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. júliusban 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-19-211-01: **Wind River VxWorks**

Kritikus szintű sérülékenységek: Puffer túlcsordulás, egész érték probléma, a műveletek nem megfelelő korlátozása a memória pufferen belül, megosztott erőforrások helytelen szinkronizációja, argumentum módosítás, IPv4 multicast-cím helytelen célhoz rendelése, argumentum befecskendezés vagy módosítás.
https://www.us-cert.gov/ics/advisories/icsa-19-211-01

ICSA-19-211-02: **Prima Systems FlexAir**

Kritikus szintű sérülékenységek: operációs rendszer parancs befecskendezés, veszélyes fájlok korlátozatlan feltöltésének lehetősége, CSRF, XSS, lehetséges értékek korlátozott száma, biztonsági mentések kitettsége hitelesítetlen területen, nem megfelelő hitelesítés, beégetett hitelesítők.
https://www.us-cert.gov/ics/advisories/icsa-19-211-02

ICSA-19-204-01: **Mitsubishi Electric FR Configurator2**

Magas szintű sérülékenységek: XML külső elem hivatkozásának nem megfelelő korlátozása, kontrollálatlan erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-204-01

ICSA-19-204-02: **NREL EnergyPlus**

Közepes szintű sérülékenység: Puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-204-02

ICSA-19-199-01: **Johnson Controls exacqVision Server**

Közepes szintű sérülékenység: Nem jegyzett keresési útvonal vagy elem.
https://www.us-cert.gov/ics/advisories/icsa-19-199-01

ICSMA-19-192-01: **Philips Holter 2010 Plus**

Alacsony szintű sérülékenység: Elavult funkció használata.
https://www.us-cert.gov/ics/advisories/icsma-19-192-01

ICSA-19-192-01: **Delta Industrial Automation CNCSoft ScreenEditor**

Magas szintű sérülékenységek: puffer túlcsordulás, pufferen kívüli olvasás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-192-01

ICSA-19-192-02: **Siemens SIMATIC WinCC and PCS7**

Magas szintű sérülékenység: Veszélyes fájlok korlátozatlan feltöltésének lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-192-02

ICSA-19-192-03: **Siemens TIA Administrator (TIA Portal)**

Magas szintű sérülékenység: Nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-192-03

ICSA-19-192-04: Siemens SIMATIC RF6XXR
Közepes szintű sérülékenységek: Nem megfelelő bemeneti hitelesítés, kriptográfiai hiányosságok.
https://www.us-cert.gov/ics/advisories/icsa-19-192-04

ICSA-19-192-05: AVEVA Vijeo Citect and Citect SCADA Floating License Manager
Kritikus szintű sérülékenységek: Nem megfelelő bemeneti hitelesítés, pufferen kívüli memória írás olvasás.
https://www.us-cert.gov/ics/advisories/icsa-19-192-05

ICSA-19-192-06: Schneider Electric Interactive Graphical SCADA System
Magas szintű sérülékenység: Puffer határain kívüli írás lehetősége.
https://www.us-cert.gov/ics/advisories/icsa-19-192-06

ICSA-19-192-07: Schneider Electric Floating License Manager
Kritikus szintű sérülékenységek: Nem megfelelő bemeneti hitelesítés, pufferen kívüli memória írás olvasás.
https://www.us-cert.gov/ics/advisories/icsa-19-192-07

ICSMA-19-190-01: GE Aestiva and Aespire Anesthesia
Közepes szintű sérülékenység: Nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsma-19-190-01

ICSA-19-190-01: Emerson DeltaV Distributed Control System
Közepes szintű sérülékenység: beégetett hitelesítők használata.
https://www.us-cert.gov/ics/advisories/icsa-19-190-01

ICSA-19-190-02: Rockwell Automation PanelView 5510
Magas szintű sérülékenység: Nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-19-190-02

ICSA-19-190-03: Schneider Electric Zelio Soft 2
Magas szintű sérülékenység: Memória felszabadítás utáni program összeomlás.
https://www.us-cert.gov/ics/advisories/icsa-19-190-03

ICSA-19-190-04: Siemens Spectrum Power
Közepes szintű sérülékenység: XSS
https://www.us-cert.gov/ics/advisories/icsa-19-190-04

ICSA-19-190-05: Siemens SIPROTEC 5 and DIGSI 5
Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-190-05

ICSA-19-183-01: Schneider Electric Modicon Controllers
Magas szintű sérülékenység: szokatlan vagy kivételes feltételek nem megfelelő ellenőrzése.
https://www.us-cert.gov/ics/advisories/icsa-19-183-01

ICSA-19-183-02: Quest KACE Systems Management Appliance
Alacsony szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-19-183-02

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.

ICS riasztások

2019. július hónapban az ICS-CERT az alábbi riasztást adta ki:

A CAN busz hálózatok repülőgépeket érintő nem biztonságos megvalósításáról szóló nyilvános jelentés alapján a rendszert érintő sérülékenységek kihasználhatók, ha egy támadó fizikailag hozzáfér egy repülőgéphez.

A repülőgéphez fizikai hozzáféréssel rendelkező támadó csatlakoztathat egy eszközt a CAN buszhoz, amely hamis adatok bevitelére ad lehetőséget, és ez hibás értékek megjelenítését okozza a repülési rendszerekben. A telemetriai mérések az iránytű és a helyzetével kapcsolatos adatok, a magasság, a légsebesség mind manipulálhatók, mely következtében hamis mérések állhatnak a pilóta rendelkezésére. A műszerek adataira támaszkodó pilóta nem képes megkülönböztetni a hamis és hiteles adatokat, ami egy érintett repülőgép irányításának elvesztését is eredményezheti.

A kockázatok csökkentése érdekében a repülőgépekhez történő fizikai hozzáférések lehetőségét csökkenteni kell, és az ellenőrzést erősíteni.

A repülőgépgyártóknak felül kell vizsgálniuk a CAN busz hálózatot a sérülékenység tudatában. Az autóipar már számol a hasonló kockázatokkal, és olyan technológiát alkalmaznak, amelyek akadályozzák a CAN busz rendszerekhez való hozzáférésekkel megvalósítható támadásokat. A légijármű gyártóknak figyelembe kell venni a CAN busz-specifikus szűrési és engedélyezési listákat, valamint gondoskodni szükséges az elkülönítésről.

A riasztásról bővebb információk a következő linken találhatók:

https://www.us-cert.gov/ics/alerts/ics-alert-19-211-01

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

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

ICS jó gyakorlatok, javaslatok

15 Kiberbiztonsági alapvetés a víz- és szennyvíz és ivóvíz szolgáltatók számára

Az ivóvíz és szennyvíz szolgáltatók az emberi életvitelhez nélkülözhetetlen szolgáltatásokat nyújtanak. Ezt kizárólag biztonságos információ technológia és üzemeltetés mellett lehetséges. A szolgáltatók hálózatait kiberbűnözők, állami és egyéb szereplők egyaránt támadhatják/támadják.

A szolgáltatók támogatása-, és a fenyegetésekre adandó válaszok kialakítására a WaterISAC publikált egy 15 alapvetésből álló kiberbiztonsági listát. 2012-ben készült az eredeti dokumentum, de mivel ezrek töltötték eddig le, ezért frissítésre került.

Az ajánlások a megfelelő technikai erőforrásokkal egészítették ki, amelyek releváns információkkal szolgálnak a mélyebb biztonsági megoldások terén.

Az útmutató segítséget nyújt a kockázatelemzés és az ellenállóképesség megfelelő kialakításában, továbbá a vészhelyzeti reagálási tervek fejlesztésében.

A 15 alapvetés a következő:

1. Információs vagyonelem leltár összeállítása,
2. Kockázatok értékelése,
3. A vezérlő rendszerek kitettségének minimalizálása,
4. A felhasználói hozzáférések megfelelő érvényesítése,
5. Jogosulatlan fizikai hozzáférés elleni védelem kialakítása,
6. Kiberbiztonsági rendszerek telepítése,
7. Megfelelő sérülékenység menedzsment kialakítása,
8. Kiberbiztonsági kultúra kialakítása a szervezetben,
9. Fejleszteni és javítani a kiberbiztonsági szabályozókat, eljárásrendeket,
10. Fenyegetettség észlelő és monitorozó rendszerek alkalmazása,
11. Megfelelő tervek megléte incidensek, vészhelyzetek, és katasztrófa esetére,
12. Belső fenyegetések kezelése,
13. Biztonságos ellátási lánc kialaktítása,
14. A szabályozók és eljárások az összes eszközt fedjék le (IoT, IIoT, Mobil stb.)
15. Vegyen részt a szervezet információ megosztó és együttműködési fórumokon.

Az útmutató bővebb információkat tartalmaz az alapvetésekkel kapcsolatban. Pdf formátumban a következő linken érhető el az útmutató:

https://www.waterisac.org/fundamentals?utm_source=hootsuite&utm_medium=linkedin&utm_term=nozomi%20networks&utm_content=d36c8fee-0fc9-47e5-b758-2e47e2b21bba&utm_campaign=

ICS képzések, oktatások

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

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

- ICS410: ICS/SCADA Security Essentials SANS; Prága, Csehország; 2019. augusztus 12-16.

A részletek a következő web-helyen találhatók:

https://www.sans.org/event/prague-august-2019/course/ics-scada-cyber-security-essentials#__utma=195150004.1547647064.1563952209.1563952209.1563952209.1

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

Az említett oktatásokon felül az ICS-CERT is kínál Online kurzusokat (a következő online kurzusokra előre leghamarabb 2019. novemberre 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

ICS konferenciák

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

Kétnapos konferencia a SCADA Technológiai Csúcstalálkozó, amely egy globális esemény. A legújabb műszaki fejlesztésekre, a SCADA és az ICS piacok gazdasági fejlődésére összpontosít. A konferencia megismételhetetlen alkalom a SCADA és ICS technológiák üzemeltetésében és biztonságában részt vevő szakemberek számára, hogy megismerjék a legújabb fejlesztéseket az alkalmazásokban, az új technológiákban, valamint a távoli és osztott berendezések tekintetében.

A konferencián információkhoz lehet jutni a kritikus infrastruktúrák és az ipari irányítási rendszerek biztonságának és technológiájának legújabb fejleményeiről.

Trends and Advancements in SCADA; SCADA and supporting ICS technologies; USA, Westin O'Hare; 2019. augusztus 28-29.

További részletek a következő webhelyen találhatók:

https://scadatechsummit.com/

ICS incidensek

Egy Raspberry PI okozta incidens

A NASA beszámolója szerint több, mint 100 GB adatot szivárogtattak ki a szervezettől, amelyek egy része 2009-ig visszamenőleg eredeztethető. Egy kiber támadó egy Raspberry PI nano számítógépet használva volt képes az említett adatok kiszivárogtatására.

A 2018. áprilisában elkövetett támadás közel egy éven keresztül észrevétlen volt az auditori jelentés szerint, és még most sem zárult le a vizsgálat, melynek a felelősök megállapítása a célja. A hekker a NASA sugárhajtású repülőgépeinek laboratóriumi hálózatába hatolt be észrevétlenül, és az űrrepülők rendszerről történő leválasztását célozta meg.

A behatolást követően a támadó érzékeny adatokhoz is hozzáfért, mint például a Mars Science Laboratory misszió fájljai, amelyek az amerikai fegyverkereskedelemre vonatkozó nemzetközi forgalom információit is tartalmazták.

Elgondolkodtató, hogy a támadó a három elsődleges JPL-hálózat közül kettőt sikeresen elért, emiatt a NASA dolgozók aggodalmukat is kifejezték, hogy megfelelő hozzáféréssel sikeres támadást hajthat végre egy támadó, amely rosszabb esetben emberéletekbe is kerülhet.

Az incidenst követően a NASA ideiglenesen lekapcsolt a JPL hálózatról több űrrepüléssel kapcsolatos rendszert is. Bár az incidens során kapcsolatot teremtő IP címek nagy része kínai, ennek ellenére nem tulajdonította a támadást a NASA egyetlen szereplőnek vagy országnak sem.

Az incidenst követően elkészült riport ajánlásokat fogalmaz meg a hálózat szegmentációjával kapcsolatban, valamint sokkal szigorúbb külső eszköz használatot fogalmaz meg.

Források:

https://www.darkreading.com/attacks-breaches/raspberry-pi-used-in-jpl-breach/d/d-id/1335034

https://www.ehackingnews.com/2019/06/hacker-uses-nanocomputer-to-steal-nasa.html

Szerző: Bár a meglehetősen hosszú riport rengeteg dologról tesz említést az incidenssel kapcsolatban, érdemes megjegyezni, hogy a folyamatba beépítésre került a külső segítségkérés, valamint az incidens nyilvánosság felé történő kommunikálása. Sajnos napjainkban kizárólag a segítségkérés a jellemző, a megfelelő kommunikáció már kevésbé. Azon szervezetek, amelyek abban reménykednek, hogy nem derül ki az incidens, és nem hozzák azt nyilvánosságra, hatalmas kockázatot vállalnak fel. Ha kommunikáció hiányában kerül nyilvánosságra egy ilyen incidens, az nagyobb károkat tud okozni, bizalom-, és reputációs veszteségek által. Érdemes előre felkészülni az ilyen esetekre, és kommunikációs stratégiát vagy eljárásrendet készíteni, természetesen az incidenskezelési eljárásrenddel összhangban.

Könyvajánló

Az ajánlott könyv az ipari irányító rendszerek biztonságát próbálja meg körül járni, az egyedi hálózatok, protokollok és alkalmazások szemszögéből. A fogalmak tisztázását követően a könyvben bemutatásra kerülnek az ipari hálózatok, az ipari irányító rendszerek kiber biztonságának története, a rendszerek tervezése, működése és architektúrái, az ipari hálózati protokollok.

Bemutatja a könyv továbbá, hogy milyen technikákkal, támadási fajtákkal lehet meghekkelni egy ipari irányító rendszert, illetve milyen kockázatok és sérülékenységek jellemzőek ezekre a rendszerekre. Szó esik továbbá a biztonság implementálásának lehetőségeiről, a hálózat szegmentálásáról, anomáliákról, fenyegetettségek detektálásáról, szabványokról és jogi szabályozókról.

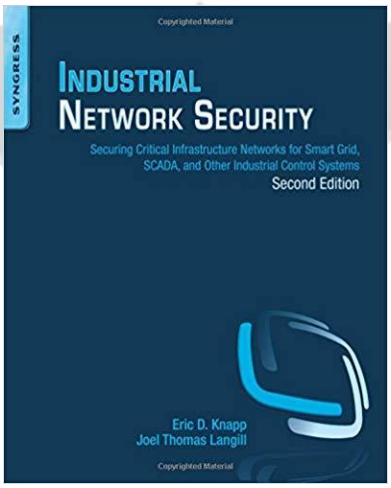
Akinek felkeltette az érdeklődését a könyv, érdemes beleolvasni. Erre a következő linken lehetősége nyílik az érdeklődőnek:

https://www.amazon.com/dp/0124201148/ref=rdr_ext_tmb

A könyv címe: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (második kiadás)

Szerzők: Eric D. Knapp és Joel Thomas Langill

Kiadás éve: 2015.



Black Cell javaslatok

Az Egyesült Államok (National Cybersecurity and Communications Integration Center - NCCIC) Nemzeti Kiberbiztonsági és Kommunikációs Integrációs Központja által publikált két oldalas dokumentum segítséget nyújt a kockázatok értékelésében, az internet és az ipari irányító rendszerek kapcsolatának vonatkozásában, nyilvánosan elérhető tool-ok ajánlásával.

A dokumentum említést tesz a Google hacking-ről, a keresőkről, mint erőforrásokról, továbbá bemutatja a Shodant, amely lehetőséget biztosít bárkinek arra, hogy az internetre csatlakoztatott eszközöket kereshesse meg bizonyos paraméterek alapján.

Az említett tool-ok segítségével a nyílt internet irányából lehet meggyőződni bizonyos irányító rendszerek nyíltságáról vagy esetleg zártságáról, és segítséget nyújtanak a sérülékenységek befoltozását követő visszaellenőrzésben is.

Az említett dokumentum a következő linken érhető el:

https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_OSTools_InternetFacingICS_S508C.pdf