Répás Sándor[243] – Rajnai Zoltán: *Virtuális erőművek szerepe az energiaellátásban és kiberbiztonsági kérdéseik*

Absztrakt: A Virtuális erőművek (Virtual Power Plant, VPP) szerepe a villamosenergia-ellátásban egyre fontosabbá válik. Elterjedésüket az információs- és telekommunikációs technológiák (ITK) fejlődése teszi lehetővé és gyorsítja fel. Az új technológiák egyre szélesebb körű alkalmazása azonban, újabb biztonsági kockázatok megjelenésével jár együtt. Rendkívül fontos területe a kritikus infrastruktúrák védelmének az energiabiztonság biztosítása. Megvizsgálásra és bemutatásra kerül a VPP-k szerepe Magyarország energiaellátásában, valamint annak kérdése, hogy kritikus infrastruktúraelemként szükséges-e kezelni a VPP-k et, vagy azok valamely részét. Bemutatásra kerül a VPP-k általános működési modellje, valamint működési sajátosságaik. A VPP-k működését lehetővé tevő információs infrastruktúrák kockázatai, valamint ajánlások is bemutatásra kerülnek.

Bevezetés

Az energiaellátás biztonsága kritikus fontosságú minden fejlett társadalom számára. Magyarország létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényében (Lrtv) meghatározott ágazatok közt is az első helyet foglalja el az energiaellátás, a villamos-energiarendszer létesítményei [1]. Kiemelt szerepét fokozza az interdependencia is, hiszen a villamos-energia ellátás hiányában más infrastruktúra elemek működésében is fennakadások keletkeznek.

Az egyre nagyobb villamos-energia felhasználás szükségessé tette a villamos-energiaellátási rendszerek (VER) folyamatos fejlesztését is. Az energia-előállítás egyre magasabb költségei, valamint a környezetvédelmi szempontok miatt előtérbe kerültek a villamos-energiát megújuló energiahordozókból előállító berendezések és technológiák, valamint a kiserőművek, a termelés a fogyasztás közelébe került, elterjedt az elosztott termelés (Dispersed/Distributed Generation, DG). Ezeket az új energiatermelő eszközöket azonban bonyolult a VER-be integrálni. Ennek az integrációnak az elősegítésére és költséghatékonyabbá tételére dolgozták ki a virtuális erőművek (VPP) modelljét. A következőkben bemutatjuk a VPP-k működését, szerepét a magyar VER-ben, valamint megvizsgáljuk fontosabb kiberbiztonsági kérdéseiket.

Virtuális erőművek

A VPP-k megjelenését az infokommunikációs technológiák (IKT) fejlődése és terjedése tette lehetővé. Megjelenésük az 1990-es éve végétől kezdődött, míg Magyarországon 2011-től indult el az első virtuális erőmű.

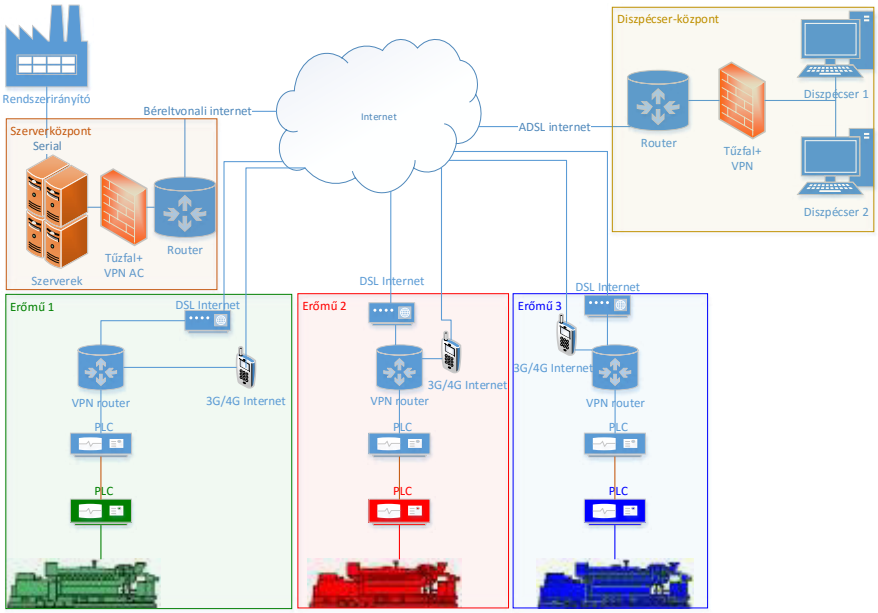
Egy kiserőmű kapacitása kevesebb, mint 50MW, és megbízhatóságuk sem éri el a nagy erőművekét, mindemellett egyéb, technikai jellegű problémák is nehezítik a VER-be integrálásukat. Ezen jellemzőik, valamint a gazdasági környezet miatt közvetlen kapcsolódásuk a magyar VER-hez nem valósítható meg költséghatékonyan. E problémák megoldásának szükségessége eredményezte az első VPP-k létrejöttét.

A VPP-k több, földrajzilag elosztott kiserőműből állnak, melyeket a villamos-energia rendszer irányítója (Transmission System Operator, TSO) egy erőműként "lát" és szabályoz. Egy-egy virtuális erőmű sokféle termelési kapacitást integrálhat. Tartozhatnak hozzá akár szél-, víz-, naperőművek, gázmotorok, kapcsolt energiatermelést végző eszközök, valamint tartalék generátorok is egyidejűleg.

Az 1. ábrán látható egy tipikus magyarországi VPP felépítése. A bal felső sarokban ábrázolt szerverközpontban fut a VPP vezérlését ellátó informatikai rendszer (Electronic Management System,

[243] Óbudai Egyetem, Biztonságtudományi Doktori Iskola rsandor@ahol.co.hu , rajnai.zoltan@bgk.uni-obuda.hu

EMS). A virtuális erőmű EMS rendszere irányítja a rendszerirányító EMS rendszertől kapott igények alapján a VPP-be integrált termelőegységek (és esetleg fogyasztók) optimális energia előállítását (esetleg fogyasztását). Az optimalizálás a sokféle, eltérő termelőegység, azok eltérő paraméterei és az eltérő szempontok miatt bonyolult feladat, mely probléma megoldásával sok publikáció foglalkozik [3], [4].



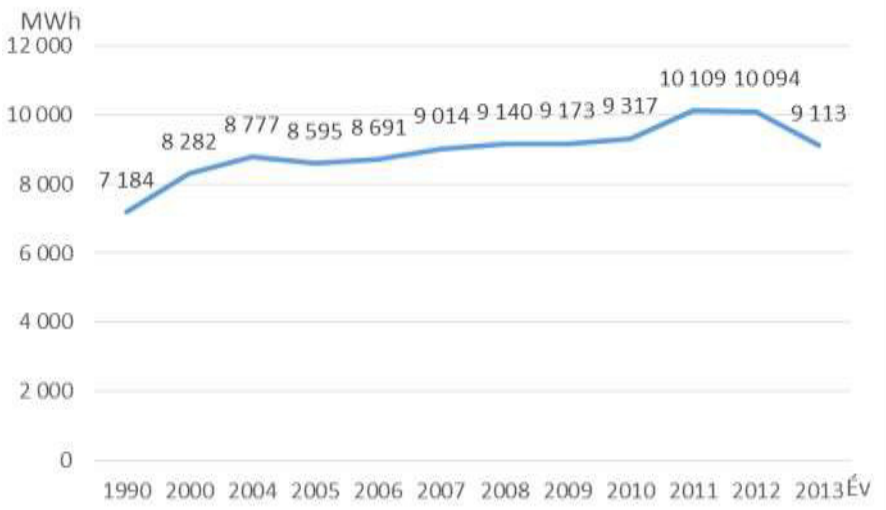
1. ábra: Tipikus virtuális erőmű felépítése

Az 1. ábra alján láthatóak az eltérő helyszíneket szimbolizáló három téglalapban a termelőegységek és az ő közvetlen vezérlésüket ellátó programozható logikai vezérlők (Programmable Logic Controller, PLC, vagy SCADA slave), melyekhez a VPP-k PLC-je kapcsolódik, valamilyen a felügyeleti, irányító és adatgyűjtő (Supervisory Control and Data Acquisition, SCADA) rendszerek területén alkalmazott felületen keresztül (a kapcsolódás módját általában a termelőegység PLC-jének képességei határozzák meg, melyhez a VPP PLC alkalmazkodni kénytelen). A VPP PLC TCP/IP kapcsolaton keresztül kapcsolódik a VPP EMS rendszeréhez. A kapcsolat biztosításához az interneten keresztül virtuális magánhálózat (Virtual Private Network, VPN) kerül kialakításra a telephelyen elhelyezett VPN képes útválasztó eszköz (router) segítségével. A távközlési hálózat kimaradásából eredő problémák kiküszöbölésére két eltérő technológiával csatlakozik a router az internetre. Az elsődleges kapcsolat általában valamilyen DSL (Digital Subscriber Line), vagy kábelmodemes csatlakozás, míg a tartalék vonal 3G WCDMA, vagy 4G LTE csatlakozás. A két vonal közti átállást az informatikai összeköttetés hibája esetén, a router automatikusan elvégzi.

A felügyelet ellátását, valamint az esetlegesen szükséges manuális beavatkozást az ábra jobb felső sarkában jelölt diszpécserközpontból végezhetik el diszpécserek. A menetrendkészítés és feltöltés a VPP EMS rendszerébe, szintén az itt elhelyezett munkaállomásokról történhet.
Az ábrán nem került külön jelölésre, de megvalósítástól függően a VPP szerverközpontja és diszpécserközpontja is rendelkezhet redundáns internetkapcsolattal.

A Virtuális erőművek szerepe a magyar villamos-energia rendszerben

A 2. ábrán ábrázoltuk a magyar ver erőműveinek bruttó (BT) teljesítőképességének alakulását. Az 1. táblázatban pedig a magyarországi VPP-k adatait foglaltuk össze. Az adatok vizsgálata alapján kijelenthető, hogy a VPP-k jelentős résztvevői a magyar villamos-energia rendszernek. A VPP-k 466MW BT összesített teljesítőképessége megközelíti egy paksi blokkét, a Magyarország számára előírt tercier szabályozási tartalék mértékét.



2. ábra: Magyar ver erőműveinek bruttó teljesítőképessége (Forrás: [5])

Táblázat 1: Magyarországi VPP-k (Forrás: [5] és [6])

VPP üzemeltető	Szabályozás	BT	Szabályozható	Gépek	Átlag BT
Dalkia szekunder csoport	S	52MW	47MW	20db	2,6MW
Dalkia tercier csoport	T	34MW	4MW	12db	2,8MW
Greenergy	S	60MW	50MW	21db	2,9MW
Eonsum	S	65MW	47MW	11db	5,9MW
Alpiq	S	54MW	50MW	10db	5,4MW
Ploop	S	59MW	13MW	14db	4,2MW
VPP	S	141MW	113MW	27db	5,2MW
Összesen		**466MW**	**325MW**	**115db**	**4,0MW**

A teljes 9113MW-nak pedig majdnem 1/5-ödét adja.

A 2. táblázatban feltüntettük a rendszerszintű koordinációban nem résztvevő kiserőművek teljesítőképességi adatait. Fontos információ, hogy ebben a táblázatban sok kiserőmű nem szerepel, ugyanakkor az adatok alapján így is kijelenthető, hogy még sok kapacitás VPP-be integrálható, ezáltal egy részük a szabályzásba is bevonható.
A megújuló energiahordozók szerepe és aránya nő, azonban ezek nem, vagy csak rendkívül kis mértékben szabályozhatóak (pl: nap, szél), így az ilyen kiserőművek termelésének ingadozását ki kel egyenlíteni (338MW), amit egyszerűbbé tehet VPP-be integrálásuk.

Táblázat 2: Rendszerszintű koordinációban nem résztvevő kiserőművek teljesítőképessége (Forrás: [5] és [6])

Típus	BT		Típus	BT
Gázmotor	117MW		Nap	2MW
Gőzturbina	69MW		Szél	281MW
Gázturbina	100MW		Víz	55MW
Biogáz motor	46MW			
Biogáz turbina	47MW			
Összesen	**380MW**		**Összesen**	**338MW**
Mindösszesen: 717MW				

Az adatok összesítése alapján a következő megállapításokat tehetjük:

- Az egyes VPP-k összteljesítménye viszonylag alacsony (az ismertetett adatokból ugyan nem látszik, de tapasztalatok alapján az egyes kiserőművek VPP-k közti mozgása gyors).
- A kiserőművek összesített teljesítőképessége több, mint duplája a VER tercier szabályozási tartalékának.
- Az ismertetett adatok alapján egyik VPP hibás működése sem okozhat rendszerszintű problémákat, azonban gazdasági károkat előidéz.
- Az összes VPP egyidejű hibás működése miatt lényegesen nagyobb probléma jelentkezhet, időponttól függően, akár rendszerszintű problémákat előidézve.
- A VPP-k növekedése, és a kiserőművek mozgása miatt a jövőben előállhat olyan helyzet, hogy bizonyos VPP-k hibás működése rendszerszintű problémákat idéz elő.
- Mindezek alapján az egyes magyarországi VPP-k jelenleg ugyan nem tekinthetőek kritikus infrastruktúráknak, de ez gyorsan változhat.

A megállapításokat figyelembe véve a VPP-k informatikai rendszereinek kialakításakor olyan megoldásokat kell alkalmazni, melyek biztosítják a megfelelő biztonsági szinten történő működést.

Virtuális erőművek támadása és védelme

Kritikus szerepükből kifolyólag az energetikai irányító rendszerek (EMS SCADA), mint célpontok népszerűsége nő a kibertámadások végrehajtása során. Jó példa erre a 2012 májusában azonosított Flame (más néven sKyWIper) malware [7], mely célzottan az EMS SCADA rendszerekkel kapcsolatos adatokat gyűjtött, valamint a 2014 júniusában megtalált Havex trojan, mely szintén energetikai irányító rendszereket támadott [8].

Az EMS SCADA rendszerek támadásával általában nem az információszerzés az elsődleges cél (bizalmasság megsértése), hanem működési zavar előidézése (rendelkezésre állás megsértése).

A virtuális erőművek kialakításánál kiemelkedően fontos szempont a költséghatékonyság. Nem dedikált összeköttetéseket használnak, hanem az interneten keresztül kialakított VPN csatornákon keresztül kommunikálnak. Így fokozottan kitettek az internet felől érkező támadásoknak. A következőkben néhány lehetséges támadástípust, azok lehetséges célpontjait, valamint a támadások várható hatását vizsgáljuk meg. Kiemelten foglalkozunk napjaink három legfontosabb kibertámadás típusával.

Szolgáltatásmegtagadás (Denial of Serivce, DoS)

Manapság az egyik leginkább elterjedt, legsűrűbben alkalmazott támadástípus a szolgáltatásmegtagadásra irányuló támadás, ennek is a több számítógép segítségével végrehajtott verziója a (Distributed Denial of Serice, DDoS)

A DoS támadások alapvető célja, hogy a hálózatra csatlakozó eszköz (pl: router, switch, webszerver, levelező szerver) üzemszerű működését megzavarja. Létezik olyan megvalósítása, mely egy az adott eszközben lévő programhibát használ ki, és akár már egy darab megfelelően összeállított IP csomag elküldésével megzavarhatja az eszköz működését, míg létezik olyan verziója is, mely egyszerűen csak túlterhelést idéz elő az eszközön, azáltal, hogy (akár szabályos) kérésekkel árasztja el a megtámadott eszközt. Utóbbi esetben az eszköz megpróbálja kiszolgálni a kéréseket, de azok olyan mennyiségben érkeznek, hogy vagy az eszköz, vagy pedig az eszköz internet csatlakozását biztosító vonal kapacitását meghaladja a kérések, vagy az arra adott válaszok mennyisége. A DoS támadásoknak sok fajtája létezik, azonban a támadók által leginkább használt jelenleg az elárasztásos DDoS támadás. Kutatók vizsgálták a DoS támadások smart gridekre gyakorolt egyes hatásait [9]-ben, míg [10]-ben részletesebb leírást és védekezési lehetőségeket találhatunk bizonyos DoS támadás típusok esetében.

A lehetséges DDoS célpontok és azok kihatása internet irányából érkező támadások esetén a következők:

- Egy kiserőmű internet csatlakozása: Kivitelezése egyszerű, kihatása korlátozott, csak csekély anyagi kárt okoz. DoS támadás megvalósításától és a VPP kiépítésétől függően, több eset lehetséges:
  - Ha a VPN router mindkét internet csatlakozását egy időben támadják, úgy a kiserőmű képtelen lesz kommunikálni a VPP EMS SCADA masterrel, így a parancsok fogadása és a mérési adatok továbbítása lehetetlenné válik.
  - Ha a VPN routernek csak egyik internet csatlakozását támadják, azonban oly módon, hogy az magát a VPN routert terheli túl, úgy a kommunikáció szintén lehetetlenné válik. Ha azonban csak az átviteli vonal túlterhelése történik meg, úgy a tartalék internetkapcsolat felhasználásával a kommunikáció zavartalanul folyhat.
- Egyidejűleg minden kiserőmű internet csatlakozása: A támadás előkészítése nehezebb, hiszen az összes kiserőmű internet csatlakozásának IP címeit meg kell szereznie a támadónak. A DoS támadás megvalósításától, a VPP kiépítésétől és a támadás időpontjától (és természetesen a VPP méretétől) függően, kihatása magas lehet, jelentős anyagi károkat okozva, azonban ebben az esetben is az előzőekben felsorolt lehetőségek állnak fent:
  - Ha a VPN routerek mindkét internet csatlakozását egy időben támadják, úgy a kiserőmű képtelen lesz kommunikálni a VPP EMS SCADA masterrel, így a parancsok fogadása és a mérési adatok továbbítása lehetetlenné válik.
  - Ha a VPN routereknek csak egyik internet csatlakozását támadják, azonban oly módon, hogy az magukat, a VPN routereket terheli túl, úgy a kommunikáció szintén lehetetlenné válik. Ha azonban csak az átviteli vonalak túlterhelése történik meg, úgy a tartalék internetkapcsolatok felhasználásával a kommunikáció zavartalanul folyhat.
- VPP szerverközpont (SCADA master helye) internet csatlakozása: Előkészítése, kivitelezése egyszerű feladat, megegyezik az egy kiserőmű internet csatlakozásának támadása esetén szükségessel, annyi különbséggel, hogy itt valószínűleg jóval nagyobb sávszélességű távközlési vonal áll rendelkezésre, melynek túlterhelése nehezebben kivitelezhető feladat lehet a támadó részére. Hatása a minden kiserőmű internet csatlakozásának támadása során elért hatást annyiban haladhatja meg, hogy a VPP diszpécserközpontja és a VPP szerverközpont közti kommunikációt is akadályozza, ezáltal a diszpécserek az aktuális adatok hiányában nem képesek megfelelő döntéseket hozni, és a kiserőművek irányításába megfelelő módon beavatkozni.
- Diszpécser központ internet csatlakozása: Előkészítése, kivitelezése egyszerű feladat, megegyezik az egy kiserőmű internet csatlakozásának támadása esetén szükségessel (kismértékben egyszerűbb is lehet). Hatása korlátozott, hiszen csak a diszpécserek adatelérését és beavatkozását akadályozza, meg azonban a VPP SCADA master a kiserőművek vezérlését problémamentesen elláthatja. Rövidtávon tehát csak minimális kárt

okoz, hosszabb távú DoS támadás esetén könnyen megoldható a szükséges napi operatív feladatok elvégzése.

Ajánlások:
Az ismertetett támadások hatásának minimalizálása érdekében az alapvető információbiztonsági ajánlások mellett még a következőket érdemes figyelembe venni:

- Az egyes végpontokon két VPN router elhelyezése csökkenti bizonyos DoS támadások kihatását.
- Két eltérő típusú router alkalmazása csökkenti a router firmware hibáját kihasználó DoS támadás sikeres kivitelezésének kockázatát is.
- A telephelyek redundáns internet vonalainak kialakítása során érdemes arra törekedni, hogy azok:
    - egy-egy telephely esetében különböző technológiát alkalmazzanak (pl: egy ADSL, és egy 4G LTE)
    - a két internet csatlakozás internetszolgáltatója lehetőség szerint eltérő adatkicserélő központot alkalmazzon.
- Fontos kérdés annak eldöntése is, hogy mit tegyen a VPP PLC-je olyan esetben, amikor a kommunikáció megszakad a VPP vezérlőközpontjával. Több eset lehetséges:
    - A VPP PLC nem avatkozik be: A kiserőmű tartja a teljesítményét. Ennek a megoldásnak a megvalósítása a legegyszerűbb a VPP implementációja során.
    - A VPP PLC gondoskodik az előzőleg a VPP vezérlőközpontjától kapott menetrend tartásáról. Ennek a megoldásnak megvalósítása a legbonyolultabb a VPP implementációja során.
    - A VPP PLC leállítja a kiserőmű termelését.
- A három felsorolt megoldás kombinációinak alkalmazása is lehetséges, de fontos annak figyelembevétele is, hogy a kommunikáció mennyi időre szakadt meg a VPP SCADA masterrel, és ennek függvényében meghozni a döntést a beavatkozásról.

A DoS támadás hatása korlátozott, "csak" a kommunikációt lehetetleníti el (rendelkezésre állás), detektálása egyszerű, a védekezés ellene azonban nagyon nehéz, azonban a tervezés során a rendszer felkészíthető a DoS támadások hatásának minimalizálására.

Malware, spyware, trojan, worm
A szolgáltatásmegtagadásnál kifinomultabb támadások kivitelezhetőek a különböző rosszindulatú programok alkalmazásával. A malware (Malicious And Unwanted Software) egy összefoglaló név a rosszindulató programokra, melyeknek egyik fajtája a spyware. A spyware feladata, hogy észrevétlenül adatokat gyűjtsön működésének helyéről, majd azokat észrevétlenül továbbítsa. A trójai program pedig olyan rosszindulatú program, mely magát hasznos alkalmazásként, programként tünteti fel, így érve el azt, hogy a gyanútlan felhasználó azt önszántából elindítsa, telpítse. Egy trójai program funkciója sokrétű lehet az adatgyűjtéstől kezdve, az egyszerű károkozáson át akár a zsarolásig bezárólag. Végül a worm egy olyan önálló program, mely önállóan terjed a hálózatban, valamint terjedésének a trójai programokhoz hasonlóan sokféle célja lehetséges. Egy rendkívül kifinomult trójai támadásra példa az iráni atomprogramot visszavető Stuxnet [11].
Egy lehetséges támadás kivitelezése rendkívül egyszerű lehet:

- Első lépésként el kell készíteni a megfelelő feladatot ellátó rosszindulatú programot. Ehhez nem feltétlenül van szükség magas programozói felkészültségre, mert rengeteg olyan eszköz érhető el bárki számára, mely segítségével percek alatt elkészíthető a kívánt funkcionalitású rosszindulatú program. Ennél egy fejlettebb, és nehezebben detektálható támadóeszköz elkészítése már nehezebb, és erőforrásigényesebb feladat. Ha a támadó sok erőforrással

rendelkezik, úgy akár még kijavítatlan hibából eredő, nulladik napi sebezhetőségeket is beépíthet a támadóprogramba. Ezek azonban lényegesen költségigényesebb megoldások. A Stuxnet 4 darab ilyen sebezhetőséget is alkalmazott terjedése érdekében.

- Második feladat a támadókód célbajuttatása. Ez történhet egy egyszerű e-mail elküldésével, mely elég érdekes ahhoz, hogy a címzett megnyissa a támadó kódot tartalmazó mellékletet. Megoldható a célpont dolgozójának fertőzött weboldalra csalogatásával, vagy egy egyszerű adathordozó postázással a célpont részére.
- A támadóprogram működéséhez, vezérléséhez szükség van még egy, vagy több a vezérlőközpont szerepét ellátó szerver üzemeltetésére.

A támadás kivitelezése során a diszpécser, vagy a diszpécserrel munkakapcsolatban áló személy megtévesztése a célszerű.
A végrehajtott támadások célja, és az okozható kár mértéke lényegsen nagyobb lehet, mint a DoS támadások esetén. Ráadásul, míg egy DoS támadás detektálása nagyon könnyű, addig egy megfelelően elkészített és használt malware detektálása magas felkészültséget igényel.
A támadónak több célja is lehet, azonban a legnagyobb kárt nem a kiserőművek egyszerű leállításával tudja okozni, hanem a VPP vezérlőközpontja és a diszpécseri munkaállomások közti kommunikáció meghamisításával. Ilyenkor a diszpécser meghamisított, de életszerű információkat lát, azokra megfelelő parancsokat ad ki. A vezérlőköpont pedig a támadó parancsait hajtja végre, nem pedig a diszpécser parancsatit.

Ajánlások
Az ismertetett behatolási módok sikerességének minimalizálása érdekében a következőkre érdemes különösen figyelni:

- A legfontosabb feladat az üzemeltetők és a rendszerrel bármilyen módon kapcsolatba kerülők rendszeres és magas fokú biztonsági képzése. Ez nagymértékben csökkentheti a malware kódoknak a VPP rendszerébe jutását.
- Az ügyviteli és az üzemirányítási célú informatikai rendszer szigorú szétválasztása, nagyon szigorú tűzfalszabályok alkalmazása és karbantartása.
- Behatolásdetektáló eszközök (Intrusion Prevention System) alkalmazása és folyamatos karbantartása, üzemeltetése.
- Az üzemviteli rendszerből internetelérés semmilyen módon ne legyen lehetséges.
- Adathordozók kezelésének szigorú szabályozása.

A DoS támadások által okozott károknál sokkal komolyabbak okozhatóak, a hamisított adatok rendszerbe juttatásával, azonban kivitelezésük komolyabb erőforrásokat igényel a DoS támadásokhoz kivitelezéséhez képest.

APT
A kiberterrorizmus és a kiberhadviselés terjedésével az advanced persistent threat (APT) támadások is előtérbe kerültek. Az APT segítségével kivitelezett támadások költségei a legmagasabbak, komoly előkészületeket és erőforrás ráfordítást igényelnek, ennek ellenére egyre több APT-vel kapcsolatos eset kerül nyilvánosságra.

Az APT támadások néhány fontosabb jellemzője:

- lopakodás,
- lassú támadás,
- fejlett kód,
- folyamatosan változó kód,
- változatos módszerek együttes alkalmazása,

- célzott támadás,
- létfontosságú célpontok kiválasztása,
- magasan képzett támadók,
- sok erőforrás áll rendelkezésre a támadás végrehajtásához.

A jellemzők alapján a VPP-k, a lehetséges kár mértéke miatt nem vonzó célpontok APT támadásokhoz. Mivel azonban a VPP-k könnyű célpontoknak tekinthetőek, a VPP-k terjedése és növekedése mindjobban potenciális célpontokká teszi őket.
Alapvetően a kártékony kódokkal végrehajtott támadásoknál bemutatottal megegyező behatolás módok, célok, károkozási módszerek és ajánlások érvényesek itt is.

Egyéb támadások

A kiserőművek üzemeltetői számára a virtuális erőmű üzemeltetése jellemzően partnerportált is kialakít, mely lehetőséget nyújt a tipikusnak mondható támadási módok alkalmazására, mint amilyen az SQL injection, buffer overflow, stb.
VPN támadások csak abban az esetben vezetnek eredményre, ha a VPN kialakítása során nem vették figyelembe a biztonsági előírásokat, és bevált gyakorlatokat. (Esetleg a VPN router vezérlőprogramjának hibája esetén.)
A távközlési infrastruktúra a VPP-k esetében az internet hálózaton alapul, így bármely támadás, mely az internet működését akadályozza jól alkalmazható a VPP-k működésének megzavarására is. Erre példa a forgalomkicserélő központok támadása.

Összefoglalás

A virtuális erőművek fontos szereplői a magyar villamos-energiarendszernek, és fontosságuk egyre nő. Kialakításuk során kiemelt szempont a költséghatékonyság. Interneten alapuló távközlési infrastruktúrájuk és egyéb jellemzőik miatt könnyű támadási célpontok. Egy-egy VPP önmagában jelenleg nem tekinthető kritikus infrastruktúrának, azonban több VPP együttes működési zavara már képes komoly zavarokat előidézni a villamos-energia rendszerbben. Mivel az energetikai rendszerek, mint kibertámadási célpontok jelentősége folyamatosan nő, így kialakításuk során kiemelt szempontként kell kezelni a kiberbiztonság biztosítását.

Referenciák

[1] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[2] Maros Dóra: Kritikus infrastruktúrák interdependenciái: A 2010 KIV gyakorlat tapasztalatai, Budapest, Magyarország, 2010. november 4-5, Óbudai Egyetem
[3] Bernhard Jansen et al: Architecture and communication of an electric vehicle virtual power plant, Gaithersburg, Amerikai Egyesült Államok, 2010. október 4-6, IEEE, pp. 149-154.
[4] Pio, Alessandro Lombardi et al: Optimal operation of a virtual power plant, Calgary, Kanada, 2009. július 26-30, IEEE, pp. 1-6.
[5] A magyar villamosenergia-rendszer (ver) 2013. évi statisztikai adatai, Budapest, Magyarország, 2014, Magyar Energetikai és Közmű-szabályozási Hivatal
[6] A magyar villamosenergia-rendszer adatai 2013, Budapest, Magyarország, 2014, MAVIR Zrt.
[7] Sami Zhioua: The middle east under malware attack dissecting cyber weapons, Philadelphia, Amerikai Egyesült Államok, 2013. július 8-11. IEEE, pp. 11-16.

[8] Advisory (ICSA-14-178-01) ICS Focused Malware, Amerikai Egyesült Államok, 2014. június 30, ICS-CERT
[9] Shichao Liu et al: Denial-of-Service (dos) attacks on load frequency control in smart grids, Washington DC, Amerikai Egyesült Államok, 2013. február 24-27, IEEE, pp. 1-6.
[10] Xueping Chen: Distributed denial of service attack and defense, Chongqing, Kína 2010. szeptember 17-19, IEEE, pp. V3-318-V3-320.
[11] Thomas M. Chen és Saeed Abu-Nimeh: Lessons from Stuxnet, Amerikai Egyesült Államok, 2011. április 5, IEEE, pp. 91-93.
[12] Frankie Li et al: Evidence of Advanced Persistent Threat: A case study of malware for political espionage, Fajardo, Puerto Rico, 2011, október 18-19, IEEE, pp. 102-109.
[13] Nagy, I. Z.: Spezielle Eintreibungstechniken zur Senkung der Außenstände, In: Kadocsa Gy (szerk.), MEB 2006: 4th International Conference on Management, Enterprise and Benchmarking. 360 p., Budapest BMF.,2006. pp. 196-208., (ISBN: 9637154477)
[14] Nagy, I. Z., Való, V.: The Lawful Execution of Employer's Rights is an Important Subsystem of Corporate Governance: a Labour Case Study, In: Michelberger, P. (szerk.), MEB 2013: 11th International Conference on Management, Enterprise and Benchmarking: Budapest: Óbudai Egyetem, 2013. pp. 107-126. (ISBN: 978-615-5018-58-9)