Funded by the
Erasmus+ Programme
of the European Union

Ievads kiberdrošībā

Kiberdrošības definīcijas

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

Iepazīties ar pašu kiberdrošības jēdzienu

Kas ir kiberdrošība?

Kas ir kiberuzbrukums?

Kursantu darba slodze

Lekcija	0,5 st.
Papildu lasīšana	4 st.
Sagatavošanās eksāmenam	1 st.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kibertelpas definīcija

- Vispirms mums ir jādefinē, kas ir kibertelpa.
- Populāro definīciju nodrošina Nacionālais standartu un tehnoloģijas institūts (NIST):

Globāls domēns informācijas vidē, ko veido savstarpēji atkarīgs informācijas sistēmu infrastruktūru tīkls, tostarp internets, telekomunikāciju tīkli, datorsistēmas un iegultie procesori un kontrolieri

Avots: https://csrc.nist.gov/glossary/term/cyberspace

Funded by the Erasmus+ Programme of the European Union

Kas ir kiberdrošība?

- Pēdējos gados termins “kiberdrošība” ir kļuvis par plaši lietotu terminu, ko arvien vairāk izmanto prakses speciālisti un sabiedrība.
- Tomēr, tāpat kā daudzām modernām parādībām, precīza kiberdrošības definīcija nav tik skaidra.
- Piem. 2000. gadu sākumā šajā kontekstā regulāri lietotie termini bija “datoru drošība”, “IT drošība” vai “informācijas drošība”.

- Termins kiberdrošība kļuva tik populārs tikai 2010. gados.

Funded by the Erasmus+ Programme of the European Union

Kas ir kiberdrošība?

- Termina kiberdrošība pieaugošā popularitāte bieži tiek saistīta ar ASV prezidentu Baraku Obamu.
- 2009. gadā Baraks Obama paziņoja: *"Es aicinu ASV iedzīvotājus atzīt kiberdrošības nozīmi un ievērot šo mēnesi ar atbilstošām aktivitātēm, pasākumiem un apmācībām, lai uzlabotu mūsu valsts drošību un noturību"* (https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-national-cybersecurity-awareness-month).

- "Kiberdrošība" ir daudz vairāk nekā tikai "datoru drošība"

Funded by the Erasmus+ Programme of the European Union

Kiberdrošības definīcijas

Nozares definīcija:

Kiberdrošība ir drošības prakšu kopums, kas saistīts ar uzbrukuma un aizsardzības darbību kombināciju, kas ietver vai paļaujas uz informācijas tehnoloģiju un/vai darbības tehnoloģiju vidi un sistēmām.

Kiberdrošība ir drošības prakses, piemēram, informācijas drošības, IT drošības un citu saistītu prakšu, superapvienojums.

Avots: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

Funded by the Erasmus+ Programme of the European Union

Kiberdrošības definīcijas

Akadēmiskā definīcija:

Pieeja un darbības, kas saistītas ar drošības riska pārvaldības procesiem, ko ievēro organizācijas un valstis, lai aizsargātu kibertelpā izmantoto datu un līdzekļu konfidencialitāti, veselumu un pieejamību. Koncepcija ietver vadlīnijas, politikas un drošības pasākumu, tehnoloģiju, rīku un apmācību kopas, lai nodrošinātu vislabāko aizsardzību kibertelpā.

Avots: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

Funded by the Erasmus+ Programme of the European Union

Kas ir kiberuzbrukums?

- Kiberdrošība ir cieši saistīta ar kiberdraudiem.
- NIST sniegtā populārā definīcija:

Uzbrukums, izmantojot kibertelpu, kura mērķis ir uzņēmuma kibertelpas izmantošana, lai izjauktu, atspējotu, iznīcinātu vai ļaunprātīgi kontrolētu skaitļošanas vidi/infrastruktūru.; vai tāds, kas iznīcina datu veselumu (integritāti) vai nozog kontrolēto informāciju

Avots: https://csrc.nist.gov/glossary/term/cyber_attack

Funded by the Erasmus+ Programme of the European Union

Daži kiberuzbrukumu veidi

- **Ļaunprātīga programmatūra** apraksta ļaunprātīgu programmatūru, tostarp spiegprogrammatūru, izspiedējprogrammatūru, vīrusus un tārpus. Tā pārkāpj tīklā esošās robežas, izmantojot noteikta veida ievainojamības. Visbiežāk – lietotājam noklikšķinot uz bīstamas saites vai e-pasta pielikuma ar riskantu programmatūru.
- **Pikšķerēšana** – krāpniecisku paziņojumu nosūtīšana. Mērķis ir simulēt nākšanu no leģitīma, patiesa avota. Parasti sūtīšana notiek pa e-pastu. Mērķis ir nozagt sensitīvus datus, piemēram, pieteikšanās informāciju, vai upura datorā instalēt ļaunprātīgu programmatūru.
- **Starpnieka uzbrukumi (MitM)** jeb noklausīšanās uzbrukumi notiek, kad uzbrucēji iesaistās divu pušu darījumā.

Funded by the Erasmus+ Programme of the European Union

Daži kiberuzbrukumu veidi

- **Pakalpojuma atteikuma uzbrukuma** mērķis ir pārpildīt datoru un tīkla resursus ar nevajadzīgu datu plūsmu (trafiku). Rezultātā sistēma nespēj izpildīt faktiskos leģitīmos pieprasījumus.
- **Strukturētās vaicājumu valodas (SQL) injekcija** notiek, serverī ievietojot ļaunprātīgu kodu, izmantojot SQL. Mērķis ir atklāt informāciju, kas parasti netiktu atklāta.
- **DNS tunelēšana** izmanto DNS protokolu, lai komunicētu ar DNS nesaistītu datu plūsmu.
- **Nulles dienas ļaunprātīga izmantošana** ir ievainojamības izmantošana, kad tā tika atrasta un paziņota, bet joprojām nav izlabota. Uzbrucēji izmanto informāciju par ievainojamību šajā laika periodā.

Funded by the Erasmus+ Programme of the European Union

Daži kiberuzbrukumu veidi

- Dažādu veidu kiberuzbrukumiem var būt nepieciešamas dažādas darbības.

- Dažiem kiberuzbrukumiem var būt nepieciešamas dziļas tehniskās zināšanas.
- Daļa kiberuzbrukumu var izmantot cilvēka psiholoģiju un manipulācijas.

- **Atcerieties:** kibernētiskās vājākais elements ir cilvēks.

Funded by the Erasmus+ Programme of the European Union

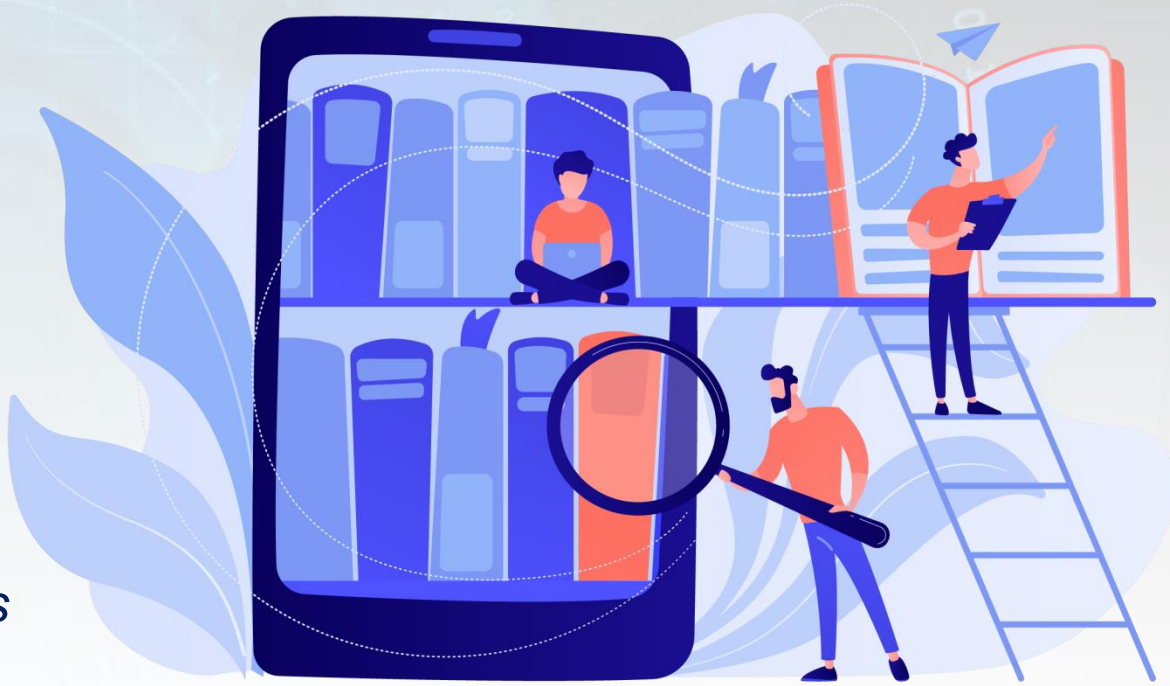
Daži pikšķerēšanas veidi

- ***E-pasta pikšķerēšana:*** populārākais pikšķerēšanas veids. Blēdis izmantos viltotu domēnu, kas līdzinās esošai un uzticamai organizācijai, kas atdarina īstu organizāciju un nosūta daudzus pieprasījumus.
- ***Mērķēta pikšķerēšana:*** ļaunprātīgi e-pasta ziņojumi, kas nosūtīti konkrētai personai, parasti augstvērtīgam mērķim. Uzbrucēji parasti apkopo informāciju par upuri.
- ***Lielo zivju pikšķerēšana*** ir vēl mērķtiecīgāka, vēršoties pret augstākā līmeņa vadītājiem.
- ***SMS pikšķerēšana un tālruņu zvanu un balss pasta pikšķerēšana:*** kā primāro uzbrukuma veidu izmanto tālruņus, nevis e-pastu. SMS pikšķerēšana ietver īsziņas, piemēram, SMS, kamēr tālruņu zvanu un balss pasta pikšķerēšana tiek veikta, izmantojot runātu sarunu.
- ***Sociālo tīklu pikšķerēšana:*** sociālo mediju iespējas tiek izmantotas, lai pārliecinātu cilvēkus atklāt sensitīvu informāciju vai lejupielādēt ļaunprātīgu programmatūru. Var izmantot arī datus, ko cilvēki publicē sociālajos saziņas līdzekļos, lai izveidotu ļoti mērķtiecīgus uzbrukumus.

Funded by the Erasmus+ Programme of the European Union

Papildu lasīšana

- *Daniels Šacs [Daniel Schatz], Rabais Bašrušs [Rabih Bashroush], Džūlija Vola [Julie Wall]. Ceļā uz lielākā mērā reprezentatīvu kiberdrošības definīciju. Digitālās kriminālistikas, drošības un tiesību žurnāls. Numurs 2, sējums 12, 2017. gads*
- *Dans Kreigens [Dan Craigen], Nadja Diakuna Tibolta [Nadia Diakun-Thibault], Rendijs Pērss [Randy Purse]. Kiberdrošības definīcija. Tehnoloģiju inovāciju pārvaldības apskats. Numurs 4, sējums 10, 2014. gads*
- *Kiberdrošības definīcija. Jaunās tehnoloģijas un problēmas definīcijas nenoteiktība: Kiberdrošības gadījums. Regulācija @ Pārvaldība, 2020. gada jūlijs*



Funded by the Erasmus+ Programme of the European Union

Pateicamies!