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. A Black Cell javaslatokat, megoldásokat kínál az ipari irányító rendszerekhez kapcsolódó tevékenységek hatékony elvégzéséhez, és ezáltal a biztonság minél magasabb szintű megteremtéséhez.

Tartalom:

ICS sérülékenységek

2019. augusztusban 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:

ICSMA-19-241-01: **Change Healthcare McKesson and Horizon Cardiology**
Magas szintű sérülékenység: nem megfelelő alapértelmezetten beállított engedélyek.
https://www.us-cert.gov/ics/advisories/icsma-19-241-01

ICSMA-19-241-02: **Philips HDI 4000 Ultrasound**
Alacsony szintű sérülékenység: elavult funkciók használata.
https://www.us-cert.gov/ics/advisories/icsma-19-241-02

ICSA-19-239-01: **Delta Controls enteliBUS Controllers**
Kritikus szintű sérülékenység: Puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-239-01

ICSA-19-239-02: **Datalogic AV7000 Linear Barcode Scanner**
Magas szintű sérülékenység: Hitelesítés megkerülés alternatív útvonal vagy csatorna használatával.
https://www.us-cert.gov/ics/advisories/icsa-19-239-02

ICSA-19-232-01: **Zebra Industrial Printers**
Közepes szintű sérülékenység: nem megfelelően védett hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-232-01

ICSA-19-227-01: **Johnson Controls Metasys**
Közepes szintű sérülékenységek: a titkosításban használt kulcspár újra felhasználása, beégetett kriptográfiai kulcs használata.
https://www.us-cert.gov/ics/advisories/icsa-19-227-01

ICSA-19-227-02: **Fuji Electric Alpha5 Smart Loader**
Magas szintű sérülékenység: puffer túlcsordulásos sérülékenység.
https://www.us-cert.gov/ics/advisories/icsa-19-227-02

ICSA-19-227-03: **Siemens SCALANCE Products**
Közepes szintű sérülékenység: Kódolási szabványok figyelmen kívül hagyása.
https://www.us-cert.gov/ics/advisories/icsa-19-227-03

ICSA-19-227-04: **Siemens SINAMICS**
Magas szintű sérülékenység: Ellenőrizetlen erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-227-04

ICSA-19-225-01: **Delta Industrial Automation DOPSoft**
Magas szintű sérülékenységek: Puffer határán kívüli adat olvasás, memória hivatkozási probléma.

https://www.us-cert.gov/ics/advisories/icsa-19-225-01

ICSA-19-225-02: OSIsoft PI Web API
Magas szintű sérülékenységek: Érzékeny információk naplófájlokban történő megjelenítése, védelmi mechanizmus hiba.
https://www.us-cert.gov/ics/advisories/icsa-19-225-02

ICSA-19-225-03: Siemens SCALANCE X Switches (Update A)
Magas szintű sérülékenység: Nem megfelelő erőforrás kezelés.
https://www.us-cert.gov/ics/advisories/icsa-19-225-03

ICSA-19-213-01: Advantech WebAccess HMI Designer
Magas szintű sérülékenység: Puffer határán kívüli írás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-213-01

ICSA-19-213-02: Fuji Electric FRENIC Loader
Alacsony szintű sérülékenység: Puffer határán kívüli adat olvasás.
https://www.us-cert.gov/ics/advisories/icsa-19-213-02

ICSA-19-213-03: 3S-Smart Software Solutions GmbH CODESYS V3
Magas szintű sérülékenységek: nem megfelelő forrás hitelesítés, kontrollálatlan memória allokáció.
https://www.us-cert.gov/ics/advisories/icsa-19-213-03

ICSA-19-213-04: 3S-Smart Software Solutions GmbH CODESYS V3
Magas szintű sérülékenység: Nem megfelelően védett hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-213-04

ICSA-19-213-05: Rockwell Automation Arena Simulation Software
Magas szintű sérülékenységek: memória hivatkozási problémák, információ jogosulatlanok számára történő hozzáférhetővé tétele.
https://www.us-cert.gov/ics/advisories/icsa-19-213-05

ICSA-19-213-06: LCDS LAquis SCADA LQS File Parsing
Magas szintű sérülékenységek: Puffer határán kívüli adat olvasás, erőforrás inkompatibilitás.
https://www.us-cert.gov/ics/advisories/icsa-19-213-06

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.

ICS riasztások

2019. augusztus hónapban az ICS-CERT a következő riasztást adta ki:

A Mitsubishi Electric smartRTU (2.02 és korábbi verziói) és INEA ME-RTU (3.0 és korábbi verziói) távoli terminál egységei vonatkozásában a következő nagyrészt távolról is kihasználható sérülékenységekről került riasztás kiadásra:

Sérülékenység	Távolról kihasználható	Hatás
OS parancs befecskendezés	Igen	Távoli kód futtatásának lehetősége admin hozzáféréssel
Nem megfelelő hozzáférés hitelesítés	Igen	Távoli kód futtatásának lehetősége admin hozzáféréssel
XSS	Igen	Káros kód futtatásának lehetősége a célzott rendszeren
Beégetett kriptográfiai kulcsok	Igen	Hitelesítés nélküli hozzáférés lehetősége/titkosított adatok nyilvánosságra kerülése
Beégetett hitelesítés	Igen	Hitelesítés nélküli hozzáférés lehetősége/admin parancsok végrehajtása
Jelszavak plaintext formában történő tárolása	Igen	Felhasználónevek és jelszavak nyilvánosságra kerülése
Nem megfelelő alapértelmezett engedélyek	Nem	Felhasználónevek és jelszavak nyilvánosságra kerülése bejelentkezett felhasználó által

A sérülékenységek felfedezőinek jelentése a következő linken olvasható: https://www.mogozobo.com/?p=3593

A sérülékenységekből fakadó kockázatok csökkentése érdekében az alábbi intézkedések megtétele javasolt:

- Gondoskodjon róla, hogy az eszközök megfelelő védelemmel rendelkezzenek a jogosulatlan hálózati hozzáférés megakadályozása érdekében.
- Gondoskodjon róla, hogy az eszközök az internet irányából ne lehessenek elérhetőek.
- Gondoskodjon róla, hogy az eszközök ne legyenek elérhetőek az üzleti hálózatról, vagy egyéb nem megbízható hálózatról.
- A változás menedzsmentnek megfelelően a tesztelés után a gyártó által kiadott javításokat telepítse. Amennyiben nem lehetséges, vagy nem áll rendelkezésre a frissítés, ellenőrizze, hogy a naplófájlok ellenőrzése megfelelően működik.
- Ha a távoli hozzáférés elvárás, akkor azt biztonságos csatornán (pl.: VPN) keresztül valósítsa meg. A VPN is sérülékeny lehet, ezért biztosítsa, hogy mindig a legfrissebb verzió álljon rendelkezésre a használat során.

A riasztás a következő linken található:

https://www.us-cert.gov/ics/alerts/ics-alert-19-225-01

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

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

ICS jó gyakorlatok, javaslatok

Az önkéntes kibervédelmi összefogás készített egy intézkedés gyűjteményt az ipari irányító rendszerek kiberbiztonságának fejlesztéséhez. A jelenleg 26 kontrollpontot meghatározó poszter folyamatosan bővítésre került az elmúlt időszakban, a informatikai biztonságot érintő újdonságokkal.

kibev
önkéntes kibervédelmi összefogás
voluntary cyber defence collaboration

Az intézkedésgyűjtemény az Amerikai Egyesült Államok Energiaügyi Minisztériuma (Department of Energy, DoE) által kiadott, "21 Steps to Improve Cyber Security of SCADA Networks" című kiadványán alapul.

Az ipari irányító rendszerek sajátosságainak megfelelően a kiadvány átfogó képet ad arra vonatkozóan, hogy miként kellene az információbiztonságot elérni, és megfelelő szinten tartani az érintett szervezeteknek.

Az intézkedés gyűjtemény a következő linken található:

http://www.kibev.hu/images/publikaciok/kibev_intezkedesek_tabla_2017_A0-v2.pdf

ICS képzések, oktatások

A teljeség igénye nélkül 2019. szeptemberben ICS biztonság tárgyában a következő tréningek, oktatások kerülnek lebonyolításra:

2019. szeptemberben a következő tréning, oktatás kerül lebonyolításra az ICS/SCADA biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS; Dubai, Egyesült Arab Emirátusok; 2019. szeptember 15-19.
- ICS410: ICS/SCADA Security Essentials SANS; Las Vegas, Nevada, USA; 2019. szeptember 9-13.
- ICS410: ICS/SCADA Security Essentials SANS; London, Egyesült Királyság; 2019. szeptember 23-27.

A részletek a következő web-helyen találhatók:

https://www.sans.org/event/dubai-september-2019/course/ics-scada-cyber-security-essentials
https://www.sans.org/find-training-beta/search?courses=2762&types=5&redirect=beta#__utma=195150004.1547647064.1563952209.1563952209.1566466053.2&__utmb=195150004.3.9.1566466119873&__utmc=195150004&__utmx=-&__utmz=195150004.1566466053.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=127680205

Az infosecinstitute.com honlap által 2019. szeptember hónapra hirdetett SCADA biztonsággal kapcsolatos képzés:

- SCADA/ICS Security Training Boot Camp; Dulles, Virginia, USA; 2019. szeptember 16-20.

A részletek a következő web-helyen találhatók:

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

A 10 éves CSCAMP 2019. szeptemberi ICS kiberbiztonsági alapokról szóló képzése a CyberTalents és még számos platina szponzor szervezésében:

- Post-Conference Training | ICS Cyber Security Essentials – ICSE; Kairó, Egyiptom; 2019. szeptember 23-24.

A részletek a következő web-helyen találhatók:

https://cairosecuritycamp.com/sessions/ics-cyber-security-essentials-icse/

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 Univesity 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 (a következő online kurzusokra előre leghamarabb 2019. decemberre lehet regisztrálni):

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

További részletek a következő webhelyen találhatók:

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

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=195150004.1547647064.1563952209.1563952209.1566466053.2&__utmb=195150004.4.9.1566466121455&__utmc=195150004&__utmx=-&__utmz=195150004.1566466053.2.2.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=10670452

ICS konferenciák

A nyár és a szabadságok elmúltával érezhetően megugrik a konferenciák száma! A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2019. szeptemberben:

ICS-Cybersec2019

Az ipari irányító rendszerek egy napos, 4. éves kibervédelmi konferenciáján szó lesz többek között az ICS és IoT rendszerek elleni támadások realitásairól, a nem menedzselt eszközök áradatának problémáiról, a kontrol rendszerek monitoring és védelmi módszereiről, a sérülékenységek csökkentésének lehetőségeiről, a Simatic S7 PLC-k elleni trükkös támadásokról, a kritikus infrastruktúrák kibervédelméről és még sok kapcsolódó témáról.

ICS-Cybersec2019; Lago event hall, Izrael; 2019. szeptember 24.

További részletek a következő webhelyen találhatók:

https://www.icscybersec.co/

ICS CSR 2019.

A 6. nemzetközi ICS és SCADA Kiberbiztonsági Kutatásokról szóló 3 napos Szimpózium szeptember közepén kerül megrendezésre. Az ICS rendszerek folyamatosan növekvő kiber fenyegetéseknek való kitettség miatt szó lesz többek között az ICS rendszerek hardver/firmware használatának biztonságáról, a biztonságos architektúrákról, a sérülékenységek monitorozásáról. Az említett témákat érintő magas színvonalú kutatások is terítékre kerülnek a rendezvényen.

6th International Symposium for ICS & SCADA Cyber Security Research 2019; University of Piraeus, Görögország, Pireusz; 2019. szeptember 10-12.

További részletek a következő webhelyen találhatók:

http://www.ics-csr.com/

Kaspersky Industrial Cybersecurity Conference 2019

A 7. nemzetközi ipari kiberbiztonsági 3 napos konferencián több, mint 20 ország szakértői képviseltetik magukat. A konferencián résztvevőknek lehetőségük lesz megvitatni az ipari irányító rendszereket érintő fontosabb témákat neves szakértőkkel, és megosztani tapasztalataikat az új technológiák ICS rendszerekbe történő implementálásáról. Új trendek, fenyegetettségek és az ellenállóképesség, mint témák szintén megjelennek a konferencián.

Kaspersky Industrial Cybersecurity Conference 2019; Szocsi, Oroszország; 2019. szeptember 18-20.

További részletek a következő webhelyen találhatók:

https://ics.kaspersky.com/conference/

CRITIS 2019

14. alkalommal kerül megrendezésre a 3 napos-, iparban és egyéb ágazatokban használt kritikus információs infrastruktúrák védelméről szóló konferencia. A téma akadémikusai, kutatói, valamint a kritikus információs infrastruktúrák üzemeltetői egyaránt jelen lesznek a rendezvényen, ahol ismertetésre kerülnek friss kutatási eredmények is, melyek közül egy kutató a Legjobb Fiatal CRITIS Kutató díját is elnyeri.

CRITIS2019 The 14th International Conference on Critical Informtaion Infrastructures Security; Linköpping, Svédország, 2019. szeptember 23-25.

További részletek a következő webhelyen találhatók:

https://critis2019.on.liu.se/index.html

International Workshop on Survivable Industrial Control Systems (SICS)

A „túlélésre képes" ipari irányító rendszerek vonatkozásában a Workshop szervezőinek a célja, hogy a területen kutatók megosszák egymással a legutóbbi eredményeiket, tanulmányaikat és tapasztalataikat, és az ICS rendszerek túléléséhez szükséges egyéb aspektusokat.

International Workshop on Survivable Industrial Control Systems (SICS); Nápoly, Olaszország; 2019. szeptember 17-20.

További részletek a következő webhelyen találhatók:

https://infosec-conferences.com/events-in-2019/sics/

ICS incidensek

Ransomware támadás okozott áram kimaradást Johannesburgban

2019 júliusának végén egy ransomware támadás okozott áramkimaradást Dél-Afrika legnagyobb városában. A város árammal történő ellátásáért felelős szervezet (City Power), mely a helyi önkormányzat tulajdonában álló cég, a Twitteren megerősítette a támadás tényét, mely alapján az adatbázisok, alkalmazások és a hálózat is érintett volt a támadásban. A napelemmel rendelkező ügyfelek nem tudtak feltölteni a rendszerbe elektromos áramot, valamit a rendszerből történő energia egység vásárlás is blokkolásra került. A szervezet a ransomware nevét nem hozta nyilvánosságra, amely okozta az esetet.

A támadás következtében a City Power honlapja elérhetetlenné vált, az ügyfelek nem tudták a számláikat fizetni, valamint a vállalat sem tudta értesítési kötelezettségét ellátni a lokális áramkimaradásokról. A támadás által több, mint negyedmillió ember volt érintett, és maradt áram nélkül.

A közösségi médiában a vállalat megnyugtatta ügyfeleit, hogy az adataik nem kompromittálódtak a támadás által. A rendszerek helyreállításának tényét közölte nem sokkal később a vállalat, azonban a honlap sokáig nem volt még elérhető. A normál működés teljeskörűsége valószínűleg több hetet is igénybe vehet. Arról, hogy volt-e releváns mentés az adatokról, nem adott hírt sem a vállalat, sem a helyi önkormányzat.

A vállalat 2 nappal később elnézést kért a kellemetlenségekért, és a mielőbbi visszaállítás kapcsán reményét fejezte ki.

Források:

https://thehackernews.com/2019/07/cyberattack-power-outage.html?m=1

https://www.bbc.com/news/technology-49125853

https://www.zdnet.com/article/ransomware-incident-leaves-some-johannesburg-residents-without-electricity/

Szerző: Az incidens vonatkozásában megfogalmazódhat a kérdés, hogy az elmúlt évek ransomware eseményei vajon miért nem késztették a szervezetet arra, hogy valós kockázatként értékelje az effajta támadásokat, és miért nem történtek meg a preventív intézkedések? Minden fórumon ezekkel az információkkal és jó tanácsokkal lehetett és lehet a mai napig találkozni.

Amiatt, hogy nem adtak információt arra vonatkozóan, hogy volt-e biztonsági mentés az érintett fájlokról, rendszerekről, arra lehet következtetni, hogy nem volt. Ha lett volna, akkor valószínűleg ezzel nyugtatták volna meg az ügyfeleket. A ransomware nevének nyilvánosságra hozatala is valószínűleg a nem megfelelő felkészültséget demonstrálta volna.

További információbiztonsági kérdések is felmerülhetnek az olvasóban, de talán a legfontosabb, hogy nem volt felkészülve a szervezet egy zsarolóvírussal elkövetett támadásra.

Könyvajánló

A könyv bemutatja, hogy mi történik abban az esetben, amikor Európa teljes elektromos hálózata összeomlik. A következmények rendkívül szerteágazók, tovább gyűrűzik szinte az emberi élet minden egyes szegletébe a probléma.

A későbbiekben hekker támadás lehetősége is felmerül. A történet bonyolódása odáig vezet, hogy a rend már kizárólag a katonaság bevetésével tartható fenn.

(A történetben hasonlóságokat lehet felfedezni a Digitális Mohács és a Digitális Mohács 2.0 alapvetéseivel. Dr. Kovács László és Dr. Krasznay Csaba a Nemzeti Közszolgálati egyetem munkatársai szintén arra próbálnak meg rávilágítani, hogy mekkora problémát jelenthetnek a kritikus infrastruktúrák elleni támadások a társadalom egészére nézve.)

A könyv több nyelven is elérhető, többek között angolul és németül. Az Európai Unió tagállamai és a szomszédos országok Bécsben rendezett 2018. júliusi kritikus infrastruktúra védelmi találkozóján is ajánlotta az Európai Bizottság a könyvet.

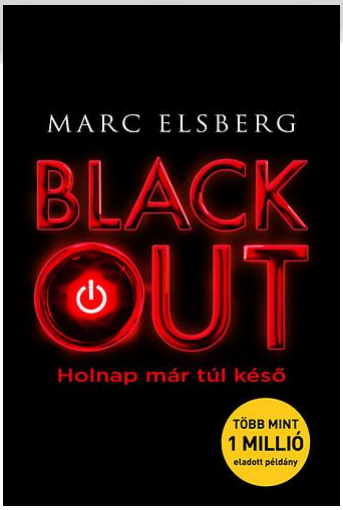
A könyv címe: Blackout - Holnap már túl késő

Szerzők: Marc Elsberg

Kiadás éve: 2016.

https://bookline.hu/product/home.action?type=22&_v=Marc_Elsberg_Blackout_Holnap_mar_tul&id=285073

https://www.amazon.de/Blackout-Marc-Elsberg/dp/1784161888



Kiegészítő információ: A 2019. 3. számú ICS hírlevélben ajánlott Industrial Network Security könyv Pdf. formátumban a következő Linken érhető el:

https://www.pdfdrive.com/industrial-network-security-securing-critical-infrastructure-networks-for-smart-grid-scada-and-other-industrial-control-systems-d176022253.html

Black Cell javaslatok

Az ICS rendszerek kiberbiztonsági megfelelésének vizsgálatához kevés jó gyakorlat vagy ajánlás áll rendelkezésre. Az egyik kiváló módszertan a NIST 800-82, amely az ipari irányító rendszerek biztonsági útmutatója.

Több olyan dologra is felhívja a figyelmet az ICS rendszerek biztonságának kialakításánál, mint a szegmentáció, port kezelés, fizikai és egyéb kockázatok, üzleti szempontok figyelembevétele a biztonság kialakítása során, és még lehetne sorolni.

Számos ICS architektúra, és annak biztonsági jó tanácsai is megjelennek a módszertanban, illetve a különböző felépítésű rendszerek kockázatainak bemutatására is nagy hangsúlyt fektet az ajánlás.

Az ICS rendszerek világában is folyamatosan változnak a körülmények, akár technológiai- akár szabályozási kérdésekről van szó, ezért a dokumentum is ennek megfelelően kerül változtatásra. Jelenleg a második verzió érhető el, de hamarosan várható a következő kiadás az újdonságok beépítésével.

A módszertan ingyenes, bárki számára elérhető a következő weboldalon:

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Bármilyen IT vagy információbiztonsági audit segít az egyedi rendszerek kockázatainak és sebezhetőségeinek az azonosításában, de a speciális módszertanok alkalmazása javasolt, annak érdekében, hogy a teljeskörűségre törekvés biztosított legyen.