FORTIX Consulting Kft.

Phishing szimuláció

A phishing vagy más néven adathalászat olyan támadási módszerek halmaza, amelyek során a támadó megpróbálja rávenni az áldozatát bizalmas adatok megadására (pl. személyazonosításra alkalmas adatok, banki és hitelkártyaadatok, valamint jelszavak).

Felhasználói tudatosságtól függően az emberek képesek lehetnek észlelni, cselekedni, jelenteni és megállítani ezeket a támadásokat. Azonban ehhez a megfelelő ismeretekre és tudatosságra van szükség. Ebben segítünk, **ellenőrzött körülmények között végzett adathalász szimuláció lefolytatásával, anélkül, hogy a szervezetet valós anyagi kár érné.** A szolgáltatás eredményeként az ügyfeleink pontos képet kapnak arról, hogy mi történne egy hasonló rosszindulatú támadás során, még a támadás valódi bekövetkezése előtt. Az általunk használt phishing tanácsadás segítségével nyomon követhetőek a felhasználói tevékenységek, valamint jelentések, diagramok állíthatók össze a teszt eredményeiről.

Az APWG jelentése szerint az elmúlt 4 évben 150%-kal nőtt az adathalász támadások száma évente.

Miért éri meg a cégeknek ezt a szolgáltatást igénybe venniük?

- **Valós, mérhető eredmény:** Felmérheti munkavállalói tudatosságát és felkészültségét az adathalász támadásokkal szemben.
- **Proaktív védekezés:** Az adathalászat szimulációval megtanítjuk a munkavállalókat a kiberbiztonsági veszélyek felismerésére és megelőzésére.
- **Növekvő tudatosság:** Személyre szabott oktatási programjaink által a munkavállalók tudatosabbak és képesek lesznek felismerni és kezelni a különböző kiberfenyegetéseket.
- **Védelem a lehetséges anyagi veszteségek ellen:** A kiberbiztonsági incidensek anyagi veszteségeket okozhatnak a vállalatoknak. A szimulációval és oktatással csökkenthetőek ezek a veszélyek.

Személyre szabott szimuláció

- Saját igényekhez illeszkedő e-mailek és landing page-ek
- Modern, jól ismert szolgáltatásokhoz alkalmazkodó sablonok
- Spear phishing célzott végrehajtása OSINT technikák alapján

Teljes körű technikai támogatás

- Szakértői előkészítés és technikai beállítások
- Rugalmasan időzített kampányok lebonyolítása
- Alapos eredményelemzés és részletes visszajelzés

Folyamatos biztonságfejlesztés

- Éves visszamérés és újabb kampányok a folyamatos fejlődésért
- Stratégiai védekezés a legújabb kiberfenyegetések ellen
- Naprakész munkatársi tudatosság és készenlét biztosítása