RedFlag Technologies Kft.

Nem csak kötelező, hanem befektetés is

- biztonságtudatossági képzés és a NIS2 kapcsolata

A kiberbiztonság napjainkban egyre fontosabb téma, hiszen a digitális világban a támadások száma és súlyossága is növekszik. Éppen ezért a biztonságtudatossági képzésnek a vállalati információbiztonság szerves részének kell lennie.

„Az információbiztonság a vállalat minden szintjén jelen kell legyen, mert csak így érhetünk el valódi védelmet a digitális világban. A biztonság nem csupán technológia, hanem egy közös felelősség is.”

A **NIS2 irányelv különös figyelmet szentel a kiberbiztonsági tudatosság növelésének**. A szervezeteknek előrelátóan kell eljárniuk, hogy mind a technológiai, mind az **emberi tényezőket figyelembe véve** javítsák biztonsági profiljukat, beleértve az **alkalmazottak folyamatos oktatását** és informálását is.

Az emberi hiba jelentős szerepet játszik a kiberbiztonsági incidensek kialakulásában. Az olyan tényezők, mint a phishing támadásokra való kattintás, a gyenge jelszavak használata, vagy a szoftverek frissítésének elmulasztása, mind növelik a sebezhetőséget.

Mik a legelterjedtebb támadási formák?

A legelterjedtebb támadások

A kiberbiztonsági fenyegetések számos formában jelentkezhetnek, de a leggyakoribb támadási módszerek, amelyek komoly veszélyt jelentenek a vállalatra, az emberi tényezőt célozzák meg.

- **Phising** - hamis e-mailek és weboldalak használata a felhasználói adatok ellopására
- **Ransomware** - a cég adatait zárolják, és csak váltságdíj ellenében oldják fel azokat
- **Malware** - kártékony adatlopó vagy egyéb megfigyelő szoftvereket juttatnak a rendszerbe
- **Social Engineering** - a befolyásolás és rábeszélés eszközével megtévesztik az embereket, manipulálják vagy meggyőzik őket

Miért fontos a humán tényező és miért kell vele foglalkoznunk?

- Az emberi tényező már akkor is a kiberbiztonság legsebezhetőbb pontja volt, amikor elkezdtük alkalmazni a jelszavakat.
- Manapság, ha rendszergazda nevében felhívunk egy titkárnőt vagy egy középvezetőt, és azt mondjuk, hogy behatolás történt, és a jelszavára van szükségünk a cég elleni kibertámadás megakadályozásához, **habozás nélkül lediktálják azt**.

Social engineering

- Mindegyik esetben előzetes információgyűjtés- és szerzés előzi meg a támadást – **OSINT elleni védekezés is fontos!**
- A leggyakoribb nem informatikai alapú támadási forma az emberi tényezőt, azaz a leggyengébb láncszemet célozza meg.
- Ez azért lényeges, mert a legtöbb vállalat számára már nyilvánvalóvá vált, hogy ha nem fektetnek be informatikai védelmi megoldásokba, akkor egy IT alapú támadás esetén a vállalat teljes működése leállhat.
- Ugyanakkor azokkal a támadásokkal, amelyeket a kiberbiztonsági szakemberek nem észlelnek, és amelyek rövid távon a cég vezetésének sem tűnnek fel, rendkívül nehéz foglalkozni. Ezért is népszerű módszer ez.

  -Idegen identitás felhasználása

  -Segítség kérése

  -Segítség nyújtása stb.

Ezekre a szituációkra a dolgozókat fel lehet és fel is kell készíteni biztonságtudatosító képzésekkel.

Melyek egy jó biztonságtudatossági képzés ismérvei?

- Egy jó képzés fő célja, hogy **a munkavállalók felismerjék, ha valami nem megfelelő egy adott helyzetben**, és ha ezt észlelik, kérdéseket tegyenek fel annak érdekében, hogy megállapítsák, jelent-e az adott szituáció kockázatot vagy sem.
- Egy jó biztonságtudatossági képzésnek **szerepkör alapúnak kell lennie**, mivel a különböző szerepkörök különböző típusú fenyegetésekkel és felelős-ségekkel szembesülnek.

Vezetők | Üzemeltetők | Felhasználók

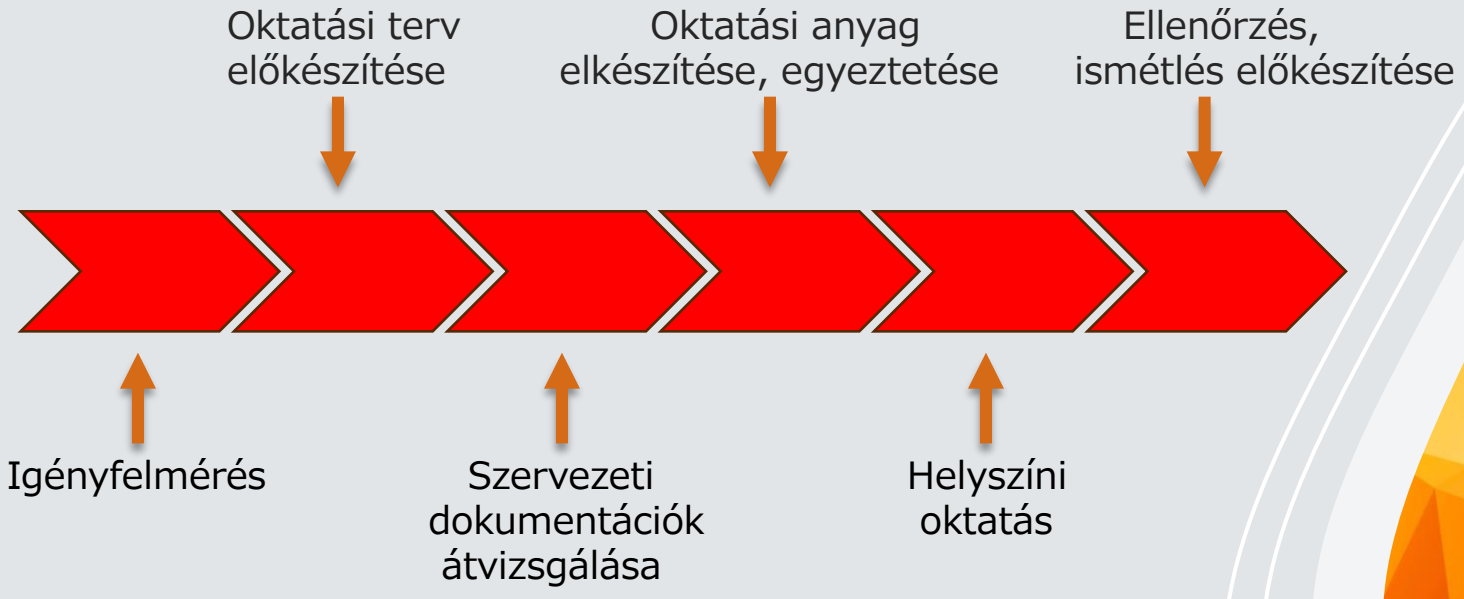
- Egy jó biztonságtudatossági képzés, **szervezet specifikus**.
  - A képzés tartalmát és módszereit kifejezetten az adott szervezet igényeihez és körülményeihez igazítják,
  - figyelembe veszi a szervezet egyedi működési szokásait
  - ténylegesen az adott szervezet saját biztonsági szabályzatait és eljárásait mutatja be.
- Egy jó biztonságtudatossági képzés, **rendszeres, mérhető, interaktív és figyelemfelkeltő**.
  - Folyamatosan frissíteni kell tudást és emlékeztetni kell a legjobb gyakorlatokra.
  - A résztvevők tudásának felmérésétől kezdve a kiberbiztonsági incidensek számának nyomon követéséig számos lehetőség.
  - Akár szimulációkat, gyakorlati feladatokat, csoportos megbeszéléseket és szerepjátékokat is alkalmazhatunk.
  - Valós példákat, aktuális eseményeket és a szervezet specifikus fenyegetéseit mutathatjuk be.
- Ezek mind segítenek abban, hogy a résztvevők **komolyan vegyék a kiberbiztonságot és alkalmazzák a tanultakat** a mindennapi munkájuk során.

Milyen támogatást kínálunk a NIS2 hatálya alá tartozó szervezetnek?

A szakmai auditra való felkészüléshez

A **felkészülés közben és azt követően is** a szervezetnél biztonságtudatossági oktatásokat tartunk.

Minden esetben szervezetspecifikus és szerepkör alapú képzést nyújtunk, amelyet előzetesen egyeztetünk is a megrendelővel.



Miért minket bízzon meg a biztonságtudatossági képzések megtartásával?

Gondoljuk végig az alábbiakat!

- **A felkészítő cégek fő profilja az információbiztonsági rendszer kialakítása.** A vállalatra vonatkozó NIS2 elvárásokat szeretnék teljesíteni, lehetőleg a határidőket betartva.
- **A felkészítő cégeknél az oktatás a felkészítési folyamat egy részterülete, míg mi erre helyezzük a hangsúlyt.** Képzéseink interaktívak és érdekesek, valós példákkal és gyakorlati feladatokkal illusztrálva.
- **A felkészítést-, sőt az auditot követően is tartunk képzéseket igazodva a megrendelő szervezeti fejlődéséhez.** Természetesen a felkészítés során folyamatosan együttműködünk a választott felkészítő céggel.
- **OSINT szolgáltatás:** Egyedülálló módon, igény esetén OSINT (Open Source Intelligence) elemzést is végzünk. Feltérképezzük, milyen nyilvánosan elérhető információk állnak rendelkezésre a megrendelő szervezetéről, amelyek egy támadó számára hasznosak lehetnek. **Ezzel segítünk felkészülni a social engineering technikák hatékonyabb kivédésére.**

RedFlagOSINT

SIMPLIFYING THE COMPLEXITY OF OPEN SOURCE INTELLIGENCE

RedFlag Technologies Kft.

Dr. Nyerges Ádám

ügyvezető,
elektronikus információbiztonsági vezető

info@redflagosint.com

+36 (1) 793-0007

1098 Budapest, Lobogó utca 5.