KRITIKUS BIZTONSÁGI KONTROLLOK

kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

A Kritikus Biztonsági Kontrollok olyan intézkedések gyűjteménye, amelyek hatékony és konkrét módszereket kínál a legveszélyesebb és legelterjedtebb kibertámadási formák ellen. A kontrollok fejlesztését, finomhangolását, ellenőrzését és támogatását önkéntes biztonsági szakértők csoportja végzi a Center for Internet Security (CIS) felügyeletével (https://www.cisecurity.org). A hozzájárulók, alkalmazók és támogatók megtalálhatóak a világ minden részén, minden üzleti területen, munkakörben. Állami és helyi önkormányzatok, erőművek és áramszolgáltatók, szállítmányozó cégek, akadémiai intézmények, pénzügyi és szövetségi kormányzati szervezetek, védelmi beszállítók és sokan mások találhatóak a több száz szervezet között, akik a megfelelési-központú megközelítést biztonság-központúra cserélték a Kritikus Biztonsági Kontrollok alkalmazásával. A felsorolt szervezetek a "Mit kell tennünk most annak érdekében, hogy megvédjük a szervezetet a célzott kibertámadásoktól?" kérdésre válaszul váltottak a kontrollok alkalmazására.

A Kritikus Biztonsági Kontrollok nem próbálják helyettesíteni az eddig használt átfogó keretrendszereket (pl. NIST SP 800-53, ISO 27001 stb.), inkább hangsúlyt és prioritást próbál helyezni azokra a gyors sikert hozó intézkedésekre, amiket célszerű elsőként bevezetni. Mivel a kontrollok a leggyakoribb támadási minták alapján kerültek kidolgozásra és az ellenőrzést kormányzati és ipari biztonsági szakemberek széles köre végezte, így megbízható alapját képezik az azonnal bevezethető, gyors sikereket biztosító intézkedéseknek. A szervezetek a kontrollok használatával gyorsan képesek meghatározni védelmi intézkedéseik értékelésénél és fejlesztésénél azokat az azonnal bevezethető és gyors sikereket hozó intézkedéseket, utána pedig erőforrásaikat az üzletileg egyedi kockázatok kezelésére fordíthatják. Ennek hátterében kontrollok támogatást biztosítanak egy nagyszabású, szabványokon alapuló, automatizált kiberbiztonság-menedzsmenthez.

Ez a poszter a 'CIS Controls Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors' című, a szervezet honlapján elérhető esetenként módosított változata, amelyet az Önkéntes Kibervédelmi Összefogás (KIBEV) tagjai fordítottak magyar nyelvre.

A Center for Internet Security (CIS) egy előremutató gondolkodású non-profit szervezet, ami a globális IT közösség erejét felhasználva igyekszik javítani az állami szervek és magánvállalatok IT rendszereit az Internetes fenyegetésektől. A CIS kontrollok és benchmark-ok azok a globális szabványok és széles körben elismert legjobb gyakorlatok, amik a leginkább átfogó védelmet tudják nyújtani az informatikai rendszerek és adatok védelme során. A CIS ezeknek a bizonyított irányelveknek a folyamatos, tapasztalt informatikai szakemberek önkéntes munkája által történő folyamatos frissítését koordinálja. A CIS ad otthont az USA állami, helyi, törzsi és regionális kormányzati szervek kiberbiztonsági információmegosztó és elemző központjának, az MS-ISAC-nek.

A KIBEV ALAPVETÉSEI:

Hazafias kötelességünknek érezzük, hogy informatikai biztonságban megszerzett tudásunkat felajánljuk a haza szolgálatára, hogy Magyarország azt felhasználhassa az ország kiberterének és kritikus infrastruktúráinak védelmében.

Nem támogatjuk és nem működünk együtt rosszindulatú informatikai tevékenységeket végző vagy azt hirdető, promótáló szervezetekkel, személyekkel. Helytelenítjük a hackerekek rosszindulatú tevékenységét és azt károsnak tartjuk a társadalom egésze számára.
Axiomaként – bizonyítás nélkül – elfogadjuk, hogy az országot és annak informatikai infrastruktúráját veszélyeztető kiberfenyegetettség valós és az ellen tennünk kell. A tagok közé történő jelentkezés önkéntes, azonban a beválasztás nem automatikus. A tagok felvételéről a KIBEV által kijelölt, szűkkörű tagság dönt.

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, kommunikációnkban konkrétumokról és egyértelmű szakmai lépésekről beszéljünk és a KIBEV-et szakmai műhelyként működtessük. Fontosnak tartjuk, hogy a tagok között szakmai alapon folyó, érdemi viták, eszmecserék alakuljanak ki és ezek tanulságaiból építkezzünk.

TOVÁBBI INFORMÁCIÓ:

Biztostu.hu
www.biztostu.hu

ICS CYBER SECURITY BLOG
icscybersec.blog.hu

CRYSYS TO BE ON THE SAFE SIDE
www.crysys.hu

saferinternet.hu
www.saferinternet.hu

Egyesült Királyság
CPNI Centre for the Protection of National Infrastructure
www.cpni.gov.uk

Egyesült Államok
CISA CYBER+INFRASTRUCTURE
www.cisa.gov

NEMZETI KIBERVÉDELMI INTÉZET
nki.gov.hu

SANS
sans.org

Kritikus Biztonsági Kontrollok	A kontrollok leírása	A Kritikus Biztonsági Kontrollok és egyes szabványok kapcsolata		
		NIST 800-53	PCI DSS	ISO 27001:2013
Alapvető biztonsági kontrollok: Olyan kontrollok, amelyeket minden szervezetnek használnia kell az alapvető biztonsági felkészültség keretében				
1 Hardvereszköz-leltár és kezelés	Folyamatosan felügyelet alatt kell tartani (leltárba venni, követni, karbantartani és ha kell, javítani) a hálózatban található összes hardver-eszközt, így biztosítva, hogy csak engedélyezett eszközök kaphatnak hozzáférést, a nem engedélyezett és nem felügyelt eszközöket pedig időben észlelni lehet és megelőzni, hogy hozzáférjenek a hálózathoz.	CA-7, CM-8 IA-3, SA-4 SC-17, SI-4, PM-5	2.4	A.8.1.1 A.9.1.2 A.13.1.1
2 Szoftvereszköz-leltár és kezelés	Folyamatosan felügyelet alatt kell tartani (leltárba venni, követni, karbantartani és ha kell, javítani) a hálózatban található összes szoftver-eszközt, így biztosítva, hogy csak engedélyezett szoftvereket lehet telepíteni és elindítani, a nem engedélyezett és nem felügyelt szoftvereket pedig időben észlelni lehet és megelőzni, hogy telepítésre vagy futtatásra kerüljenek.	CA-7, CM-2 CM-8, CM-10 CM-11, SA-4 SC-18, SC-34 SI-4, PM-5		A.12.5.1 A.12.6.2
3 Folyamatos sérülékenység-vizsgálat, ellenintézkedés és megszüntetés	Folyamatosan gyűjteni és értékelni kell az elérhető információkat, amelyekből azonosítani lehet az esetleges sérülékenységeket, kitettségeket, valamint törekedni kell a sérülékenységek csökkkentésére, megszüntetésére, valamint minimalizálni azt az időt, amely egy támadó rendelkezésére áll.	CA-2, SC-34 CA-7, SI-4 RA-5, SI-7	6.1 6.2 11.2	A.12.6.1 A.14.2.8
4 Adminisztrátori és kiemelt jogosultságok ellenőrzött használata	Azok a folyamatok és eszközök, amelyekkel a számítógépeken, hálózatokon és alkalmazásokban használt adminisztrátori és kiemelt jogosultságok használatát, delegálását és módosítását lehet nyomon követni, ellenőrizni és szükség esetén korrigálni.	AC-2, AC-19, IA-4 AC-6, CA-7, IA-5 AC-17, IA-2, SI-4	2.1 7.1, 7.3 8.1, 8.2, 8.3, 8.7	A.12.6.1 A.14.2.8
5 Biztonságos hardver és szoftver beállítások (konfigurációk) mobil eszközökön, laptopokon, munkaállomásokon és szervereken	Szigorú konfiguráció- és változáskezelési eljárásokat alkalmazva létre kell hozni, ki kell kényszeríteni és alkalmazni kell, valamint folyamatosan felügyelni egy biztonságos konfigurációt a laptopok, szerverek és munkaállomások számára annak érdekében, hogy megelőzhessük, hogy a támadók kihasználhassák a sérülékeny szolgáltatásokat és beállításokat.	CA-7, CM-6, CM-11 SC-14, CM-2, CM-7 MA-4, SC-34, CM-3 CM-8, RA-5, SI-2, CM-5, CM-9, SA-4, SI-4	2.2 2.3 6.2 11.5	A.9.1.1, A.9.2.2 A.9.2.3, A.9.2.4 A.9.2.5, A.9.2.6 A.9.3.1, A.9.4.1 A.9.4.2, A.9.2.3 A.9.4.4
6 Karbantartás, figyelemmel követés, ellenőrzés és a biztonsági naplók elemzése	Gyűjteni, kezelni és elemezni kell azokat a naplóbejegyzéseket, amelyek segítségével észlelhetővé és felismerhetővé válnak a támadások, segíthetik a támadás hatásainak csökkentését illetve a helyreállást egy biztonsági incidens után.	AC-23, AU-5, AU-9, AU-13 SI-4, AU-2, AU-6, AU-10, AU-14 AU-3, AU-7, AU-11, CA-7, AU-4, AU-8, AU-12, IA-10	10.1, 10.2 10.3, 10.4 10.5, 10.6 10.7	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1
Elengedhetetlen műszaki kontrollok: Technológiai legjobb gyakorlatok, amik egyértelmű biztonsági előnyöket nyújtanak, elsődleges és okos lépésnek számítanak alkalmazni bármilyen szervezet számára				
7 Elektronikus levelező kliensek és webböngészők védelme	Minimalizálni kell a elektronikus levelezőrendszereken és webböngészőkön keresztül a felhasználókat célzó támadók lehetőségeit és a támadási felületeket.	CA-2, CA-7, CP-4 IA-5, IR-3	4.1, 4.2 6.1, 6.5 8.2 12.3	A.14.2.8 A.16.1.7 A.17.1.3 A.18.2.2 A.18.2.3
8 Rosszindulatú kód elleni védekezés	Felügyelet alatt kell tartani a rosszindulatú programok telepítését, terjedését és futását a szervezet számos pontján, ezzel egyidőben optimalizálni kell a biztonsági rendszerek automatizált frissítési, adatgyűjtési és korrekciós műveleteit.	CA-7, SI-3 SC-39, SI-4 RA-5, SI-7	5.1 5.2 5.3 5.4	A.8.3.1 A.12.2.1 A.13.2.3
9 Korlátozott és ellenőrzött hálózati portok, protokollok és szolgáltatások	Folyamatosan kezelni és kontroll alatt kell tartani (nyomon követni, ellenőrizni és ha kell, javítani) a hálózatban használt portokat, protokollokat és szolgáltatásokat, ezzel csökkentve a támadók lehetőségeit egy sikeres támadásra.	AC-4, CM-6, SC-22 CA-7, CM-8, SC-41 CA-9, SC-20, SI-4 CM-2, SC-21	1.4	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2
10 Adatvisszaállítási képesség	Szigorú konfiguráció- és változáskezelési eljárásokat alkalmazva létre kell hozni, alkalmazni kell és folyamatosan felügyelni egy biztonságos konfigurációt a hálózati infrastruktúra eszközei számára annak érdekében, hogy megelőzhessük, hogy támadók kihasználhassák a sérülékeny szolgáltatásokat és beállításokat.	PR.AC-5 PR.IP-1 PR.PT-4	1.1-1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3
11 Biztonságos hálózati eszköz, tűzfal-, router- és switch konfigurációk	Szigorú konfiguráció- és változáskezelési eljárásokat alkalmazva létre kell hozni, alkalmazni kell és folyamatosan felügyelni egy biztonságos konfigurációt a hálózati infrastruktúra eszközei számára annak érdekében, hogy megelőzhessük, hogy támadók kihasználhassák a sérülékeny szolgáltatásokat és beállításokat.	AC-4, CM-2, CM-8 CA-3, CM-3, MA-4 CA-7, CM-5, SC-24 CA-9, CM-6, SI-4	1.1 1.2 2.2 6.2	A.9.1.2 A.13.1.1 A.13.1.3
12 Határvédelem	Észlelni, megelőzni, szükség esetén javítani kell azokat az eseményeket, amelyek kárt okozhatnak a különböző megbízhatósági szintű hálózatok között közlekedő adatfolyamokban.	AC-4, CA-7, SC-7 AC-17, CA-9, SC-8 AC-20, CM-2, SI-4 CA-3, SA-9	1.1, 1.2, 1.3 8.3, 10.8 11.4	A.9.1.2, A.13.1.1 A.12.4.1, A.13.1.3 A.12.7.1, A.13.2.3
13 Adatvédelem, adatszivárgás elleni védelem	Azok a folyamatok és eszközök, amelyekkel meg lehet előzni vagy csökkenteni lehet az adatok eltulajdonításából eredő károkat, ezzel biztosítva az érzékeny adatok bizalmasságát és sértetlenségét.	AC-3, CA-9, SC-8, SI-4 AC-4, IR-9, SC-28 AC-23, MP-5, SC-31 CA-7, SA-18, SC-41	3.6 4.1 4.2 4.3	A.8.3.1 A.10.1.1-A.10.1.2 A.13.2.3 A.18.1.5
14 Hozzáférés-kezelés a „szükséges-elégséges tudás" elve alapján	Azon folyamatok és eszközök, amelyekkel nyomon lehet követni, ellenőrizni és szükség esetén korrigálni lehet a hozzáféréseket a kritikus fontosságú eszközökhöz (adatok, erőforrások, rendszerek stb.). A szervezeten belüli formális folyamat alapján szükséges meghatározni, hogy az egyes személyeknek, számítógépeknek és alkalmazásoknak milyen hozzáférésekre, jogosultsági szintekre van szükségük.	AC-1, AC-6, RA-2 AC-2, AC-24, SC-16 AC-3, CA-7, SI-4 MP-3	1.3, 1.4 4.3 7.1, 7.2, 7.3 8.7	A.8.3.1 A.9.1.1 A.10.1.1
15 Vezeték nélküli eszközök felügyelete	Ide tartoznak mindazok a folyamatok és eszközök, amelyekkel követni, ellenőrizni, megelőzni, javítani lehet és ki lehet alakítani a vezeték nélküli hálózatok, hozzáférési pontok és vezeték nélküli kliensek biztonságát.	AC-18, CA-7, SC-17 AC-19, CM-2, SC-40 CA-3, IA-3, SI-4 SC-8	4.3 11.1	A.10.1.1 A.12.4.1 A.12.7.1
16 Hozzáférés felügyelet és ellenőrzés	Az életciklus-modell alapján folyamatosan kezelni és ellenőrizni kell a rendszer- és alkalmazás-felhasználókat, a létrehozásuk, használatuk, inaktív állapuk és törlésük során egyaránt, annak érdekében, hogy minimalizáljuk a támadók lehetőségeit, hogy ezeken a felhasználókon keresztül hajtsanak végre támadásokat.	AC-2, AC-12, SC-17 AC-3, CA-7, SC-23 AC-7, IA-5, SI-4 AC-11, IA-10	7.1, 7.2, 7.3 8.7, 8.8	A.9.1.1 A.9.2.1-A.9.2.6 A.9.3.1 A.9.4.1-A.9.4.3 A.11.2.8
Szervezeti kontrollok: Ezek a kontrollok a szervezet kiberbiztonsági folyamataira és az azokban résztvevő emberekre koncentrálnak				
17 Biztonságtudatossági ismeretek fejlesztését célzó képzések bevezetése	A szervezeten belül minden szerepkör számára (elsősorban az üzletileg kritikus szerepköröknek) azonosítani kell azokat a képességeket és tudást, amelyek ahhoz szükségesek, hogy meg lehessen védeni a szervezetet. Ki kell dolgozni és végre kell hajtani egy integrált tervet, amely értékeli a jelenlegi helyzetet, feltárja a hiányosságokat és szabályzatokon, szervezeti szintű terveken képzéseken és biztonságtudatossági oktatásokon keresztül javítja, valamint csökkenti a gyenge pontokat.	AT-1, AT-4, PM-13 AT-2, SA-11, PM-14 AT-3, SA-16, PM-16	12.6	A.7.2.2
18 Alkalmazásszoftverek biztonsága	Folyamatos felügyelet alatt kell tartani a biztonsági életciklusát minden egyedileg fejlesztett és vásárolt szoftvernek annak érdekében, hogy megelőzhető, észlelhető és javítható legyen minden ismert biztonsági hiányosság, gyengeség.	SA-13, SA-20, SI-11 SA-15, SA-21, SI-15 SA-16, SC-39, SI-16 SA-17, SI-10	6.3 6.5 6.6 6.7	A.9.4.5 A.12.1.4 A.14.2.1, A.14.2.6 A.14.2.7, A.14.2.8
19 Incidensek kezelésének képessége	Incidenskezelési környezet (tervek, szerepkörök, képzések, kommunikációs eljárások, felsővezetői felügyelet) kialakításával és bevezetésével védeni kell a szervezet adatait és jó hírnevét. Ezekkel az intézkedésekkel biztosítható, hogy egy támadást gyorsan fel ismerhető legyen és utána hatékonyan megelőzhető a károkozás, felszámolhatóvá válik a támadó jelenléte a szervezet informatikai rendszereiben és helyreállítható a hálózat és a rendszerek integritását.	IR-1, IR-4, IR-7 IR-2, IR-5, IR-8 IR-3, IR-6, IR-10	12.10	A.6.1.3, A.7.2.1 A.16.1.2, A.16.1.4 A.16.1.5, A.16.1.6 A.16.1.7
20 Behatolás tesztek és „Red Team" gyakorlatok	A támadók céljait és módszereit szimulálva tesztelni kell a szervezet általános védekező-képességét (technológiát, folyamatokat és embereket egyaránt).	CA-2, CA-8, PM-6 CA-5, RA-6, PM-14 CA-6, SI-6	11.3	A.14.2.8 A.18.2.1 A.18.2.3

ÖT KULCSTEVÉKENYSÉG A HATÉKONY KIBERBIZTONSÁGI PROGRAM KIALAKÍTÁSÁHOZ:

1. A megfelelő keretrendszer kiválasztása: Olyan biztonsági keretrendszert érdemes választani, ami támogatja a szervezet tevékenységét, a biztonsági program megvalósítását és a kiberbiztonság összetett világának egyszerűsítésével segíti, hogy az üzleti területek vezetői megértsék a kiberbiztonsági programot.
2. A kontrollok és a keretrendszer összehangolása: A kiberbiztonsági keretrendszereket lehet együtt is alkalmazni. Ez a poszter a Kritikus Biztonsági Kontrollokat rendeli össze az NIST, a PCI DSS és az ISO 27001 kiberbiztonsági keretrendszerekben leírt kategóriákkal és funkciókkal.
3. Kockázatelemzés és kezelés: A kontrollok és keretrendszerek mentén vázolt tevékenységeken túl meg kell határozni, hogy melyik képességek és tevékenységek mennyire fontosak a szervezetnek.
4. Érettség és előrehaladás mérése: Kockázat-alapú megközelítéssel priorizálni kell a biztonsági kontrollokat az elvárt állapot elérése érdekében. Egy ütemterv kidolgozása lehetővé teszi az érettség és az előrehaladás időbeli mérését.
5. A biztonság ellenőrzése és mérése: A hatékony biztonsági intézkedések folyamatos fejlesztéséhez
   - létre kell hozni és alkalmazni kell a megfelelő biztonsági mutatókat;
   - megfelelő gyakorisággal ellenőrizni kell ezeket a mutatókat, hogy minimalizálni lehessen az incidensek negatív hatásait;
   - gyors és hatékony lépéseket kell tenni a biztonság általános szintjének javítása érdekében.

Egy operációs rendszernek több mint 200 biztonsági beállítási kombinációja lehet, és az internetes támadások, valamint a biztonsági esettanulmányok mindig azonos következtetésre jutottak, miszerint a rossz konfigurációs (beállítási) döntések és a kezelésük jelentősen hozzájárulnak sikeres támadásokhoz.
Ezenkívül minden megfelelő biztonsági keretrendszer megköveteli a biztonságos konfigurációt a végponti rendszereken.

CIS Benchmarks a legjobb gyakorlatokat írja le a végponti biztonságos konfigurációval kapcsolatosan.

Több mint száz különféle technológiára alkalmas biztonsági útmutatót tartalmaz, amelyet egy egyedülálló módon, konszezuson alapúló folyamat útján fejlesztettek ki kiberbiztonsági szakemberek és szakértők segítségével.
Az operációs rendszereket bemutató példák az egyetlen konszenzuson alapuló, a bevált gyakorlatokkal kapcsolatos biztonsági konfigurációs útmutató, amelyet mind a kormány, az üzleti, az ipar és a tudományos élet által kidolgozott és elfogadott.

További információkat talál a https://www.cisecurity.org/cis-benchmarks weboldalon.

A kiberbiztonság a vezetés minden szintjét bevonja

Felfelé haladva a ranglétrán az üzleti tudás növekszik

Lefelé haladva a ranglétrán a technikai tudás növekszik

FELSŐVEZETŐ
Fókuszban
az üzleti célok
Szerepek
Board - CEO, CFO, CIO
CISO, CSO, Business units

BIZTONSÁGI VEZETŐ
Fókuszban
a biztonsági program
Szerepek
CISO, CSO, CIO, CIRO, VP, igazgató

BIZTONSÁGI MENEDSZER
Fókuszban
a technológia irányítás
Szerepek
technikai igazgató, menedszer, csoportvezető

TECHNIKAI
Fókuszban
a technológia
Szerepek
biztonsági mérnök, biztonsági elemző

CIS RAM

CIS Kockázatkezelési módszertan (CIS RAM) segít nekünk olyan kérdések megválaszolásában, mint „Mennyi biztonság elég?" és „Mit jelent az alapos gondosság, vagy a józan ész elve".

A CIS RAM egy hatékony eszköz a CIS-kontrollok priorizálásának és végrehajtásának irányításához és kiegészíti a technikailag releváns információkkal az üzlet számára kritikus kockázati döntési folyamatot. Úgy tervezték, hogy összhangban álljon az ismert biztonsági keretrendszerekkel és a hozzájuk kapcsolódó kockázatértékelési módszerekkel. A CIS RAM lehetővé teszi a változó biztonsági érettségű szervezetek számára az egyensúly megalkotását a biztonsági ellenőrzések, a kockázatok és a szervezeti igények végrehajtása között. A CIS RAM központi eleme a Duty of Care kockázatelemzés (DoCRA) módszertana, amely lehetővé teszi a szervezeteknek, hogy mérlegeljék az ellenőrzések végrehajtásának elmulasztásával járó kockázatokat és a szervezetet esetlegesen terhelő tényezőket.