IT juht: läksin isegi petukirja õnge

5 kuud tagasi - 11.06.2026 Autor: AM

Küberkurjategijate veenvamad petukirjad sunnivad ettevõtteid kasutama praktilisi õngitsussimulatsioone, et kasvatada töötajate valmisolekut päris rünnakuteks.

Phishbite'i kaasasutaja ja küberturvalisuse ekspert Urmo Keskel ütles, et pelgalt koolitustest ja slaidiesitlustest ei piisa, sest oskus tekib alles päris olukorda harjutades. Tema sõnul kasutab platvorm simuleeritud õngitsusrünnakuid, mis matkivad tegelikke petukirju ja võimaldavad töötajatel eksimustest õppida ettevõttele kahju tekitamata.

Keskel tõi välja, et Phishbite'i andmetel eksib teenuse kasutamise jooksul vähemalt korra 59% töötajatest isegi pikemaajaliselt koolitatud organisatsioonides. Tema hinnangul ei ole küsimus selles, kas keegi eksib, vaid selles, kas viga tehakse päris petturi või kontrollitud harjutuse käigus.

Regulaarne testimine näitab valmisolekut

Keskel selgitas, et üksikud koolitused ei anna täielikku pilti töötajate tegelikust käitumisest. Tema sõnul aitavad järjepidevad simulatsioonid mõista, millised mustrid inimesi eksitavad, ning suunata koolitusi sinna, kus neist on kõige rohkem kasu.

Phishbite'i keskmiste tulemuste järgi langeb eksimuste määr pärast järjepidevat koolitamist ja testimist märkimisväärselt. Keskel ütles, et muutus ei väljendu ainult statistikas, vaid ka selles, et töötajad hakkavad rohkem jälgima saatja aadresse, kontrollima linke ja küsima üle ka siis, kui kiri tundub usaldusväärne.

Barruses kasvas teadlikkus

Puidutööstusettevõtte Barrus IT juht Vaido Otsar ütles, et ettevõttes olid küberhügieeni koolitused olemas ka enne Phishbite'i kasutuselevõttu, kuid praktiline lähenemine tõi uue taseme. Tema sõnul on teadlikkus märgatavalt kasvanud ning töötajad jälgivad nüüd rohkem.

Otsar lisas, et pärast poolt aastat Phishbite'iga koostööd on töötajate eksimuse protsent jõudnud nulli. Tema sõnul olid alguses tulemused üllatavad, sest kirjad tundusid väga turvalised, kuid kogemus näitas kiiresti, kui lihtne on petta saada.

Ka juhid võivad eksida

Otsar tunnistas, et pettused on muutunud nii kvaliteetseks, et ta on ühel korral ise valele lingile klikkinud. Tema sõnul juhtus see samal päeval, kui päris kiri ja petukiri olid postkastis praktiliselt kõrvuti.

Keskel rõhutas, et küberturvalisusest ei tohiks rääkida süüdlaste otsimise võtmes. Tema sõnul õpib organisatsioon rohkem siis, kui keskendub sellele, miks eksimus juhtus ja kuidas seda tulevikus vältida.

Iga vale klikk võib tuua kahju

Ühest kompromiteeritud kasutajakontost võib piisata, et anda ründajatele ligipääs tundlikele andmetele, ettevõtte süsteemidele või finantsprotsessidele. Barrus peab regulaarseid õngitsusteste seetõttu ennetusmeetmeks, mitte kontrollimiseks.

Otsari sõnul on väärtuslik see, et töötajatele saab regulaarselt ülevaateid jagada ja teadlikkust pidevalt fookuses hoida. Keskel lisas, et küberturvalisust ei saa käsitleda ühekordse tegevusena, sest kurjategijad täiustavad oma meetodeid iga päev.

Taust: Phishbite kasutab simuleeritud õngitsusrünnakuid, et harjutada töötajaid päris pettuste äratundmiseks. Ettevõtte sõnul on tulemused paranenud siis, kui testimine ja koolitamine toimuvad järjepidevalt, mitte üks kord aastas.

Puuduv või ebaselge materjal: artiklitekst ei täpsusta, millal Phishbite tegevust alustas, kus ettevõte tegutseb ega kui paljusid organisatsioone teenus veel kasutab.

- Lahendused
- Turvalisus

Pilt

CYBER
SECURITY