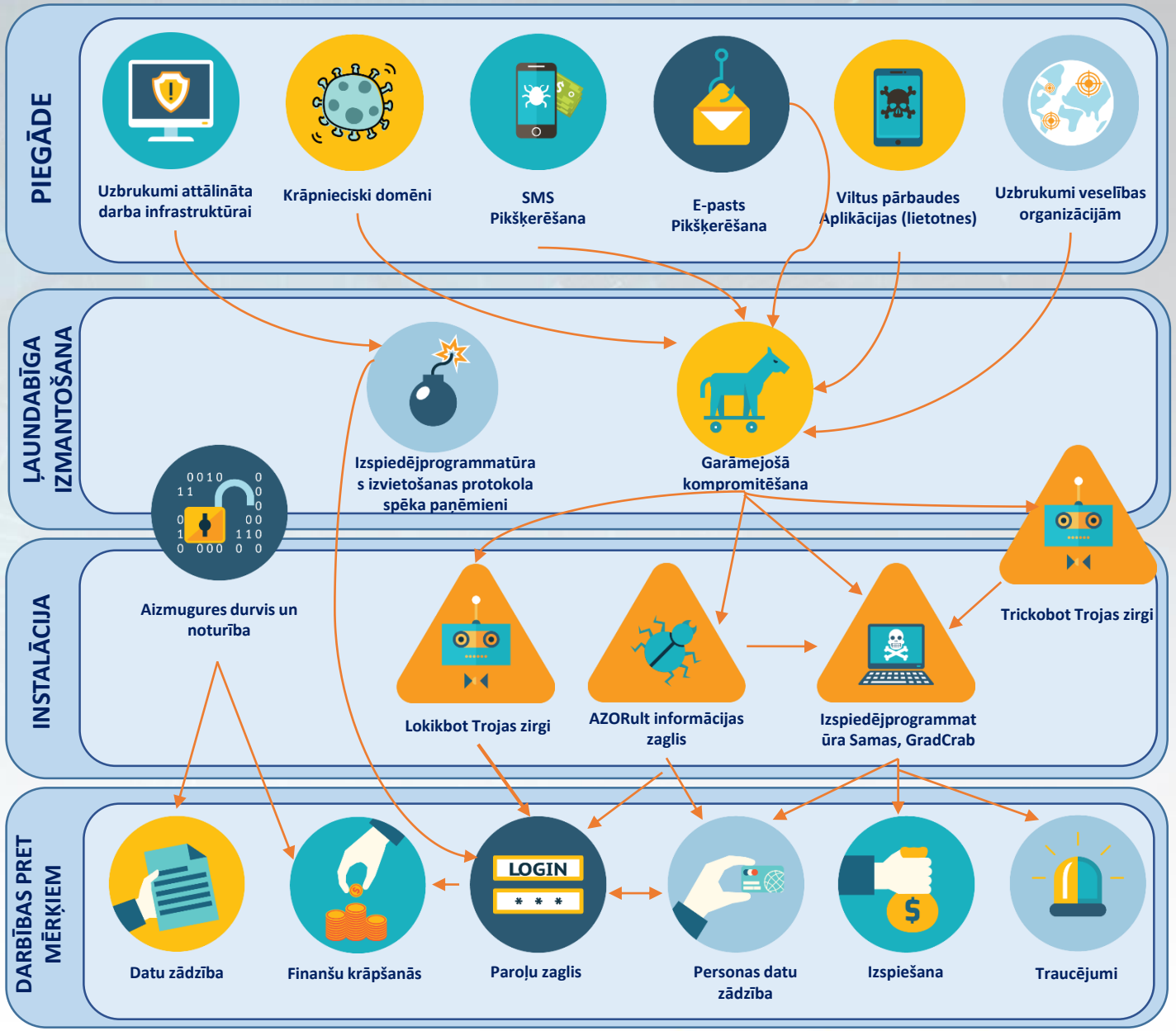
Avots: https://www.freepik.com/

Desmit jaunas tendences uzbrukuma vektoros

8. Apmulsināšanas metodes būs sarežģītākas
9. Palielināsies pārtraukto lietojumprogrammu un neizlabotu sistēmu automatizēta izmantošana
10. Kiberdraudi virzās uz nomalēm

Avots: https://www.freepik.com/

COVID-19 Draudu reljefs, izstrādātājs – ENISA



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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kiberdrošības realitātes: Iedzīvotāji

70% interneta lietotāju datoru ES ir piedzīvojuši vismaz vienu ļaunprātīgas programmatūras klases uzbrukumu

549 301 unikālam lietotājam ES ir uzbrukusi izspiedējvīrusa programmatūra

1 523 148 unikāliem lietotājiem ES ir uzbrukuši datu racēji

Visā pasaulē izveidoti 6,95 miljoni jaunu pikšķerēšanas un krāpniecības vietņu, un lielākais jauno pikšķerēšanas un krāpniecības vietņu skaits vienā mēnesī ir 206 310 (pieaugums par 73% salīdzinājumā ar 2019. gadu).

Funded by the Erasmus+ Programme of the European Union

Kiberdrošības realitātes: Uzņēmējdarbība un darījumu pasaule

87% organizāciju ir piedzīvojušas jau zināmas, esošās ievainojamības, izmantošanas mēģinājumu

46% organizāciju vismaz viens darbinieks ir lejupielādējis ļaunprātīgu mobilo lietojumprogrammu, kas apdraud viņu tīklus un datus

Tiek lēsts, ka izpirkuma programmatūra uzņēmumiem visā pasaulē ir izmaksājusi 20 miljardus ASV dolāru 2020. gadā, salīdzinot ar 11,5 miljardiem ASV dolāru 2019. gadā.

Pētījumi liecina, ka 2020. gada trešajā ceturksnī gandrīz puse no visiem izpirkuma programmatūras gadījumiem ietvēra zagtu datu izpaušanas draudus, un vidējais izpirkuma maksas maksājums bija 233 817 ASV dolāri, kas ir par 30% vairāk nekā 2020. gada otrajā ceturksnī.

Tiek lēsts, ka kibernoziegumi visā pasaulē līdz 2025. gadam izmaksās 10,5 triljonus USD gadā, salīdzinot ar USD 3 triljoniem 2015. gadā.

43% kiberuzbrukumu ir vērsti pret mazajiem uzņēmumiem, bet tikai 14% ir gatavi sevi aizstāvēt.

Kiberdrošības realitāte ES

2019. gadā ES ir reģistrējusi aptuveni 450 uzbrukumus kritiskajām infrastruktūrām enerģētikas un ūdensapgādes nozarēs, kā arī informācijas un komunikācijas tehnoloģijām veselības, transporta un finanšu nozarēs.

Avots: https://www.freepik.com/

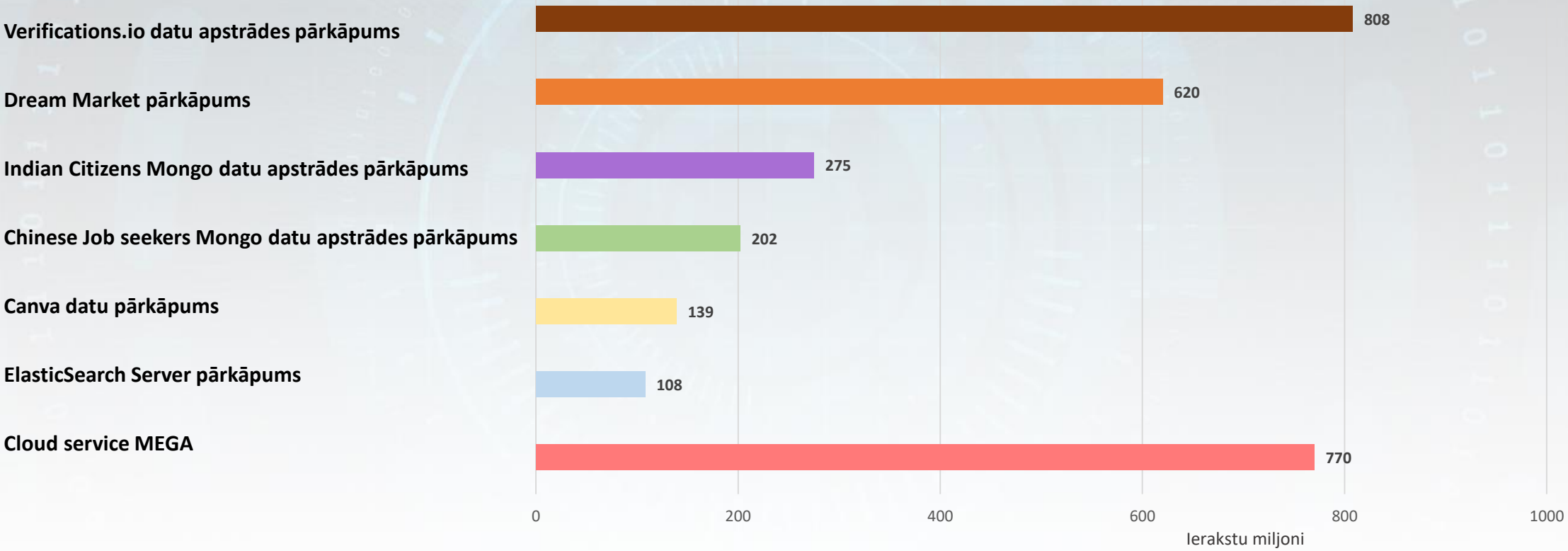
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Galvenie kiberdrošības incidenti 2019. – 2021. gadā

ENISA Apdraudējumu reljefs, 2020. gads

Populārākie datu pārkāpumu incidenti



Avots: ENISA Apdraudējumu reljefs, 2020. gads

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Datu pārkāpumi: Galvenās sekas

Informācijas zudums Ja datu aizsardzības pārkāpuma rezultātā ir zaudēti sensitīvi personas dati, sekas var būt postošas

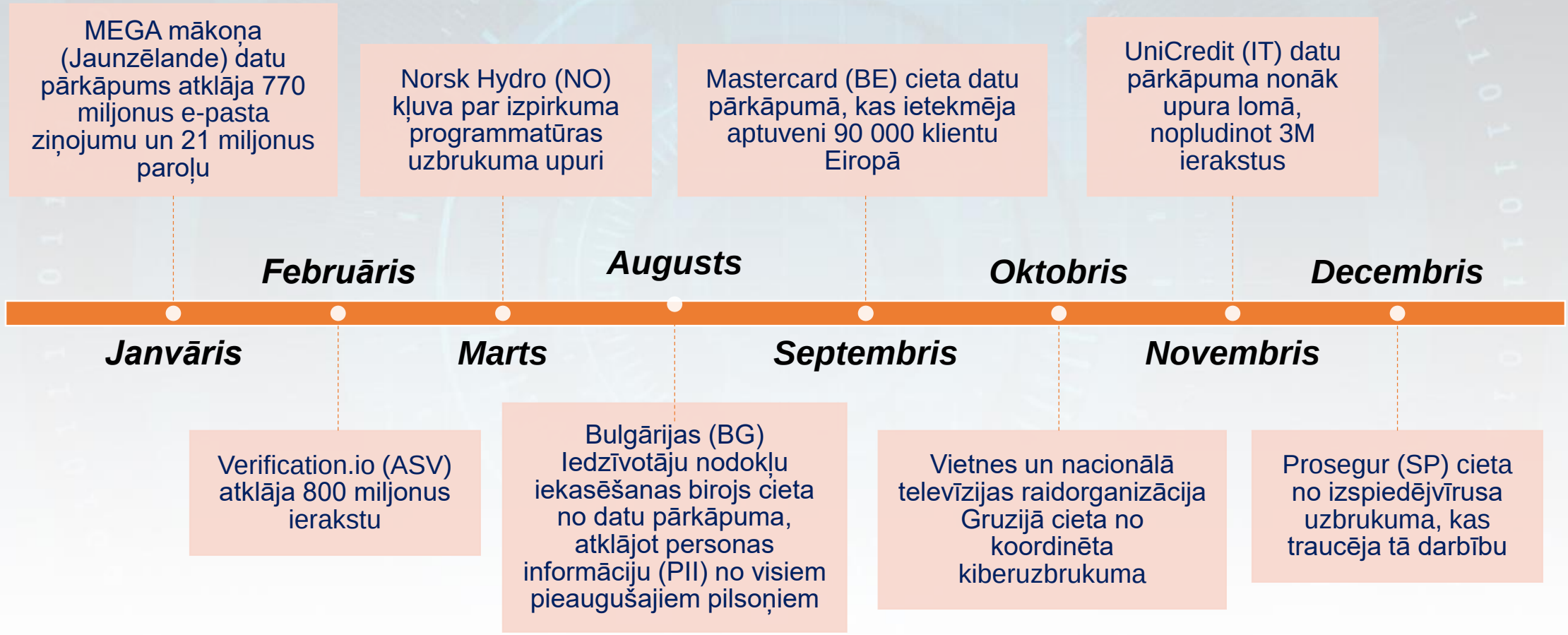
Tiesvedības un sodi: Regulatīvu un kolektīvu prasību rašanās pret uzņēmumiem, kas nespēj aizsargāt datus, un jauni tiesību akti, piemēram, ES GDPR, var tikt izmantoti, lai uzliktu bargus sodus.

Papildu investīcijas: Organizācijām, iespējams, vajadzēs tērēt līdzekļus sistēmu remontam un arhitektūru jauninā̄šanai, kā arī ieguldīt jaunos kiberdrošības pakalpojumos un kiberkriminālistikas ekspertīzē.

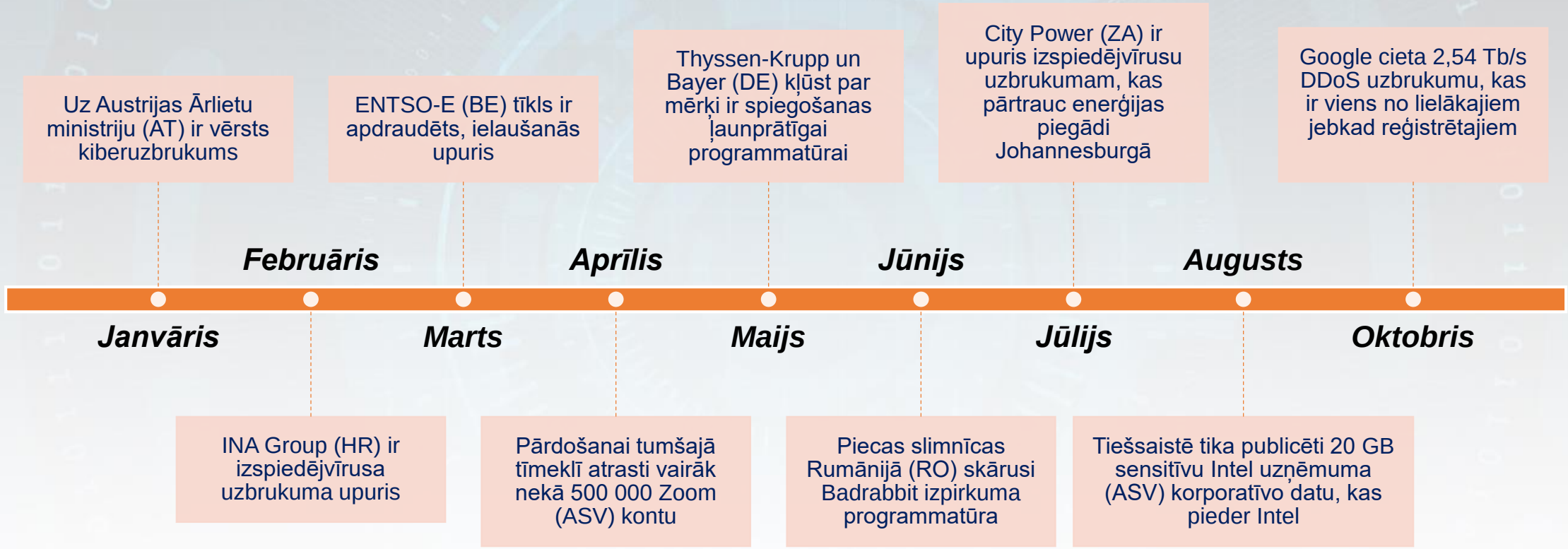
Kaitējums reputācijai: Forbes Insight ziņojumā konstatēts, ka 46% organizāciju ir cietušas reputācijas bojājumus datu pārkāpumu dēļ.

Funded by the Erasmus+ Programme of the European Union

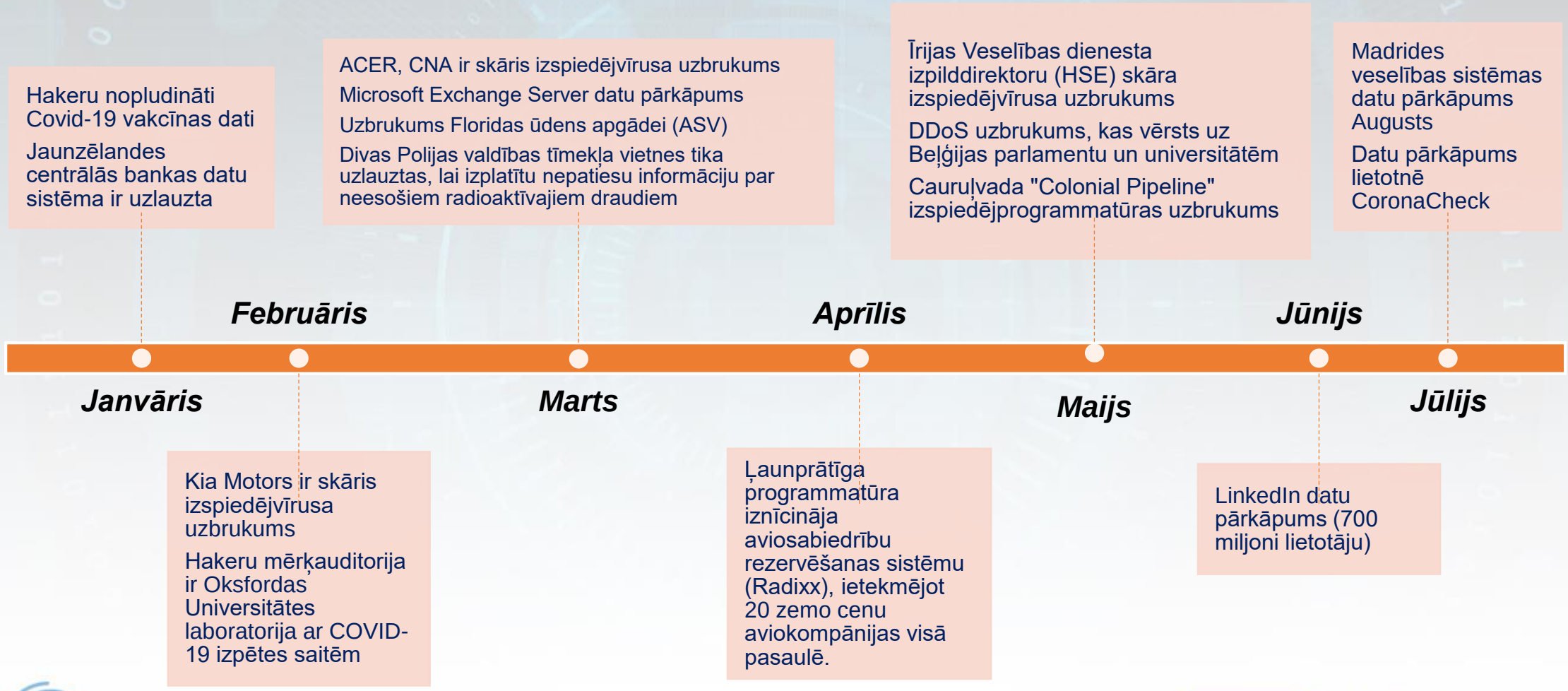
Galvenie kiberdrošības incidenti 2019. gadā



Galvenie kiberdrošības incidenti 2020. gadā



Kiberdrošības incidentu piemērs 2021. gadā



Seši veidi, kā kibernoziegumi ietekmē uzņēmējdarbību

Palielinātas izmaksas

Darbības traucējumi

Piespiedu izmaiņas uzņēmējdarbības praksē

Reputācijas kaitējums

Negūta peļņa

Nozagts intelektuālais īpašums

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Nozares, kas visvairāk nokļuvušas mērķa lomā no 2019. līdz 2020. gadam

- Digitālie pakalpojumi
- Valsts administrācija
- Tehnoloģiju nozare
- Finanšu nozare
- Veselības aprūpes nozare

Funded by the Erasmus+ Programme of the European Union

Populārākās pikšķerēšanas tēmas 2020. gadā

COVID-19

ATTĀLINĀTAIS DARBS

E-KOMERCIJA

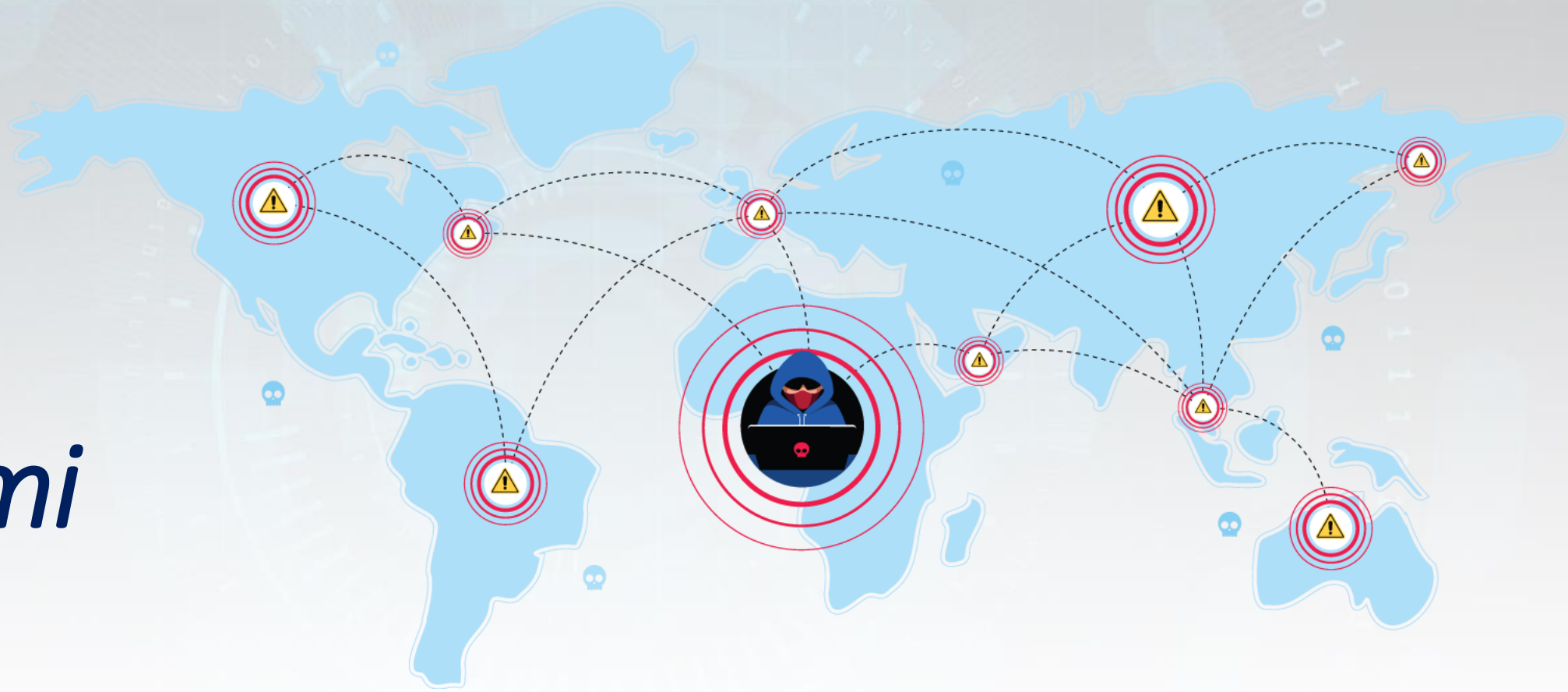
MAZUMTIRDZNIECĪBA

SPĒĻU INDUSTRIJA

Funded by the Erasmus+ Programme of the European Union

Pētījumi

2020. gads



CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Twitter

Daži no atzītākajiem un visaugstāk novērtētajiem globālajiem Twitter vārdiem (kontiem) tika apdraudēti un izmantoti, lai pakalpojumā Twitter nopludinātu krāpnieciskas ziņas par Bitcoin.

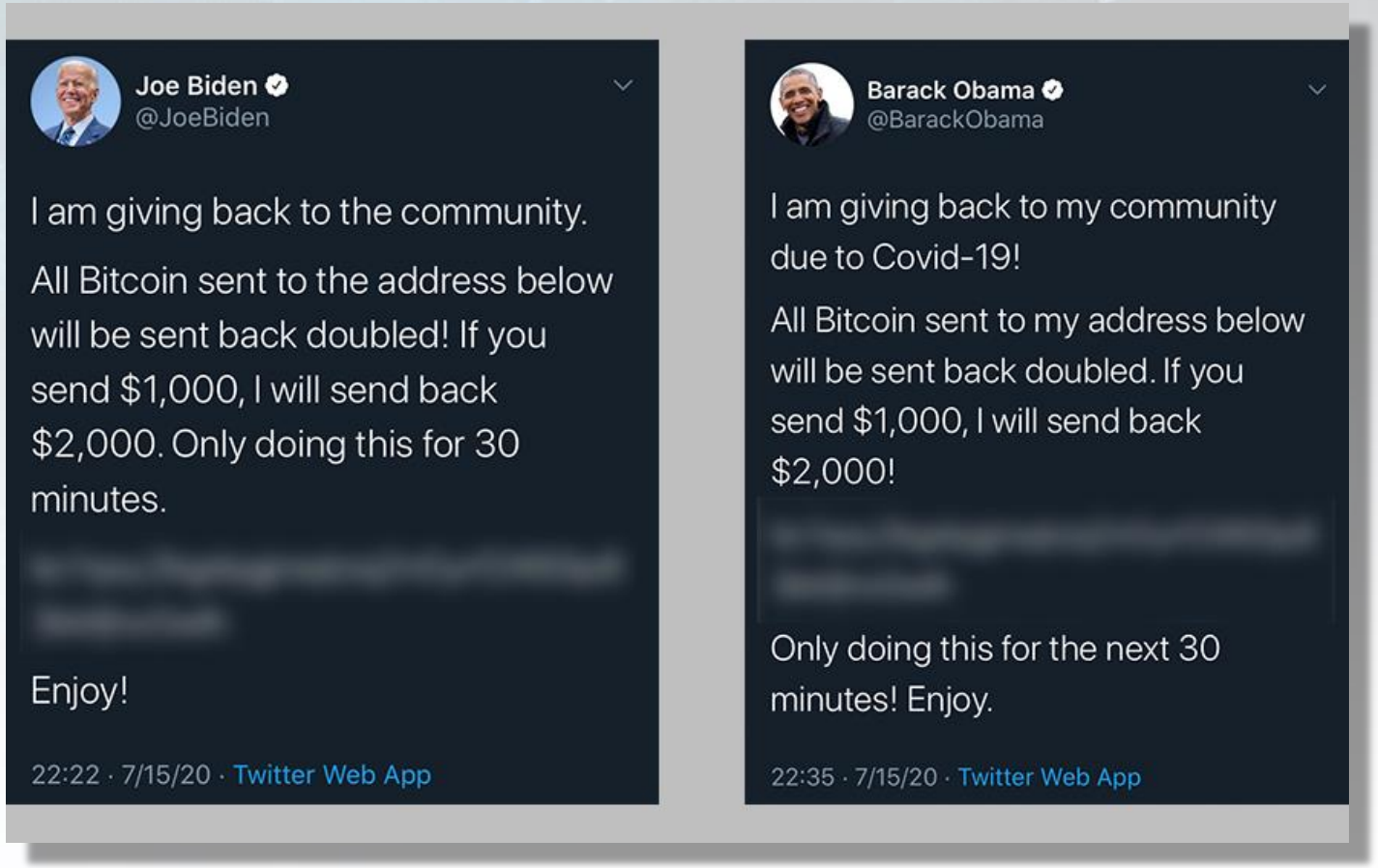
Avots: https://www.freepik.com/

Kā notika īstenošana?

- Noziedznieki izmantoja tālruņa pikšķerēšanas uzbrukumu, lai iegūtu Twitter darbinieku akreditācijas datus, kuriem bija piekļuve iekšējiem atbalsta rīkiem.
- Twitter nāca klajā ar paziņojumu:
  - *"Mēs esam atklājuši, mūsuprāt, koordinētu sociālās inženierijas uzbrukumu, ko veica cilvēki, kuri veiksmīgi uzbruka dažiem mūsu darbiniekiem, kuriem bija piekļuve iekšējām sistēmām un rīkiem."*
- Vairākiem aizdomās turamajiem ir izvirzītas apsūdzības saistībā ar šo uzbrukumu

Apdraudētie lietotāji

Apple un Uber bija starp uzņēmumu kontiem, uz kuriem tika vērsti uzbrukumi, bet arī Bils Geitss, Elons Masks, Džefs Bezoss, Vorens Bafets, Kanje Vests un Floids Meivezers.



Avots: BBC ziņas

Pakalpojums Zoom piedzīvoja vairākus drošības incidentus, jo īpaši aptuveni 500 000 lietotāju kontu, kas parādījās pārdošanai tumšā tīmekļa forumā.

Avots: https://www.freepik.com/

Kā notika īstenošana?

Tiek ziņots, ka konti tika iegūti, izmantojot lietotāju ID un paroles, kas tika atklātas iepriekšējos pārkāpumos, ko sauc arī par akreditācijas datu iepildīšanu.

Hakeri pēc tam varēja piekļūt svarīgai personiskai vai korporatīvai informācijai, kura bija obligāti jāuzglabā drošībā. Turklāt Zoom kodus bija viegli uzminēt, tāpēc lietotāji varēja pievienoties sapulcēm bez uzaicinājuma, un pārtraukt vai kopīgot nepiemērotus materiālus, ko sauc arī par Zoom bombardēšanu.

Grieķijas bankas

Pēc tam, tika uzlauzta kāda Grieķijas tūrisma un ceļojumu vietne, Grieķijas četras galvenās bankas sekoja drošības protokoliem un tām bija jāatceļ un jāaizvieto aptuveni 15 000 klientu kredītkaršu vai debetkaršu.

Avots: https://www.freepik.com/

Kā notika īstenošana?

- Konkrētas atbildes nav.
- Būtisks izziņas avots ir tas, vai tūrisma vietne atbilda maksājumu karšu nozares datu drošības standartiem (PCI DSS) vai nē.
- Šī nav pirmā reize, kad uzbrukums tiek vērsts pret Grieķijas bankām – iepriekš tās bija piedzīvojušas DDoS un izspiedējvīrusu uzbrukumus, izraisot traucējumus banku darbībā, piemēram, tiešsaistes banku darbībā.

Funded by the Erasmus+ Programme of the European Union

Uzbrukums slimnīcai Čehijas Republikā

Brno universitātes slimnīcu Brno pilsētā Čehijā skāris kiberuzbrukums tieši COVID-19 uzliesmojuma vidū.

Avots: https://www.freepik.com/

Slimnīcai bija nepieciešams:

- *atlikt steidzamas operācijas un jaunus akūtus pacientus pārsūtīt uz tuvējo Svētās Annas universitātes slimnīcu;*
- *incidenta laikā slēgt visu savu IT tīklu.*

Kopsavilkums

- 2019. gadā palielinājās draudu iespēju sarežģītība, daudziem kibernoziedzniekiem izmantojot ļaundabīgas ekspluatācijas, akreditācijas datu zādzības un daudzpakāpju uzbrukumus.
- Datu pārkāpumu gadījumu skaits joprojām ir ļoti augsts, un nozagtās finanšu informācijas un lietotāju akreditācijas datu apjoms pieaug.
- ENISA prognozē, ka nākamajā desmitgadē kiberdrošības riskus un draudus būs arvien grūtāk atklāt un novērtēt, jo draudu reljefs kļūst arvien sarežģītāks, bet arī uzbrukuma placdarba paplašināšanās dēļ.

Uzdevumi

Apskatiet sniegto gadījumu izpēti.

- *Apspriediet, kādas varētu būt sekas gan uzņēmumiem, kuriem uzbrukts, gan lietotājiem.*
- *Pārrunājiet, kādas kiberdrošības incidentu tendences mēs redzam 2021. gadā. Ko mēs varam sagaidīt nākamajos gados?*
- *Pārrunājiet prasmju pilnveides nozīmi, ņemot vērā iespējamos kiberuzbrukumu radītos riskus*

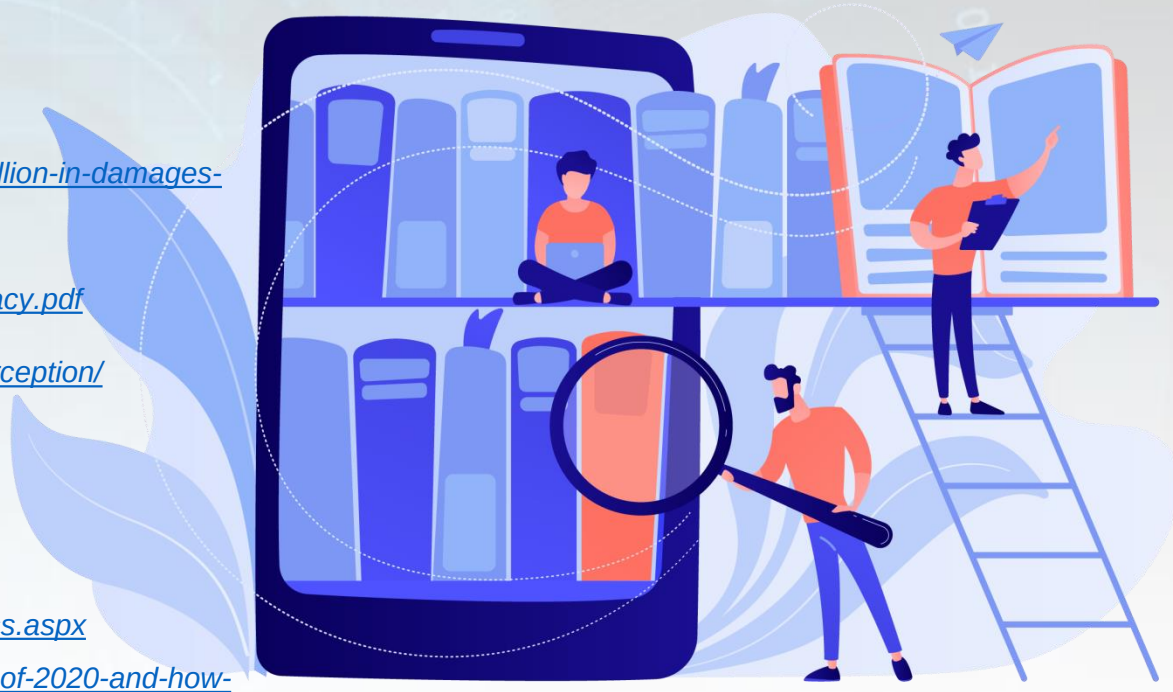
Funded by the Erasmus+ Programme of the European Union

Papildu lasīšana

Pārskats par kiberdrošības reljefa tendencēm

Šīs lekcijas sagatavošanā izmantotie materiāli

- 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

Īsi video

- Martins Kasado "Jaunumi kiberuzbrukumos"

  https://youtu.be/AQP0On85ZdQ

- 5 visbīstamākie jaunie uzbrukuma paņēmieni un kā tiem pretoties

  https://youtu.be/xz7IFVJf3Lk

- Desmit kiberdrošības tendences

  https://youtu.be/kkP9URO8XJ8

Pateicamies!