

FORTIX

FORTIX Consulting Kft.

PHISHING szimuláció

Az IBM 2021-es kutatása azt mutatja, hogy az összes információbiztonsági incidens 17%-a phishing támadás következménye, és ezzel az egyik leggyakoribb támadásfajta.

Az adathalászat egy internetes csalási forma, amellyel csálók próbálnak személyes vagy vállalati adatokat, esetleg pénzt szerezni vagy megfertőzni a célpont számítógépes eszközét. A megtévesztő szándék azonban leleplezhető, ha tudjuk, mire kell odafigyelni!



A phishing támadás az embert, a felhasználót célozza.

A kiberbűnözők olyan emberi érzéseinkre és ösztöneinkre alapoznak, mint: a segítségnyújtás, a probléma okozástól való félem, a kapzsiság. A felhasználó lehet az, aki: bedőlhet neki, segítheti, bajba kerülhet, áldozatul eshet...

De a felhasználó lehet az, aki: észlelheti, tehet ellene, jelentheti, megállíthatja!



Mi történik, ha megnyitok egy adathalász e-mailt?

Ha egy linket nyitunk meg belőle, a támadók megszerezhetik jelszavainkat, személyes adatainkat, bankkártya adatainkat stb. Ha az e-mail csatolmányt is tartalmaz, akkor annak megnyitásával nagyon könnyen aktiválhatunk egy vírust, vagy egyéb kártékony kódot, ami akár a teljes céges hálózatot lebéníthatja. Ez ellen pedig sajnos a legújabb antivírus program sem nyújt teljes védelmet.

Az általunk végzett phishing szimuláció célja, hogy valósághű helyzetben felmérje munkavállalóinak biztonságtudatosságát a hétköznapi életben, továbbá, hogy átfogó képet alkossunk a biztonságtudatossági oktatások eredményeiről. Valós, mérhető eredményt ad a felhasználók tudatosságáról.

Az általunk használt phishing eszköz képes a felhasználói tevékenység követésére (kizárólag az általunk küldött e-mail tekintetében), az eszközökből kinyerhető naplókából jelentés és tetszőleges diagram kimutatás készíthető. A kampány eredményétől függően akár kiegészítő, személyre szabott oktatás is megvalósítható (awareness education).

*<https://liangroup.net/blog/wp-content/uploads/2021/07/Cost-of-a-Data-Breach-Report-2021.pdf>