11. 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 2

ICS KÉPZÉSEK, OKTATÁSOK 3

ICS KONFERENCIÁK 6

ICS INCIDENSEK 7

KÖNYVAJÁNLÓ 8

BLACK CELL JAVASLATOK 9

ICS SÉRÜLÉKENYSÉGEK 10

ICS RIASZTÁSOK 14

ICS jó gyakorlatok, javaslatok

Biztosan sokat hallottak már a hibrid fenyegetésekről (vagy hibrid hadviselésről).

Hibrid hadviselés: A hibrid hadviselésnek nincs általánosan elfogadott meghatározása. A NATO walesi csúcstalálkozójának zárónyilatkozata (2014. szeptember) szerint a hibrid fenyegetés széles körű nyílt és fedett katonai, félkatonai és nem katonai eszközök és eljárások alkalmazása egy szorosan integrált műveleti terv mentén. Forrás: Kiss Álmos Péter; A hibrid hadviselés természetrajza.

A nemzetek által szponzorált kibercsoportok megpróbálják kihasználni bármilyen természeti katasztrófa, vagy nemzetközi szintű figyelmet egy adott problémára összpontosító helyzetben, amikor a biztonságra (információ-, vagy informatikai) kevesebb figyelem jut. A jelen pandémiás helyzet (COVID-19 világjárvány) tökéletesen alkalmas arra, hogy a bizonytalan helyzetet ártó szándékkal használja fel egy kibercsoport, akár a kritikus infrastruktúrák (ICS üzemeltetők) rendszereinek támadásával.

Több biztonsággal foglalkozó médium is cikkezett és cikkezik arról, hogy a koronavírus-járványt kihasználva próbálnak meg a kibertámadók sikeres támadásokat végrehajtani, phishing vagy ransomware alkalmazásával, de akár egyéb módokon: álhírek terjesztésével, vagy a létfontosságú rendszerek működésének megbénításával, ellehetetlenítésével.

Mivel a kritikus infrastruktúrák (ivóvíz-szolgáltatók, villamosenergia- vagy gázszolgáltatók) ilyen helyzetben különösen ki vannak téve az említett fenyegetéseknek, javasolt még inkább a védelemre koncentrálni. Érdemes tudatosító kampányt intézni a szervezetben dolgozók figyelmének felkeltése céljából, hogy a pandémiás helyzetben fokozott figyelem szükséges (pl. e-mailek csatolmányainak megnyitása, linkekre történő kattintás, járványügyi friss információk lánclevelekben történő továbbítása, gyanús naplófájlok kezelése stb. – lehetne sorolni – vonatkozásában.)

Javasolt a nemzeti és európai kijelölt létfontosságú rendszerelem üzemeltetőknek az Üzemeltetői Biztonsági Tervben kifejteni rendkívüli eseményként a pandémiás helyzetet és annak kezelésének céljából végrehajtandó feladatokat, figyelembe véve a hibrid hadviselés szcenárióit és azok esetleges következményeit.

Javasolt az információmegosztás adott támadás esetében mind a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Eseménykezelő Központtal, mind pedig olyan szervezetekkel, akik hasonló tevékenységet látnak el. Az egyéni érdekeket ebben az esetben felül kell, hogy írja a közérdek. Amennyiben nem így jár el egy kritikus infrastruktúra üzemeltető, abban az esetben a szervezet kiesik egy olyan láncból, ahol a későbbiekben ő nem fog rendelkezni azokkal az információkkal, amelyek szükségesek a további kibertámadások észleléséhez és elhárításához.

Összességében a stresszhelyzet még inkább nő ilyen esetekben, javasolt a személyzet felkészítése, akár üzletmenet-folytonossági képzések-, akár éles gyakorlatok tartása keretein belül.

ICS képzések, oktatások

A teljesség igénye nélkül 2020. áprilisban, ICS biztonság tárgyában a következő tréningek, oktatások kerülnek lebonyolításra:

2020. áprilisban a SANS nem tart ICS képzéseket, oktatásokat, a COVID-19 világjárványra tekintettel. A következő képzést 2020. júniusára hirdették meg.

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 nem kizárólag helyhez kötötten szervez képzéseket az ipari irányító rendszerek biztonságával kapcsolatban, hanem online kurzust is indít:

- ICS410: ICS/SCADA Security Essentials SANS

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

ICS konferenciák

2020. áprilisában a koronavírus járványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop vagy elmarad, vagy valamely későbbi időpontra került elhalasztásra.

Javasoljuk a konferenciák helyett a webinárok és oktató videók látogatását, mely jelen helyzetben célravezető!

Változás esetén információkat közlünk a hírlevélre feliratkozókkal.

ICS incidensek

Feltörték az ENTSO-E Európai villamosenergia irányítók európai szervezete informatikai hálózatát

A villamosenergia piac koordinátor szervezetének IT hálózatába hekkerek hatoltak be. Az ENTSO-E az európai villamosenergia átviteli rendszerek üzemeltetőinek koordinátor szervezete tájékoztatta erről a nyilvánosságot.

Leszögezte a szervezet, hogy az irodai rendszerek nincsenek kapcsolatban az ipari rendszerekkel, kritikus rendszerek nem voltak érintettek a kibertámadásban. Az incidens vizsgálatát követően a folytonosság fenntartása, valamint a kockázatok mérséklése és további hasonló támadások elkerülése érdekében kockázatelemzést végzett a szervezet, és a kockázatcsökkentő intézkedéseket megtette.

Az ENTSO-E 35 európai ország 42 villamos energia hálózati üzemeltetőjének koordinátora. A szervezethez érkezett kérdés az incidenst követően, hogy ki a felelős a támadásért, de erre a kérdésre nem érkezett egzakt válasz.

A Fingrid, vagyis a Helsinki székhelyű átvitelirendszer-üzemeltető (TSO) elmondása alapján a energia-azonosító kódok kiadása lelassult, ez negatív hatással lehet az európai villamos-energia kereskedelemre. Erre a két szervezet közötti adatállomány átviteli rendszer problémák miatt kerülhet sor.

További északi országok üzemeltetői is megszólaltak az ügyben. A lehetséges hatásokat még vizsgálják, és megpróbálnak a rendszereket érinthető fenyegetésekre megfelelő választ adni.

A felelős egyelőre nincs meghatározva, és megjegyezte az ENTSO-E, hogy a villamos-energia rendszerek üzemeltetői lehettek a támadás célkeresztjében.

Az incidensről további információk az alábbi linkeken állnak rendelkezésre:

https://www.cyberscoop.com/european-entso-breach-fingrid/

https://www.zdnet.com/article/european-electricity-association-warns-of-office-network-breach/

Könyvajánló

A szerző bemutatja, hogy az IT szabványok szerinti védelemmel ellátott SCADA rendszereket milyen módon támadják, és hogy mennyire nem helyes ez a fajta védelem, illetve a mélységi védelem teljes hiánya az, ami a támadásokat lehetővé teszi.

A SCADA rendszereket nem IT megoldással kell védeni, hanem OT megoldásokkal, amelyek rétegzett biztonsági megoldásokkal érhetők el, amely olcsóbb és praktikusabb az IT védelmi megoldásoknál. 100%-os biztonság természetesen nem létezik, de törekedni kell a magas szintű SCADA biztonság megteremtésére.

A SCADA rendszereket támadni óhajtó csoportok és személyek dolgát meg kell nehezíteni, ehhez nyújt segítséget a könyv.

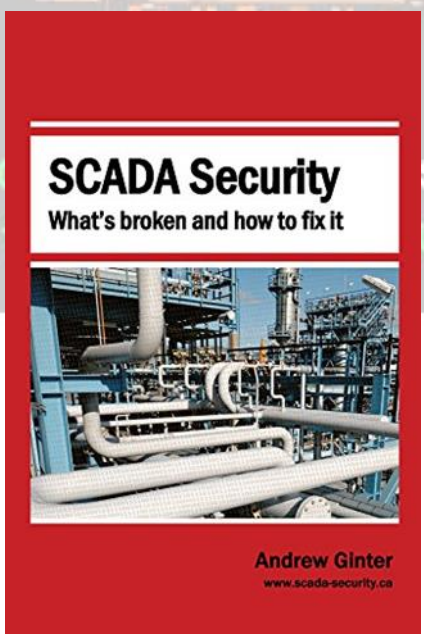
A könyv címe: SCADA Security What's broken and how to fix it

Szerző: Andrew Ginter

Kiadás éve: 2016.

A kiadvány elérhető a következő linken:

https://www.amazon.com/SCADA-Security-Whats-Broken-How-ebook/dp/B01M0WWK8F/ref=pd_sim_351_6/139-2402915-3452033?_encoding=UTF8&pd_rd_i=B01M0WWK8F&pd_rd_r=8f15284d-167d-4b5b-8c44-2ea0595e1d67&pd_rd_w=XX0dA&pd_rd_wg=EwuBL&pf_rd_p=65e3eab0-d81f-4a76-93ff-f0b7b1d6cd3d&pf_rd_r=9VE162XYEFPHEM16WVTT&psc=1&refRID=9VE162XYEFPHEM16WVTT



Black Cell javaslatok

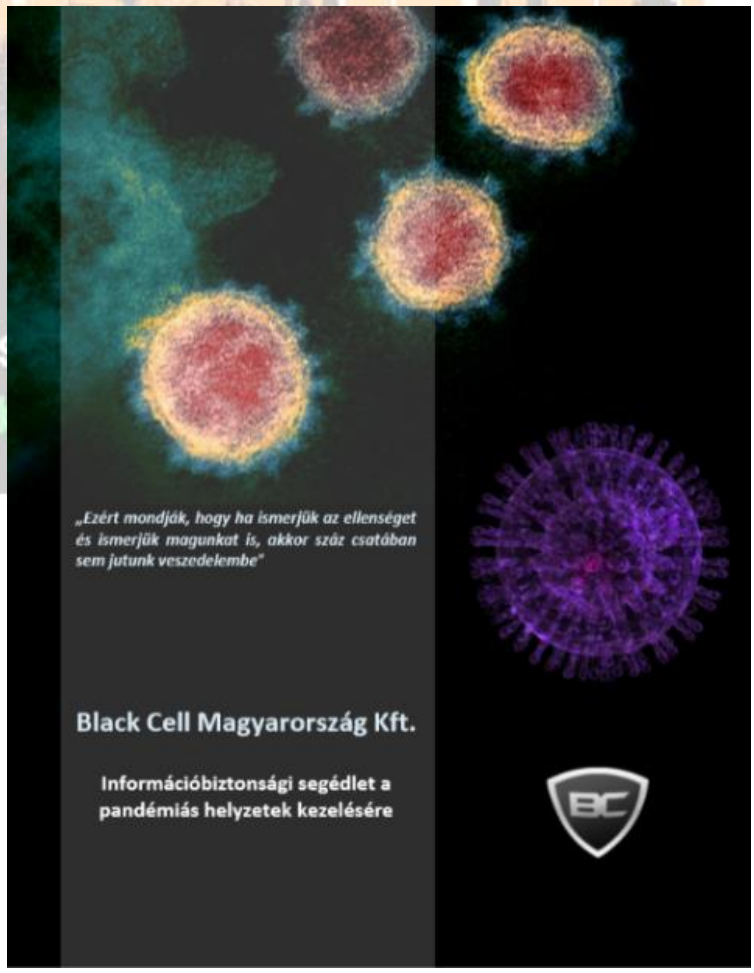
Nem lehet elmenni szó nélkül a WHO által világjárvánnyá (pandémia) nyilvánított új típusú koronavírus (COVID-19) és hatásai mellett. Mint az sokak számára nyilvánvaló, a járvány nem kizárólag az egészségügyi ágazatot érinti, hanem szinte minden más ágazatot is, az egymástól való függőségek miatt.

Ahogy az adatkezeléseket és az adatvédelmet is érinti a koronavírus hatása (lsd. Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye: https://naih.hu/files/NAIH_2020_2586.pdf) úgy az információbiztonságot, ezen belül leginkább az üzletmenet-folytonosságot is számottevően befolyásolja.

Ajánlott minden szervezetnek készítenie egy pandémiás tervet, amely segítséget nyújt abban, hogy megfelelően felkészüljön a szervezet a járványokkal összefüggésben kialakuló, nem várt események megfelelő kezelésére.

Az ipari irányító rendszerek üzemeltetői sem kivételek azon szervezetek alól, amelyek érintettek a világjárványban. A humán erőforrás korlátozott rendelkezésre állásának-, valamint a távoli munkavégzés feltételeinek hiánya meghatározó kiesést eredményezhet, legyen gazdasági vagy egyéb biztonsági kérdésről szó.

A kritikus infrastruktúrák üzemeltetőinek még inkább figyelni kell a helyzet megfelelő kezelésére, mert például kijárási korlátozások (pl. karantén) esetében is szükség van elektromos áramra, illetve ivóvízre, továbbá a közlekedés sem állhat le, mert az élelmiszer és egyéb áruellátás leállása emberi életeket sodorhat veszélybe.



A Black Cell szakértői elkészítették az információbiztonsági segédletet a pandémiás helyzetek kezelésére, amely rávilágít arra, hogy mi mindent kell figyelembe venni egy szervezetnek, hogy a pandémiás helyzeteket megfelelően kezelni tudja.

Az információbiztonsági segédlet a pandémiás helyzetek kezelésére a következő linken érhető el: https://blackcell.hu/pandemias-segedlet/.

ICS sérülékenységek

2020. márciusban 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-20-086-01: **Advantech WebAccess**
Magas szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-086-01

ICSA-20-077-01: **Delta Electronics Industrial Automation CNCSoft ScreenEditor**
Magas szintű sérülékenységek: puffer túlcsordulás, memória puffer határon kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-20-077-01

ICSA-20-072-01: **ABB eSOMS**
Magas szintű sérülékenységek: böngészők érzékeny információ használata, rétegek közötti korlátozás nem megfelelősége, helytelen http fejléc kezelés, védelmi mechanizmus hiba, érzékeny süti kezelés hiba, érzékeny információk feltárása jogosulatlanok számára, gyenge jelszó elvárások, SQL befecskendezés, XSS, érzékeny információk egyszerű szöveges formátumban történő tárolása, titkosítás nem megfelelő erőssége.
https://www.us-cert.gov/ics/advisories/icsa-20-072-01

ICSA-20-072-02: **ABB Asset Suite**
Magas szintű sérülékenység: felhasználói kulcson keresztüli hitelesítés megkerülés.
https://www.us-cert.gov/ics/advisories/icsa-20-072-02

ICSA-20-072-03: **Rockwell Automation Allen-Bradley Stratix 5950**
Közepes szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-072-03

ICSA-20-070-01: **Siemens SiNVR 3**
Magas szintű sérülékenységek: útvonal bejárás, állományok egyszerű szöveges formában történő tárolása, SQL befecskendezés, XSS, nem megfelelő bemeneti hitelesítés hibás naplózása, gyenge kriptográfiai jelszóvédelem.
https://www.us-cert.gov/ics/advisories/icsa-20-070-01

ICSA-20-070-02: **SIMATIC S7-300 CPUs and SINUMERIK Controller over Profinet**
Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-070-02

ICSA-20-070-03: **Siemens Spectrum Power 5**
Közepes szintű sérülékenység: karakterkezelési hiba.
https://www.us-cert.gov/ics/advisories/icsa-20-070-03

ICSA-20-070-04: **Johnson Controls Kantech EntraPass**
Kritikus szintű sérülékenység: nem megfelelő bemeneti hitelesítés.

https://www.us-cert.gov/ics/advisories/icsa-20-070-04

ICSA-20-070-05: Johnson Controls Metasys

Magas szintű sérülékenység: külső XML elemek nem megfelelő korlátozása.
https://www.us-cert.gov/ics/advisories/icsa-20-070-05

ICSA-20-070-06: Rockwell Automation MicroLogix Controllers and RSLogix 500 Software

Kritikus szintű sérülékenységek: beégetett kriptográfiai kulcs használat, kockázatos jelszóvédelmi algoritmus alkalmazása, kliens oldali hitelesítés használata, érzékeny információk egyszerű szöveges formában történő tárolása.
https://www.us-cert.gov/ics/advisories/icsa-20-070-06

ICSA-20-042-04: Siemens PROFINET-IO Stack (Update A)

Magas szintű sérülékenység: ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-042-04

ICSA-20-042-05: Siemens SIMATIC S7 (Update A)

Közepes szintű sérülékenység: erőforrás kimerítés.
https://www.us-cert.gov/ics/advisories/icsa-20-042-05

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update A)

Magas szintű sérülékenység: puffer méret nem megfelelő kalkulációja.
https://www.us-cert.gov/ics/advisories/icsa-20-042-06

ICSA-20-042-11: Siemens SIMATIC S7-1500 (Update A)

Magas szintű sérülékenység: erőforrás kimerítés.
https://www.us-cert.gov/ics/advisories/icsa-20-042-11

ICSA-19-351-02: Siemens SPPA-T3000 (Update A)

Kritikus szintű sérülékenységek: nem megfelelő bemeneti hitelesítés és autentikáció, érzékeny információk egyszerű szöveges formában történő továbbítása, kontrollálatlan file feltöltés lehetősége, puffer túlcsordulás, puffer határain kívüli olvasás lehetősége, nem megfelelő hozzáférés ellenőrzés, információ feltárás, hiányzó hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-351-02

ICSA-19-344-04: Siemens SIMATIC Products (Update B)

Alacsony szintű sérülékenység: veszélyes funkció feltárás.
https://www.us-cert.gov/ics/advisories/icsa-19-344-04

ICSA-19-344-06: Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A)

Közepes szintű sérülékenységek: kockázatos kritptográfiai algoritmus használat, hitelesítés támogatásának a hiánya.
https://www.us-cert.gov/ics/advisories/icsa-19-344-06

ICSA-19-283-01: Siemens Industrial Real-Time (IRT) Devices (Update C)

Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.

https://www.us-cert.gov/ics/advisories/icsa-19-283-01

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

ICSA-19-253-03: Siemens Industrial Products (Update E)
Magas szintű sérülékenységek: értékkezelési hiba, ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-253-03

ICSA-19-099-03: Siemens Industrial Products with OPC UA (Update F)
Magas szintű sérülékenység: nem megfelelő kivétel kezelés.
https://www.us-cert.gov/ics/advisories/ICSA-19-099-03

ICSA-19-099-06: Siemens SIMATIC, SIMOCODE, SINAMICS, SITOP, and TIM (Update G)
Magas szintű sérülékenység: pufferen kívüli adatolvasás.
https://www.us-cert.gov/ics/advisories/ICSA-19-099-06

ICSA-16-348-05: Siemens S7-300/400 PLC Vulnerabilities (Update E)
Magas szintű sérülékenységek: információ feltárás, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/ICSA-16-348-05

ICSA-20-065-01: WAGO I/O-CHECK
Kritikus szintű sérülékenységek: adatküldéskor történő információ feltárás, puffer túlcsordulás, kritikus funkció hiányzó hitelesítési eljárása, puffer nem megfelelő értékkezelése.
https://www.us-cert.gov/ics/advisories/icsa-20-065-01

ICSA-20-063-01: Emerson ValveLink
Magas szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-063-01

ICSA-20-063-02: PHOENIX CONTACT Emalytics Controller ILC
Kritikus szintű sérülékenység: kritikus erőforrásokhoz történő nem megfelelő engedély hozzárendelés.
https://www.us-cert.gov/ics/advisories/icsa-20-063-02

ICSA-20-063-03: Omron PLC CJ Series
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-20-063-03

ICSA-20-063-04: Moxa AWK-3131A Series Industrial AP/Bridge/Client
Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, beégetett kriptográfiai kulcs használata, operációs rendszerbe parancs befecskendezés, beégetett hitelesítés, puffer túlcsordulás, pufferen kívüli olvasás, hitelesítés megkerülése alternatív útvonalon vagy csatornán.
https://www.us-cert.gov/ics/advisories/icsa-20-063-04

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. március hónapban az ICS-CERT az alábbi riasztást adta ki:

A Bluetooth Low Energy protokoll több sérülékenységéről adott ki riasztást az ICS-CERT, mely számos IoT, okos-eszköz, orvostechnikai eszköz és egyéb vezeték nélküli megoldás biztonságát veszélyezteti.

A riasztás kiadását megelőzően értesítésre kerültek az érintett szállítók, valamint a sérülékenységek befoltozására és frissítések kiadására lettek felkérve. A sérülékenységek távolról nem kihasználhatók.

A sérülékenységek listáját, valamint azok kihasználásának hatásait táblázatos formában az ICS CERT honlapján meg lehet találni.

Javasolt feltárni az ICS üzemeltetőknek, hogy milyen hatása lehet az adott sérülékenységeknek az OT biztonságra. Érdemes figyelemmel kísérni a sérülékenységeket befoltozó javítócsomagok megjelenéséről szóló információkat, és a patch telepítések segítséget nyújthatnak a sérülékenységi ablak bezárásához.

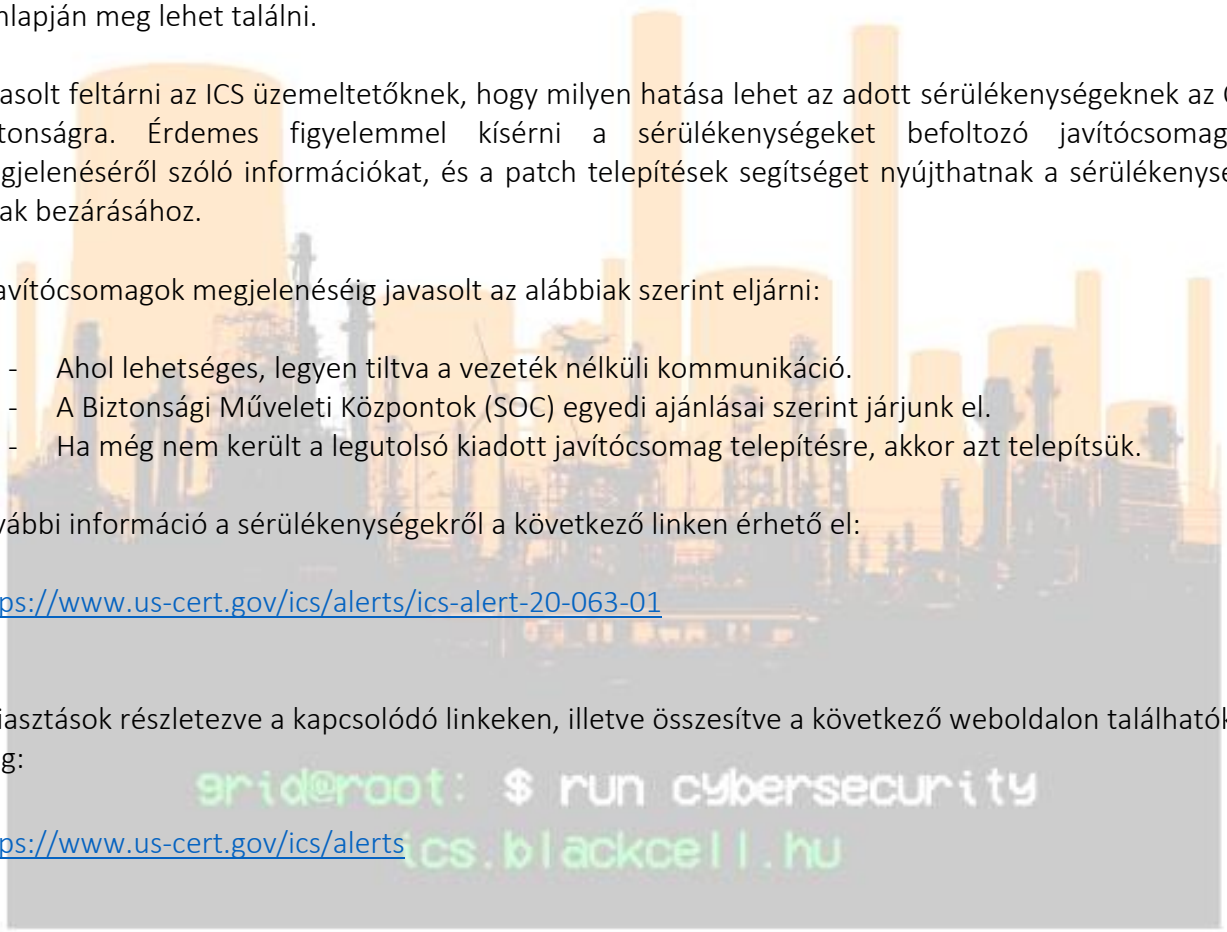
A javítócsomagok megjelenéséig javasolt az alábbiak szerint eljárni:

- Ahol lehetséges, legyen tiltva a vezeték nélküli kommunikáció.
- A Biztonsági Műveleti Központok (SOC) egyedi ajánlásai szerint járjunk el.
- Ha még nem került a legutolsó kiadott javítócsomag telepítésre, akkor azt telepítsük.

További információ a sérülékenységekről a következő linken érhető el:

https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01

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



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