20 KRITIKUS BIZTONSÁGI KONTROLL

kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

A 20 kritikus kontroll költséghatékony számítógépes és hálózati védelmet tesz lehetővé, mérhetővé, skálázhatóvá és megbízhatóvá téve a folyamatokat a teljes (USA) kormányzaton belül, a védelmi iparágban és egyéb olyan szervezeteknél, amelyeknek védendő információi és rendszerei vannak. A kontrollok az aktuális fenyegetések alapján készültek. A kiválasztás a nagy kormányzati szervezetek konszenzusa alapján történt, mely szervezetek aszerint védekeznek a kibertámadások ellen, hogy mely kontrollok a legkritikusabbak az ismert támadások elleni védekezésben.

Az anyag meghivatkozza az Ausztrál védelmi hivatal hasonló tartalmú dokumentumát, a NIST 800-53 anyagát, vagy éppen a brit Nemzeti Infrastruktúra Védelmi Központ (CPNI) kapcsolódó tanácsait.

A poszter célja, hogy összefoglalva felvillantsa azokat a kontrollokat, melyek a leghatékonyabban járulhatnak hozzá a szervezet védelméhez. Egyben rangsorolja is a potenciális támadásokat, és a támadáshoz szükséges tudást, ill. sikeres támadás esetén a támadás hatását. Ezek alkalmazása, ill. a saját szervezetre történő átültetése megkerülhetetlen, jelen anyag csak segítség abban, hogy a fontos dolgokra felhívja a figyelmet.

Ez a poszter a '20 Critical Security Controls' című, a www.sans.org/critical-security-controls oldalon elérhető SANS publikáció esetenként módosított változata, amelyet az Önkéntes Kibervédelmi Összefogás (KIBEV) tagjai fordítottak magyar nyelvre.

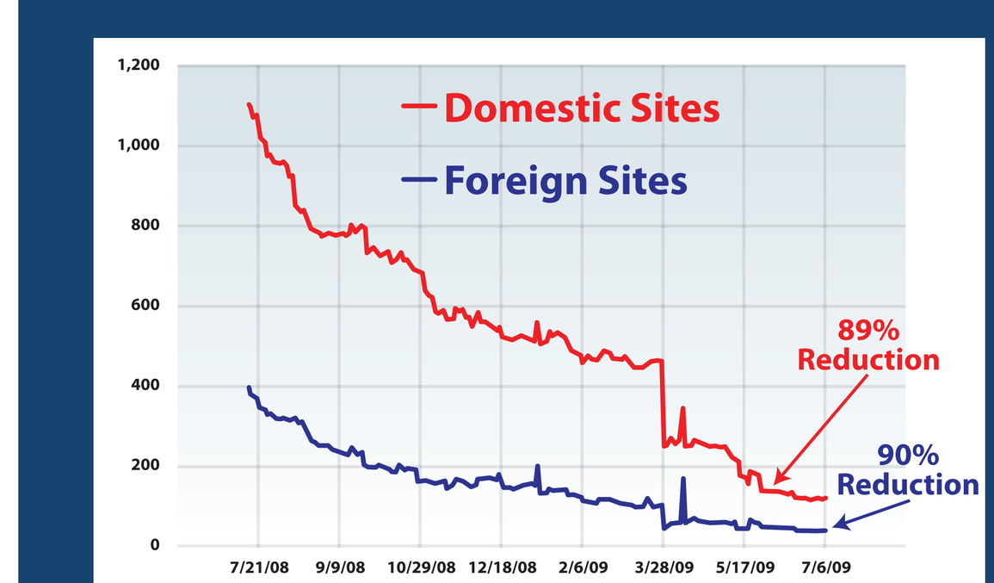
A 20 kritikus kontroll automatizálásában rejlő értékek bizonyítékai

A kritikus kontrollok automatizálása által napi rendszerességű, hiteles adatokat kaphatunk az informatikai eszközöket fenyegető támadásokkal szembeni ellenálló képességről, valamint a rendszergazda számára lesz egy fontossági lista azon tevékenységekről, amelyekkel fenntarthatják a rendszereik elvárt szintű biztonságát. Ezzel egyidőben kiküszöbölhetjük, hogy a kiadás pillanatában már elavult vékony audit jelentésekre dobjunk ki pénzt.

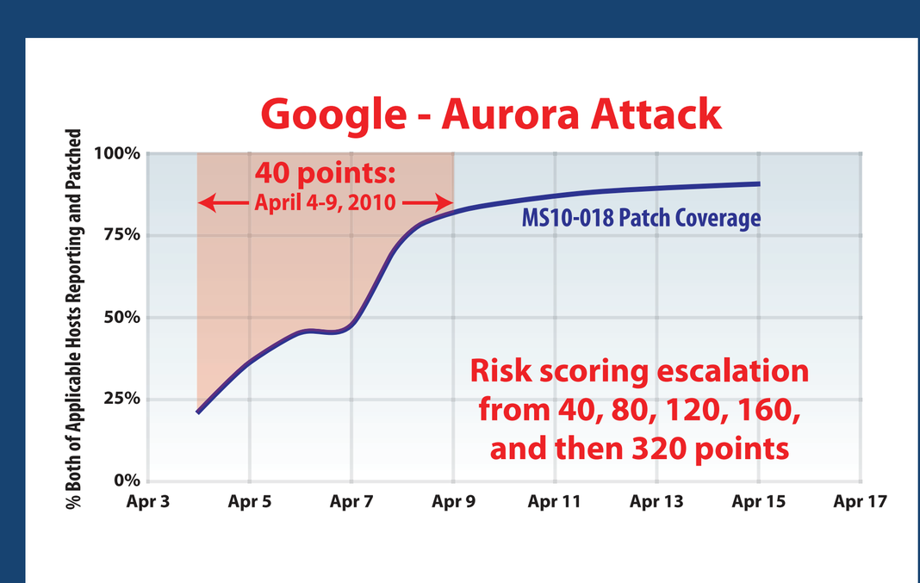
Az ilyen állítások azonban bizonyítást igényelnek.

Az Egyesült Államok Külügyminisztériumában az elsők között vezették be a teljes szervezetet lefedő automatizált biztonsági felügyeletet, amely egységes pontozási rendszerével egyértelmű információkat biztosít a rendszergazdáknak a napi feladatok során végrehajtandó intézkedésekről. Ennek a következő eredményei vannak:

A bevezetés utáni első évben a Külügyminisztérium több százezer számítógépére vonatkoztatott kockázati mutatószámok közel 90%-kal csökkentek, míg ugyanez a mutatószám más szövetségi intézményeknél alig változott, és a csökkenés ma is tart (1. diagram). Ami még fontosabb, amikor egy újabb jelentős fenyegetés jelenik meg, a Külügyminisztérium képes volt a rendszerei 90%-án tíz napon belül alkalmazni az elérhető javításokat (2. diagram), míg más szervezetek az automatizálás, a pontrendszer és a rendszergazdai feladatok fontossági sorrendje nélkül több hónap alatt is csak a rendszereik 20-65%-ában tudta javítani a sérülékenységeket.



1. diagram: 90 %-os kockázatcsökkenés kevesebb mint egy év alatt



2. diagram: Fenyegetés-alapú kockázatcsökkentés: Egy magas besorolású javításnak adott 40 pontos kockázat 80%-os gyors helyreállítást eredményez, 320 pontra emelve a besorolási értéket a megfelelés már 90 %-os.

20 kritikus biztonsági kontroll			Az amerikai Nemzetbiztonsági hivatal értékelése a 20 kritikus biztonsági konrollról				Kapcsolódó NIST speciális pulikáció: 800-53, Revision 3, Priority 1 Kontrollok
	A kritikus biztonsági kontroll megnevezése	A kritikus biztonsági kontroll leírása	Fontosság	Hatása egy támadás sikerességére	Függőségek	Technológiai érettség	
1	Jogosult és jogosulatlan eszközök leltára	**Csökkenteni kell a támadók lehetőségét, hogy jogosulatlan vagy védtelen rendszereket találhassanak és használhassanak ki:** Aktív feltérképező és beállításkezelő rendszert kell alkalmazni, hogy naprakész leltárral rendelkezzünk a vállalati hálózathoz csatlakozó eszközökről, beleértve a szervereket, az asztali gépeket, a hordozható számítógépeket és a távoli eszközöket.	1	Nagyon magas	Alapvető	Magas	CM-8 (a, c, d, 2, 3, 4) PM-5, PM-6
2	Jogosult és jogosulatlan szoftverek leltára	**Azonosítani kell a sebezhető vagy rosszindulatú szoftvereket, hogy csökkentsük vagy kizárjuk a támadásokat:** Készíteni kell minden rendszer esetében egy engedélyezett szoftvereket tartalmazó listát, és ki kell alakítani egy eszközparkot a telepített szoftverek nyomon követésére (beleértve a típusát, verziószámát és a kiegészítő frissítéseket), és figyelni kell a jogosulatlan vagy szükségtelen szoftvereket.	1	Nagyon magas	Alapvető	Magas	CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9 PM-6,SA-6, SA-7
3	Biztonságos beállítások hardvereken és szoftverekben laptopokra, munkaállomásokra és szerverekre	**Meg kell előzni, hogy a támadók hálózatokon vagy böngészőkön keresztül könnyű elérést biztosító szolgáltatásokat vagy beállításokat használjanak ki:** Biztonságos telepítőkészletet kell létrehozni, melyet az újonnan telepítendő rendszerekre lehet alkalmazni, ezt biztonságos tárhelyen kell elérhetővé tenni, időnkénti ellenőrzéssel és frissítéssel, és egy beállítás-kezelő rendszerbeni nyomon követéssel.	1a	Nagyon magas	Adottság	Magas	CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
4	Folyamatos sebezhetőségi felmérés és felszámolás	**Kezdeményező módon kell azonosítani és javítani a biztonsági kutatók vagy szállítók által jelentett szoftver sebezhetőségeket:** Rendszeres időközönként automatikus sebezhetőség-vizsgáló alkalmazásokat kell futtatni minden rendszerrel szemben, és gyorsan fel kell számolni minden sebezhetőséget, a kritikusakat 48 órán belül.	1a	Nagyon magas	Adottság	Magas	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)
5	Rosszindulatú kód elleni védekezés	**Meg kell akadályozni, hogy rosszindulatú kódok befolyásoljanak rendszerbeállításokat és tartalmakat, érzékeny adatokat szerezzenek meg, vagy terjedjenek:** Vírus és kémprogramok elleni automatikus védelmet kell alkalmazni a munkaállomások, szerverek és mobil eszközök folyamatos figyelése és védelme érdekében.	1a	Magas / közepes	Adottság	Magas / közepes	SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)
6	Alkalmazói szoftverek biztonsága	**Semlegesíteni kell a Web-alapú és egyéb szoftver termékek sebezhetőségeit:** Gondosan tesztelni kell a belső fejlesztések és a harmadik fél által fejlesztett alkalmazások biztonságát, beleértve a fejlesztői hibákat és a rosszindulatú kódokat is. Olyan Web-alkalmazás tűzfalat kell telepíteni, amely minden forgalmat vizsgál és minden felhasználói adatot hibaellenőrzésnek vet alá (az adat megfelelő méretét és típusát egyaránt vizsgálva).	2	Magas	Adottság	Közepes	CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
7	Vezetéknélküli eszközök felügyelete	**Védeni kell a biztonsági határvonalat a jogosulatlan vezeték nélküli hozzáférésektől:** Csak akkor szabad engedélyezni a vezeték nélküli csatornán kapcsolódni szándékozó eszközöket, ha azok engedélyezett beállítással és biztonsági profillal rendelkeznek, és dokumentált tulajdonoshoz rendelve valamilyen üzleti igényt elégítenek ki.	2	Magas	Adottság	Közepes	AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)
8	Adatvisszaállítási képesség	**A támadásból származó károk minimalizálása:** Megbízható terv megvalósítása, ami alapján egy támadás informatikai rendszerekre gyakorolt hatásait meg lehet szüntetni. Automatikusan menteni kell minden információt, amire az egyes rendszerek teljes helyreállítása során szükség lehet, beleértve az operációs rendszert, az alkalmazást és az adatokat. Minden rendszerről készüljön legalább heti mentés, az érzékeny rendszerekről ennél gyakrabban. Rendszeresen tesztelni kell a visszaállítási eljárásokat.	2	Közepes	Adottság	Közepes	CP-9 (a, b, d, 1, 3), CP-10 (6)
9	Biztonsági ismeretek felmérése és megfelelő képzés a hiányosságok pótlására	**A tudásban meglévő hiányosságokat fel kell mérni és a megfelelő képzésekkel és gyakorlatokkal pótolni kell azokat:** Fejleszteni kell a biztonsági ismeretek felmérésének tervét és képzéseket kell társítani az egyes munkakörökhöz szükséges képességekhez. Ezeket az eredményeket felhasználva kell biztonsági eljárások fejlesztését hatékony erőforrás-tervezéssel támogatni.	2	Közepes	Adottság	Közepes	AT-1, AT-2 (1), AT-3 (1)
10	Biztonságossá kell tenni a hálózati eszközök, tűzfalak, router-ek és switch-ek konfigurációját	**Ki kell zárni azokat a hálózati pontokat, amelyekből kapcsolódási pontokat lehet kialakítani az Internetre, más szervezetek hálózatához vagy belső hálózati szegmensekhez:** A tűzfalak, router-ek és switch-ek konfigurációját össze kell hasonlítani a szabványokkal minden hálózati eszköz típus esetén. Meg kell győződni arról, hogy a standard konfigurációtól történő bármilyen eltérés megfelelően dokumentált és jóváhagyott és az ideiglenes módosítások visszavonásra kerülnek, amint az üzleti igény megszűnik.	3	Magas / közepes	Adottság / Függő	Közepes / alacsony	AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), RA-5, IA-2 (1, 6), IA-5, IA-8, SC-9, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18)
11	Korlátozott és ellenőrzött hálózati portok, protokollok és szolgáltatások	**Távoli hozzáférést csak arra jogosult felhasználók és szolgáltatások számára szabad engedélyezni:** Host-alapú tűzfalakat, port-szűrést és port-scannelő eszközöket kell alkalmazni, hogy a nem engedélyezett forgalom blokkolása megvalósuljon. Megfelelő konfigurációval biztosítani kell, hogy a webszerverek, levelezőszerverek, fájl és nyomtató szolgáltatások és a DNS-szerverek távoli hozzáférése megfelelően korlátozott legyen. Le kell tiltani a nem szükséges szoftverkomponensek automatikus telepítését. A szervereket tűzfallal kell védeni, kivéve, ha a távoli hozzáférést üzleti okok indokolják.	3	Magas / közepes	Adottság / Függő	Közepes / alacsony	CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)
12	Rendszergazdai jogosultságok ellenőrzött használata	**A munkaállomások, laptopok és szerverek rendszergazdai felhasználói fiókjait védeni és használatukat jóvá kell hagyni, annak érdekében, hogy meg lehessen előzni két gyakori támadási formát:** (1) felhasználó megtévesztése, hogy nyisson meg egy kártékony e-mail mellékletet vagy fájlt, illetve látogasson meg egy kártékony weboldalt; és (2) egy adminisztrátori jelszó feltörése, ezzel szerezve hozzáférést a célba vett számítógéphez. Erős jelszavakat kell használni (pl. nem szótári szó, hosszú és sokféle karakterből álló sorozat – ld. http://href.hu/x/ifur).	4	Magas / közepes	Függő	Közepes	AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
13	Határvédelem	**Felügyelni és vizsgálni kell a hálózat határain átmenő adatforgalmat, támadásokat és kompromittált számítógépekre utaló bizonyítékokat keresve:** Többrétegű határvédelmi rendszert kell létrehozni, tűzfalak, proxy-k, DMZ és egyéb hálózati eszközök felhasználásával. Szűrni kell a bejövő és kimenő forgalmat, beleértve az üzleti partnerek hálózatait (extranet) is.	4	Magas / közepes	Függő	Közepes	AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7
14	Karbantartás, ellenőrzés és a biztonsági naplók elemzése	**Részletes naplózást kell használni, hogy felfedezhetőek és azonosíthatóak legyenek a támadások, beleértve a támadások kiindulópontjait, a kártékony szoftverek telepítését és a megfertőzött számítógépek tevékenységét:** minden hardvernek és a rájuk telepített szoftvereknek szabványosított naplózást kell végezniük, ide értve a dátumot, az időbélyeget, a forrás és cél címeket és egyéb információkat minden csomagról és/vagy tranzakcióról. A naplóbejegyzéseket dedikált szervereken kell tárolni, és legalább kétheti riportokat kell készíteni az anomáliák észleléséről és dokumentálásáról.	4	Közepes	Függő	Közepes	AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)
15	Hozzáférés-kezelés a „szükséges és elégséges” elv alapján	**Részletes naplózást kell használni, hogy felfedezhetőek és azonosíthatóak legyenek a támadások, beleértve a támadások kiindulópontjait, a kártékony szoftverek telepítését és a megfertőzött számítógépek tevékenységét:** minden hardvernek és a rájuk telepített szoftvereknek szabványosított naplózást kell végezniük, ide értve a dátumot, az időbélyeget, a forrás és cél címeket és egyéb információkat minden csomagról és/vagy tranzakcióról. A naplóbejegyzéseket dedikált szervereken kell tárolni, és legalább kétheti riportokat kell készíteni az anomáliák észleléséről és dokumentálásáról.	4	Közepes	Függő	Közepes / alacsony	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6 MP-3, RA-2 (a)
16	Hozzáférés ellenőrzés	**Meg kell akadályozni, hogy a támadók jogosult felhasználókat személyesítsenek meg.** Ennek elérésére felhasználói hozzáférést meg kell szüntetni, amelyhez nem tartozik üzleti (vagy rendszer) folyamathoz és nincs felelőse. A megszűnt munkaviszonyú dolgozók (vagy szerződésesek) hozzáféréseit azonnal hatállyal meg kell szüntetni. A használaton kívüli hozzáféréseket le kell tiltani és az azokhoz tartozó fájlokat (adatokat) izolálni kell. Megfelelő erősségű jelszavak használatát ki kell kényszeríteni.	4	Közepes	Függő	Közepes / alacsony	AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3
17	Adatszivárgás elleni védelem	**Meg kell akadályozni, hogy érzékeny adatokat hálózaon keresztül, illetve fizikai formában ellopjanak.** Ennek érdekében ellenőrizni kell a hálózati határoló eszközökön (proxy/tűzfal) a forgalamat, ezzel a lehető legkisebb kitattséget biztosítani. Ellenőrzés alá kell venni az embereket, a folyamatokat és a rendszereket egy centralizált menedzsment-rendszer használatával.	5	Közepes / alacsony	Függő	Alacsony	AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7
18	Incidensek kezelésének képessége	**Meg kell védeni a szervezet jó hírnevét és a birtokolt információkat.** Ennek érdekében egy olyan (jól működő és tesztelt) incidens-menedzsment rendszert kell kialakítani, mely világosan meghatározza a feladatokat és felelősségeket egy bekövetkező támadás gyors felderítése, a károk minimalizálása, a támadó semlegesítése és a rendszer integritásának helyreállítása érdekében.	5	Közepes	Függő	Alacsony	IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8
19	Biztonságos hálózat-tervezés	**Meg kell előzni, hogy hálózat rossz szegmentációjával az támadási felületet biztosítson.** Ennek érdekében robosztus, biztonságos hálózati tervezést kell megvalósítani, annak érdekében, hogy a kívánt biztonsági elvárásokat ne lehessen megkerülni. Legalább három rétegű hálózati szervezést kell alkalmazni: DMZ, belső hálózat és privát hálózati szeegmensek. Lehetővé kell tenni új biztonsági (hozzáférési kontroll) elemek gyors bevezethetőségét, melyekkel a támadások gyorsan visszaverhetők.	6	Alacsony	Közvetett	Alacsony	IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7
20	Behatolás tesztek és „Red Team” gyakorlatok	**Szimulált behatolástesztek segítségével kell erősíteni a szervezet reakcióképességét.** Rendszeres belső és külső behatolás-teszteket kell végrehajtani, hogy a rendszerekben található sebezhetőségek napvilágra kerüljenek és hogy a támadásból adódó valós károk felmérhetők legyenek. Belső „Red Team"v csapattal végzett gyakorlatok - melyek célja rendszer- és adathozzáférés szerzése kritikus rendszerekben - végrehajtásával tovább növelhető a védelmi- és válaszképesség.	6	Alacsony	Közvetett	Közepes / alacsony	CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)

www.biztostu.hu
buhera.blog.hu
www.saferinternet.hu
www.cert-hungary.hu
cert.hu

Ausztrália — Australian Government Department of Defence
Egyesült Királyság — CPNI Centre for the Protection of National Infrastructure
Egyesült Államok — Homeland Security

SANS Winter 2012