
Az Ön havi biztonságtudatossági hírlevele

# Kiberbiztonsági karrier

## Áttekintés

A kiberbiztonság valami olyasmi, amiről szinte mindennap olvashat a hírekben, ugyanis a szervezetek és kormányok rendszerei folyamatosan áldozatául esnek az informatikai támadásoknak. Óriási a kereslet a kiberbiztonsági szakemberek iránt, akiktől segítséget várnak a növekedő fenyegetéssel szemben. A becslések szerint már közel három millió ilyen nyitott állás létezik világszerte. Gondolkozott már azon, hogy kiberbiztonsági szakértőként dolgozzon? Ez egy gyors léptékű, dinamikusan fejlődő szakma rengeteg specializálódási területtel, mint például a digitális nyomelemzés, a végpontvédelem, a kritikus infrastruktúrák védelme, az incidenskezelés, a biztonságos programozás, valamint az információbiztonság tudatosság fejlesztése. A kiberbiztonsági karrier ráadásul a világ szinte bármely pontján munkalehetőséget biztosíthat, kiemelkedő juttatásokkal és lehetőségekkel.

## Szükségem van ehhez informatikai végzettségre?

Egyáltalán nem. A legjobb biztonsági szakértők közül néhánynak nincs is technikai háttere: az angol nyelvtanártól kezdve, medikusokon vagy történészeken át autószerelőkig, művészekig vagy háziasszonyokig terjed a skála. A kulcs a tanulás szenvedélye – a kiberbiztonság arról szól, hogy megtanuljuk, hogyan működnek a dolgok. Amint megértjük, hogy a technológia miként működik, jobban meg tudjuk azt védeni. Ami nagyon izgalmas a kiberbiztonságban, az az, hogy az ezzel kapcsolatos ismereteket a saját tempónkban, a saját otthonunk kényelmében sajátíthatjuk el.

## Hogyan kezdjünk neki?

Nem tudja, hogyan álljon neki? Kezdje a különböző technológiák felfedezésével, azokkal, amelyek érdeklik.

**Programozás:** Tanulja meg a programozás alapjait, ehhez jó kiindulási alap a Python, a HTML vagy a Javascript programozási nyelv. Nem tudja, honnan kezdje a tanulást? Fontolja meg az online képzéseken való részvételt. vagy ragadjon meg egy kezdőknek szóló programozási tankönyvet.

**Rendszer:** Tanulja meg az operációs rendszerek kezelésének alapjait, mint például a Linux, vagy a Windows. Ha igazán belevetné magát az informatika „sűrűjébe”, kezdje a Linux-szal. Egy Linux rendszer parancssorból történő irányításának ismerete olyan erős képesség, ami segítséget jelent majd, bármilyen irányba is induljon később.

**Alkalmazások:** Tanulja meg, hogyan konfiguráljon, futtasson és tartson karban olyan alkalmazásokat, mint egy webszerver vagy egy DNS szerver.

**Hálózatok: A hálózati forgalom elfogása és elemzése során ismerje meg, hogyan működnek a hálózatok, és hogyan „beszélnek” egymással a számítógépek és informatikai eszközök. Ez jó móka lehet, mivel otthona már így is jó eséllyel egy önálló hálózati környezet, amire mindenféle eszköz rákapcsolódik.**

A tanulás legjobb módja egy otthoni labor kialakítása. Mindez elég könnyen kivitelezhető, hiszen ugyanazon fizikai eszközön akár többféle virtuális operációs rendszert is kialakíthat, vagy létrehozhat egy környezetet felhő alapú szolgáltatások segítségével is, mint például az Amazon AWS, vagy a Microsoft Azure. Amint az operációs rendszerei működőképesek, vegye őket használatba, tanuljon meg mindent, amit csak tud. Egy másik lehetőség, hogy személyes kapcsolatokat alakít ki, és együtt dolgozik olyanokkal, akik szintén a kiberbiztonság területén tevékenykednek. Fontolja meg, hogy részt vesz egy kiberbiztonági konferencián (ezeket gyakran csak „con”-nak hívják). A legtöbb (amerikai) nagyvárosban rendeznek néhányat évente. Egy jól ismert kiberbiztonsági rendezvénysorozat, amit kifejezetten a kezdők megsegítésére terveztek, a Bsides. A legnehezebb feladat az első rendezvényt, vagy találkozót megtalálni. Amint már részt vett egyen, az ismeretségi köre és lehetőségei exponenciálisan nőni fognak. A tanulás másik lehetséges formája a YouTube videók megtekintése, az online fórumok vagy a kiberbiztonsági szakértők blogjaira való feliratkozás, vagy részvétel egy online Capture the Flag (CTF) rendezvényen. Végezetül számos program létezik, ami segíthet a karrierje elindításában, beleértve a CyberTalent Immersion Akadémiákat, a Cyber Aces-t, és a Cyber Patriot programokat.

Nem utolsósorban ne engedje, hogy a tanulmányi, vagy szakmai háttere visszatartsa. Nem számít mivel foglalkozott korábban, valami egyedit és különlegeset hozhat így a kiberbiztonság területére. A kulcs a tanulás iránti szenvedély. Amint elkezdi fejleszteni tudását és elkezd megismerkedni másokkal az adott területről, a lehetőségek jönni fognak.

## Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

## A szerzőről

***Heather Mahalik*** *(@heathermahalik) a ManTech CARD-nál a Digitális Nyomrögzítés szakterület igazgatója, valamint a „SANS Digital Forensics and Incident Response (DFIR)” és a “SANS Digitális nyomelemzés és Incidens kezelés” tanfolyamok instruktora. Csaknem 17 éve foglalkozik kiberbiztonsággal és imádja a munkáját. Ő vezeti a www.smarterforensics.com blogot.*

## Források

| | |
|---|---|
| Bsides: | http://www.securitybsides.com |
| CyberTalent Immersion Academies: | https://www.sans.org/cybertalent/cybersecurity-career/seekers |
| Cyber Aces: | https://www.cyberaces.org |
| Cyber Patriot: | https://www.uscyberpatriot.org/ |
| Code Academy: | www.codeacademy.com |