

20 KRITIKUS BIZTONSÁGI KONTROLL



A 20 kritikus kontroll

külsőhatékony számítógépes és hálózati védelmet tesz lehetővé, mérhetővé, skálázhatóvá és meghízhatóvá téve a folyamatokat a teljes (USA) kormányzaton belül, a védelmi lapárgában 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.

A poszter célja továbbra is az, hogy összefoglalva rávilágítson azokra a kontrollokra, 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 áttültetése 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 2013 tavaszi kiadásának esetenként módosított változata, amelyet az Önkéntes Kibervédelmi Összefogás (KIBEV) tagjai fordítottak magyar nyelvre.

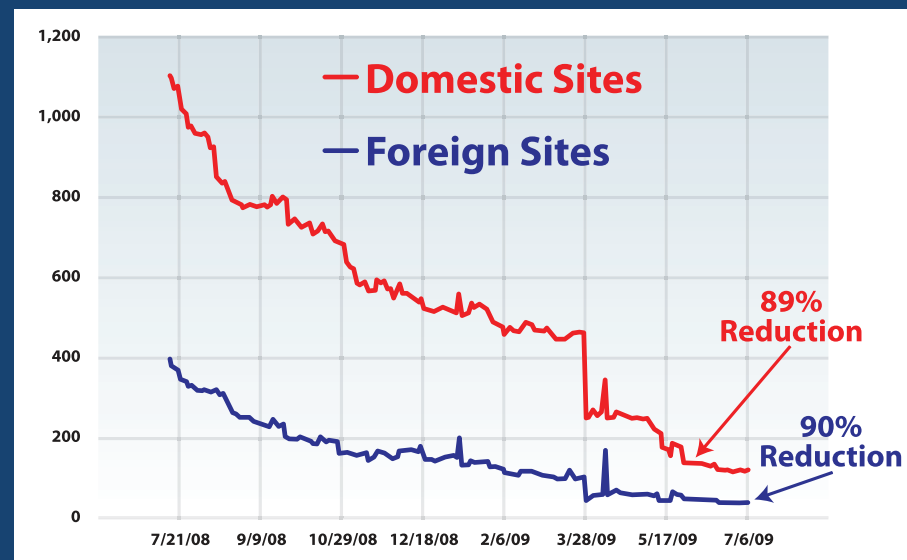
A 20 kritikus kontroll automatizálásában rejlő értékek bizonyítékai

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

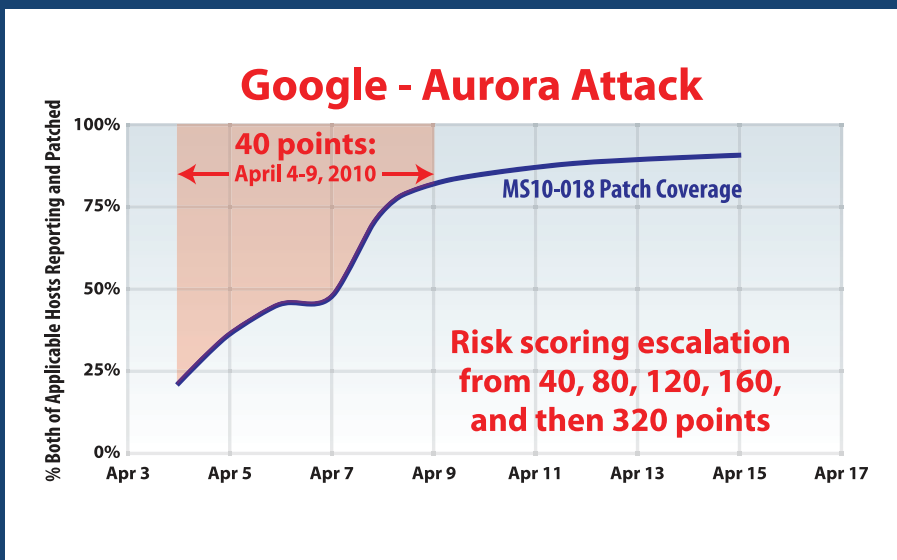
Az ilyen állítások azonban bizonyítást igényelnek.

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

A bevezetés utáni első évben a Külgügyminisztérium több százezer számítógépre 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 jelent meg, a Külgügyminisztérium 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 nélküli több hónap alatt is csak a rendszereik 20-65 %-ában tudta javítani a sérülékenységeket.



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



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

Az első lépések: az 5 leggyorsabban eredményt hozó kontroll

A kritikus kontrollok jelentik egy szervezet valós biztonsági fenyegetettségek elleni védelmének leginkább költséghatékony módját. A 2-4. kritikus kontrollok alapján lehet kidolgozni az 5 leggyorsabban eredményt hozó intézkedést. Ezeknek az intézkedéseknek azonnali hatásuk van a célzott támadások elleni védekezésben.

Ezek a kontrollok az alábbiak:

1. Engedélyezett alkalmazások listájának összeállítása (2. kontroll)
2. Biztonságos konfigurációk általános használata (3. kontroll)
3. Alkalmazások hibajavításának telepítése a kiadás után 48 órán belül (4. kontroll)
4. Rendszerszoftverek hibajavításainak telepítése a kiadás után 48 órán belül (4. kontroll)
5. Az adminisztrátori jogosultságokkal rendelkező felhasználók számának minimalisra csökkentése (3. és 12. kontroll)

Mit kell megvédeni? Célszerű készíteni egy listát az üzleti és háttér-területek számára legfontosabb folyamatokról, valamint egy feltárt az információkról és informatikai eszközökről, amelyek az egyes folyamatok működéséhez szükségesek. Ezek az információk létfontosságúak a kritikus kontrollok bevezetéséhez használható jelenlegi képességek felméréséhez.

Hol vannak hiányosságok? Minden, az üzleti vagy háttér-területek számára fontos eszköz esetében össze kell hasonlítani a meglévő kontrollokat a kritikus kontrollokkal, feltárva, hogy a jelenlegi kontrollok megfelelőek-e.

Mik a prioritások? Az előző lépés során feltárt hiányosságok és a szervezetre jellemző kockázatok alapján célszerű az 5 leggyorsabban eredményt hozó kontrollt bevezetni és stratégiát készíteni a többi kontroll bevezetésére.

Mit lehet automatizálni? A kontrollok bevezetésének tervezése során célszerű az integrált és automatizált eszközökre épített biztonsági folyamatok kialakítására koncentrálni, amelyek sok rutinfeladatot vehetnek le a biztonsági és üzemeltetői kollektíváról. A kontrollok kialakítása során kiemelt szempont volt az automatizálhatóság. A cél pontos és időszéri adatok gyorsabb és hatékonyabb biztosítása a rendszerüzemeltetőknek és azoknak, akik proaktív módon képesek megakadályozni támadásokat.

20 kritikus biztonsági kontroll		Az amerikai Nemzetbiztonsági hivatal értékelése a 20 kritikus biztonsági kontrollról				Kapcsolódó kontrollok az NST 800-53 rev. 3 kiadványában
A kritikus biztonsági kontroll megnevezése		Fontosság	Hatása egy támadás sikerességére	Függőségek	Technológiai érettség	
1 Engedélyezett és nem engedélyezett eszközök listára	Csökkenteni kell a támadók lehetőségét, hogy jogosulatlan vagy védtelen rendszerek találhassanak ki: Aktív feltérképező és beállításkéző rendszert kell alkalmazni, hogy naprakész listával rendelkezünk a vállalati hálózathoz csatlakozó eszközökről, beleértve a szervereket, a munkaadókat, hardwarzó számítógépeket és távoli eszközöket.	1	Nagyon magas	Alapvető	Magas	CM-8 (a, c, d, 2, 3, 4) PM-6
2 Engedélyezett és nem engedélyezett szoftverek listára	Azonosítani kell a sebezhető vagy rosszindulatú szoftvereket, hogy csökkentjük vagy kizárjuk a támadásokat: Készíteni kell minden rendszer esetében egy engedélyezett szoftvereket tartalmazó listát és ki kell alakítani egy eszközparkot a telepített szoftverek követésére (beleértve a típusát, verziószámát és a kiegészítő frissítéseket is) 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 hardver és szoftver beállítások laptopokon, munkaadóállomásokon és szervereken	Meg kell előzni, hogy a támadók a hálózaton vagy bűngészőkön keresztül könnyű elérést biztosító szolgáltatásokat vagy beállításokat használjanak ki: Biztonságos telephelyeztetet lehet érvényesíteni, melyet az újonnan telepítendő rendszerekre lehet alkalmazni, ezt biztonságos tárolóhelyen kell elérhetővé tenni, időszakos ellenőrzéssel és frissítéssel, valamint egy beállítás-kező rendszerben történő 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 sérülékenység-vizsgálat és megszüntetés	Kezdeményező módon kell azonosítani és javítani a biztonsági kufatók vagy szállítók által jelentett szofver sebezhetőségeket: Rendszeres időközönként automatikus sebezhetőség-vizsgáló alkalmazásokat kell futtatni minden rendszerrel szemben, és gyorsan fel kell szüntetni minden sebezhetőséget, a kritikusokat 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 szerezenek meg vagy terjedjenek: Vírus és kemprogramok elleni automatikus védelmet kell alkalmazni a munkaadóállomások, 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 szofver termékek sebezhetőségét: Gondosan tesztelni kell a belső fejlesztések és a harmadik fél által fejlesztett alkalmazások biztonsági jellemzőit, mielőtt az egyes rendszerek teljes helyreállítása során szükség lehet, beleértve az operációs rendszert, az alkalmazást és az adatokat. Minden rendszerrel készülni legalább heti mentés, az érzékeny rendszerekől ennél gyakrabban. Rendszeresen tesztelni kell a visszaállítási eljárásokat.	2	Magas	Adottság	Közepes	CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
7 Vezeték nélküli eszközök felügyelete	Védeni kell a biztonsági határvonalat a jogosulatlan vezeték nélküli hozzáférésektől: Csak akkor szabad engedélyezni a vezeték nélküli csatlakozás kapcsolódni szükséges eszközök, ha azok engedélyezett beállításokkal és biztonsági profilokkal rendelkeznek, és dokumentált tulajdonosuk 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. A támadók, router-ek és switch-ek konfigurációját össze kell hasonlítani a szabványosított állapotú típusú eszközökkel, 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.	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 megévő hiányosságokat fel kell mérni és a megfelelő képzésekkel és gyakorlatokkal pótolni kell azokat: Fejleszteni kell a biztonsági ismeretek felmérésének tervét és képzéseket kell tartítani az egyes munkatörkhöz szükséges képességekhez. Ezeket az eredményeket felhasználva kell biztonsági eljárások fejlesztését hatékony erőforrással levezéssel 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 zární azokat a hálózati pontokat, amelyekből kapcsolódási pontokat lehet kialakítani az internetre, más szervezetek hálózatahoz vagy belső hálózati szegmensekhez: A tűzfalak, router-ek és switch-ek konfigurációját össze kell hasonlítani a szabványosított állapotú típusú eszközökkel, 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-7, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18)
11 Korlátozott és ellenőrzött hálózati portok, protokollok és szolgáltatások	Távoli hozzáférést csak arra feljogosított felhasználók és szolgáltatások számára szabad engedélyezni: Host-alapú tűzfalakok, port-szűrés és port-scannelő eszközöket kell alkalmazni, hogy a nem engedélyezett forgalom blokkolása megvalósuljon. Megfelelő konfigurációval biztosítani kell, hogy a webszerverek, levelezőszerverek, fáj- és nyomtatógépek és a DNS-szerverek távoli hozzáférése megfelelően korlátozott legyen. Le kell tiltani a nem szükséges szofverkomponensek automatikus telepítését. A szervereket tűzfalakkal meg 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 munkaadóállomások, laptopok és szerverek rendszergazdai felhasználói fiókjait védeni és használatukat jóvá kell hagyni, annak érdekében, hogy meg lehessen előzni két gyakori támadást formát: (1) felhasználó megváltoztatása, hogy nyíson meg egy kártevőnek e-mail megküldését vagy fájlt, illetve látogasson meg egy kártevőnek weboldalát; és (2) egy adminisztrátori jelszó felmérése, ezzel szerezve hozzáférést a célba vett számítógéphez. Erős, komplex jelszavakkal kell használni (pl. nem szóközű szó, hosszú és sokféle karakterből álló sorozat – ld. http://href.hu/x/jur).	4	Magas / közepes	Függő	Közepes	AC-4 (2, 5), AC-17 (3), AC-19, AU-2 (4)
13 Hátvédelem	Felügyelni és vizsgálni kell a hálózat határain átmenő adathorgalmat, támadásokat és kompromittált számítógépekre utaló bizonyítékokat keresve: Többrelegű 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 felleldezhettek és azonosíthatók legyenek a támadások, beleértve a támadások kitudulópontjait, a kártevőny szofverek telepítését és a megfigyelt számológépek levelezését: minden hardver és a rájuk telepített szofvereknek naplózást kell végznük, ide értve a dátumot, az időbélyeget, a forrás és cél címeket és egyéb információkat minden csomagról és/vagy tranzakcióról. A naplóbegyezkéssel dedikált szervereken kell tárolni, és legalább kétheti napotokat 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	Meg kell előzni, hogy a támadók érzékeny adatokhoz szerezenek hozzáférést: Külkéteintően kell beazonosítani és elkülöníteni a kritikus adatokat a belső hálózati felhasználók számára könnyen elérhető információktól. Létre kell hozni egy olyan, többszörli adat besorolási rendszert, ami az adatok illetékletlen kezébe kerülésének hatáson alapú és biztonsági kék, hogy csak azonosított felhasználók kaphatnak hozzáférést a nem publikus adatokhoz és fájlokhoz.	4	Közepes	Függő	Közepes / alacsony	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-4, AC-4, MP-3, RA-2 (a)
16 Hozzáférés ellenőrzés	Meg kell akadályozni, hogy a támadók jogosult felhasználókat személyesítsenek meg: minden felhasználói hozzáférést meg kell szüntetni, amely nem tartozik üzleti (vagy rendszer) folyamatokhoz és nincs feladata. A megadott munkaviszonyú (vagy szerződéses) dolgozók hozzáféréseit azonnali hatállyal meg kell szüntetni. A használaton kívüli hozzáféréseket le kell tiltani és az azokhoz tartozó fájlokat (adatokat) izolálni kell. Megfelelő erősségű jelszavak használatát 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 hálózaton keresztül, illetve fizikai formában ellopjanak: ellenőrizni kell a hálózati határoló eszközökön (proxy/tűzfal) a forgalmat, ezzel a lehető legkisebb kitértéséget 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 új hírnevét és a birtokolt információkat: olyan jól működő és tesztelt incidens-menedzsment rendszert kell kialakítani, mely világosan meghatározza a felelősokat és felelősségeket egy bekövetkező támadás gyors feloldása, a károk minimalizálása, a támadó semlegesítése és a rendszer integrálásának 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 a hálózat rossz szegmentációjával támadókat felületen biztosítson: robosztus, biztonságos hálózati tervezést kell megvalósítani, annak érdekében, hogy a kívülről biztonsági elvárásokat ne legyen megkérülni. Legalább három rétegű hálózati tervezést kell alkalmazni DMZ, belső hálózati és privát hálózati szegmensek. 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	Számoltó behatolástesztek segítségével kell ellenőzni a szervezet reakcióképességét: rendszeres belső és külső behatolás-tesztekkel kell végrehajtani, hogy a rendszerekben található sebezhetőségek napvilágra kerüljenek és hogy a támadásból adódó valós károk felmérhetők legyenek. Belső „Red Team” csoporttal 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)

Hol lehet további információkat találni? Egy (nem teljes) lista az általunk legfontosabbnak tartott forrásokról:



7 ok, amiért a felsővezetők támogatják a szakembereket, akik a 20 Kritikus Kontroll bevezetését végzik:

1. A közreműködők

Egy több, mint 100, megbízható kormányzati szervezetből, magánvállalkozásból és elismert szakértőkből álló közösség biztosítja, hogy a kritikus kontrollok folyamatosan és alaposan frissítve legyenek annak érdekében, hogy segítségükkel hatékonyan lehessen küzdeni a feltűnő fenyegetésekkel. A Consortium for Cybersecurity Action (CCA) néven ismert közösségben többek között az amerikai NSA és a Belbiztonsági minisztérium, a brit Centre for the Protection of National Infrastructure, a Mandiant, a Qualys, a Symantec, a McAfee, az nCircle és a CoreImpact is aktív közreműködő. A CCA-Tony Sager, az NSA sérülékenység-vizsgáló csapatának egykori főnöke vezeti és számos széles körben elismert szakértő támogatja, többek között Ed Skoudis, Dr. Eric Cole, Dr. Johannes Wlirrich és John Pescatore.

2. A kiemelt fontosságú biztonsági intézkedésekre kell koncentrálni

A különböző megfelelési rendszerek szó szerint több ezer biztonsági követelményt tartalmaznak és mindezt egyformán fontosnak tartják. Konszenzus alapján ki kell választani a legnagyobb hasznot jelentő kontroll-területeket és azokra kell összpontosítani elsőként. A kritikus kontrollok a támadás alapú védekezés filozófiája mentén lettek összeállítva, ami az aktuális támadásokról rendelkezésre álló speciális tudás figyelembe vételével, kockázati alapon állít fel hatékony védelmi eljárásokat. Nem próbálnak minden biztonsági problémát megoldani, hanem azokra a lépésekre koncentrálnak, amelyekkel az ismert támadásokat lehet kivédeni. Ez lehetővé teszi a felsővezetők számára, hogy a rendelkezésre álló erőforrásokot költséghatékony módon a legnagyobb érték védelmére fordítsák.

3. Sikerek

A kritikus kontrollok érvényesítésének automatizált és folyamatos ellenőrzésével az amerikai Külgügyminisztérium több, mint 90 %-kal csökkentette az informatikai rendszerek kockázatait.

4. Az alkalmazók

A kritikus kontrollokat számos ország több száz nagyvállalata vezette már be, minden fontosabb szektor lefedve. Többek között kormányzati szervek, pénzügyi és energiaiparkorban tevékenykedő cégek, akadémiai, védelmi, tanácsadó, építőipari, egészségügyi és szállítási vállalatok. Az Amerikai Egyesült Államok Belbiztonsági minisztériuma is bevezette a kritikus kontrollokat és szerződéses támogatást nyújt a szövetségi, állami és helyi hatóságoknak a szükséges technológia implementálásához. A brit Kritikus Infrastruktúrávédelmi Központ (Center for the Protection of National Infrastructure - CPNI) a Kritikus Kontrollokat választotta a kiemelt nemzeti informatikai biztonsági intézkedések és kontrollok alapjául.

5. Ezeket a kontrollokat számos eszköz támogatja

A Kritikus Kontrollok kiválasztása során nem csupán az volt szempont, hogy hatékonyak legyenek a valós fenyegetések elhárításában, de a könnyű automatizálhatóság és a biztonságos folyamatok menedzsmentje is. Tucatnyi biztonsági eszköz szállítja is tagja a CCA-nak, akik a szakértelmükkel segítettek fejleszteni a kontrollokat. Sok más szállító is támogatja a kontrollokat termékekkel és szolgáltatásokkal. Több szállító publikált tanulmányokat ügyfeleiről, akik sikeresen vezették be és tették a napi rutin részévé a kontrollokat, valamint általános leírást adtak arról, hogy a termékek hogyan kapcsolódnak a kontrollokhoz. A vállalkozások számos ingyenes és nyílt forrású megoldást is igénybe tudnak venni.

6. A kontrollok kapcsolata már létező biztonsági keretrendszerekkel

A Kritikus Kontrollok célja kiegészíteni a már létező keret- és megfelelési rendszereket egy közösségi egyetértés alapján történő, kis számú, végrehajtható intézkedést tartalmazó terv kialakításával, amelyek az elérhető legnagyobb biztonsági fejlődést biztosítják a támadások megállítására érdekében. A Kontrollok jól illeszkednek a már meglévő keretrendszerekhez és logikus kitudulási pontokat nyújtanak a nagyobb, átfogóbb keretrendszerekben megvalomázottakban történő megfelelés során. A mérésre és automatizálásra helyezett hangsúlyuk a kontrollok kifejezetten támogatják a folyamatos nyomon követés és dinamikus kibervédelmi eljárások kialakítását.

7. A kontrollok egy végrehajtható tervet kínálnak a biztonság fejlesztésére

A Kritikus Kontrollok bevezetői közül sokan mesélnek hasonló történeteket: a kontrollok felsővezetőknek történő bemutatása gyakran vezetett egy "Vagy úgy"-felismeréshez a biztonság fejlesztésének értékelési kapcsolatban. A kezdeti időben a kontrollokhoz képest meglévő eltérések felmérése biztosítja a kitudulási értékeket. A gyors sikerek demonstrálják, hogy a kontrollok azonnali eredményeket hoznak. A bevezetési ütemterv fejlesztését és jóváhagyását a felsővezetés bevonásával kell elvégezni. Az ütemterv szerinti előrehaladás lesz ezután a jelentési mechanizmus, amely azonosítja az erőforrás-problémákat és támogatja a döntéshozatalt. Ez a megközelítés segít, hogy a fókusz a technológia és az emberi teendő helyett a végrehajtás előrehaladására és irányítására tehető.

A KIBEV alapvetései:

Hazafias kötelességünknek érezzük, hogy informatikai biztonságban megszerzett tudásunkat felajánljuk a haza szolgálatára, hogy Magyarországot az ország kibertérének és kritikus infrastruktúráinak védelmében.

Nem támogatjuk és nem működünk együtt rosszindulatú informatikai tevékenységeket végző vagy azt hirdető, promótáló szervezetekkel, személyekkel. Helytelenülünk a hackerek rosszindulatú tevékenységét és azt károsnak tartjuk a társadalom egészé számára.

Axiomaként – bizonyítás nélkül – elfogadjuk, hogy az országot és annak informatikai infrastruktúráját veszélyeztető kibervegetettség valós és az ellen tennünk kell.

A tagok közé történő jelentkezés önkéntes, a beválasztás nem automatikus. A tagok felveteléről a KIBEV által kijelölt, szűk körű tagság dönt, a későbbi lefelekedendő etikai kódex figyelembevételel.

Belső körünkbe olyan felelős tagokat várunk, akik által üzemeltett rendszerek kiesése érezhető fennakadást jelent az ország működésében.

Feltett szándékunk, hogy a tagok hasznos tartalommal lássák el egymást, kommunikációkban konkrétumokról és egyértelmű szakmai lépésekről beszéljünk.

Fontosnak tartjuk, hogy a tagok között szakmai alapon folya, érdemi viták, eszmecsere alakuljanak ki és ezek tanulságából építkezünk.

