CTI Jelentés

IoT eszközök biztonsági kérdései - Az ipar

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
1996
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés

Az IoT (Internet of Things, magyarra fordítva: a "dolgok internete") olyan internetre csatlakoztatott eszközök összesége, amelyek képesek kommunikálni más eszközökkel és hálózatokkal, de funkcionalitásuktól függően sokféle feladatra képesek. Sok IoT eszköz az internetkapcsolatot felhasználva teszi lehetővé, hogy a felhasználók távolról is elérhessék és működtethessék az eszközöket, valamint biztosítani tudják a távoli adatbázisokhoz való hozzáférést.

Egyes megközelítések szerint az okostelefonok és a számítógépek is ide tartoznak, azonban van, aki azt vallja, hogy csak azokat az eszközöket lehet az IoT kategóriába sorolni, amelyeknek van IP címe, nem Windows, Linux, Android vagy iOS operációs rendszert futtat, nem igényel közvetlen hozzáférést belső tárolóeszközökhöz és nem tárol személyes adatokat. 2021-ben körülbelül 25 milliárd ilyen eszköz csatlakozott az internetre, és számuk évről évre rendkívüli mértékben növekszik. Egyes becslések szerint 2030-ra elérheti a 75-100 milliárdot is, ami a Föld teljes lakosságára levetítve emberenként 10 ilyen küszéléket fog jelenteni. A piaci és fogyasztói adatokra specializálódott német vállalat, a Statista szerint 2021-ben az IoT eszközök összértéke átlépte a 440 milliárd dollárt és 2030-ba akár az 1000 milliárd dollárt is elérheti. Egyre többen okosítják otthonaikat, egyre több modern egészségügyi központ épül világszerte és egyre több multinacionális vállalat automatizálja a gyártását. Ezekben - és más szektorokban is - egyre nagyobb szerepet kap a mesterséges intelligencia és az internetre csatlakoztatható IoT eszközök.

Minden ilyen új berendezés biztonsági kockázatot jelenthet, ugyanis sok esetben a bővülő piaci igények kielégítése, az időnyomás és a profitorientáltság a megfelelő védelem rovására mehet a gyártók részéről. Legyünk cégünknél egyszerű felhasználói vagy felelősei az ipari méretű IoT kiépítésekért, nagyon fontos, hogy megfelelő tudatossággal járjunk el a folyamatnak minden szakaszában a tervezéstől a karbantartásig.

A dokumentum célja, hogy bemutassa az olvasó számára a piacon elérhető ipari IoT eszközök sokaságát, a villamosenergia szektorban elfoglalt helyét és ismertesse annak fontosságát kiberbiztonsági aspektusból.

Jelen CTI tájékoztató a második része egy, az IoT eszközöket érintő biztonsági kérdések minisorozatnak, amelynek első része IoT eszközök biztonsági kérdései - Az okosotthon címmel elérhető a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban NBSZ NKI) honlapján.

Az ipari IoT

A dolgok ipari internete (Industrial Internet of Things - IIoT) a számítógépekkel összekapcsolt érzékelőkre, műszerekre és olyan egyéb eszközökre utal, amelyek hálózatba vannak kapcsolva a számítógépek ipari alkalmazásaival, beleértve a gyártást és az energiagazdálkodást is. Ez a rendszer lehetővé teszi az adatgyűjtést, amelyeknek a feldolgozása képes javítani és folyamatosan optimalizálni a termelékenységet és a nyújtott szolgáltatások zökkenőmentességét. A 21. században már feltétlenül szükséges szolgáltatásról van szó a versenyképesség és a termelési hatékonyság fenntartása érdekében.

Az egyszerű IoT eszközökhöz hasonlóan az ipari berendezések biztonsága is aggodalomra adhat okot a vállalatok számára. Míg korábban nem, vagy csak nagyon kis mértékben lehetett arra számítani, hogy egy kiberbűnöző ilyen rendszert vesz célba, ez mára már teljesen megváltozott. Egy ország kritikus infrastruktúra szolgáltatóinak és magának az államnak is hatalmas figyelmet kell fordítania arra, hogy tökéletesen biztonságosak legyenek minden tekintetben, de mi történik akkor, ha ezt egy ember, csoport vagy akár geopolitikai érdekeket szolgáló kiterjedt szervezet igyekszik felhasználni az adott szolgáltató, vállalat vagy akár egy egész ország ellehetetlenítésére?

Ha az infrastruktúrát nemzetbiztonsági szempontból vizsgáljuk, akkor megkülönböztetünk kritikus infrastruktúrákat, amelyek működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe. Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, amelyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

[A kritikus információs infrastruktúrák]

Az összes kritikus infrastruktúra nélkülözhetetlen egy ország működőképessége szempontjából, mindegyik elengedhetetlen komponense az államnak, így nem lehet fontossági sorrendet felállítani köztük. Viszont ha kiberbiztonsági szempontból vizsgáljuk ezek támadhatóságát, az energiaellátás kiemelkedik az összes többi közül. Erre ad tanúbizonyságot a 2015. december 23-án bekövetkezett kibertámadás az ukrán energiahálózat ellen, amelynek következtében 230.000 ember maradt áram nélkül a nyugat-ukrajnai Ivano-Frankivszk tartományban. Magyarországnak érdeke, hogy ilyen ne történhessen meg vele a jövőben.

Ennek érdekében 2018-ban a Magyar Elektrotechnikai Egyesület szervezett egy beszélgetést annak reményében, hogy a villamosenergetikai szakma és a kiberbiztonsági szakma közelebb kerüljön egymáshoz. Ebben a témában készült egy epizód a Kibertámadás! podcastünkben, amelyben szó esik a SeConSys nevű kezdeményezésről. A 2020 decemberében megjelent a *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*, amelynek aktuális 2021-es verziójai letölthető a SeconSys oldaláról.

Európában a villamosenergetikai rendszerek egyre komplexebb hálózatokat jelentenek. A villamosenergia termelése és felhasználása egyre kevésbé ismer országhatárokat, több ország is külföldről szerzi be villamosenergiájának jelentős részét. Ez az összekapcsoltság csak tovább fokozza az igényt a villamosenergetikai rendszerek kibervédelmére. Ennek tükrében a kézikönyvben összegyűjtésre kerültek a legjobb gyakorlatok és tapasztalatok, hogy segítséget nyújtson az üzemeltetők és szakértők számára az ICS/SCADA rendszerek biztonságának magasabb szintre emeléséhez.

SCADA (Supervisory Control And Data Aquisition): Olyan felügyeleti, szabályozó és adatgyűjtő rendszer, amely biztosítja az ipari berendezések távoli felügyeletét. Az adatgyűjtés és tárolás következtében egyrészről valós időben kaphatunk pontos adatokat az ipari folyamatokról, másrészről visszamenőleg is vizsgálhatjuk azok.

ICS (Industrial Control System): Az ipari vezérlőrendszer kifejezés az ipari folyamatokat működtető és automatizáló, különböző típusú vezérlőrendszerek és kapcsolódó műszerek gyűjteményére utal. Magában foglalja az összes kapcsolódó eszközt, rendszert, hálózatot és vezérlést.

IIoT eszközök

A piacon elérhető ipari IoT eszközök skálája széleskörű, folyamatosan jönnek létre az újabb IoT eszközök és új felhasználási módokat és területeket találnak ki a gyártók is. Éppen ezért csupán néhány, jelenleg is alkalmazásban álló rendszer kerül jelenleg bemutatásra:

1. **Olaj- és gázipari érzékelők:** olyan IoT eszközök, amelyek értesítéseket küldenek az üzemeltetőknek, ha szivárgás keletkezett valahol a rendszerben. Például az Aptomar gyárt ilyen eszközöket, továbbá bizonyos szolgáltatásokat is kínál az olaj- és gázipari létesítmények felügyeletéhez.

2. **Nyomkövető eszközök:** a szállítási és logisztikai iparágban elengedhetetlen, ha egy adott vállalat rendelkezik gépjárművekkel, hogy azok nyomon követhetők legyenek. Az ATrack GPS szolgáltatást kínál eszközök és járművek nyomon követésére. Technológiáját számos más gyártónak és nyomkövető szolgáltatónak szállítja.

3. **Logisztikai szenzorok:** Ezek olyan érzékelők, amelyek beépíthetők a termékszállítmányokba, folyamatosan nyomon követik a környezet hőmérsékletét és páratartalmát, a csomagokat ért ütéseket, a beeső fénymennyiséget, a küldemény dőlését vagy esetleges felborulását és a csomagra nehezedő nyomást. Ezeket az adatokat egy integrált elemzőrendszer követi nyomon, amely lehetővé teszi a gyártók és a logisztikai vállalatok számára, hogy a szállítási alatt is lássák, hogy mi történik a termékeikkel. Az egyik legnagyobb gyártó a CargoSense, amely ilyen szenzorok gyártásával foglalkozik.

4 **Ipari érzékelők:** A gyártók internetre csatlakoztatott érzékelőberendezéseket használhatnak arra, hogy adatokat gyűjtsenek gyári eszközeikről, és hogy nyomon kövessék az összeszerelősorokat az esetleges problémák kiszűrése céljából. Az IoT érzékelők a berendezések és az egyes erőforrások nyomon követésével támogatják a gyártási folyamatokat, az üzemeltetés átláthatóságát, a karbantartás ütemezését és a logisztikát. A Filament termékei a környezet megfigyelésére és az adatok hálózaton keresztüli továbbítására használatosak.

5 **Intelligens gépjárművek:** A különböző méretű autók és teherautók egyre több IoT funkcióval rendelkeznek. A gyártók kitűzött célja, hogy megalkossák a teljes mértékben önvezető gépjárműveket és idővel a világ lehető legnagyobb részére kiterjesszék azok értékesítését. Ennek elérésében több gyártó is közreműködik, mint például a Nissan, a Tesla, a Mercedes, a Volkswagen/Audi, de érdekelt az iparágban a Google, az Amazon és a Bosch is.

6 **Intelligens kamerák:** Minden vállalat szeretné megvédeni a tulajdonát, így évről-évre többet hajlandók befektetni az egyre modernebb biztonsági megoldásokba. Ilyenek például az olyan internetre csatlakoztatott okoskamerák, amelyek távolról vezérelhetők és felvételeiket biztonságos, külső helyszíneken tárolják. Egyes IoT kamerák olyan szoftvereket használnak, amelyek segítik a betolakodók és fegyverek felismerését, és riasztást küldenek, ha ilyet észlelnek.

7 **Gyártó robotok:** A szerelősorokon egyre nagyobb hangsúlyt kap az automatizálás. Az IoT képességekkel rendelkező gyártási robotok távolról vezérelhetők és programozhatók. A Rethink robotjai képesek együttműködni és tanulni, precíz gyártási és tesztelési feladatokat ellátni.

8 **Mezőgazdasági eszközök:** A mezőgazdaságban ezek az eszközök képesek távolról adatokat gyűjteni és valós időben továbbítani azokat, például a talajnedvességről, vegyszertartalomról, gátszintekről vagy akár az állatok egészségügyi állapotáról. Ilyen eszközök lehetnek például szivattyúk, traktorok, meteorológiai állomások vagy drónok.

Incidensek

A korábban említett okok miatt, minden ország számára sarkalatos pont, ha egy kritikus infrastruktúráját támadás ér. A legtöbb esetben ransomware, adatlopás vagy olyan malware támadás fenyegeti ezeket a rendszereket, amelyek célja a szolgáltatások ellehetetlenítése.

A Blaster worm nevű vírus egy Windows sérülékenységet használt ki 2003 augusztusában az USA egyes államaiban. A hatása eltérő, néhány órától több hétig tartó áramkimaradást okozott több mint 50 millió ember számára.

Szintén Windows sérülékenységet használt ki 2010-ben Iránban a Stuxnet malware. A támadók az urándúsító centrifugákat vezérlő PLC-ket célozták és a támadás következményeként tönkre is tettek több százat ezekből, szabotálva az urándúsító folyamatokat.

A 2015 decemberében végrehajtott ukrán áramszolgáltatók elleni támadás egy komplex művelet volt, mivel nem csak a SCADA rendszereket tették üzemképtelenné az elkövetők, hanem DDoS támadással elérhetetlenné tették az áramszolgáltatók webszervereit és ügyfélszolgálatait.

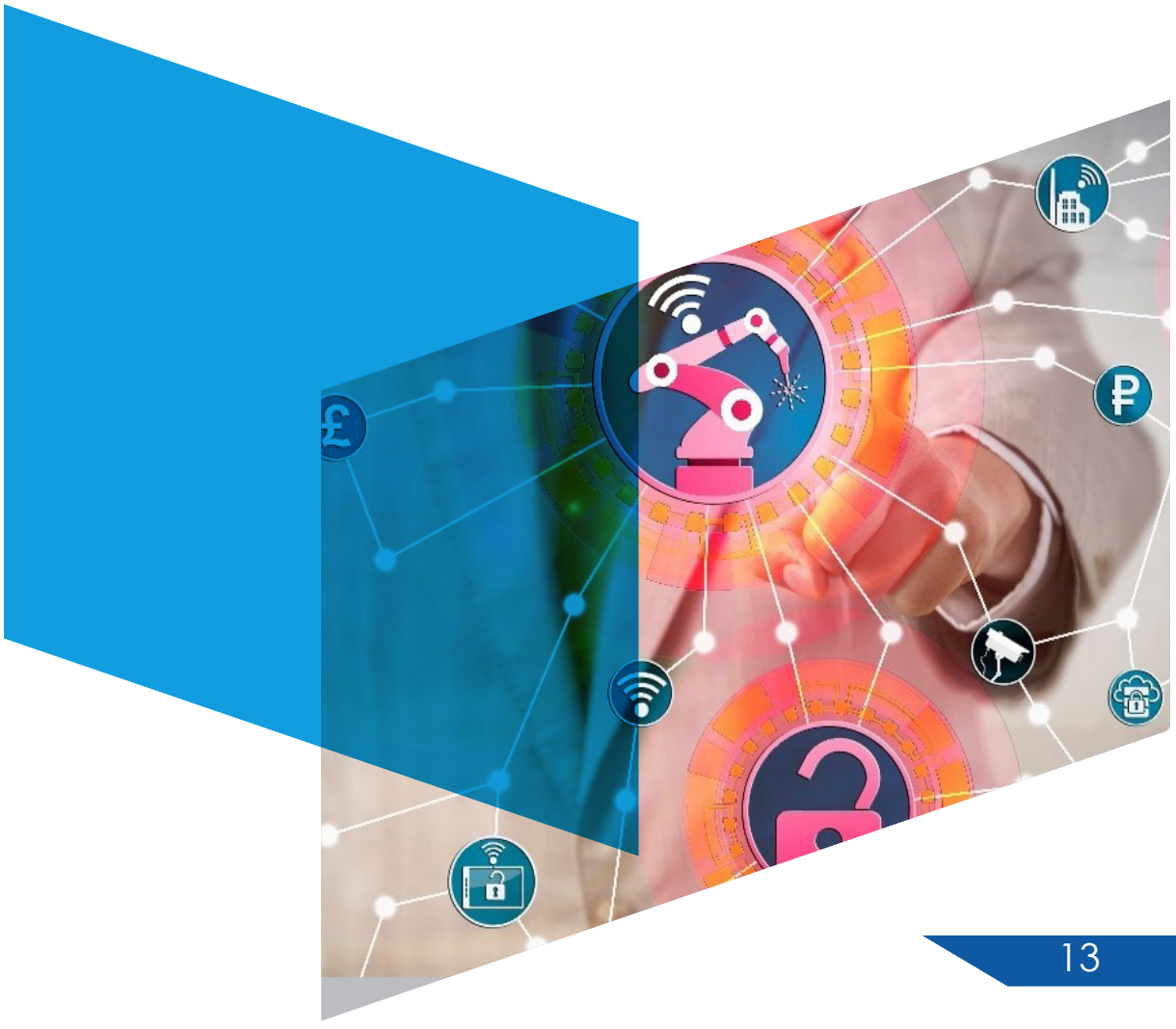
2019-ben a Dél-Afrikai Köztársaságban történt zsarolóvírustámadás következtében sok ezer lakos áram nélkül maradt.

2020-ban, Portugáliában ért egy közmű szolgáltatót zsarolóvírus támadás és adatlopás, amelynek következtében több TB-nyi adatot loptak el és titkosítottak.

További villamosenergia rendszereket ért incidensekről olvashat a SeConSys kézikönyv 1. számú mellékletében.

Összefoglalás

Afelől kétségünk sem lehet, hogy az ipari IoT-k világa feltörekvőben van, egyre több rendszert automatizálnak és olyan munkafolyamatokat látnak el gépek, amelyek sok esetben már emberi beavatkozást sem igényelnek. Ezeket a rendszereket magas fokú alapossággal kell megtervezni, létrehozni és karbantartani, ugyanis akár emberéletek is múlhatnak egy-egy mulasztáson. A szakembereknek összpontosítaniuk kell a termelési folyamat minden szakaszában, különben végzetes incidens történhet. Minden esetben törekedni kell arra, hogy ne következhessen be olyan kibertámadás, amely az anyagi károkozáson túl akár fizikai sérüléseket is képes okozni az ipari IoT világában.



NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022