Egyenirányító az adatoknak

Nagy Péter – *EASTRON Kft.*

Az informatikai rendszerek biztonságát fenyegető támadások sokáig elkerülték az ipari rendszereket. A gyakorlat azonban megmutatta, hogy a PC-ktől jelentősen eltérő felépítés sem véd meg az ilyen támadások ellen – ráadásul az ipari rendszerek elleni kibertámadások sokszor létfontosságú infrastruktúrák vagy „veszélyes üzemek" biztonságát fenyegetik. Az ipari irányítástechnika üzemeltetői tehát nem kerülhetik meg többé az informatika biztonsági kérdéseit. A szerzőnek az idei DCS-konferencián elhangzott előadását összefoglaló cikk az adatvédelem egy lehetséges eszközét, az adatdiódát mutatja be.

A 2012. év jelentős előrelépést hozott a kritikus infrastruktúrák kibertámadás elleni védelmében. Sok, nálunk talán intenzívebben fenyegetett ország rendelkezik már fejlett védekező mechanizmusokkal, és intézményrendszerrel létrehozták a maguk Department of Homeland Security-jét, Bundesamt für Sicherheit in der Informationstechnik-jét vagy Cyber Security and Information Assurance hivatalát.

A probléma felismerésére Magyarországon egy új törvény megjelenése utal „a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről". A törvényről annyit mindenképpen érdemes tudni, hogy definiálja a kritikus infrastruktúrákat és a szervezetek feladatait, és helyszíni ellenőrzést lefolytató szerv kijelölésére is felhatalmazza a kormányt.

A biztonságos társadalom megteremtésének egyik pillére a kijelölt létfontosságú ágazatok és alágazatok kiberbiztonsága. A fenyegetések sokrétűek, és amint azt 2009, az iráni urándúsító telep berendezései elleni Stuxnet-támadás éve óta megtanultuk, igen összetettek is lehetnek. Támadási felületet jelenthetnek a kezelői vagy szállítói hibák, az elégedetlen alkalmazottak, de adott esetben idegen kormányok vagy terroristák és hackerek is. Jelentős tudással, adatokkal rendelkező cégeknek – ezek nem feltétlenül mindig nagyvállalatok – esetenként az ipari kémkedéssel is számolniuk kell. A kockázat és sérülékenység csökkentésnek sok módja van, a védelmi intézkedéseknek a létesítményhez és annak informatikai rendszereihez kell illeszkedni. Ennek kialakítása a vállalatvezetés és a kijelölt biztonsági és műszaki szakemberek közös feladata.

A fontos létesítményekkel kapcsolatban mindenképpen fejlett és tartós fenyegetéssel kell számolni olyannyira, hogy ennek a támadásfajtának már saját elnevezése is megszületett: Advanced Persistent Threat (APT – fejlett, tartós fenyegetettség). Ennek mintapéldája a kifejezetten ipari létesítmények (elsőként az iráni urániumdúsító telep) vezérlőrendszereinek sebezhetőségeit kihasználó Stuxnet féregprogram, vagy a Budapesti Műszaki Egyetemen működő CrySyS Adat- és Rendszerbiztonsági Laboratóruma által felderített és analizált Duqu kártevő. A fenyegetettség fejlettségére jellemző, hogy a támadók számos eszközt használnak fel céljuk eléréséhez. Rendelkeznek az ehhez szükséges, jelentős erőforrásokkal, amelyek révén nulladik napi sebezhetőségek[1] kihasználására alkalmas kódokat tudnak készíteni, vagy egyszerűen vásárolják az ilyen programokat. Céljuk, hogy elkerüljék, illetve áttörjék a kiszemelt rendszert elhatároló védelmeket. A NIST (National Institute of Standards and Technology) szakemberei így fogalmaztak: „a támadók alkalmazkodnak a védők erőfeszítéseihez annak érdekében, hogy azokkal szembeszállhassanak".

A támadások tartósak és kitartóak is. A támadók jól meghatározott céllal tevékenykednek, és többnyire már alaposan felkészülve lépnek akcióba. Gondoskodnak a fenntartható hozzáférésről. Persze már nem „ajtóstól" rohanják le a támadás célpontját, kezdetben nem is vetnek be egyszerű portszkenneléseket, SQL-injekcós támadásokat vagy más automatizált károkozásra alkalmas eszközöket, csak gyűjtik az adatokat.

A mai komplex akciók komoly fenyegetést jelenthetnek az informatikai rendszerekre és az adatokra. Ennek megfelelően a védekezés sem kivitelezhető hatékonyan csupán hagyományos biztonsági eszközök bevetésével. Ezen feltételek mellett felvetődik a szegmentálás igénye. A vállalati termelési, automatizálási rendszerek esetén ez már szinte előírás (amint az ANSI/ISA–99.02.01–2009 kvázi szabványban is megjelenik).

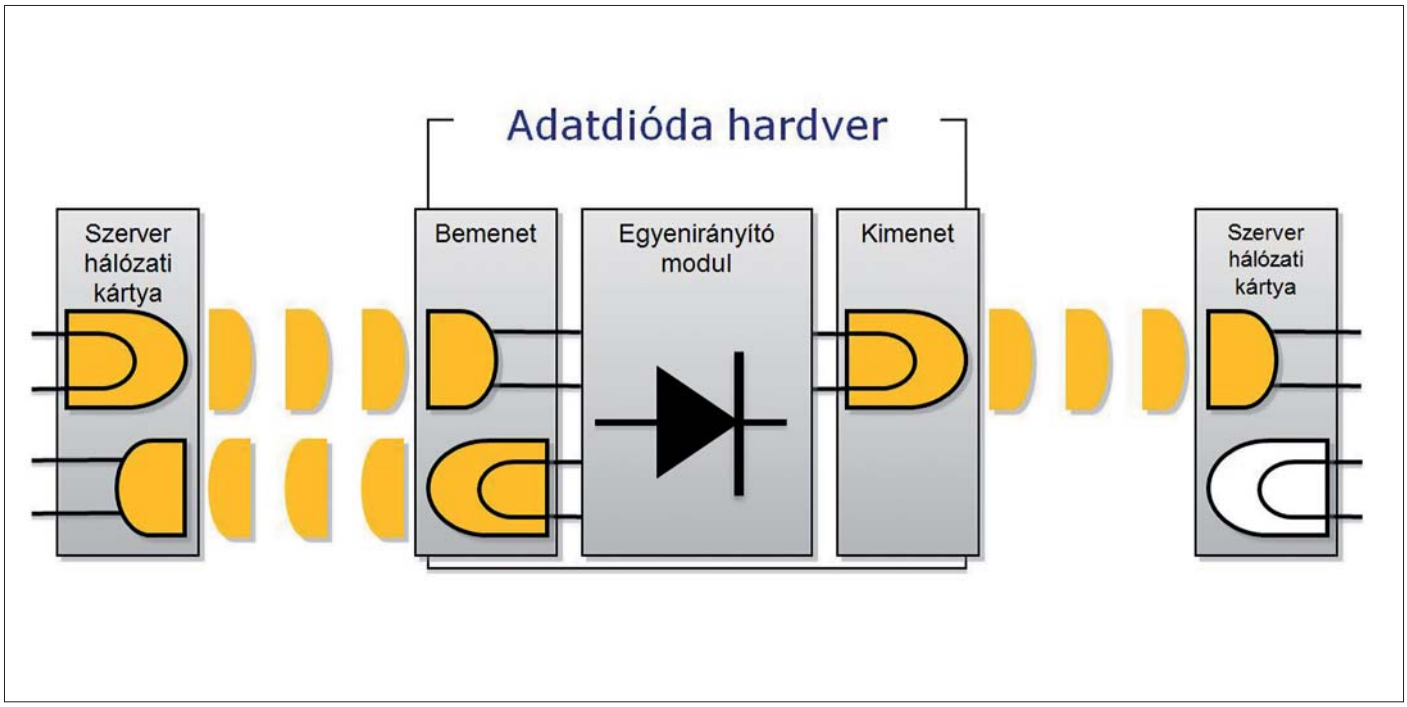
A belső, fokozottan érzékeny (core) és a külső „irodai" rendszerek teljes szétválasztása, az ún. air gap (légrés, kézi adattovábbítás a rendszer egymással elektronikusan össze nem kapcsolt részei között). Természetesen az air gap-nek – az esetenként még viselhető késedelmen túl is – vannak hátulütői: mivel a tévedés lehetőségét is magában hordozó, fizikailag is könnyen támadható és korrumpálható emberi beavatkozást tételez fel.

Az adatdióda

Az elektronikus biztonsági zóna létrehozására – a természetesen megfelelő fizikai védelem alatt álló – adatdióda adhat ellenőrzött és tervezhető megoldást. Ez nem mai találmány. A Manhattan-projekttel együtt indult Sandia National Laboratories már 10 évvel ezelőtt az egyirányú hálózati kapcsolatról cikkezett.

Hogyan működik az adatdióda? A szétválasztandó hálózati területek között egyirányú adatkapcsolatot valósít meg, innen a dióda elnevezés. A kapcsolat egyirányúságát fizikai elven, egy ellenirányú adatátvitelre technikailag eleve alkalmatlan adatátviteli szakasz beiktatásával biztosítja. Ezt kezdetben még soros vonallal oldották meg, de napjainkban már akár 1 Gbit/s-os sebességgel, optikai összeköttetéssel is megvalósítható. A visszahatásmentességről az optikai adó és vevő gondoskodik, mivel a jelek ezen az egyszeres összeköttetésen csak egy irányban képesek áthaladni. A fejlett adatdióda-megoldások Common Criteria

1 Nulladik napi támadás (zero day attack) olyan sebezhetőséget vesz célba, amelyet még nem publikáltak. A hibáról esetleg még a támadás célpontjául szolgáló szoftver fejlesztője sem tud, és ezért a sebezhetőséget megszüntető javítóprogram sem áll még rendelkezésre – *A szerk. megj.*



1.ábra Az adatdióda vázlatos felépítése

EAL 7+ minősítésűek, és megfelelnek a NERC CIP-követelményeknek. Ezek a ma elérhető legmagasabb biztonsági színvonalat képviselik. A rendkívül erőforrás-igényes fejlesztési és tanúsítási folyamat miatt csak néhány gyártó rendelkezik ilyen minősítéssel.

Az adatdióda (1. ábra) működési elvéből következik, hogy csak bizonyos típusú alkalmazások kiszolgálására alkalmas. Az adatintegritást és a flow control-t (adatfolyam vezérlést) a diódához tervezett előtét, gyakran proxinak nevezett szerverpár hozza létre.

2.ábra Ilyen egy adatdióda

Az adatdióda tipikus alkalmazási területe az előre kiválasztott információk megosztása lehet. Például alkalmas fájlátvitelre (FTP- vagy CIFS – SMB-alapon), elektronikus levelek továbbítására az elhatárolt területről, video- vagy audiojelek továbbítására, de akár távoli nyomtatásra, adatbázisok replikálására vagy weblapok tükrözésére is. Az adatdióda felhasználásának speciális területe a kiválasztott, például a vállalatirányítási vagy karbantartási rendszerek működéséhez szükséges folyamatirányítási adatok átvitele.

A vállalati döntéshozók az üzemkészség magas szintjére törekedve könnyen kerülnek az Epimenidész-paradoxon által leírt csapdahelyzetbe (a *krétai* Epimenidész kijelentette, hogy *minden krétai* hazudik). Ennek egy „korszerű” változata, amikor az üzemeltetőnek a hatékony hibaelhárításhoz aktuális információval kell ellátnia a javítással megbízott szervezetet, amely ma már sok esetben központosított, a gazdaságosság miatt „kiszervezett” részleg, vagy a rendszerszállító által fenntartott szervizszolgáltató. Emiatt a karbantartók, javítók infrastruktúrája szétválik az üzemi rendszertől. Ha az üzemeltető nem ad online adatokat, leromlik a rendelkezésre állás, nem érhető el a kívánt szerződéses szolgáltatási szint (SLA - Service Level Agreement). Ha viszont összeköti az üzem hálózati rendszerét a szervizszolgáltatóéval, támadási felületet ad, és ezzel okoz kárt.

Ez a látszólagos ellentmondás az adatdiódák alkalmazásával feloldható. Ez az egyszerű fizikai eszköz (2. ábra) a zárt hálózatot igénylő, magas biztonsági fokozatú rendszerek létrehozását támogatja. Az adatdióda-megoldások megtervezése szoros és hatékony együttműködést igényel a vállalat műszaki és informatikai területei között. A létrehozott új szolgáltatások költsége a gyors adattovábbítással, kockázatmentesen kedvezőbb lehet, mint egy DMZ[2]-vel együttes tűzfal rendszeré.

EASTRON Kft.
1134 Budapest, Váci út 49.
Tel.: +36 1 467 2030, +36 1 222 5528
Fax: +36 1 467 2035
E-mail: eastinfo@eastron.hu
www.eastron.hu

2 DMZ: DeMilitarized Zone (a.m. fegyvermentes övezet). Adatbizonsági értelemben egyfajta biztonsági „határhálózat” megnevezésére használják. Az internet és a biztonságos belső hálózat között csak ezen keresztül történhet kommunikáció, amely mind az internettel, mind a biztonságos helyi hálózattal tűzfalon keresztül kerülhet kapcsolatba.