Hogyan épít egy Bank CTI információkat?

Korvin András Gábor
osztályvezető
OTP Bankcsoport Kibervédelmi Központ

A kiberfenyegetettségi hírszerzési ciklus

A kiberfenyegetettségi hírszerzés egy ciklikusan ismétlődő elemekből álló folyamat:

A kiberfenyegetettségi hírszerzési ciklus öt fázisból áll: ***1) tervezés és irányítás; 2) gyűjtés; 3) feldolgozás; 4) elemzés; 5) terjesztés***

***adat**: a hír vagy információ értelmezhető, lejegyezhető formája. Valakinek vagy valaminek a megismeréséhez hozzásegítő tény, részlet.*

***Információ**: adat vagy hír megerősített, ellenőrzött és további felhasználásra kész formája.*

A tervezés és irányítás során a hírigény meghatározására kerül sor, melynek során annak végfelhasználója (itt SOC vagy IB terület) konkrét témára vagy célra kéri hírek szerzését. **A gyűjtés** során nyers adatok gyűjtése és azok generálása történik. Az adat nem ugyanaz, mint az információ, ezért át kell alakítani, és ezért át kell mennie **a feldolgozási és elemzési fázisokon**. **A feldolgozás** során a nyers adatokat szűrik és felkészítik az elemzéshez. **Az elemzés** során a megszerzett adatok és hírek információvá válnak. Végül **a terjesztési fázisban** az új hírszerzési információt a különböző felhasználóknak továbbítják a szükséges mértékben.

A fenyegetésekkel kapcsolatos hírszerzés forrásai

Különböző források, ahonnan fenyegetésekkel kapcsolatos adatok gyűjtése lehetséges:

Belső hálózatok és biztonsági eszközök: A szervezet hálózati és biztonsági eszközeiből származó metaadatok és naplóállományok.

Külső hírcsatornák: Iparági szervezetektől, kiberbiztonsági szállítóktól és fenyegetési adatcsatornáktól származó adatok.

Emberi források (HUMINT): Beszélgetések hozzáértő, a témára rálátó forrásokkal.

Nyílt források (OSINT): Hírek, blogok, webhelyek és fórumok.

Zárt források: Dark web, zárt közösségek, informális társulások belső kommunikációja, stb.

Adatgyűjtési folyamat

A kiberfenyegetettségekkel kapcsolatos adatok gyűjtésének lépései:

Adatösszesítés: Adat-, és hírgyűjtés különböző forrásokból.

Adatfeldolgozás: Adatok lefordítása használható formátumokra (pl. STIX/TAXII, JSON, YARA).

Adatértékelés: A megbízhatóság és a relevancia értékelése.

Adatgazdagítás: Kontextus és elemzés hozzáadása.

Kihívások

A fenyegetésekkel kapcsolatos adatok és hírek gyűjtésével kapcsolatos gyakori kihívások:

Adatbőség, entrópia és zaj: A releváns (~actionable intel) adatok kiszűrése a zajból.

Időszerűség: A fenyegetettséggel összefüggő és adatok, hírek valós idejű frissítésének/naprakészségének biztosítása.

Minőség: A kiberfenyegetettséggel összefüggő adatok, hírek pontosságának és hitelességének ellenőrzése.

Minőség: A pontosság és hitelesség ellenőrzése

A fenyegetésekkel kapcsolatos adatok és hírek gyűjtésével kapcsolatos bevált gyakorlatok:

Automatizálás, ahol lehetséges: Használjunk eszközöket az adatgyűjtés és az adatkorreláció egyszerűsítéséhez.

Együttműködés: Kapcsolattartás biztonsági szakemberekkel és szervezetekkel (Pl.: MNB, NKI, Bankszövetség).

Naprakészség: Rendszeresen frissítsük fenyegetésintelligencia-forrásainkat, ide értve a közösségi, a szolgáltatói és a szervezeti forrásokat is.

Mi kell a Cyber Threat Intelligence (CTI) képesség kiépítéséhez?

A CTI mibenlétének a megértése: A fenyegetésfelderítés lényege, hogy értelmes információkat nyerjen ki a fenyegetések szereplőinek tevékenységével kapcsolatos rendelkezésre álló adatokból. Ez az információ betekintést nyújt a támadói oldal működésébe és segít a szervezeteknek megérteni a külső kiberfenyegetések kockázatait.

A kiberfenyegetések felderítésének fontosságának a megértése: Minden olyan vállalkozásnak, amely olyan adatokat tárol, amelyek értékesek lehetnek a hackerek számára, biztonsági terveinek elemeként figyelembe kell vennie a kiberfenyegetések felderítését. A fenyegetésfelderítés támogatja a szervezeteket azáltal, hogy betekintést nyújt a fenyegetések mechanizmusaiba, lehetővé téve számukra védelmi stratégiák és keretrendszerek kiépítését, valamint a támadási felület csökkentését.

A Fenyegetésfelderítés felhasználása: A Fenyegetésfelderítés segít a téves riasztások szűrésében, valamint a szervezet által leginkább veszélyeztetett speciális fenyegetések és biztonsági rések felismerésében. Ez lehetővé teszi, hogy a Security Operations Center (SOC) időben tudjon megelőző-elhárító lépéseket tenni.

Együttműködés és információmegosztás: Kiemelten fontos a társszervezetek között a releváns, strukturált és bővített fenyegetési információk megosztása (pl. Bankcsoporton belül).

Folyamatos tanulás és alkalmazkodás: A támadások mechanikája és dinamikája folyamatosan fejlődik, és fontos, hogy naprakészek legyünk a legújabb eszközökkel, technikákkal és gyakorlatokkal kapcsolatban. **A CTI képesség kiépítése nem egyszeri erőfeszítés.** Folyamatos tanulást és alkalmazkodást igényel a folyamatosan változó környezet megértéséhez. Az is fontos, hogy megfelelő csapat és erőforrások álljanak rendelkezésre az összegyűjtött CTI hatékony kezeléséhez és felhasználásához.

Gyakorlati példák + kérdések

Köszönöm a figyelmet!