kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

INTÉZKEDÉS-GYŰJTEMÉNY
AZ IPARI RENDSZEREK KIBERBIZTONSÁGÁNAK FEJLESZTÉSÉHEZ

Ez az intézkedés-gyűjtemény az Amerikai Egyesült Államok Energiaügyi Minisztériuma (Department of Energy, DoE) által kiadott, "21 Steps to Improve Cyber Security of SCADA Networks" című kiadványán alapul. A DoE kiadványát mi, az Önkéntes Kibervédelmi Összefogás (KIBEV) tagjai dolgoztuk át és alkalmaztuk a magyar viszonyokra. Az eredeti 21 intézkedést további 5, általunk hasznosnak ítélt intézkedéssel egészítettük ki.

A különböző ipari (ICS) és folyamatirányító (SCADA) rendszerek a modern ipari társadalmak zavartalan működésének nélkülözhetetlen eszközei és mint ilyenek, részei a nemzeti kritikus infrastruktúrának is. Emiatt elengedhetetlen, hogy megfelelő szintű védelemmel rendelkezzenek a kibertérből származó (és egyre gyakorabban támadásban manifesztálódó) fenyegetésekkel szemben.

Történeti okokból az ICS rendszerek fejlesztése hosszú évtizedeken át a teljesítmény-maximalizálásra és a vezérlési funkciók közel 100%-os rendelkezésre állására koncentrált - így az információbiztonság sajátos szempontjai csak alacsony prioritást kaptak. Következményeként napjainkban az ICS rendszerek sokkal több súlyos sérülékenységet hordoznak, mint az átlagos üzleti szoftverrendszerek. Márpedig a sérülékenység olyan beépített rendszerhiba, amelynek javítására csak akkor kerül sor, ha egy-egy támadás során kihasználják. Emiatt a sérülékenységi hibák észlelése, majd javítása is sokkal több időt, munkát igényel az ICS rendszerek fejlesztőitől, üzemeltetőitől.

Poszterünk összegyűjti azokat az intézkedéseket, amelyek alkalmazásával jelentős kockázat csökkenés érhető el a különböző ipari rendszerek működtetésében. Ahol lehet, intézkedési javaslatainkat összekapcsoljuk a KIBEV által az elmúlt években több lépcsőben finomított "Kritikus Biztonsági Kontrollok" kiadványunkban megfogalmazott kontrollokkal.

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, 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, a beválasztás nem automatikus. A tagok felvételéről a KIBEV által kijelölt, szűkkörű tagság dönt, a később lefektetendő etikai kódex figyelembevételével.

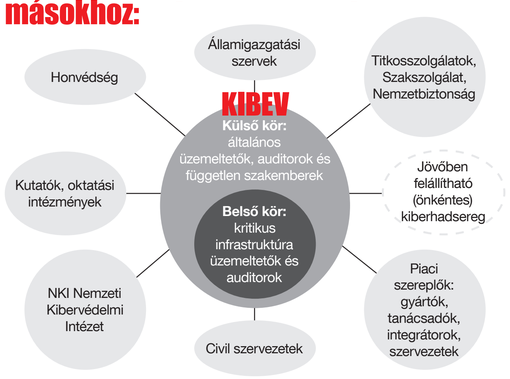
Belső körünkbe olyan felelős tagokat várunk, akik által üzemeltett rendszerek kiesése érezhető fennakadást jelent az ország működésében.

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

Fontosnak tartjuk, hogy a tagok között szakmai alapon folyó, érdemi viták, eszmecserék alakuljanak ki és ezek tanulságaiból építkezzünk.

További információkat a www.kibev.hu címen lehet találni.

A KIBEV felépítése és kapcsolódása másokhoz:



		Intézkedés megnevezése	Intézkedés rövid leírása	Kapcsolódó Kritikus Biztonsági Kontrollok
ICS hálózatok biztonságát javító intézkedések	1	ICS hálózatok kapcsolatainak azonosítása	Szigorú kockázatelemzéssel kell felülvizsgálni az ICS hálózat külső kapcsolatait. Értékelni kell az egyes kapcsolatok kockázatait (pl. szükségességét). Az elemzésnek vizsgálni kell, hogy az egyes kapcsolatok milyen üzleti/technológiai célokat szolgálnak és védelmük (ha van) arányos-e a célokkal.	CIS-CSC 1, 7, 15
	2	Az ICS hálózatok nem feltétlenül szükséges kapcsolatainak megszüntetése	Az ICS hálózatok kapcsolatainak beazonosítása és kockázat értékelésére alapozva meg kell szüntetni az ICS rendszerek nem létfontosságú külső hálózati kapcsolatait.	CIS-CSC 7, 9, 15
	3	Az ICS rendszerek hálózati kapcsolatainak megerősítése	Sérülékenység vizsgálattal vagy behatolás tesztekkel fel kell tárni az ICS rendszer külső hálózati kapcsolatainak biztonsági réseit. A kockázatelemzés eredményének ismeretében gondoskodni kell a rések elzárásáról és szükség szerint további biztonsági intézkedésekről.	CIS-CSC 7, 11, 15
	4	ICS rendszerek megerősítése	Sérülékenység vizsgálattal vagy behatolás tesztekkel fel kell tárni az ICS rendszerek biztonsági hiányosságait és ezeket a kockázatelemzés eredményéhez igazítva kell kezelni, szükség esetén a megfelelő biztonsági intézkedésekkel vállalható szintre kell csökkenteni a kockázatokat (pl. nem létfontosságú szolgáltatások letiltása, nem szükséges szoftverek/csomagok eltávolítása, törvényi vagy előírási megfelelés során is a biztonságos kialakítás szem előtt tartásával, stb.).	CIS-CSC 1, 2, 3
	5	A rendszer biztonságát nem szabad titkos protokollokra építeni	Az egyedi, a gyártó tulajdonát képező ICS protokollok használata nem teszi biztonságosabbá az ICS rendszereket. Nem szabad csak erre hagyatkozni. Legyen elvárás az ICS rendszer forgalmazójával szemben, hogy a használt ICS rendszerekben nyiltan tárjon fel minden gyártói/support interfészt és beégetett support hozzáférést.	CIS-CSC 11
	6	Az ICS eszközök és rendszerek gyártói/forgalmazói által támogatott biztonsági funkciók tényleges alkalmazása	A régebbi ICS rendszerekkel szemben egyes újabb fejlesztésű rendszerek már beépített biztonsági funkciókat is tartalmaznak. Ezek többségét kényelmi okoból alapértelmezés szerint gyakran kikapcsolják. A használt ICS rendszerek dokumentációja és a termék support felvilágosításai alapján fel kell mérni, hogy milyen beépített biztonsági funkciókkal működtethetők az egyes ICS eszközök. Ezeket milyen beállításokkal lehet használni. Meg kell találni azokat a beállításokat, amelyekkel az ICS funkciók sérülése és teljesítmény csökkenése nélkül a lehető legmagasabb biztonsági szint érhető el és ezeket a beállításokat használni is kell.	CIS-CSC 6
	7	Erős kontrollok bevezetése minden ICS hálózati hozzáférés esetén	Azoknál az ICS rendszereknél, ahol nem megoldható a gyártói/support interfészek, beégetett felhasználói fiókok letiltása, gondoskodni kell a kommunikációs csatornák biztonságossá tételéről. Többszintű védelem kialakítása javasolt, többszörös autentikáció, több átjáró alkalmazása.	CIS-CSC 5, 14, 16
	8	Behatolás észlelő és incidens-monitoring rendszerek/ szakemberek alkalmazása	Az ICS rendszereket érő támadások hatékony kezelésére IDS és SIEM rendszerekkel célszerű felügyelni az ICS üzemet és az ezektől érkező jelzések követésére szakembereket kell alkalmazni.	CIS-CSC 19
	9	Rendszeres műszaki auditok végrehajtása	Az elvárt biztonsági szint folyamatos fenntartásában kritikus szerepe van az ICS rendszerek műszaki auditálásának. Az ICS audit alapvetően azonos a más informatikai rendszerauditokkal. Ugyanúgy része a sérülékenység vizsgálat, a kockázat elemzés, a feltárt hiányosságok felszámolására tett javaslatok kidolgozása és a megtett intézkedések hatásosságának visszaellenőrzése (az audit ismétlése). Itt azonban figyelni kell arra, hogy az audit hatással lehet az ICS rendszer teljesítményére. Minden vizsgálat válaszidő-növekedéssel járhat és ez egyes kritikus esetekben nem elfogadható. Tehát az ICS rendszerauditot — az összes szempontot szem előtt tartva — a lehető legnagyobb körültekintéssel szabad csak végezni.	CIS-CSC 4
	10	Az ICS rendszer távoli telephely kapcsolatainak biztonsági felülvizsgálata rendszeres fizikai biztonsági ellenőrzéssel	Rendszeresen fel kell mérni és értékelni kell a távoli telephelyeket és a telephelyek fizikai biztonságát. Különösen, ha ott egyes ICS rendszer-elemek üzemelnek, ti. minden ilyen fizikai hely hozzáférést biztosíthat az ICS hálózathoz. Az egyes helyszínek biztonsági állapotának állandónak (legalább érintetlennek) kell maradni ahhoz, hogy megelőzhető vagy észlelhető legyen egy onnan kezdeményezett jogosulatlan hozzáférés. Lehetőleg kerüljük az állandó személyzet nélküli ICS telephelyek létesítését vagy olyan hálózati telephelyek fenntartását, amelyek kiegészítő biztonsági intézkedések nélkül üzemelnek (pl. port security nélkül).	CIS-CSC 17
	11	ICS Red Team létrehozása a lehetséges támadási vektorok azonosítására és értékelésére	A megfelelő szaktudással rendelkező szakemberekből (ICS üzemeltetők, IT biztonsági szakértők, etikus hackerek, stb.) “Red Team”-et kell felállítani. Olyan csapatot, amely képes az ICS rendszerben vagy annak hálózatában potenciális támadási vektorokat azonosítani. Az ICS rendszer üzemeltetőinek tudását (pl. a Red Team “támadók” ellen gyakorlatozva) olyan támadási formák azonosítására használhatjuk, amelyek egy sérülékenység vizsgálat vagy egy behatolás teszt során nem kerülnének felszínre.	CIS-CSC 20
Kiberbiztonsági program javítását célzó vezetői intézkedések	12	A vezetők, a rendszeradminisztrátorok és a felhasználók kiberbiztonsági szerepeinek, felelősségeinek és jogainak egyértelmű meghatározása/elkülönítése	Egyértelműen (az összeférhetetlenségek kizárásával) meg kell határozni a szervezet munkatársaival szemben támasztott biztonsági elvárásokat, felelősségi köröket, valamint a szerepköröket el kell választani egymástól. Az elvárt biztonsági szint kijelölésével és fenntartásával megbízott személyeknek elegendő jogosultságot kell kapni a feladatuk ellátásához. Elkerülve ezzel a egyedi megfontolások alapján született biztonsági szabályokat és eljárásokat. Az egyedi szabályozásra ugyanis inkább a kivétel, semmint a szabály a jellemző, amelyek szétzilált megvalósításhoz és hatástalan működéshez vezetnek. Ki kell alakítani a kiberbiztonság szervezeti struktúráját: meghatározva az egyes szerepeket, jogokat és felelősségeket, egyértelműsítve az incidensek vagy egyéb vészhelyzetek riasztási láncait, feladatait.	-
	13	A hálózati architektúra meghatározása és ezen belül a kritikus üzleti folyamatok-, az érzékeny információ tároló rendszerek azonosítása	Egy hatékony védelmi stratégia kialakításához robosztus (és jól dokumentált) információbiztonsági rendszer szükséges. Elengedhetetlen, hogy már az IT és ICS hálózatok tervezése és kialakítása során is folyamatosan szem előtt tartsuk a biztonsági megfontolásokat. A hálózat felépítését és működését a teljes életciklusra vetítve kell átlátni, érteni. Enélkül lehetetlen megfelelő kockázatelemzést végezni és a védelmi intézkedések sem lehetnek hatékonyak.	CIS-CSC 1, 2
	14	Szigorú és minden részletre érzékeny kockázatkezelési folyamat kialakítása	Egy hatékony kiberbiztonsági program működtetéséhez elengedhetetlen az átfogó és részletekbe menő kockázat elemzés. Csak a kockázat elemzés képes megalapozni a sérülékenységek negatív hatásainak csökkentését és képes megőrizni a rendszer integritását. Kiindulásként a jelen (az összes ismert) fenyegetések kockázat elemzését célszerű elkészíteni, majd erre építve egy folyamatos kockázat értékeléssel lehet elérni, hogy az ICS rendszerbeli változások dacára hatásosak maradjanak biztonsági intézkedéseink.	CIS-CSC 4, 20
	15	Mélységi védelmen alapuló hálózatbiztonsági stratégia kialakítása	A hálózatbiztonsági intézkedések kidolgozásakor általános alapelv legyen a mélységi védelem kialakítása és fenntartása. A mélységi védelem koncepcióját a leendő biztonsági intézkedések hatékonysága érdekében már a hálózat és az ICS rendszer tervezése során be kell építeni. Célszerű a hálózat és az ICS rendszer minden szintjén műszaki és adminisztratív kontrollokat alkalmazni, hogy a kockázatokat a lehető legnagyobb mértékben sikerüljön csökkenteni.	CIS-CSC 8, 12
	16	A kiberbiztonsági követelmények egyértelmű meghatározása	Az egyes ICS rendszereket üzemeltető szervezeteknek formalizált szabályzatok és eljárások kialakításával kell meghatározniuk a struktúrált biztonsági programok elvárás- és felelősségi rendszerét. Egy formalizált biztonsági program elengedhetetlen egy következetes, szabványokon alapuló kiberbiztonsági rendszer megteremtéséhez. Amely rendszer a szervezet egészére nézve következetes, szabály vezérelt és képes kiküszöbölni az egyedi, a személyes kezdeményezésekre alapuló biztonsági intézkedéseket, valamint mindenki számára egyértelmű felelősségi- és jogköröket határoz meg. Az ilyen rendszer intézkedései segítenek minimalizálni a bennfenntes, vagy belső szabálysértők jelentette kockázatokat.	-
	17	Hatékony konfigurációkezelési folyamat kialakítása	A kívánt hálózatbiztonsági szint fenntartásához nélkülözhetetlen egy jól működő konfiguráció kezelés fenntartása. Az ilyen konfiguráció kezelés egyaránt lefedi a hardveres és szoftveres változások kezelését. Olyan folyamatokat kell kialakítani, amelyek képesek érzékelni, értékelni és kontrollálni a változás igényeket, és a változások üzleti, biztonsági hatása megjelenik a folyamatban. Ehhez az első lépést az alaposan tesztelt és jól dokumentált biztonsági alapkonfigurációk jelentik.	CIS-CSC 3, 11
	18	Rendszeres önértékelés elvégzése	Robosztus teljesítmény értékeléssel kell gondoskodni a kiberbiztonsági szabályok hatékonyságáról és külön azok műszaki megvalósításának hatékonyságáról. Ehhez rendelkeznünk kell az önértékelés képességével. A legkedvezőbb hatást az önértékeléssel azonosított problémák és azok alapvető okainak megtalálásával érjük el és képesek vagyunk végrehajtani az ezeket javító intézkedéseket. Az önértékelési folyamatnak szerves része kell legyen a rendszeres sérülékenység vizsgálat, az automatizált hálózat-audit, valamint a szervezeti és egyéni teljesmény vizsgálat.	CIS-CSC 4, 17
	19	Mentési- és katasztrófa-elhárítási terv kialakítása	Olyan katasztrófa-elhárítási tervet kell készíteni, amely lehetővé teszi egy vészhelyzet (pl. kibertámadás) esetén a normál működés minél gyorsabb helyreállítását. A mentések nélkülözhetetlen részét képezik minden ilyen tervnek. A katasztrófaelhárítási tervet rendszeresen tesztelni kell, ezzel biztosítva, hogy működni fognak egy valódi vészhelyzetben is és a munkatársak rutinszerűen ismerjék a terv rájuk vonatkozó részeit. A tesztelések eredményei alapján a katasztrófa-elhárítási tervet rendszeresen felül kell vizsgálni és a szükséges módosításokat át kell vezetni rajta, valamint a változtatást is tesztelni szükséges.	CIS-CSC 10
	20	A kiberbiztonsággal és az egyéni felelősség vállalással kapcsolatos (felső)vezetői elvárások megfogalmazása	A hatékony kiberbiztonság kialakításához nélkülözhetetlen a szervezet (felső)vezetésének elkötelezettsége és támogatása. A (felső) vezetőknek világosan kell meg fogalmazniuk a szilárd biztonsággal kapcsolatos elvárásaikat és ezt a beosztott vezetőkön keresztül az egész szervezet felé kommunikálniuk kell. Szintén elengedhetetlen, hogy a (felső)vezetés olyan szervezetet alkosson a kiberbiztonsági program megvalósítására, amely biztosítja a program következetes megvalósítását, fenntartását. A vezetőknek el kell érniük, hogy a szervezet minden tagja ismerje, napi munkája során használja és vállalja a maga felelősségét a kiberbiztonság fenntartásáért.	-
	21	Az ICS rendszeradatok kompromittálódásának megelőzésére szolgáló rendszabályok bevezetése	Gondoskodni kell arról, hogy az ICS rendszeradatokat csak az arra kifejezetten dokumentáltan feljogosított személyek ismerhessék meg, biztosítva ezáltal, hogy egy lehetséges “social engineering” támadás minél kisebb eséllyel legyen kivitelezhető. Tilos az ICS rendszer- vagy hálózati adatokat közzétenni, vagy ha a közzétételt jogszabály írná elő, akkor mentességet kell kieszközölni a közzététellel szemben. Ugyancsak tilos közzétenni az ICS rendszer üzemeltetők adatait. Rendszeres képzéssel gondoskodni kell az ICS rendszer használók (fejlesztők, üzemeltetők, felhasználók, biztonságiak) biztonság-tudatosságának fenntartásáról.	CIS-CSC 13
További intézkedések	22	Kizárólag az engedélyezett alkalmazások futtatása	Az ICS/SCADA rendszerek nagyfokú statikusságára alapozva olyan szoftver megoldást kell használni, amely biztosítja, hogy csak az engedélyezett alkalmazások legyenek a rendszeren futtathatók, végrehajthatók!	CIS-CSC 2
	23	Titkosított adatátviteli protokollok alkalmazása	Biztosítani kell - amennyiben ez műszakilag lehetséges -, hogy az ICS/SCADA rendszerek minden belső és külső adatcseréje titkosítva, vagy titkosított csatornán bonyolódjon! Ezzel megelőzve, hogy bizalmas adatok (pl. felhasználói azonosítók vagy jelszavak) illetéktelenek kezébe kerüljenek.	CIS-CSC 11
	24	Incidens kezelési eljárás kidolgozása és gyakorlása	Az ICS/SCADA rendszerek üzembiztonságával és rendelkezésre állásával kapcsolatban számos jó BCP/DRP terv létezik és általában az üzemeltető szervezetek ezeket rendszeresen ellenőrzik is. Ugyanilyen szintű kiberbiztonsági incidenskezelési eljárást kell kidolgozni és rendszeresen gyakorolni (pl. behatolás-védelemre vagy red team gyakorlatokhoz).	CIS-CSC 18
	25	Több faktoros azonosítás alkalmazása	Kiemelt fontosságú, hogy az ICS/SCADA rendszerekhez - ahol ez műszakilag megoldható - több faktoros azonosítást rendszeresítsünk. Ha ez nem lehetséges, akkor legalább az ICS/SCADA rendszer hálózati hozzáféréseit célszerű többfaktoros azonosítással megerősíteni.	CIS-CSC 20
	26	Az ICS hálózatban üzemelő eszköz-jelszavak rendszeres cseréje	Erős hozzáférési kontrollok és jelszópolitika kialakításáról és alkalmazásáról kell gondoskodnunk az ICS/SCADA rendszer üzemében. Ezt a kiszolgáló távközlési hálózat olyan elemeinél kényszeríthetjük ki, mint a tűzfalak, aktív hálózati határok, stb. Továbbá szükségszerű az aktív hálózati elemeket felügyelő management rendszer erős kontrollja (pl. gondoskodni kell az aktív hálózati elemek alapértelmezett jelszavainak módszeres átállításáról).	CIS-CSC 12, 15

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

ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
ics-cert.us-cert.gov

SIEMENS
www.siemens.com/cert/en/cert-security-advisories.htm

CONTROL
PROMOTING EXCELLENCE IN PROCESS AUTOMATION
www.controlglobal.com/blogs/unfettered

SANS Industrial Control Systems
ics.sans.org/blog

ICS CYBER SECURITY BLOG
icscybersec.blog.hu