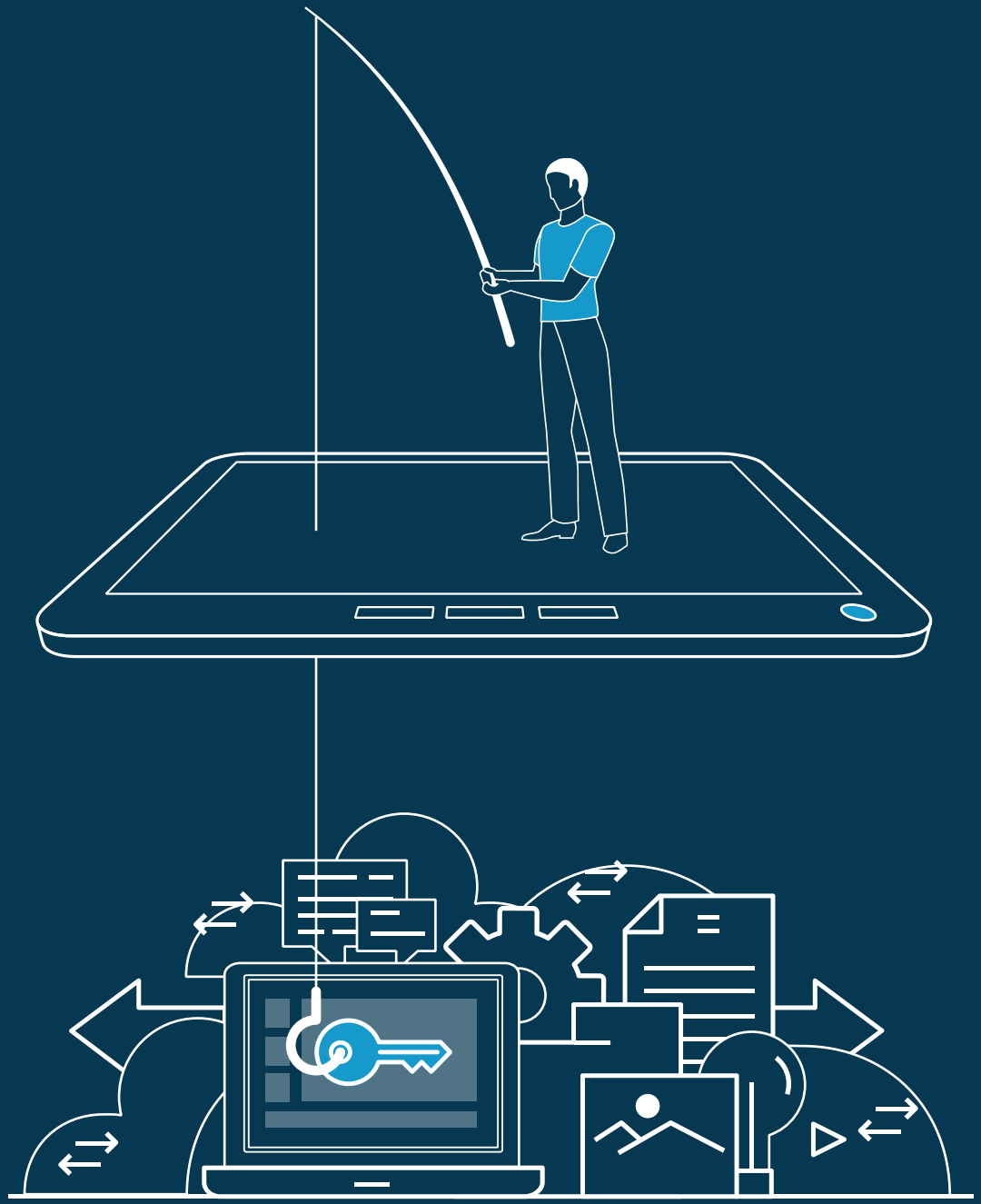


BALASYS

Hogyan védekezzünk a kiemelt felhasználói azonosító lopás ellen

Lehet, hogy a legnagyobb veszély már az Ön rendszerében van?

TARTALOM

Kiemelt felhasználói azonosító lopás

BEVEZETÉS

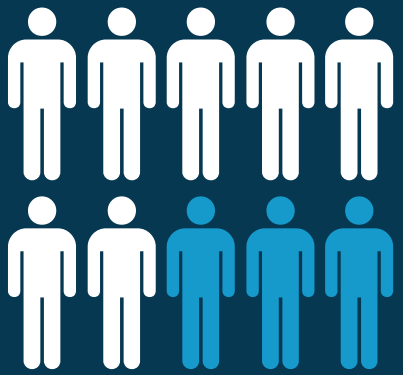
Mi a közös a 21. század tíz legnagyobb adatlopásában? A kiemelt személyazonosságlopásra, és a kiemelt felhasználói fiókok hitelesítési adataival való visszaélésre sokszor fény derült az óriás adatlopások utólagos vizsgálatában.[1] Ezen incidensek során, megfelelő erőforrásokkal rendelkező külső szereplők – néhányuk állami támogatással a háta mögött – törték fel kiemelt felhasználók magasabb jogosultságot biztosító fiókjait, például rendszergazdai vagy szolgáltatási fiókokat. Ez lehetővé tette számukra, hogy nagy mennyiségű adatot gyűjtsenek össze, majd lopjanak el.

Noha nehéz számszerűsíteni ezeknek a támadásoknak a hatását, több milliárd szenzitív adat érintett, mint például hitelkártya adatok, jelszavak, munkavállalói információk, egészségügyi nyilvántartások és még sok egyéb, hasonlóan érzékeny információ. Egy kiemelt felhasználó – aki hozzáfér adminisztrátori és szolgáltatási jelszavakhoz – fiókjának feltörésével a kiber bűnözők ipari méretekben képesek adatokat lopni. És ezek az óriási adatlopások még nem is tartalmazzák azokat a biztonsági incidenseket, amelyeket szabotázs céljából hajtottak végre stratégiai fontosságú rendszereken, mint például amilyen a 2015-ben és 2016-ban Ukrajnában bekövetkezett, a nemzeti energiahálózatot megcélzó támadás volt.

Ez a tanulmány rávilágít arra, hogy miért jelentenek nagy kockázatot a vállalkozásokra a kiemelt felhasználók, hogy a támadók hogyan használják ki a sérülékenységeket, hogy a jelenlegi módszerekkel miért nem sikerül megállítani ezeket a támadásokat, és végül, hogy az Ön szervezete hogyan védheti meg magát.

80%

A biztonsági incidensek 80%-ában kiemelt felhasználói fiókokhoz tartozó hitelesítési adatokat használtak.



7/10

A 10 legnagyobb adatlopás közül 7-ben kiemelt felhasználói fiókokhoz tartozó hitelesítési adatok voltak érintettek.

A PROBLÉMA NAGYSÁGA

A Forrester elemző cég szerint, a biztonsági incidensek 80%-ában kiemelt felhasználói fiókokhoz tartozó hitelesítési adatokat használtak.[2] Az alábbi táblázat az elmúlt évek néhány nagyobb adatlopásáról tartalmaz információkat. Ezek a célzott támadások, vagy APT (Advanced Persistent Threat) támadások tankönyvi példáinak számítanak, amelyekben az elkövetők egy nagyon konkrét cél érdekében támadtak.

Áldozat	Hatás
Yahoo	A Yahoo két adatlopást is bejelentett 2016-ban. A kiberbűnözők hozzá tudtak férni a cég felhasználói adatbázisához, és észrevétlenek maradtak közel két évig, amely végül 1,5 milliárd felhasználói fiók adatainak kiszivárgását eredményezte. Az FBI szerint egy „félig-kiemelt" státuszú Yahoo alkalmazotton keresztül sikerült beférkőzni a cégbe, pszichológiai manipuláció vagy spear phishing felhasználásával.[3] Az incidens eredményeképp a Yahoo értéke 350 millió dollárral csökkent, épp a Verizon általi felvásárlás közepette.[4]
eBay	„Hackerek megszerezték néhány alkalmazottunk bejelentkezéshez használt adatait, lehetővé téve az eBay belső hálózatához való engedély nélküli hozzáférést" – jelentette be 2014-ben az eBay. A cég mind a 145 millió felhasználóját felkérte jelszavának megváltoztatására, de semmilyen részletet nem közölt a támadásról, azonban tekintve annak méretét, és azt hogy a bejelentés, „néhány alkalmazottunk bejelentkezéshez használt adatai"-ról szólt, szakértői vélemények szerint a támadók kiemelt felhasználói fiókokhoz férhettek hozzá.
Target Stores	2013 decemberében a Target Stores nagymértékű adatlopást jelentett be. A támadók egy külsős alvállalkozó felhasználói fiókját törték fel, egy kis hűtéssel és légkondicionálókkal foglalkozó cég munkatársáét, akinek hozzáférése volt a Target belső hálózatához. Az elkövetőknek sikerült több szerverhez is hozzáférést szerezni, és végül malware-t telepíteni a Target POS (Point of Sale) termináljaira. Az eredmény? Százmillió vásárló bankkártya adatait lopták el. Az eset következményeként a Target CEO-ja lemondott; az incidenshez kapcsolódó költségek 292 millió dollárra rúgtak.[5]
JP Morgan Chase	2014 júliusában hackerek beférkőztek egy alkalmazott számítógépébe. Ebből a belépési pontból sikerült a legmagasabb adminisztrátori jogosultságot megszerezniük, majd több mint 90 szerver fölött átvették az irányítást. Az adatlopás 76 millió háztartás és 7 millió kisvállalkozás adatait érintette. [6]
US Office of Personnel Management (OPM)	Az OPM incidens 2012-ben kezdődött, de csak két évvel később fedezték fel, egy második, 2014-es támadás alkalmával . Összességében a támadók több mint 21,5 millió jelenlegi és egykori szövetségi alkalmazott személyes adatait lopták el.[7] Az így megszerzett 14 millió átvilágítási jelentés gyakran rendkívül érzékeny információt is tartalmazott a célszemélyekről, mint például a szexuális viselkedése, házasságon kívüli kapcsolatai, vagy szerencsejáték miatti anyagi problémái. A CIA több tisztjét is kénytelen volt visszarendelni pekingi állomáshelyéről az OPM adatlopási ügy miatt.[8] Ezen felül nem bizonyított, hogy a támadók nem állítottak ki biztonsági tanúsítványokat azoknak, akik nekik vagy esetleg megbízóiknak dolgoznak.[9]
Sony's PlayStation Network	2014 áprilisában a Sony megerősítette a hírt, hogy behatoltak a Playstation hálózatába, és 77 millió PSN (Playstation Network) és 24,6 millió Sony Entertainment Online előfizető személyes adatait lopták el, többek között valódi neveket, címeket, PSN felhasználói azonosítókat és jelszavakat, és e-mail címeket. Az incidens következményeként a PSN szolgáltatást 23 napig szüneteltették. Az eset teljes költségeit a Sony 171 millió dollárra becsülte. [10]
Anthem	2015 februárjában az Anthem bejelentette, hogy 78,8 millió jelenlegi és egykori biztosítottjuk adatai érintettek egy hackertámadásban. Az adatlopás, amely során az elkövető legalább 50 felhasználói fiókot használt fel, és legalább 90 számítógépre hatolt be, egy adathalász email-lel kezdődött. Az eset után az Anthem 260 millió dollár értékben ígért biztonsági beruházásokat.[11]

MELYEK A KIEMELT FELHASZNÁLÓI FIÓKOK?

A Forrester meghatározása szerint a jogosultság- és hozzáférés-kezelés (Identity and Access management, IAM) azoknak a szabályoknak, folyamatoknak és technológiáknak összessége, amelyet egy üzleti szervezet alkalmaz, hogy digitális identitásokat hozzon létre, és vezérelje ezeknek a szervezet eszközeihez való hozzáférését dinamikus értékrendszereken keresztül.[13] Ez a gyakorlat komplexebbé és kockázatosabbá válik, ha a kiemelt felhasználói fiókokra alkalmazzuk. Ezek az alábbiak:

Adminisztrátori fiókok

Azokat a felhasználói fiókokat foglalják magukba, amelyeket adminisztrátori pozícióban dolgozók használnak, akik olyan, magasabb jogosultsággal rendelkeznek, amellyel minden standard és kiemelt felhasználói tevékenységet végrehajthatnak.

Rendszergazdai fiókok

Ezeket a fiókokat – mint például a „root” a Linux/Unix rendszereknél, vagy az „Administrator” a Windows rendszereknél – eleve beépítették a rendszerekbe vagy alkalmazásokba.

Operatív fiókok

Ezek a fiókok rendszeradminisztrációra és telepítésre használt megosztott fiókokat illetve a rendszer (vagy alkalmazás) fiókokat foglalják magukba. A rendszerfiókok teszik lehetővé a szoftverek közötti interakciót, illetve különféle rendszer szolgáltatások futtatását a számítógépeken.

HOGYAN SZERZIK MEG A TÁMADÓK A KIEMELT FEL-HASZNÁLÓK AZONOSÍTÓIT?

A szakma már régen rájött, hogy a határvédelmi megoldások önmagukban nem képesek távol tartani a rosszfiúkat. A digitális gazdaság korában, amikor az webes alkalmazások, a BYOD (Bring Your Own Device) és a hibrid hálózatok mindennapjaink részévé váltak, és majdnem végtelen számú ponton lehet behatolni egy hálózatba a hackerek több módon is kihasználhatják ezeket a lehetőségeket.

KÜLSŐ FELDERÍTÉS

A MEGFELELŐ ÁLDOZAT FELKUTATÁSA

A kezdeti célpont kiválasztása

Noha vannak rá példák, hogy kiemelt felhasználók – például rendszeradminisztrátorok – esnek áldozatul a támadók manipulatív próbálkozásainak, azonban sokkal valószínűbb, hogy a támadók egy könnyebb célponttal kezdik. Az átlagos alkalmazottak sokkal kevésbé járatosak az IT-ban, mint az ezzel foglalkozó szakemberek, éppen ezért könnyebb célpontot jelentenek. Amint a támadóknak sikerült megszerezniük egy felhasználói fiókhoz tartozó azonosítókat, eredeti céljuk, a kiemelt felhasználói fiókok felé fordulnak. Sokszor előfordul, hogy a támadás első célpontja még csak nem is a célzott vállalatnál dolgozik. A Target esetében a támadók először egy apró, hűtéssel és ventillátorokkal foglalkozó céget céloztak meg, hogy behatoljanak a célvállalathoz. A cég ugyanis rendelkezett a Target hálózatához való hozzáféréssel. Az OPM (Office of Personnel Management) támadásnál az elkövetők szintén egy külső szolgáltató azonosítóit szerezték meg.

A támadók számára elérhető tengernyi információ láttán – amelyet nagyrészt maga az áldozat oszt meg a különböző közösségi média felületeken: Facebook, LinkedIn, Instagram vagy épp a Twitter –a bűnözők képesek meggyőző üzeneteket gyártani, amivel manipulálhatják a felhasználókat. És ha a közösségi média nem lenne elég, az online fórumok, mint például a Reddit vagy a Stackexchenge újabb információforrást jelenthetnek.

A HÍDFŐÁLLÁS KIALAKÍTÁSA

A támadóknak több módszerük is van arra, hogy beférkőzzenek az IT környezetbe, és gyakran kombinálják is ezeket annak érdekében, hogy egy hídfőállást építsenek ki a rendszeren belül, ahonnan belső felderítést folytathatnak, és további azonosítókat gyűjthetnek.

Pszichológiai manipuláció (Social engineering)

A legtöbb támadás azzal kezdődik, hogy egy gyanútlan felhasználót rávesznek valamire, ami a támadók további céljainak eléréséhez szükséges. Egy, általában e-mailen, közösségi médián, vagy chatprogramokon keresztül történő ún. phishing kísérlet során a támadó megpróbálja meggyőzni az áldozatot, hogy osszon meg vele valamilyen értékes információt (például jelszót), de gyakran csak arra kéri, hogy nyisson meg egy dokumentumot vagy kattintson egy linkre. Mindkettő lehetővé teszi, hogy a támadó malware-t töltsön le és telepítsen az áldozat számítógépére.

Az APT támadások elkövetői azonban ritkán dolgoznak olyan esetleges módszerekkel, aminek során sok felhasználónak küldenek általános üzeneteket. Ezzel szemben sokkal jellemzőbb, hogy előzetes kutatásaikra alapozva fogalmaznak meg sokkal meggyőzőbb, személyre szabott üzeneteket.

The Payload - Malware tools

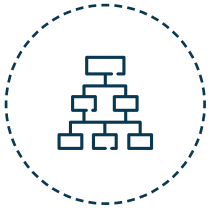
A célzott támadások során a kezdeti behatolás célja mindig az, hogy valamilyen software-t telepítsenek a gépre, amely segítheti a támadókat abban, hogy átvegyék a számítógép felett az irányítást, vagy összegyűjtsenek különböző információkat, például a belépéshez szükséges azonosítókat. A billentyűzet-figyelő eszközök (keyloggerek), amelyeket arra terveztek, hogy minden egyes billentyűzet leütést rögzítsenek, tökéletesek erre a célra. Más eszközök, mint például a Mimikatz és a WCE képesek a helyben tárolt bejelentkezési adatok összegyűjtésére. Ezek az eszközök az Interneten könnyen hozzáférhetők, és rendkívül hatékonyak.

BELSŐ FELDERÍTÉS

A KULCSOK FELKUTATÁSA

Ha a támadóknak sikerült behatolniuk a rendszerbe, megkezdik a belső felderítést. Megpróbálnak minél több információt begyűjteni az IT környezetről, feltérképezik a hálózatokat és az egész rendszert. Ezt számtalan hálózatdiagnosztikai segédprogrammal megoldhatják, ilyen például a Ping, a Traceroute vagy a Netsat. A DNS adatbázisok és a port szkennerek, mint például az Nmap, nagyon értékes információt szolgáltatnak a hálózati környezetről.

JOGOSULTSÁGOK ESZKALÁLÁSA



A KULCSOK MEGSZERZÉSE

A hálózati térkép pontos ismeretével a támadók hozzákezdhetnek magasabb jogosultságok megszerzéséhez, aminek végső célja egy tartományvezérlőhöz (DC) való hozzáférés. A pass-the-hash vagy az SSH kulcs megszerzése, illetve a kernel és service exploitok gyakran használt módszerek a jogosultságok eszkalálására.

Pass-the-hash

Az elmúlt évtizedekben a jelszóhasználat az IT biztonság szinonimájává vált. Amikor a jelszavakat tárolják, akkor egy ún. hash átalakítás segítségével titkosítják őket. Általában, ha a támadó titkosított jelszót lop el, akkor vissza kell azt fejtenie, ami nehéz és időigényes. A Windows rendszereken a jelszó hasheket a Local Security Authority Subsystem (LSASS) tárolja. Ha a támadók hozzáférnek a hashekhez, főleg az adminisztrátori jogosultságot nyújtókhoz, akkor letöltik, és felhasználják őket, hogy további gépekhez és rendszerekhez férjenek hozzá. A távoli szerveren vagy alkalmazáson ugyanis már nincs szükségük magára a szöveges jelszóra, mivel azonosíthatják magukat pusztán a hash-sel is.

Az SSH kulcs megszerzése

Számos szervezet az SSH (Secure Shell) protokollt használja, hogy távolról kezelje a Linux/Unix operációs rendszert futtató számítógépeit. Az SSH kulcsokat, az SSH protokollban a hozzáféréshez szükséges hitelesítési adatokat, általában automatikus folyamatokhoz és jelszó nélküli SSH loginok implementálásához használják a rendszergazdák, illetve a power userek. A támadók általában malware-t használnak, hogy összegyűjtsék ezeket a kulcsokat, amelyek aztán belépési pontot (backdoor) biztosíthatnak számukra. Ezen keresztül további szerverekre is bejuthatnak, és egész hálózatokra beférkőzhetnek. Az SSH kulcsok gyakran adminisztrátori vagy root jogosultsági szinttel rendelkeznek, így lehetővé teszik malware telepítését is.

Exploitok

Az expolitok olyan programok, amelyek kihasználják az alkalmazások és operációs rendszerek gyenge pontjait. Lehetővé teszik, hogy a hackerek átvegyék az irányítást egy rendszer fölött vagy azt, hogy magasabb jogosultságot szerezzenek. A Linux operációs rendszerek szoftveres sebezhetőségeit kihasználó exploitok egy parancssori utasítás segítségével próbálnak meg superuseri jogosultságot adni a felhasználónak. A Linux rendszereken a root felhasználóhoz tartozó jogosultságok megszerzése sok esetben mindössze annyiból áll, hogy a támadó letölt a célrendszerre egy kernel expolitot, lefordítja, majd lefuttatja azt.[13]

A Linux rendszerek esetében a támadók egyéb módszereket is használhatnak a sebezhető pontok felkutatására, a SUID (set user ID), illetve a SUDO (substitute user do) alkalmazásokkal. Megfelelő konfigurálás hiányában a támadók könnyen kihasználhatják a rendszer gyengeségeit ezekkel az alkalmazásokkal, és root felhasználói jogosultságra tehetnek szert, amely gyakorlatilag teljes kontrollt tesz lehetővé a megcélzott rendszeren.[14]

HOGYAN VÉDHETI MEG SZERVEZETÉT A KIEMELT FEL-HASZNÁLÓK AZO-NOSÍTÓIVAL VALÓ VISSZAÉLÉSTŐL?

Egyszerű változtatások a folyamatokban

A leggyorsabb módja a kiemelt felhasználói kockázatok csökkentésére a gyenge biztonsági házirendek felülvizsgálata. Az alábbiakban néhány könnyen végrehajtható, a szervezet számára azonnali eredményt hozó intézkedést javaslunk:

Állítson össze átfogó és naprakész listát a kiemelt felhasználói fiókokról

A hálózati környezetek méretének növekedésével az adminisztratív és operatív felhasználói fiókok száma is nő. Egy több ezer vagy tízezer szervert és hálózati eszközt használó szervezetnek gyakran nincs pontos nyilvántartása ezekről az eszközökről, és a hozzá tartozó kiemelt felhasználói fiókokról sem.

Korlátozza minden egyes kiemelt felhasználói fiók hozzáférését

Korlátozza az egyes felhasználói fiókok hozzáférését, a legkevesebb szükséges jogosultság elve alapján (Least privilege principle): minden fiókhoz csak annyi hozzáférést rendeljen, amekkora okvetlenül szükséges a fiókhoz tartozó feladat végrehajtásához. Például, ha egy fiókot azért hoztak létre, hogy egyetlen applikációt kezeljen, akkor annak a fióknak csak annyi jogosultság szükséges, amivel konfigurálhatja, és szükség esetén újraindíthatja az applikációt. Hasonlóképpen; ha lehetséges, ne hozzon létre fiókot olyan rendszereken, ahol az a fiók nem feltétlenül szükséges.

Törölje a már nem szükséges fiókokat

A nem megfelelő kiléptetés gyakran biztonsági réseket eredményez, mint például azok a bejelentkezési információk, amelyek egy kolléga távozása után is érvényesek maradnak. Az alvállalkozók esetében a helyzet még bonyolultabb lehet, különösen, ha csak egy időszakos projekt keretében kaptak hozzáférést.

Vezessen be jelszó szabályokat

A komoly biztonsági profillal rendelkező cégek általában „hivatalos” jelszóházirendet alkalmaznak a kiemelt felhasználói fiókokhoz, amely általában megköveteli az alapértelmezett jelszavak rendszeres cseréjét, és az erős jelszavak használatát. Ezen felül tiltja a kiemelt felhasználói fiókok jelszavainak megosztását. Ezek az egyszerű intézkedések eléggé nyilvánvalónak tűnnek, de számos kisebb-nagyobb szervezet a mai napig nem alkalmazza őket, így nagyban megkönnyítik a hackerek dolgát.

Akadályozza meg, hogy a felhasználók kiskapukat használjanak

A kiemelt fiókokat azért kapják a felhasználóik, hogy a napi munkájukat elvégezhessék. Mint ahogyan mások, ezek az emberek is a lehető leghatékonyabban akarnak dolgozni, ezért ugyanúgy hajlamosak kiskapukat használni, mint bárki más. A felhasználók rendszeres oktatásával, a „jó gyakorlatokat” példaként felhasználva nagymértékben csökkenthetjük szerveztünk kockázatait.

FOLYAMATTÁMOGATÓ TECHNOLÓGIÁK

kiemelt felhasználói hozzáférés-kezelés

JELSZÓKEZELÉS

Minél nagyobb egy szervezet IT hálózata, annál nehezebb biztonságosan kezelni a kiemelt felhasználói fiókjait; ezt már a közepes méretű cégeknél sem lehet megoldani megfelelő céleszközök nélkül.

Számos szervezet első lépése valamilyen jelszókezelő szoftver, amelyet kifejezetten a kiemelt felhasználói fiókok kezelésére terveztek. Az ilyen megoldások kontrollálják a kiemelt fiókokhoz való hozzáférést, erős jelszavakat generálnak, azokat randomizálják, majd egy jelszószéfben tárolják őket. A jelszókezelők bevezetésének számos előnye van:

A Az erős jelszavak használata megnehezíti a hacker dolgát.

B A jelszavakat egyetlen központi helyen kezelik; ezt könnyebb biztonságossá tenni.

C A jelszókezelő megoldások automatizálják az erős jelszavak generálását és cseréjét, akár több ezer vagy tízezer fiókhoz is.

D A jelszókezelők képesek adott időtartamig, vagy csak bizonyos intervallumban érvényes hozzáférést adni a kiemelt fiókokhoz.

Azonban a jelszókezelőknek megvannak a maguk korlátai is. Ha egy támadónak sikerült megszereznie egy kiemelt fiók bejelentkezési adatait, szabadon mozoghat a teljes hálózaton belül. Továbbá ezek az eszközök nem mutatják meg, hogy egy támadó mit csinált, miután feltörte a fiókot. Valójában a legtöbb, korábban említett betörési példánál, több mint valószínű, hogy a cégek használtak valamilyen jelszókezelő megoldást, tovább csökkentve a kiemelt felhasználóik adataival való visszaélés kockázatait, a szervezeteknek el kell mélyíteniük védelmüket.

KIEMELT FELHASZNÁLÓI MUNKAMENET-KEZELÉS (PRIVILEGED SESSION MANAGEMENT)

Ha a támadó már megszerezte a kiemelt felhasználói fiók azonosítóit, óriási kárt okozhat az Ön szervezetének. Egy kiemelt felhasználói munkamenet-kezelő megoldás központi hozzáférés-ellenőrzési pontot hoz létre, amely az alábbi előnyökkel jár:

A Rendszabályokkal korlátozható a felhasználók tevékenysége, akár az általuk kiadható parancsok is.

B A hitelesítő eszközök, például a jelszókezelők, vagy a többfaktoros hitelesítők számára is használható integrációs pont.

C Valós idejű felügyelet, amely lehetővé teszi, hogy a biztonsági csapat felügyelje, és közelről figyelje a kiemelt felhasználók tevékenységét.

D Kereshető munkamenet rögzítés, aminek segítségével megválaszolható, hogy ki, mikor, és mit csinált a kritikus IT eszközökön.

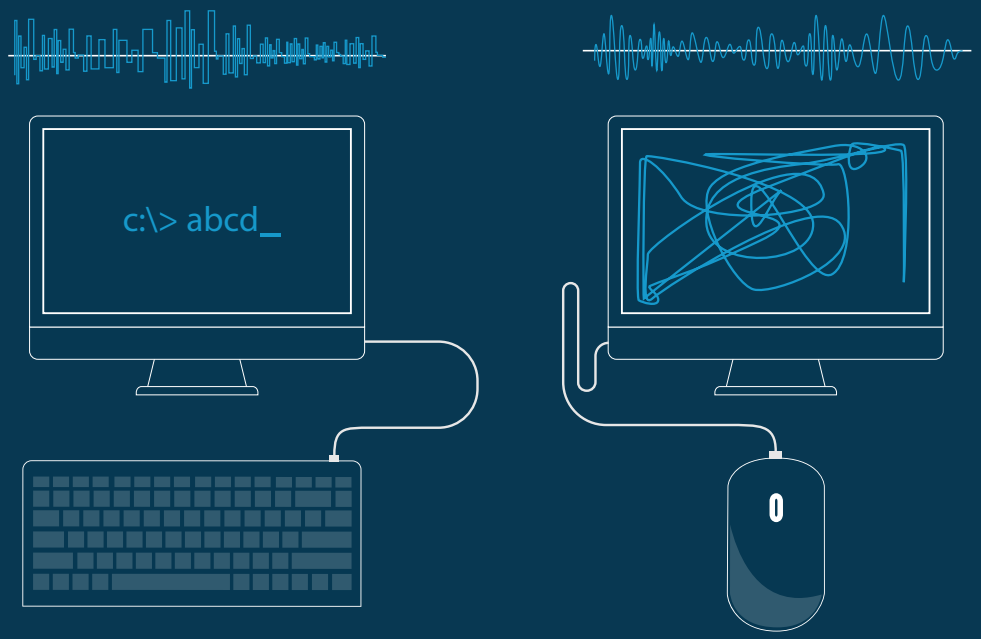
E A Four Eyes Authorizaton néven ismert kettős ellenőrzés lehetősége: bizonyos tevékenységekhez egy engedélyező személy jóváhagyása szükséges.

F Riasztás, vagy a kapcsolat azonnali megszakítása a biztonsági rendszabályok megszegése esetén.

A kiemelt felhasználói munkamenet-kezelés megerősíti a kiemelt felhasználói fiókokat, és korlátozza az általuk hozzáférhető eszközök és a kiadható parancsok körét, így csökkenti az adatvesztés kockázatát. Ugyanakkor azt nem tudja megállapítani, hogy egy adott fiókot feltörtek-e. Az elmúlt években a gépi tanulási algoritmusokon alapuló technológiák ezt is lehetővé tették.

"Ha mindössze egy felhasználónév és egy jelszó választ el a jogosultságok eszkalációjától, vagy egy újabb eszköz feltörésétől, akkor nem tettél eleget ahhoz, hogy megállítsd a támadókat."

– Verizon Data Breach Report 2017



FELHASZNÁLÓI VISELKEDÉSELEMZÉS A KIEMELT FELHASZNÁLÓK KONTEXTUSÁBAN

„Csak az amatőrök támadják a gépeket, a profik az embereket célozzák meg. Így minden megoldásnak az emberi problémát kell megoldania, nem a matematikai problémát."

- Bruce Schneier

A célzott támadások elleni harc egyik nagy kihívása, hogy a támadók ismeretlen vagy „zero day" módszereket, és malware eszközöket használnak a céljaik eléréséhez. A hagyományos biztonsági eszközök, mint például a SIEM-ek (Security and Event Management), gyakran képtelenek észlelni ezeket a támadásokat, mivel szabály alapú megközelítéssel dolgoznak. Bármilyen, eddig nem ismert szabályon alapuló módszer felderítetlen marad. Ebben a helyzetben segíthet a felhasználói viselkedéselemzés.

A biológusok meghatározása szerint a viselkedés az élő szervezetek belülről koordinált válaszainak összessége a külső és/vagy belső ingerekre – így gyakorlatilag viselkedésnek minősül minden, amit tudatosan csinálunk. Hasonlóképpen, a digitális viselkedés mindaz, amit a digitális világban teszünk. A gépelési jellemzők, a számítógépünk, tabletünk vagy telefonunk képernyőfelbontása, a kedvenc applikációink, vagy weblapjaink, és a digitális lábnyomunk számos más tulajdonsága gyakran sokkal jobban jellemez bennünket, mint a viselkedésünk. A felhasználói viselkedéselemző (User Behaviour Analytics, UBA) megoldások képesek felismerni és megkülönböztetni a felhasználókat a digitális tevékenységük alapján.

Fejlett statisztikai és adatgyűjtő megoldásaiknak köszönhetően a felhasználói viselkedést elemző eszközök képesek viselkedésprofilok építésére, és a felhasználói tevékenység folyamatos megfigyelése révén fel tudják ismerni a megszokottól eltérő tevékenységet. A kiemelt felhasználók aktuális tevékenységét a digitális lábnyomukkal folyamatosan összehasonlítva lehetővé válik a támadásokhoz kapcsolódó szokatlan viselkedés észlelése.

Mindezt a gépi tanulási algoritmusok teszik lehetővé, amelyek képessé teszik a számítógépet arra, hogy tanuljon, anélkül, hogy konkrétan erre programozták volna. Noha a számítógépek egyre gyorsabban képesek expliciten megfogalmazott, akár komplex parancsokat is végrehajtani, sokkal gyengébben teljesítenek, ha olyan problémákat kell megoldaniuk, amelyek egyszerű logikai szabályok segítségével nem modellezhetők.

Az UBA megoldásokat már számos biztonsági területen alkalmazzák a hitelkártya-csalástól kezdve a pénzügyi csalások felderítéséig. A kiemelt felhasználók azonosítóival való visszaélések felderítéséhez kifejezetten hatékony a kiemelt felhasználói tevékenység felügyeleti eszköz adataira épülő elemzési technikáikat alkalmazni. Már a munkamenetek tipikus metaadatai, mint például a bejelentkezési idő, a munkamenet hossza és helye vagy a célszerver címe is elég sok adatot szolgáltat az elemzéshez, de ennél jóval átfogóbb elemzés is lehetséges.

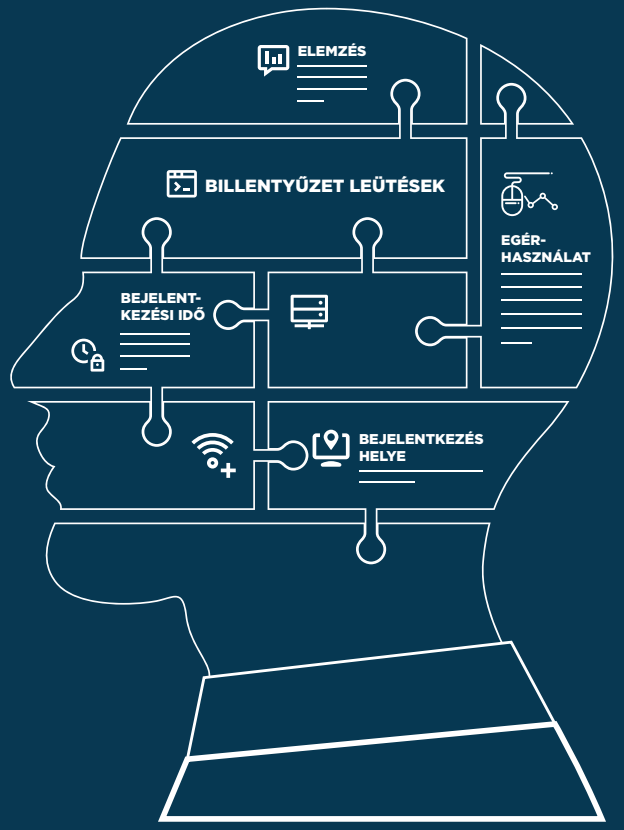
FOLYAMATOS HITELESÍTÉS

Ha több adatunk van a kiemelt felhasználók munkameneteiről, akkor a viselkedéselemző algoritmusok fel tudják fedezni a viselkedési anomáliákat. Míg a legtöbben ismerik a fiziológiai biometrián alapuló azonosítást, - ujjlenyomatok, írisz és retinafelismerők – a viselkedési biometria viszonylag ismeretlen. Az, hogy egy adott ember hogyan lép interakcióba egy számítógéppel az egér és a billentyűzet segítségével, valójában alkalmas az azonosításra, mivel egyedi.

A billentyűzetleütés ritmusának vagy dinamikájának elemzése azt vizsgálja, hogyan használja egy adott személy a billentyűzetet. A leütést leginkább jellemző mérőszámok az ún. dwell time (amilyen hosszan lenyomva tartják a billentyűt) illetve a flight time (a két leütés között eltelt idő).

Az egérmozgatás-elemzés alapelve nem az egér kurzorának pozíciója, hanem a pozíció relatív kiterjedése, miközben változik. A legfontosabb jellemző maga a mozgási sebesség. A mozdulatlanul töltött idő egy mozgatás és klikkelés között ugyanolyan tipikus, mint két kattintás, vagy egy kettőskattintás között. Sőt, a szögsebesség is fontos jellemző lehet.

A felhasználói viselkedéselemezés az egyik legizgalmasabb trend az IT világában, mert folyamatos hitelesítést biztosít. Ahogyan a kibertámadások egyre növekvő számából is látjuk, az egyszerű hitelesítési megoldások a barát/ellenség azonosítására nem nyújtanak elégséges védelmet. A folyamatos hitelesítés azonban megfelelő védelmet ígér a kiemelt felhasználók személyazonosságának ellopásával szemben.



KONKLÚZIÓ

A kiemelt felhasználók adataival való visszaélést széles körben használják az adatlopások esetében. Számos közismert szervezet esett már áldozatul kifinomult módszerekkel dolgozó, komoly pénzügyi támogatást élvező kiberbűnözőknek, de a támadások kockázatának csökkentésére megvannak a megfelelő módszerek. A Kiemelt Felhasználói Hozzáférés-kezelő (PAM) termékek, kombinálva a legújabb elemző megoldásokkal, és néhány viszonylag egyszerűen végrehajtható folyamat-változtatással segíthet felderíteni a feltört felhasználói fiókokat, és megállítani a támadókat, mielőtt valódi károkat okozhatnának szervezetének.

Tudjon meg többet a Safeguard for Privileged Sessions-ről

Tudjon meg többet a Safeguard for Privileged Analytics-ról

Beszéljen szakértőnkkel

JEGYZETEK

1. “The 16 biggest data breaches of the 21st century” CSO Online, September 2017
2. The Forrester Wave™: Privileged Identity Management, Q3 2016
3. “How did Yahoo get breached? Employee got spear phished, FBI suggests” Arstechnica, March 2017
4. Yahoo 2016 10-K Securities and Exchange Commission filing
5. Target 2016 Annual Report
6. “J.P.Morgan hackers came in the front door – in June. Two months of mayhem”, Bloomberg August 2014
7. “Congressional Report Slam OPM on Data Breach”, Krebs on Security, September 2016
8. “Analysis: Why the OPM Breach Is So Bad”, Bankinfo Security, June 2015
9. “Congressional Report Slam OPM on Data Breach”, Krebs on Security, September 2016
10. “Congressional Report Slam OPM on Data Breach”, Krebs on Security, September 2016
11. “Limiting the impact of data breaches - The case of the Sony Playstation Network”, strategy&, PWC, 2011
12. “A New In-Depth Analysis of Anthem Breach”, Bankinfo Security, January 2017
13. “Evolve Your IAM Strategy For Your Digital Business”, Forrester Research, Inc., August 18, 2017
14. SANS “Attack and Defend Linux Privilege Escalation Techniques of 2016” Long

A BALASYSRŐL

A Balasys egy IT biztonsági megoldásszállító, mely forgalmazóként képviseli a One Identity(Balabit) termékeket Magyarországon. A 2000-ben létrejött teljes egészében magyar tulajdonú vállalat alapítása óta a hazai informatikai biztonsági piac meghatározó szereplője, ahol az általa fejlesztett és forgalmazott termékek technológiai vezető szerepet töltenek be. Ügyfélkörébe a hazai államigazgatási-, pénzügyi-, telekommunikációs szektor meghatározó szereplői és egyéb nagyvállalatok tartoznak. A vállalat több mint tizenöt éves tapasztalattal és kiforrott megoldásokkal rendelkezik a hálózatbiztonsági és határvédelmi technológiák területén. Aktív kutatás-fejlesztési tevékenységet folytat a saját fejlesztésű Zorp technológiáján, ügyfeleit pedig magas színvonalú szolgáltatásokkal támogatja.

www.balasys.hu

BALASYS