Kas tööarvutit ja -telefoni tohiks kasutada isiklike asjade ajamiseks?

5 tundi tagasi - 03.06.2026 Autor: AM

Tööarvutit ja -telefoni kasutatakse enamasti ka tööd mitte puudutavateks tegevusteks. Telia küberturbe insener Tarvo Kunzi sõnul kipub aga just see suurendama riske, mille mõju võib ulatuda kogu ettevõtteni.

„Esimene asi, mida tasub endale meelde tuletada, on see, et tööarvuti ja töötelefon ei ole isiklikud seadmed, vaid töövahendid, mis on sulle usaldatud. Sellega kaasneb ka vastutus, sest kliendid, kolleegid ja koostööpartnerid usaldavad oma isikuandmeid, dokumente ja muud konfidentsiaalset infot ning iga töötaja roll on aidata seda usaldust hoida," sõnas Telia küberturbe insener Tarvo Kunz.

Ta rõhutab, et mõõdukas isiklik veebikasutus tööseadmes ei pruugi olla probleem, kuid konkreetsed piirid sõltuvad alati tööandja reeglitest ja töötaja ametist. „Kui sa ei ole kindel, mis reeglid sinu tööseadmes kehtivad, siis tasub enne küsida, mitte hiljem tagajärgedega tegeleda," märkis ta.

Viimaste aastate jooksul on tööseadmetesse jõudnud uue riskikohana tehisintellekti tööriistad, mida kasutatakse ka tööülesannete täitmiseks, kuid sageli mõtlemata sellele, kuhu sisestatud andmed tegelikult jõuavad.

„Tööandmete sisestamine isiklikku või juhuslikku AI teenusesse on turvarisk, sest kasutaja ei tea, kuhu need andmed välja jõuavad või kuidas neid hiljem kasutatakse. Töövahendina tuleks kasutada ainult neid AI lahendusi, mille tööandja on heaks kiitnud," selgitas ta.

Tööseadmete kasutamisel tasub järgida häid turva- ja privaatsustavasid

Küberintsidendid saavad sageli alguse väga lihtsatest olukordadest, näiteks ootamatust e-kirjast, valest lingist või pahatahtlikust manusest. Kunzi sõnul alahinnatakse sageli ka brauserilaienduste ja tasuta tarkvara riske.

Ta toob välja levinumad reeglid, mis tagavad turvalisuse:

- Hoia töö- ja eraelu tööseadmetes lahus ning väldi isiklike failide ja kontode kasutamist, et tööandja ja isiklikud andmed ei seguneks.
- Ära saada töötaile isiklikule meilile ega pilveteenusesse, sest nii võivad tundlikud andmed sattuda valedesse kohtadesse.
- Tööseadet peaks kasutama ainult selle omanik, kuna kõik tegevused on seotud sinu kasutajakonto ja vastutusega.
- Kontrolli ootamatute kirjade puhul alati saatjat, linke ja manuseid ning kahtluse korral küsi abi IT-toelt.
- Ära paigalda tarkvara ega brauserilaiendusi ilma IT loata, sest need võivad kujutada turvariski.
- Väldi põhjendamatute USB-seadmete ühendamist tööarvutiga, kuna need võivad sisaldada pahavara.
- Avalikku WiFit kasuta vaid tööandja juhiste järgi või eelista telefoni hotspot'i, et vältida ebaturvalist ühendust.
- Lukusta arvutiekraan alati, kui seadme juurest lahkud, et kõrvalised inimesed ei pääseks andmetele ligi.
- Ära hoia paroole tööseadme märkmetes, Excelis või ekraanipiltidena. Kasuta tugevaid ja kordumatuid paroole, kaheastmelist autentimist ning turvalist paroolihaldurit, eelistatult tööandja heaks kiidetud lahendust.

„Üldiselt kehtivad arvutitele ja telefonidele samad küberturvalisuse põhimõtted, kuid mobiiltelefonide puhul kiputakse riske sageli alahindama. Äppide paigaldamine on telefonis väga lihtne ja seetõttu ei tajuta seda alati samasuguse riskina nagu arvutisse tarkvara installimist," ütles Kunz. Ta lisas, et enne uue rakenduse paigaldamist töötelefonile tasub alati kontrollida, kas see on tööandja poolt lubatud. Samuti ei tasu töömeilidest, dokumentidest ega koosolekutest teha ekraanipilte ilma otsese vajaduseta, sest nii võib tundlik info tahtmatult lekkida.

Turvariskide maandamine on tema sõnul võimalik näiteks seadmehaldusega. „Ettevõte peab teadma, millised seadmed ja tarkvara tema võrgus kasutusel on, sest ilma selle ülevaateta on keeruline tuvastada intsidente, tagada turvauuendusi või reageerida olukorras, kus mõni seade kaob," selgitas Kunz.

- Lahendused

- Mobiiltelefonid
- Sülearvutid
- Turvalisus

Pilt