OUCH! 2022. február

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Bárki kezdhet karriert a kiberbiztonság területén

Áttekintés

Szinte minden nap olvashatunk a hírekben a kiberbiztonságról, miután szerte a világon folyamatosak a zsarolóvírus támadások, csalások és számítógépes támadások, amelyek a különböző szervezeteket és a kormányokat sújtják. Az ilyen fenyegetések elleni védelem érdekében óriási igény mutatkozik a kiberbiztonság terén képzett szakemberek iránt. A legújabb tanulmányok becslése szerint világszerte csaknem 3 millió kiberbiztonsági állás áll betöltetlenül.

Gondolkozott már azon, hogy kiberbiztonsági szakemberként dolgozzon? Ez egy pörgős, dinamikus terület, ahol rengeteg izgalmas és speciális terület közül lehet választani. Ezek a pozíciók olyan területeket foglalnak magukban, mint a (digitális) kriminalisztika, tudatosság és képzés, végpontbiztonság, kritikus infrastruktúra, incidenskezelés, biztonságos kódolás és jogi szabályozás. A kiberbiztonsági karrier azt is lehetővé teszi, hogy szinte bárhol dolgozhassunk a világon, különféle előnyökkel és lehetőséggel, így valódi változást érjünk el.

Szükség van ehhez számítástechnikai végzettségre?

Egyáltalán nem. A legjobb biztonsági szakemberek közül sokan nem rendelkeznek műszaki háttérrel. A kulcs a tanulási szenvedély. Miután megértettük, hogy hogyan működnek a technológiák – és miként törhetőek fel – biztonságosabbá tehetjük őket. A kiberbiztonság azért izgalmas, mert saját tempónkban kezdhetjük el a tanulást az otthonunk kényelmében.

Hogyan kezdjünk hozzá?

Kezdjük el a különböző területek felfedezését, hogy meghatározhassuk a fő érdeklődési köröket. Kezdhetjük csak az otthoni számítógépekkel vagy eszközökkel.

- **Programozás**: Ismerjük meg a programozás alapjait! A Python, a HTML vagy a JavaScript mind jó nyelvek a kezdéshez. Vegyük fontolóra egy online oktatóoldal használatát, vagy szerezzünk be egy programozásról szóló, kezdőknek szánt könyvet.
- **Rendszergazda**: Ismerjük meg az operációs rendszerek, például a Linux vagy a Windows rendszergazdai kezelésének alapjait. Ha igazán ki akarunk tűnni, szerezzünk szakértelmet a parancssori felület kezelésében és a szkriptírásban.
- **Alkalmazáskezelés**: Ismerjük meg, hogyan konfigurálhatjuk, futtathatjuk vagy tarthatjuk karban az alkalmazásokat, például a webszervereket!

- **Hálózatkezelés**: Fedezzük fel, miként kommunikálnak egymással a számítógépek és a hálózati eszközök a forgalom rögzítésével és elemzésével! Ez jó szórakozás is lehet, mivel az otthonunk nagy valószínűséggel már egy kész hálózati környezet, amelyhez mindenféle eszköz csatlakozik.
- **Felhő-alapú technológiák**: Ismerjük meg a felhőszolgáltatások működését és azok kiaknázásának különböző módjait!

Állítsuk össze saját otthoni laborunkat! Használhatunk online felhőforrásokat, például az Amazon AWS-ét, vagy a Microsoft Azure-ját. Esetleg virtuális operációs rendszereket is létrehozhatunk ugyanazon a fizikai számítógépen virtualizációs szolgáltatásokkal. Ha közvetlenül hardverrel szeretnénk dolgozni, vásároljunk egyszerű, olcsó számítógépeket, mint például a Raspberry Pi vagy az Arduino. Ha beüzemeltük rendszereinket, kezdjük el használni őket, és tanuljunk meg mindent a konfigurálásukról és optimalizálásukról, vagy kezdjünk el programozni és kódolni ezeken a rendszereken! Nincs jó vagy rossz út az induláshoz, csak kövessük, amerre az érdeklődési körünk visz!

Egy másik nagyszerű módja az indulásnak, ha találkozunk és együttműködünk másokkal. Fontoljuk meg, hogy részt vegyünk egy helyi kiberbiztonsági konferencián, vagy egy olyan virtuális „konferencián", mint például a Bsides vagy a SANS New2Cyber! A legnehezebb az első esemény vagy találkozás megtalálása. Miután részt vettünk egy ilyen konferencián, igyekezzünk kapcsolatba lépni más résztvevőkkel, és bővítsük a szakmai hálózatunkat!

A kiberbiztonság tanulásának további lehetőségei közé tartoznak a YouTube videók, a podcastok hallgatása, az online fórumok látogatása, a biztonsági szakemberek blogjaira való feliratkozás vagy az online Capture the Flag (CTF) eseményeken való részvétel. Végezetül, ne hagyjuk, hogy végzettségünk vagy hátterünk visszatartson bennünket! A tanulás és mások segítése iránti szenvedély, valamint a „megszokásokon túli gondolkodás" képessége kulcsfontosságú tulajdonságok. Ha elkezdjük fejleszteni a technikai készségeinket és találkozunk másokkal, előbb-utóbb jönnek majd a lehetőségek.

A szerzőről

Lodrina Cherne (@hexplates) biztonsági ügyvéd a Cybereasonnál. Célja az innováció előmozdítása, a kiberbiztonsági szabványokkal és eljárásokkal kapcsolatos legjobb gyakorlatok fejlesztése. Emellett okleveles oktató a SANS Institute-nál, ahol segít az információbiztonsági szakembereknek a digitális kriminalisztika és az incidensreagálás (DFIR) területén.

Források

Security Bsides Conferences: http://www.securitybsides.com/
Women in Cybersecurity: https://www.wicys.org/
New2Cyber YouTube Playlist: https://youtube.com/playlist?list=PLtgaAEEmVe6BQkZiJC5nIk9xx74QTGtsZ
SANS Cyber Academies: https://www.sans.org/scholarship-academies/
SANS Cyber Aces: https://www.cyberaces.org/
Cybersecurity Podcasts: https://www.sans.org/blog/cybersecurity-podcast-roundup/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)