

Zoom.us ja turvalisus

Viimasel ajal on Zoom.us saanud palju uusi kasutajaid nii EKA-st kui maailmast. Seepärast on selle vastu huvi kasvanud ka häkkeritel, spämmijatel ja lisandunud on küsitava väärtusega info. Seepärast kordaks üle mõned faktid:

- 1) Zoom.us on ajalooliselt edastanud koostööpartneritele oma kasutajate andmeid (nimi, aadress, e-posti aadress, telefoninumber, ettevõtte, amet) - tänu sellele on reaalne oht, et kasutajad võivad saada suunatud reklaame.
- 2) Zoomi vestluse aknasse on teoreetiliselt võimalusi häkkeril edastada mõni link või reklaam. Seeläbi on omakorda võimalik ära kasutada operatsioonisüsteemi turvaauke ja kasutajate usaldust või uudishimu. Hiljuti eksisteeris ka turvaauk, läbi mille oli võimalik varastada Windowsi kasutajalt parooli.
- 3) Paroolita Zoomi koosolekute aadresse on võimalik spämmirobotitel ära arvata ja liitudes vestlusega saata vahele reklaame või koguda andmeid.
- 4) Zoomi pilve salvestatud vestlused ja salvestatud videod võivad olla potentsiaalne oht andmelekkeks.
- 5) Koosolekutele liitudes läbi kohaliku telefoninumbri, on võimalik liituda koosolekuga ilma parooli teadmata (piisab koosoleku ID teadmisest)

Sellest tulenevalt soovitusel:

- 1) Kaitske oma koosolekud parooliga, aga hoidke ka jooksvalt silma peal sellel, kes koosolekul viibivad.
- 2) Ärke klikake tundmatutel linkidel!
- 3) Jälgige, et Teil oleks uuendatud versioon tarkvarast (sh. turvapaigatud op.süsteem). Värske versioon Zoom-ist on allalaetav: <https://zoom.us/download>
- 4) Zoom.us võimaldab vestlusega liituda läbi lauatelefoni 6601699, mis hea võimalus selleks juhuks, kui arvutiga või internetiga probleeme (ei vaja interneti olemasolu), aga samas kui ei vaja seda võimalust, siis delikaatset infot puudutavate koosolekuid ette valmistades lülitage telefoniga liitumise võimalus välja, kuniks turvaauk parandatud (parooli mittekusimine).
- 5) Kuigi muretum võib tunduda, kui kasutajad saavad liituda enne koosoleku korraldaja sisenemist, siis võib teatud juhtudel see tähendada ka probleeme või segadust. (kaaluda võimalust "Join Before Host" kriitiliselt)
- 6) Kui on teada, et Zoomi vahendusel faile pole vaja edastada, kaaluge võimalust "Disable File Transfer", et vähendada võimalust mõnel viirusel sealt kaudu ennast levitada.
- 7) Kui vestluselt eemaldatud kasutajad ei tohiks vestlusele tagasisi siseneda, siis kaaluge võimalust "Disable Allow Removed Participants to Rejoin"

Lisainfo ja allikad:

<https://protonmail.com/blog/zoom-privacy-issues/>

<https://kool.digiabi.ee/digitund/zoomida-voi-mitte-zoomida-see-on-kusimus/>

<https://blogs.harvard.edu/doc/2020/03/27/zoom/>

<https://mashable.com/article/zoom-vulnerability-windows-passwords/?europa=true> (korras)

<https://forte.delfi.ee/news/tarkvara/menukas-videokonverentsi-rakenduses-zoom-on-paroole-lekitav-turvaauk?id=89434851>

<https://www.artun.ee/eriolukord/distantsope/>

Alternatiivid:

Google Meet <https://meet.google.com/> - EKA kasutajatel tasuta

Google Hangouts <https://hangouts.google.com/> - EKA kasutajatel tasuta

Cisco Webex - EKA'l olemas litsentsid (väljastab it@artun.ee)

MS Teams - EKA kasutajatel võimalus kasutada (küsimuste korral it@artun.ee)

Skype

3.04.2020

Kristjan Eichler

IT Talitus, IT peaspetsialist

Eesti Kunstiakadeemia