KARDOS TAMÁS ZSOLT

A jövőálló Egységes Digitális Rádió-távközlő Rendszer (EDR) információbiztonsági kérdései

Information security issues for a future-proof EDR system

DOI: HTTPS://DOI.ORG/10.53793/RV.2022.1.4

Absztrakt

Kutatásom célja bemutatni, hogy a jövőálló EDR rendszer (Egységes Digitális Rádió-távközlő Rendszer) milyen biztonsági kihívásokkal kell, hogy szembenézzen a jelen és a jövőbeli információbiztonsági környezet, a használandó 5G technológia használata, valamint a piaci alapú mobilszolgáltatók esetleges bevonása miatt.

KULCSSZAVAK: EGYSÉGES DIGITÁLIS RÁDIÓ-TÁVKÖZLŐ RENDSZER (EDR), INFORMÁCIÓ BIZTONSÁG, KIBERBIZTONSÁG

Abstract

The aim of my research is to show what security challenges the future EDR (Unified Digital Radiocommunication System) will face due to the current and future information security environment, the 5G technology to be used, and the possible involvement of public mobile operators.

KEYWORDS: UNIFIED DIGITAL RADIO COMMUNICATIONS SYSTEM (EDR), INFORMATION SECURITY, CYBERSECURITY

Bevezetés

Az információs társadalom és a kritikus infrastruktúrákat veszélyeztető fenyegetések egyre nagyobb kihívások elé állítják a közrendvédelmi és katasztrófavédelmi, azaz a készenléti szolgálatokat. Ahhoz, hogy ezek a szervezetek minél hatékonyabban láthassák el feladatukat, szükséges, hogy az infokommunikációs hálózatuk is megfeleljen a mai kor magas követelményeinek.

Az EDR hálózat által jelenleg nyújtott hangalapú kommunikáción túl szükség lesz a készenléti szolgálatok feladatainak ellátásához az EDR hálózat korlátozott adatátviteli képességégének növelésére, ehhez a szélessávú EDR rendszer megtervezésére és kivitelezésére. Korábbi cikkemben, a Rendvédelem folyóirat 2021/3-es lapszámban (Kardos 2021) bemutattam az EDR rendszer továbbfejlesztési lehetőségeit, mely alapvetően az 5G technológia használatán alapul. Jelen cikkemben az 5G technológián alapuló, jövőálló EDR rendszer információbiztonsági kérdéseit tekintem át. Az információbiztonsági aspektusokat külön vizsgálom a jelenleg üzemelő EDR rendszer, valamint a bevezetni kívánt EDR 2.0/3.0 összehasonlításán keresztül, ezen rendszerek nagymértékű koncepcionális eltérése okán. Ebben a cikkben leggyakrabban az információbiztonság szót használom, mellyel nagymértékben megegyezik a kiberbiztonság fogalma, melyet szintén használni fogok.

A jelen kor információbiztonsági kihívásai és megfontolásai

Nagy változások történtek az információbiztonság, a komputerbiztonság kapcsán az elmúlt években. Míg korábban a biztonság nem, csupán a megbízhatóság volt alapvető cél, ma már elengedhetetlen egy rendszer teljes életciklusán keresztül, a tervezéstől a beszerzésen át, és az üzemeltetés során is alapvetően alárendelni folyamatainkat a biztonságnak. Ebből adódóan a jövőálló EDR rendszer kialakításakor is szükséges az alábbi, a teljes hálózati biztonságot lefedő megfontolásokat is figyelembe venni:

1. Átfogó és kockázatalapú biztonsági intézkedések;
2. Szakadatlan folyamatnak tekinthető, mely magában foglalja:
   a) Beszállítók kiválasztását – hálózati elemek előállítását – hálózatok üzemeltetését (a teljes élettartam alatt);
   b) Nem technikai tényezők figyelembevételét – a beszállító kockázati profiljának kialakításakor;
   c) Nemzetbiztonsági szempontok figyelembevételét;

d) Beszállítói lánc és beszállítótól való függés minimalizálását;
e) Életcikluson átívelő biztonsági megfontolások figyelembevételét a szabványosítás, fejlesztés, bevezetés és üzemeltetés során.

Az EDR rendszert üzemeltető Pro-M Zrt. tervei szerint (Pro-M Zrt. középtávú fejlesztési stratégia 2019) a szélessávú készenléti rendszer az alábbi két fázisban valósul meg:

1. EDR 2.0 – Szélessávú adatszolgáltatás a TETRA hang mellett
2. EDR 3.0 – Hang és adatszolgáltatás 3GPP szabványos szélessávú hálózaton (4G/5G).

2025-ig cél a megfelelő önálló, dedikált 4G/5G rádiós hálózat (RAN) kiépítése, a TETRA rádiós hálózat integrációja és a forgalom átterhelése elsődlegesen a dedikált rádiós hálózatra, a publikus rádiós hálózat igénybevétel fenntartása ad-hoc igények kielégítésére.

A jelenlegi EDR rendszer és a jövőbeli EDR 2.0/EDR 3.0 rendszer rövid összehasonlítása

Mik az eltérések?

A jelenlegi EDR rendszert és a jövőbeli EDR 2.0/EDR 3.0 rendszert összehasonlítva az egyik fő eltérés a használat módja, a másik az információk köre és élettartama, a harmadik a technológia kommerciális volta, a negyedik az üzemeltetés kérdése. Ezeket fejtem ki részletesen a következőkben.

A legfontosabb megérteni, hogy az eddigi zárt, speciális hardware és software elemeket felváltja – többek között a költséghatékonyság miatt – a piaci, nyílt, „bárki által elérhető" HW és SW (a rövidítések értelmezése az 1. táblázatban). Ez alapvető hozzáállásbeli változtatást igényel a teljes életcikluson át (tervezés, beszerzés, kivitelezés és üzemeltetés) során. Ez összecseng az információbiztonság holisztikus szemléletével, mely az utóbbi években nyert teret.

Mire fogjuk használni az új generációs szélessávú EDR rendszert?

A hangalapú információtovábbítás mellett megjelenik, és alapvető lesz a képi információ és adatátvitel is. Nagy a változás, mert eddig a hang alapú információ érvényessége lényegesen korlátozottabb volt: egy kiadott parancs akkor, a kiadás pillanatában fontos információ, évekkel később a bizonyító erőn kívül kevésbé hordoz védendő információt. A jelentős mennyiségű adattovábbítás nagy változást okoz. Az EDR rendszer felhasználói vélhetően jelentős mennyiségű védendő, szenzitív, akár személyes, különleges adatot is forgalmazni fognak. Ha ehhez hozzávesszük, hogy a rögzítést/belehallgatást/hozzáférést biztosítani szükséges, a probléma még nagyobb. Ráadásul, ha a hálózat bizonyos elemeit publikus mobilszolgáltatók birtokolják, vagy akár csak üzemeltetik, látható, hogy a problémák hatványozódnak.

Hogy és milyen elemekből épül fel az új generációs szélessávú EDR rendszer?

Fontos kihangsúlyozni, hogy az országos lefedés költséghatékony biztosíthatósága miatt a hálózat legtöbb eleme nem speciális, csak bizonyos rendvédelmi szervek által elérhető berendezés lesz. Az azokat működtető SW-k jelentős része sem lesz speciális, hanem vélhetően kommerciális. A végpontok, hálózati elemek száma is jelentősen emelkedni fog, így a védendő elemek száma is nőni fog, melyek egy részét publikus mobil operátor birtokol, és akár egy harmadik fél üzemeltet és tart karban. Mivel az EDR rendszer rendelkezésre állása is kiemelt fontosságú, ezért ez külön megfontolást és intézkedéseket igényel, ha más külső fél rendszere is kritikus jelentőségű a rendszer működése szempontjából.

Az alábbi táblázatban röviden összehasonlítom a jelenlegi és a jövőbeli EDR rendszereket (1. táblázat).

Összehasonlítás	**EDR 1.0 – TETRA saját és speciális rendszer**	**EDR 2.0 (EDR 3.0) - 4G/5G (3GPP) saját + szolgáltatói rendszer + speciális rendszerelemek**
Adatfolyam	csak hang gyakorlatilag	minden adat (hang és adat)
Adat érvényessége	„hang elszáll”	„adat megmarad”
Adatok köre	hang alapvetően	hang/adat/lokáció/viselkedés/különleges adatok akár központi állami adattárházakból származó személyes adatok, az egészségügyi és bűnügyi rendszerekből különleges személyes adatok
Adat kódolás	speciális	piaci termék/speciális?
Adatok tárolása	saját adatbázis/saját felhő	csak kormányzati felhőben, minden adatot az országon belül, megbízhatóan védett környezetben kell tárolni
HW (végpont) -terminál	speciális	piaci termék
HW (hálózat) -átvitel + rádióállomás	speciális	piaci termék akár
HW (központi)	speciális	piaci termék akár
HW tulajdonos	saját	saját/szolgáltatói (RAN/Core)
HW infrastruktúra védelme	saját	saját/szolgáltatói (RAN/Core) + rengeteg RAN végpont (nagy intelligencia!)
HW infrastruktúra mérete	350 bázisállomás + 4 központ	akár többezer site (szolgáltatói), átviteli pontok stb., adatközpontok és adathálózat miatt lényegesen nagyobb
SW	speciális	piaci termék (javarészt)
SW frissítés	speciális -ritka	speciális/piaci – folyamatos
SW/HW ellátási lánc	speciális	speciális/piaci
SW/HW fejlesztés	lassú	folyamatos
SW/HW szállítók száma	néhány	számos
Szabványosítás	lezárult	folyamatban lévő
Biztonságra törekvés	folyamatos	folyamatos – része a tervezett életciklusnak
Támadók köre	limitált	akár az egész világ?
Felügyelet – Reagálás/megelőzés	alapvetően O&M – NOC + SOC reagálás	O&M – NOC és SOC + EWS + CERT-ek felügyelet + reagálás + megelőzés + supply chain + folyamatos tesztelés
Rendelkezésre állás	saját hatáskör, magas	részben piaci alapon
Üzemeltetési biztonság	saját hatáskör, magas	részben piaci alapon

1. táblázat: EDR 1.0 és EDR 2.0/3.0 információbiztonsági összehasonlítása

Forrás: Saját szerkesztés

A lehetséges információbiztonsági megoldások

Az EDR rendszer esetében a gyakorlati információbiztonsági védelem alapja nem különbözik az egyéb rendszerek esetében használt alábbi hármas megközelítéstől:

1. felderítés
2. kockázatértékelés
3. észlelés.

Az információbiztonsági problémák/incidensek megelőzését célzó ajánlásokat a következő pontokban foglalhatjuk össze szintén egy hármas megközelítéssel (SeConSys 2021):

1. megelőzés
2. észlelés
3. reagálás.

A következőkben ezen hármas megközelítéseket fejtem ki bővebben.

Fenyegetettség felderítése

Az EDR rendszer kiemelt fontossága is indokolja, hogy a rendszerre leselkedő fenyegetéseket felderítéssel tervezzük megelőzni. A jövőálló 2.0 és 3.0 EDR rendszerek fenyegetettsége a technológia változása miatt lényegesen magasabb, mint a korábbi zárt, ellenőrzött HW/SW komponensekből álló EDR 1.0 esetében. A fenyegetettség felderítése így már szükségszerűen megjelenik a rendszert üzemeltető szervezet szervezeti felépítésében is:

- stratégiai (biztonsági vezetés, szervezeti vezetés)
- taktikai (biztonsági csoportok, hálózati csoportok, eseménykezelő csoportok)
- műveleti (veszélyvadász, eseménykezelő csoport, biztonsági vezetés).

Globális fenyegetés felderítés: listák és szabályok használata az alábbiak mentén:

- IoC: Indicator of Compromise: kompromittálódásra utaló jel
- Yara szabályrendszer (malware) – rosszindulatú programok kutatásában és felismerésében használt eszköz
- Hash/Url/IP/DNS listák és szabálycsomagok használata
- CTI (Cyber Threat Intelligence) – kiberfenyegetettség felderítés
- Honeypot 4G/5G specifkus protokollok emulálása a generikus protokollok mellett
  passzív sebezhetőségi hírszerzés: központi adattár (5G szolgáltatók, PPDR szolgáltatók), sebezhetőségek megosztása, CVE-kre figyelmeztetés
- Early warning system – csatlakozás a Nemzeti Kibervédelmi Intézet Korai Figyelmeztető Rendszeréhez
- CVE Number Authorities – például, ha a rendszer elemeinek beszállítója, a CVE No Authorotites azt jelzi, hogy kiemelten kezeli a sérülékenységek kezelését (Samsung, E/// stb.).

Kockázatértékelés

A távközlési rendszerre és rendszerelemeire vonatkozó fenyegetettségeket a kapcsolódó támadási vektorok és az egyes támadó profilok alapján szükséges értékelni.

Néhány támadási vektor:

- Sérülékenységeket kihasználó támadások: a sikeres támadások mindig valamilyen – fizikai, logikai, szervezeti, humán – sérülékenység kihasználására épülnek. Esetünkben az EDR 2.0/3.0 rendszerek fizikai sérülékenysége az, ami jelentősen növekedhet a hálózat topológiája miatt (pl. nagyszámú, nehezen ellenőrizhető rádióállomás).
- Hálózati behatolás: ennek lehetősége szintén nagyobb a szélessávú EDR rendszer esetében, mert a hálózat lényegesen kiterjedtebb és összetettebb.
- Kriptográfiai sérülékenységek kihasználása.
- Protokoll és API hibák kihasználása.
- Sérülékenységek mindkét fő osztálya, a publikusan ismert, valamint a zero-day sérülékenység is lényegesen nagyobb számban fordulhat elő a piaci SW/HW elemek használata miatt.
- Beszállítótól érkező támadás: az esetleges – az egy beszállítótól való függés csökkentése miatti – többszállítós kialakítás növelheti ennek a támadási formának jelentőségét.

Támadói profilok

A rendszereket fenyegető támadások forrása sokféle lehet. Egyes támadókat motiváció, az információszerzési képesség mélysége, a technikai tudás szintje, valamint a rendelkezésre álló erőforrások mennyisége alapján érdemes osztályozni. Az EDR 1.0 rendszer speciális volta miatt sokkal felkészültebb, több speciális (akár belső) információ birtokában lévő támadó járhatott csak sikerrel, az EDR 2.0/3.0 esetében a potenciális sikeres elkövetők köre jelentősen bővül és a szükséges (belső vagy publikus) információ és tudás alacsonyabb szintje is elegendő lehet egy sikeres támadáshoz.

Észlelés

- Helyzetismeret (az üzemeltető minden pillanatban pontosan tudja, hogy mi történik a rendszerében) biztosítása az üzemeltető személyzet részére (NOC-SOC kommunikáció, változáskövetés), monitoring rendszer.
- Naplógyűjtés, kezelés és elemzés (központi naplógyűjtés és feldolgozás – pl. Graylog és biztonsági log gyűjtés és elemzés – SIEM).
- Rosszindulatú kód (malware) észlelés.

Megelőzés

- Sebezhetőség vizsgálat
  - CVE adatbázis nyomonkövetése
  - teszt rendszer kialakítása, mely penetrációs tesztelési célra is használható
  - tesztelés hatókör meghatározása kockázatkezelési eredmények alapján
  - beszállítók sebezhetőség vizsgálata, mint követelmény
- Konfiguráció- és javításkezelés
  - CMDB (Configuration Management Data Base) építése és használata konfigurációkezeléshez – egyes elemek egymásra hatása, ez alapján az infrastruktúra kritikus elemeinek meghatározása (vagy pl. hibaterjedés elemzése)
  - kiadás menedzsment (tesztelés, telepítés, adminisztráció)
  - Legacy rendszerek figyelemmel kísérése (EoL = End of Life)
  - EoL SW és HW
  - már beszerzésnél figyelembe venni a folyamatos gyártói támogatás/javítás/kezelés meglétét
- IAM (Identity and Access Management)
- PAM (Privileged Access Management)
- Határvédelem
  - fizikai védelem (pl. tamper resistant csatlakozások, letiltott konzol csatlakozások stb.)
  - ACL (Access Class List) alkalmazása
  - VLAN (Virtual Lan)-ok használata
  - Port Security és hálózati hozzáférés szabályzás, pl. ISE (Identity Service Engine – Cisco terminology) – klines gépek csatlakozásának szükségessége esetén
  - adatdióda használata
  - DPI (Deep Packet Inspection) – mély csomag ellenőrzés
  - Malware szűrés határpontokon
  - tűzfalcsoport alkalmazása (határvédelmi és pl. belső tűzfal) – eltérő gyártótól beszerezve
  - SPI (Stateful Packet Inspection)
- Hálózatbiztonsági zónastruktúra kialakítása (megfelelő elkülönült biztonsági zónacsoportok kialakítása, virtualizáció és Out-Of-Band menedzsment zónacsoport kialakítása)
- Behatolás megelőzése
  - IDPS (Intrusion Detection and Prevention System) – Behatolás észlelő és megelőző rendszer (IDS vs IPS)
  - SIEM (Security Information and Event Management) – Biztonsági Információ és esemény kezelés
  - SPI (Stateful Packet Inspection)
- Adatbiztonság
  - titkosított protokollok használata érzékeny adatok védelmére
  - jelszavak ne legyenek nyílt szövegben tárolva és küldve
  - vezeték nélküli és nyílt hálózaton történő távoli elérések kriptográfiailag védetten történjenek.

Észlelés

Korábban kifejtésre került.

Reagálás

EDR esetében sem lehet egy esetleges támadás esetén a rendszert leállítani, sőt, inkább szinte bármi áron üzemben kell tartani.

Ehhez eleve úgy kell a rendszerek működését megtervezni, hogy lehetséges legyen a támadással érintett (az IDS által jelzett) rendszerek elszigetelése az ép rendszerektől. A támadás elhárítása után – akár már alatta is – meg kell kezdeni a begyűjtött adatok feldolgozását, értékelését (forensics támogatása). A támadásra adandó reagálás sürgős, a személyzetnek stresszhelyzetben kell dolgoznia, éppen ezért fontos az előzetesen kialakított, jóváhagyott és rendszeresen tesztelt biztonsági eseménykezelési tervben kialakított eljárások, jelentések, kommunikációk megfelelő és folyamatos végrehajtása.

A támadás során vélhetően érintett hálózatoktól való minél jobb elkülönítés érdekében legyen fizikailag elválasztott menedzsment-hálózat a naplógyűjtésre és a biztonsági beállítások elvégzésére.

Legyen eljárásrend a támadás elhárítása után az esemény kiértékelésre.

Az értékelés eredményei beépítendők a megelőzési- és észlelési stratégiákba.

A támadás elhárítása és elemzése után az összes tevékenységet ajánlott tételesen átvizsgálni, értékelni, majd a tanulságokat visszacsatolni, a szükséges folyamat-, szabályozás-, technológia- stb. fejlesztéseket elvégezni.

Összefoglalás

A jelenleg működő EDR 1.0 és jövőbeli EDR 2.0/3.0 információbiztonsági kérdéseket összehasonlítva láthatjuk, hogy komplex, nem csak a teljes rendszert lefedő, hanem a rendszer megvalósításának teljes életciklusát figyelembe vevő folyamatot kell elképzelnünk, mely kiterjed a beszerzés, a tervezés, a kivitelezés, a beüzemelés és a majdani üzemeltetés fázisaira is. Az információbiztonsági szemlélet pedig nem csak a műszaki területre korlátozódik immár, hanem meg kell jelennie a szervezeti felépítésben, a saját üzemeltető személyzet, de még a külső beszállítók és szolgáltató partnerek kiválasztásába és folyamatos felügyeletébe is.

Melléklet

1. sz. melléklet: Rövidítések jegyzéke

Fogalom, rövidítés	Kifejtés	Magyar megnevezés
BB-PPDR	Broadband Public Protection and Disaster Recovery	Szélessávú Közrend és Katasztrófa Elhárítási Rendszer
CMDB	Configuration Management Data Base	Konfiguráció menedzsment adatbázis
CORE	Core Network	Maghálózat
CERT	Computer Emergency Response Team	Eseménykezelő központ
CTI	Cyber Threat Intelligence	Kiberfenyegetettség felderítés
CVE	Common Vulnerability and Exposures	Ismert sérülékenységek és kitettségek
EDR		Egységes Digitális Rádió-Távközlő Hálózat
EWS	Early Warning System	Korai figyelmeztető rendszer
IAM	Identity and Access Management	Azonosítás- és hozzáférés kezelés
IDS	Intrusion Detection System	Behatolás észlelő rendszer
IPS	Intrusion Prevention System	Behatolás megelőző rendszer
IDPS	Intrusion Detection and Prevention System	Behatolás észlelő és megelőző rendszer
NOC	Network Operation Center	Hálózati irányító központ
O&M	Operations and Maintenance	Üzemeltetés és karbantartás
PAM	Privileged Access Management	Privilegizált hozzáférés kezelés
SIEM	Security Information and Event Management	Biztonsági Információ és esemény kezelés
SOC	Security Operation Center	Biztonsági Üzemeltetési Központ
SPI	Stateful Packet Inspection	Állapotfüggő csomagfelügyelet
RAN	Radio Access Network	Rádiós hozzáférési hálózat
TETRA	Terrestrial Trunked Radio	Földfelszíni trönkölt rádió

Irodalomjegyzék

Kardos, T. Zs. (2021) Az Egységes Digitális Rádió-távközlő Rendszer (EDR) továbbfejlesztési lehetőségei. *Rendvédelem folyóirat*, X. évf. 2021/3. sz. pp. 12-18. DOI: 10.53793/RV.2021.3.2 https://bm-tt.hu/wp-content/uploads/2022/02/2021_3_Kardos_Tamas_Zsolt.pdf [Letöltve: 2022.04.26.].

Nemzeti Kibervédelmi Intézet Korai Figyelmeztető Rendszere https://nki.gov.hu/ews/.

Pro-M Zrt. középtávú fejlesztési stratégia (2019) https://www.pro-m.hu/Hirek/2019/ProMNews/ [Letöltve: 2021.07.30.].

SeConSys (2021) Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve. Nemzeti Kibervédelmi Intézet.