CTI elemzés

Az OT rendszerek hálózatbiztonsága

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalomjegyzék

Bevezetés

A digitalizáció korunk egyik legmeghatározóbb technológiai folyamata, amely az emberi élet szinte minden területén átalakította a működési modelleket, a szolgáltatásokat és a döntéshozatali mechanizmusokat. Ez alól az ipari környezetek sem jelentenek kivételt, különösen azok a rendszerek, amelyek közvetlen kapcsolatban állnak a fizikai világgal. Az operatív technológiák, vagyis az OT rendszerek világa a digitalizáció térnyerésével alapvetően megváltozott. A korábban jellemző mechanikus működtetést, manuális beavatkozást és helyszíni mérést fokozatosan digitális vezérlési, felügyeleti és adatfeldolgozási megoldások váltották fel, elsősorban a hatékonyság növelése, a termelési folyamatok optimalizálása és a költségek csökkentése érdekében.

Az ehhez szükséges mérnöki és informatikai tudás az elmúlt évtizedekben fokozatosan épült be az ipari környezetekbe, aminek következtében az OT és az IT fejlődési útja egyre szorosabban összekapcsolódott. Míg korábban az ipari vezérlőrendszerek jellemzően zárt, izolált és erősen specializált környezetekben működtek, addig napjainkra egyre gyakoribbá vált az IP alapú kommunikáció, a távoli hozzáférés, a központi naplózás, az analitikai rendszerekhez történő adatkapcsolat, valamint a felhőalapú vagy hibrid megoldások megjelenése. Ez a fejlődés jelentős üzemeltetési előnyöket hozott, ugyanakkor új kiberbiztonsági kockázatokat is teremtett. Az OT hálózatbiztonság ezért ma már nem pusztán technikai kérdés, hanem a fizikai folyamatok folytonosságának, a termelés biztonságának, a berendezések épségének és adott esetben az emberi élet védelmének egyik alapvető feltétele.

Betekintés az OT hálózatokba

Az OT környezetek hálózatbiztonságának megértéséhez először át kell tekinteni azokra a hálózati logikákra, architektúrákra, rendszerelemekre és protokollokra, amelyek az ipari rendszerek működését meghatározzák. Mint minden hálózat tervezésekor, itt is alapvető követelmény az adott szervezet működési igényeinek, infrastruktúrájának, kockázati környezetének és üzembiztonsági elvárásainak pontos felmérése. Az OT hálózatok egyik legfontosabb sajátossága, hogy elsődleges céljuk a fizikai folyamatok állandó, kiszámítható és megbízható fenntartása. Emiatt ezekben a környezetekben a rendelkezésre állás, a determinisztikus működés és a biztonságos üzemmenet jellemzően nagyobb prioritást kap, mint az informatikában megszokott rugalmasság vagy gyors változtathatóság.

Egy vállalati IT rendszerben egy frissítés, újraindítás vagy rövid szolgáltatáskiesés sok esetben elfogadható kompromisszum lehet. Egy ipari vezérlőhálózatban azonban egy váratlan megszakítás termeléskiesést, berendezéshibát, környezeti kárt vagy akár balesetet is okozhat. Ebből következik, hogy az OT hálózatokat nem lehet egyszerűen ugyanazzal a szemlélettel kezelni, mint az általános irodai vagy vállalati informatikai rendszereket. Az ipari környezetekben minden biztonsági intézkedést úgy kell megtervezni, hogy az ne veszélyeztesse a működés folytonosságát, ugyanakkor képes legyen csökkenteni a támadási felületet és korlátozni a potenciális incidensek hatását.

Az OT hálózatok logikai felépítésének egyik legismertebb és leggyakrabban hivatkozott modellje a Purdue-modell. A Purdue-modell az ipari rendszerek elemeit jól elkülöníthető, egymásra épülő logikai szintekbe rendezi, és ezzel keretet ad a hálózati

szegmentáció, a hozzáféréskezelés és a biztonsági kontrollok kialakításához. Bár nem az OSI modell megfelelője, szerkezeti logikájában hasonlóan rétegzett megközelítést alkalmaz, vagyis segít átláthatóvá tenni, hogy az egyes rendszerelemek milyen szerepet töltenek be az ipari működésben, és milyen biztonsági követelmények kapcsolódnak hozzájuk.

- **0. szint, fizikai folyamatok**: A legalacsonyabb szinten a fizikai világgal közvetlen kapcsolatban álló elemek találhatók. Ide tartoznak például az érzékelők, relék, mérőműszerek, vezérlőelemek és egyéb, a fizikai folyamatokhoz közvetlenül kapcsolódó berendezések. Ezek működése és integritása kiemelt jelentőségű, mivel hibás működésük vagy manipulációjuk közvetlenül befolyásolhatja a fizikai folyamatokat. Egy rosszul értelmezett mérési adat, egy jogosulatlan beavatkozás vagy egy késve végrehajtott vezérlési művelet súlyos következményekkel járhat.

- **1. szint, alapvető vezérlés**: A fizikai réteg felett helyezkednek el azok a vezérlőelemek, amelyek a beérkező adatok és az előre meghatározott logikák alapján irányítják a folyamatokat. Ide tartoznak a programozható logikai vezérlők, vagyis a PLC eszközök. Ezek a rendszerek gyakran közvetlen kapcsolatban állnak a fizikai folyamatokhoz kapcsolódó berendezésekkel, és valós időben hajtanak végre vezérlési műveleteket. Ehhez a szinthez kapcsolódhatnak olyan biztonsági vagy védelmi rendszerek is, amelyek kritikus meghibásodás esetén automatikusan megszakítják vagy biztonságos állapotba helyezik a folyamatot. Ezek a védelmi funkciók logikai és működési szempontból gyakran elkülönülnek a normál vezérlőrendszerektől.

- **2. szint, ipari felügyelet és vezérlés**: Ezen a szinten találhatók azok a rendszerek, amelyek a vezérlőkből érkező adatokat összegyűjtik, feldolgozzák, megjelenítik, és adott esetben emberi beavatkozást tesznek lehetővé. Ide tartoznak a SCADA rendszerek és a HMI felületek. Ezek kulcsszerepet töltenek be az ipari folyamatok felügyeletében, hiszen az operátorok ezeken keresztül követhetik a rendszer állapotát, azonosíthatják az eltéréseket, és indíthatnak beavatkozásokat. Fontos megjegyezni, hogy a SCADA rendszerek besorolása az implementáció függvénye: a felügyeleti és adatgyűjtő funkciók klasszikusan a 2. és a 3. szint határán helyezkednek el, ezért egyes architektúrákban a 3. szinthez közelebb is megjelenhetnek.

- **3. szint, üzemviteli műveletek és vezérlés**: Ebben a rétegben jelennek meg az ipari működést támogató üzemirányítási szolgáltatások. Ide tartozhatnak például a mérnöki munkaállomások, üzemviteli szerverek, adattároló rendszerek, helyi címtárszolgáltatások, DNS, NTP és DHCP kiszolgálók, valamint az ütemezési vagy gyártásirányítási rendszerek. A 3. szint gyakran éles határvonalat jelent a kritikusabb ipari rendszerek és a felsőbb vállalati hálózati rétegek között.

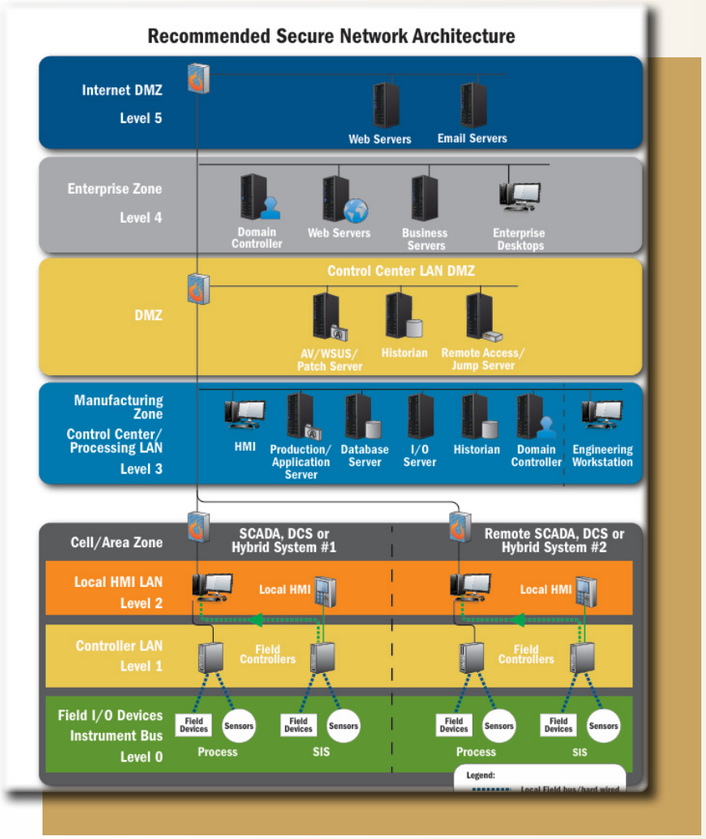
- **3,5. szint, demilitarizált zóna**: A demilitarizált zóna, vagyis a DMZ az alsóbb ipari rétegek egyik legfontosabb védelmi vonala. Feladata, hogy biztonságos átmeneti területként működjön a kevésbé megbízható külső vagy vállalati hálózatok, valamint a kritikus OT rendszerek között. A DMZ célja nem az, hogy szabad átjárást biztosítson a zónák között, hanem az, hogy ellenőrzött, naplózott és szabályozott kommunikációs pontokat hozzon létre. Itt helyezkedhetnek el például proxy szerverek, jump

szerverek, frissítési kiszolgálók, adatközvetítő rendszerek vagy távoli hozzáférési átjárók.

- **4. szint, vállalati hálózat**: Ez a réteg a szervezet üzleti folyamatait támogató belső informatikai környezetet foglalja magában. Ide tartoznak a megszokott irodai szolgáltatások, felhasználói munkaállomások, vállalati alkalmazások, fájlszerverek, levelezési rendszerek és egyéb üzleti támogató komponensek. Ezen a szinten már általánosnak tekinthető az internethasználat, a távoli hozzáférés, valamint a külső szolgáltatásokkal történő rendszeres kommunikáció.

- **5. szint, nagyvállalati vagy külső hálózati kapcsolatok**: Ezen a szinten a vállalat több telephelyét, globális infrastruktúráját, központi üzleti rendszereit, külső szolgáltatásait és felhőalapú megoldásait összekötő környezetek találhatók. Ide sorolhatók például a vállalatirányítási rendszerek, ügyfélkapcsolati rendszerek, üzleti intelligencia platformok, központi felhőszolgáltatások és telephelyek közötti hálózati kapcsolatok.

A Purdue-modell az 1990-es években született, mégis a mai napig meghatározó szemléleti keretet biztosít az ipari hálózatok biztonsági tervezéséhez. Bár a modell kialakításakor az OT rendszerek jellemzően jóval zártabban működtek, mint napjaink ipari IoT és Ipar 4.0 környezetei, az alapgondolat továbbra is érvényes. A rétegek elkülönítése, a hálózati szegmentáció, a jogosultságok kontrollált kezelése és a kommunikációs útvonalak szabályozása olyan biztonsági alapelvek, amelyek az internetkapcsolattal rendelkező modern ipari eszközök esetében is nélkülözhetetlenek.

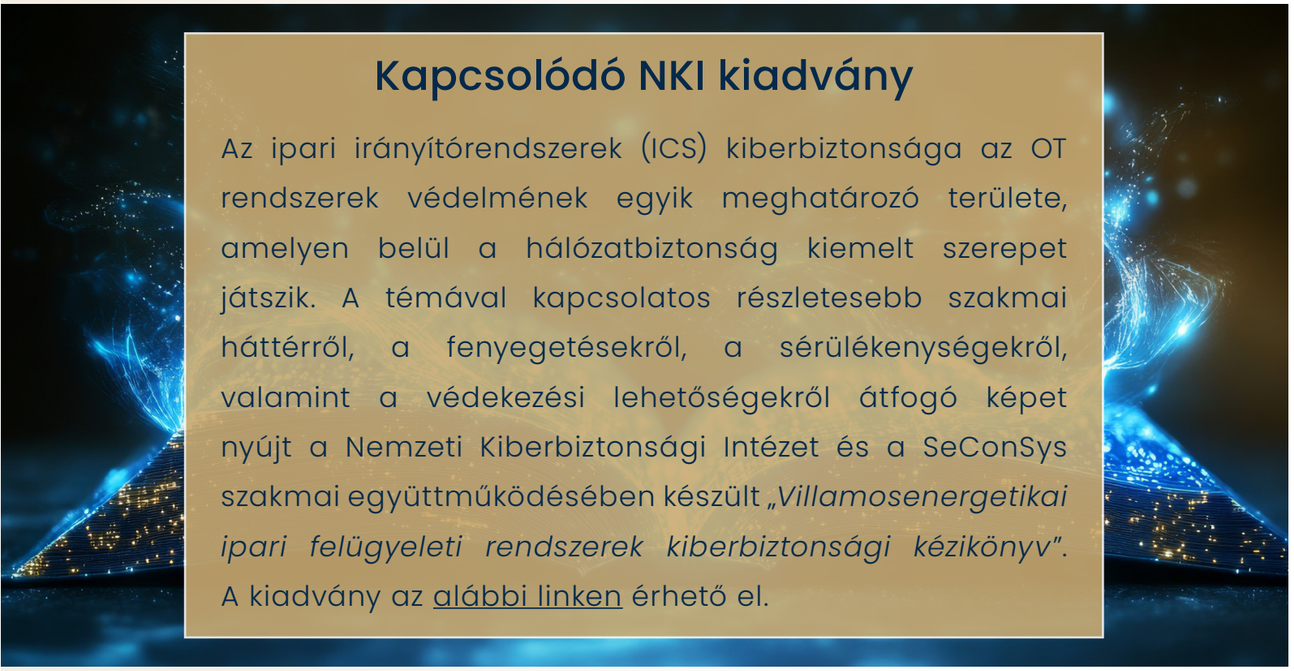


Logikai vázlat a Purdue-modell felépítéséről

Kép forrása: CISA

Az OT és az IT közötti különbségek felismerése nélkül nehéz jó hálózatbiztonsági döntéseket hozni. A két terület technológiai érintkezése nyilvánvaló, hiszen az OT rendszerekben is találhatók Windows vagy Linux alapú komponensek, IP alapú kommunikációs megoldások, szerverek, távoli hozzáférési lehetőségek és vállalati vagy felhős rendszerek felé irányuló adatkapcsolatok. Ettől azonban az OT nem tekinthető egyszerűen informatikai rendszernek más környezetben. Az elsődleges védendő érték ugyanis nem önmagában az adat, hanem a fizikai folyamat, a termelés folytonossága, a berendezések stabil működése és a kritikus állapotok elkerülése.

Ez a hangsúlyeltolódás a biztonsági architektúrát is alapvetően meghatározza. Az OT rendszerekben a rendelkezésre állás és a safety követelményei sok esetben megelőzik a bizalmasság klasszikus információbiztonsági szempontját. Ez természetesen nem jelenti azt, hogy az adatvédelem vagy a bizalmasság lényegtelen lenne, hanem azt, hogy egy gyártósor, energetikai folyamat vagy közműszolgáltatás leállása azonnali és súlyos következményekkel járhat. Az OT környezetekben ezért a frissítések, biztonsági szoftverek telepítése, hálózati szabályok módosítása vagy akár egy egyszerű konfigurációváltoztatás is szigorúbb tervezést, tesztelést és változáskezelést igényel. A hosszú életciklusú berendezések, a beszállítói függőségek, a korlátozott leállási ablakok és a tanúsítási követelmények miatt sokszor nem az a kérdés, hogy elméletileg mi lenne a legbiztonságosabb megoldás, hanem az, hogy mi vezethető be úgy, hogy közben az üzembiztonsági kockázat elfogadható szinten maradjon.



Kapcsolódó NKI kiadvány

Az ipari irányítórendszerek (ICS) kiberbiztonsága az OT rendszerek védelmének egyik meghatározó területe, amelyen belül a hálózatbiztonság kiemelt szerepet játszik. A témával kapcsolatos részletesebb szakmai háttérről, a fenyegetésekről, a sérülékenységekről, valamint a védekezési lehetőségekről átfogó képet nyújt a Nemzeti Kiberbiztonsági Intézet és a SeConSys szakmai együttműködésében készült *„Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyv”*. A kiadvány az alábbi linken érhető el.

Hálózatszegmentálás az OT rendszerekben

A hálózatszegmentálás lényege, hogy a teljes kommunikációs környezetet nem egységes, szabad átjárást biztosító hálózatként kezeljük, hanem biztonsági, működési és funkcionális szempontok alapján elkülönített zónákra bontjuk. Az OT környezetekben ennek különösen nagy jelentősége van, mivel egy lapos, rosszul tagolt hálózatban a kompromittáció gyorsan átterjedhet az egyik komponensről a másikra. Ilyen esetben a szervezet csak késve, vagy egyáltalán nem képes érzékelni, hogy a támadó meddig jutott el, milyen rendszerekhez fért hozzá, és milyen hatással lehet a fizikai folyamatokra.

A megfelelően kialakított szegmentáció ezzel szemben korlátozza az oldalirányú mozgást, csökkenti a támadási felületet, és olyan ellenőrzési pontokat hoz létre, ahol az adatforgalom naplózható, szűrhető, hitelesíthető és szükség esetén megszakítható. Fontos azonban kiemelni, hogy a hálózatszegmentálás jóval többet jelent annál, mint hogy alhálózatokat, VLAN struktúrákat és tűzfalszabályokat hozunk létre. A megfelelő szegmentáció a teljes kiberbiztonsági architektúra egyik alapja. Ellenőrzési pontok és éles határvonalak kialakításával lehetővé teszi a zónák demarkálását, a szerepkörök és felelősségek meghatározását, az eszközök és adatok integritásának védelmét, valamint a megszokottól eltérő hálózati viselkedés azonosítását.

Egy jól megtervezett hálózatszegmentációs modell ezért nem csupán technikai hálózatbiztonsági megoldás, hanem a szervezet kiberbiztonsági stratégiájának egyik meghatározó eleme. Az

OT környezetek speciális tulajdonságai miatt a zónák kialakításánál különösen fontos, hogy a működési igények, a kritikus folyamatok, az eszközök szerepe, a kommunikációs irányok és a biztonsági követelmények együttesen jelenjenek meg a tervezésben.

A megfelelő biztonsági zónák kialakításához három alapvető pillér azonosítható.

Hálózati határvédelem

A hálózatbiztonsági zónákat előre meghatározott, dokumentált és ellenőrizhető módon kell elhatárolni egymástól. A zónahatárok célja, hogy világos legyen, mely rendszerek tartoznak az adott biztonsági tartományba, milyen kommunikáció engedélyezett, és milyen kontrollokon keresztül lehet kapcsolatot létesíteni más zónákkal. Ennek keretében biztosítani kell, hogy a csatlakoztatott eszközök megfelelő jogosultságokkal rendelkezzenek, a zónák közötti interfészek és átjárók megbízhatóak, a belépési pontok előre meghatározottak, valamint a határvédelmi eszközök ellenállóak legyenek a támadásokkal szemben.

A határvédelem fontos része a hálózati forgalom szűrése és monitorozása, a titkosított forgalom kockázatalapú ellenőrzése, a felhasználói és gépi hitelesítés alkalmazása, valamint a változáskezelési szabályok betartása. Az OT környezetekben különösen fontos, hogy a határvédelmi szabályok ne csupán általános informatikai logika alapján készüljenek, hanem igazodjanak az ipari folyamatokhoz, a vezérlési ciklusokhoz, a protokollok sajátosságaihoz és a biztonságos üzemmenet követelményeihez.

Hálózati forgalomirányítás

A biztonsági zónák önmagukban nem nyújtanak megfelelő védelmet, ha a köztük lévő forgalom nincs pontosan kontrollálva. A zónák közötti kommunikációnak minden esetben előre meghatározott szabályokon kell alapulnia. Csak olyan forgalom engedélyezhető, amely üzletileg vagy üzemeltetésileg indokolt, megbízható forrásból származik, meghatározott célrendszer felé irányul, és megfelel a biztonsági követelményeknek.

A forgalomirányítás során biztosítani kell, hogy a zónák között kizárólag engedélyezett kommunikáció történhessen, a kártékony vagy rendellenes forgalom elemzése és szűrése a lehetőségekhez mérten megvalósuljon, az engedélyezett forgalom csak kijelölt erőforrások irányába haladhasson, a kifelé irányuló kommunikáció pedig ne jelentsen indokolatlan többletkockázatot az adott zóna számára. OT környezetben különösen lényeges, hogy a forgalomszabályozás ne csak IP címekre és portokra épüljön, hanem lehetőség szerint vegye figyelembe az ipari protokollok parancsszintű sajátosságait is.

Általános zónakontroll

A zónakontrollok olyan alapkövetelmények, amelyeket a zónák elhelyezkedésétől és jellegétől függetlenül minden hálózati tartományban érvényesíteni kell. Ennek része, hogy az egyes alhálózatok és szegmensek világosan hozzárendelt zónákhoz tartozzanak, ne keveredjenek más zónák funkcióival, és csak jóváhagyott belépési pontokon keresztül kapcsolódjanak más hálózati területekhez. A szervereknek és klienseknek nem célszerű több zónából közvetlenül elérhetőnek lenniük, mivel ez gyengíti a szegmentációt és növeli az oldalirányú mozgás lehetőségét.

Minden zónára vonatkozóan naprakész dokumentációt kell fenntartani, beleértve a műszaki rajzokat, a kommunikációs mátrixokat, a kapcsolódási pontokat, a zónahatárokat, a tűzfalszabályokat és az alkalmazott biztonsági kontrollokat. Az OT környezetekben ez nem csupán adminisztratív feladat, hanem incidenskezelési, auditálási és üzemeltetési szempontból is alapvető követelmény.

A fenti irányelvek alapján jól látható, hogy a zónafelügyelet kialakítása jelentős felelősséggel jár. Bármilyen hiányosság a zónák meghatározásában, a határvédelmi szabályokban, a dokumentációban vagy a forgalomszabályozásban komoly kockázatot jelenthet az OT rendszerek átfogó integritására. A zónák mindegyike saját funkcionális és biztonsági szereppel rendelkezik, amelyet saját határain belül kell érvényesítenie.

Tipikus hálózati zónák

Nyilvános hozzáférési zóna

A nyilvános hozzáférési zóna az a hálózati terület, amely közvetlen kapcsolatban állhat a nyilvános internettel. Feladata, hogy közvetítse és kezelje a szervezet online szolgáltatásai, külső felhasználói, partnerei és a belső környezetek közötti kapcsolatokat. Mivel ez a szervezet külső irányba néző határterülete, az architektúra egyik leginkább kitett eleme, ezért különösen erős védelmi intézkedéseket igényel.

A szervezeteknek úgy kell kialakítaniuk ezt a zónát, hogy támogassa az online szolgáltatásokat, ugyanakkor ütközőzónaként működjön az internet és a belső környezetek között. Ide tartozhatnak az internetes alkalmazások kiszolgálását vagy közvetítését végző rendszerek, a külső levelezési szolgáltatások, valamint a távoli hozzáférés egyes komponensei. A külső elérések koncentrált kezelése csökkenti a belső zónák közvetlen kitettségét, és erősebb elkülönítést tesz lehetővé a külső és belső rendszerek között.

Operációs zóna

Az operációs zóna a szervezet általános üzleti és vállalati működését támogató környezet. Ebben a zónában találhatók a hétköznapi irodai végpontok, felhasználói rendszerek, vállalati alkalmazások, munkaszerverek és egyéb belső szolgáltatások. Az itt megjelenő forgalom származhat belső forrásból, de elérheti a szervezetet külső irányból is, például a nyilvános hozzáférési zónán keresztül biztosított távoli hozzáférési szolgáltatások útján.

Az operációs zónán belül célszerű a klienseket és a szervereket külön alzónákba szervezni, mivel ez csökkenti a potenciális kitettségeket és megkönnyíti az üzemeltetést. Az itt kezelt érzékeny információkat megfelelő végpontvédelmi, hozzáféréskezelési és naplózási kontrollokkal kell védeni. Ugyanakkor ez a zóna nem feltétlenül alkalmas arra, hogy nagy mennyiségben kezeljen kiemelten érzékeny adatokat vagy olyan kritikus rendszereket, amelyek kompromittálódása súlyos incidenshez vezethet. Az ilyen rendszereket magasabb védelmi szintű zónákban indokolt elhelyezni.

Korlátozott zóna

A korlátozott zóna olyan szolgáltatások és rendszerek számára fenntartott terület, amelyek magasabb megbízhatósági, integritási és védelmi követelményekkel rendelkeznek. Az itt működő rendszerek kompromittálódása jelentős üzleti zavart okozhat, ezért ez a terület a szokásos vállalati működési környezetnél szigorúbban védett.

A korlátozott zónát úgy kell kialakítani, hogy kizárólag jóváhagyott belépési pontokon keresztül kapcsolódjon más zónákhoz. A kliensek és szerverek elkülönítése itt is indokolt, az érintett rendszereket pedig emelt szintű biztonsági megerősítésnek kell alávetni. Ez a zóna nagy mennyiségű érzékeny adatot vagy kritikus üzleti alkalmazást is tartalmazhat, amelyek az átlagos vállalati szolgáltatásoknál magasabb fokú integritásvédelmet, rendelkezésre állást és bizalmasságot igényelnek.

Ipari vezérlési korlátozott zóna

Az ipari vezérlési korlátozott zóna erősen kontrollált hálózati környezetet biztosít az ipari vezérlőrendszerek számára. Ez az a zóna, amelyben a legérzékenyebb ICS szolgáltatások

és rendszerek működhetnek. Az itt bekövetkező kompromittálódás közvetlenül hathat a fizikai folyamatokra, és akár emberi egészséget, biztonságot vagy a környezetet is veszélyeztetheti. Emiatt ezt a zónát az architektúra egyik legszigorúbban védett területeként kell kezelni.

Az ipari vezérlési korlátozott zóna és a nyilvános hozzáférési zóna között minden közvetlen kapcsolatot tiltani kell. Az ipari vezérlési környezet kizárólag kontrollált és jóváhagyott belépési pontokon keresztül kapcsolódhat más belső zónákhoz. Az itt működő rendszereket a környezet kritikus jellegének megfelelően kell megerősíteni, a hozzáféréseket szigorúan szabályozni, a kommunikációt naplózni és monitorozni. Ez a zóna tartalmazhat jelentős mennyiségű operatív adatot, kritikus ipari alkalmazást és olyan rendszereket, amelyek alapvető szerepet játszanak az ipari folyamatok felügyeletében vagy vezérlésében.

Ipari vezérlési alzónák

Az ipari vezérlési korlátozott zónán belül az egyes ipari egységek további alzónákat alakíthatnak ki annak érdekében, hogy elkülönítsék egymástól a különböző ipari funkciókat, folyamatokat, rendszereket vagy telephelyeket. Ezek az alzónák finomítják a szegmentációs modellt, és lehetővé teszik, hogy a szervezet eltérő, célzott kontrollokat rendeljen a különböző operatív területekhez.

Az ilyen alzónák semmilyen körülmények között nem kapcsolódhatnak közvetlenül a nyilvános hozzáférési zónához. Külső partnerkapcsolatokat, például SCADA támogatási célú hozzáféréseket kizárólag erre kijelölt, kontrollált és naplózott útvonalakon keresztül szabad biztosítani. Minden olyan ipari egységnek, amely ilyen alzónákat

alakít ki, kötelező ezekhez kapcsolódó dokumentációt készítenie és karbantartania. A dokumentációnak tartalmaznia kell a műszaki rajzokat, az alzónák hivatalos meghatározását, az alkalmazott kontrollok leírását, a forgalomszabályozási követelményeket, a határvédelmi követelményeket, valamint a követett szabványokra vagy szabályozási keretrendszerekre történő hivatkozást.

Megbízható partner zóna

A megbízható partner zóna olyan közvetlenül csatlakoztatott szolgáltatásokat és kapcsolatokat támogat, amelyek megbízható külső partnerekkel állnak összefüggésben. Ez a zóna felfogható a belső környezetek logikai kiterjesztéseként olyan külső szervezetek irányába, amelyekkel a vállalat formális együttműködési vagy szerződéses kapcsolatban áll. Ugyanakkor fontos hangsúlyozni, hogy a partnerkapcsolat önmagában nem jelent teljes bizalmat. A partneri kapcsolatok továbbra is kockázatot hordoznak, ezért a megbízható partner zónát szigorúan szabályozni kell.

A megbízható partner zóna nem kapcsolódhat közvetlenül a kritikus ipari vezérlési környezetekhez vagy a legszigorúbban védett belső zónákhoz. A kapcsolódásokat minden esetben jóváhagyott belépési pontokon, szabályozott forgalmi útvonalakon és dokumentált követelményeken keresztül kell megvalósítani. A zónára vonatkozó követelményeket egyedileg kell meghatározni, figyelembe véve a partnerkapcsolat jellegét, az érintett rendszereket, a kapcsolódás üzleti célját és a potenciális kockázatokat.

A megbízható partner zóna tipikus példái közé tartozhatnak a pénzügyi intézményekkel kialakított integrációk, a beszállítói kapcsolatok, a kiszervezett IT környezetek, valamint a leányvállalatokhoz vagy kapcsolódó szervezetekhez kialakított interfészek. Ezek a kapcsolatok üzletileg indokoltak lehetnek, de továbbra is kontrollált és jól körülhatárolt kiterjesztésként kell kezelni őket, nem pedig korlátlanul megbízható útvonalként.

Ipari protokollok és hálózatbiztonság

A modern ipari rendszerek működésének alapja a megbízható kommunikáció. A műszerek, szenzorok, vezérlők, felügyeleti rendszerek és aktuátorok közötti adatcsere nem csupán a hatékony működés feltétele, hanem a biztonságos és kiszámítható üzemeltetés egyik alapja is. Legyen szó vezetékes vagy vezeték nélküli megoldásokról, az ipari kommunikáció minden esetben valamilyen protokollra épül. Az OT környezetekben azonban a protokollok nem pusztán információt továbbítanak, hanem közvetve vagy közvetlenül fizikai folyamatokra hatnak. Emiatt a kommunikáció megbízhatósága,

védettsége és ellenőrizhetősége jóval nagyobb jelentőséggel bír, mint elsőre gondolnánk.

Az ipari protokollok vizsgálatakor nem elegendő kizárólag a funkcionalitást értékelni. Figyelembe kell venni a címzési logikát, a hálózati továbbíthatóságot, az autentikációs és titkosítási lehetőségeket, a naplózhatóságot, a jogosultsági modellt, valamint azt is, hogy az adott protokoll mennyire illeszthető modern biztonsági kontrollokhoz. Ez különösen fontos a hálózatszegmentáció szempontjából, hiszen a szegmentáció egyik kulcseleme a kommunikáció felügyelete, ellenőrizhetősége és korlátozása. Amennyiben egy protokoll valamelyik biztonsági szempontból hiányos, az a teljes hálózati architektúra kockázati szintjét növelheti.

Az OT világában használt számos protokoll eredetileg olyan korszakban született, amikor az ipari rendszerek zárt, fizikailag elkülönített és erősen kontrollált környezetekben működtek. Emiatt több régebbi protokoll nem tartalmaz natív titkosítást, erős hitelesítést vagy részletes jogosultságkezelést. A titkosítás hiánya, a gyenge autentikáció, az üzenetek könnyű lehallgathatósága és a parancsok manipulálhatósága ezért gyakran visszatérő probléma az OT biztonság területén. A Purdue-modellre és a zónaalapú biztonsági megközelítésre épülő architektúrák éppen abból az alapfeltevésből indulnak ki, hogy a környezet egyetlen komponensében sem szabad feltétlenül megbízni. A védelemnek ezért több rétegben, ellenőrzött határokon és jól dokumentált kommunikációs útvonalakon kell érvényesülnie.

Modbus

A Modbus az egyik legrégebbi és legszélesebb körben alkalmazott kommunikációs protokoll az ipari automatizálásban. A Modicon által 1979-ben kialakított megoldás eredeti célja az volt, hogy különböző buszokon és hálózatokon keresztül összekapcsolt eszközök között egyszerű és megbízható kommunikációt tegyen lehetővé. Egyszerűsége, robusztussága és széles gyártói támogatottsága miatt hosszú idő alatt kvázi ipari szabvánnyá vált.

A protokoll meghatározó változatai közé tartozik a Modbus RTU és a Modbus TCP. A Modbus RTU tipikusan soros kommunikációs közegben, például RS 232 vagy RS 485 kapcsolaton keresztül működik, és klasszikusan mester és szolga architektúrát alkalmaz. Jellemző felhasználási területe a PLC eszközök és terepi berendezések közötti kommunikáció. A Modbus TCP ezt a logikát Ethernet alapú hálózatokra ülteti át, lehetővé téve a PLC eszközök, HMI rendszerek és más ipari komponensek közötti kommunikációt IP alapú hálózatokon keresztül. Ez megkönnyíti az integrációt, ugyanakkor növeli annak szükségességét, hogy a kommunikációt megfelelő hálózati szegmentációval, forgalomszűréssel és hozzáférés kontrollal védjék.

OPC és OPC UA

Az OPC, vagyis Open Platform Communications olyan szabványok és specifikációk összefoglaló neve, amelyek célja az ipari hardverek és szoftveralkalmazások közötti adatcsere biztosítása. Az OPC Foundation által az 1990-es években létrehozott kezdeményezés egyik fő célja az interoperabilitás javítása volt, különösen a különböző gyártók rendszerei között.

Az OPC fejlődésének eredményeként jött létre az OPC UA, amely korszerűbb, platformfüggetlenebb és biztonsági szempontból fejlettebb architektúrát képvisel. A klasszikus OPC erősen kötődött a Microsoft COM és DCOM technológiáihoz, és elsősorban HMI, SCADA, PLC és más ipari rendszerek közötti adatcserére használták. Az OPC UA ezzel szemben szolgáltatásorientált architektúrára épül, platformfüggetlen, és natívan támogat olyan biztonsági funkciókat, mint a titkosítás, a hitelesítés és az auditálás. Ez különösen alkalmassá teszi modern ipari IoT környezetekben, heterogén rendszerekben és több gyártót érintő integrációkban történő alkalmazásra.

PROFIBUS

A PROFIBUS, vagyis Process Field Bus, az ipari automatizálásban széles körben alkalmazott terepibusz szabvány, amelyet a gyár és folyamatautomatizálási rendszerek valós idejű kommunikációjára fejlesztettek ki. A technológia az 1980-as évek végén jelent meg, és különösen Európában vált meghatározóvá a vezérlőrendszerek és terepi eszközök közötti megbízható kommunikáció biztosításában.

Két fő típusa a PROFIBUS DP és a PROFIBUS PA. A DP változat nagy sebességű, RS 485 alapú soros kommunikációt alkalmaz, és gyors, ciklikus adatcserére tervezték a vezérlőrendszerek és a decentralizált eszközök között. Emiatt elsősorban gyárautomatizálási környezetekben használják. A PA változat ezzel szemben olyan folyamatipari és veszélyes környezetekben alkalmazható, ahol a fokozott üzembiztonság kiemelt követelmény. Sajátossága, hogy egyetlen kábelen képes adatkommunikációt és tápellátást biztosítani, ami jelentős rugalmasságot nyújt a terepi eszközök telepítése során.

DNP3

A DNP3, vagyis Distributed Network Protocol 3, elsősorban a közműszektorban, különösen a villamosenergia és víziközmű rendszerekben alkalmazott kommunikációs protokoll. Fő feladata a SCADA rendszerek, távoli terminálegységek és más terepi berendezések közötti megbízható adatcsere biztosítása. A protokoll fejlesztésének egyik legfontosabb célja a robusztus működés, a nagy távolságú kommunikáció támogatása és a gyártók közötti interoperabilitás biztosítása volt.

A DNP3 elterjedtsége különösen a kritikus infrastruktúrák területén figyelemre méltó, ahol a kommunikáció megbízhatósága és időbelisége alapvető jelentőségű. A villamosenergia rendszerek, alállomások és víziközmű hálózatok felügyeletében a DNP3 máig fontos szerepet tölt be, mivel jól illeszkedik a nagy kiterjedésű, távfelügyeleti jellegű rendszerek kommunikációs igényeihez. Biztonsági szempontból ugyanakkor itt is kiemelt jelentőségű a megfelelő szegmentáció, a forgalom ellenőrzése és a protokollbiztonsági képességek következetes alkalmazása.

Kitekintés az ipari IoT világába

Napjainkban széles körben elterjedtté vált az okos eszközök használata. A lakóépületek világítását, fűtését, multimédiás rendszereit, takarítását és biztonsági funkcióit egyre gyakrabban hálózatba kapcsolt szenzorok, vezérlők és automatizált berendezések támogatják. A fizikai világot érzékelő és befolyásoló eszközök egyre szorosabban kapcsolódnak az információs rendszerekhez. Az adat ebben a környezetben komoly értéket képvisel, mivel hozzájárulhat a kényelmesebb, hatékonyabb és költségtakarékosabb működéshez.

Ugyanez a jelenség az ipari környezetekben is megjelent, az OT rendszerek esetében azonban jóval nagyobb követelmények kapcsolódnak hozzá. Az ipari IoT olyan érzékelőkből, műszerekből, gépekből és egyéb eszközökből áll, amelyek hálózatba kapcsolva támogatják az ipari és gyártási folyamatok fejlesztését, optimalizálását és felügyeletét. Bár több szempontból is felfedezhető hasonlóság az otthoni okoseszközök és az ipari IoT megoldások között, az OT környezetek alapvető követelményei jóval szigorúbbak. Itt nem csupán kényelmi funkciókról van szó, hanem olyan rendszerekről, amelyeknek megbízhatóan, biztonságosan és kiszámíthatóan kell működniük akár kritikus ipari folyamatok részeként is.

Az ipari IoT rendszerek kategorizálására gyakran háromrétegű architektúrát alkalmaznak. Ez az élrétegből, a platformrétegből és a vállalati rétegből áll. A rétegek együtt dolgozzák fel az adatáramlásokat és a vezérlési folyamatokat, kapcsolatukat pedig különböző hálózattípusok biztosítják, így például a közelségi hálózat, a hozzáférési hálózat és a szolgáltatási hálózat.

A vállalati réteg tipikusan az üzleti vagy szakterületi alkalmazások, döntéstámogató rendszerek és felhasználói felületek helye. Ide futnak be az alsóbb rétegekből érkező adatok, és innen indulhatnak olyan vezérlési vagy optimalizálási utasítások, amelyek hatással lehetnek a többi rétegre. Ebben a rétegben jelenhetnek meg például az üzleti elemzések, jelentések, karbantartási előrejelzések, termelési mutatók és vezetői döntéstámogató megoldások.

A platformréteg köztes szerepet tölt be a vállalati és az élréteg között. Egyrészt továbbítja a vezérlési parancsokat az alsóbb rétegek felé, másrészt összegyűjti, rendszerezi és elemzi a különböző forrásokból érkező adatokat. Emellett eszköz és erőforráskezelési funkciókat is ellát, valamint általános szolgáltatásokat biztosít, például lekérdezési, analitikai vagy adatfeldolgozási képességeket. A konkrét megvalósítástól függően ez a réteg működhet helyszíni adatközpontban, külső adatközpontban vagy felhőkörnyezetben is.

Az élréteg feladata az adatok összegyűjtése az élcsomópontoktól, például érzékelőktől, aktuátoroktól, ipari berendezésektől és egyéb OT vagyonelemektől. Az élréteg nem feltétlenül jelent önálló fizikai elválasztást, mivel logikai értelemben is értelmezhető. Elhelyezkedése és kialakítása nagyban függ az adott megoldás földrajzi kiterjedésétől, telepítési környezetétől és működési céljától. Az élhálózati feldolgozás lényege, hogy a számítási erőforrások és alkalmazási szolgáltatások ne kizárólag a központi adatközpontban vagy a felhőben legyenek jelen, hanem az adatforráshoz közelebb is. Ennek eredményeként az élréteg nem csupán adatgyűjtési pontként működik, hanem részt vesz az adatok helyi feldolgozásában, elemzésében és azonnali felhasználásában is.

Az ilyen architektúra teljesen elosztott működésre képes, ezért többféle kommunikációs és együttműködési modellt támogat. Ide tartozhatnak az eszközök közötti közvetlen kapcsolatok, az élhálózaton található berendezések együttműködése, az elosztott lekérdezések, az adatok több helyszínen történő kezelése, valamint az adatirányítási feladatok. A közelségi hálózat az érzékelőket, aktuátorokat, eszközöket és más OT vagyonelemeket kapcsolja az architektúrához, jellemzően egy vagy több klaszteren keresztül egy olyan átjáróhoz, amely más hálózatok felé teremt kapcsolatot.

A hozzáférési hálózat az élréteg és a platformréteg közötti adat és vezérlési kapcsolatot biztosítja. Ez megvalósulhat vállalati hálózaton keresztül, nyilvános internetre épülő magánhálózati megoldással, vagy akár mobilhálózati kapcsolaton keresztül is. A szolgáltatási hálózat ezzel párhuzamosan a platformréteg, a vállalati réteg és az egyes szolgáltatások közötti összeköttetést biztosítja.

Az élhálózati számítástechnika decentralizált informatikai megközelítés, amelyben a számítási erőforrások és alkalmazási szolgáltatások nem kizárólag központi adatközpontokban vagy felhőkörnyezetben helyezkednek el, hanem megoszlanak az adatforrás és a központi feldolgozás közötti kommunikációs útvonal mentén. Ez a modell egyszerre értelmezhető vertikálisan, az eszközszinttől a felhőig, valamint horizontálisan is, az ipari IoT alrendszerei között.

Az élhálózat szerepe nem merül ki abban, hogy adatokat gyűjt és továbbít a központi feldolgozás irányába. Ugyanilyen fontos feladata, hogy a helyben keletkező adatokat közvetlenül feldolgozza, elemezze, és szükség esetén azonnali műveleteket indítson. Ez különösen értékes olyan ipari folyamatok esetében, ahol a késleltetés, a hálózati kapcsolat megszakadása vagy a központi feldolgozás túlterheltsége működési kockázatot jelenthet. Az élhálózati feldolgozás ezért az ipari működés optimalizálásának egyik alapvető eszköze.

Az ipari IoT rendszerek védelme során általános biztonsági ajánlások alkalmazhatók, ugyanakkor a tényleges kontrollokat minden esetben kockázatalapú értékelésre kell építeni. A megfelelő biztonsági intézkedéseket az adott rendszer üzleti, működési és védelmi követelményeihez kell igazítani. Kiemelten fontos a zónák és kommunikációs útvonalak pontos meghatározása, az eszközök azonosítása, a hozzáférések kontrollja, a naplózás és monitorozás, a beszállítói kapcsolatok kezelése, valamint annak biztosítása, hogy az ipari IoT megoldások ne gyengítsék az OT környezet alapvető biztonsági és üzemeltetési elveit.

Források

ARAVIND0X7. (2024) *Getting Started With OT Security: Understanding OT Protocols (Part 2)* https://aravind07.medium.com/getting-started-with-ot-security-understanding-ot-protocols-part-2-b789b5e073f6 (Letöltve: 2026. március 31.)

BERGE, JONAS. (2001) *Fieldbuses for Process Control: Engineering, Operation, and Maintenance.* ISA, Research Triangle Park.

GARTON, DAVID. (2019) *Purdue Model Framework for industrial control systems and cybersecurity segmentation.* https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf (Letöltve: 2026. március 30.)

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT). (2016) *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* https://www.cisa.gov/sites/default/files/2023-01/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (Letöltve: 2026. március 30.)

STOUFFER, K. ET AL. (2023) *Guide to Operational Technology (OT) Security.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf **(Letöltve: 2026. április 1.)**

Zpedia. *What Is the Purdue Model for ICS Security?* https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security (Letöltve: 2026. április 1.)

NEMZETI
KIBERBIZTONSÁGI
INTÉZET

Kibertámadás!
podcast

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet

titkarsag@nki.gov.hu

nki.gov.hu

+36 (1) 325 7672

2026