Küberrünnaku simulatsioon

Enne kui ka vahetult pärast küberturvalisuse koolitust soovitame ettevõttel läbi teha küberrünnaku simulatsioon. Sel moel on tulemused veelgi paremini märgatavad. Ründesimulatsioon võimaldab käivitada realistlikke rünnaku-stsenaariume, mis aitavad tuvastada ja leida haavatavaid kasutajaid enne, kui tõeline rünnak mõjutab kogu organisatsiooni.

Simulatsioon testib turvameetmeid mitmesuguste kasutajale suunatud tehnikate abil, sealhulgas:

- **Identimisteabe hankimine:** ründaja saadab sõnumi URL-iga, mis suunab kasutajad veebisaidile (sageli tuntud kaubamärk). Eesmärk on tundliku teabe varastamine.
- **Pahavara manus:** ründaja saadab adressaadile sõnumi manusega, mis peale avamist käivitab kasutaja seadmes suvalise koodi, et ründaja saaks ettevõtte võrgus veelgi sügavamale kaevuda.
- **Link manuses:** hübriidsõnum, kus ründaja saadab kirja, mille manuses on pahaloomuline URL.
- **Pahavara link:** ründaja saadab sõnumi, mis sisaldab linki kasutajale tuntud failijagamissaidile (nt SharePoint Online või Dropbox).Lingile klikkamine vabastab suvalise koodi, mis võimaldab ründajal ettevõtte võrku imbuda.
- **Drive-by-URL:** ründaja saadab sõnumi URL-iga, mis peale klõpsamist viib veebileheküljele, kust omakorda proovib käivitada taustakoodi, et koguda teavet adressaadi kohta või juurutada tema seadmes suvaline pahatahtlik kood.

Simulatsiooni eelduseks on Microsoft Defender for Office 365 (Plan2) litsentsi olemasolu.

Viimast saab soetada ka ainult simulatsiooni perioodiks, mis kestab 1 kuu.

Simulatsiooni käigus tehakse teie Microsoft 365 keskkonnas vastavad seadistused ning simulatsiooni jooksutatakse 1 kuu vältel, mille järel luuakse tulemusi kokkuvõttev raport.

Investeeringud:

Microsoft Defender for Office 365 (Plan2): 5 € kasutaja kohta 1 kuu
Teenuse seadistus ja tulemuste raport: 600 €