# 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. júniusban 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-19-178-01: **Medtronic MiniMed 508 and Paradigm Series Insulin Pumps**
Magas szintű sérülékenység: Nem megfelelő hozzáférés ellenőrzés.
https://www.us-cert.gov/ics/advisories/icsma-19-178-01

ICSA-19-178-01: **ABB PB610 Panel Builder 600**
Magas szintű sérülékenységek: beégetett hitelesítő használat, nem megfelelő hitelesítés, útvonal bejárás, nem megfelelő input validáció, puffer túlcsordulás.
https://www.us-cert.gov/ics/advisories/icsa-19-178-01

ICSA-19-178-02: **ABB CP651 HMI**
Magas szintű sérülékenység: beégetett hitelesítő használat.
https://www.us-cert.gov/ics/advisories/icsa-19-178-02

ICSA-19-178-03: **ABB CP635 HMI**
Magas szintű sérülékenység: beégetett hitelesítő használat.
https://www.us-cert.gov/ics/advisories/icsa-19-178-03

ICSA-19-178-04: **SICK MSC800**
Kritikus szintű sérülékenység: beégetett hitelesítő használat.
https://www.us-cert.gov/ics/advisories/icsa-19-178-04

ICSA-19-178-05: **Advantech WebAccess/SCADA**
Kritikus szintű sérülékenységek: Útvonal bejárás, puffer túlcsordulás, határokon kívüli olvasás és írás lehetősége, nem megbízható forrás miatti pointer működési hiba.
https://www.us-cert.gov/ics/advisories/icsa-19-178-05

ICSA-19-171-01: **PHOENIX CONTACT Automation Worx Software Suite**
Magas szintű sérülékenységek: Nem inicializált Pointer elérés, pufferen kívüli adat olvasás, memória felszabadítás utáni program összeomlás.
https://ics-cert.us-cert.gov/advisories/ICSA-19-171-01

ICSMA-19-164-01: **BD Alaris Gateway Workstation**
Kritikus szintű sérülékenységek: nem megfelelő hozzáférés ellenőrzés, veszélyes típusú fájl feltöltés korlátozásának hiánya.
https://ics-cert.us-cert.gov/advisories/ICSMA-19-164-01

ICSA-19-164-01: **Johnson Controls exacqVision Enterprise System Manager**
Közepes szintű sérülékenység: nem megfelelő hitelesítés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-164-01

ICSA-19-164-02: WAGO Industrial Managed Switches 852-303, 852-1305, and 852-1505

Kritikus szintű sérülékenységek: beégetett hitelesítés használat, beégetett kriptográfiai kulcs használat, ismert sérülékenységekkel rendelkező összetevő használata.
https://ics-cert.us-cert.gov/advisories/ICSA-19-164-02

ICSA-19-162-01: Siemens Siveillance VMS

Magas szintű sérülékenységek: Nem megfelelő hitelesítés, nem megfelelő felhasználó menedzsment, hiányzó hitelesítés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-01

ICSA-19-162-02: Siemens SIMATIC Ident MV420 and MV440 Families

Magas szintű sérülékenységek: Nem megfelelő privilégium menedzsment, szenzitív információk egyszerű szöveges formában történő továbbítása.
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-02

ICSA-19-162-03: Siemens LOGO!8 Devices

Magas szintű sérülékenységek: A műveletek nem megfelelő korlátozása a memóriapuffer határain belül, session rögzítés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-03

ICSA-19-162-04: Siemens SCALANCE X

Magas szintű sérülékenység: Jelszavak visszaállítható formában történő tárolása.
https://ics-cert.us-cert.gov/advisories/ICSA-19-162-04

ICSA-19-157-01: Optergy Proton Enterprise Building Management System

Kritikus szintű sérülékenységek: információ feltárás, CSRF, korlátozatlan fájl feltöltés, nyílt átirányítás, rejtett funkcionalitások, veszélyes mód vagy funkció feltárás, beégetett hitelesítő használat.
https://ics-cert.us-cert.gov/advisories/ICSA-19-157-01

ICSA-19-157-02: Panasonic Control FPWIN Pro

Magas szintű sérülékenységek: Puffer túlcsordulás, nem kompatibilis típus használat erőforrás hozzáférés esetén.
https://ics-cert.us-cert.gov/advisories/ICSA-19-157-02

ICSA-19-155-01: PHOENIX CONTACT PLCNext AXC F 2152

Magas szintű sérülékenységek: Kulcs menedzsment hibák, nem megfelelő hozzáférés ellenőrzés, közbeékelődéses támadás (M-I-T-M), ismert sérülékenységekkel rendelkező összetevő használata.
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-01

ICSA-19-155-02: PHOENIX CONTACT FL NAT SMx

Magas szintű sérülékenység: nem megfelelő hozzáférés ellenőrzés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-02

ICSA-19-155-03: **Geutebrück G-Cam and G-Code**
Magas szintű sérülékenységek: XSS, operációs rendszer parancs befecskendezés.
https://ics-cert.us-cert.gov/advisories/ICSA-19-155-03

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

**DICOM (Digital Imaging and Communications in Medicine)** – Digitális orvosi kommunikációs és képalkotó sérülékenységéről adott ki riasztást az ICS-CERT.

Az input validációs sérülékenység távolról nem kihasználható, és az egészségügyi ágazat szereplői érintettek. A hordozhatóság tekintetében .dcm fájlkiterjesztés van használatban.

A sérülékenység sikeres kihasználása lehetővé teszi, hogy a támadó végrehajtható kódot ágyazzon be az orvosi képalkotó eszközök által használt képfájlokba. A támadás okozta incidens súlyossága a szándék, és a végrehajtandó kód függvénye. Windows környezetben futtatható a kód, és közben nem zavarja a DICOM funkcionalitását. A sérülékenységről bővebb információ a következő linken érhető el: https://nvd.nist.gov/vuln/detail/CVE-2019-11687

A sérülékenység hatásainak és kockázatainak csökkentése érdekében a DICOM egy jelentést adott ki, amely a következő linken érhető el: https://www.dicomstandard.org/dicom-in-the-news/

Javasolt a sérülékenység vonatkozásában felkeresni az antivírus szolgáltatót, annak érdekében, hogy a megfelelő megoldás megszülethessen a kockázatok csökkentésére, a megfelelő fájltípus monitorozása által. Ha nem rendelkezik a szervezet vírusvédelmi megoldással, abban az esetben meg kell győződni az érintett eszközökkel kapcsolatos csatlakoztatható - hordozható eszközök megfelelő kontrolljairól.

További információk a következő weboldalon találhatók: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-19-162-01

## ICS jó gyakorlatok, javaslatok

Az ipari irányító rendszerek javarésze már több mint 25-30 éves. Nem szabad figyelmen kívül hagyni, hogy a rendszereknek az évek alatt kialakult hiányosságai vannak, és bizonyos hibák megoldhatók valamely alternatív megoldással. Ezek a sajátosságok azok, amelyekkel, ha nincs tisztában egy szervezet, akkor az üzletmenet folytonosság fenntartása problémát okozhat.

A több évtizeddel ezelőtti világban nem volt akkora fluktuáció a szervezeteknél, mint manapság, és azok a személyek, akik ismerik a régebbről eredő hibákat és alternatív megoldásokat egy ipari irányító rendszer működésében, valamint annak minden apró részletét, azon munkavállalók tudása rengeteget ér. Ha egy ilyen személy bármilyen okból akadályoztatva van (betegség, nyugdíjazás), akkor a tudás, amely az egyén birtokában van, kikerül a szervezetből.

A mai világban már sokkal magasabb a fluktuáció a felgyorsult világ, valamint az igények gyors változása következtében. Ebből fakadóan nincs ideje azt a tapasztalatot, azt a tudást megszerezni egy üzemeltetésben dolgozónak, mint amennyi a régebbi kollégáknak volt. Javasolt azon szakemberek tudását még a nyugdíjba vonulás előtt papírra vetni, a mai dolgozók számára is értelmezhető formában és módon, hogy az üzemeltetést tovább folytató emberek is tisztában legyenek az adott ipari irányító rendszerek effajta sajátosságaival.

Ez a folyamat a tudásmenedzsment egy szelete. Egy szervezet kockázatelemzése-, és egyéb humán erőforrással kapcsolatos döntései során nem szabad figyelmen kívül hagyni a szervezet dolgozóinak fejében meglévő tudását.

Akit bővebben érdekel a téma, további információkat találhat tudásmenedzsment témában a következő linken:

https://hetpecset.hu/site/uploads/files/bencsikeloadas.pdf

Az előadás a Hétpecsét Információbiztonsági Egyesület, 2018 január 17-én megtartott Információvédelem menedzselése LXXIX. Szakmai Fórumon hangzott el.

## ICS képzések, oktatások

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

Az IT biztonság és az ICS környezet kombinációjának középpontba állításával kerül megrendezésre a következő oktatás:

- Industrial Control System Cyber Security Management System; Cipaganti, Coblong, West Java, Indonesia; 2019. július 15-19.

A részletek a következő webhelyen találhatók:

http://fedco.co.id/event/industrial-control-system-cyber-security-management-system-11/

2019. júliusában a következő tréningek, oktatások kerülnek lebonyolításra az ICS biztonság kapcsán a SANS szervezésében:

- ICS410: ICS/SCADA Security Essentials SANS Pittsburgh 2019; USA, Pittsburgh; 2019. július 8-12.
- ICS410: ICS/SCADA Security Essentials SANS San Francisco Summer 2019; USA, San Francisco; 2019. július 22-26.

A részletek a következő webhelyen találhatók:

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

### 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. júliusában:

Kétnapos konferencia keretében lesz lehetősége a jelentkezőknek az ipari irányító rendszerekről tanulni, történeteket és tapasztalatokat megosztani. A konferencia az ICS biztonság stratégiai, technikai és üzleti vetületeire fog koncentrálni.

National SCADA Conference; Ausztrália, Sydney; 2019. július 30-31.

További részletek a következő webhelyen találhatók:

http://www.scada-conference.com/

## ICS incidensek

### Dél-Amerika áramszünet, 44 millió érintett

Habár egyes források szerint nem hekker támadás következménye, de nem lehet szó nélkül elmenni a dél-amerikai áramszünet mellett. 2019. június 15-16-i hétvégén áram nélkül maradt területét tekintve Argentína, Chile, Uruguay és Paraguay 44 millió lakosa. A pontos okait egyelőre még mindig nem tudják a szakértők az incidensnek, de nem kizárható, hogy egy kibertámadás okozta a kiterjedésétt tekintve egyedülálló eseményt.

Az extrém időjárási körülmények miatti okokat sem zárta ki a szakma, ugyanis a hétvégén erős esőzések voltak a latin-amerikai kontinens déli részén.

Akár kibertámadás, akár extrém időjárás okozta az áramkimaradást, elgondolkodtató mindenképp, hogy a logikai és fizikai védelmi intézkedések megfelelően implementáltak voltak-e a teljes hálózat tekintetében. Az extrém időjárási körülményekre a klímaváltozás okán fel kell készülni, egyre gyakrabban várhatók ilyen események, továbbá a kibertámadások okozta károknak nem szabadna, hogy ekkora területen ellehetetleníthesse az áramszolgáltatást. Ez mindenképp felveti azt a kérdést, hogy miként kerültek részekre osztva, szeparálva a rendszer bizonyos részei, hogy a hatások ne gyűrűzhessenek tovább, és ne érinthessék a teljes hálózatot?

További információkhoz az alábbi linkeken lehet hozzáférni:

https://www.bloomberg.com/opinion/articles/2019-06-17/argentina-blaming-hackers-for-outage-makes-smart-grids-look-dumb

https://www.securitynewspaper.com/2019/06/17/power-blackout-in-argentina-uruguay-paraguay-and-brazil-is-this-the-biggest-cyberattack-ever/

https://www.wired.com/story/argentinas-blackout-and-the-storm-battered-future-of-the-grid/

### Az USA kibertámadása az iráni rakétairányító rendszere ellen

Az Irán és az USA között, a Hormuzi-szorosban zajló konfliktusnak (tankerhajók elleni támadások, drón lelövése) a következménye az iráni fegyverrendszerek számítógépei-, illetve a légvédelmi rakétairányító rendszerek elleni kibertámadás.

Megerősített információ nincs egyelőre arról, hogy mennyire sikeres az USA által végrehajtott kibertámadás, de az AP hírügynökség szerint sikerült kiiktatni az iráni Forradalmi Gárda fegyverrendszerét, amely közreműködött a drón lelövésében.

A múltban már volt példa politikai motivációból elkövetett ipari irányító rendszerek elleni támadásra a két ország részvételével (Stuxnet, 2010.), akkor szintén az USA indított támadást, az iráni urándúsító rendszer ellen, amely sikeres volt.

A mostani támadás részletei még nem ismertek, azonban fontos megjegyezni, hogy a politikai akarat által vezérelt kiber hadseregek támadásba lendülése rendkívüli fenyegetést jelenthet az ipari irányító rendszerekre, közvetetten meghatározó számú emberi életre.

További információk:

https://index.hu/techtud/2019/06/23/usa_iran_dron_kibertamadas_trump/

https://www.tellerreport.com/news/2019-06-23---a-cyber-attack-on-iran-.Sk-cDQR3kH.html

https://www.securityweek.com/us-launched-cyber-attacks-iran-after-drone-shootdown-reports

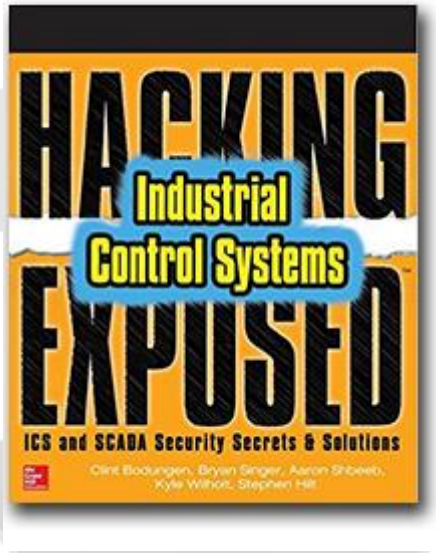
## Könyvajánló

A következő könyvben az ipari irányító rendszerek penetrációs tesztelésének részletes technikai leírását találhatják meg a téma iránt érdeklődők. Kifejtésre kerül a könyvben, hogy miként kell menedzselni egy ICS penetrációs teszt projektet, hogy kell azt végrehajtani, hogy az biztonságos legyen, és milyen módon kell a védelmet kialakítani a külső támadásokkal szemben.

A könyv címe: "Hacking Exposed, Industrial Control Systems: ICS and SCADA Security Secrets & Solutions"

Szerzők: Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt

Kiadás dátuma: 2016. szeptember 16.



## Black Cell javaslatok

Az ICS biztonsággal több szervezet is foglalkozik, és hasznos tudásbázist lehet kiépíteni, ha a kiadott Whitepaper-ek és egyéb dokumentumok jó gyakorlatait összegyűjtjük, és a saját rendszereinkre vonatkozó részeket implementáljuk.

Ilyen a Veracity Industrial Networks által kiadott Whitepaper, mely a következő két fő témát vesézi ki:

- Az ICS hálózat átláthatóságának és kontrolljának hiánya
- Az örökölt rendszerek kihívásai

A Whitepaper a következő weboldalról tölthető le:

https://veracity.io/download/veracity-ics-whitepaper/