Valesti seadistatud Google Workspace või Microsoft 365 ohustab pea iga kümnenda firma turvalisust

1 aasta tagasi - 08.05.2025 Autor: AM

Kuigi Google Workspace ja Microsoft 365 on levinud tööriistad koostööks ja failide jagamiseks, ei saa unustada, et nende turvaline kasutamine algab õigetest seadistustest.

Telia viis oma äriklientide seas läbi kasutusel oleva pilvekeskkondade Microsoft 365 ja Google Workspace'i seadistuste kontrolli. Selgus, et keskmiselt 45% ettevõtete endi tehtud seadistustest vajab parendamist ja 10% praegusest seadistustest kujutavad lausa võimalikku turvaohtu ettevõtte andmetele.

Telia küberturbelahenduste arhitekt toob välja kuus levinumat turvaohtu ja seadistusprobleemi, mida kontoritarkvara puhul kindlasti tähele panna.

"Kuigi Google Workspace ja Microsoft 365 muudavad töö sujuvamaks, tuleks enne kasutuselevõttu kindlasti üle vaadata vaikeseaded, et vältida andmete lekkimise riski," ütles Telia küberturbe lahenduste arhitekt Matis Palm. Tema sõnul saab välja tuua kuus levinumat turvaohtu ja seadistusprobleemi, mida ettevõtted tavaliselt ei teadvusta või pole osanud seadistada, kuid mida on vältida väga lihtne.

1. Google Drive ja OneDrive abil jagatavatele failidele on liialt vaba ligipääs ning jagamine ei ole piiratud

Ta toob näite igapäevaelust: töötaja jagab faili lingiga, mille vaikesätted lubavad juurdepääsu kõigile, kellel on link – ka võõrastele. See võib viia andmelekkeni, rikkuda andmekaitsenõudeid ja ohustada ettevõtte mainet.

"Töötajal puudub sageli ülevaade, kes failidele ligi pääseb ja mida nendega tehakse. Selleks on soovitatav määrata jagatud linkidele aegumistähtaeg, kasutada välisjagamisel kinnitamisprotsesse või eraldi OneDrive/SharePointi saite ning piirata failijagamist ainult ettevõttesisestele kasutajatele," rääkis Palm.

2. Gmaili või Outlooki (Exchange Online) kaitse on puudulik

Teises näites igapäevaelust saab töötaja näiliselt kirja oma juhilt, kus palutakse kiiresti maksta arve. Kuna töötaja ei oska vahet teha, et tegemist ei ole tema ülemuse korrektse töökontoga, siis kiiruse huvides teeb ta ülekande ära.

"Tegemist oli petukirjaga, mille saatja aadress oli oskuslikult võltsitud ning mida töötaja meilisüsteem ei suutnud tuvastada," selgitab Palm. Selliste olukordade ennetamiseks tuleks kasutada rämpsposti ja pettuste vastaseid filtreid – näiteks Microsoft Defender for Office 365 Plan 1 või Business Premium litsentsi.

Lisaks peaks tööandja investeerima töötajate küberteadlikkusse, kasutades selleks interaktiivseid koolitusplatvorme, mis aitavad töötajatel õppida ära tundma kahtlasi e-kirju ja potentsiaalseid petuskeeme. Näiteks tuleks õpetada, et arvelduskonto muutusi käsitlevates meilivestlustes tuleb rakendada nn „nelja silma põhimõtet“ ning võimalusel kinnitada olulised muudatused ka teise kanali, näiteks telefonikõne kaudu.

3. Kõik (ka endised töötajad) on administraatorid

Siin on ka kolmas näide igapäevaelust: ettevõtte IT-osakond läheb kergemat teed pidi ja annab igale platvormi kasutajale maksimaalsed õigused nii pilvekeskkonnas kui tööarvutis. Samal ajal puudub ettevõttel korrektne protsess, mida teha endiste töötajate kasutajatega.

Telia küberturbe lahenduste arhitekt rõhutab nn „väikseimate õiguste“ põhimõtte (*Least Privilege*) järgimise olulisust: igale töötajale tuleks anda vaid need ligipääsuõigused, mis on konkreetselt vajalikud tema tööülesannete täitmiseks.

Kõik õigused peaksid olema seotud dokumenteeritud profiiliga, mille alusel need ajutiselt aktiveeritakse ja pärast töö lõppu eemaldatakse. Administraatori õigused peaksid olema ainult valitud kasutajatel ja neile peab rakenduma mitmikautentimine ning soovitatavalt ka füüsiline autentimisseade (nt YubiKey või TitanKey). Samuti on oluline, et ettevõttel oleks selge protsess endiste töötajate õiguste eemaldamiseks, vältimaks pahatahtlikke tegevusi pärast töösuhte lõppemist.

4. Tööfaile saab salvestada igasse seadmesse

Neljas näide igapäevaelust: töötaja salvestab ärikriitilised dokumendid isiklikku telefoni ja tööarvutisse, mis puhkuse ajal varastatakse. Ettevõttel puudub info salvestatud andmete kohta ning võimalus seadmeid hallata või andmeid kustutada. Selline olukord sai tekkida, kuna ettevõte ei olnud piiranud, millistest seadmetest pääseb ligi Microsoft 365 keskkonnale ega kehtestanud

failisalvestuse reegleid.

"Ligipääs tundlikele andmetele peaks olema lubatud vaid turvalistest, ettevõtte kontrollitavatest seadmetest. Selleks tasub kasutada seadmehaldustarkvara, nagu Microsoft Intune või Miradore Online Premium," soovitab Palm. Samuti soovitab ta kehtestada tehnilised turvanõuded, mis võimaldavad vajadusel kadunud seadmetest andmed kaugkustutada ning piirata USB-mäluseadmete kasutamist tööarvutites.

5. Teamsis ja Google Chatis puuduvad piirangud

Järgmises näites igapäevaelust on ettevõtte Teamsi kanalisse lisatud väline partner saanud ligipääsu kogu meeskonna suhtlusele ja failidele, sh tundlikule infole, mis ei ole temaga seotud. Partner lisati ajutiselt ühe projekti tarbeks, kuid puudusid selged ligipääsupiirangud ja külaliskasutajate ("*guest*") õiguste haldus. Kuna Teams on seotud ka dokumentide ja märkmete jagamise tööriistadega (nt OneDrive, Google Drive), võivad tagajärjed olla ulatuslikud.

"Ettevõtted peaksid lubama välistel partneritel ligipääsu ainult konkreetsetele projektidele ja piirama täpselt, mida nad näevad ja teha saavad. Lisaks on oluline koolitada töötajaid Teamsi õiguste, võimaluste ja turvapiirangute osas, et vältida infoturberiske," soovitab Palm.

6. Turbealarmid ei ole sisse lülitatud ja/või keegi ei jälgi neid

Näide igapäevaelust: pärast ühe teenusepakkuja juures toimunud andmeleket on tumeveebi sattunud ka ettevõtte viie töötaja kontode kasutajanimed ja paroolid. Nendega logitakse ettevõtte keskkonda teiselt poolt maakera, kuid keegi isegi ei märka seda, sest puudub nii alarmteavitus kui ka mitmefaktoriline autentimine.

"Sisselogimiste ja turvahäirete monitooring peab olema alati aktiivne. Samuti tuleks regulaarselt jälgida Microsofti turbeportaali kaudu tekkinud alarme, mis annavad infot selle kohta, kes, kust ja millal on keskkonda sisse loginud," rõhutab Palm, "lisaks on soovitatav rakendada Conditional Access-poliitikat, et saada teavitusi kahtlastest sisselogimistest – näiteks tundmatutest asukohtadest või seadmetest, mis ei ole ettevõtte poolt hallatud."

Palm rõhutab, et Google Workspace’i ja Microsoft 365 kasutamisel ei tohi liiga mugavaks muutuda ning ettevõtte juhtkond või IT-osakond peaks regulaarselt hoidma silma peal sellel, kuidas on jagatud töötajate vahel ligipääsud, kuidas faile jagatakse ning kas on olemas nii inimesed kui ka protsessid, kelle ülesanne on jälgida eri turbeintsidente.

- Uudised

- Tarkvara
- Turvalisus

Pilt