10. 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

Az NCCIC (National Cybersecurity and Communications Integration Center – Amerikai Kiberbiztonsági és Kommunikációs Központ) számos jó gyakorlatot (dokumentumot) tesz közzé a honlapján, amely az ipari irányító rendszerek biztonságát hivatottak elősegíteni.

Ilyen az Ipari irányító rendszerek antivírus megoldásainak frissítéséről szóló dokumentum is. A dokumentumban kifejtésre kerül, hogy a rétegzett védelem része az antivírus szoftverek naprakészen tartása, frissítése. Mivel az ICS elemek gyakran demilitarizált zónában (DMZ) vannak elhelyezve, de az IT hálózatnak szükséges az ICS szerverek elérése, a megfelelő szeparáltság fenntartása miatt komplikált és nehéz feladat az antivírus megoldások naprakészen tartása.

Az antivírus megoldások megfelelő frissítésére ajánlott stratégiát kidolgozni. Többféle megoldás létezik, az egyik, hogy a vendor szerveréről a frissítés letöltésre kerül, és egy erre a célra dedikált adathordozón biztosításra kerül a cél szerverre történő eljuttatása a frissítésnek. Ebben az esetben meg kell róla győződni, hogy valóban a gyártó frissítése kerül a szerverre, és nem egy káros kód. Az adathordozókkal kapcsolatos biztonsági előírásokat is be kell tartani. Az adathordozóval kapcsolatos biztonsági intézkedésekről és a frissítés módjáról is további részletes információval szolgál a dokumentum.

A másik megoldás az automatikus frissítések implementációja. Ebben az esetben előfordul, hogy nincs ciklikus redundancia ellenőrzés, az alkalmazásban, vagy a kommunikációs protokollban. A frissítés integritása azonban magasabb szintű, mint a nem automatikus frissítések esetében. Az automatizmus is megállhat, vagy sérülhet a folyamat, ezért szükséges biztosítani a mechanikus frissítés lehetőségét is. Az automatikus frissítés során gyakran nem kerül a változás menedzsment minden előírása betartásra, ezért ezzel a nem megfelelőségi lehetőséggel számolni kell ebben az esetben.

Ha a frissítés nem várt következményekkel járna, és a tesztelés során sem kerülnek elő az adott problémák, abban az esetben biztosítani kell azt, hogy a frissítést megelőző állapot visszaállítható legyen. A változásmenedzsmentnek dokumentáltnak kell lenni, annak érdekében, hogy a megfelelő információk a megfelelő időben a megfelelő személyek részére rendelkezésre álljanak.

Minden esetben úgy szükséges megválasztani az antivírus megoldások frissítési megoldását, hogy a szervezet és az ICS rendszerek sajátosságai figyelembevételre kerülnek. A működési és biztonsági igényeknek találkozni kell egymással.

A dokumentum ajánlást tesz a biztonságos hálózati architektúra felépítésére vonatkozóan, illetve az ipari rendszerek különböző egységei (HMI, SCADA, DCS, szenzorok stb.) közötti adatkapcsolatok is bemutatásra kerülnek, ezáltal feltérképezhetők a gyenge pontok, és az antivírus megoldások frissítési korlátjai. További részletek a dokumentumban találhatók meg.

A dokumentum a következő linken érhető el:

https://www.us-cert.gov/sites/default/files/recommended_practices/Recommended%20Practice%20Updating%20Antivirus%20in%20an%20Industrial%20Control%20System_S508C.pdf

ICS képzések, oktatások

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

2020. márciusban a következő tréning, oktatás kerül lebonyolításra az ICS/SCADA biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS; Orlando, Florida, USA; 2020. március 4-8.
- ICS410: ICS/SCADA Security Essentials SANS; Szingapúr, Szingapúr; 2020. március 16-20.
- ICS410: ICS/SCADA Security Essentials SANS; Oslo, Norvégia; 2020. március 23-27.
- ICS410: ICS/SCADA Security Essentials SANS; Abu Dhabi, Egyesült Arab Emirátusok; 2020. március 29 – április 2.

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 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:

- 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:

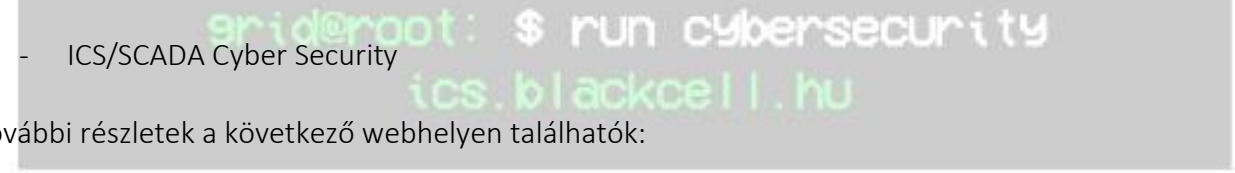
- ICS410: ICS/SCADA Security Essentials SANS

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

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

A teljesség igénye nélkül a következő konferenciák kerülnek megrendezésre 2020. márciusban:

SANS ICS Security Summit

A SANS szervezésében folyamatosan megrendezésre kerülő ipari irányító rendszerek biztonságáról szóló találkozón szó lesz az ellátási láncok biztonságáról, Közép- és Dél-Amerikai esettanulmányok által az említett kontinens országainak ICS biztonsági helyzetéről, valamint az IT és az OT közötti kapcsolatról.

Bemutatásra kerül az ICS hálózati csomagok elfogásáról szóló elemzés, továbbá az incidens kezelési program felépítésének módszere. Az ICS fenyegetések és az ICS ATT&CK részleteivel is megismerkedhetnek a látogatók, ahogy a célzott támadásokkal is. A tűzfal és protokoll biztonság is téma lesz a konferencián, valamint egy brazil esettanulmány is bemutatásra kerül, a kritikus infrastruktúrák védelméről.

SANS ICS Security Summit; Orlando, Florida, USA; 2020. március 2-3.

További részletek a következő webhelyen találhatók:

https://www.sans.org/event/ics-security-summit-2020/summit-agenda?msc=home

Cyber Security for Industrial Control Systems

A 2 napos konferencián szó lesz többek között a területet érintő jogi és egyéb szabályozókról, a NIS direktíva hatásairól, és a bevezetés óta eddig megszerzett tapasztalatokról. Az IIoT, vagyis az ipari dolgok internete témában az energia-, a közlekedés-, és a gyártási ágazatok jövőbeli kihívásai is említésre kerülnek.

Az ipari kontrol hálózat kockázatainak gyakorlati tapasztalatai is megosztásra kerülnek, illetve az ICS/OT tervezés során a biztonsági tervezés, mint napjaink alap elvárása. A fenyegetési térkép változása is bemutatásra kerül, továbbá a humán faktor, mint az ipari rendszerek kritikus siker tényezője.

Cyber Security for Industrial Control Systems; London, Egyesült Királyság; 2020. március 5-6.

További részletek a következő webhelyen találhatók:

https://events2.theiet.org/cyber-ics/programme.cfm

Africa ICS Cybersecurity Conference and Exhibitions 2020

A 4 napos negyedik alkalommal megrendezésre kerülő ipari irányító rendszerek kiberbiztonságáról szóló konferencia betekintést nyújt a résztvevők számára az afrikai gyakorlatba a témában. A konferencia az ICS/SCADA üzemeltetők vezetőinek, a kormányzati érintetteknek, az üzemeltetésben résztvevőknek szól.

A rendezvény lehetőséget biztosít megvitatni az ICS/SCADA kiberbiztonsági stratégiák és szabályozók megfelelőségét, technikai témáit, valamint a piacon fellelhető innovatív megoldások is középpontba kerülnek.

Africa ICS Cybersecurity Conference and Exhibitions 2020; Nairobi, Kenya; 2020. március 10-13.

További részletek a következő webhelyen találhatók:

https://www.itspmagazine.com/events/africa-ics-cybersecurity-conference-and-exhibitions-2020

CYBER SECURITY FOR CRITICAL ASSETS (Industrial Cyber Security Summit USA)

A 8. alkalommal megrendezésre kerülő kétnapos rendezvény a kritikus elemeket helyezi középpontba, a sérülékenységek, és a fenyegetések tükrében. IT és OT szakemberek véleményét lehet megismerni a regisztrálóknak, amelyek panelbeszélgetéseken ismerhetők meg. A maradványkockázatok csökkentésére is javaslatot tesznek a szakértők.

Az OT vállalati szabályozásának struktúrája is a konferencia témái között szerepel, valamint a humán és gépi interakciók kultúrájának mikéntje.

Industrial Cyber Security Summit USA; Houston, Texas, USA; 2020. március 24-25.

További részletek a következő webhelyen találhatók:

https://usa.cs4ca.com/agenda/

ICS incidensek

A Snake Ransomware az ipari irányító rendszerek folyamatait és állományait támadja

A SentinelOne jelentése szerint a közelmúltban felfedezett Snake Ransomware az ipari irányító rendszerek folyamatait és állományait támadja. A zsaroló program Goland programnyelven íródott, és az egész világon jelen lévő ICS rendszereket támadja.

A zsarolóvírus úgy került kialakításra, hogy ne az egész hálózat legyen a célkeresztben, hanem egyes számítógépek és szerverek. A kutatók azonban nem tudták még teljesen feltérképezni a Snake Ransomware-t. Mint más zsarolóvírusok, a Snake is futása esetén törli az árnyékmentéseket, és megpróbál sok SCADA rendszer béli folyamatot ellehetetleníteni, mint például a távoli menedzsment, hálózati és szoftver menedzsment stb.

Ezt követően a malware titkosítja a fájlokat a rendszerben, a Windows rendszer fájlokat és mappákat kivéve. A fájl kiterjesztések 5 karakter hosszúsággal megnőnek. A titkosítási folyamatot követően a váltságdíjról szóló levél a következő helyen kerül elhelyezésre: C:\Users\Public\Desktop folder; ez tartalmazza az e-mail címet is: bapcocrypt@ctemplar.com, annak érdekében, hogy a fizetési utasítások egyeztethetők legyenek a támadókkal.

A Snake kampányszerűen a 2019-es év végén jelent meg, és leginkább a GE termékcsalád van veszélyben a károkozó által a szakértők szerint. Egyes közel-keleti kiberbiztonsági cégek Iránt sejtik a támadások mögött.

A szakértők olyan hasonlattal éltek a Snake zsarolóvírussal kapcsolatban, hogy olyan, mintha bekötött szemmel vezetnénk a rendszert, és még a kormányt is elvennék tőlünk. A Snake leállítja a kritikus hálózati folyamatokat, ez lehetővé teszi az átjárást a HMI/SCADA, MES (Manufacturing Execution Systems) és EMI (Enterprise Manufacturing Intelligence) kapcsolatok között. Enélkül pedig nemcsak vakon és kormány nélkül kellene vezetni, hanem még meg is süketülnénk, és megnémulnánk…

Szakértők szerint a támadók e-mail címében lévő Bapco kifejezés utalhat a Bahrein Petroleum Company ellen elkövetett Dustman kártevővel megvalósított támadásra. Szaúd-Arábia Nemzeti Kiberbiztonsági Hatósága is megerősítette, hogy a Dustman kártevőt az energia szektor és egyéb ipari rendszer üzemeltető szervezetek ellen vetették be a Közel-Keleten.

További információk a következő linken találhatók:

https://securityaffairs.co/wordpress/96939/malware/snake-ransomware-ics.html

A Snake Ransomware eltávolításáról információk a következő webhelyen találhatók meg:

https://www.pcrisk.com/removal-guides/16723-snake-ransomware

Könyvajánló

A könyv elolvasásával az olvasó betekintést nyerhet az ipari dolgok internetének (Industrial Internet of Things - IIoT) architektúrájának biztonsági koncepcióiba, továbbá az olyan komplex témakörök is tisztázásra kerülnek az ipart illetően, mint a blokklánc technológia, vagy a kriptográfia. Az ipari szabványokat is érinti a könyv, mint amelyek segítséget nyújtanak a IIoT biztonsági tervezés során.

A szerző segít megérteni a több-szintű IIoT biztonsági keretrendszer kritikus pontjainak azonosítását, betekintést enged az azonosítási, és konfigurációs kérdésekbe, a felhő alapú kapcsolatok biztonságába, valamint esettanulmányokkal szemlélteti az IoT fenyegetettség lemodellezését, a kockázatok menedzsmentjét és a kockázatcsökkentés tervezését.

A könyv a témához kapcsolódó valamennyi érintettnek szól, vagyis a kutatóknak, biztonsági szakembereknek, architektúra tervezőknek és fejlesztőknek, üzemeltetőknek, továbbá az üzletben érdekelt feleknek.

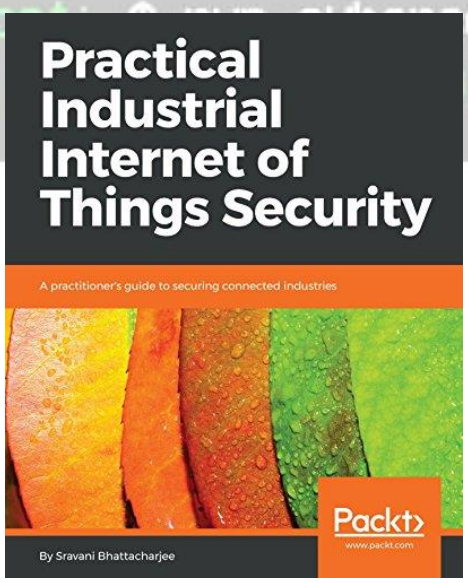
A könyv címe: **Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries**

Szerző: Sravani Bhattacharjee

Kiadás éve: 2018.

A kiadvány elérhető a következő linken:

https://www.amazon.com/Practical-Industrial-Internet-Things-Security-ebook/dp/B078MTMN77/ref=pd_sim_351_4/139-2402915-3452033?_encoding=UTF8&pd_rd_i=B078MTMN77&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

A Black Cell az ICS/OT kiberbiztonsági portfóliójában megjelentetett egy ICS/OT SNAPSHOT 2019 című tanulmányt, amely bemutatja a hazai interneten elérhető ipari vezérlőket, valamint az eredményeket elemzi.

Néhány idézet kedvcsináló gyanánt a riportból:

„A titkosítatlan protokollhasználat azzal a kockázattal jár, hogy hozzáférhetővé, lehallgathatóvá és módosíthatóvá válhat az adatforgalom. A titkosítatlan kommunikáció során a bizalmasság és a sértetlenség (integritás) nem biztosítható."

„Az Interneten elérhetővé tett ICS/OT eszközök magas fenyegetettség mellett üzemelnek. A specifikus, operációs rendszer és alkalmazás-sérülékenységek vagy a DoS/DDoS támadások miatt az elérhetővé tett eszközök nem csak az üzemi folyamatokra, de a mögöttes infrastruktúrára is kockázatot jelenthetnek. Egy kompromittált eszközről akár a mögöttes hálózat eszközei is hozzáférhetővé válhatnak."

„A lejárt és érvénytelen, emiatt pedig megbízhatatlan tanúsítvány kockázata, hogy a szolgáltatás nem veszi észre, ha valaki Man-in-The Middle módon belenyúl az adatforgalomba és lehallgatja a kommunikációt. A kommunikáció bizalmassága és sértetlensége (integritása) nem biztosítható."

„A Shodan eszközkereső jelenleg 127 ezer „ICS" címkével ellátott eszközt tart nyilván, de ha a szélesebb kritériumrendszert alkalmazzák, és a különféle komponenseket is beleszámolják a statisztikába, akkor 2019-ben körülbelül 250 ezer ICS/OT eszköz érhető el az Interneten. – 2019. december"

Minden ICS/SCADA üzemeltető szervezet részére javasoljuk a Riport letöltését és tanulmányozását annak érdekében, hogy a saját sérülékenységeikkel tisztában legyenek, és a szervezet képes legyen felkészülni az említett sérülékenységek befoltozására, kezelésére.

A riport a következő linken elérhető, és onnan letölthető:

https://blackcell.hu/ics-ot-kiberbiztonsagi-portfolio/

A tanulmány alapján íródott elemző Index cikk a következő linken érhető el:

https://index.hu/techtud/2020/02/06/magyar_ipari_vezerlorendszerek_az_interneten_kiberbiztonsag_serulekeny_hekkerek_black_cell/

ICS sérülékenységek

2020. februárban 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-20-056-01: **Moxa MB3xxx Series Protocol Gateways**

Kritikus szintű sérülékenységek: puffer túlcsordulás, CSRF, kockázatos kriptográfiai algoritmus használata, információ feltárás, érzékeny információk egyszerű szöveges formában történő továbbítása és tárolása, gyenge jelszó policy, nem megfelelően specifikált kommunikációs csatorna.
https://www.us-cert.gov/ics/advisories/icsa-20-056-01

ICSA-20-056-02: **Moxa ioLogik 2542-HSPA Series Controllers and IOs, and IOxpress Configuration Utility**

Magas szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő tárolása, nem megfelelően specifikált kommunikációs csatorna.
https://www.us-cert.gov/ics/advisories/icsa-20-056-02

ICSA-20-056-03: **Moxa PT-7528 and PT-7828 Series Ethernet Switches**

Kritikus szintű sérülékenységek: puffer túlcsordulás, kockázatos kriptográfiai algoritmus használata, beégetett kriptográfiai kulcs és hitelesítők használata, gyenge jelszó policy, információ feltárás.
https://www.us-cert.gov/ics/advisories/icsa-20-056-03

ICSA-20-056-04: **Moxa EDS-G516E and EDS-510E Series Ethernet Switches**

Kritikus szintű sérülékenységek: puffer túlcsordulás, kockázatos kriptográfiai algoritmus használata, beégetett kriptográfiai kulcs és hitelesítők használata, érzékeny információk egyszerű szöveges formában történő továbbítása, gyenge jelszó policy.
https://www.us-cert.gov/ics/advisories/icsa-20-056-04

ICSA-20-056-05: **Honeywell WIN-PAK**

Magas szintű sérülékenységek: CSRF, http fejléc hiba, elavult funkciók használata.
https://www.us-cert.gov/ics/advisories/icsa-20-056-05

ICSA-20-051-01: **B&R Industrial Automation Automation Studio and Automation Runtime**

Kritikus szintű sérülékenység: nem megfelelő hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-051-01

ICSA-20-051-02: **Rockwell Automation FactoryTalk Diagnostics**

Kritikus szintű sérülékenység: nem megbízható adatok érvényesítési hibája.
https://www.us-cert.gov/ics/advisories/icsa-20-051-02

ICSA-20-051-03: **Honeywell NOTI-FIRE-NET Web Server (NWS-3)**

Kritikus szintű sérülékenységek: útvonal bejárás, hitelesítés megkerülése.
https://www.us-cert.gov/ics/advisories/icsa-20-051-03

ICSA-20-051-04: **Auto-Maskin RP210E, DCU210E, and Marine Observer Pro (Android App)**

Kritikus szintű sérülékenységek: érzékeny információk egyszerű szöveges formában történő továbbítása, hitelesítési hiba, beégetett hitelesítés használata, elrontott jelszó esetén gyenge helyreállítási mechanizmus, gyenge jelszó elvárások.
https://www.us-cert.gov/ics/advisories/icsa-20-051-04

ICSMA-20-049-01: **Spacelabs Xhibit Telemetry Receiver (XTR)**
Kritikus szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsma-20-049-01

ICSMA-20-049-02: **GE Ultrasound products**
Közepes szintű sérülékenység: védelmi mechanizmus hiba.
https://www.us-cert.gov/ics/advisories/icsma-20-049-02

ICSA-20-049-01: **Honeywell INNCOM INNControl 3**
Közepes szintű sérülékenység: nem megfelelő privilégium menedzsment.
https://www.us-cert.gov/ics/advisories/icsa-20-049-01

ICSA-20-049-02: **Emerson OpenEnterprise**
Magas szintű sérülékenység: puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-20-049-02

ICSA-19-274-01: **Interpeak IPnet TCP/IP Stack (Update C)**
Kritikus szintű sérülékenységek: puffer túlcsordulás, memória pufferen belüli műveletek nem megfelelő korlátozása, értékkezelési hiba, null pointer dereferencia, nem megfelelő szinkronizáció, argumentum befecskendezés.
https://www.us-cert.gov/ics/advisories/icsa-19-274-01

ICSA-20-044-01: **Schneider Electric Modicon Ethernet Serial RTU**
Magas szintű sérülékenységek: a szokásostól eltérő és kivételes állapotok nem megfelelő ellenőrzése, nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsa-20-044-01

ICSA-20-044-02: **Schneider Electric Magelis HMI Panels**
Magas szintű sérülékenység: a szokásostól eltérő és kivételes állapotok nem megfelelő ellenőrzése.
https://www.us-cert.gov/ics/advisories/icsa-20-044-02

ICSA-20-042-01: **Synergy Systems & Solutions HUSKY RTU**
Kritikus szintű sérülékenységek: nem megfelelő hitelesítés, nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-042-01

ICSA-20-042-02: **Siemens Industrial Products SNMP Vulnerabilities**
Magas szintű sérülékenységek: adatfeldolgozási hibák, nulla pointer dereferencia.
https://www.us-cert.gov/ics/advisories/icsa-20-042-02

ICSA-20-042-03: **Siemens SIMATIC CP 1543-1**

Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, iterációs problémák.
https://www.us-cert.gov/ics/advisories/icsa-20-042-03

ICSA-20-042-04: Siemens PROFINET-IO Stack
Magas szintű sérülékenység: erőforrás felhasználás kontrolljának hiánya.
https://www.us-cert.gov/ics/advisories/icsa-20-042-04

ICSA-20-042-05: Siemens SIMATIC S7
Közepes szintű sérülékenység: erőforrás felhasználás kontrolljának hiánya.
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
Magas szintű sérülékenység: pufferméret nem megfelelő kalkulációja.
https://www.us-cert.gov/ics/advisories/icsa-20-042-06

ICSA-20-042-07: Siemens SCALANCE X Switches
Alacsony szintű sérülékenység: védelmi mechanizmus hiba.
https://www.us-cert.gov/ics/advisories/icsa-20-042-07

ICSA-20-042-08: Siemens SIPORT MP
Közepes szintű sérülékenység: elégtelen naplózás.
https://www.us-cert.gov/ics/advisories/icsa-20-042-08

ICSA-20-042-09: Siemens OZW Web Server
Közepes szintű sérülékenység: információ felfedés.
https://www.us-cert.gov/ics/advisories/icsa-20-042-09

ICSA-20-042-10: Siemens SCALANCE S-600
Magas szintű sérülékenységek: erőforrás felhasználás kontrolljának hiánya, XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-042-10

ICSA-20-042-11: Siemens SIMATIC S7-1500
Magas szintű sérülékenység: erőforrás felhasználás kontrolljának hiánya.
https://www.us-cert.gov/ics/advisories/icsa-20-042-11

ICSA-20-042-12: Siemens SIPROTEC 4 and SIPROTEC Compact
Magas szintű sérülékenység: nem megfelelő bemeneti hitelesítés.
https://www.us-cert.gov/ics/advisories/icsa-20-042-12

ICSA-20-042-13: Digi ConnectPort LTS 32 MEI
Alacsony szintű sérülékenységek: veszélyes fájlfeltöltés korlátozás hiánya, XSS.
https://www.us-cert.gov/ics/advisories/icsa-20-042-13

ICSA-19-344-04: Siemens SIMATIC Products (Update A)
Alacsony szintű sérülékenység: kockázatos kriptográfiai algoritmus használata.
https://www.us-cert.gov/ics/advisories/icsa-19-344-04

ICSA-19-283-01: Siemens Industrial Real-Time (IRT) Devices (Update B)
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 C)
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://www.us-cert.gov/ics/advisories/icsa-19-283-02

ICSA-19-099-03: Siemens Industrial Products with OPC UA (Update E)
Magas szintű sérülékenység: funkcióbeli kivételek figyelmen kívül hagyása.
https://www.us-cert.gov/ics/advisories/ICSA-19-099-03

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

ICSA-20-035-01: AutomationDirect C-More Touch Panels
Kritikus szintű sérülékenység: a hitelesítő adatok nem megfelelő védelme.
https://www.us-cert.gov/ics/advisories/icsa-20-035-01

ICSMA-19-080-01: Medtronic Conexus Radio Frequency Telemetry Protocol (Update A)
Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, szenzitív információk szabad szöveges formában történő továbbítása.
https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

ICSMA-18-058-01: Medtronic 2090 Carelink Programmer Vulnerabilities (Update C)
Magas szintű sérülékenységek: jelszavak visszafejthető formában történő tárolása, útvonal bejárás, kommunikációs csatornák nem megfelelő korlátozása.
https://www.us-cert.gov/ics/advisories/ICSMA-18-058-01

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. február hónapban az ICS-CERT nem adott ki riasztást.

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

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

Riasztás zsarolóvírus támadásról gázüzemek ellen

Jelen riasztás szerepelhetne az ICS incidensek részben is.

Az Egyesült Államok beli Kiber- és Infrastruktúra biztonsági Ügynökség (Cybersecurity and Infrastructure Security Agency (CISA)) riasztást adott ki a kritikus infrastruktúra üzemeltetők részére, a közelmúltban történt gázüzemet ért zsarolóvírus támadás miatt, amely a gázcsövek üzemeltetését akadályozta.

A meg nem nevezett szervezet IT rendszerébe e-mailen keresztül bejuttatott Spearphishing linkre kattintva jutott be a rendszerbe a zsarolóvírus, amely IT rendszer nem volt elszigetelve az OT rendszertől, emiatt érintette a gázszállító rendszer működéséért felelős rendszer fájljait is a titkostás.

A PLC-k nem voltak a támadásban érintettek, és a szervezet nem veszítette el a kontrollt a rendszer üzemeltetése feleltt. Sajnálatos módon a szervezet vészhelyzet kezelési terve nem kezelte a kibertámadás okozta helyzeteket, ezért a vezetőség a rendszer biztonságos leállítása mellett döntött. Két napra elvesztette a termelőképességét és ezáltal a bevételeket a cég, aztán sikerült helyreállítani a normál üzletmenetet.

A CISA azért adta ki a riasztását, hogy a hasonló energia ágazati szereplők kerüljék el azokat a hibákat, amelyeket az áldozat szervezet elkövetett.

Javaslatok a CISA által az incidens elkerülésére:

- Gondoskodjon róla, hogy a szervezet vészhelyzeti-, vagy katasztrófa elhárítási terve rendelkezzen a kibertámadások okozta helyzetek kezeléséről. Tartalmazzanak a tervek szándékos leállítás esetére is megoldásokat.
- Az üzletmenet-folytonosság biztosítása érdekében az alternatív vezérlőrendszerekre történő átállás lehetőségét biztosítsa, például kézi működtetés.
- Biztosítsa a lehetőségét az üzletmenet-folytonossági tervek gyakorlaton történő megismertetésének, az üzemeltetésben résztvevő személyek számára.
- Azonosítsa a szervezeténél az egyedüli hibapontokat (Single Point of Failure - SPF) annak érdekében, hogy a redundanciát biztosíthassa, és ne lehessen egy eszköz vagy folyamat megállításával a teljes termelést leállítani.
- Alakítson redundáns kommunikációs képességeket a terepen lévő létesítmények (Field devices) és a koordináló létesítmény között.

- Ismerje fel a kibertámadások által az emberi életeket fenyegető fizikai kockázatokat, és integrálja a kiberbiztonsági eljárásokat a szervezet biztonsági képzési programjába, mely képzések az OT üzemeltetésben részt vevő személyekre (pl.: mérnökökre) és a szállítóikra is kiterjedjen.

A technikai és architektúrális fenygetések megelőzésére:

- Valósítsa meg a hálózati szegmentációt az IT és az OT rendszerek között. DMZ megoldás használata javasolt.
- Szervezze az OT eszközöket logikai zónákba, a kritikusság követelményeit figyelembe véve. Alkalmazzon hálózati forgalom monitorozást a zónák közötti adatforgalomban. Tiltsa az ICS protokollokon az IT hálózatból történő adatátvitelt.
- Az IT és OT eszközök távoli eléréséhez használjon többfaktoros hitelesítést.
- Az IT és az OT rendszerek vonatkozásában is legyen rendszeres adatmentés, és győződjön meg róla, hogy a zsarolóvírus rendszerbe történő kerülése esetén az incidensben a biztonsági mentések nem érintettek. A visszaállítási mechanizmus legyen rendszeresen tesztelve.

Egyéb javaslat, és a riasztással kapcsolatos további információ a következő linken érhető el:

https://www.us-cert.gov/ncas/alerts/aa20-049a

További cikkek az incidenssel kapcsolatban:

https://hvg.hu/tudomany/20200220_zsarolovirus_hackertamadas_kiberbiztonsag
https://www.bbc.com/news/technology-51564905
https://www.nextgov.com/cybersecurity/2020/02/cisa-shares-details-about-ransomware-shut-down-pipeline-operator/163209/

A riasztás során a MITRE ATT&CK keretrendszerben megfogalmazott technikák és ismeretanyag került felhasználásra.