IT juht: läksin isegi petukirja õnge

3 tundi tagasi - 11.06.2026 Autor: AM

Enamik ettevõtteid teab praegusel ajal, et küberhügieen on oluline. Töötajatele tehakse koolitusi, saadetakse juhendeid ja jagatakse soovitusi, kuidas pettusi ära tunda. Ometi näitab reaalsus, et teadmistest üksi ei piisa.

“Küberkurjategijad muutuvad järjest osavamaks ning petukirjad järjest veenvamaks. Seetõttu on üha rohkem ettevõtteid jõudnud arusaamisele, et küberturvalisust ei saa õpetada ainult slaidiesitluste ja loengutega,” räägib küberturvalisuse ekspert ja küberhügeeni koolitamise platvormi Phishbite kaasasutaja Urmo Keskel.

„Rattaga sõitma ei
õpi raamatut lugedes ja ujuma ei õpi loengusaalis. Sama kehtib ka küberhügieeni kohta. Teadmine on vajalik, aga päris oskus tekib alles siis, kui inimene puutub olukorraga ise kokku ja peab tegema otsuse,“ lisab ta.

Miks ühest koolitusest ei piisa?

Paljud organisatsioonid
korraldavad kord aastas küberhügieeni parandamiseks küll koolituse või kaks ning eeldavad seejärel, et töötajad oskavad aasta läbi pettusi vältida.

Praktika näitab aga midagi
muud. „Militaarmaailmas moodustavad õppused ja praktilised harjutused suure osa
väljaõppest. Keegi ei eelda, et sõdur õpib kriitilises olukorras tegutsema ainult käsiraamatut lugedes. Ka küberturvalisuses on oluline harjutada päris olukordi turvalises keskkonnas,“ selgitab Keskel.

Just selleks kasutab
Phishbite simuleeritud õngitsusrünnakuid, mis matkivad päriselus levivaid petukirju. Töötajad saavad kogeda, kui veenvad tänapäevased pettused tegelikult on, ning õppida eksimustest olukorras, kus ettevõttele kahju ei sünni.

Phishbite'i andmed
näitavad, et isegi pikemaajaliselt koolitatud organisatsioonides eksib teenuse

kasutamise jooksul vähemalt korra 59% töötajatest. See number võib esmapilgul tunduda kõrge, kuid tegelikult näitab see midagi olulist: eksimine on inimlik ja puudutab peaaegu kõiki.

„Küsimus ei ole selles, kas keegi eksib. Küsimus on selles, kas inimene teeb selle vea päris petturi või kontrollitud harjutuse käigus," ütleb Keskel.

Läbipaistvus aitab riske juhtida

Lisaks teadlikkuse kasvatamisele annab regulaarne testimine ettevõtetele võimaluse mõõta oma tegelikku valmisolekut. Tihti eeldatakse, et töötajad oskavad petukirju hästi ära tunda, kuid alles pikemaajaline harjutamine ja erinevate stsenaariumite läbimängimine näitab, millised mustrid inimesi eksitavad. Üksik simulatsioon ei anna täielikku pilti, kuid järjepidev testimine aitab mõista riske, jälgida arengut ning suunata koolitusi sinna, kus neist on kõige rohkem kasu.

Phishbite'i keskmiste tulemuste järgi langeb eksimuste määr pärast järjepidevat koolitamist ja testimist märkimisväärselt. Kõige olulisem muutus ei ole aga ainult statistikas, vaid töötajate käitumises.

Inimesed hakkavad rohkem tähele panema saatja aadresse, kontrollima linke ja küsima üle ka siis, kui kiri tundub esmapilgul usaldusväärne.

Barrus: teadlikkus on märgatavalt kasvanud

Puidutööstusettevõtte Barrus IT juht Vaido Otsar ütleb, et ettevõttes olid küberhügieeni koolitused olemas ka enne Phishbite'i kasutuselevõttu, kuid praktiline lähenemine tõi täiesti uue taseme.

„Meil olid enne küberhügieeni koolitused olemas, aga seda ei ole kunagi küllalt. Tänaseks on sellest teenusest palju abi. Inimesed jälgivad rohkem ja teadlikkus on ilmselgelt kasvanud," räägib Otsar ning sõnab, et pärast poolt aastat Phishbite'iga koostööd on täna tema töötajate eksimuse protsent jõudnud 0-ni.

“Ma ütlen alati, et ainus aktsepteeritav number sellel teemal on 0,” ütleb ta.

Tema sõnul olid esimesed tulemused isegi mõnevõrra üllatavad. „Alguses eksisime päris palju, sest kirjad tundusid hästi turvalised. Inimesed said kiiresti aru, kui lihtne on tegelikult petta saada ja tähelepanu läks palju paremaks.“

See näitab hästi, kui palju mõjutab inimese otsuseid harjumus ja usaldus. Kui kiri näeb välja tuttav, tehakse otsuseid sageli automaatselt.

Ka juhid eksivad

Üks levinumaid müüte küberturvalisuses on see, et teadlik inimene pettuse ohvriks ei lange. Otsari kogemus näitab vastupidist.

„Pettused on muutunud nii kvaliteetseks, et ükskord klikisin isegi ise. Samal päeval oli päris kiri ja petukiri praktiliselt kõrvuti postkastis. See näitab hästi, et keegi ei ole tegelikult kaitstud.“

Just seetõttu peab Keskel oluliseks, et küberturvalisusest ei räägitaks süüdlaste otsimise võtmes. „Kui eesmärk on leida inimene, kes eksis, siis ei õpi organisatsioon midagi. Kui eesmärk on õppida, miks eksimus juhtus ja kuidas seda tulevikus vältida, siis muutub kogu ettevõte tugevamaks.“

Iga vale klikk võib tähendada suurt kahju

Ühest kompromiteeritud kasutajakontost võib piisata, et anda ründajatele ligipääs tundlikele andmetele, ettevõtte süsteemidele või finantsprotsessidele. Seetõttu ei näe Barrus regulaarseid õngitsusteste mitte kontrollimehhanismi, vaid ennetusmeetmena. „Teenuse juures on väärtuslik see, et saame töötajatele regulaarselt ülevaateid jagada ja teadlikkust pidevalt fookuses hoida. Sellised simulatsioonid on vajalikud kogu aeg ja iga kuu, sest ühe pettuse ära tundmisest ei piisa,” lisab Otsar.

Keskeli sõnul on suurim
viga käsitleda küberturvalisust ühekordse tegevusena „Küberkurjategijad täiustavad oma meetodeid iga päev. Kui meie koolitame inimesi kord aastas, siis ei ole see võrdne võitlus. Teadlikkus vajab regulaarset värskendamist, praktilist kogemust ning harjumuse loomist," räägib Keskel.

Nii nagu hea füüsiline vorm
ei sünni ühest trennist, ei teki ka küberhügieen ühest koolitusest. Tulemus sünnib järjepidevusest, harjutamisest ja valmisolekust õppida ja just seal peitubki organisatsioonide suurim võimalus vähendada riske enne, kui päris pettur
uksele koputab.

- Lahendused
- Turvalisus

Pilt