Energetikai létesítményeket ért incidensek

(2020. szeptemberi állapot)

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
1	Salt River Project	USA, Phoenix metropolitan area	1994	Lane Jarret Davis jogosulatlan hozzáférést szerzett egy betárcsázós modemen keresztül az SRP egyes rendszereihez, köztük legalább 5 órán keresztül a Phoenix város tágabb környezetének vízellátásáért felelős SCADA rendszerhez is.	Egy tartalék számítógéphez csatlakoztatott betárcsázós modem	SCADA	Pénzügyi veszteség 40.000 USD, nincs információ a fizikai folyamatokra gyakorolt hatásról	https://www.risidata.com/Database/Detail/salt-river-project-hack
2	US Navy - San Diego-i közműszolgáltatók	USA, San Diego	1999	1999 novemberben az amerikai haditengerészet San Diego-i öböl közelében végrehajtott hadgyakorlata során a haditengerészeti radarok olyan EMI (elektromágneses interferencia) hatást generáltak, ami zavart okozott a San Diego megyei vízmű és a San Diego-i gáz- és elektromos művek ICS rendszereiben használt távkezelt berendezések kapcsolataiban és a távkezelésben.	Vezeték nélküli kommunikáció zavarása (nem szándékos)	SCADA, PLC, RTU	Az érintett alállomásokon vissza kellett állni manuális vezérlésre.	https://www.risidata.com/Database/Detail/navy-radar-shuts-down-scada-systems
3	CA ISO	USA, Califiornia	2001	2001-ben a kaliforniai független villamosenergia-ipari rendszerirányító IT rendszereit érte támadás. A támadók két, nem megfelelően tűzfalazott és Internetről elérhető webszerver kompromittálásán keresztül fértek hozzá a rendszerirányító belső hálózatához. Az incidens kiváltó okaként alapvetően a nem kellően biztonságtudatos tervezést és kivitelezést tartják, illetve az időkritikus üzleti folyamatok biztonságos működés fölé emelt prioritását	Nem megfelelően szegmentált hálózat, gyenge biztonsági intézkedések Internetről elérhető webszerverek esetén	Nem érintett ICS rendszereket	Nem ismert	https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf
4	Blaster worm	USA, Kanada	2003	Egyes források szerint a 2003-as nagy Észak-keleti áramszünet (ami az USA Észak-keleti államai mellett egyes Dél-Kelet-kanadai régiókban is üzemzavart okozott) hátterében a Blaster féregtámadás állt. Bár az incidens utáni elemzések szerint az érintett szolgáltatók ICS/SCADA rendszerei nem Windows operációs rendszeren futottak, de egyes monitoring rendszerek igen. A Blaster ezeket tette használhatatlanná, ami miatt az üzemzavar-elhárításért felelős villamosmérnökök nem tudták időben észlelni és megelőzni a nagy kiterjedésű üzemzavart.	Automatikusan kihasználható Windows sérülékenységen keresztül terjedő féreg	-	Kb. 55 millió fogyasztó maradt villamos áram nélkül hosszabb-rövidebb időre (4 órától két hétig terjedő időszakokról állnak rendelkezésre információk)	https://blogs.scientificamerican.com/observations/expert-a-virus-caused-the-blackout-of-2003-will-the-next-one-be-intentional/
5	Stuxnet	Natanz, Irán	2010	A Stuxnet néven ismert autonóm ICS malware az iráni urándúsító infrastruktúra és folyamat megzavarását célzó támadás volt, ami 4 különböző Windows 0-day sérülékenységet használt ki a terjedéshez és a WinCC DLL lecserélésével hajtott végre man-in-the-middle támadást az urándúsító centrifugákat vezérlő PLC-k ellen.	USB adathordozók, automatikus futtatás, szerver kompromittálás, man-in-the-middle	WinCC, PLC	Urándúsítási folyamat szabotálása, urándúsító centrifugák (minimum több 100 darab) fizikai meghibásodása)	https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
6	Havex/ Dragonfly	Európa, USA	2014	ICS rendszerek és ICS fejlesztő/felhasználó európai és Észak-amerikai vállalatok ellen indított, elsődlegesen információszerzésre specializált támadás-sorozat, ami kifejezetten kritikus infrastruktúrákat (elsődlegesen az energia-szektort) és beszállítóikat célozta.	Spear-phising, watering hole, RAT (Remote Access Tool)	A kompromittált gyártók weboldalain elhelyezett ICS szoftvertelepítő fájlokkal telepített rendszerek.	Mivel a támadások célja az információszerzés volt, ezért az incidenseknek a fizikai világra és folyamatokra gyakorolt hatása nem ismert.	https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
7	Calpine	USA	2014	Támadók kompromittálták a Calpine (jelentős szereplő az USA villamos-energia szektorában) szélerőműveket irányító SCADA rendszerének egyes elemeit és manuális szabályozásra állították az automata vezérlést.	Beszállítói lánc támadása (Supply-Chain Attack)	ICS/SCADA	Az incidensnek nem volt közvetlen hatása a villamosenergia-rendszerre.	https://apnews.com/c8d531ec05e0403a90e9d3ec0b8f83c2
8	Malware-támadás ázsiai atomerőművek ellen	Japán, Dél-Korea	2014	Malware-támadás ért egy japán (Monju) és egy Dél-koreai (Korea Hydro and Nuclear Power Plant) atomerőmű vezérlőtermében használt egyes rendszereket.	Malware-támadás	Nem ismert	Nem ismert	http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html
9	Ukrán áram-szolgáltatók	Nyugat-Ukrajna	2015.12.23	Támadók 4 Nyugat-ukrajnai áramszolgáltató ICS rendszereit kompromittálva idéztek elő számos alállomáson jelentős üzemzavart, majd törölték a SCADA rendszerek diszkjeit és illegális firmware-frissítésekkel használhatatlanná tettek számos RTU-t. A támadók utolsó lépésként DDoS-támadásokkal elérhetetlenné tették az érintett áramszolgáltatók webszervereit és hibabejelentésre használt telefonos ügyfélszolgálatait. A szolgáltatás helyreállítását jelentősen gyorsította az érintett áramszolgáltatóknál az automatizálás alacsony szintje, így képesek voltak gyorsan átállni manuális vezérlésre.	Spear-phising, BlackEnergy, KillDisk	ICS/SCADA, RTU	Mintegy 225.000 fogyasztót és 135 MW teljesítményt érintő áramkimaradás. Az incidensben érintett RTU-k teljes körű cseréje hónapokat (egyes esetekben 4-6 hónapot) vett igénybe.	https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
10	Izraeli közmű-szabályozó hatóság	Izrael	2016	Súlyos kibertámadás érte az izraeli közműszabályozó hatóság több rendszerét. Az incidens részletei nem ismertek.	Nem ismert	-	Nem ismert	https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/

Energetikai létesítményeket ért incidensek
(2020. szeptemberi állapot)

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
11	Malware-támadás német atomerőmű ellen	Német-ország	2016	Malware-t találtak a Gundremmingen-i atomerőmű rendszereiben. Az erőmű vezérléséért felelős rendszereket az incidens nem érintette.	Nem-célzott malware-támadás, a malware egy hétköznapi kártevő volt, az erőművi rendszerbe történő bejutási módja nem ismert	-	Az incidensnek nem volt közvetlen hatása az erőmű alap funkcióira.	https://securityaffairs.co/wordpress/46708/security/virus-gundremmingen-nuclear-plant.html
12	Industroyer/ CrashOverride	Ukrajna, kijevi körzet	2016.12.17	Az Ukrenergo ukrán rendszerirányító elleni támadás a negyedik ismert, ICS rendszereket célzó támadás és a második, amiben autonóm, ICS rendszer ellen készített malware-t használtak a támadók (az első a Stuxnet volt). Egyes elemzők szerint a támadók célja nem egy sima üzemzavar előidézése volt, hanem azt tervezeték, hogy az üzemzavar előidézése után, amikor az Ukrenergo szakemberei a szolgáltatás helyreállításán dolgoznak, DoS-támadásokkal kiiktatnak több védelmet, majd az így védtelenül maradt alállomási berendezések egy túlterhelés esetén akár végzetes károkat is szenvedhettek volna, ami akár több hónapos, fél éves, éves áramkimaradásokat is okozhatott volna. Az elemzés szerint ez végül csak azért nem következett be, mert a támadók hibát vétettek a DoS-támadáshoz használt számítógépes kódok fejlesztése esetén.	Industroyer/CrashOverride ICS malware	ICS/SCADA RTU Digitális védelem	200 MW teljesítmény kiesése a villamosenergia-rendszerből (az érintett felhasználók száma ismeretlen)	https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf
13	NotPetya	Ukrajna, Csernobil	2017. június	Az EternalBlue sérülékenységet kihasználó NotPetya ransomware (más források szerint cryptowiper malware) támadása miatt a Csernobili atomerőmű környezetében használt sugárzásmérő rendszer működése ellehetetlenült. Az érintett rendszer működését manuális vezérlésre kellett állítani	Feltételezhetően nem célzott malware-támadás, ami egy 3 hónapja ismert, javítással is rendelkező sérülékenység kihasználására épült.	Mérő- és adatgyűjtő rendszerek	Az erőmű rendszereire az incidensnek nem volt hatása.	https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html
14	Ír villamos-energia ipari rendszer-irányítók	Írország, Észak-Írország	2017. augusztus	Az EirGrid ír rendszerirányító és Észak-irországi leányvállalata, a SONI ellen intéztek támadást ismeretlenek, a becslések szerint 2 hónapig lehallgatva a két villamosipari rendszerirányító hálózati forgalmát.	A két érintett szervezet Interneten elérhető hálózati eszközeiről a támadók GRE tunnel alkalmazásával kitükrözték a hálózati forgalmat és kb. két hónapon keresztül hallgatták le a két rendszerirányító Internetes kommunikációját.	-	Az incidensnek nem volt ismert hatása a villamosenergia-rendszerre.	https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html
15	Támadások az USA villamosenergia-rendszere ellen	USA	2018. július	Az amerikai Belbiztonsági Minisztérium (Department of Homeland Security, DHS) egy publikus webes előadás-sorozatot tartott az USA kritikus infrastruktúrája elleni orosz kibertámadásokról . Az előadás-sorozat egyik újdonsága az volt, hogy a támadók a különböző célba vett kritikus infrastuktúrákat gyakran azok beszállítóin (nem csak fejlesztő, hanem gyakran szolgáltatást biztosító vállalatokon) keresztül, a beszállító rendszereit és gyakran termékeit kompromittálva támadták. Érdemes megfigyelni a hasonlóságot a Havex-nél már bemutatott módszerrel, amikor európai ICS gyártók letölthető binárisait cserélték le malware-rel fertőzött változatokra, így támadva a kiszemelt szervezeteket.	Beszállítói lánc támadása (Supply-Chain Attack)	Nem ismert	Az incidenseknek nem volt ismert hatása a villamosenergia-rendszerre.	https://www.us-cert.gov/sites/default/files/c3vp/Russian_Activity_Webinar_Slides.pdf
16	Ransomware-támadás a johannesburgi áram-solgáltató ellen	Dél-Afrikai Köztár-ság	2019. július	Ransomware-támadás érte a johannesburgi áramszolgáltató rendszereit, aminek következtében – bár az áramszolgáltató ICS rendszereit állításaik szerint nem érintette az incidens – mégis egyes ügyfeleknél, (akik, (hasonlóan a magyar feltöltő kártyás mobil telefont konstrukciót használókhoz hasonlóanhasonló módon) előre fizettek a villamosáramért), hosszabb áramkimaradások voltak.	Ransomware-támadás, ami az áramszolgáltató adatbázisait és más rendszereit tette használhatatlanná	-	A rendelkezésre álló információk szerint az incidens nem érintette a villamosenergia-rendszer irányításáért felelős ICS rendszereket, de az előre fizető felhasználók egy bizonyos hányadánál áramkimaradások voltak	https://www.reuters.com/article/us-safrica-city-power/johannesburg-power-body-hit-by-ransomware-attack-idUSKCN1UK15N

Energetikai létesítményeket ért incidensek
(2020. szeptemberi állapot)

#	Incidens azonosítója	Incidens helye	Incidens publikálás időpontja	Incidens leírása	Támadási vektor	Érintett ICS rendszerek	Incidens hatásai	Források
17	DoS-támadás a vezérlő-központ és az alállomás közötti kommunikációt biztosító berendezések ellen	USA	2019. szeptember	Az USA nyugati felén található sPower nevű villamosenergia-ipari cég vezérlő központja és távoli, kisebb erőművei közötti kommunikációt biztosító egyik eszköz (egy tűzfal) sérülékenységeit kihasználva támadók DoS-támadással átmenetileg ellehetetlenítették az erőművi alállomások távfelügyeletét.	Az internetre csatlakoztatott tűzfal webes adminisztrátori felületének egy ismert, de nem javított hibáját kihasználva folyamatos újraindításokat idéztek elő a támadók	-	A kommunikáció kiesése a felügyeleti funkciók átmeneti degradálódását okozta, de nincs információ ennek nyomán kialakult üzemzavarról vagy fogyasztókat érintő áramkimaradásokról.	https://www.eenews.net/stories/1061111289
18	Malware-támadás indiai atomerőmű rendszerei ellen	India	2019. október	Feltételezhetően célzott malware-támadás érte a Kudankulam atomerőművet (KKNPP) Indiában. A malware-t a Dtrack néven ismert, a feltételezések szerint Észak-koreai állami hátterű Lazarus csoporthoz köthető malware-ként azonosították.	A rendelkezésre álló információk szerint a malware a KKNPP ügyviteli hálózatait fertőzte meg, feltehetősen Internet-eléréssel rendelkező hostokon keresztül.	Nem ismert	Az incidensnek a KKNPP és az indiai szabályozó szerv közlése szerint nem volt hatása az erőmű irányítástechnikai rendszereire	https://dragos.com/blog/industry-news/assessment-of-reported-malware-infection-at-nuclear-facility/
19	Kibertámadás az ENTSO-E ellen	Belgium	2020. március	Támadás érte az ENTSO-E (European Network of Transmission System Operators for Electricity) irodai rendszereit. Az ENTSO-E közleménye szerint a rendszereinek nincs kapcsolata az európai villamosenergia-ipari TSO-k rendszereivel.	Nem ismert.	Nincs	Nem ismert	https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/
20	EDP ransomware-támadás	Portugália	2020. április	Nagyszabású ranswomware-támadás és adatlopás érte a portugál központú, multinacionális, gáz és villamosenergia-szektorban tevékenykedő EDP-csoportot. A támadók a RagnarLocker malware-t használták és a fájlok titkosítása mellett az ellopott adatok nyilvánosságra hozásával is zsarolták az EDP-t.	Feltételezhetően fertőzött MS Office dokumentumokban, e-mail csatolmányként érkezett a malware.	Nincs	Kb. 10 TB-nyi adatot loptak el illetve titkosítottak a támadók.	https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
21	Elexon elleni támadás	UK	2020. május	Közelebbről nem részletezett kibertámadás érte a Nagy-britanniai villamosenergia-piacot működtető Elexon IT rendszereit. A beszámolók szerint az incidensben az Elexon legfontosabb rendszerei nem voltak érintettek.	Nem ismert	Nincs	Egyes rendszereket kb. egy napra le kellett állítaniuk.	https://www.theguardian.com/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system https://theenergyst.com/elexon-hit-by-cyber-attack/
22	K-Electric ransomware-támadás	Karacsi, Pakisztán	2020. szeptember	Pakisztán legnagyobb, Karacsi városa és környékének villamosenergia-ellátásáért felelős vállalatának rendszereit érte ransomware-támadás. A NetWalker ransomware egyes, Interneten elérhető szolgáltatásokat tett használhatatlanná az áramszolgáltató ügyfelei számára. Az elérhető információk alapján a K-Electric üzemirányító rendszereit az incidens nem érintette.	Nem ismert	Nincs	A K-Electric egyes online szolgáltatásai (pl. számlákhoz történő ügyfél-hozzáférések) átmenetileg leálltak.	https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-pakistans-largest-private-power-utility/