15. Hírlevél az ipari irányító rendszerek biztonságáról

A Black Cell elkötelezett az ipari irányító rendszerek (Industrial Control Systems – ICS), és/vagy kritikus infrastruktúrák biztonságának megteremtésében, ezért havonta hírlevelet bocsát ki a témában. A hírlevélben az érintett szervezetek, illetve kritikus infrastruktúra üzemeltetők tájékozódhatnak, valamint információkat nyerhetnek az ipari irányító rendszerek sérülékenységeiről; jó gyakorlatokról; a témát érintő képzésekről, oktatásokról, és konferenciákról; az ipari irányító rendszerek üzemeltetőit ért incidensekről. Az ipari irányító rendszerek biztonságáról szóló könyveket is ajánlunk, lehetőség szerint online elérhetőséggel. A Black Cell javaslatokat, megoldásokat kínál az ipari irányító rendszerekhez kapcsolódó tevékenységek hatékony elvégzéséhez, és ezáltal a biztonság minél magasabb szintű megteremtéséhez. A hírlevélben foglaltakkal kapcsolatosan bővebb információért forduljon bizalommal a cara (kukac) blackcell.hu e-mail címen szakértőinkhez.

Tartalom:

ICS jó gyakorlatok, javaslatok

2020. áprilisában a villamos-energia alágazat idő tényezőtől való függőségéről adott ki az ENISA (Európai Hálózat- és Információbiztonsági Ügynökség) egy publikációt. A dokumentum címe: Power sector dependency on time service.

A dokumentum bemutatja azokat a technológiákat, amelyek az idő mérését hivatott szolgálni, továbbá szcenáriókat ad meg, amelyek során az idő tényezőnek nagy jelentősége van.

A szcenáriók során bemutatásra kerülnek az architektúrák, valamint a fenyegetések és kockázatok, illetve a hipotézis, amely az adott szcenárió során a fenyegetés megvalósulását, és a támadási vektorokat mutatja be.

A bizalmasság, sértetlenség és rendelkezésre állás követelményeinek sérüléseit bemutató szcenáriókat a villamos-energia alágazati szereplőknek javasolt megvizsgálni, és az azonosított kockázatokat követően a mitigáló intézkedéseket implementálni a szervezet kockázatmenedzsment rendszerében meghatározott eljárások figyelembevétele mellett.

A dokumentumban a hatások és a szcenáriók bekövetkezési valószínűségei is értékelésre kerülnek, ezzel is segítve az érintett szervezetek munkáját. Az adott kockázatok kezelésére jó gyakorlatokat is megoszt a publikáció, bizonyos technikai részleteket is bemutatva.

A dokumentum utolsó részében kihívásokat és ajánlásokat mutat be az ENISA. A kihívások a következők:

1. Beépíthető zavarás gátló komponensek hiánya
2. Védeni kell a bázis állomásokat a csalásokkal szemben
3. Hálózati biztonsági intézkedések hiánya az adatátvitel biztonságának szavatolására
4. Alacsony szintű rendelkezésre álló szabvány
5. Az ellenálló képesség és a hibák automatikus észlelésének hiánya

Az ajánlások, melyeket a kihívások kezelésére fogalmaz meg a dokumentum, a következők:

1. A gyártóknak fejleszteni szükséges olyan, az alállomások automatizálását célzó eszközöket, amelyek a biztonságot szem előtt tartva a zavarásgátló komponenseket is tartalmazzák.

2. Az üzemeltetőknek elektronikus periméter implementálással kell felkészülni a csalások elleni védelemre, például jelfeldolgozási technikák alkalmazása a szinkronizáció védelmének biztosítására. Az üzemeltetőknek olyan technológiát szükséges alkalmazni, amely képes az adatok elleni spoofing támadások észlelésére (GPS időbélyegek alkalmazása).

3. Az üzemeltetőknek alkalmazni szükséges a hálózati szegregációt, a hálózatok és protokollok védelme érdekében, illetve megfelelő adatszűrési technológiát kell alkalmazni, és a hozzáférési szabályokat megfelelően kell kialakítani. Közbenső szűrőként kell alkalmazni a tűzfalakat és az ipari vezérlőket. A hálózat védelme érdekében funkcionális ellenőrzési mechanizmust is be lehet építeni a rendszerbe.

4. A modern okoshálózatok automatizálásához nincs meg a szükséges szabványkörnyezet, amely elősegíthetné a megfelelő tanúsítással a kívánt cél elérését. Az üzemeltetőknek olyan megoldásokat kell implementálni, amelyek általánosan elfogadott követelményeknek megfelelnek. Ezen gyakorlat elősegítheti a megfelelő szabványkörnyezet kialakulását.

5. Az átviteli és az elosztási rétegek automatikusan ellenőrzik a villamos-energia hálózatot valós idejű PMU mérésekkel. Ehhez azonban felügyeleti folyamatok szükségesek. Az üzemeltetőknek eszközöket és eljárásokat kell alkalmazni, hogy javítsák a hálózat ellenálló képességét, a rossz indulatú-, befecskendezett adatokkal szembeni védelem kialakítása érdekében.

A Power sector dependency on time service dokumentum megtalálható a következő linken:

https://www.enisa.europa.eu/publications/power-sector-dependency

ICS képzések, oktatások

A teljeség igénye nélkül 2020. júliusban, ICS biztonság tárgyában a SANS nem tart ICS képzéseket, oktatásokat, a COVID-19 világjárványra tekintettel, kizárólag online formában.

A részletek a következő webhelyen találhatók:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Időszakosan induló online kurzusok:

A https://www.coursera.org/ honlapon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során video oktatásokon vehet részt a jelentkező, és feladatok megoldásával demonstrálhatja tudását a szakterületet érintően. Az online tanfolyam elvégzését követően a University of Colorado Boulder tanúsítványt állít ki a végzettek részére. A következő kurzusok végezhetők el:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

További részletek a következő webhelyen találhatók:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

Az említett oktatásokon felül az ICS-CERT is kínál Online kurzusokat:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation

További részletek a következő webhelyen találhatók:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Az **ICS-CERT Virtual Learning Portal** (VLP) a következő képzések elvégzését teszi lehetővé:

- Operational Security (OPSEC) for Control Systems (100W) - 1 óra
- Differences in Deployments of ICS (210W-1) – 1.5 óra
- Influence of Common IT Components on ICS (210W-2) – 1.5 óra
- Common ICS Components (210W-3) – 1.5 óra
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 óra
- Cybersecurity Risk (210W-5) – 1.5 óra
- Current Trends (Threat) (210W-6) – 1.5 óra
- Current Trends (Vulnerabilities) (210W-7) – 1.5 óra
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 óra

- Attack Methodologies in IT & ICS (210W-9) – 1.5 óra
- Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10) – 1.5 óra

A részletek a VLP képzések ugyanazon a linken érhetők el, mint a többi ICS-CERT online kurzus.

A SANS online képzései az ipari irányító rendszerek biztonságával kapcsolatban:

- ICS410: ICS/SCADA Security Essentials

További részletek a következő webhelyen találhatók:

https://www.sans.org/find-training-beta/search?courses=2762&types=10&redirect=beta#__utma=195150004.1547647064.1563952209.1566466056.1568274011.4&__utmb=195150004.2.9.1568274014545&__utmc=195150004&__utmx=-&__utmz=195150004.1568274011.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=17428089

Az ipari irányító rendszerek és a SCADA rendszerek biztonságáról szóló Online kurzus érhető el az Udemy honlapján, ahol a jelentkező megtanulhatja az ICS/SCADA biztonság alapjait, technológiai megoldásokat, szoftver kezelést, szabályozási megoldásokat.

- ICS/SCADA Cyber Security

További részletek a következő webhelyen találhatók:

https://www.udemy.com/ics-scada-cyber-security/

A Department of Homeland Security 2 napos képzése során a résztvevők megismerhetik a különböző vezérlő rendszerek biztonságával kapcsolatos tudnivalókat.

- SCADA security training

A koronavírus világjárványra tekintettel az online kurzusok élő közvetítéssel valósulnak meg.

További részletek a következő webhelyen találhatók:

https://www.tonex.com/training-courses/scada-security-training/

A SCADAhacker-com honlapon is megtalálható az ipari irányító rendszerek biztonságáról szóló online kurzus:

- Understanding, Assessing and Securing Industrial Control Systems

Az oktatás 40-120 órát vesz igénybe, és 8 modul segít eligazodni az ICS rendszerek kiberbiztonságának világában. A képzés a „blue teaming” tevékenységre fókuszál az ICS és SCADA rendszerek vonatkozásában.

A képzés alkalmas bizonyos képesítéssel rendelkező személyek (például: CISSP, CEH stb.) tudásának ICS specifikusság tételére.

További részletek a következő webhelyen találhatók:

https://scadahacker.com/training.html

A School of security ICS és SCADA Rendszerek biztonsági oktatást tart online, mely oktatás felkészíti a résztvevőket, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

Az oktatás az ICS és SCADA rendszerek alapjait, sérülékenységeit, kockázatmenedzsment alapjait, biztonsági kontrollok implementációit, szerver biztonságát, hálózat- és eszköz biztonságát, biztonsági programjainak fejlesztését, és a hálózat nélküli SCADA biztonságot mutatja be részletesen.

A tanfolyamok 0-3 vagy 4-12 hónap időtávban van lehetőség elvégezni, igény szerint. A részletekkel kapcsolatos további információ a következő honlapon található:

https://www.enosecurity.com/training-tutorials-courses/ics-scada-security-essentials-training/

Az INFOSEC-Flex SCADA/ICS Security Training Boot Camp elnevezésű online oktatása lehetőséget biztonsít a SCADA és ICS rendszerek elleni külső és belső támadások elleni felkészülésre.

A kurzus elvégzése garanciát ad a réztvevőknek arra, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

A 4 napos online kurzus leghamarabbi időpontja, melyre lehet regisztrálni a következő:

2020. 08. 03 – 07. Ezt követően a következő kurzus 2020. szeptemberben kerül megrendezésre.

A SCADA és ICS biztonsági alapjain kívül a szabályozási környezet is részleteiben bemutatásra kerül, ahogy a SCADA biztonsági kontrollok, és a SCADA penteszt is.

A képzéssel kapcsolatos további információk a következő linken érhetők el:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

ICS konferenciák

2020. augusztásban a koronavírus járványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop vagy elmarad, vagy valamely későbbi időpontra került eltolásra. Az alábbi konferenciák azonban virtuálisan kerülnek megtartásra.

SCADA Technology Summit

A digitális konferencián számos érdekes ICS és SCADA biztonsággal kapcsolatos előadást láthatnak a résztvevők. Ilyen előadás például a felhő alapú mesterséges intelligencia használata a SCADA rendszerek tekintetében, vagy a misszió kritikus SCADA műveletek és azok biztonsága.

Érdekes előadásnak ígérkezik a SCADA rendszerek kommunikáció védelmének növekvő igényéről tartandó prezentáció is. Az előadóktól lehet kérdezni, és a konferencián számos ICS és SCADA biztonsággal kapcsolatos újdonságról lehet információhoz jutni.

SCADA Technology Summit; (online konferencia), 2020. augusztus 26-27.

További információk a következő linken találhatók:

https://www.scadatechsummit.com/

ICIS 2020: 14. International Conference on Industrial Security

A nemzetközi online konferencián számos speciális kutatás és annak eredménye ismerhető meg, amely az egészségügyben és a víz ágazatban található rendszerek biztonságát hivatottak szolgálni. A konferencián résztvevők e-book formában is kézhez kapják a kutatási eredményeket.

ICIS 2020: 14. International Conference on Industrial Security; (online konferencia – Olaszország, Róma); 2020. augusztus 20-21.

További információk a következő linken találhatók:

https://waset.org/industrial-security-conference-in-august-2020-in-rome

ICS incidensek

Az ENEL villamosenergia társaság ransomware támadást szenvedett el

A Black Cell 14. ICS hírlevelében bemutatott Honda elleni SNAKE ransomware támadást követően valószínűsíthető, hogy az ENEL villamosenergia szolgáltató társaság is ugyanezen zsarolóvírus áldozatául esett.

A támadás a belső hálózatot érintette, melyet vasárnap este (2020. június 7.) észlelt a szervezet antivírus megoldása. A támadást követően a vállalati rendszer leválasztásra került, és bizonyos ideig nem volt elérhető annak érdekében, hogy minden kockázat megszűntetésre kerüljön. A vállalat tájékoztatása szerint minden kapcsolatot helyreállítottak hétfő reggelre.

A vállalat szóvivője elmondta, hogy a támadás nem okozott problémát a távoli vezérlő rendszerekben, az elosztó állomásokon és az erőművekben, továbbá ügyfél adatok nem kompromittálódtak a támadás során. A szóvivő figyelmeztetett, hogy az ügyfélszolgálati tevékenység során előfordulhatnak rövidebb szünetek.

A társaság a zsarolóvírust nem nevezte meg, azonban biztonsági kutatók megerősítették, hogy a virustotal adatbázisban enelint.global domainről történő SNAKE ransomware ellenőrzést hajtottak végre, amely megerősíti a feltételezést, mely szerint az említett SNAKE támadásról volt szó.

Arról jelenleg nincs információ, hogy hogyan sikerült a támadóknak a belső hálózatig eljutni, azonban valószínűsítik, hogy a távoli karbantartások végrehajtásához használt távoli asztali kapcsolatokon keresztül történhetett a támadás, mivel az RDP kapcsolatok elérhetők voltak az internet felől.

A HONDA és az ENEL tekintetében is az az információ látott napvilágot, hogy nem volt sikeres a támadás, azonban azt nem tudták pontosan megállapítani egyik esetben sem, hogy pontosan mikor történt a behatolás, valamint, hogy sikerült e bármilyen adatot ellopni a támadóknak.

A Dragos kiberbiztonsági vállalat megerősítette, hogy a SNAKE ransomware elsődlegesen az ipari irányító rendszereket veszi célba, és erről a korábbi híradásokban is figyelmeztettek a szakportálok.

Az incidenssel kapcsolatos további információk a következő webhelyeken érhetők el:

https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

Szerző: Javasoljuk, hogy az ipari irányító rendszereket üzemeltető szervezetek a nyíltan elérhető SNAKE ransomware-ről fellelhető információkat gyűjtsék be, azokat részleteiben elemezzék. Amennyiben segítségre van szüksége az adott szervezetnek, hogy a SNAKE zsarolóvírussal kapcsolatos elemzéshez jusson, keressenek fel szakértőket, akik az adott szervezet SNAKE támadással kapcsolatos sérülékenységeit is feltárják, és javaslatokat tesznek azok megszűntetésére. Szakértőink a következő elérhetőségeken állnak rendelkezésre: info@blackcell.hu; +36 1 605 0302;

Könyvajánló

A SCADA rendszerek felelősek az ipari és kritikus infrastruktúra folyamatok ellenőrzéséért, monitorozásáért. Az elmúlt években számos SCADA rendszereket ért támadásról lehetett hallani és olvasni.

Az említett támadások az apróbb zavaroktól egészen az emberéletek elvesztéséig széles skálán mozogtak. A könyv szerzője kifejti a könyvben, hogy szükséges a SCADA rendszerek biztonsági elemzése, és tesztelése, a fenyegetések középpontba állításával, bár ez kétségkívül erőforrás és idő igényes feladat.

A könyv bemutatja a SCADA biztonsági környezetet, a lehetséges támadásokat és azok elleni védelmi technikákat, de bizonyos PLC-k elleni támadások teszteléséről is említést tesz a szerző a könyvben.

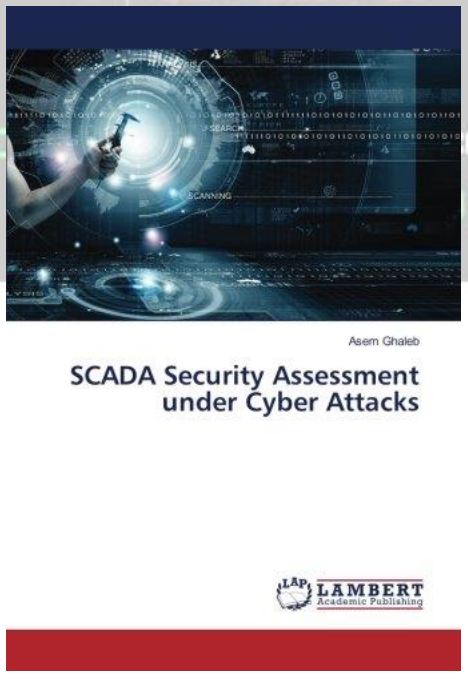
A könyv címe: SCADA Security Assessment under Cyber Attacks

Szerzők/szerkesztők: Asem Ghaleb

Kiadás éve: 2018.

A kiadvány elérhető a következő linken:

https://www.amazon.co.uk/dp/6138319222?slotNum=20&linkCode=g12&imprToken=tR0wLxCKj.JdVedlEkfUKg&creativeASIN=6138319222&tag=uuid07-21



Black Cell javaslatok

Az ICS biztonság kialakítása során számos tényezőt figyelembe kell venni. Vannak olyan elvárások, amelyeket nem lehet figyelmen kívül hagyni. A NIST 800-82 r2 ajánlás rövid részlete segítséget nyújthat abban, hogy azonosítsuk ezeket az elvárásokat és biztonságos ICS környezetet és rendszert alakíthassunk ki:

- Időzítési és teljesítmény elvárások: Az ICS-ek tekintetében időkritikus az elfogadható szintű késések és kiesések kritériuma. Egyes rendszerek alap elvárása, hogy a megbízható válasz, meghatározott időben az elvárt helyen rendelkezésre álljon. A magas szintű teljesítmény nem tipikus elvárás az ICS rendszerekkel szemben. Az IT rendszereknél azonban a magas fokú teljesítmény alap elvárás, de a késés vagy kiesés bizonyos szintig elfogadható. Ezzel szemben az ICS automatikus válaszidői, vagy humán beavatkozás során történő válaszidői kritikusak lehetnek. Egyes ICS-ek valós idejű működési környezeti (Real Time Operating Systems – RTOS) elvárásokkal kerültek létrehozásra, ahol az azonnali válasz valós időben alap elvárás.

- Rendelkezésre állással kapcsolatos elvárások: Számos ICS folyamatnak folyamatosan kell működnie. A rendszer nem várt kiesése a gyártási folyamatok során nem elfogadható. A kimaradásokat előre kell tervezni néhány nappal, vagy akár egy héttel is. A magas rendelkezésre állás biztosításához elengedhetetlen a széles körű, telepítés előtti tesztelés. A vezérlőrendszereket gyakran nem lehet könnyen leállítani és újraindítani, a termelést meghatározóan befolyásoló lépések nélkül. Egyes esetekben az előállított termékek vagy használt berendezések fontosabbak, mint a közvetített információk. Ezért az olyan tipikus informatikai megoldások használata, mint például az újraindítás, általában nem elfogadható megoldás a magas rendelkezésre állás, megbízhatóság és az ICS karbantarthatóság követelményeire gyakorolt kedvezőtlen hatás miatt. Sok ICS alkalmaz redundáns megoldásokat, amelyek paralel futnak, így az eredeti megoldás kiváltható a folyamat sérülése nélkül.

- Kockázat menedzsmenttel kapcsolatos elvárások: Egy tipikus IT rendszerben a legnagyobb fejtörést az adatok bizalmasságának és sértetlenségének biztosítása jelentik. Az ICS rendszerek esetében elsődleges az emberi élet védelme, ezáltal a hibatűrő tolerancia kap meghatározó figyelmet. Ezen túlmenően a közegészség, a bizalomvesztés, a szabályozásoknak történő megfelelés, szellemi tulajdon és berendezések elvesztése is lehet kockázat. Az ICS üzemeltetéséért, biztosításáért és fenntartásáért felelős személyzetnek meg kell értenie a emberélet biztonsága és az ICS biztonság közötti fontos kapcsolatot. Bármilyen biztonsági intézkedés, amely veszélyezteti ezt, az elfogadhatatlan.

- Fizikai hatások: Az ICS rendszerek terepen lévő eszközei (PLC, működtető állomás, DCS kontroller) közvetlenül felelősek a fizikai folyamatok kontrolljáért. Az ICS-ek komplex interakcióban vannak a fizikai folyamatokkal, amelyek a fizikai eseményekért felelősek. A potenciális fizikai hatások megértése érdekében elvárás a kontrollrendszereket üzemeltető és az adott fizikai terepen lévő szakértők közötti kommunikáció.

- Rendszer üzemeltetési elvárások: Az ICS üzemeltetési rendszerek és vezérlési hálózatok az IT üzemeltetési rendszerektől eltérnek. A vezérlési hálózatok OT mérnökök által és nem IT személyzet által működtetettek. Bizonyos feltételezések-, amelyek szerint a különbségek nem

jelentősek, és a specifikumok kezelése figyelmen kívül hagyásra kerül, katasztrofális következményekkel járhatnak a rendszer működésére nézve.

- Erőforrás korlátok: Az ICS, és azok valós idejű működtetéséért felelős rendszerek gyakran erőforrásukban korlátozottak, sokszor nem rendelkeznek modern informatikai biztonsági képességekkel. Sok rendszer kapcsán előfordulhat, hogy nem rendelkezik a kívánt funkciókkal, beleértve a titkosítási lehetőségeket, a hibanaplózást és a jelszavas védelmet. Az IT biztonsági gyakorlatok korlátozások nélküli használata időzítési és rendelkezésre állási problémákat okozhat az ICS rendszerekben. Előfordulhat, hogy az ICS rendszerelemek nem rendelkeznek a megfelelő IT erőforrásokkal, hogy ezeket a rendszereket a jelenlegi biztonsági képességekkel utólag felruházzák. Erőforrások vagy funkciók hozzáadása utólag sokszor nem lehetséges.

- Kommunikációs elvárások: A kommunikációs protokollok és az adathordozók, amelyeket az ICS környezetek használnak a terepen lévő eszközök vezérlésére és a folyamatokon belüli kommunikációra, általában különböznek a legtöbb informatikai környezettől, azok egyediek, így a kezelésüket is ennek megfelelően szükséges megtervezni.

- Változás menedzsment: A változáskezelés elsődleges fontosságú mind az informatikai, mind a vezérlési rendszerek integritásának megőrzése szempontjából. A nem frissített szoftverek az egyik legnagyobb sebezhetőségei a rendszereknek. Az informatikai rendszerek, köztük a biztonsági hibajavítások szoftverfrissítéseit rendszerint időben, megfelelő biztonsági irányelvek és eljárások alapján alkalmazzák. Ezek a folyamatok gyakran automatizáltak. Az ICS rendszerek kapcsán ezek már gyakran nem valósulnak meg időben. A frissítéseket tesztelni szükséges mind a frissítés szállítója, mind az alkalmazó részéről, mielőtt a frissítések megtörténnének. Az ICS üzemeltetőknek ráadásul előre tervezni kell ezeket a frissítéseket az esetleges leállásokhoz igazítva. Szintén probléma, hogy sok ICS az operációs rendszerek régebbi verzióit használja, amelyeket az adott gyártó már nem támogat. Következésképpen a rendelkezésre álló javítások nem alkalmazhatók. A firmware-ekre az eddigiek ugyanúgy érvényesek. A változáskezelési folyamat részeként, az ICS frissítésekor, a szakértők (OT mérnökök) gondos értékelése elvárás a biztonsági és informatikai személyzettel közösen.

- Menedzselt támogatás: A tipikus IT rendszerek különböző támogatási modelleket alkalmaznak, a különböző architektúrák függvényében. Az ICS-ek tekintetében a szolgáltatás támogatása néha egyetlen szállítón keresztül történik, amely lehet, hogy nem rendelkezik egy másik gyártótól származó, diverzifikált és interoperábilis támogatási megoldással. Bizonyos esetekben a harmadik féltől származó biztonsági megoldások nem engedélyezettek az ICS-szállítói licenc és a szolgáltatási szerződések miatt, és a szolgáltatás-támogatás elveszhet, ha harmadik féltől származó alkalmazások telepítései jóváhagyás nélkül valósulnak meg.

- Komponens élettartam: Az IT komponensek élettartama általánosságban 3-5 évre tehető, a technológia változása erre meghatározó hatással van. Az ICS rendszerek esetében ez inkább 10-15 évre vagy ennél is hosszabb időre tehető.

- Komponensek elhelyezkedése: az IT komponensek, és az ICS komponensek közül néhány fizikailag könnyen hozzáférhető létesítményekben található. A biztonsági mentések fizikailag távolabb találhatóak jó esetben. Az elosztott ICS-komponensek elkülönítettek, távoli elhelyezésűek lehetnek, és nehézséget okozhat a fizikai elérésük. A komponens helyének,

fizikai környezetének figyelembe kell vennie a szükséges fizikai és környezeti biztonsági intézkedéseket is.

Javasoljuk a fenti felsorolásban meghatározott ICS elvárások és sajátosságok figyelembevételét, ha egy megfelelően biztonságos, ellenálló rendszert szeretne egy szervezet kialakítani!

ICS sérülékenységek

2020. júliusában az alábbi ipari irányító rendszereket érintő sérülékenységeket publikálta a National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs), vagyis az ICS-CERT:

ICSA-20-210-01: **Secomea GateManager**

Kritikus szintű sérülékenységek: Nulla Byte vagy a NUL karakter nem megfelelő neutralizációja, maximális és minimális értékkezelési hiba, beégetett hitelesítő használata, jelszó hash nem megfelelő számítási használat.
https://us-cert.cisa.gov/ics/advisories/icsa-20-210-01

ICSA-20-210-02: **Softing Industrial Automation OPC**

Kritikus szintű sérülékenységek: puffer túlcsordulás, erőforrás ellenőrizetlen felhasználása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-210-02

ICSA-20-210-03: **HMS Industrial Networks eCatcher**

Kritikus szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-210-03

ICSA-20-182-01: **Delta Industrial Automation DOPSoft (Update A)**

Magas szintű sérülékenységek: puffer memórián kívüli olvasás lehetősége, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-182-01

ICSA-20-205-01: **Schneider Electric Triconex TriStation and Tricon Communication Module**

Kritikus szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, ellenőrizetlen erőforrás felhasználás, rejtett funkcionalitás, nem megfelelő hozzáférés ellenőrzés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-205-01

ICSA-20-168-01: **Treck TCP/IP Stack (Update E)**

Kritikus szintű sérülékenységek: A hosszparaméterek nem megfelelő kezelése, nem megfelelő bemeneti érvényesítés, memória címhívási hiba, egész szám túlcsordulás, nem megfelelő hozzáférés ellenőrzés, helytelen nulla szám kezelés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

ICSMA-20-196-01: **Capsule Technologies SmartLinx Neuron 2**

Magas szintű sérülékenység: védelmi mechanizmus hiba.
https://us-cert.cisa.gov/ics/advisories/icsma-20-196-01

ICSA-20-196-01: **Advantech iView**

Kritikus szintű sérülékenységek: SQL befecskendezés, útvonal bejárás, parancs befecskendezés, nem megfelelő bemeneti érvényesítés, kritikus funkció hiányzó hitelesítése, nem megfelelő hozzáférés ellenőrzés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-01

ICSA-20-196-02: **Moxa EDR-G902 and EDR-G903 Series Routers**

Kritikus szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-02

ICSA-20-196-03: Siemens SICAM MMU, SICAM T, and SICAM SGU
Kritikus szintű sérülékenységek: memória puffer határain kívüli olvasás lehetősége, kritikus funkció hiányzó hitelesítése, szenzitív információk hiányzó titkosítása, nem megfelelő jelszó hash használat, klasszikus puffer túlcsordulás, XSS, hitelesítés megkerülése.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-03

ICSA-20-196-04: Siemens SIMATIC HMI Panels
Közepes szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő továbbítása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-04

ICSA-20-196-05: Siemens UMC Stack
Közepes szintű sérülékenységek: nem jegyzett keresési útvonal vagy elem, nem megfelelő erőforrás felhasználás, nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-196-06: Siemens SIMATIC S7-200 SMART CPU Family
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-06

ICSA-20-196-07: Siemens Opcenter Execution Core
Magas szintű sérülékenységek: XSS, SQL befecskendezés, nem megfelelő hozzáférés ellenőrzés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-07

ICSA-20-196-08: Siemens LOGO! Web Server
Kritikus szintű sérülékenység: klasszikus puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-08

ICSMA-20-170-02: Baxter PrismaFlex and PrisMax (Update B)
Magas szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, nem megfelelő hitelesítés, beégetett jelszavak használata.
https://us-cert.cisa.gov/ics/advisories/icsma-20-170-02

ICSA-20-168-01: Treck TCP/IP Stack (Update D)
Kritikus szintű sérülékenységek: Hosszparaméterek nem megfelelő kezelése, nem megfelelő bemeneti érvényesítés, memóriacím duplán történő hívása, memória puffer határain kívüli olvasás lehetősége, nem megfelelő hozzáférés ellenőrzés, egészszám túlcsordulás, nem megfelelő érvénytelenítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update A)
Közepes szintű sérülékenység: Nem jegyzett keresési útvonal vagy elem.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSA-20-161-05: Siemens SIMATIC, SINAMICS (Update A)
Magas szintű sérülékenység: ellenőrizetlen elem a keresési útvonalban, puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-05

ICSA-20-070-02: Siemens SIMATIC S7-300 CPUs and SINUMERIK Controller over Profinet (Update A)
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-070-02

ICSA-20-042-02: Siemens Industrial Products SNMP Vulnerabilities (Update A)
Magas szintű sérülékenység: adatfeldolgozási hiba, null pointer dereferencia.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-02

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update D)
Magas szintű sérülékenység: nem megfelelő puffer méret kalkuláció.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-06

ICSA-19-318-02: Siemens S7-1200 and S7-200 SMART CPUs (Update B)
Közepes szintű sérülékenység: veszélyes funkciónak vagy módszernek való kitettség.
https://us-cert.cisa.gov/ics/advisories/icsa-19-318-02

ICSA-19-283-02: Siemens PROFINET Devices (Update F)
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02

ICSA-19-227-03: Siemens SCALANCE Products (Update A)
Közepes szintű sérülékenység: kódolási szabványok nem megfelelő betartása.
https://us-cert.cisa.gov/ics/advisories/icsa-19-227-03

ICSA-17-339-01: Siemens Industrial Products (Update O)
Magas szintű sérülékenység: nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01

ICSA-17-129-02: Siemens devices using the PROFINET Discovery and Configuration Protocol (Update Q)
Közepes szintű sérülékenység: nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

ICSA-20-191-01: Phoenix Contact Automation Worx Software Suite
Magas szintű sérülékenységek: puffer túlcsordulás, puffer határain kívüli olvasás lehetősége.
https://us-cert.cisa.gov/ics/advisories/icsa-20-191-01

ICSA-20-191-02: Rockwell Automation Logix Designer Studio 5000
Alacsony szintű sérülékenység: nem megfelelő külső XML korlátozás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-191-02

ICSA-20-189-01: Grundfos CIM 500

Magas szintű sérülékenységek: kritikus funkció hiányzó hitelesítése, hitelesítők védtelen formában történő tárolása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-189-01

ICSA-20-189-02: Mitsubishi Electric GOT2000 Series

Kritikus szintű sérülékenységek: memória pufferen belüli műveletek nem megfelelő korlátozása, munkamenet rögzítés, null pointer dereferencia, nem megfelelő hozzáférés ellenőrzés, argumentum befecskendezés, erőforrás menedzsment hibák.
https://us-cert.cisa.gov/ics/advisories/icsa-20-189-02

ICSMA-20-184-01: OpenClinic GA

Kritikus szintű sérülékenységek: hitelesítés megkerülése alternatív útvonalon vagy csatornán, túlzott hitelesítési kísérletek nem megfelelő korlátozása, nem megfelelő hitelesítés, hiányzó hitelesítés, privilegizált jogosultságokkal történő cselekmények korlátozatlansága, útvonal bejárás, veszélyes fájltípus korlátozás nélküli feltöltési lehetősége, XSS, karbantartás nélküli külső komponensek használata, rejtett funkcionalitás, hitelesítő adatok nem megfelelő védelme.
https://www.us-cert.gov/ics/advisories/icsma-20-184-01

ICSA-20-184-01: Nortek Linear eMerge 50P/5000P

Kritikus szintű sérülékenységek: útvonal bejárás, parancs befecskendezés, veszélyes fájltípus korlátozás nélküli feltöltési lehetősége, CSRF, nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-184-01

ICSA-20-184-02: ABB System 800xA Information Manager

Magas szintű sérülékenység: XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-184-02

ICSA-20-182-01: Delta Industrial Automation DOPSoft

Magas szintű sérülékenységek: puffer túlcsordulás, puffer határain kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-20-182-01

ICSA-20-182-02: Mitsubishi Electric Factory Automation Engineering Software Products

Magas szintű sérülékenységek: nem megfelelő XML korlátozás, ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-182-02

A sérülékenységek részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://ics-cert.us-cert.gov/advisories

A sérülékenységek részletes leírását, a megoldási javaslatokat, és az érintett termékek teljeskörű listáját a sérülékenységhez tartozó linken lehet megtalálni.

Javasolt a sérülékenységek folyamatos nyomon követése, mert a gyengeségek kezelésére és a sérülékenységek befoltozására vonatkozó releváns információk is megjelennek a részletes leírásokban.

ICS riasztások

2020. július hónapban az ICS-CERT nem adott ki riasztást.

A korábban kiadott riasztások részletezve a kapcsolódó linkeken, illetve összesítve a következő weboldalon találhatók meg:

https://www.us-cert.gov/ics/alerts