Infoturbejuht annab nõu: kuidas avalikus kohas turvaliselt arvutitööd teha?

2 aastat tagasi - 19.10.2023 Autor: AM

Uueks normaalsuseks muutunud hübriidtöö toob endaga kaasa olukordi, kus töötame arvutiga aeg ajalt ka avalikus kohas. Millised ohud avalikus ruumis varitseda võivad ja kuidas seal võimalikult turvaliselt arvutitööd teha, räägib Euroopa küberturvalisuse kuul Riigi IT Keskuse infoturbeosakonna juhataja Andri Rebane.

“Kõige esimene ja elementaarsem asi, millele avalikus kohas arvutiga töötades tähelepanu pöörata, on jälgida teraselt oma ümbrust ja eelkõige seljatagust,” rõhutab infoturbejuht Andri Rebane. Nimelt valitseb avalikus ruumis oht langeda üle õla piilumise ehk shoulder surfingu ohvriks, kuna on palju erinevaid nurki, mille alt keegi võib meie ekraani piiluda. Seda riski aitavad maandada spetsiaalsed ekraanile paigaldatavad privaatsusfiltrid, mis oluliselt piiravad ekraani nähtavust külje pealt vaadates. “Otse selja tagant vaadates on aga ikkagi terve ekraan nähtav, nii et avalikus kohas tasub enne tööülesandega alustamist alati mõelda, millise infoga me parasjagu töötame ja kas on üleüldse mõistlik teha seda just avalikus ruumis,“ selgitab ta.

Lisaks on avalikus kohas töötades oma andmete kaitsmiseks väga oluline mitte jätta sülearvutit järelvalveta. “Kui soovime näiteks kohvikus töötades kasvõi hetkeks arvuti tagant kaugemale liikuda, et minna näiteks kohvi tooma, siis tuleb oma arvuti tingimata lukustada,“ tuletab Rebane meelde. Arvuti lukustamine ja sisselogimisel parooli või mitmikautentimise kasutamine on küberturvalisuse jaoks hea mõte igal juhul, mitte ainult avalikus ruumis. Avalikus ruumis arvuti juurest lahkumisel ainuüksi selle lukustamisest ei piisa - tuleb veenduda, et kõrvalistel isikutel pole võimalust arvutit endaga kaasa võtta.

Avalikule wifi võrgule tasub eelistada mobiilset kuumkohta

Kui võimalik, soovitab Rebane avaliku wifi-võrgu kasutamist üldse vältida ja eelistada mobiilset kuumkohta. “Kui me lahkume kodust, siis lukustame alati kõik uksed. Piltlikult öeldes tähendab avaliku wifi kasutamine seda, et oleme tagaukse lukust lahti jätnud ja igaühel on võimalus meie andmetele ligi pääseda,” selgitab ta.

Parooliga kaitstud võrgud on küll mõnevõrra turvalisemad kui paroolita võrgud, ent avalik wifi on siiski arvestatav turvarisk. “Kui tööandja on teie arvutisse paigaldanud virtuaalse privaatse võrgu ehk VPN-i, siis tuleks see avalikus kohas tööle asudes kindlasti sisse lülitada, sest VPN ühendust kasutades ei ole kolmandatel osapooltel võimalik teie liiklust jälgida,” juhib infoturbe asjatundja tähelepanu veel ühele turvalisele võimalusele.

Koosolekute pidamisega tasub olla ettevaatlik

Veebikoosolekud on tänapäeval enamuse jaoks igapäevase töö osa ja teinekord tekib vajadus neid pidada ootamatult. Avalikus kohas töötades tuleb igal juhul rohkem tähelepanu pöörata sellele, kellega ja millest me räägime. “Eriti kõrvaklappe kasutades on kerge tekkima niinimetatud mullis olemise tunne, kus me kipume ära unustama, et ei viibi tegelikult privaatses ruumis ja meie infovahetusest saavad osa täiesti võõrad inimesed. Sageli räägime kõrvaklappe kasutades ka ise oluliselt valjemini ja meie juttu on veel kaugemale kuulda,” ütleb Rebane.

Arvuti vajab järjepidevat tähelepanu

Lisaks eeltoodule soovitab infoturbejuht pöörata järjepidevalt tähelepanu sellele, et arvuti oleks töökorras ja hästi hooldatud. “Aeg ajalt tasub ette võtta digikoristus ja kustutada arvutist ebavajalik info nagu sirvimise ajalugu ja küpsisefailid,” toob ta ühe näitena.

Teine küberturvalisuse seisukohast oluline liigutus on aegsasti ära teha rakendustarkvara süsteemivärskendused ja neile järgnev seadme taaskäivitus. “Inimestel on vahel kombeks värskendusi edasi lükata, aga tegelikult on targem nad kohe ära teha, sest tihti on värskenduste üheks eesmärgiks avastatud turvaaukude parandamine,” ütleb ta kokkuvõtteks.

- Tegijad
- Lahendused

- Tarkvara
- Turvalisus

Pilt