17. 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:

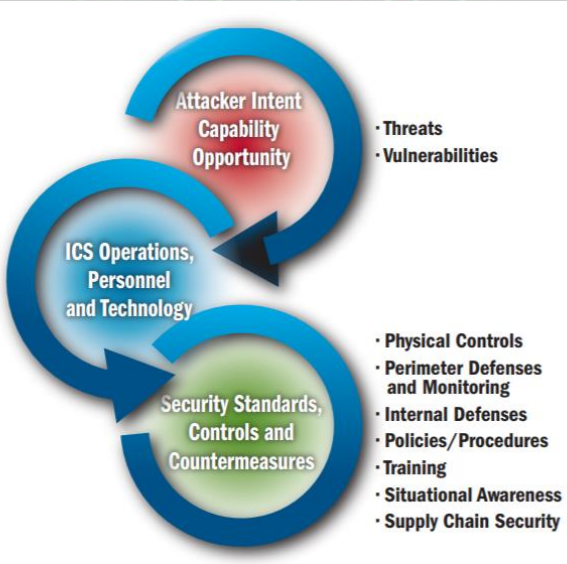
ICS jó gyakorlatok, javaslatok

Napjainkban, az egyre növekvő kiberfenyegetések világában elengedhetetlen, hogy egy ipari irányító rendszert üzemeltető szervezet mélységi védelmet alakítson ki. A belső fenyegetésekkel, továbbá az egykori munkavállalók esetleges rosszindulatú cselekedeteivel egyaránt hatványozottabban kell számolni (2017-2019 összevetésben), erre világít rá a „SANS 2019 State of OT/ICS Cybersecurity Survey" felmérése is:

Table 2. Actors Involved in Incidents

	2017	2019
Intentional Malicious		
Hackers	56.3%	44.8%
Foreign nation-states or state-sponsored parties	0.0%	27.6%
Organized crime	0.0%	24.1%
Activists, activist organizations, hacktivists	12.5%	17.2%
Competitors	12.5%	10.3%
Former employees	0.0%	10.3%
Former equipment providers	0.0%	6.9%
Both/Unknown		
Current employees	31.3%	34.5%
Unknown (sources were unidentified)	31.3%	17.2%
Unintentional		
Current service providers, consultants, contractors	12.5%	31.0%
Nonmalicious actors (internal)		20.7%
Current equipment providers	18.8%	13.8%
Domestic intelligence services	0.0%	6.9%
Suppliers or partners	12.5%	6.9%

A mélységi védelem (Defense-In-Depth) kialakítására számos jó gyakorlat hozzáférhető az interneten keresztül is. Az ICS-CERT is kiadta még 2016-ban ajánlását, hogy miként alakítson ki egy ICS rendszert üzemeltető szervezet mélységi védelmet az IT infrastruktúrával összhangban. Az ajánlásban szereplő következő ábra tökéletesen szemlélteti a mélységi védelem alapvető tervezési lépéseit:



Az ábrán jól látható, hogy a külső interneten keresztül történő hozzáféréseket azonosítani kell, és ezt követően értékelni kell a kockázatokat (azonosítani a fenyegetéseket és a kihasználható sérülékenységeket). Ezek egyaránt hatással vannak a humán és a technológiai tényezőkre, ezt is szükséges figyelembe venni a tervezés során. Előzőek alapján kell kialakítani a fizikai védelmet, a határvédelmet és annak ellenőrzési mechanizmusait, a belső védelmi intézkedéseket, szabályzatokat és eljárásokat. Rendkívül fontos az információbiztonság tudatosság oktatása, továbbá az ellátási láncokkal kapcsolatos biztonság kialakítása.

Az üzleti igények is értékelésével például azt is értékelni kell, ha egy adott örökölt (legacy) rendszer nem képes bizonyos mélységi védelmi intézkedés megvalósítására, és költséghatékony lehet-e, valamint az üzletet jobban támogató egy olyan új rendszer bevezetése, amely képes a mélységi védelmi intézkedések implementálására.

Javasolt olyan rendszerek üzemeltetése, amelyek képesek az ICS specifikus protokollok monitorozására, és az ezzel kapcsolatos nem-megfelelőségek kezelésére, ezek segíthetik a logikai mélységi védelem kialakítását.

A tudásmenedzsment és a változásmenedzsment felelőssége, hogy az egykori, vagy jogviszonyban álló munkavállalók ne tudjanak káros cselekményeket eredményesen végrehajtani az ICS rendszerekben, akár fizikai, akár logikai értelemben. Teljesen nem lehet a humán kockázatokat redukálni, de szükséges ezen kockázatok kezelése a mélységi védelemmenedzsment során.

Az ICS-CERT ajánlása, mely további nagyon hasznos tanácsokkal szolgál, a következő linken érhető el:

https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

A SANS felmérését a következő weboldalról lehet letölteni:

https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf

ICS képzések, oktatások

A COVID-19 világjárványra tekintettel 2020. októberben ICS biztonság tárgyában a SANS kizárólag online formában tart ICS képzéseket, oktatásokat.

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/ weboldalon lehetőség van online elvégezni bizonyos ipari irányító rendszerek biztonságával kapcsolatos tanfolyamokat, melyek során videóalapú 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 tanfolyamot elvégző személyek részére. A következő kurzusok végezhetők el:

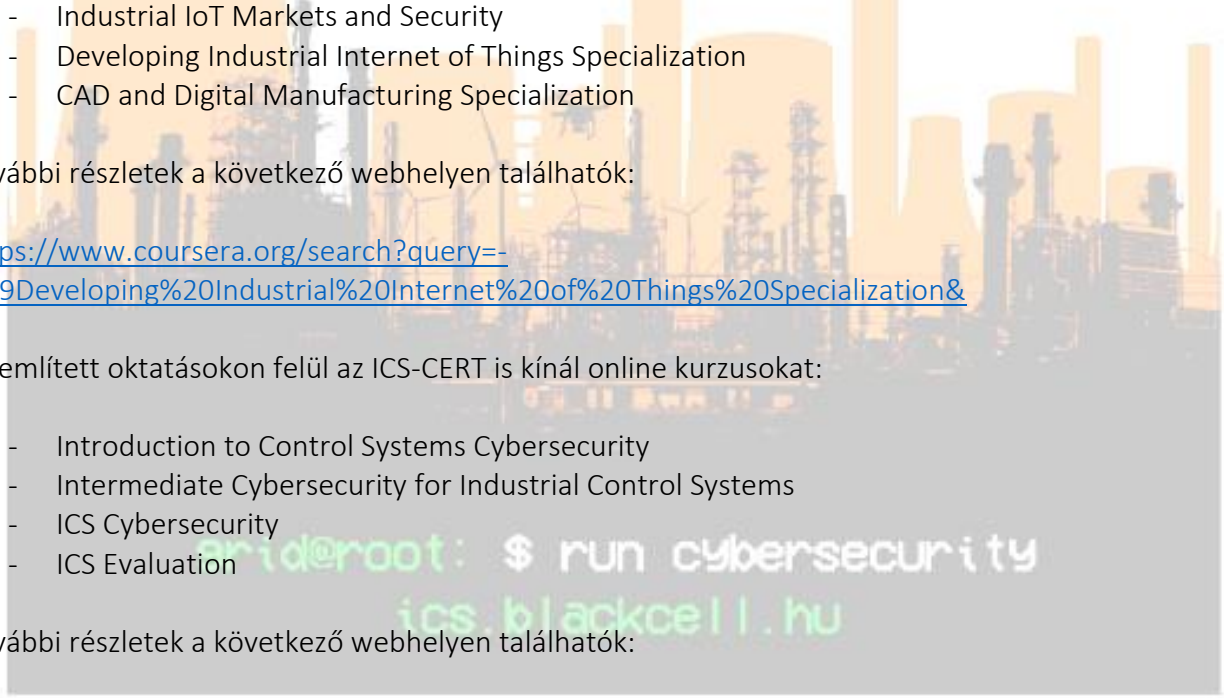
- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- CAD and Digital Manufacturing Specialization

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 online képzései az ipari irányító rendszerek biztonságával kapcsolatban:

- ICS410: ICS/SCADA Security Essentials
  - 2020.10.5-9.
  - 2020.10.26-31.

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, szoftverkezelést, 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 kétnapos képzése során a résztvevők megismerhetik a különböző vezérlőrendszerek 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

A School of security ICS és SCADA Rendszerek biztonsági oktatást tart online, mely oktatás felkészíti a résztvevőket, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

Az oktatás az ICS és SCADA rendszerek alapjait, sérülékenységeit, kockázatmenedzsment alapjait, biztonsági kontrollok implementációit, szerver biztonságát, hálózat- és eszköz biztonságát, biztonsági programjainak fejlesztését, és a hálózat nélküli SCADA biztonságot mutatja be részletesen.

A tanfolyamok 0-3 vagy 4-12 hónap időtávban van lehetőség elvégezni, igény szerint. A részletekkel kapcsolatos további információ a következő honlapon található:

https://www.enosecurity.com/training-tutorials-courses/ics-scada-security-essentials-training/

Az INFOSEC-Flex SCADA/ICS Security Training Boot Camp elnevezésű online oktatása lehetőséget biztosít a SCADA és ICS rendszerek elleni külső és belső támadások elleni felkészülésre.

A kurzus elvégzése garanciát ad a résztvevőknek arra, hogy tanúsított SCADA biztonsági szakemberek legyenek (Certified SCADA Security Architect).

A 4 napos online kurzus a SCADA és ICS biztonsági alapjain kívül a szabályozási környezet is részleteiben bemutatja, ahogy a SCADA biztonsági kontrollokat és a SCADA penetrációs teszt is.

A képzéssel kapcsolatos további információk a következő linken érhetők el:

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

ICS konferenciák

Az októberi hónap az egész világban a kibervédelemről szól, az európai kiberbiztonsági hónapról szóló weboldalon további információkhoz lehet jutni az európai rendezvényekről:

https://cybersecuritymonth.eu/

2020. októberében a koronavírus világjárványra tekintettel számos ICS és SCADA biztonság tárgyában tervezett konferencia és workshop virtuálisan vagy a helyszínen biztonsági intézkedések betartása mellett kerül megtartásra.

Industrial Control Systems (ICS) Cyber Security Conference 2020

A Securityweek 2020. októberi ICS kiberbiztonsági konferenciája eredetileg Atlantában került volna megrendezésre, de a koronavírus járványra tekintettel virtuálisan kerül megtartásra.

A konferencián az ipari irányító rendszerek gyártói, felhasználói, üzemeltetői, szolgáltatói, valamint kormányzati szereplők is részt vesznek a konferencián. Megvitathatják a résztvevők a legújabb ICS rendszereket érintő kiberbiztonsági trendeket, eseményeket és azok kezelését, komplex kritikus infrastruktúra védelmi megközelítésben.

Industrial Control Systems (ICS) Cyber Security Conference; (Virtuális konferencia, Egyesült Államok); 2020.10.19-22.

További információk a következő linken találhatók:

https://www.icscybersecurityconference.com/

CS3STHLM 2020

A 2014 óta megrendezésre kerülő ICS/SCADA, valamint kritikus infrastruktúra védelmi kiberbiztonsági konferencia is a COVID-19 miatt a virtuális térben kerül megtartásra. A 3 napos konferencián gyakorlati útmutatókkal ismerkedhetnek meg a résztvevők, valamint az ICS kiberbiztonsági terület szakmai kiválóságainak előadásaival.

A konferencia két részből tevődik össze, egy gyakorlati részből, ahol bemutatják a szakemberek laboratórium körülmények között az ICS/SCADA rendszerek biztonsági aspektusait, valamint egy előadásokból és beszélgetésekből álló részből, ahol tapasztalatcserére is lehetősége nyílik a résztvevőknek.

CS3STHLM 2020; (Stockholm, Svédország, virtuális konferencia); 2020.10.19-22.

További információk a következő linken találhatók:

https://cs3sthlm.se/

SCADA SECURITY CEE Conference

Az első CEE SCADA biztonsági konferencia a következő témákra fókuszál: a legújabb és a jövőbeni kiberfenyegetések és azok megoldásai, technológiai trendek az ICS biztonságában. A konferencián megvitatásra kerülnek az Ipar 4.0 és az ICS biztonság ellentmondásai.

Az említett témákon túl szó lesz a humán tényező jelentőségéről, továbbá a kiberbiztonsági területen kiaknázható üzleti lehetőségekről is.

SCADA SECURITY CEE Conference; (Prága Csehország, Hotel DAP); 2020.10.12-13.

További információk a következő linken találhatók:

https://cybersecuritymonth.eu/ecsm-countries/czech-republic/scada-security-cee-conference

CS4CA Cyber Security for Critical Assets Summit

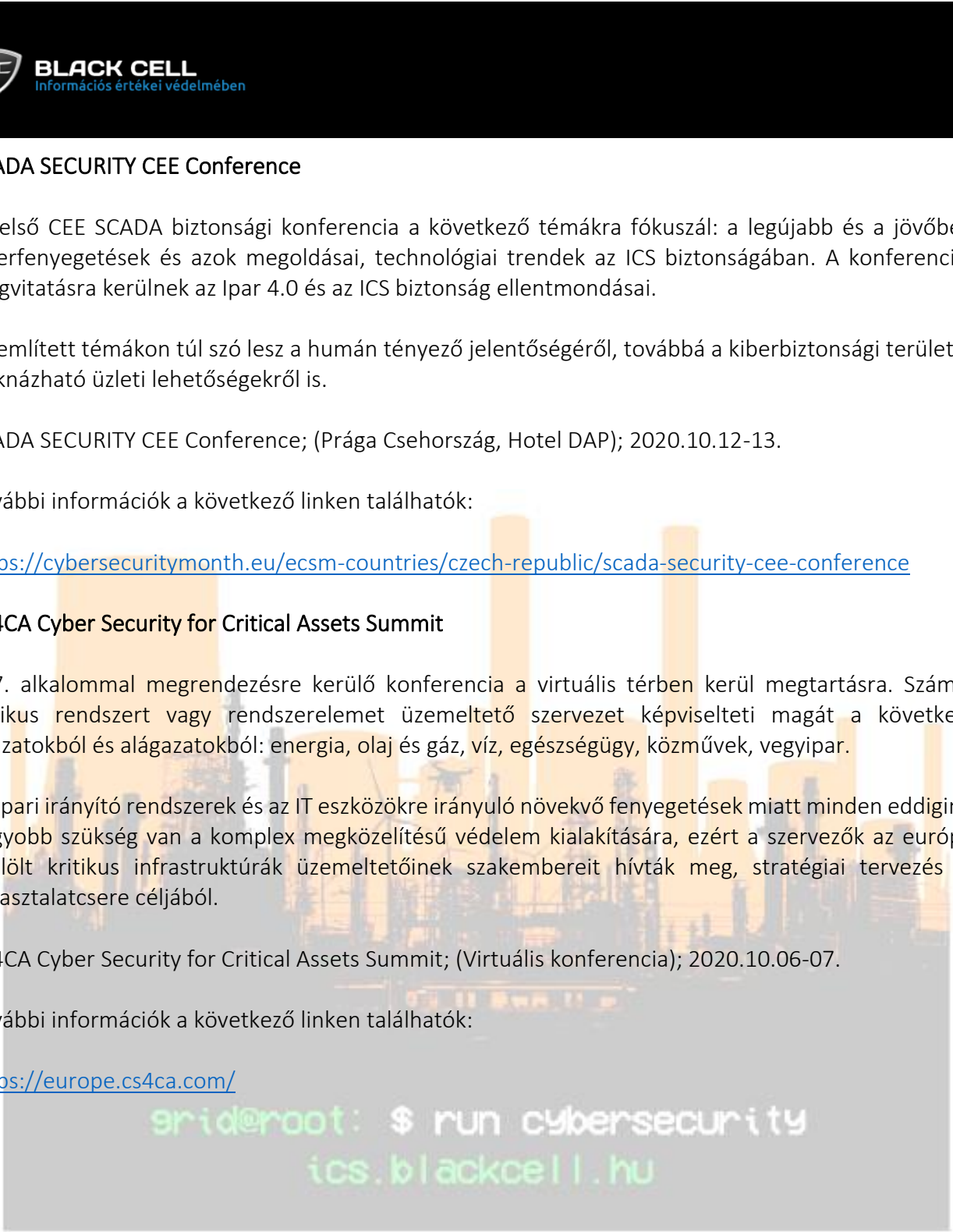
A 7. alkalommal megrendezésre kerülő konferencia a virtuális térben kerül megtartásra. Számos kritikus rendszert vagy rendszerelemet üzemeltető szervezet képviselteti magát a következő ágazatokból és alágazatokból: energia, olaj és gáz, víz, egészségügy, közművek, vegyipar.

Az ipari irányító rendszerek és az IT eszközökre irányuló növekvő fenyegetések miatt minden eddiginél nagyobb szükség van a komplex megközelítésű védelem kialakítására, ezért a szervezők az európai kijelölt kritikus infrastruktúrák üzemeltetőinek szakembereit hívták meg, stratégiai tervezés és tapasztalatcsere céljából.

CS4CA Cyber Security for Critical Assets Summit; (Virtuális konferencia); 2020.10.06-07.

További információk a következő linken találhatók:

https://europe.cs4ca.com/



ICS üzemeltetői incidensek

Pakisztáni áramszolgáltató elleni zsarolóvírus támadás

A pakisztáni Karacsi városának áramszolgáltatóját (K-Electric) zsarolóvírus-támadás érte, melyet a Netwalker nevű zsarolóvírussal követtek el a támadók. A K-Electric termelési, továbbítási (TSO), elosztási (DSO) feladatokat is ellát, és közel 2,5 millió ügyfelet szolgál ki.

Az incidens 2020. szeptember 7-én azzal indult, hogy az ügyfelek nem tudták elérni a szolgáltatást a felhasználói adataikkal, azonban ez az áramellátást nem befolyásolta. A K-Electric megpróbálta az ügyfeleket átirányítani a szolgáltatáshoz egy másik állomáson keresztül.

A támadók 3,85 millió dollárt követeltek Bitcoinban a szervezettől, a 7 napos határidő elteltével a támadók 7,7 millió dollárra növelték a váltságdíjat. A támadók azt is állították, hogy titkosítatlan fájlokat loptak el a K-Electrictől, mielőtt letitkosították a rendszereit.

A Netwalker zsarolóvírussal támadó rosszindulatú aktorok elkezdték kihasználni a sérülékeny virtuális magánhálózatokat (VPN), a webalkalmazások felhasználói felületének elemeit és a távoli asztali kapcsolatok gyenge jelszavait, hogy hozzáférjenek az áldozatok hálózataihoz.

A rendelkezésre álló információk alapján a termelési rendszert nem érintette a ransomware támadás.

A hasonló támadások elkerülésére a következő tanácsokat adta az FBI:

- Kritikus adatok offline mentése,
- Legyen biztonsági másolat a felhőben, vagy biztonságos külső hardveren,
- Biztosítsa az adatok sértetlenségét, ne lehessen módosítani azokat,
- Minden hoszton legyen telepítve naprakész antivírus megoldás,
- Csak biztonságos hálózatokon végezzen tevékenységet, kerülje a nyilvános Wifi hálózatokat,
- Használjon biztonságos VPN megoldást,
- Használjon kétfaktoros autentikációt, és alkalmazzon erős jelszó szabályokat,
- Az eszközökön telepítse a frissítéseket, azok legyenek mindig naprakészek.

Az incidensről további információk a következő linkeken érhetők el:

https://www.dawn.com/news/1578882

https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/

https://securityaffairs.co/wordpress/108075/malware/k-electric-netwalker-ransomware-attack.html

Könyvajánló

A SCADA Systems and Cyber Security for Critical Infrastructures című könyv bepillantást ad a SCADA biztonságba és annak javítási-, fejlesztési lehetőségeibe. A szerző megvizsgálja azokat a tényezőket, melyek a rendszerek sérülékenységeit okozhatják, valamint olyan új kritériumokat mutat be, mint például a titkosítás, és új hitelesítési módok, amelyek segítenek az ellenálló rendszer kialakítása érdekében. Az össz-veszély megközelítést segíti, hogy kritikus infrastruktúra szinten kerül a vizsgálat lefolytatásra, ezzel is érzékeltetve a SCADA rendszerek védelmének komplexitását.

A könyvben bemutatásra kerül egy olyan átfogó kiberbiztonsági modell és megközelítés, amely a SCADA rendszerek biztonsági elemzését és tervezését hivatott elősegíteni.

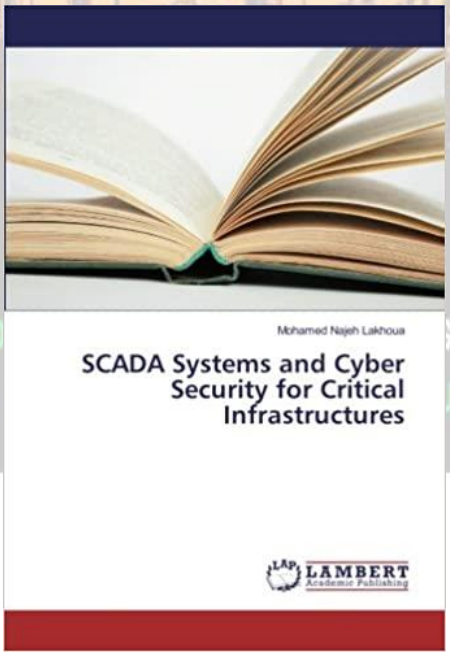
A könyv címe: **SCADA Systems and Cyber Security for Critical Infrastructures**

Szerzők/szerkesztők: Mohamed Najeh Lakhoua

Kiadás éve: 2018.

A kiadvány elérhető a következő linken:

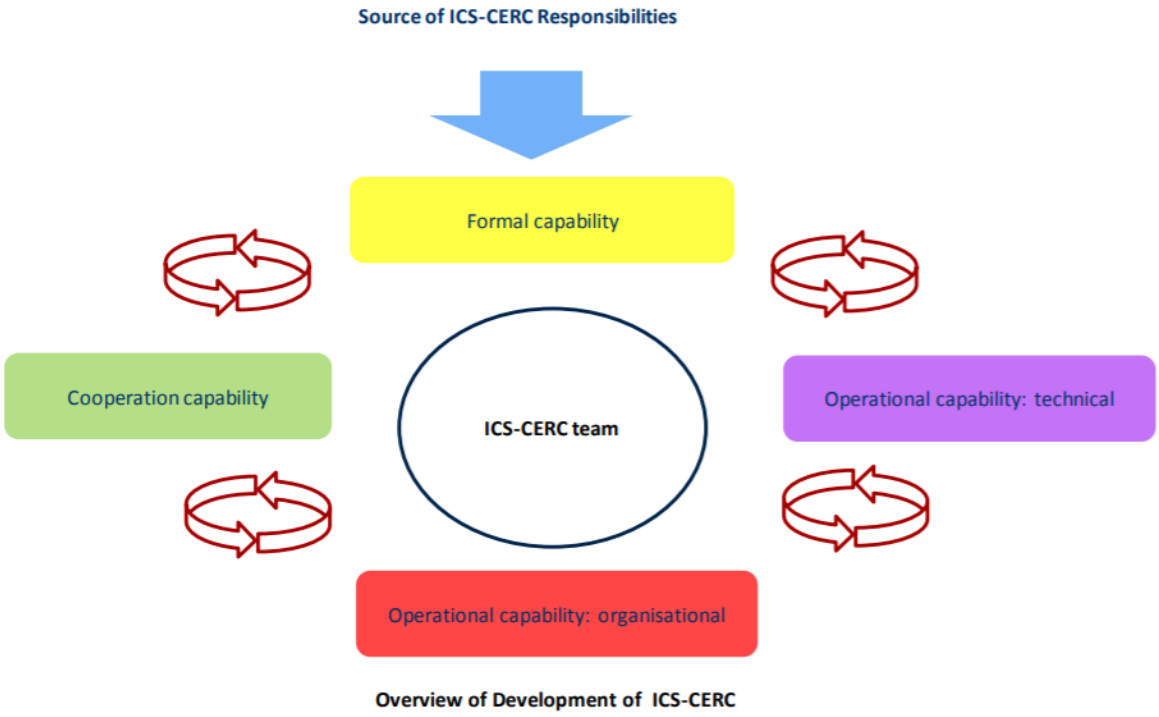
https://www.amazon.co.uk/dp/6135856553?linkCode=gs2&tag=uuid07-21



Black Cell javaslatok

Az ipari irányító rendszereket üzemeltető szervezeteknek mindenképpen rendelkezésre kell álljon a képessége az ICS rendszerek biztonságának szavatolására. Ezt kizárólag megfelelő menedzsmenttel lehet megoldani. Az ICS rendszerek incidensekkel szembeni ellenálló- és válaszképessége a szervezet felkészültségén múlik.

Négy tényező létfontosságú az említett képességek megfelelő alkalmazásához, melyet a következő ábra szemléltet:



Forrás: ENISA 2013. Good practice guide for CERTs in the area of Industrial Control Systems

1. Formális képességek (szerepek és felelősségek). Minden egyes szereplőnek - legyen az belső vagy külső fél, munkaszerződéssel vagy megbízási szerződéssel feladatot ellátó személy vagy szervezet – tisztában kell lennie a feladatával és felelősségével. Ezt megfelelő dokumentáltsággal és ellenőrzéssel el lehet érni.

2. Működtetési (technikai) képességek. A megfelelő technikai erőforrások megléte mellett szükséges a kompetencia rendelkezésre állása is.

3. Működtetési (szervezeti) képességek. A 2. pontban megfogalmazott képességek biztosítása csak akkor lehetséges, ha a szervezettség és menedzsment megfelelő. Ez beszerzési, költségvetési, humán erőforrás-, illetve tudásmenedzsment függvénye.

4. Együttműködési képességek. A szervezeten belüli és kívüli kooperáció nagyon fontos az incidensek kezelése során. Enélkül nem lesz hatékony a biztonsági események kezelése, amely

egy ICS/SCADA rendszert ér. Időveszteség, költségnövekedés és még számos más negatív hatás következhet be az együttműködés nem megfelelősége, vagy hiánya miatt.

Az említett képességek fontosságáról, továbbá azok alkalmazásának lehetőségeiről és kockázatairól további információkhoz lehet jutni az ENISA ajánlásának elolvasásával. Az ajánlás a következő linken érhető el:

https://www.enisa.europa.eu/publications/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems

A Black Cell Magyarország Kft. szolgáltatási portfóliójában számos ponton segítséget tud nyújtani szervezetek számára a megfelelő képességek kialakításában. A szervezettség, működtetési és együttműködési képességek biztosítása érdekében a Kockázatmenedzsment és megfelelés üzletág szakértői, a technikai és technológiai képesség kialakításában a SOC és VAR/MSS üzletágak szakértői állnak rendelkezésre. Az ipari irányító rendszerek biztonságával kapcsolatos Black Cell portfólió a következő linken található:

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

ICS sérülékenységek

2020. szeptemberében 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-13-011-01: **3S CoDeSys** (Update A)
Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, útvonal bejárás.
https://us-cert.cisa.gov/ics/advisories/ICSA-13-011-01

ICSA-20-266-01: **GE Digital APM Classic**
Magas szintű sérülékenységek: felhasználói kulccsal történő engedélyezés megkerülés, egyirányú „sózatlan" hash használat.
https://us-cert.cisa.gov/ics/advisories/icsa-20-266-01

ICSA-20-266-02: **GE Reason S20 Ethernet Switch**
Közepes szintű sérülékenység: XSS.
https://us-cert.cisa.gov/ics/advisories/icsa-20-266-02

ICSMA-20-261-01: **Philips Clinical Collaboration Platform**
Közepes szintű sérülékenységek: CSRF, védelmi mechanizmus hiba, algoritmikus és konfigurációs hiba, weboldal attribútum helytelen script semlegesítése.
https://us-cert.cisa.gov/ics/advisories/icsma-20-261-01

ICSA-20-261-01: **Advantech WebAccess Node**
Magas szintű sérülékenység: kritikus erőforrás nem megfelelő engedély kiosztása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-261-01

ICSA-20-203-01: **Wibu-Systems CodeMeter** (Update A)
Kritikus szintű sérülékenységek: helytelen értékkel történő puffer hozzáférés, nem megfelelő erősségű titkosítás, eredetellenőrzési hiba, nem megfelelő bemeneti érvényesítés, kriptográfiai aláírás helytelen ellenőrzése, nem megfelelő erőforrás leállítás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-20-177-01: **ENTTEC Lighting Controllers** (Update A)
Magas szintű sérülékenységek: beégetett kriptográfiai kulcs használata, XSS, nem megfelelő hozzáférés ellenőrzés, kritikus erőforrás nem megfelelő engedély kiosztása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-177-01

ICSMA-20-254-01: **Philips Patient Monitoring Devices**
Közepes szintű sérülékenységek: CSV fájl semlegesítési probléma, XSS, nem megfelelő hitelesítés, tanúsítvány visszavonás nem megfelelő ellenőrzése, bemeneti szintaktikai hiba nem megfelelő validálása, erőforrás feltárás.
https://us-cert.cisa.gov/ics/advisories/icsma-20-254-01

ICSA-20-254-01: **AVEVA Enterprise Data Management Web**
Kritikus szintű sérülékenység: SQL befecskendezés.

https://us-cert.cisa.gov/ics/advisories/icsa-20-254-01

ICSA-20-254-02: **FATEK Automation PLC WinProladder**
Magas szintű sérülékenység: puffer túlcsordulás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-254-02

ICSA-20-254-03: **HMS Networks Ewon Flexy and Cosy**
Alacsony szintű sérülékenység: nem megbízható domain policy.
https://us-cert.cisa.gov/ics/advisories/icsa-20-254-03

ICSA-20-252-01: **Siemens SIMATIC RTLS Locating Manager**
Magas szintű sérülékenységek: nem megfelelő alapértelmezett engedélyek, nem jegyzett keresési útvonal vagy elem.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-01

ICSA-20-252-02: **Siemens SIMATIC S7-300 and S7-400 CPUs**
Közepes szintű sérülékenység: nem megfelelően védett hitelesítő adatok.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02

ICSA-20-252-03: **Siemens License Management Utility**
Magas szintű sérülékenység: szükségtelen privilégium használat.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-03

ICSA-20-252-04: **Siemens Spectrum Power**
Alacsony szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő tárolása, címjegyzéken keresztül történő információ feltárás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-04

ICSA-20-252-05: **Siemens Siveillance Video Client**
Közepes szintű sérülékenység: érzékeny információk egyszerű szöveges formában történő továbbítása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-05

ICSA-20-252-06: **Siemens SIMATIC HMI Products**
Közepes szintű sérülékenységek: túlzott számú hitelesítési kísérletek korlátozásának hiánya, hitelesítés megkerülése.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-06

ICSA-20-252-07: **Siemens Industrial Products**
Közepes szintű sérülékenység: érzékeny információk jogosulatlanok számára történő feltárása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

ICSA-20-252-08: **Siemens Polarion Subversion Webclient**
Magas szintű sérülékenységek: speciális karakterek nem megfelelő semlegesítése, CSRF.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-08

ICSA-20-203-01: **Wibu-Systems CodeMeter**

Kritikus szintű sérülékenységek: Puffer hozzáférés helytelen hosszúsági értékkel, nem megfelelő erősségű titkosítás, eredet ellenőrzési hiba, nem megfelelő bemeneti érvényesítés, kriptográfiai ellenőrzés nem megfelelő ellenőrzése, az erőforrások nem megfelelő leállítása.
https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-20-196-05: Siemens UMC Stack (Update B)
Közepes szintű sérülékenységek: nem jegyzett keresési út vagy elem, nem megfelelő erőforrás felhasználás, nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update C)
Közepes szintű sérülékenység: nem jegyzett keresési út vagy elem.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSA-20-105-05: Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update B)
Magas szintű sérülékenységek: nem megfelelő erőforrás felhasználás, nem megfelelő bemeneti érvényesítés.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-05

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update B)
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update E)
Magas szintű sérülékenység: nem megfelelő puffer méret számítás.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-06

ICSA-19-283-02: Siemens PROFINET Devices (Update H)
Magas szintű sérülékenység: nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02

ICSA-19-253-03: Siemens Industrial Products (Update I)
Magas szintű sérülékenységek: túlzott adat-lekérdezési műveletek, egész szám túlcsordulás, nem megfelelő erőforrás felhasználás.
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03

ICSA-20-245-01: Mitsubishi Electric Multiple Products
Magas szintű sérülékenység: értékszámítás kiszámíthatósága.
https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01

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