



FORTIX Consulting Kft.

SÉRÜLÉKENYSÉG MENEDZSMENT

Modern világunk technikai fejlődésével lépést tartani egyetlen szervezet informatikai csapatának sem egyszerű feladat.

Nem csupán folyamatosan felkészültnnek kell lenni, de a biztonságos üzemeltetéshez egyre több tényezőt kell figyelembe venni

- IoT (a dolgok Internetje) terjedése, minden mindennel kapcsolatban van, kapcsolatban lehet.
- A rendszerek egyre nagyobbá, komplexebbé válnak.
- Az informatika mára már infokommunikációvá vált és a mindennapi életben szinte minden területen meghatározó tényező lett.
- Új, eddig nem ismert megoldások, szolgáltatások jelennek meg.
- A rohanó világ a fejlesztésre is rányomta a bélyegét. A fejlesztők között is folyamatos verseny folyik, hogy ki tud gyorsabban és olcsóbban előállítani egy terméket.
- Az új rendszerek új kihívásokat jelentenek a felhasználóknak, a fejlesztőknek, az üzemeltetőknek egyaránt.
- Az új rendszerek új lehetőségeket nyújtanak a támadóknak, de nem csak az új rendszereken, hanem a már meglévő régieken is.



A kibertámadások célja és módja sokféle lehet.

Közös bennük az, hogy valahogyan be kell jutni a rendszerbe, hogy a kívánt célt megvalósíthassák. Ehhez rést kell találni a védelemben.

A legegyszerűbb – és egyben a leggyakoribb is – azon rések megtalálása, amelyeket már ismertek, amelyeket már publikáltak.

Ezt a támadók is jól tudják, és előszeretettel használják is idegen rendszerekbe történő bejutásra, azokban történő mozgásra.



A sérülékenység vizsgálat célja az, hogy az ilyen réseket, sérülékenységeket megtaláljuk még az előtt, hogy azokat a támadók találnák meg és használnák ki.

A begyűjtött adatok kiértékelésre és riportálásra kerülnek a szervezet felé. A sérülékenység vizsgáló szakember számos eszközt használhat a vizsgálatok elvégzésére.

Ezek lehetnek automatizált eszközök, amelyeket helyileg, vagy felhőben futtathatnak; de lehetnek manuális módszerek is. A sérülékenység vizsgálat folyamán feltárt kockázatok a sérülékenység menedzsment keretében prioritizálásra és kezelésre kerülnek, melyet a szervezettel együtt működve végzünk.

A sérülékenység menedzsment nem egy projekt, aminek kezdete és vége van. A sérülékenység menedzsment egy tevékenység, amely által a szervezet rendszerei folyamatos monitorozás és korrigálás alatt áll. A folyamat célja, hogy a szervezet rendszereit folyamatosan a lehető legbiztonságosabban tartsa az állandóan változó körülmények ellenére.