HADMÉRNÖK

X. Évfolyam 2. szám - 2015. június

GYURÁK Gábor
gabor@gyurak.hu

KRITIKUS INFRASTRUKTÚRÁK VÉDELME HÁLÓZATI BEHATOLÁS JELZŐ RENDSZEREKKEL

Absztrakt

A cikk bemutatja a kritikus infrastruktúrákat, különösen a SCADA rendszereket veszélyeztető, kibertérből érkező fenyegetéseket. Ezen rendszerek védelmére különféle megoldások léteznek, amelyek közül a behatolás jelző (IDS, Intrusion Detection System) és behatolás megelőző (IPS, Intrusion Prevention System) rendszerek kerülnek vizsgálatra. A leggyakrabban alkalmazott IDS rendszerek összehasonlításra kerülnek a hagyományos és ipari informatikai rendszerekben való alkalmazhatóságuk tükrében.

This paper describes how cyber attacks threat critical infrastructures, especially SCADA systems. Security solutions are exists, but the most complex intrusion detection systems (IDS) and intrusion prevention systems(IPS) are examined in this paper. Feasibility of commonly used IDS systems is compared between normal and industrial IT systems.

Kulcsszavak: *kritikus infrastruktúra, kibertámadás, hálózati behatolás jelzés, SCADA rendszerek ~ critical infrastructure, cyber attack, network intrusion detection, SCADA systems*

BEVEZETÉS

A kritikus infrastruktúrák a társadalom és a gazdaság működéséhez nélkülözhetetlen, létfontosságú létesítmények. Ebbe a kategóriába sorolható a vízszolgáltatás, az áramellátás, a telekommunikáció és még számos további terület is. Manapság ezeket az infrastruktúrákat szinte kivétel nélkül hálózatba kötött számítógépes rendszerek működtetik. Ezen rendszerek kibervédelme egyre fontosabb feladat, hiszen világszerte egyre több támadás éri őket a kibertérből. A leghíresebb támadás 2010-ben történt, amikor egy Stuxnet nevű féreg megtámadta a Siemens Simatic WinCC típus SCADA (Supervisory Control And Data Acqisition) rendszert. A támadás Irán nukleáris létesítményei ellen irányult, és úgy vonult be a történelembe, mint az első malware[1], amely komoly károkat okozott egy ipari infrastruktúrában. [8]

Egy adott informatikai rendszerbe történő betörést a szakirodalom behatolásként nevesíti. A behatolás során a támadó kihasználja az adott rendszer sérülékenységeit. Az ilyen eseményeket a lehető legrövidebb időn belül fel kell ismerni, és minimalizálni kell a károkozás lehetőségét. A behatolás jelző rendszerek (IDS, Intrusion Detection System) az informatikai rendszerek riasztóberendezései, amelyek a támadások felderítésére szolgálnak.

Az ipari vezérlő rendszerek (ICS, Industrial Control System) informatikai rendszerei sok mindenben különböznek a hagyományos informatikai rendszerek felépítésétől, ezért ezek vonatkozásában az általános biztonsági megoldások sem alkalmazhatók közvetlenül.

Jelen cikk célja bemutatni a kritikus infrastruktúrák kibertámadások elleni védekezési lehetőségeit a behatolás jelző rendszerek szemszögéből. A hagyományos és ipari informatikai rendszerek tulajdonságainak összehasonlításán keresztül vizsgálatra kerül a legelterjedtebb behatolás jelző rendszerek alkalmazhatósága ezen a területen.

KRITIKUS INFRASTRUKTÚRÁK KIBER- FENYEGETETTSÉGE

Kritikus infrastruktúrák

Modern világunk egy nagyon bonyolult rendszer, amelyet különböző infrastruktúrák alapoznak meg. Az infrastruktúrák „a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. a lakások, a közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere”. [1] Különösen fontos szerepet betöltő infrastruktúrák esetén *létfontosságú infrastruktúrákról*[2] beszélünk. Nem magától értetődő, hogy egy infrastruktúrát mikor tekintünk kritikusnak. Általánosságban azt mondhatjuk, hogy akkor kritikus egy infrastruktúra, ha az jelentős mértékben befolyásolja használóinak életét. Ha abból a szempontból közelítjük meg a kérdést, hogy a rendszer kiesése mekkora problémát okoz, akkor érdemes egy doktori értekezés meghatározását tekinteni, amely az alábbiak szerint definiálja a fogalmat:

„Azon létesítmények, eszközök vagy szolgáltatások, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítmények, eszközök és szolgáltatások, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba vagy a közbiztonságba vetett bizalmat jelentősen csökkentené.” [3]

[1] A malware a malicious software rövidítése, kártékony programot jelent.

[2] Nemzetközi színtéren az angol critical szó alapján leginkább kritikus infrastruktúraként találkozhatunk a fogalommal. A témában járatos szakemberek is ekként említik, de a törvényhozók felismerve a magyar nyelv különleges leíró képességét, a témához kapcsolódó törvény [2] címében is a karakteresebb „létfontosságú” jelzőt használják.

A különböző nemzetek eltérő módon viszonyulnak a kérdéshez. Vannak olyan országok, amelyek egy infrastruktúrát kritikusnak tekintenek, míg más országok ugyanazt az infrastruktúrát nem tekintik annak. Ez a cikk Magyarország szempontjából vizsgálja a kérdést.

Hazánkban kritikus infrastruktúrának tekintjük a teljesség igénye nélkül az alábbiakat:

- energiaellátás,
- infokommunikációs rendszerek,
- közlekedés,
- víz- és élelmiszer ellátás,
- egészségügy,
- pénzügy,
- ipar,
- jogrend és közbiztonság. [4]

A huszadik század közepén indult hihetetlen mértékű technikai fejlődés lehetővé tette, hogy a korábban a mezőgazdaságra, majd az iparra épülő társadalmakat felváltsa egy új alapokra épülő társadalmi rendszer. Az 1970-es években Daniel Bell már posztindusztriális társadalomról beszél, amelyben a foglalkoztatottak egy része már nem vesz részt megfogható javak előállításában. Több tudóssal[3] egyetértésben megállapítja, hogy a társadalom működése alapvető változásoknak néz elébe. Ma már tudjuk, hogy ez a változás lezajlott, és eredményeként létrejött az információs társadalom. Ennek a társadalomnak a sajátossága, hogy az információ-technológia központi szerepet tölt be az élet minden területén. Ezek a technológiák „beszivárogtak" a gazdaságba, az oktatásba, az iparba, de még a művészetekbe is. Természetesen az információs társadalmat működtető infrastruktúrákban és kritikus infrastruktúrákban is kulcsfontosságú szerep jut ezeknek a rendszereknek.

A kritikus infrastruktúrák mellett megjelenik egy új fogalom, a kritikus információs infrastruktúra. A fogalmat ismét kiválóan érzékelteti a korábban említett doktori értekezés:

„Azok az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrák működőképességét jelentősen csökkentené." [3]

A definíció alapján – és a nemzetközi normáknak megfelelően - a kritikus információs infrastruktúrák közé tartoznak az alábbi rendszerek:

- kommunikációs hálózatok,
- energiaellátó rendszerek informatikai rendszerei,
- közlekedési rendszerek informatikai rendszerei,
- víz- és élelmiszerellátó rendszerek informatikai rendszerei,
- egészségügyi rendszerek informatikai rendszerei,
- pénzügyi rendszer informatikai rendszerei,
- egyéb kritikus infrastruktúrák informatikai rendszerei.

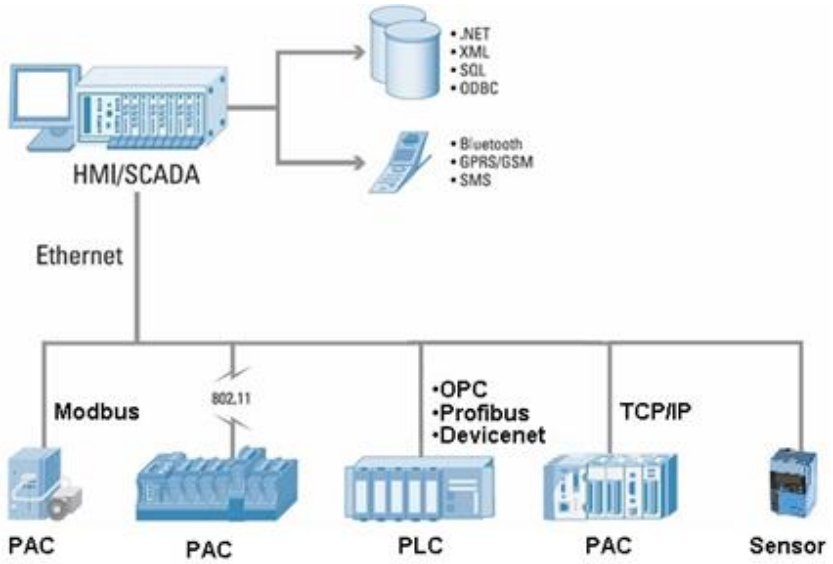
A definícióban szereplő két kategória jól elkülöníthető a felsorolásban is. A kommunikációs hálózatok alapfeladata a kommunikáció biztosítása a szolgáltatást igénybevevő felek között. Ilyenek többek között a mobiltelefon hálózatok, a PSTN[4], az ISDN[5] és az egyre nagyobb szerephez jutó VoIP[6] és egyéb IP alapú kommunikációs technológiák. A másik kategóriában a kritikus infrastruktúrák működéséhez nélkülözhetetlen informatikai rendszerek tartoznak.

[3] Fritz Machlup – tudásipar fogalma (1962), Marc Porat – információs gazdaság elmélete (1977)
[4] Public Switched Telephone Network (Nyilvános kapcsolt telefonhálózat, analóg)
[5] Integrated Services Digital Network (Integrált szolgáltatást nyújtó telefonhálózat, digitális)
[6] Voice over Internet Protocol (Internet Protokoll segítségével megvalósuló telefonszolgáltatás)

Az informatikai rendszer[7] fogalommal nap mint nap találkozunk és tapasztaljuk, hogy mennyire képlékeny meghatározásról van szó. Jelen cikk keretein belül a legtágabb értelemben vett informatikai rendszerekről [5] van szó, amelybe beletartoznak a számítógép hálózatok, a számítógépes rendszerek, az infokommunikációs- és a navigációs-rendszerek. Kitüntetett figyelmet kapnak továbbá a következő fejezetben ismertetésre kerülő ipari vezérlőrendszerek is, amelyek szintén kritikus fontosságú elemei egyes infrastruktúráknak.

Ipari vezérlőrendszer, mint kritikus infrastruktúra építőelem

A kritikus infrastruktúrákban sok helyen találkozunk automatizált fizikai folyamatokkal, amelyeket számítógépes rendszerek irányítanak. Ezeket ipari vezérlő rendszereknek nevezzük (ICS, Industrial Controlled Systems). Az ICS alrendszerekből tevődik össze, amelyek közül mindenképpen említésre méltók a SCADA (Supervisory Control and Data Acquisition) folyamatirányító rendszerek, DCS (Distributed Control Systems) elosztott vezérlőrendszerek és egyéb PLC (Programmable Logical Controller) programozható vezérlő rendszerek.



1. ábra. Nyitott architektúrájú SCADA rendszer[8]

Az ICS rendszerek elleni támadások és a védelmi módszerek megértéséhez ismerni kell a rendszert felépítő komponenseket. A rendszer alapvetően kilenc komponensből épül fel: [10]

- Vezérlő szerver: a DCS és PLC felügyeleti szoftver futtatásáért felelős;
- SCADA szerver: a SCADA rendszer irányítását végzi;
- HMI (Human Machine Interface): az adminisztrációs személyzetnek nyújt kapcsolódási felületet a rendszerhez (vészhelyzet esetén például ezen keresztül felülbírálható az automatikus vezérlés);
- Adatrögzítő: a rendszeren belüli folyamatok információinak rögzítését végzi;
- RTU (Remote Terminal Unit): speciális adatgyűjtő és vezérlő egység távoli SCADA állomások támogatására;
- PLC: villamos vagy villamosan működtetett folyamatok irányítására használt berendezés;
- IED (Intelligent Electronic Devices): intelligens beavatkozó és szenzor egység, amely megvalósítja az adatgyűjtést, kommunikációt és a közvetlen vezérlést;

[7] Az angol Information Technology System rövidítéseként a magyar nyelvben is gyakran használjuk az IT rendszer kifejezést.
[8] Forrás: National Instruments (http://www.ni.com/white-paper/5970/en/, letöltve: 2014.11.14)

- I/O (Input/Output) szerver: az alrendszerek (PLC, RTU, IED) illesztését szolgálja a vezérlő szerverhez;
- Kommunikációs hálózat: tipikusan ipari Ethernet protokollal megvalósított kommunikációs hálózat.

Kibertámadások

Az előző fejezetben bemutatott kritikus infrastruktúra és kritikus információs infrastruktúra elemek védelme különösen fontos feladat. A rendszereket veszélyeztető tényezők között megkülönböztethetünk szándékos és nem szándékos károkozást. Nem szándékos károkozást eredményezhet egy földrengés, de akár egy képzetlen felhasználó tevékenysége is. Szándékos károkat okozhatnak hackerek, hacker csoportok, elbocsátott alkalmazottak, de akár ellenséges államok szervezett kiber-hadseregei is. A cikkben a kritikus információs infrastruktúrák elleni, kibertérből érkező fenyegetésekkel és az azok elleni védekezés lehetőségeivel foglalkozunk.

A kibertér az elektronikus kommunikációs eszközöket és rendszereket magába foglaló világ, amely fontos mozgatórúgója az információs társadalomnak. A kibertér jelentőségét mutatja az is, hogy a hadviselés a hagyományos tereken (szárazföld, víz, levegő, világűr) kívül megjelent a kibertérben is, melynek eredményeként ma már kiberhadviseléről, kiberháborúról, kiberterrorizmusról is beszélhetünk. A „kiber" előtag arra utal, hogy ezek a tevékenységek az információs térben zajlanak. [6]

Az információs társadalomban zajló folyamatokkal párhuzamosan az ICS rendszerek is kombinálva lettek informatikai rendszerekkel, amelynek eredményeként komplex összekapcsolt rendszerek (hálózatok) jöttek létre. Az így létrejött rendszereknek olyan veszélyekkel is szembe kell nézniük, amelyekkel korábban nem kellett foglalkozni. A klasszikus IT és ICS rendszerek összekapcsolása számos előnnyel jár, de az IT rendszerek sérülékenységei közvetett módon támadhatóvá teszik az ICS-t is. A sérülékenységeket kihasználva a támadó betörhet a vezérlő rendszerbe és módosításokkal destabilizálhatja akár az egész kritikus infrastruktúrát, ami katasztrófához is vezethet.

A következő incidensek alátámasztják, hogy valós veszélyről van szó, és a támadások időnként eredményesek:

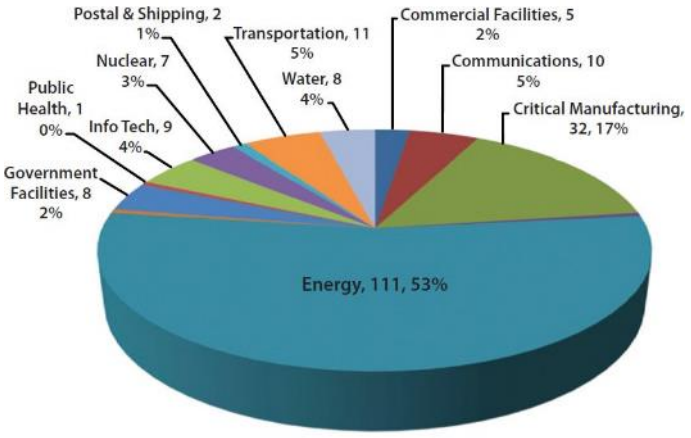
- Atomerőmű elleni támadás, Ohio, Egyesült Államok (2003) [7]: a SLAMMER nevű féreg az egyik alkalmazott telefonján keresztül jutott be az atomerőmű vezérlő rendszerébe, kijátszva a vállalati tűzfalat;
- Szennyvíztisztító elleni támadás, Queensland, Ausztrália (2000) [7]: egy elbocsátott alkalmazott illetéktelenül belépett az irányító rendszerbe és átvette a vezérlést, amellyel több millió liter szennyvizet juttatott egy folyóba;
- A STUXNET féreg nukleáris létesítmények elleni támadása, Irán (2010) [8]: a féreg több atomdúsító centrifugát tett tönkre, amely évekkel visszavezette Irán atomprogramját;
- A FLAME nevű malware közel-keleti olajfinomítók elleni támadása (2012). [9]

A Stuxnet, a Flame és a magyar vonatkozásaiban is méltán híres Duqu[9] malware képességei jól mutatják azt a tendenciát, amely egyre inkább ráirányítja a figyelmet a kritikus infrastruktúrák kibertámadások elleni védelmére.

A kiber-fenyegetések elleni harcban fontos szerepe van a nemzeti és nemzetközi kiberbiztonsági stratégiáknak és azoknak az incidenskezelő szervezeteknek (CERT, Computer Emergeny Response Team), amelyek feladata az ilyen fenyegetések felismerése és reagálása. Speciálisan a kritikus infrastruktúra területén is működnek ilyen szervezetek. Például az

[9] A Duqu egy kártékony program, amelyet a Budapesti Műszaki és Gazdaságtudományi Egyetemen működő Crysys labor munkatársai analizáltak először a világon. (http://www.crysys.hu)

Egyesült Államokban ilyen szervezet az ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), amelynek deklarált célja az USA-ban működő kritikus infrastruktúra üzemeltetők és a kormány közötti együttműködés kialakítása és fenntartása a kibervédelem érdekében. A szervezet továbbá rendszeresen jelentéseket ad ki az incidensekről. Az ICS-CERT rendszeresen készít jelentéseket, amelyekből egy példát mutat be az alábbi ábra.



2. ábra. Az USA kritikus infrastruktúráit ért támadások, 2013. I. félév[10]

HÁLÓZATI BEHATOLÁS JELZŐ RENDSZEREK JELLEMZŐI

A behatolás jelző rendszerek vagy *IDS* (Intrusion Detection System) rendszerek az informatikai biztonság rendszertana [11] szerint a támadás észlelési fázishoz kapcsolódnak. Az IDS rendszereket beavatkozó szervekkel kiegészítve már behatolás megelőző azaz *IPS* (Intrusion Prevention System) rendszerekről beszélhetünk. [13]

Az RFC2828[11] definíciója szerint a behatolás jelző rendszerek olyan biztonsági szolgáltatások, amelyek monitorozzák és analizálják a rendszer eseményeit annak érdekében, hogy valós időben vagy közel valós időben figyelmeztessék a személyzetet az illetéktelen hozzáférésekről. Az IDS rendszerek alapvető működési elve, hogy szenzorok segítségével figyelik az informatikai rendszer paramétereit és gyanús események bekövetkezésekor riasztanak.

A hálózati behatolás jelző rendszerek csoportosítása

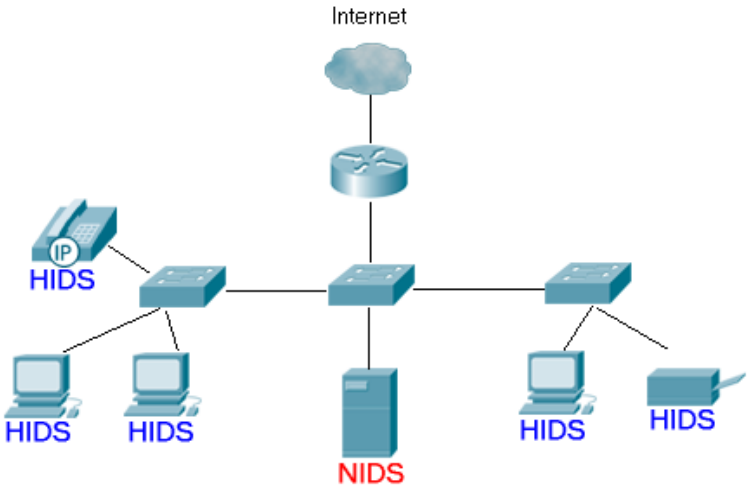
A behatolás jelző rendszerek csoportosíthatók az érzékelés helye szerint és a működési módjuk szerint. [13]

Hely szerinti csoportosítás

Az érzékelés helye szerint lehetnek NIDS (Network Based IDS), azaz hálózat alapú és lehetnek HIDS (Host Based IDS), azaz hoszt alapú behatolás jelző rendszerek.

A NIDS rendszerek szenzorai a hálózati forgalom monitorozásával (pl.: TCP szegmensek fejrész paraméterei, portszámok, IP címek, URL-ek) keresik a gyanús eseményeket, míg a HIDS-ek a hosztokon futó alkalmazások naplói és egyéb rendszer paraméterek (pl.: rendszer folyamatok, CPU használat) alapján következtetnek a támadásokra.

[10] Forrás: ICS-CERT Monitor, April/May/June 2013 (https://ics-cert.us-cert.gov/monitors, letöltve: 2014.11.21)
[11] RFC2828 – Internet Security Glossary (http://www.rfc-base.org/rfc-2828.html)



3. ábra NIDS és HIDS rendszerek (saját készítésű ábra)

Működési mód szerinti csoportosítás

Alapvetően kétféle módon működnek az IDS rendszerek. Az egyik típusba tartoznak az *ujjlenyomat alapú* (signature-based vagy misuse) IDS megoldások. Ezek lényege, hogy egy adatbázisban tárolva vannak a korábbról megismert támadások jellegzetességei és a rendszer ilyen támadásokra utaló jeleket keres. Ennek előnye a gyorsaságában és egyszerűségében rejlik.

A másik típusba tartoznak az *anomália felderítő* (anomaly detection) IDS megoldások, amelyek képesek az ismeretlen támadások felderítésére is. Működési elvüket tekintve először megtanulják a rendszer normális működését, majd a normális működéstől eltérést észlelve hívják fel a figyelmet a lehetséges behatolásra.

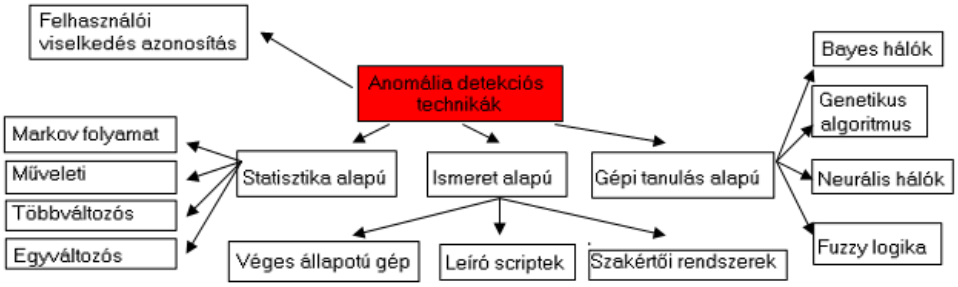
A klasszikus IT rendszerek gyakorlatában szinte kizárólag az ujjlenyomat alapú IDS-eket alkalmazzák, mert az anomália alapú rendszerek jóval bonyolultabbak és erőforrás igényesebbek.

A hálózati behatolás jelző rendszerek hatékonysága

A korábbiakban rávilágítottunk az informatikai rendszerek és szolgáltatások rohamos fejlődésére és láttuk, hogy a támadók eszközrendszere is folyamatosan változik. Egy új támadás esetén (zero-day attack) azok a rendszerek, amelyek csupán az ismert támadások kivédésére vannak felkészítve, csődöt fognak mondani. Ebbe a kategóriába tartoznak a signature-based IDS rendszerek (pl.: SNORT).

A zero-day támadásokkal szemben csak az anomália felderítő képességekkel ellátott rendszerek tudják felvenni a harcot (pl.: POSEIDON). Ezek előnye ugyan egyértelmű, mégis a gyakorlatban alig használják őket a fent említett okok miatt.

Az anomália alapú behatolás detektáló rendszerek megvalósítására, a normális felhasználói viselkedést leíró modell létrehozására, számos technika létezik. Ezek közül a gépi tanulás módszereket foglalja össze az alábbi ábra.



4. ábra. Anomália detektációs technikák

A gépi tanulás alapú megvalósítás népszerű kutatási terület és a témában számos publikáció került napvilágra, amelyek többsége 98%-os detektációs arányról és alig 1%-os hibás riasztásról számolt be. [14] A gépi tanulás alapú rendszerek implementálása számos nehézséget jelent, és ezzel magyarázható az, hogy noha a gépi tanulás számos területeken hatékonyan alkalmazható, a behatolás detektálás jellegzetességei miatt nem hozta eddig a várt sikert. Míg egyes publikációk gépi tanuláson alapuló IDS-ek elterjedését prognosztizálják, addig mások [12] ezen rendszerek árnyoldalaira és problémáira hívják fel a figyelmet. Többek között problémát okoz a tanulási fázis, ugyanis nincsenek megfelelő adatok a tanításhoz. A rendelkezésre álló adatsorok régiek, elavultak és nem tükrözik egy valóságos rendszer működését.

KRITIKUS INFRASTRUKTÚRÁK VÉDELME

IDS megoldások

Az informatikai rendszerek védelmére leggyakrabban a Snort[12], a Bro[13], a Suricata[14], Cisco[15], a Prelude[16] és az Ossec[17] IDS megoldások valamelyikét alkalmazzák, de tudatosítani kell, hogy ezek hagyományos IT infrastruktúrák védelmére lettek kifejlesztve. Ez azt jelenti, hogy nem nyújtanak vagy csak nagyon korlátozott módon nyújtanak támogatást olyan rendszerek, protokollok felügyeletére, amelyek egy ipari környezetben megtalálhatók. Szinte minden megoldás alapértelmezésben támogatja az olyan széles körben használt protokollok vizsgálatát, mint a TCP (Transmission Control Protocol), a DNS (Domain Name System) vagy a HTTP (HyperText Transfer Protocol), de az elektromos hálózatok tipikus SCADA protokollját, a DNP3-t (Distributed Network Protocol) csak a Bro támogatja. A témában született kutatások áttanulmányozása után kijelenthetjük, hogy léteznek olyan fejlesztések, amelyek az ICS rendszerek behatolás detektálására fókuszálnak, azonban ezek nagyon korlátozott képességekkel rendelkeznek, és szinte kivétel nélkül egyetlen hoszt védelmére összpontosítanak.

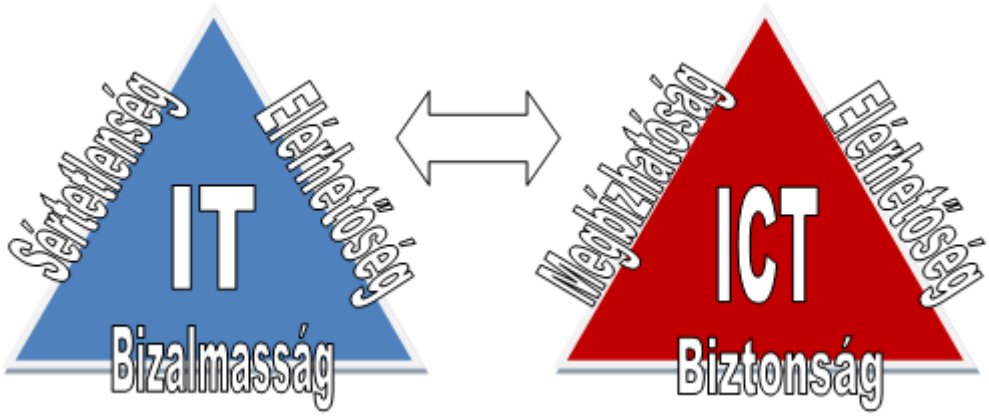
ICS és hagyományos IT rendszerek összehasonlítása

Az ipari vezérlő rendszerek és a hagyományos informatikai rendszerek között a cikk témájához igazodva az alábbi szempontok szerint érdemes a különbségeket vizsgálni:

- *Elérhetőség:* Hagyományos esetben megengedhető némi kiesés, de ICS esetében folyamatos elérhetőséget kell biztosítani.
- *Időzítés:* Ipari rendszerek esetében nem megengedett a késleltetés, ezzel szemben hagyományos esetben ez nem okoz különösebb problémát.
- *Komponensek élettartama:* Mindenki számára ismert tény, hogy a hagyományos informatikai rendszerek hardver és szoftver komponensei elavulnak, ezért azokat néhány évente le kell cserélni. Ipari rendszerek esetében ennél sokkal hosszabb, több évtizedes távlatban kell gondolkozni.
- *Javítások (patch menedzsment):* IT rendszerek esetében gyakran kell foltozni (patchelni), a másik esetben lényegesen ritkábban.
- *Támogatás:* ICS esetben általában homogén rendszerekkel van dolgunk, míg a hagyományos IT rendszerek nem egységes felépítésűek, többféle gyártótól származó hardver és szoftver elemekből épülnek fel.

[12] www.snort.org
[13] www.bro.org
[14] www.suricata-ids.org
[15] www.cisco.com
[16] www.prelude-ids.org
[17] www.ossec.net

A két rendszert a fenti szempontok alapján összehasonlítva alapvető különbséget látunk közöttük. Ezek önmagukban is nagyon fontosak, de van még egy lényeges különbség. A biztonsági stratégiát illetően a hagyományos IT rendszerek az úgynevezett CIA szempontokat tekintik elsődlegesnek. Ez azt jelenti, hogy a legfontosabb cél az adatok bizalmasságának (**C**onfidentiality), sértetlenségének (**I**ntegrity) és elérhetőségének (**A**vailability) biztosítása. Ezzel szemben az ipari rendszerekben az SRA elvnek kell érvényesülni, amely a biztonság (**S**afety), megbízhatóság (**R**eliability) és elérhetőség (**A**vailability) hármast tartja szem előtt.



5. ábra. CIA és SRA modellek

A néhány évtizeddel korábban üzembe helyezett, és még ma is működő ICS rendszerek tervezésekor kizárólag az SRA elvekre alapoztak, hiszen akkoriban szó sem volt kiber-fenyegetésekről. Ma már tudjuk, hogy erre is fel kell készülni, és a hatékony védelem érdekében az ICS rendszerekbe is be kell építeni az informatikai rendszerek riasztóberendezéseit, az IDS rendszereket.

Az általánosan használt IDS alkalmazások önmagukban nem alkalmasak az ICS rendszerek védelmére, mert nem tudják vizsgálni a SCADA specifikus protokollokat. Utóbbihoz speciális szaktudás beépítésére van szükség, amely az informatikában és az ipari vezérlőrendszerekben járatos szakemberek együttműködését kívánja meg.

Új kihívások a hálózati behatolás jelzésben

A fejezet célja felfedni azokat a specialitásokat, amelyekre az ICS rendszerben felhasznált behatolás jelzőket fel kell készíteni. A vizsgálat során a különböző típusú IDS-ek szemszögéből tekintjük át a teendőket.

Ujjlenyomat-alapú rendszerek kérdései

Első megközelítésben az ujjlenyomat alapú rendszerek hatékonyságának kulcskérdése a támadások mintázatait tartalmazó adatbázis naprakész állapotban tartása. Ehhez szükség lenne egy olyan megbízható szervezetre, amely biztosítja ezeket az információkat. Sajnos ilyen szervezet még nem létezik, és komoly előkészítő munkának kell megelőznie a létrehozását, mivel a kritikus infrastruktúrák kiber-védelmének hatékonysága lenne a cél. Voltak már próbálkozások egy vízellátó SCADA rendszerének védelmére ujjlenyomat alapú IDS rendszerrel, de ez a klasszikus mintaillesztési megoldást használta. [15] Fontos hangsúlyozni, hogy ez a védelmi rendszer csak az ismert támadásokkal szemben jelent védelmet, az ismeretlen támadások kivédésére nem alkalmas.

A SCADA rendszerek protokolljai – a klasszikus TCP/IP modell protokolljaihoz hasonlóan – jól leírhatók formális modellekkel. Javaslatom szerint a klasszikus IDS rendszereket kiegészítve ezen modellekkel elérhető lenne, hogy az ujjlenyomat alapú mintaillesztő rendszer a támadási mintázatok helyett a modellnek megfelelő viselkedési mintákat keresse a rendszer működésében, és akkor riasszon, ha nem találja meg a modell által elvárt mintát.

Anomália-alapú rendszerek kérdései

A megoldás lényege, hogy az IDS egy tanulási fázis során megtanulja a rendszer normál működését és ezt követően jelezzen, ha a normálistól eltérő működést észlel. A módszer elvben alkalmas az ismeretlen támadások felderítésére is, de a rendszer óriási hibája a tanítás nehézségében rejlik. Mivel minden rendszer más, ezért a tanítást minden rendszeren egyedileg kell(ene) elvégezni. Problémát jelent az, hogy a tanítási fázis alatt nem lehetünk biztosak abban, hogy valóban normál működés közben monitorozzuk a rendszert és nem vagyunk éppen támadás alatt. Problémát jelent az is, hogy a rendszer teszteléséhez szükséges adatsorok nem állnak rendelkezésére a kutatóknak. A témához kapcsolódó kutatásokban [16] leggyakrabban alkalmazott adatsor a KDD'99[18], amely nem ICT specifikus adatokat tartalmaz, és mára már elavultnak tekinthető.

Szükség lenne olyan adatsorokra, amelyek a kutatásokban felhasználhatóak lennének a rendszerek teszteléséhez és a teljesítmények méréséhez. Valószínűleg az érzékeny adatok miatt önként egyik ICS üzemeltető sem fogja közzétenni ilyen jellegű méréseit, de mindenképpen érdemes lenne nemzetközi szinten is lépéseket tenni az ügy érdekében

ÖSSZEGZÉS

A cikk áttekintette a kritikus infrastruktúrák jelentőségét és azok kiber-fenyegetettségét. Megállapítottuk, hogy a kritikus infrastruktúrákban található ipari vezérlő rendszerek egyre nagyobb mértékben össze vannak kapcsolva hagyományos informatikai rendszerekkel, hálózatokkal, amelyek miatt új kihívásokkal kell szembenézni a rendszerek védelmének megszervezésekor. Az egyre kifinomultabb támadási módszerek szükségessé teszik hálózati behatolás jelző rendszerek telepítését az ipari rendszerekbe is. Kézenfekvő lenne a hagyományos IT rendszerekben alkalmazott klasszikus IDS megoldások használata. Az ICS és hagyományos IT rendszerek összehasonlításával bemutatásra kerültek azok a különbségek, amelyek a közvetlen alkalmazást nem teszik lehetővé. Bemutatásra kerültek továbbá olyan problémák is, amelyek egyelőre hátráltatják a területen végzett kutatásokat.

Felhasznált irodalom

[1] Magyar értelmező kéziszótár, Akadémiai kiadó, Budapest, 2006

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[3] Muha Lajos – A Magyar Köztársaság információs infrastruktúráinak védelme, Doktori értekezés, ZMNE, Budapest, 2007

[4] Haig Zsolt, Kovács László – Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Nemzeti Közszolgálati Egyetem, Budapest, 2012

[5] Munk Sándor – Információbiztonság vs. informatikai biztonság, Hadmérnök, Robothadviselés 7. konferencia különszám, Budapest, 2007

[6] Haig Zsolt, Kovács László, Ványa László, Vass Sándor – Elektronikai hadviselés, Nemzeti Közszolgálati Egyetem, Budapest, 2014

[7] A. Nicholson, S. Webber – SCADA security in the light of cyber-warfare, Computers&Security, vol. 31, 2012.

[18] http://kdd.ics.uci.edu

[8] Kovács László, Sipos Mariann – A Stuxnet és ami mögötte van, Hadmérnök, VII. évfolyam 1. szám, 2011

[9] K. Munro – Deconstructing flame: The limitations of traditional defense, Computer Fraud & Security, vol. 2012, 2012

[10] K. Stouffer, J. Falco, K. Kent – Guide to supervisory control and data acquisition (SCADA) and industrial control systems security, NIST ajánlás, 2011

[11] Muha Lajos - Az informatikai biztonság egy lehetséges rendszertana: Az információbiztonság egy lehetséges taxonómiája. Bolyai Szemle XVII: (4), 2008

[12] Robin Sommer, Vern Paxson - Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010

[13] William Stallings, Lawrie Brown – Computer Security Principles and Practice, Pearson, 2012

[14] Zhenwei Yu, Jeffery J.P. Tsai – Intrusion Detection A Machine Learning Approach, Imperial College Press, USA, 2011

[15] K. Xiao, N. Chen, S. Ren – A workflow-based non-intrusive approach for enhancing the survivability of critical infrastructures in cyber environment, SEES, 2007

[16] H. Tsang, S. Kwong – Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction, IEEE ICIT, 2005