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.

2019. június 6-án az ipari irányító rendszerek kritikus rendszerelemeinek beazonosításához kialakított metodológiáról, a Crown Jewels Analysis-ról további információkhoz juthat, ha a következő linken megtekinti a 15:00 órától kezdődő webinárt: https://blackcell.hu/keynote/.

Amennyiben a Black Cell Compliance, Audit & Risk Assessment üzletágának szolgáltatásairól többet szeretne megtudni, kérem látogassa meg a https://blackcell.hu/ webcímet vagy keressen bennünket a CARA@BlackCell.hu e-mail címen vagy a +36 1 605 0302 telefonszámon.

Tartalom:

ICS sérülékenységek

2019. májusában 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-19-150-01: AVEVA Vijeo Citect and CitectSCADA
Közepes szintű sérülékenység: nem megfelelő hitelesítés védelem.
https://ics-cert.us-cert.gov/advisories/ICSA-19-150-01

ICSA-19-148-01: Emerson Ovation OCR400 Controller
Közepes szintű sérülékenységek: Puffer túlcsordulás.
https://ics-cert.us-cert.gov/advisories/ICSA-19-148-01

ICSA-19-141-01: Computrols CBAS Web
Magas szintű sérülékenységek: CSRF, XSS, eltérés okozta információ expozíció, parancs befecskendezés, forráskódon keresztüli információ expozíció, beégetett kriptográfiai kulcsok, SQL befecskendezés, hitelesítés megkerülése alternatív úton, nem megfelelő erősségű titkosítás.
https://ics-cert.us-cert.gov/advisories/ICSA-19-141-01

ICSA-19-141-02: Mitsubishi Electric MELSEC-Q Series Ethernet Module
Magas szintű sérülékenység: Kontrollálatlan hozzáférés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-141-02

ICSA-19-136-01: Schneider Electric Modicon Controllers
Közepes szintű sérülékenység: Nem megfelelő véletlen érték használat.
https://ics-cert.us-cert.gov/advisories/ICSA-19-136-01

ICSA-19-136-02: Fuji Electric Alpha7 PC Loader
Alacsony szintű sérülékenység: nem megfelelő, határokon kívül lévő adatok olvasása.
https://ics-cert.us-cert.gov/advisories/ICSA-19-136-02

ICSA-19-134-01: Omron Network Configurator for DeviceNet
Magas szintű sérülékenység: Keresési útvonal kontrolljának hiánya.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-01

ICSA-19-134-02: Siemens SIMATIC WinCC and SIMATIC PCS 7
Kritikus szintű sérülékenység: kritikus funkciók hitelesítésének hiánya.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-02-0

ICSA-19-134-03: Siemens LOGO! Soft Comfort
Magas szintű sérülékenység: megbízhatatlan adatok nem megfelelő meghatározása.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-03

ICSA-19-134-04: Siemens LOGO!8 BM
Kritikus szintű sérülékenységek: kritikus funkciók hitelesítésének hiánya, értékek helytelen kezelése, jelszavak plaintext formában történő tárolása.

https://ics-cert.us-cert.gov/advisories/ICSA-19-134-04

ICSA-19-134-05: Siemens SINAMICS PERFECT HARMONY GH180 Drives NXG I and NXG II
Közepes szintű sérülékenység: Kontrollálatlan hozzáférés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-05

ICSA-19-134-06: Siemens SINAMICS PERFECT HARMONY GH180 Fieldbus Network
Közepes szintű sérülékenység: Nem megfelelő input hitelesítés
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-06

ICSA-19-134-07: Siemens SCALANCE W1750D
Kritikus szintű sérülékenységek: parancs befecskendezés, információ expozíció, XSS.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-07

ICSA-19-134-08: Siemens SIMATIC PCS 7, WinCC, TIA Portal
Kritikus szintű sérülékenységek: SQL befecskendezés, kivételek nem megfelelő kezelése, nem megfelelő funkció korlátozás.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-08

ICSA-19-134-09: Siemens SIMATIC Panels and WinCC (TIA Portal)
Közepes szintű sérülékenységek: beégetett hitelesítők használata, hitelesítés nem megfelelő védelme, XSS.
https://ics-cert.us-cert.gov/advisories/ICSA-19-134-09

ICSA-19-122-01: Orpak SiteOmat
Kritikus szintű sérülékenységek: beégetett hitelesítők használata, XSS, SQL befecskendezés, adatok titkosításának a hiánya, kód befecskendezés, puffer túlcsordulás.
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-01

ICSA-19-122-02: GE Communicator
Magas szintű sérülékenységek: Keresési útvonal kontrolljának hiánya, nem megfelelő hozzáférés ellenőrzés, beégetett hitelesítők használata.
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-02

ICSA-19-122-03: Sierra Wireless AirLink ALEOS
Kritikus szintű sérülékenységek: OS parancs befecskendezés, beégetett hitelesítők használata, korlátozás nélküli fájl feltöltés, XSS, CSRF, információ expozíció, adatok titkosításának a hiánya.
https://ics-cert.us-cert.gov/advisories/ICSA-19-122-03

A sérülékenységek részletei 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. május hónapban az ICS-CERT nem adott ki riasztást.

ICS jó gyakorlatok, javaslatok

Az ENISA 2019. május 20-án publikálta az „Industry 4.0 - Cybersecurity Challenges and Recommendations" dokumentumát, amelyben az ipari 4.0 és az IoT biztonsági intézkedéseinek és megoldások elfogadásának főbb kihívásait mutatja be. Ezen túlmenően az ENISA magas szintű ajánlásokat ad a különböző érdekelteknek az ipari 4.0 és az IoT biztonsági intézkedések bevezetésének megkönnyítése érdekében.

A dokumentum a következő webhelyről tölthető le:

https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

2019. május 7-én a NCCoE és a NIST publikációt tett közzé az Energia szektor szcenárió alapú kiberbiztonságáról, melyben különböző forgatókönyvek alapján az energia ágazatban lévő összekapcsolt rendszerek információcseréjének biztonságáról van szó.

A dokumentum a következő webhelyről tölthető le:

https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-iiot-project-description-draft.pdf

ICS képzések, oktatások

A teljeség igénye nélkül 2019. júniusában a következő tréningek, oktatások kerülnek lebonyolításra az ICS biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials, SANSFIRE 2019; USA, Washington, DC; 2019. június 17-21.
- ICS410: ICS/SCADA Security Essentials, SANS ICS Europe 2019; Németország, München; 2019. június 25-29.

A részletek a következő web-helyen találhatók:

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

- SCADA/ICS Security Training Boot Camp; Online végezhető kurzus; 2019. június 17-21.

A részletek a következő web-helyen találhatók:

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

- NIST Open Industrial Digital Ecosystem Summit and OAGi Symposium; National Cybersecurity Center of Excellence (NCCoE), 9700 Great Seneca Highway, Rockville, MD 20850; 2019. június 3-6.

A részletek a következő web-helyen találhatók:

https://www.nist.gov/news-events/events/2019/06/nist-open-industrial-digital-ecosystem-summit-and-oagi-symposium

Időszakosan induló online kurzusok:

A 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/courses?query=Industrial%20IoT%20Markets%20and%20Security&

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/

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

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- 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 SCADAhacker.com szintén kínál Online kurzust az ipari irányító rendszerek biztonságáról, amely a következőkre koncentrál: az ipari irányító rendszerek architektúrájának biztonságára, mély technikai ismeretekre, az ICS specifikus kontrollok implementációjára.

- Understanding, Assessing and Securing Industrial Control Systems

További részletek a következő webhelyen találhatók:

https://www.scadahacker.com/training.html

ICS konferenciák

A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2019. júniusában:

Kétnapos workshop keretében az ipari irányító rendszerek fenyegetéseinek megértése, és az elérhető kiberbiztonsági megoldások kerülnek középpontba. A munkaműhely keretében egy támadás felismerése, valamint a technikai elemzés is kiemelt témaként jelenik meg.

Asia ICS Cyber Security Conference; Ibis Hotel Bencoolen Singapore; 2019. június 20-21.

További részletek a következő webhelyen találhatók:

https://asiaicsc.com/

Kétszer két napos konferencia keretében a SCADA biztonság iránt érdeklődők a technikai területeken az üzembiztonság és sz informatikai biztonság kapcsán juthat új információkhoz. A workshop végén tanúsítványt is kapnak a résztvevők a workshopot követően.

SCADA & ICS cyber security workshops; Perth – 2019. június 24-25. és Sydney 2019. június 27-28.

További részletek a következő webhelyen találhatók:

https://www.mysecuritymarketplace.com/product/scada-ics-cyber-security-workshops/

Kétnapos konferencia kerül megrendezésre az energia, közlekedés és a termelési ágazati szereplők részére az ipari IoT kapcsán, melyen a való életből hozott példák elemzésével lehetőség lesz megvitatni a konzekvenciákat csoportos beszélgetések alkalmával.

Industrial IoT USA; Chicago, Illinois; 2019. június 18-19.

További részletek a következő webhelyen találhatók:

https://www.industrialiotseries.com/usa/?ref=infosec-conferences.com

ICS incidensek

Az Egyesült Államokban DDoS támadás okozott incidenst az elektromos hálózat üzemeltetése során

A Western Electricity Coordinating Council (WECC) által monitorozott és felügyelt rendszert érintette az incidens. Elektromos-áramkimaradás nem történt, de egy kiberesemény következtében az érintett rendszereket helyre kellett állítani, amely körülbelül 8 és fél órás rendszerkimaradást okozott. A későbbiek során kiderült, hogy DDoS támadás áll az esemény mögött. Nem egyértelmű, hogy mely berendezések voltak pontosan a támadók célkeresztjében. A támadás nem egy összehangolt hekkerakció, hanem egy ismert sérülékenységkihasználás következménye, amely azóta kijavításra került. A The Electricity Information Sharing and Analysis Center figyelmeztette az üzemeltetőt, hogy tájékoztassa a többi szolgáltatót. Gyakran elhangzik, hogy az ipari irányító rendszerekre nagyobb veszélyt jelent a DDoS támadás, mint az IT rendszerekre. Szakértők elmondása alapján az ilyen típusú események mutatnak rá, hogy mennyire fontos a felügyeleti rendszerek bevezetése. A tavaly közzétett jelentések azt mutatták, hogy az incidensek leginkább az energiaszektorban, az ipari irányító rendszerek sérülékenységeivel vannak összefüggésben, és hogy számos interfész (HMI) érintett ebben. 2019. év elején kiderült, hogy egy amerikai energiavállalat 10 millió dolláros bírságot kapott a North American Electric Reliability Corporation-től (NERC) a kritikus infrastruktúra védelmi (CIP) szabványok 130 alkalommal történő megsértése miatt.

Forrás: https://www.securityweek.com/dos-attack-blamed-us-grid-disruptions-report
További információk: https://www.eenews.net/stories/1060281821

Black Cell javaslatok

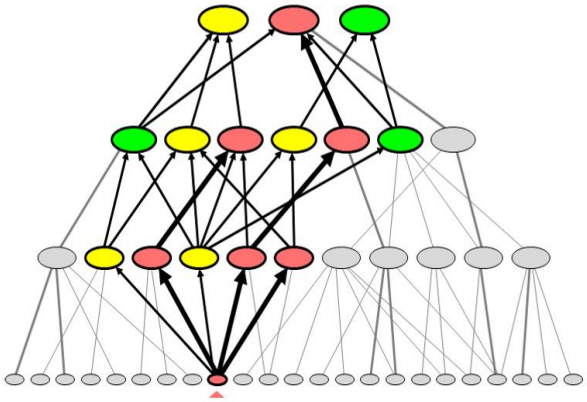
Az ipari irányító rendszerek üzemeltetése nagymértékben informatikai alapokon nyugszik, és az információbiztonsági szempontok figyelembevétele az üzletmenet-folytonosság garantálásához elmaradhatatlan. Ahhoz, hogy tisztában legyen az üzemeltető, hogy melyek a szervezeti célok elérése szempontjából kritikus IT eszközök, javasolt a Crown Jewels Analysis elvégzése. Az elemzés elvégzését követően meghatározhatók azok az IT eszközök, amelyek védelmét prioritásként kell kezelni, és a védelmet azokra kell összpontosítani.

2019. június 6-án az elemzésről bővebb információkhoz juthat, ha megtekinti a 15:00 órától kezdődő webinárt. https://blackcell.hu/keynote/

Napjainkban az egyik legnagyobb fenyegetést egy szervezet elektronikus információs rendszereire a célzott támadások, valamint az állandó fenyegetések (APT – Advanced Persistent Threat) jelentik. Ahhoz, hogy egy szervezet tisztában legyen a fenyegetések és támadások szervezeten belül található, a külső támadók lehetséges célpontjaival, azonosítania kell azon IT eszközeit, amelyektől függ a szervezet működése.

A CJA segítségével azonosításra kerülnek a szervezet működése szempontjából kritikus IT eszközök, melyekre a későbbiekben felépíthető a kockázatokkal arányos védelmi rendszer, megelőzhetők a célzott támadások, és a minimális szintre csökkenthető az APT csoportok, vagy egyéb támadó által elkövetett állandó fenyegetések kockázata.

Egy szervezet védelmi stratégiájának felépítéséhez mindenképp szükséges a Koronaékszerek ismerete, enélkül felesleges erőforrás allokáció mellett hamis biztonságérzet alakulhat ki a felsővezetők, és a szervezeti biztonság megteremtésében résztvevő egyéb szereplők körében.



A koronaékszerek azonosításán túl számos más előnnyel járhat a CJA elvégzése, és lehetőség nyílik az eredmények rendkívül sokrétű felhasználására.

https://blackcell.hu/crown-jewels-analysis/