CTI elemzés

A hackerek világa



1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezetés 4

A „hacker” fogalom kialakulása és története 5

A hackerek típusai 6

Fehér kalapos hackerek 7

Fekete kalapos hackerek 10

Script kiddie 12

Magányos kiberbűnözők 14

Szervezett kiberbűnözői csoportok 16

APT-csoportok 18

Hacktivista csoportok 20

Insider támadók 22

Szürke kalapos hackerek 24

Zöld kalapos hackerek 26

Kék kalapos hackerek 28

A Blue Hat és a Blue Team közötti különbség 28

Piros kalapos hackerek 30

A Red Hat és a Red Team közötti különbség 31

A mesterséges intelligencia szerepe a kibertámadásokban 32

Összegzés 34

Források 36



Bevezetés

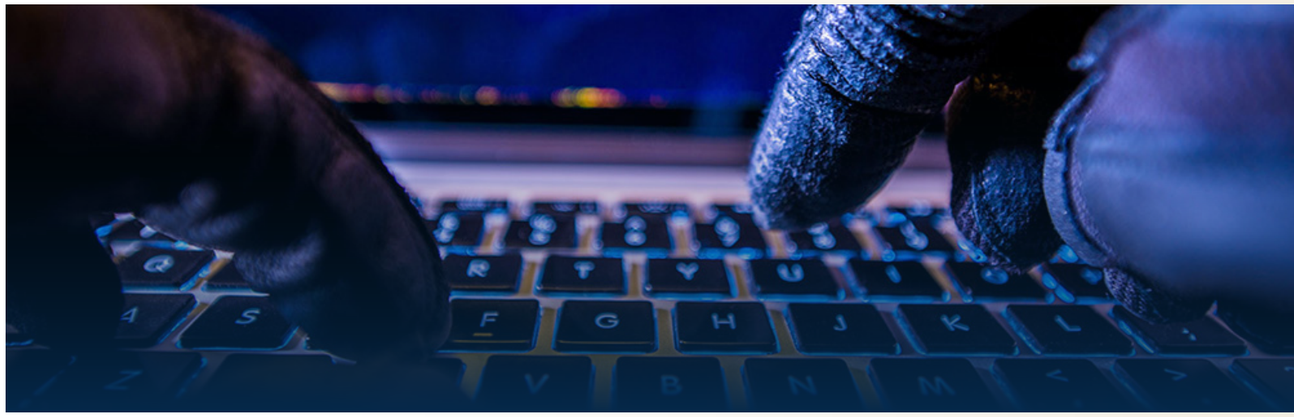
A digitális adatok védelme, valamint azok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása az információbiztonság egyik alapvető követelménye (CIA-elv).

A digitális infrastruktúrák fejlődésével és az informatikai rendszerek egyre szélesebb körű alkalmazásával párhuzamosan a kibertérben megjelenő fenyegetések folyamatosan egyre összetettebbé és gyakoribbá válnak. Az adatlopások, zsarolóvírus-támadások, elosztott szolgáltatásmegtagadás támadások (Distributed Denial of Service, DDoS), valamint az államilag támogatott kiberműveletek jelentős gazdasági, társadalmi és nemzetbiztonsági kockázatot is hordoznak önmagukban.

A kibertámadásokkal összefüggésben gyakran használt fogalom a „hacker" kifejezés, amelynek jelentése a köznyelvben sok esetben leegyszerűsített és sok esetben kizárólag a rosszindulatú informatikai tevékenységgel azonosítják. A hackertevékenység megítélését, annak célja, alkalmazási módja és jogszerűsége határozza meg. Ennek alapján megkülönböztethetők a rendszerek védelmét támogató etikus szakemberek, valamint a tudásukat jogellenes célokra felhasználó szereplők.

A kibertámadások célja anyagi haszonszerzés, ipari kémkedés, politikai befolyásszerzés vagy kritikus infrastruktúrák működésének megzavarása is lehet. Ezzel szemben az etikus hackelés és a penetrációs tesztelés a kiberbiztonság szerves részét képezik, mivel lehetőséget biztosítanak a rendszerekben, hálózatokban és alkalmazásokban fennálló hiányosságok azonosítására és kezelésére.

Jelen CTI elemzés célja a hacker fogalom kialakulásának és történeti fejlődésének rövid bemutatása, valamint az egyes hackertípusok és azok jellemzőinek részletes ismertetése. A jelentés emellett kitér arra is, hogy a különböző szereplők milyen célokkal és módszerekkel alkalmazhatják technikai ismereteiket, illetve milyen szerepet tölthetnek be a kiberbiztonságban.



A „hacker" fogalom kialakulása és története

A hacker kifejezés eredetileg a technikai leleményességet, a kreatív problémamegoldást és a rendszerek működésének mélyebb megértését jelentette. A hackerkultúra az 1960-as években, elsősorban egyetemi és kutatói környezetben alakult ki, ahol a tudásmegosztás, az együttműködés és az innováció fontos szerepet kapott. A személyi számítógépek és az internet elterjedésével azonban a fogalom jelentése fokozatosan átalakult, és a hacker kifejezés egyre inkább összekapcsolódott a jogosulatlan hozzáféréssel és a kiberbűnözéssel.

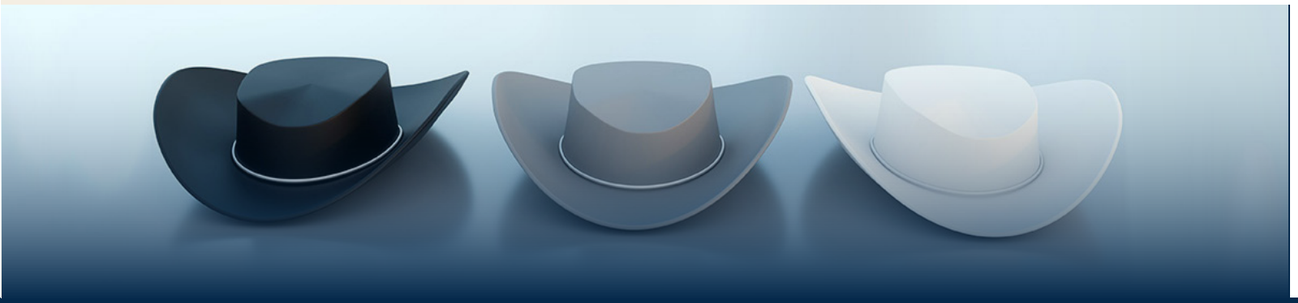
A hackerek típusai

A hacker nem egy egységes kategóriát, hanem különböző célokkal és szerepkörökkel rendelkező személyek és csoportok összefoglaló megnevezését jelenti. A hackertevékenység sokrétű, ezért többféle osztályozási rendszer alakult ki a különböző szereplők elkülönítésére. A kategorizálás során általában

- a tevékenység jogszerűségét,
- célját,
- módszereit,
- technikai felkészültségét és
- az elkövetők motivációját veszik figyelembe.

A legelterjedtebb a kalapszínek szerinti (hat model) kategorizálás, amely elsősorban a hackerek etikai megítélése és tevékenységük jellege alapján különíti el az egyes csoportokat. Megkülönböztetünk fehér kalapos (white hat), fekete kalapos (black hat), szürke kalapos (grey hat), zöld kalapos (green hat), kék kalapos (blue hat) és piros kalapos (red hat) hackereket is. Az egyes kategóriák között nem mindig húzható éles határvonal, mivel egy hacker tevékenysége, motivációja vagy szerepe idővel változhat.

A következő alfejezetek a legfontosabb hackertípusokat mutatják be, kitérve azok céljaira, módszereire, etikai és jogi megítélésére, valamint a kiberbiztonságban betöltött szerepükre.



Fehér kalapos hackerek

A fehér kalapos hackerek (White Hat Hackers), más néven etikus hackerek (Ethical Hackers), a kiberbiztonsági ökoszisztéma meghatározó szereplői. Elsődleges céljuk az informatikai rendszerek biztonságának növelése, a sérülékenységek feltárása és a támadási felületek azonosítása. Tevékenységük során a támadókhoz hasonló módszereket alkalmaznak, azonban munkájuk minden esetben jogszerű keretek között, a rendszerért felelős szervezet előzetes engedélyével történik.

A fehér kalapos hackerek jellemzően vállalatok, állami szervezetek, kritikus infrastruktúrát üzemeltető intézmények vagy információbiztonsági szolgáltatók megbízásából dolgoznak. A vizsgálatok megkezdése előtt meghatározzák a tesztelés célját, hatókörét, módszereit és korlátait, ezáltal biztosítva, hogy az ellenőrzések ne veszélyeztessék a szervezetek működését, és megfeleljenek a jogszabályi követelményeknek.

A white hat hackerek munkájának fontos részét képezhetik a biztonsági auditok, a sérülékenységvizsgálatok és a penetrációs tesztelések. Ezen tevékenységek célja, hogy egy informatikai rendszer, alkalmazás vagy hálózati infrastruktúra mennyire ellenálló a valós támadási kísérletekkel szemben. A vizsgálatok eredményei alapján az etikus hacker a technikai hibák feltárásán túl azok kockázatát is értékelheti, és javaslatokat fogalmazhat meg a problémák kezelésére és a szükséges kockázatcsökkentő intézkedések meghatározása. Ezzel közvetlenül támogathatja az informatikai és információbiztonsági csapatok munkáját.

A vizsgálatok hatóköre az adott megbízástól függően rendkívül széleskörű lehet. Kiterjedhet webalkalmazásokra, mobilalkalmazásokra, szerverekre, operációs rendszerekre, adatbázisokra, hálózati eszközökre, vezeték nélküli hálózatokra és felhőalapú környezetekre, valamint az ezeket összekapcsoló hitelesítési és hozzáférés-kezelési mechanizmusokra. Egy átfogó biztonsági értékelés során az egyes rendszerek technikai sérülékenységeit vizsgálják, illetve azt is, hogy a különböző komponensek együtt milyen lehetőségeket kínálnak a támadók számára.

A webalkalmazások biztonsági vizsgálatánál például az autentikáció és az autorizáció megfelelő működése, a munkamenetek kezelése, a bemeneti adatok validálása, a hozzáférés-vezérlés, valamint az érzékeny adatok kezelése is a vizsgálat részét képezheti.

A bemeneti adatok nem megfelelő ellenőrzése például SQL injection vagy cross-site scripting (XSS) típusú sérülékenységekhez vezethet. SQL injection esetén a nem megfelelően kezelt felhasználói bemenet lehetőséget teremthet arra, hogy a támadó által megadott bemeneti adatok az alkalmazás által összeállított adatbázis-lekérdezés részévé váljanak. Megfelelő körülmények között ez jogosulatlan hozzáférést vagy akár az adatbázis tartalmának módosítását is lehetővé teheti. A biztonsági vizsgálat során annak felmérése is fontos, hogy a sebezhetőség kihasználása milyen hozzáférést tehet lehetővé vagy következményeket vonhat maga után.

Az autentikáció biztonsága szintén kiemelt vizsgálati terület. Az etikus hacker ellenőrizheti például, hogy megfelelően védettek-e a bejelentkezési mechanizmusok, megfelelően működik-e a munkamenetek kezelése, érvényesül-e a többtényezős hitelesítés, illetve megkerülhető-e az autentikáció vagy a jogosultság-ellenőrzés.

A hálózati és szerveroldali vizsgálatok során más típusú problémák kerülhetnek előtérbe. Ilyen lehet például a nem megfelelő rendszerkonfiguráció, a működéshez nem szükséges, de elérhető hálózati szolgáltatás, a hibásan kialakított hozzáférés-vezérlés, az elavult vagy sérülékeny szoftverkomponens, illetve a biztonsági frissítések hiánya. A sérülékenységvizsgálat során automatizált eszközöket is alkalmazhatnak az ismert sérülékenységek és konfigurációs problémák azonosítására.

A penetrációs tesztelés során az előre meghatározott szabályok és engedélyezett határok között az etikus hacker ellenőrzött módon megpróbálhatja igazolni, hogy egy azonosított sérülékenység a gyakorlatban valóban kihasználható-e, és a sikeres kihasználás milyen következményekkel járhat. A cél a sérülékenység tényleges kockázatának demonstrálása.

Az etikus hacker munkája ezért több egymásra épülő tevékenységből áll. A vizsgálati célok és a hatókör meghatározásából, a célrendszerek feltérképezéséből, a sérülékenységek azonosításából és szakértői ellenőrzéséből, a kockázatok értékeléséből, majd az eredmények dokumentálásából és a javítási javaslatok megfogalmazásából. A folyamat végén általában részletes jelentés készül, amely bemutatja a feltárt problémákat, azok súlyosságát és hatását, valamint a javasolt biztonsági intézkedéseket. A white hat hacker nem egyszerűen „betörni próbál” egy rendszerbe, hanem ellenőrzött körülmények között azt vizsgálja, hogy egy támadó milyen lehetőségeket használhatna ki, és hogyan lehet ezeket még a tényleges támadás előtt megszüntetni.

A technikai vizsgálatok mellett a social engineering technikák alkalmazásának tesztelése is szerepet kaphat. Ilyenkor szintén ellenőrzött körülmények között azt vizsgálják, hogy a munkatársak

mennyire képesek felismerni és elhárítani a megtévesztési kísérleteket, például az adathalász üzeneteket. A cél a szervezet biztonságtudatosságának és védekezési képességének felmérése.

A white hat hackerek munkája több területen is erősítheti egy szervezet biztonságát. A sérülékenységek proaktív feltárásával csökkenthető az adatvesztés, a szolgáltatáskimaradás és az egyéb kibertámadásokból eredő károk kockázata. Munkájuk emellett támogathatja a különböző biztonsági követelményeknek és szabványoknak való megfelelést, valamint erősítheti a szervezet biztonságtudatosságát.

2026-ban Pap Gergő kiberbiztonsági kutató két kritikus nulladik napi sérülékenységet azonosított az Acer Wave 7 mesh routerekben, amelyeket felelős közzététel keretében jelzett a gyártónak. Ugyancsak egy biztonsági kutató jelentette a Chrome V8 JavaScript- és WebAssembly-motorjának egyik aktívan kihasznált nulladik napi sérülékenységét, amelyet a Google később javított.

Fekete kalapos hackerek

A fekete kalapos hackerek (Black Hat Hackers) informatikai tudásukat jogosulatlan hozzáférés megszerzésére, rendszerek kompromittálására vagy egyéb jogellenes célok megvalósítására használják fel. Tevékenységük közvetlenül veszélyeztetheti az információbiztonság alapvető követelményeit.

A kiberbűnözés az elmúlt évtizedekben jelentős átalakuláson ment keresztül, az egyéni elkövetők mellett egyre nagyobb szerepet töltenek be a nemzetközi kiberbűnözői hálózatok. Ezek a csoportok különböző területekre specializálódva, fejlett technikai eszközökkel és üzletszerű működési modellekkel rendelkeznek.

Egyes támadók elsősorban kíváncsiságból vagy elismerésszerzés céljából végeznek jogosulatlan tevékenységet, míg mások pénzügyi haszonszerzésre, politikai befolyásszerzésre, ipari kémkedésre vagy stratégiai célok elérésére törekednek. A kiberfenyegetések fejlődésével a korábbi támadási formák mellett egyre összetettebb és kifinomultabb módszerek is megjelentek, például a zsarolóvírus-szolgáltatásként működő modellek (Ransomware-as-a-Service), a célzott kiberműveletek és a mesterséges intelligenciát alkalmazó támadási technikák.

A fekete kalapos hackerek csoportosítása több szempont alapján történhet, például:

- a technikai felkészültség,
- az alkalmazott módszerek,
- a szervezettség és
- a motiváció alapján.

A fekete kalapos hackerek főbb csoportjai:

1. Script kiddie
2. Magányos kiberbűnözők
3. Szervezett kiberbűnözői csoportok
4. APT-csoportok
5. Hacktivista csoportok
6. Insider támadók



Script kiddie

A fekete kalapos hackerek hierarchiájának legalacsonyabb szintjén helyezkednek el. A script kiddie elnevezés arra utal, hogy ezek a támadók jellemzően előre elkészített, mások által fejlesztett programokat és eszközöket alkalmaznak, amelyeket minimális módosítással vagy akár változtatás nélkül használnak.

A script kiddie-k az 1990-es évek közepétől váltak ismertté. Technikai tudásuk általában nem elegendő új sérülékenységek azonosítására vagy saját exploitok fejlesztésére, ezért mások által készített, könnyen hozzáférhető programokra, exploitokra és szkriptekre támaszkodnak. Ezek segítségével ismert sérülékenységeket használhatnak ki, illetve egyszerűbb kibertámadásokat hajthatnak végre anélkül, hogy teljes mértékben értenék az alkalmazott eszközök vagy technikák működését. A script kiddie-k motivációját többnyire

- a kíváncsiság,
- a szórakozás,
- a technikai eszközök kipróbálása, valamint
- a kortársaik előtti elismerés megszerzése határozza meg.

Képesek egy weboldal működésének megzavarására vagy egy egyszerű informatikai rendszer kompromittálására. Az internetes közösségekben megszerezhető hírnév és elismerés sok esetben fontosabb motivációt jelent számukra, mint a közvetlen pénzügyi haszon.

A script kiddie-khez köthető támadások:

- Brute Force támadások
  - Password Guessing - jelszópróbálgatás
  - Password Cracking - Jelszó-hash-ek feltörése, például Rainbow Table módszerrel, mely a jelszó-hash-ek feltörésének egyik klasszikus módszere
  - Password Spraying – a támadó egy vagy néhány gyakori jelszót próbál ki sok különböző felhasználói fiókkal szemben
  - Credential Stuffing - kiszivárgott hitelesítő adatok újrafelhasználása
- DoS és DDos támadások,
- weboldalak tartalmának módosítása (website defacement), valamint
- ismert sérülékenységek kihasználása.

Bár a script kiddie-k technikai felkészültsége általában elmarad a tapasztaltabb támadókétól, tevékenységüket nem érdemes lebecsülni. Az automatizált támadóeszközök alkalmazása lehetővé teszi számukra, hogy rövid idő alatt nagyszámú célpont ellen hajtsanak végre támadásokat. Egy rosszul konfigurált kisvállalati szerver, egy elavult webalkalmazás vagy egy nem megfelelő védelemmel ellátott otthoni hálózat fokozottan ki van téve támadásaiknak.

A Matrix néven ismert támadássorozat során egy támadó IoT-eszközök ismert sérülékenységeit, gyenge hitelesítési adatait és hibás konfigurációit kihasználva botnetet épített ki, amelyet DDoS-támadások indítására használt. A könnyen hozzáférhető támadási eszközök és nyilvánosan elérhető szkriptek a korlátozott technikai tudással rendelkező támadók számára is lehetővé tehetik összetett támadási műveletek végrehajtását.

A script kiddie-k elleni védekezés alapja a rendszeres biztonsági frissítések telepítése, a sérülékenységek folyamatos kezelése, az erős hitelesítési mechanizmusok alkalmazása, a tűzfalak, IDS és IPS rendszerek használata, valamint a naplóállományok rendszeres elemzése.

Magányos kiberbűnözők

A „Lone Hackers” vagy „Independent Cybercriminals” csoport tagjai már jelentősen magasabb szintű technikai felkészültséggel rendelkeznek, és képesek önállóan megtervezni, előkészíteni és végrehajtani különböző kibertámadásokat. Gyakran saját programokat fejlesztenek, módosítják a meglévő támadóeszközöket, illetve képesek azonosítására és kihasználására is.

Elsődleges motivációjuk a pénzügyi haszonszerzés. Célpontjaik rendkívül változatosak lehetnek, például kis- és középvállalkozások, online kereskedelmi rendszerek, pénzügyi szolgáltatók vagy magánszemélyek. A támadások során megszerzett adatok, például felhasználói fiókok, bankkártyaadatok, személyes információk vagy vállalati dokumentumok jelentős értéket képviselnek az illegális online piactereken.

A támadásaik során alkalmazott módszereik kifinomultabbak. Például alkalmaznak:

- adathalász támadásokat (phishing),
- célzott adathalász kampányokat (spear phishing),
- hitelesítési adatok megszerzésére irányuló módszereket,
- webalkalmazások sérülékenységeinek kihasználását (például SQL vagy XSS), valamint
- különböző rosszindulatú programokat (malware).

A zsarolóvírusok (ransomware) alkalmazása az elmúlt években a kiberbűnözés egyik meghatározó trendjévé vált, és továbbra is a szervezeteket fenyegető egyik legsúlyosabb kiberbiztonsági kockázatok között szerepel. A zsarolóvírusok alkalmazása során a támadók titkosítják az áldozat adatait, majd váltságdíjat követelnek azok visszaállításáért. Bár a nagyszabású zsarolóvírus-kampányokat

jellemzően a szervezett kiberbűnözői csoportok hajtják végre, kisebb volumenű támadásokra egyéni elkövetők is képesek.

Az anonimitás fenntartása, illetve a tevékenységük nyomon követhetőségének csökkentése érdekében titkosított kommunikációs csatornákat, anonim hálózatokat (Tor), valamint kriptovalutákat használnak a pénzügyi tranzakciók lebonyolítására.

A kiberbűnözés egyik sajátossága, hogy az ellopott adatoknak önmagukban is piaci értékük van. A magányos kiberbűnözők a megszerzett információkat saját felhasználás mellett akár a darkweb piacterein is értékesítheik. Ezeken a platformokon személyes adatok, hitelkártya-információk, bejelentkezési adatok, vállalati hozzáférések vagy akár teljes adatbázisok is megvásárolhatók.

A finn Vastaamo pszichoterápiás szolgáltató feltörését egy magányosan tevékenykedő kiberbűnöző követte el, akit a bíróság szerint pénzügyi haszonszerzés motivált. Kivimäki először a vállalatot, majd több ezer beteget is megzsarolt, miközben mintegy 33 ezer páciens érzékeny adataihoz jutott hozzá.

Az ellenük való védekezés a megfelelő szervezeti intézkedések mellett a felhasználók biztonságtudatosságára épül. Ennek részeként a fejlett végpontvédelmi megoldások, a többtényezős hitelesítés (MFA), a hálózati forgalom monitorozása, a rendszeres sérülékenységvizsgálatok és a biztonságtudatos felhasználói magatartás egyaránt hozzájárulnak a fenyegetések kockázatának csökkentéséhez. Mivel a támadók gyakran a felhasználók figyelmetlenségét vagy bizalmát használják ki, kiemelt jelentősége van a rendszeres információbiztonsági képzéseknek és az adathalász támadások felismerésére irányuló tudatosító előadásoknak.

Szervezett kiberbűnözői csoportok

A fekete kalapos hackerek hierarchiájának következő szintjét a szervezett kiberbűnözői csoportok (Organized Cybercrime Groups) alkotják. Alkothatnak nemzetközi hálózatokat, amelyek elsődleges célja a jelentős pénzügyi haszonszerzés. Jól szervezett működés, egyértelműen meghatározott feladatkörök, jelentős pénzügyi erőforrások és hosszú távú működési stratégia jellemzi.

A szervezett kiberbűnözői csoportok egyik legfontosabb sajátossága a munkamegosztás. Ezekben a szervezetekben a különböző feladatokat eltérő szakterületekre specializálódott személyek végzik. Míg egyes tagok kizárólag rosszindulatú szoftverek fejlesztésével foglalkoznak, addig mások a célpontok felderítésére, a rendszerekbe történő behatolásra, az ellopott adatok értékesítésére vagy a pénzügyi tranzakciók lebonyolítására szakosodnak. Ezáltal jelentősen növelik a támadásaik hatékonyságát.

A szervezett kiberbűnözésre jellemző a Cybercrime-as-a-Service (CaaS) modell. A szolgáltatásként kínált kiberbűnözés lehetővé teszi, hogy a támadók kész eszközökhöz, infrastruktúrához és szolgáltatásokhoz férjenek hozzá anélkül, hogy saját fejlesztési vagy technikai háttérrel rendelkeznének. Ennek legelterjedtebb formái a következők:

- Ransomware-as-a-Service (RaaS)
- Phishing-as-a-Service (PhaaS)
- Malware-as-a-Service (MaaS)

Célpontjaik elsősorban olyan szervezetek, amelyek jelentős pénzügyi erőforrásokkal vagy jelentős mennyiségű érzékeny adattal rendelkeznek (például pénzügyi intézmények, egészségügyi szolgáltatók, energetikai vállalatok, ipari termelőcégek, logisztikai vállalatok, oktatási intézmények, valamint a kritikus infrastruktúrát működtető szervezetek).

A támadók módszerei folyamatosan fejlődnek. A támadók által alkalmazott technikák közé tartoznak:

- célzott adathalász kampányok (Spear Phishing),
- üzleti e-mail kompromittáció (Business Email Compromise, BEC),
- zsarolóvírusok,
- távoli hozzáférést biztosító kártevők (Remote Access Trojan, RAT),
- ellátási láncot érintő támadásokat (Supply Chain Attack), valamint
- még nem ismert sérülékenységek kihasználása (Zero-day Exploits).

A támadások előkészítése során a támadók részletes információkat gyűjtenek a célpont informatikai infrastruktúrájáról, alkalmazott technológiáiról és szervezeti működéséről.

A LockBit, a zsarolóvírus-szolgáltatásra (RaaS) épülő kiberbűnözői csoportok között vált ismertté, amelyhez több mint 2000 áldozatot és 120 millió dollárt meghaladó váltságdíjbevételt kapcsoltak. A csoport elleni nemzetközi Operation Cronos művelet során szervereket és kriptotárcákat foglaltak le, valamint több mint ezer dekódoló kulcsot szereztek vissza.

A szervezett kiberbűnözői csoportok elleni védekezés jelentős kihívást jelent a szervezetek számára. A hagyományos biztonsági intézkedések, mint például a vírusvédelem vagy a tűzfalak önmagukban sokszor nem bizonyulnak elegendőnek. A korszerű védekezés több rétegből álló biztonsági architektúrát igényel, amely magában foglalja

a folyamatos sérülékenység-kezelést, a többtényezős hitelesítést, a hálózati forgalom valós idejű monitorozását, az események elemzését (SIEM), a végpontvédelmi megoldásokat, valamint a rendszeres biztonságtudatossági képzéseket. Emellett kiemelt jelentőséggel bír a nemzetközi bűnüldöző szervezetek és a nemzeti kiberbiztonsági szervek közötti együttműködés.

APT-csoportok

Az Advanced Persistent Threat (APT) csoportok a fekete kalapos hackerek hierarchiájának legmagasabb szintjét képviselik. Az APT elnevezés a csoportok fejlett technikai képességeire, a kompromittált rendszerekben való tartós és rejtett jelenlétére, valamint az általuk hordozott súlyos nemzetbiztonsági és gazdasági kockázatra utal. Az APT-csoportok elsődleges céljai:

- stratégiai jelentőségű információk megszerzése,
- geopolitikai érdekek érvényesítése,
- ipari kémkedés, valamint
- kritikus infrastruktúrák befolyásolása vagy működésének megzavarása.

Az APT-csoportok működésének egyik legfontosabb sajátossága a célzott támadási stratégia. Az államilag támogatott kiberműveletek jól szervezett, több egymásra épülő szakaszból állnak. A támadásokat gyakran megelőzi a célpont felderítése, amelynek során a támadók információkat gyűjthetnek az érintett szervezet informatikai infrastruktúrájáról, alkalmazott technológiáiról, munkatársairól és szervezeti felépítéséről. A megszerzett információk alapján többféle úton kísérelhetik meg a kezdeti hozzáférés megszerzését (Initial Access), például célzott adathalászattal, internet felől elérhető sérülékeny rendszerek kihasználásával vagy

az ellátási lánc valamely elemének kompromittálásával. A tartós hozzáférés fenntartása érdekében perzisztenciát is kialakíthatnak, így egyes hozzáférési pontok megszüntetése esetén is folytathatják tevékenységüket. A kompromittált környezetben végzett oldalirányú mozgás (Lateral Movement) szintén gyakori lehet, de nem minden támadóműveletben figyelhető meg. A támadók alkalmazhatnak Living off the Land (LotL) technikákat, vagyis a célrendszer legitim eszközeit és szolgáltatásait használják fel rosszindulatú műveleteik végrehajtására.

Az APT-csoportok támadási eszköztárát jellemzően az alábbi technikák alkotják:

- zero-day sérülékenységek kihasználása,
- egyedi fejlesztésű kártevők alkalmazása,
- ellátásilánc-támadások (Supply Chain Attack)
- fejlett titkosítási és rejtőzködési technikák alkalmazása,
- többlépcsős támadási láncok használata.

Az APT-csoportok fejlett technikai képességeik, jelentős erőforrásaik és stratégiai céljaik miatt különösen komoly kiberbiztonsági kihívást jelentenek. Tevékenységük egyik sajátossága, hogy a kompromittált rendszerekben hosszú időn keresztül képesek észrevétlenül jelen maradni. A Mandiant M-Trends 2026 jelentése szerint 2025-ben a kiberkémkedési incidensek esetében a medián jelenléti idő 122 nap volt, szemben a globális 14 napos mediánnal.

Számos korábbi támadási kampány szemlélteti, hogy milyen módszereket és eszközöket alkalmaznak a támadásaik során. Például a Kínához köthető APT40 kiberkémkedési célból több ország kormányzati és kritikus infrastruktúrához kapcsolódó szervezetét vette

célba. Hasonlóan járt el a Mustang Panda, amely indiai kormányzati hálózatok és az energiaipar, ezen belül a vízenergia-szektor ellen indított célzott műveleteket. Az orosz kötődésű APT28 pedig egy kampány során 13 ország, köztük Magyarország szervezeteit támadta. A 2022-ben Ukrajnát célzó „Viasat hack" kibertámadást orosz állami hátterű támadói csoporthoz, a Sandwormhoz (APT44) kapcsolják. Az APT-csoportok tevékenysége több országot érintő, geopolitikai célokat követő műveletekben is megjelenhet.

Az APT-csoportok elleni védekezés összetett, többrétegű megközelítést igényel, amely magában foglalja a megelőző, felderítő és reagáló intézkedéseket. A védekezés fontos része a sérülékenységek azonosítása és mielőbbi javítása, a hálózati infrastruktúra megfelelő szegmentálása, valamint a hozzáférések szigorú szabályozása és a többtényezős hitelesítés alkalmazása. Mindezek mellett a munkatársak biztonságtudatosságának fejlesztése és a rendszeres kiberbiztonsági incidenskezelési gyakorlatok is nélkülözhetetlenek.

Az APT csoportok tevékenységéről bővebben A magyar energiaszektor kiberbiztonsági fenyegetettségei c., A FrostyNeighbor fenyegető csoport elemzése c., illetve Az Ukrajnát célzó „Viasat-hack" hatása Európában c. CTI jelentésekben olvashatunk.

Hacktivista csoportok

A hacktivisták (Hacktivists) a fekete kalapos hackerek egyik sajátos csoportját alkotják. A hacktivizmus (hacktivism) a „hacking" és az „aktivizmus" szavak összevonásából kialakult fogalom, amely olyan kibertérben végrehajtott tevékenységeket jelöl, amelyek célja politikai, társadalmi vagy ideológiai célok támogatása, a közvélemény figyelmének felkeltése, illetve egy szervezet, vállalat vagy állami intézmény elleni tiltakozás kifejezése.

Célpontjaik lehetnek kormányzati szervek, politikai pártok, multinacionális vállalatok, pénzügyi intézmények, nemzetközi szervezetek, valamint olyan intézmények, amelyek működését saját értékrendjük alapján kifogásolhatónak tartják.

A hacktivisták által alkalmazott támadási módszerek elsősorban a nyilvánosság figyelmének felkeltésére irányulnak. Az egyik legelterjedtebb támadási forma a DDoS, amely során nagyszámú, különböző forrásból érkező eszköz egyidejű kérésekkel terheli túl a célrendszert, így annak szolgáltatásai átmenetileg elérhetetlenné válhatnak.

Szintén gyakori eszköz a website defacement, amelynek során a támadók megváltoztatják egy szervezet hivatalos honlapját, és saját politikai vagy ideológiai üzenetüket jelenítik meg rajtuk. A 2024 januárjában a Demokratikus Koalíció újpesti szervezetének honlapját ért támadás során a támadó jogosulatlanul módosította az oldal tartalmát, és saját üzenetét, valamint egy román zászlót helyezett el rajta.

Egy másik elterjedt módszer a megszerzett adatok kiszivárogtatása és nyilvánosságra hozatala, amely során bizalmas dokumentumokat vagy belső kommunikációt hoznak nyilvánosságra annak érdekében, hogy kellemetlen helyzetbe hozzák célpontjukat, vagy bizonyítékot szolgáltassanak vélt vagy valós visszaélésekre.

A hacktivista csoportok szervezeti felépítése általában lazább, mint a szervezett kiberbűnözői hálózatoké. Sok esetben nincs állandó vezetőjük vagy formális hierarchiájuk. A résztvevők különböző online platformokon, fórumokon vagy titkosított kommunikációs csatornákon keresztül szervezik tevékenységüket, és gyakran csak egy-egy konkrét akció idejére működnek együtt. Ez a működési modell

jelentősen megnehezíti a bűnüldöző szervek számára az egyes tagok azonosítását és felelősségre vonását. A legismertebb és legnagyobb nemzetközi figyelmet kapott hacktivista mozgalom egyike az Anonymous.

Az Oroszországot támogató hacktivistákhoz (Passion, Anonymous Russia) köthető csoportok európai és amerikai kórházak, valamint az Európai Parlament weboldala ellen is indítottak DDoS-támadásokat. Hacktivista csoportokhoz köthető kibertámadás érte továbbá a 2023-as cseh elnökválasztást, míg a 2026-os téli olimpia digitális infrastruktúráját is célozták.

Insider támadók

Az insider támadók azok a személyek, akik a szervezet informatikai rendszereihez, adataihoz vagy más erőforrásaihoz már eleve rendelkeznek valamilyen jogosultsággal. Nem feltétlenül kívülről, technikai eszközökkel próbálnak behatolni a rendszerbe. Éppen az teszi veszélyessé őket, hogy munkájukból, szerződéses kapcsolatukból vagy korábbi jogosultságaikból adódóan már rendelkezhetnek a támadás végrehajtásához szükséges hozzáféréssel.

Az insider támadásnak többféle formája lehet. A rosszindulatú belső támadó szándékosan él vissza jogosultságaival saját vagy más személy javára, például bizalmas adatok megszerzése, üzleti titkok eltulajdonítása, rendszerek jogosulatlan módosítása vagy anyagi haszonszerzés céljából. Előfordulhat, hogy egy munkavállaló elégedetlenségből vagy bosszúból okoz kárt, más esetekben pedig külső támadók szervezik be, befolyásolják vagy fizetik le, és rajta keresztül jutnak hozzá a szervezet erőforrásaihoz.

Az insider támadások kockázata nem kizárólag a szándékos

károkozásokból ered. Gondatlan vagy figyelmetlen felhasználó is okozhat kiberbiztonsági incidenst, például ha érzékeny adatokat téves címzettnek küldd el, nem megfelelően kezeli azokat, vagy egy adathalász támadás során megadja hitelesítő adatait. Ezek ezt követően illetéktelen személyek kezébe kerülhetnek és jogosulatlan hozzáférésre használhatók fel.

Az insider támadásokra jellemző, hogy a támadó legitim felhasználói jogosultságokkal rendelkezhet, ezért tevékenységét nehezebb megkülönböztetni a normál munkavégzéstől. A kockázat csökkentésében fontos szerepet kap a legkisebb jogosultság elvének alkalmazása, a hozzáférések rendszeres felülvizsgálata, a kiemelt jogosultságok ellenőrzése, valamint a naplózás és a gyanús tevékenységek felismerése. Különösen fontos a korábbi munkavállalók és külső közreműködők hozzáféréseinek visszavonása is.

Erre példa az Apple egyik korábbi alkalmazottjának esete is. A vállalat szerint a volt mérnök egy hitelesítési hiba kihasználásával, valamint egy másik alkalmazott felhasználói fiókjával visszaélve jutott hozzá több ezer bizalmas dokumentumhoz, köztük még be nem jelentett termékek műszaki anyagaihoz.

Az insider egy olyan személy, aki a szervezeten belül legitim hozzáférését felhasználva vesz részt egy támadásban vagy okoz biztonsági incidenst.



Szürke kalapos hackerek

A szürke kalapos hackerek (Gray Hat Hackers) a fehér és a fekete kalapos hackerek közötti átmeneti kategóriát jelentik. Tevékenységeik hátterében nem áll károkozási vagy anyagi haszonszerzési szándék, de módszereik gyakran sértik a jogszabályokat vagy az adott rendszer használatának feltételeit.

A szürke kalapos hackerek tevékenységére magyar példát is találunk. 2017-ben egy fiatal programozó biztonsági rést fedezett fel a Magyar Telekom informatikai rendszerében, amelyről tájékoztatta is a vállalatot. A rendszer további, engedély nélküli tesztelése miatt azonban a Telekom feljelentést tett, és az ügy büntetőeljáráshoz vezetett. A bíróság 2019-ben 600 ezer forint pénzbüntetést szabott ki rá. Az eset tanulsága, hogy a sérülékenység feltárásának célja nem feltétlenül károkozás, ugyanakkor a vizsgálatot a hacker nem a tulajdonos kifejezett engedélyével végezte, így tevékenysége jogi és etikai szempontból is túlmutatott az etikus hackelés keretein.

A szürke kalapos hackerek legfontosabb sajátossága, hogy engedély nélkül vizsgálják mások informatikai rendszereit sebezhetőségek után kutatva. A sérülékenységek felderítését jellemzően azért végzik, hogy felhívják a figyelmet egy problémára, illetve hozzájáruljanak annak kijavításához.

A szürke kalapos hackerek motivációja rendkívül változatos lehet. A leggyakoribb célok közé tartozik:

- a kíváncsiság és a szakmai kihívások,
- a sebezhetőségek azonosítása és javításának segítése,
- szakmai elismerés,
- pénzbeli jutalom vagy a Bug Bounty díjazás.

A Bug Bounty program egy olyan kezdeményezés, amelynek során vállalatok vagy szervezetek pénzbeli jutalmat (vagy egyéb elismerést) kínálnak etikus hackereknek, más néven „bug huntereknek” azokért a felfedezett sérülékenységekért, amelyeket a cég rendszereiben, szoftvereiben vagy webalkalmazásaiban találnak. A cél az, hogy a sebezhetőségeket még azelőtt azonosítsák és kijavítsák, mielőtt rosszindulatú támadók kihasználnák őket.

A szürke kalapos hackerek által alkalmazott technikák nagyrészt megegyeznek az etikus hackerek által használt módszerekkel. A fő különbséget azonban az jelenti, hogy a tevékenység a rendszer tulajdonosának előzetes engedélyével történik-e. Munkájuk során sérülékenységvizsgálatokat, hálózati felderítést, portszkennelést, webalkalmazások elemzését, konfigurációs hibák feltárását és különböző penetrációs technikákat alkalmazhatnak. A sérülékenységek feltárását követően a szürke kalapos hackerek jellemzően háromféleképpen járhatnak el:

a) Értesítik a rendszer tulajdonosát, és lehetőséget biztosítanak számára a hiba kijavítására.

b) Nyilvánosságra hozzák a sérülékenységet, amennyiben úgy ítélik meg, hogy a szervezet nem reagált megfelelően. Ez különösen kockázatos, mivel a nyilvánosságra került technikai részleteket rosszindulatú támadók is felhasználhatják a sérülékenység kihasználására.

c) Bejelentik a sérülékenységet, amennyiben az adott szervezet ilyen lehetőséget biztosít.

A szürke kalapos hackerek tevékenységére több példa is található, köztük olyan esetek, amikor biztonsági kutatók a sérülékenységek

felfedezése után nem a felelős közzététel szabályait követik. 2026-ban több kutató, köztük a Nightmare Eclipse néven publikáló szakember és az Ammar Askar is, javítás vagy a gyártóval való egyeztetés előtt hozott nyilvánosságra nulladik napi sérülékenységeket és működő PoC-kódokat, részben a Microsoft sérülékenységkezelési gyakorlatával kapcsolatos elégedetlenségük miatt.

A kiberbiztonságban egyre nagyobb jelentőséget kap a felelős sérülékenységközlés (Responsible Disclosure), vagy a koordinált sérülékenységközlés (Coordinated Vulnerability Disclosure, CVD). Ennek során a sérülékenységet felfedező kutató először bizalmasan értesíti az érintett szervezetet, és megfelelő időt biztosít a hiba kijavítására, mielőtt annak részletei nyilvánosságra hozná.

Zöld kalapos hackerek

A zöld kalapos hackerek (Green Hat Hacker) jellemzően a kiberbiztonság és a hackelés területén tapasztalatot szerző kezdő vagy autodidakta módon tanuló személyek. Technikai felkészültségük még korlátozott, viszont nagyon motiváltak a tanulást illetően. Céljuk elsősorban a szükséges ismeretek megszerzése és a kiberbiztonság különböző területein való fejlődés. Érdeklődésük középpontjában általában a számítógépes hálózatok működése, az operációs rendszerek felépítése, valamint a programozási nyelvek megismerése áll. A zöld kalapos hackerek motivációja elsősorban a tanulás és a szakmai fejlődés mellett:

- az informatikai rendszerek működésének megértése,
- a programozási és hálózatbiztonsági ismeretek fejlesztése,
- új technológiák megismerése.

A zöld kalapos hackerek nem feltétlenül rosszindulatúak, azonban tapasztalatuk hiánya miatt nem mindig mérik fel megfelelően tevékenységük következményeit. Ezért a gyakorlati tudás megszerzése szempontjából különösen fontos az ellenőrzött, jogszerű környezet, például a kiberbiztonsági laborok és a Capture The Flag (CTF) versenyek, mint például a HCSC verseny.

A Hungarian Cyber Security Challenge (HCSC) a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ-NKI) által szervezett kiberbiztonsági verseny, melynek célja a hazai tehetségek felkutatása, a kiberbiztonsági közösség építése és az utánpótlás nevelése. A megmérettetésen CTF és forensic image jellegű feladatokat kell megoldani egy dedikált platformon. Ezek a környezetek valós rendszereket modelleznek, ugyanakkor a gyakorlás kizárólag ellenőrzött, jogszerű környezetben történik. Fontos megjegyezni, hogy a verseny lebonyolítását biztosító infrastruktúra ellen irányuló, a feladatok keretein túlmutató jogosulatlan támadások büntetőjogi felelősségre vonást eredményezhetnek A verseny kvalifikációs lehetőséget jelent az Európai Kiberbiztonsági Versenyre (ECSC) is.

A zöld kalapos jelző elsősorban a technikai tapasztalat és a szakmai fejlődés szempontjából értelmezhető, és önmagában nem határozza meg az adott személy későbbi tevékenységének jogszerűségét vagy motivációját.



Kék kalapos hackerek

A kék kalapos hacker (Blue Hat Hacker) a hackerek kategorizálásának egyik kevésbé egységesen használt fogalma. Olyan külső biztonsági szakembert jelöl, akit egy szervezet azért kér fel, hogy egy informatikai rendszer vagy alkalmazás biztonságát még annak bevezetése előtt, vagy jelentősebb módosítását követően vizsgálja. A cél a sérülékenységek azonosítása, hogy azokat még az éles környezetben történő használat előtt ki lehessen javítani. A biztonsági vizsgálat kiterjedhet:

- webalkalmazások és API-k biztonsági tesztelésére,
- mobilalkalmazások biztonsági vizsgálatára,
- hálózati és infrastruktúra-elemek ellenőrzésére,
- hitelesítési és hozzáférés-vezérlési mechanizmusok vizsgálatára,
- konfigurációk ellenőrzésére,
- jogosultságkezelési hibák feltárására,
- ismert sérülékenységek és egyéb hiányosságok azonosítására.

A tevékenység az etikus hackeléshez áll közel, és megfelelő felhatalmazás mellett, meghatározott hatókörben történik. A kék kalapos hackerek jellemzően nem vesznek részt az adott rendszer fejlesztésében, ők általában külső, független szakemberek.

A Blue Hat és a Blue Team közötti különbség

A kék kalapos hacker fogalma nem egyenlő a Blue Team-mel. A Blue Hat elsősorban a külső, engedéllyel végzett vizsgálatokhoz kapcsolódó, nem teljesen egységesen definiált elnevezés, míg a Blue Team a szervezet informatikai rendszereinek folyamatos védelméért, a fenyegetések észleléséért és az incidensekre történő

reagálásért felelős védelmi szerepkör. A Blue Team olyan területeket foglal magában, mint:

- a kiberbiztonsági események folyamatos monitorozása,
- napló- és riasztási adatok elemzése,
- gyanús tevékenységek és támadási kísérletek azonosítása,
- incidensek kivizsgálása és kezelése,
- fenyegetésvadászat (Threat Hunting),
- kártevők és támadási módszerek elemzése,
- a védelmi intézkedések és észlelési szabályok fejlesztése,
- incidensek utáni helyreállítás és a védelem megerősítése.

Ezek a feladatok gyakran Security Operations Center (SOC) keretében valósulnak meg. A szervezetek kiberbiztonsági védelmét gyakran a SOC támogatja, azonban önálló SOC működtetése elsősorban a nagyobb méretű vagy magasabb kockázatú szervezetekre jellemző, míg a Blue Team tágabb védelmi szerepkört takar.

A Blue Team működésében olyan technológiák játszhatnak szerepet, mint a SIEM, a végpontészlelés és -reagálási megoldások (Endpoint Detection and Response, EDR), a hálózatbiztonsági eszközök, valamint a fenyegetési információk (Threat Intelligence).



Piros kalapos hackerek

A fogalom többféle értelmezésben jelenik meg, de olyan szereplőkre használják, akik technikai ismereteiket a rosszindulatú kibertevékenységek megzavarására és a támadók elleni aktív fellépésre használják. A red hat hackerek tevékenysége egyes esetekben a támadók tevékenységének megszakítására vagy az általuk használt infrastruktúra működésének megzavarására is irányulhat.

A piros kalapos hackerek tevékenységét gyakran hozzák összefüggésbe az úgynevezett hack back, vagyis visszatámadás koncepciójával. A hack back olyan ellenlépést jelent, amelynek során egy kibertámadás célpontja vagy annak megbízottja a hagyományos védekezésen túlmenően megpróbál fellépni a támadóval, illetve az általa használt infrastruktúrával szemben.

A red hat hackerek elsődleges motivációját általában a rosszindulatú kibertevékenységek visszaszorítása és a kiberfenyegetések elhárítása jelenti. Tevékenységük mögött állhat a kiberbűnözői infrastruktúrák működésének megzavarására, a támadások megakadályozására vagy a további károkozás mérséklésére irányuló szándék.

A támadók elleni fellépés célja önmagában nem teszi jogszerűvé az alkalmazott módszereket. Az engedély nélküli rendszerekhez való hozzáférés, azok módosítása vagy működésük szándékos megzavarása jogi következményekkel járhat.

A red hat hackerekhez tevékenységei:

- kiberbűnözői infrastruktúrák felderítése és azonosítása;
- támadási infrastruktúrák működésének megzavarására irányuló kísérletek;
- botnetek működésének akadályozása;

- kártevők kommunikációjának és vezérlési infrastruktúrájának vizsgálata;
- kompromittált rendszerek elemzése;
- a támadásokhoz használt infrastruktúra feltérképezése.

A tevékenységük egy része túlmutathat a hagyományos, passzív vagy aktív védekezésen. A támadó infrastruktúrájának jogosulatlan elérése vagy működésének szándékos megzavarása ezért jogi és etikai szempontból is vitatható lehet. A red hat hackerek tevékenységét gyakran a kiberbiztonság egyik határterületeként, illetve bizonyos értelmezésekben a cyber vigilantism (kiberönbíráskodás jellegű kibertevékenység) körébe sorolják.

A Red Hat és a Red Team közötti különbség

A Red Hat Hackers és a Red Team fogalma nem azonos. A red hat hacker egy nem egységesen definiált hacker-kategória, amelyhez egyes értelmezésekben a támadók elleni aktív fellépést jelenti. Ezzel szemben a Red Team egy szervezeti és biztonsági tesztelési szerepkör, amelynek célja egy szervezet védelmi képességeinek ellenőrzése.

A Red Team a szervezet megbízásából, előre meghatározott hatókörben és engedélyezett keretek között valós támadási technikákat szimulál annak érdekében, hogy feltárja a szervezet technikai és szervezeti biztonsági hiányosságait. A vizsgálat során a csapat támadói szemléletet követ, miközben tevékenységét szabályozott és dokumentált keretek között végzi.

A két fogalom közötti legfontosabb különbség az, hogy míg a Red Team előzetes felhatalmazás alapján, ellenőrzött környezetben végzi a biztonsági tesztelést, addig a red hat hackerekhez kapcsolt tevékenységek egyes értelmezések szerint a támadók ellen irányuló, akár engedély nélküli ellenlépéseket is magukban foglalhatnak.

A mesterséges intelligencia szerepe a kibertámadásokban

A mesterséges intelligencia (MI) fejlődése a kiberbiztonság területén a védekezési lehetőségek átalakítása mellette a kibertámadások eszköztárára és módszereire is jelentős hatással van. Az MI-alapú technológiák széles körű hozzáférhetősége egyes támadási műveletek automatizálását és személyre szabását is megkönnyítheti. Ennek következtében az MI egyre inkább olyan támogató technológiává válik, amelyet a kiberbűnözők a hagyományos eszközök mellett különböző támadási célokra is felhasználhatnak.

Az egyik alkalmazási terület a social engineering és az adathalászat. A generatív MI rövid idő alatt természetes nyelvezetű, nyelvtanilag pontos és a célponthoz igazított szövegek előállítására képes. Ez megkönnyítheti olyan adathalász e-mailek, üzenetek és egyéb megtévesztő kommunikációs tartalmak létrehozását, amelyek nehezebben különböztethetők meg a valódi üzenetektől. A korábbi, könnyen felismerhető nyelvi hibákat tartalmazó csaló levelekhez képest a generatív MI alkalmazásával meggyőzőbbé válhatnak a megtévesztő tartalmak, valamint nagyobb számú címzetthez is eljuttathatók.

Az MI alkalmazása a megtévesztés új formáinak megjelenéséhez is hozzájárult. A deepfake-technológia és a hangklónozás lehetővé teszi olyan valósághű hang- és videótartalmak előállítását, amelyek valós személyek hangját, arcvonásait vagy egyéb egyedi jellemzőit utánozzák. Ezek social engineering támadásokkal kombinálva alkalmasak lehetnek például egy vezető vagy munkatárs megszemélyesítésére. A cél a felhasználó döntésének befolyásolása és bizalmának elnyerése. Az ilyen támadások különösen

azért jelentenek komoly kihívást, mert a digitális kommunikációban egyre nehezebb kizárólag a hang vagy a kép alapján megállapítani, hogy a kommunikáló személy valóban az, akinek mondja magát.

A mesterséges intelligencia a rosszindulatú programok fejlesztésében és módosításában is szerepet kaphat. Az MI-alapú eszközök egyes esetekben támogatást nyújthatnak a kód létrehozásához, módosításához vagy elemzéséhez, ezáltal olyan feladatokat is megkönnyítve, amelyek korábban magasabb szintű programozási ismereteket igényeltek. Az OPSWAT szerint az MI-vel támogatott rosszindulatú programok képesek lehetnek alkalmazkodni a környezetükhöz, illetve nehezebben észlelhetők a hagyományos biztonsági rendszerek számára.

Az MI a támadások előkészítése során nagy mennyiségű nyilvánosan elérhető információ feldolgozásával támogathatja a célpontok feltérképezését, a releváns adatok rendszerezését és a lehetséges támadási felületek azonosítását. Ezáltal a korlátozott technikai tudással rendelkezők számára is alacsonyabbá válhat a kiberbűnözésbe való bekapcsolódás küszöbe. A komplexebb támadásokhoz szükséges szakértelem egy része így részben hozzáférhetővé válhat automatizált szolgáltatások formájában. Ez különösen a szolgáltatásként kínált kiberbűnözési modellek esetében lehet jelentős, ahol a technikai infrastruktúrát és egyes támadási képességeket a felhasználók szolgáltatásként vehetik igénybe.

A mesterséges intelligencia a kibertérben olyan eszköz, amelynek hatása elsősorban attól függ, hogy ki, milyen célból és milyen környezetben alkalmazza. A kiberbiztonság egyik kihívása, hogy a védelmi rendszerek milyen mértékben tudják kihasználni az MI képességeit, miközben kezelik azokat a kockázatokat is, amelyeket ugyanez a technológia a támadók számára is előteremt.

Összegzés

A hackerek tevékenysége szorosan kapcsolódik a számítástechnika és az informatikai rendszerek fejlődéséhez. A hacker fogalma az elmúlt évtizedekben jelentős változáson ment keresztül, a korai hackerközösségek tagjait elsősorban a technológia működésének mélyebb megértése, az innováció és a kreatív problémamegoldás motiválta. A fogalom napjainkban azonban összekapcsolódik a kiberbűnözéssel.

A hacker megnevezés a jogellenes vagy károkozó tevékenység mellett olyan személyt is jelölhet, aki magas szintű technikai ismeretekkel rendelkezik, és ezeket biztonsági vagy egyéb legitim célokra alkalmazza. Kiberbiztonsági szempontból ezért annak célja, alkalmazásának módja és jogszerűsége tekinthető meghatározónak.

A kiberbiztonság nem kizárólag technológiai kérdés, mivel a szervezetek biztonságát jelentős mértékben az emberi tényező is befolyásolja. Számos kibertámadás a felhasználók megtévesztésére, illetve az emberi hibák és a sérülékenységek kihasználására épít. Emiatt a megfelelő biztonságtudatosság a technológiai védelmi megoldásokkal együtt a szervezeti biztonság egyik fontos elemét képezi. A szervezeteknek ezért a technikai védelem mellett hangsúlyt kell fektetniük a munkatársak rendszeres kiberbiztonsági képzésére, a biztonságtudatos szervezeti kultúra kialakítására, valamint a hatékony és jól meghatározott incidenskezelési folyamatok fenntartására.

Napjaink egyik legjelentősebb kihívását a mesterséges intelligencia gyors fejlődése és széles körű alkalmazása jelenti. Az MI-alapú technológiák új lehetőségeket teremtenek a fenyegetések felismerésében, a biztonsági események elemzésében és a védekezési folyamatok támogatásában, ugyanakkor a támadók számára is lehetővé tehetik egyes műveletek automatizálását és hatékonyabb végrehajtását.



CTI elemzés NEMZETI KIBERBIZTONSÁGI INTÉZET

Források

Progmatic. (2023) *Mit csinál egy etikus hacker?* https://progmatic.hu/mit-csinal-egy-etikus-hacker/ (Letöltve: 2026. július 8.)

Promanconsulting. (2025) *Hogyan támogatják az etikus hackerek a kiberbiztonságot?* https://promanconsulting.hu/etikus-hacker/ (Letöltve: 2026. július 8.)

Pallas70. (2022) *Mit érdemes tudni a hackerekről?* https://pallas70.hu/kepzes-hirek/cikkek/mit-erdemes-tudni-a-hackerekrol (Letöltve: 2026. július 8.)

Ludovika. (2021) *„A kibertámadás nem olyan, mint egy kuruc portya" – 1. rész* https://www.ludovika.hu/magazin/aula/2021/07/16/a-kibertamadas-nem-olyan-mint-egy-kuruc-portya-1-resz/ (Letöltve: 2026. július 8.)

Cisco. (2026) *What is a hacker?* https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-hacker.html (Letöltve: 2026. július 8.)

Geeksforgeeks. (2026) *Hackers and Their Types* https://www.geeksforgeeks.org/what-is-a-hacker/ (Letöltve: 2026. július 8.)

Malwarebytes. (2026) *Hacker* https://www.malwarebytes.com/cybersecurity/basics/hacker (Letöltve: 2026. július 8.)

Huntress. (2025) *What is a Hacker?* https://www.huntress.com/cybersecurity-101/topic/hackers-defined (Letöltve: 2026. július 8.)

Utulsa. (2025) *5 Types of Hackers* https://online.utulsa.edu/blog/types-of-hackers/ (Letöltve: 2026. július 8.)

Kaspersky. (2026) *Black hat, White hat, and Gray hat hackers – Definition and Explanation* https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (Letöltve: 2026. július 8.)

Kaspersky. (2026) *What is hacking? And how to prevent it* https://www.kaspersky.com/resource-center/definitions/what-is-hacking (Letöltve: 2026. július 13.)

Kaspersky. (2026) *What is WannaCry ransomware?* https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (Letöltve: 2026. július 13.)

Kaspersky. (2026) *What is a Black-Hat hacker?* https://www.kaspersky.com/resource-center/threats/black-hat-hacker (Letöltve: 2026. július 13.)

Kaspersky. (2026) *Top 7 Mobile Security Threats* https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (Letöltve: 2026. július 13.)

Kaspersky. (2026) *Social Engineering – Definition* https://www.kaspersky.com/resource-center/threats/social-engineering-05-level (Letöltve: 2026. július 13.)

Kaspersky. (2026) *What Is Ransomware? How It Works and How to Protect Yourself* https://www.kaspersky.com/resource-center/threats/ransomware (Letöltve: 2026. július 13.)

Kaspersky. (2026) *Types of Malware* https://www.kaspersky.com/resource-center/threats/malware-classifications (Letöltve: 2026. július 13.)

Ibm. (2025) *What is ethical hacking?* https://www.ibm.com/think/topics/ethical-hacking (Letöltve: 2026. július 13.)

NKI. (2026) *Az internet sötét oldala* https://nki.gov.hu/it-biztonsag/elemzesek/az-internet-sotet-oldala/ (Letöltve: 2026. július 14.)

NKI. (2023) *APT csoportok* https://nki.gov.hu/it-biztonsag/elemzesek/apt_csoportok/ (Letöltve: 2026. július 14.)

NKI. (2023) *Adathalász csalások, visszaélések a bankok nevében* https://nki.gov.hu/it-biztonsag/elemzesek/adathalasz-csalasok-visszaelesek-a-bankok-neveben/ (Letöltve: 2026. július 14.)

NKI. (2022) *Adathalászat – a leghatékonyabb kiberfegyver* https://nki.gov.hu/it-biztonsag/elemzesek/adathalaszat-a-leghatekonyabb-kiberfegyver/ (Letöltve: 2026. július 14.)

NKI. (2022) *Az Ukrajnát célzó „Viasat-hack" hatása Európában* https://nki.gov.hu/it-biztonsag/elemzesek/az-ukrajnat-celzo-viasat-hack-hatasa-europaban/ (Letöltve: 2026. július 14.)

NKI. (2022) *Ransomware as a Service (RaaS) – Zsarolóvírus-szolgáltatás* https://nki.gov.hu/it-biztonsag/elemzesek/ransomware-as-a-service-raas-zsarolovirus-szolgaltatas/ (Letöltve: 2026. július 14.)

NKI. (2023) *Kulcs a digitális élethez – a biztonságos jelszókezelésről* https://nki.gov.hu/it-biztonsag/elemzesek/kulcs-a-digitalis-elethez-a-biztonsagos-jelszokezelesrol/ (Letöltve: 2026. július 14.)

Geeksforgeeks. (2025) *Difference between Hackers and Crackers* https://www.geeksforgeeks.org/computer-networks/difference-between-hackers-and-crackers/ (Letöltve: 2026. július 23.)

Ecpi. (2026) *What is Hacking and Cracking in Cybersecurity?* https://www.ecpi.edu/blog/what-is-hacking-and-cracking-in-cybersecurity (Letöltve: 2026. július 23.)

Insside. (2024) *Understanding crackers: what they are and how to protect your company* https://www.insside.net/en/crackers-hackers-what-are-they/ (Letöltve: 2026. július 23.)

Masterfield. (2026) *Lelőtte a vonat wifijét, a saját jelét rakta a helyére. 14 évesen feltörte a tanár gépét, mára már pedig világszinten elismert hekker. Ismerd meg a történetét!*

https://masterfield.hu/hu/hirek/1628-vilag-egyik-legjobb-hackere (Letöltve: 2026. július 23.)

Jc-cybersecurity. (2024) *Types of Hackers – The 6 Hats Explained* https://www.jc-cybersecurity.co.uk/types-of-hackers-the-6-hats-explained (Letöltve: 2026. július 23.)

Cymulate. (2026) *Red Team vs Blue Team vs Purple Team in Cybersecurity* https://cymulate.com/blog/red-blue-purple-team-in-cybersecurity/ (Letöltve: 2026. július 23.)

NKI. (2025) *Mi az a Ransomware-as-a-Service (RaaS)?* https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-ransomware-as-a-service-raas/ (Letöltve: 2026. július 23.)

NKI. (2025) *Mi az a Phishing-as-a-Service (PhaaS)?* https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-phishing-as-a-service-phaas/ (Letöltve: 2026. július 23.)

NKI. (2025) *Mi az a Malware-as-a-service (MaaS)?* https://nki.gov.hu/it-biztonsag/tudastar/mi-az-a-malware-as-a-service-maas/ (Letöltve: 2026. július 23.)

NKI. (2025) *Végpontvédelem és annak megvalósítása I. – Technológiai alapok és veszélyforrások* https://nki.gov.hu/it-biztonsag/elemzesek/vegpontvedelem-es-annak-megvalositasa-i-technologiai-alapok-es-veszelyforrasok/ (Letöltve: 2026. július 23.)

NKI. (2024) *A SIEM rendszerek működése* https://nki.gov.hu/it-biztonsag/elemzesek/a-siem-rendszerek-mukodese/ (Letöltve: 2026. július 23.)

NKI. (2025) *Végpontvédelem és annak megvalósítása II. – Szervezeti stratégia, oktatás és jövőálló biztonság* https://nki.gov.hu/it-biztonsag/elemzesek/vegpontvedelem-es-annak-megvalositasa-ii-szervezeti-strategia-oktatas-es-jovoallo-biztonsag/ (Letöltve: 2026. július 23.)

Hackerone. (2026) *Why You Need Responsible Disclosure and How to Get Started* https://www.hackerone.com/knowledge-center/why-you-need-responsible-disclosure-and-how-get-started (Letöltve: 2026. július 23.)

Itszotar. (2025) *Bug bounty program: a sérülékenységjutalmazó programok működése és célja* https://itszotar.hu/bug-bounty-program-a-serulekenysegjutalmazo-programok-mukodese-es-celja/ (Letöltve: 2026. július 23.)

Bankszovetseg. (2025) *Kibervédelmi fogalmak és értelmezésük* https://bankszovetseg.hu/Public/gep/2025/2025_3%20magyar/403-446%20-%20KovacsL_Tertak%20Kibervedelmi%20fogalmak.pdf (Letöltve: 2026. augusztus 10.)

Okta. (2026) *Ethical Hacking: What It Is & Examples* https://www.okta.com/identity-101/ethical-hacking/ (Letöltve: 2026. augusztus 10.)

Americantv. (2026) *Green Hat Hacker 2026* https://www.americantv.com/green-hat-hacker.php (Letöltve: 2026. augusztus 10.)

Zimperium. (2026) *Blue Hat Hacker* https://zimperium.com/glossary/blue-hat-hacker (Letöltve: 2026. augusztus 10.)

Promanconsulting. (2025) *Mindent a pentestről: A behatolásteszt folyamata és előnyei* https://promanconsulting.hu/pentest/ (Letöltve: 2026. augusztus 12.)

Promanconsulting. (2025) *Hogyan támogatják az etikus hackerek a kiberbiztonságot?* https://promanconsulting.hu/etikus-hacker/ (Letöltve: 2026. augusztus 12.)

Mitre. (2026) *Brute Force* https://attack.mitre.org/techniques/T1110/ (Letöltve: 2026. szeptember 4.)

Cloudflare. (2026) *What is credential stuffing?* https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/ (Letöltve: 2026. szeptember 4.)

Nist. (2008) *Technical Guide to Information Security Testing and Assessment* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (Letöltve: 2026. szeptember 4.)

Wstg. (2026) *OWASP Web Security Testing Guide* https://wstg.owasp.org/latest/1-About/ (Letöltve: 2026. szeptember 4.)

Enisa. (2025) *The ENISA Threat Landscape (ETL) report* https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape (Letöltve: 2026. szeptember 4.)

Telex. (2024) *Unatkozó tinédzser hekkelte meg a DK-t, és azt állítja, a párt egyik vezetőjét is* https://telex.hu/techtud/2024/01/30/dk-ujpest-honlap-weboldal-hekkertamadas-hekkeles-defacement-adatszivargas-emailcimek-elkoveto-hekker-interju (Letöltve: 2026. szeptember 4.)

NKI. (2026) *Zsarolóvírus-támadás érte a román ANCPI rendszerét* https://nki.gov.hu/it-biztonsag/hirek/zsarolovirus-tamadas-erte-a-roman-ancpi-rendszeret/ (Letöltve: 2026. szeptember 4.)

NKI. (2025) *Tájékoztatás a SECTOR 16 csoport magyar geotermikus rendszer elleni támadásával kapcsolatban* https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-sector-16-csoport-magyar-geotermikus-rendszer-elleni-tamadasaval-kapcsolatban/ (Letöltve: 2026. szeptember 4.)

HVG. (2019) *Pénzbüntetéssel megúszta az etikus hacker, aki szólt a Telekomnak, hogy óriási hiba van a rendszerében* https://hvg.hu/tudomany/20190711_etikus_hacker_magyar_telekom_biztonsagi_res (Letöltve: 2026. szeptember 4.)

Bdo. (2024) *A mesterséges intelligencia szerepe a kiberbiztonságban: hogyan észleljük és előzzük meg a támadásokat?* https://www.bdo.hu/hu-hu/aktualitasok-blog/blog/a-mesterseges-intelligencia-szerepe-a-kiberbiztonsagban-hogyan-eszleljuk-es-elozzuk-meg-a-tamadasok (Letöltve: 2026. szeptember 9.)

Tárkányi Edina – Németh Richárd. (2025) *A mesterséges intelligencia szerepe a social engineering támadások megelőzésében, Belügyi Szemle, Évf. 73 szám 8 1579-1597* https://belugyiszemlejournal.org/index.php/belugyiszemle/issue/view/183/202 (Letöltve: 2026. szeptember 9.)

Biztonsagpolitika. (2025) *Mesterséges intelligencia használata a kibervédelemben és kibertámadások során* https://biztonsagpolitika.hu/kiemelt/mesterseges-intelligencia-hasznalata-a-kibervedelemben-es-kibertamadasok-soran (Letöltve: 2026. szeptember 9.)

Opswat. (2025) *AI Hacking: Hogyan használják a hackerek a mesterséges intelligenciát a kibertámadásokban?* https://hungarian.opswat.com/blog/ai-hacking-how-hackers-use-artificial-intelligence-in-cyberattacks (Letöltve: 2026. szeptember 9.)

NKI. (2024) *A „script kiddie”-k nagyobb fenyegetést jelentenek, mint valaha* https://nki.gov.hu/it-biztonsag/hirek/a-script-kiddie-k-nagyobb-fenyegetest-jelentenek-mint-valaha/ (Letöltve: 2026. szeptember 10.)

Therecord. (2026) *Finland issues wanted notice for hacker behind massive psychotherapy data breach* https://therecord.media/finland-issues-wanted-notice-for-hacker-vastaamo-breach (Letöltve: 2026. szeptember 10.)

NKI. (2024) *Elkapták a LockBit két tagját, dekódoló érhető el!* https://nki.gov.hu/it-biztonsag/hirek/elkaptak-a-lockbit-ket-tagjat-dekodolo-erheto-el/ (Letöltve: 2026. szeptember 10.)

Google. (2026) *M-Trends 2026: Data, Insights, and Strategies From the Frontlines* https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026 (Letöltve: 2026. szeptember 10.)

NKI. (2026) *A FrostyNeighbor fenyegető csoport elemzése* https://nki.gov.hu/it-biztonsag/elemzesek/a-frostyneighbor-fenyegeto-csoport-elemzese/ (Letöltve: 2026. szeptember 10.)

NKI. (2023) *Az orosz APT28 hackerei 13 nemzetet vettek célba* https://nki.gov.hu/it-biztonsag/hirek/az-orosz-apt28-hackerei-13-nemzetet-vettek-celba/ (Letöltve: 2026. szeptember 10.)

NKI. (2026) *A Mustang Panda az indiai kormányt és az energiaipart vette célba* https://nki.gov.hu/it-biztonsag/hirek/a-mustang-panda-az-indiai-kormanyt-es-az-energiaipart-vette-celba/ (Letöltve: 2026. szeptember 10.)

NKI. (2024) *A kiberbiztonsági ügynökségek az APT40 támadásaira figyelmeztetnek* https://nki.gov.hu/it-biztonsag/hirek/a-kiberbiztonsagi-ugynoksegek-az-apt40-tamadasaira-figyelmeztetnek/ (Letöltve: 2026. szeptember 10.)

NKI. (2023) *DDoSaaS platfomok segítségével támadnak európai kórházakat* https://nki.gov.hu/it-biztonsag/hirek/ddos-as-a-service-platfomok-segitsegevel-tamadjak-a-korhazakat/ (Letöltve: 2026. szeptember 10.)

NKI. (2022) *Túlterheléses támadás érte az Európai Parlament weboldalát* https://nki.gov.hu/it-biztonsag/hirek/tulterheleses-tamadas-erte-az-europai-parlament-weboldalat/ (Letöltve: 2026. szeptember 10.)

NKI. (2026) *Kibertámadások kockázatai a 2026-os Téli Olimpia digitális ökoszisztémájában* https://nki.gov.hu/it-biztonsag/hirek/kibertamadasok-kockazatai-a-2026-os-teli-olimpia-digitalis-okoszisztemajaban/ (Letöltve: 2026. szeptember 10.)

NKI. (2023) *Kibertámadás érte a 2023-as cseh elnökválasztást* https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-erte-a-2023-as-cseh-elnokvalasztast/ (Letöltve: 2026. szeptember 10.)

NKI. (2022) *Céges sérülékenységi információkkal próbált pénzt keresni, fülön csípték a dolgozót* https://nki.gov.hu/it-biztonsag/hirek/belso-fenyegetes-%E2%94%80-a-kiberbiztonsagi-cegeknel-is-megtortenhet/ (Letöltve: 2026. szeptember 10.)

NKI. (2026) *Üzleti titkok ellopása miatt pert indított az Apple* https://nki.gov.hu/it-biztonsag/hirek/uzleti-titkok-ellopasa-miatt-pert-inditott-az-apple/ (Letöltve: 2026. szeptember 11.)

NKI. (2026) *Nightmare Eclipse hat Windows zero-dayje és a Microsoft-konfliktus* https://nki.gov.hu/it-biztonsag/hirek/nightmare-eclipse-hat-windows-zero-dayje-es-a-microsoft-konfliktus/ (Letöltve: 2026. szeptember 11.)

NKI. (2026) *VS Code nulladik napi sérülékenységet hozott nyilvánosságra egy kutató* https://nki.gov.hu/it-biztonsag/hirek/vs-code-nulladik-napi-serulekenyseget-hozott-nyilvanossagra-egy-kutato/ (Letöltve: 2026. szeptember 11.)

NKI. (2026) *Zero day sebezhetőséget is javít a Chrome biztonsági frissítése* https://nki.gov.hu/it-biztonsag/hirek/zero-day-sebezhetoseget-is-javit-a-chrome-biztonsagi-frissitese/ (Letöltve: 2026. szeptember 11.)

NKI. (2021) *Tanulj meg hackelni! – Felkészülés a HCSC-re* https://nki.gov.hu/it-biztonsag/tanacsok/tanulj-meg-hackelni-felkeszules-a-hcsc-re/ (Letöltve: 2026. szeptember 11.)

NKI. (2026) *Mi az a HCSC?* https://hcsc.nki.gov.hu/ (Letöltve: 2026. szeptember 11.)

NKI. (2026) *Rekordösszeg a Pwn2Own Berlin 2026-on: 47 zero-day hibáért 1,3 millió dollár járt* https://nki.gov.hu/it-biztonsag/hirek/rekordosszeg-a-pwn2own-berlin-2026-on-47-zero-day-hibaert-13-millio-dollar-jart/ (Letöltve: 2026. szeptember 11.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET



Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026