Funded by the Erasmus+ Programme of the European Union

Küberturvalisus Euroopa Liidus (EL / EU)

Ülevaade küberturvalisuse maastiku tendentsidest

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

Omandada lisateavet hiljutiste küberturvalisuse suundumuste, esilekerkivate ohtude ja tegelikkuse ning peamiste küberturbeintsidentide kohta.

Õpilase töökoormus

Loengud	1,5 h
Audio- ja videomaterjal	1 h
Juhtumiuuringud	1,5 h
Lisalugemine	2 h
Eksamiks valmistumine	2 h

Funded by the Erasmus+ Programme of the European Union

2019-2021

küberjulgeolekuohtude tendentsid

ENISA hinnangul on kaks peamist fakti oluliselt kaasa aidanud olulistele muutustele EL-i küberohtude maastikul

1. *COVID-19 pandeemia põhjustatud ainulaadsed järsud muutused*
2. *Ohutegurite kasv ja vastase võimekuse pidev suurenemine*

Funded by the Erasmus+ Programme of the European Union

2019-2021

Küberturvalisuse ohu tendentsid

1. Küberturvalisuse ründepind laieneb jätkuvalt

2. Rünnakud on pärast COVID-19 pandeemiat uus sotsiaalne ja majanduslik normaalsus

3. Tõsine trend – sotsiaalmeedia platvormide kasutamine suunatud rünnakutes

4. Täpselt sihitud ja püsivad rünnakud kõrge väärtusega andmete vastu

5. Massiivselt hajutatud lühikese kestusega ja laia mõjuga rünnakud

Funded by the Erasmus+ Programme of the European Union

2019-2021

Küberturvalisuse ohu tendentsid

6. Enamiku küberrünnakute taga on rahaline motivatsioon

7. Lunavara on endiselt laialt levinud ja kulukas

8. Paljud küberjulge-olekuintsidendid jäävad märkamatuks või nende avasta-miseks kulub aega.

9. Organisatsioonid investeerivad rohkem valmisolekusse end kaitsta

10. Andmepüügi-ohvrite arv kasvab jätkuvalt

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Peamised ohud 2018		Suundumus
1	Malware - Pahavara	-----
2	Web-based attacks - Veebipõhised	↗
3	Web application attacks - Veebirakenduste	-----
4	Phishing - Andmepüük	↗
5	Denial of service - teenusetõkestus	↗
6	Spam - Spämm	-----
7	Botnets - Botivõrgud	↗
8	Data Breaches - Andmete rikkumised	↗
9	Insider threat - Siseringi oht	↙
10	Physical manipulation, damage, theft – füüsiline rünne	----- ↗
11	Information leakage - Andmeleke	↗
12	Identity theft – Identiteedi vargus	↗
13	Cryptojacking - kaevekaaperdus	↙
14	Ransomware - Lunavara	↙
15	Cyber espionage	

Peamised ohud 2019-2020		Suundumus	Muutus pingereas
1	Malware - Pahavara	-----	-----
2	Web-based attacks - Veebipõhised	-----	↗
3	Phishing - Andmepüük	↗	↗
4	Web application attacks - Veebirakenduste	-----	↙
5	Spam - Spämm	↙	↗
6	Denial of service - teenusetõkestus	↙	↙
7	Identity theft – Identiteedi vargus	↗	↗
8	Data Breaches - Andmete rikkumised	-----	-----
9	Insider threat - Siseringi oht	↗	-----
10	Botnets - Botivõrgud	↙	↙
11	Physical manipulation, damage, theft – füüsiline rünne	----- ↗	↙ ↙
12	Information leakage - Andmeleke	↗	↗
13	Ransomware - Lunavara	↙	↗
14	Cyber espionage - Küberspionaaž	↙	↙
15	Cryptojacking - kaevekaaperdus		

Legend: **Trend:** ↙ Langev ----- Stabiilne ↗ Tõusev **Pingerida:** ↗ Üles ----- Sama ↙ Alla

Source: ENISA "Threat Landscape 2019 -2020" report

Viis esilekerkivat suundumust küberohtudest

1. **Pahavara uuendatakse pidevalt**

   Pahavara perekonna tüvesid täiendatakse uuteks versioonideks, millel on lisafunktsioonid, levitamis- ja levimehhanismid, nt. , Emotet

2. **Ohud muutuvad täielikult mobiilseks**

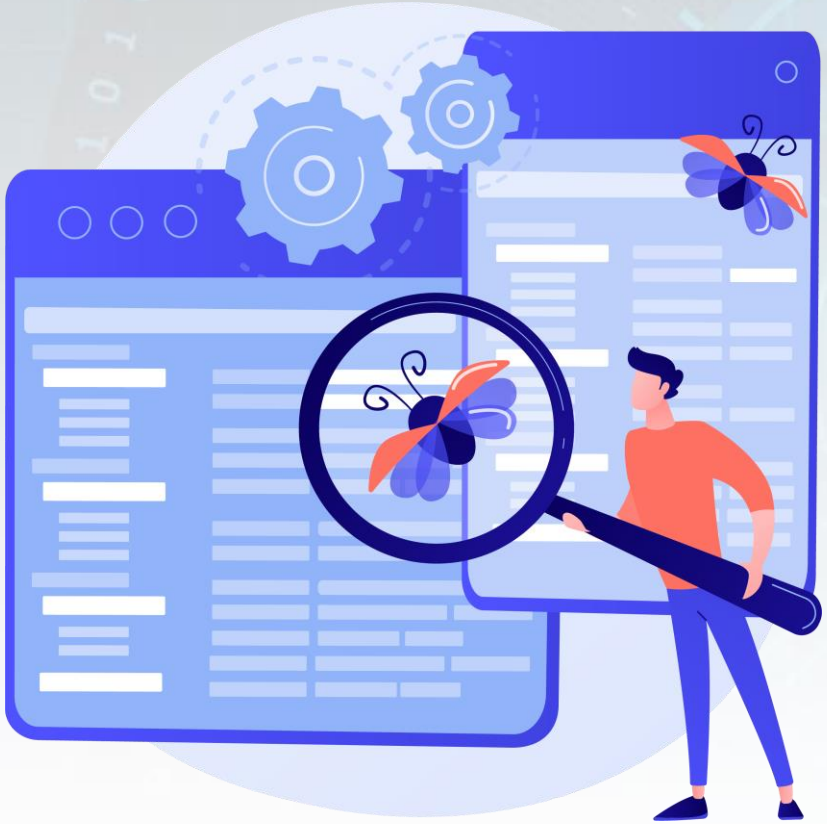
   Kasutajad sõltuvad oma kõige tundlikumate kontode kaitsmisel üha enam mobiilseadmetest

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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Viis esilekerkivat suundumust küberohtudest



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

3. **Uute failitüüpide kasutamine**

   Näiteks plaadi pildifailid (ISO ja IMG) pahavara levitamiseks

   Endiselt kasutatakse kõige sagedamini DOC-, PDF-, ZIP- ja XLS-faile

4. **Koordineeritud ja sihitud lunavararünnakute arv**

   2019. aastal oli tegemist keerukate ja sihipäraste lunavara kuritarvituste, nt tervishoiu ja avaliku sektoriga.

Funded by the Erasmus+ Programme of the European Union

Viis esilekerkivat suundumust küberohtudest

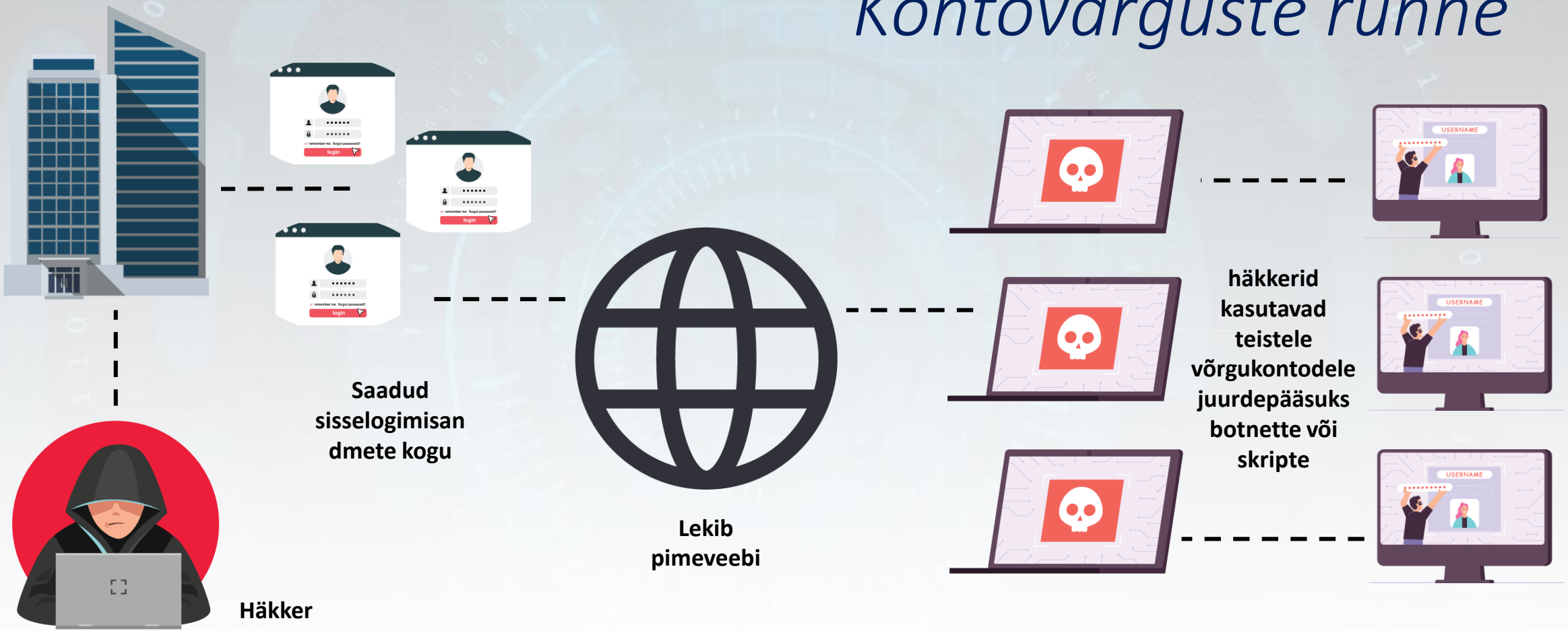
5. Laialt levinud kontovarguste rünnakud

Need rünnakud vohavad kümne aasta jooksul ebatavaliselt suure hulga andmetega seotud rikkumiste ja triljonite isikuandmete varastamise tõttu.

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

Funded by the Erasmus+ Programme of the European Union

Credential Stuffing Attack
Kontovarguste rünne



Adapted from Comparitech

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kümme tärkavat suundumust rünnakuvektorites

1. Rünnakud levivad massiliselt lühikese kestusega ja laiema mõjuga

2. Täpselt sihitud ja püsivad rünnakud kavandatakse täpselt määratletud ja pikaajaliste eesmärkidega

3. Pahatahtlikud osalejad kasutavad sihitud rünnakutes digitaalseid platvorme

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

Kümme tärkavat suundumust rünnakuvektorites

4. Äriprotsesside ärakasutamine suureneb
5. Rünnakupind jätkab laienemist
6. Kaugtööd kasutatakse ära koduseadmete kaudu
7. Ründajad on paremini valmistunud

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

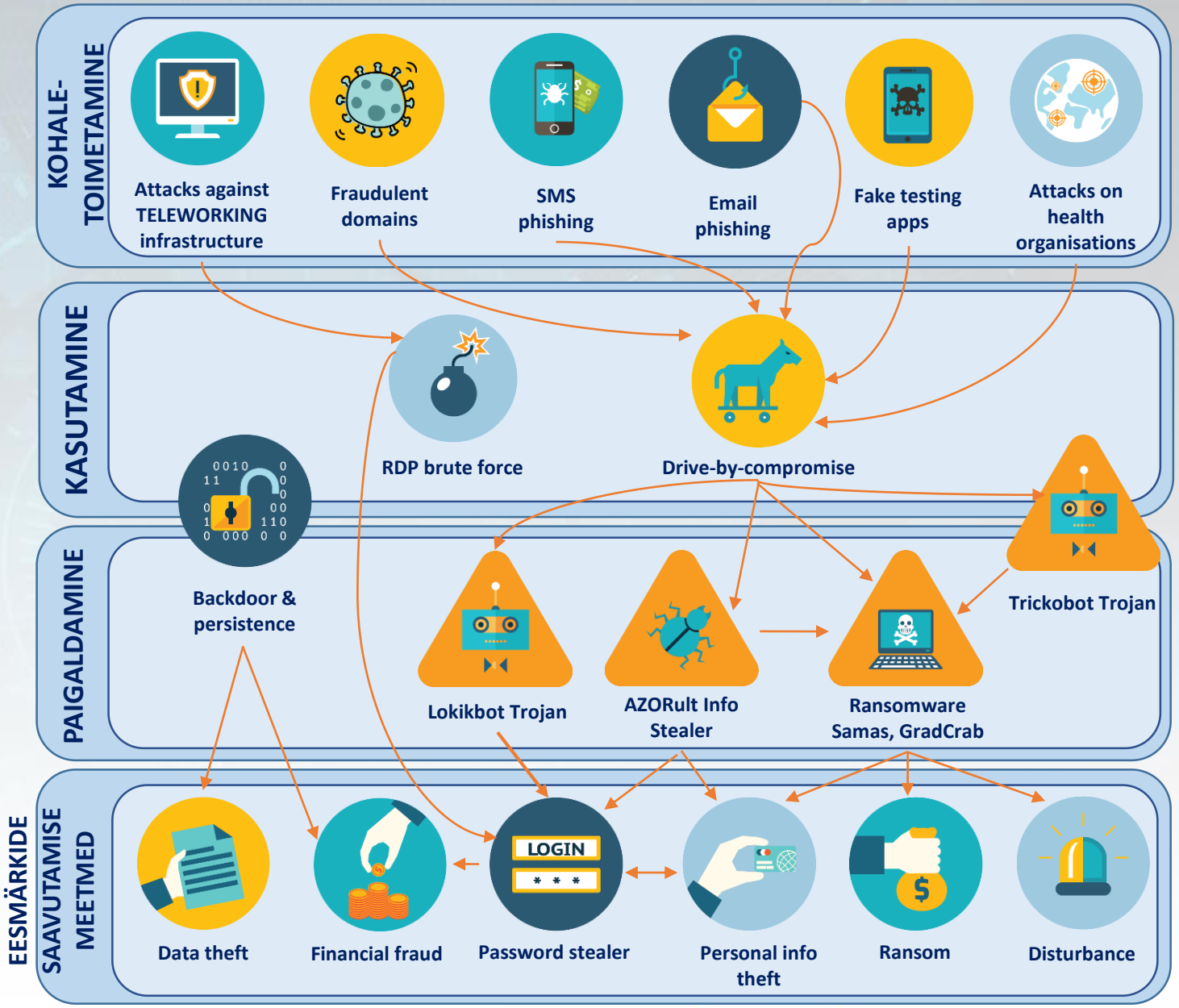
Kümme tärkavat suundumust rünnakuvektorites

8. Hägustamise tehnikad muutuvad keerukamaks
9. Suureneb katkenud rakenduste ja parandamata süsteemide automatiseeritud kasutamine
10. Küberohud liiguvad üksikseadmetele lähemale

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

Funded by the Erasmus+ Programme of the European Union

COVID-19 ohumaastik ENISA poolt



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

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Küberjulgeoleku tegelikkus: kodanikud

70% ELi Interneti-kasutajate arvutitest on kogenud vähemalt ühte pahavara-klassi rünnakut

549 301 unikaalset kasutajat EL-is rünnati lunavaraga

Kaevurid ründasid ELis 1 523 148 unikaalset kasutajat

Üle maailma on loodud 6,95 miljonit uut andmepüügi- ja kelmuste lehte, kusjuures ühe kuu suurim uute andmepüügi- ja kelmuste saitide arv on 206 310 (kasv 2019. aastaga võrreldes 73%).

Funded by the Erasmus+ Programme of the European Union

Küberturvalisuse tegelikkus: äri

87% organisatsioonidest on kogenud juba tuntud, olemasoleva haavatavuse ärakasutamise katset

46% organisatsioonidest on lasknud vähemalt ühel töötajal alla laadida pahatahtliku mobiilirakenduse, mis ohustab nende võrke ja andmeid

Hinnanguliselt on lunavara läinud ettevõtetele 2020. aastal maailmas maksma 20 miljardit dollarit, võrreldes 11,5 miljardi dollariga 2019. aastal.

Uuringud näitavad, et 2020. aasta kolmandas kvartalis hõlmasid peaaegu pooled kõigist lunavarajuhtumitest varastatud andmete avaldamise ohtu ja keskmine lunaraha maksis 233 817 dollarit, mis on 30% rohkem kui 2020. aasta II kvartalis.

Küberkuritegevus läheb ettevõtetele kogu maailmas maksma hinnanguliselt 10,5 triljonit dollarit aastaks 2025. aastal, võrreldes 3 triljoni dollariga 2015. aastal

43% küberrünnakutest on suunatud väikeettevõtete vastu, kuid vaid 14% on valmis end kaitsma.

Küberjulgeoleku tegelik olukord ELis

2019. aastal on EL registreerinud umbes 450 rünnakut kriitiliste infrastruktuuride vastu energia- ja veevarustussektoris ning info- ja sidetehnoloogiate vastu tervishoiu-, transpordi- ja rahandussektoris.

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

Funded by the Erasmus+ Programme of the European Union

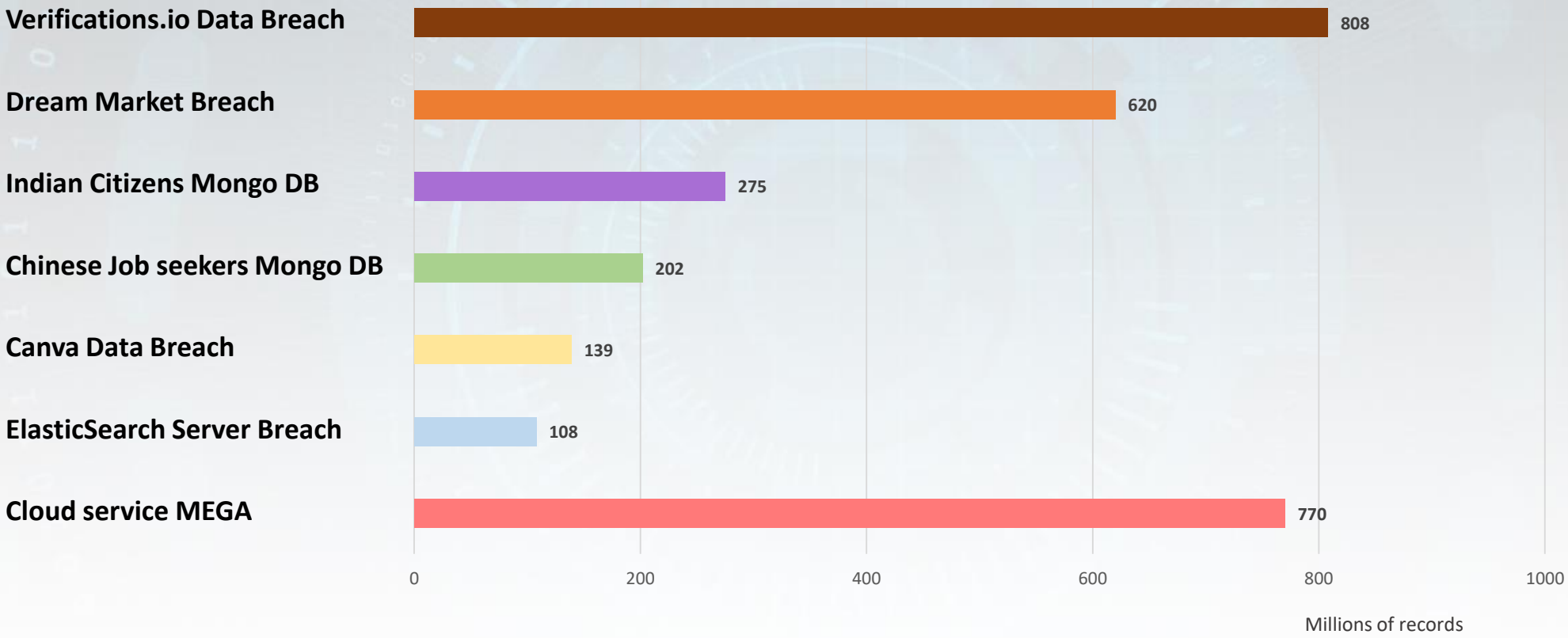
Peamised küberturvalisuse intsidendid aastatel 2019–2021

ENISA Threat Landscape 2020

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Peamised andmete rikkumise juhtumid



Source: ENISA "Threat Landscape 2020"

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Andmete rikkumised: peamised tagajärjed

Teabe kadu: Kui andmetega seotud rikkumine on kaasa toonud delikaatsete isikuandmete kadumise, võivad tagajärjed olla laastavad.

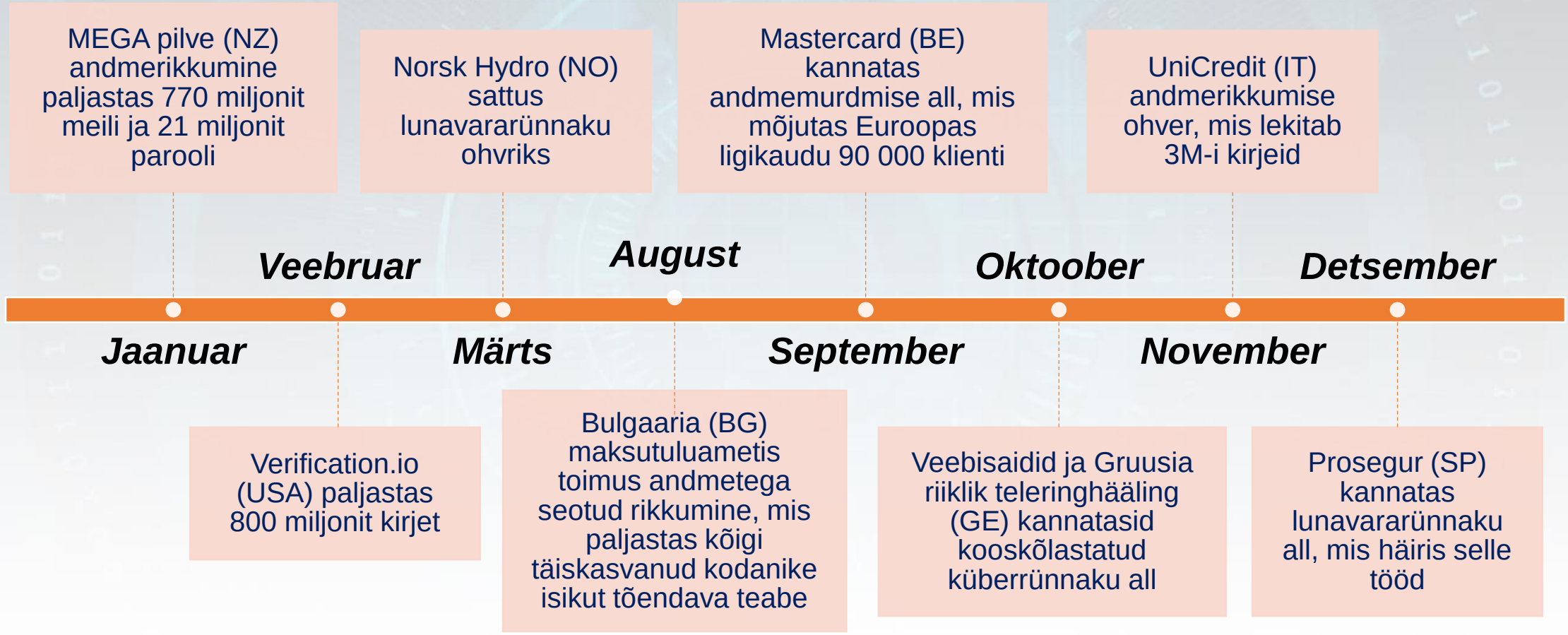
Kohtuasjad ja karistused: Regulatiivsete ja kollektiivsete hagide esilekerkimist ettevõtete vastu, kes ei suuda andmeid kaitsta, ning uusi seadusi, nagu ELi GDPR, saab kasutada karmide karistuste määramiseks.

Lisainvesteeringud: Organisatsioonidel võib tekkida vajadus kulutada raha süsteemide parandamiseks ja arhitektuuride uuendamiseks, samuti investeerida uutesse küberturvateenustesse ja küberkohtuekspertiisi.

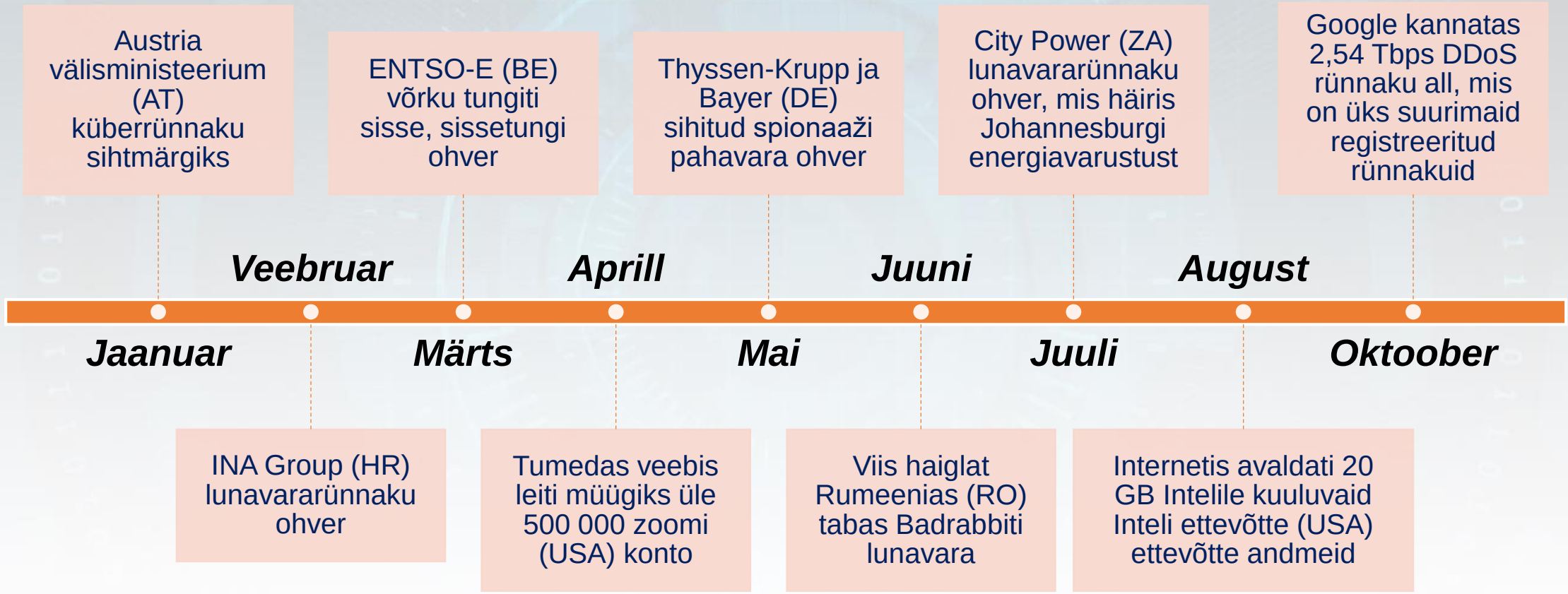
Maine kahjustamine: Forbes Insighti aruanne leidis, et 46% organisatsioonidest on saanud andmetega seotud rikkumise tõttu mainekahju.

Funded by the Erasmus+ Programme of the European Union

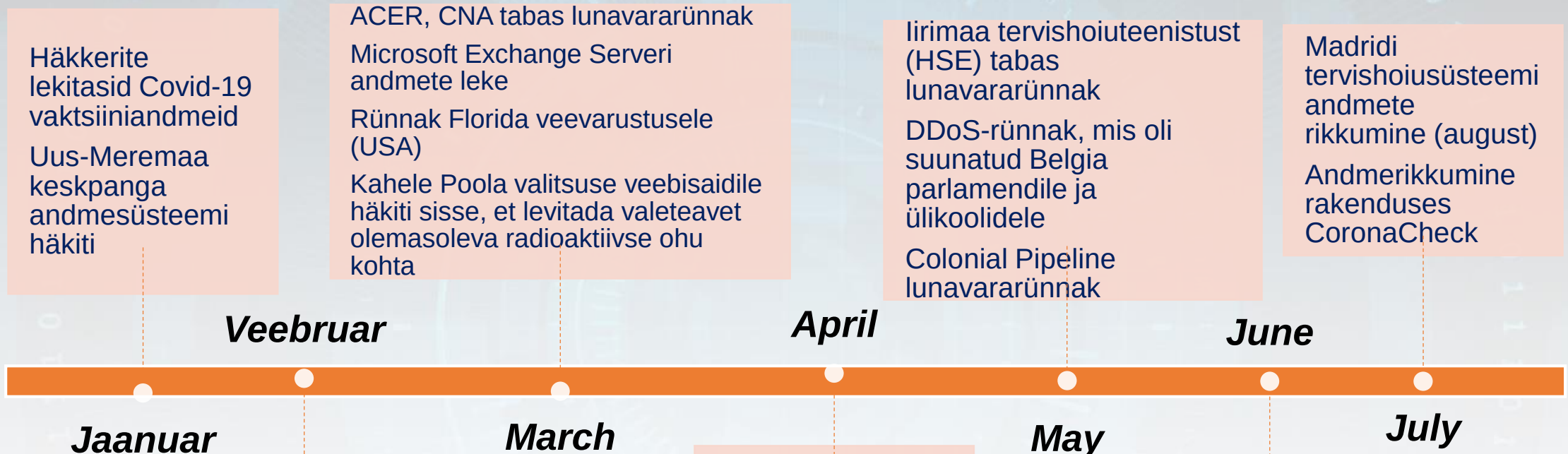
Peamised küberjulgeolekuintsidendid 2019. aastal



Peamised küberjulgeolekuintsidendid 2020. aastal



Küberjulgeolekuintsidendid 2021. aasta alguses



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kuus viisi, kuidas küberkuritegevus äritegevust mõjutab

Suurendab kulusid

Tõrked teenuse pakkumises

Muudab äritavasid

Maine kahjustumine

Kaotatud müük

Varastatud intellektuaal-ne omand

Enim sihitud sektorid 2019–2020

Digiteenused

Valitsused

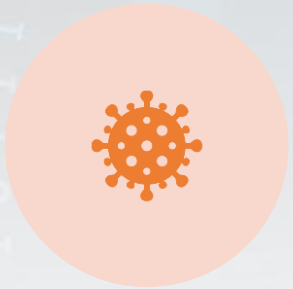
Tehnoloogia

Pangandus

Meditsiin

Funded by the Erasmus+ Programme of the European Union

2020. aasta populaarseimad andmepüügiteemad



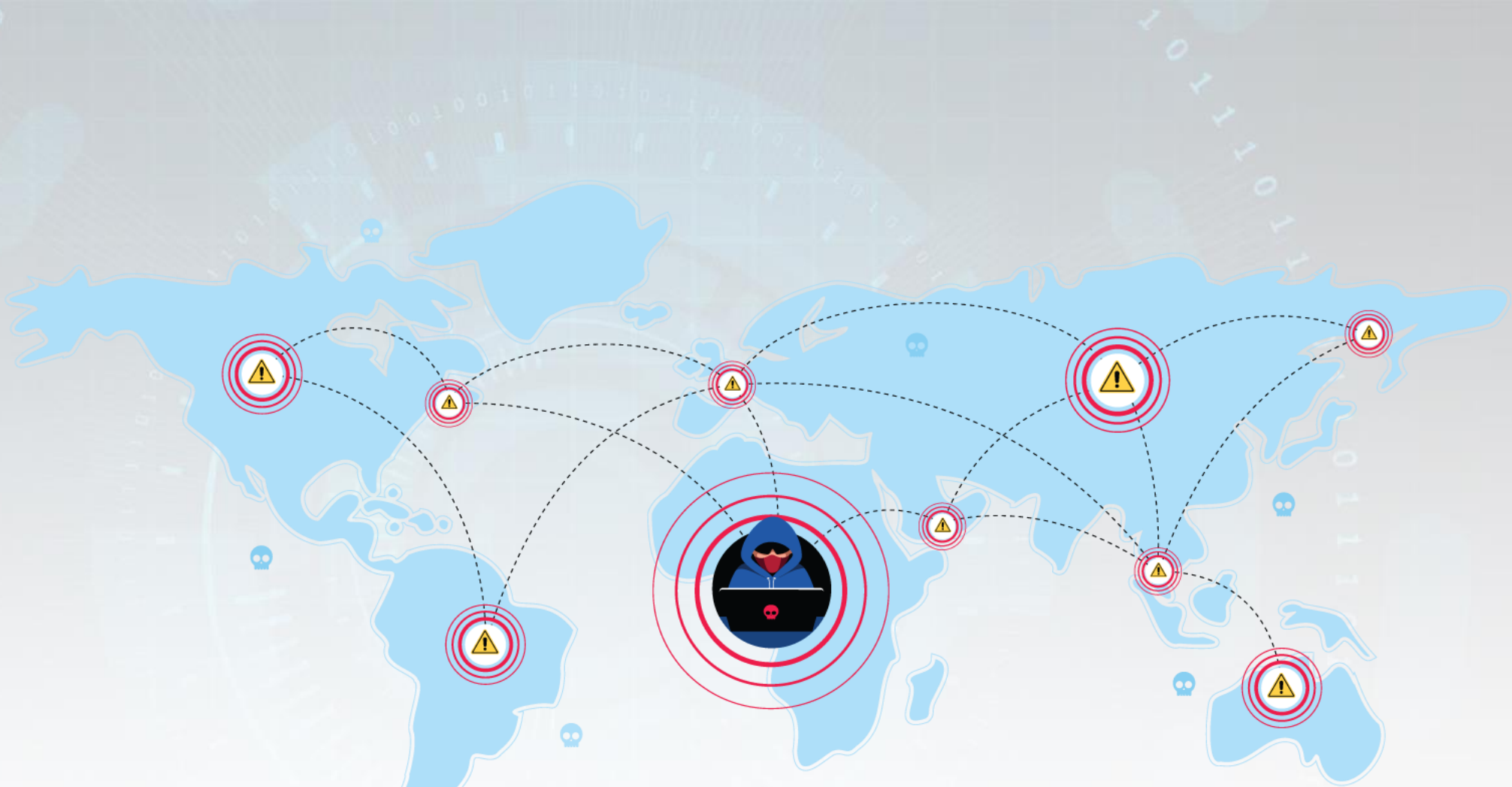
COVID-19

KAUGTÖÖ

INTERNETI KAUBANDUS

JAEMÜÜK

MÄNGUNDUS



Aasta 2020

Juhtumiuuringud

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Twitter

Mõned kõige tunnustatumad ja kõrgelt hinnatud ülemaailmsed Twitteri kontod sattusid ohtu ja neid kasutati Bitcoini kohta petturlikuks säutsuks (info levitamsieks).

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

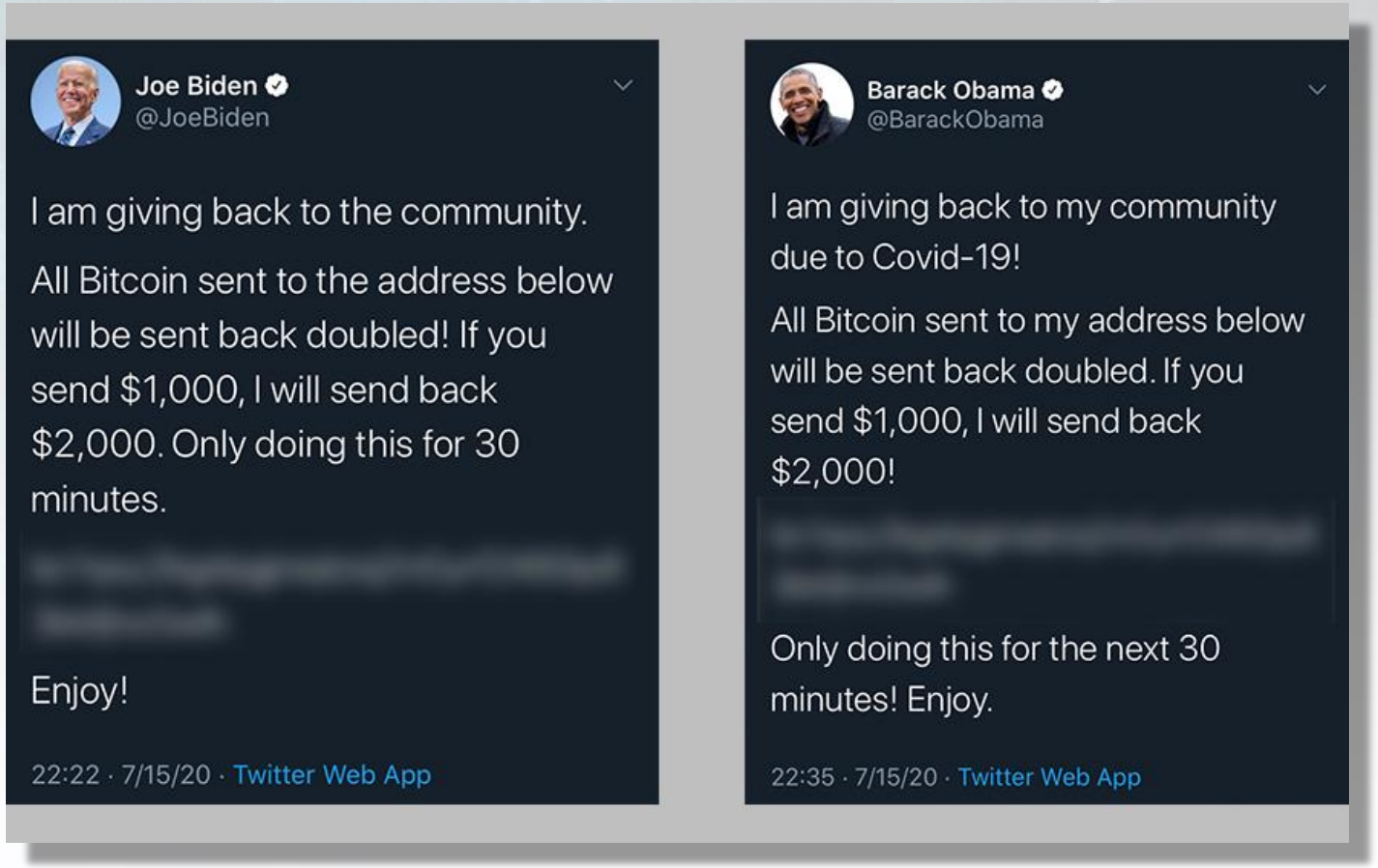
Kuidas seda tehti?

- Kurjategijad kasutasid telefoni teel andmepüügi rünnakut, et saada Twitteri töötajate kontodele ligipääs, kellel oli juurdepääs sisemistele tugitööriistadele.
- Twitter tegi avalduse, milles öeldakseg
  - *"Avastasime meie arvates koordineeritud sotsiaalse manipuleerimise rünnaku inimeste poolt, kes võtsid edukalt sihikule mõned meie töötajad, kellel oli juurdepääs sisemistele süsteemidele ja tööriistadele."*
- Selle rünnakuga seoses on esitatud süüdistus mitmele kahtlusalusele

Funded by the Erasmus+ Programme of the European Union

Sihitud kontode rünnakud

Apple ja Uber olid sihitud ettevõttete kontod, samuti Bill Gates, Elon Musk, Jeff Bezos, Warren Buffett, Kanye West ja Floyd Mayweather



Source: BBC News

Funded by the Erasmus+ Programme of the European Union

Zoom koges mitmeid turvaintsidente, eriti umbes 500 000 kasutajakontot, mis ilmusid müügiks tumeveebis

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

Kuidas seda tehti?

Väidetavalt saadi kontod varasemate rikkumiste käigus paljastatud kasutajatunnuste ja paroolide abil, mida nimetatakse ka *credential stuffing*.

Häkkerid võivad seejärel pääseda ligi olulisele isiklikule või ettevõtte teabele, mida oleks pidanud kaitsma. Lisaks olid zoomi koosolekute koodid kergesti äraarvatavad, nii et kasutajad said koosolekutel ilma kutseta liituda ja sobimatuid materjale katkestada või jagada, mida tuntakse ka kui Zoom bombing.

Funded by the Erasmus+ Programme of the European Union

Kreeka pangad

Pärast Kreeka reisiveebisaidi häkkimist järgisid Kreeka neli peamist panka turvaprotokolle ning pidid tühistama ja asendama ligikaudu 15 000 kliendi krediit- või deebetkaarti.

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

Kuidas seda tehti?

- Kindlat vastust pole
- Peamine uurimise allikas on see, kas turismiveebisait järgis maksekaarditööstuse andmeturbe standardeid (PCI DSS) või mitte.
- See ei ole esimene kord, kui Kreeka pangad on sihikule võetud – varem on nad kogenud DDoS-i ja lunavararünnakuid, mis on põhjustanud häireid pangategevuses, näiteks Interneti-panganduses.

Funded by the Erasmus+ Programme of the European Union

Haigla Tšehhi Vabariigis

- Tšehhis Brno linnas asuvat Brno ülikooli haiglat tabas küberrünnak keset COVID-19 puhangut

Haigla pidi:

- *kiireloomulised kirurgilised sekkumised edasi lükkama ja uued ägedad patsiendid ümber suunama lähedalasuvasse St. Anne ülikooli haiglasse,*
- *sulges intsidendi ajaks kogu oma IT-võrgu.*

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

Kokkuvõte

- Ohuvõimalused arenesid 2019. aastal, kuna paljud küberkurjategijad kasutasid spetsiaalseid tarkvarasid, volikirjade varastamist ja mitmeastmelisi rünnakuid.
- Andmerikkumiste arv on endiselt väga suur ning varastatud finantsteabe ja kasutajaandmete hulk kasvab.
- ENISA ennustab, et eeloleval kümnendil muutub küberjulgeoleku riskide ja ohtude tuvastamine ja hindamine raskemaks, sest ohumaastik muutub keerukamaks ning ründepind laieneb.

Funded by the Erasmus+ Programme of the European Union

Ülesanded

- Heitke pilk pakutavatele juhtumiuuringutele
  - *Arutage, millised võivad olla tagajärjed nii rünnatud ettevõtetele kui ka kasutajatele?*
  - *Arutage, milliseid küberjulgeolekuintsidentide suundumusi me 2022. aastal näeme? Mida peaksime ootama lähiaastatel?*
  - *Arutage oskuste täiendamise tähtsust, pidades silmas küberrünnakutest tulenevaid võimalikke riske*

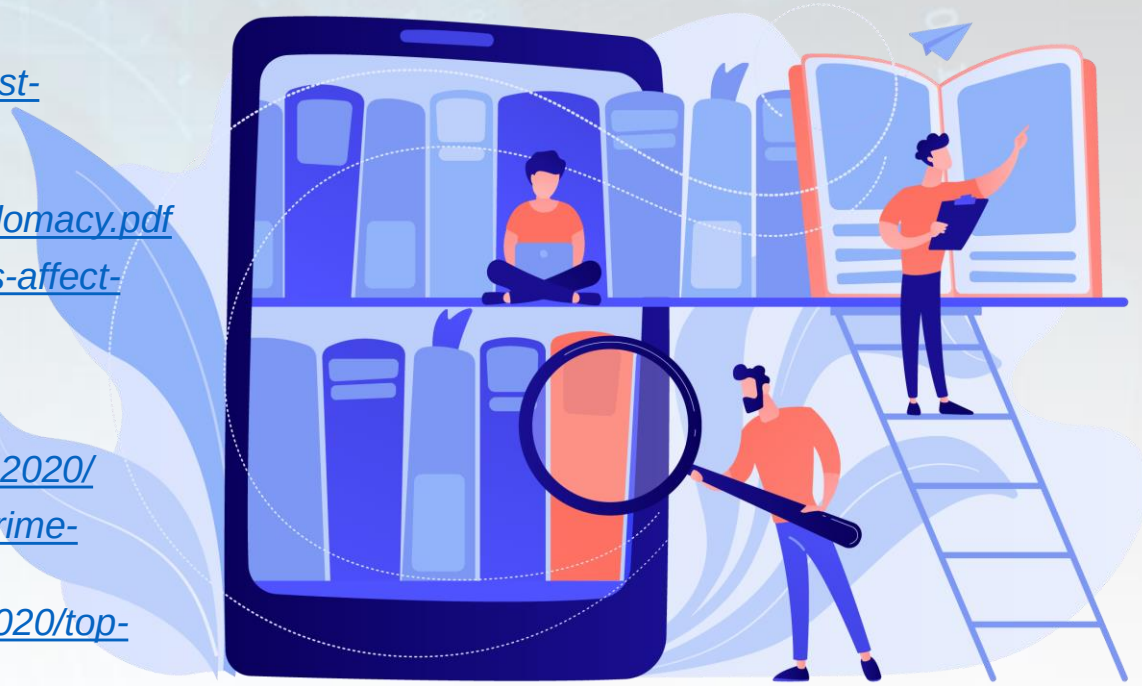
Funded by the Erasmus+ Programme of the European Union

Lisalugemine

Overview on the Tendencies of Cybersecurity Landscape

Material used in preparation of this lecture

- 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/



Lühivideod

- Martin Casado “The Latest in Cyber Attacks”

  https://youtu.be/AQP0On85ZdQ

- The 5 Most Dangerous New Attack Techniques and How to Counter Them

  https://youtu.be/xz7IFVJf3Lk

- Ten Cyber Security Trends

  https://youtu.be/kkP9URO8XJ8

Tänan kuulamast!