HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 87–102.
DOI: 10.32567/hm.2025.4.6

Tóth Ádám[1]

Zero trust network access az ipari (OT) kiberbiztonságban

Ipari rendszerek távelérésének új megközelítése

Zero Trust Network Access Solutions in Operational Technology Environments

New Approaches of Remote Access in Industrial Environments

Absztrakt

A cikk az ipari rendszerek (OT) távelérésének kiberbiztonsági kihívásait vizsgálja, különös tekintettel a VPN-alapú megoldások sérülékenységeire és a zero trust architektúrára épülő zero trust network access (ZTNA) technológia bevezetésének lehetőségeire. A cikk összehasonlítja a VPN és a ZTNA működését, bemutatva az előnyöket és korlátokat, mint például a legkisebb jogosultság elvének való megfelelés mértéke, az identitásalapú hozzáférés-kezelés és az egyszerűbb szabálykezelés. Emellett vizsgálja a ZTNA OT-környezetbe történő integrációs lehetőségeit a Purdue-modellt is figyelembevéve, kitérve az architekturális megvalósíthatósági lehetőségekre, felhívva a figyelmet az implementáció egyéb kihívásaira. A szakirodalmi áttekintés alapján megállapítható, hogy a ZTNA növelheti az OT kiberbiztonságát, ugyanakkor sikeres bevezetése a megfelelő infrastruktúra-előkészítésen, fokozatos bevezetésen és a költség-haszon arány mérlegelésén is múlik.

Kulcsszavak: ipari rendszerek, OT, távoli elérés, ZTNA, zero trust, zero trust architektúra

[1] Óbudai Egyetem Neumann János Informatikai Kar.

Abstract

The thesis examines the cybersecurity challenges of remote access to industrial systems (OT), with particular emphasis on the vulnerabilities of VPN-based solutions and the potential implementation of zero trust network access (ZTNA) technology built on zero trust architecture. It compares the operation of VPN and ZTNA, highlighting advantages and limitations such as the extent to which the principle of least privilege is enforced, identity-based access management, and simplified policy control. The study also explores the possibilities for integrating ZTNA into OT environments, taking into account the Purdue model and addressing architectural feasibility as well as other implementation challenges. The findings indicate that while ZTNA can enhance OT cybersecurity, its successful deployment depends on proper infrastructure preparation, gradual rollout, and careful consideration of the cost–benefit ratio.

Keywords: industrial control systems, OT, remote access, ZTNA, zero trust, zero trust architecture

Bevezetés

Tudományos problémafelvetés

A Dragos ipari (*operational technology,* OT) kiberbiztonsági szervezet 2025-ös átfogó jelentése[2] szerint 2024-ben a zsarolóvírus-támadás volt az egyik leggyakoribb OT-t érintő támadási módszer. A zsarolóvírusokra specializálódott támadó csoportok (*advanced persistent threat,* APT) az összes támadás 60%-ában vettek célba ipari létesítményeket. Ezen támadásokat nagy részben a távoli elérést biztosító megoldásokon keresztül hajtották végre. A legtöbb támadó csoport által alkalmazott támadási vektorok között szerepel a virtuális magánhálózatok (*virtual private network,* VPN), illetve egyéb távelérést biztosító megoldások sérülékenységeinek kihasználása, és az azokkal kapcsolatos azonosítók, jelszavak *(credential)* megszerzése.

Az Escal Institute of Advanced Technologies (SANS) intézet által összeállított, öt legkritikusabb OT kiberbiztonsági kontrollt tartalmazó listában szintén szerepel a biztonságos távoli elérés biztosítása mint kritikus védelmi intézkedés.[3]

A fentiek alapján azonosítható probléma tehát az OT-környezetek távoli elérésének kompromittációjából adódó támadások bekövetkezése.

Kutatási cél

Az azonosított probléma okán felmerül a kérdés, hogy vajon létezik-e az OT távoli elérésére a jelenleg széles körben alkalmazott megoldásoknál biztonságosabb technológia.

[2] Dragos 2025.
[3] Lee–Conway 2022.

Célom egy modernebb, más megközelítésre épített technológiai megoldás vizsgálata az OT távoli elérésével kapcsolatos biztonságának növelése érdekében.

A cikk szakirodalmi áttekintés útján körbejárja a jelenlegi megoldásokkal kapcsolatos problémákat, és a *zero trust* elvre épített *zero trust network access* (ZTNA) megoldások OT-ban való alkalmazási lehetőségeit vizsgálja.

A vizsgálattal szemben az alábbi kérdéseket fogalmaztam meg:

- Mik a jelenleg alkalmazott megoldások az OT távelérésére? Milyen támadási technikák merülnek fel az OT távoli elérésének esetében?
- Mennyiben nyújtanak nagyobb védelmet a ZTNA-megoldások a VPN-megoldásokkal szemben?
- Mennyire IT-ra szabottak a jelenlegi ZTNA-megoldások, lehetséges-e ZTNA-megoldásokat az OT-ba is implementálni? Milyen kihívások elé állíthatja a szervezeteket egy ilyen implementáció?
- Összességében lehetséges-e ZTNA-megoldás alkalmazása az OT-ban, és ha igen, akkor milyen szempontokat figyelembe véve hozhat felelős döntést a szervezet annak alkalmazásáról?

Hipotézisek

A téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

- Általánosságban a ZTNA-megoldások alkalmasak a VPN kiváltására, és nagyobb biztonságot képesek nyújtani a VPN-megoldásoknál.
- Architekturális szempontból lehetséges a ZTNA alkalmazása az OT-ban.
- Az OT rugalmatlansága, technológiai szempontból való lemaradottsága miatt a ZTNA-megoldások OT-ba való integrációja nehézségekkel jár.

Kutatási módszer

A vizsgálat során a releváns szakirodalom, gyártói ajánlások és leírások, publikáció, technológiai megoldások működésének áttekintésén keresztül kaptam válaszokat. A szakirodalom tanulmányozása során olyan naprakész forrásokat kerestem, amelyek a *zero trust* elvnek való megfeleléssel, *zero trust* architektúra kialakításával, a ZTNA-megoldásokkal, OT-architektúramegoldásokkal kapcsolatosak. Továbbá egyéb internetes tartalmakat (tanulmányok, blogbejegyzések, gyártói útmutatók, marketingcélú anyagok stb.) is tanulmányoztam annak céljából, hogy kiderítsem, jelenleg milyen piaci kezdeményezések jelennek meg a ZTNA-megoldások OT-integrációjának kérdése körül, vannak-e konkrét megoldások vagy gyártói javaslatok ZTNA-megoldások OT-környezetbe való implementálásával kapcsolatban.

A fenti vizsgálati kérdésekre adott válaszok alapján a cikk több részre tagolódik:

- A OT-ban jelenleg széles körben alkalmazott és leginkább biztonságosnak tekintett VPN-megoldások alkalmazási lehetőségeinek ismertetése.
- Az OT távoli elérésével összefüggő támadási technikák ismertetése, elsősorban VPN-sérülékenységeken keresztül vizsgálva.

- A ZTNA-megoldások funkcionalitásának ismertetése.
- Összehasonlítás a VPN- és ZTNA-megoldások között a ZTNA által nyújtott magasabb szintű védelem bizonyítására.
- A ZTNA-megoldások implementációjának vizsgálata, architekturális megoldási lehetőségek, a ZTNA Purdue-modellbe való illesztése és az implementáció kihívásai.
- Általános következtetések levonása, a megvalósítás eldöntésének támogatása.

Virtuális magánhálózat (VPN) az ipari irányítási rendszerek távoli elérésére

Az OT-környezetekben is egyre gyakrabban használnak távelérési megoldásokat. Használatuk célja általában a fizikailag messze lévő eszközök elérése, az egyes eszközök, rendszerek külső felek (beszállítók, partnerek, karbantartók) általi támogatásának lehetősége távolról. Az OT-ban népszerű távoli elérést biztosító megoldások közül a VPN-nel foglalkozom, mivel az OT távoli elérésére jelenleg a VPN a leggyakrabban használt és biztonságosnak tekintett megoldás, ezért más megoldásokra (például RDP, VNC stb.) nem térek ki.

A VPN-technológiák megfelelően biztonságos távoli elérést képesek adni. Természetesen sok múlik a megfelelő típus, protokoll kiválasztásán, az architekturális kialakításon, a konfiguráción és egyéb tulajdonságokon, amelyeket a továbbiakban még részletesen érinteni fogok. A felhasználás tekintetében a VPN főbb típusai az alábbiak.

- Kliens-telephely közti/távoli elérésű (client-to-site/Remote access) VPN. A legáltalánosabban használt, egyéni felhasználóknak szánt modell. OT-ban gyakoriak azok a belső és külső karbantartók, akik a szervezet által menedzselt eszközről kívánják elérni az OT-hálózatot. Hasonló célból alkalmazható még a felhőalapú VPN (cloud VPN/VPN as a Service, VPNaaS) is. Ennek előnye, hogy a host oldalon nem szükséges semmilyen infrastrukturális feltételt szabni, hiszen a felhasználó a webes felületen keresztül használja a szolgáltatást, ami egyszerűvé teszi a konfigurációt is. A VPNaaS-megoldások az OT-ban is előfordulhatnak, hiszen a fejlettebb VPN-eszközöket felhős platformon keresztül lehet konfigurálni (platform service). Az általános célú felhős VPN az OT-ban nem fordul elő, mivel az OT nem hosztolja ki az infrastruktúráját a felhőbe.
- Telephelyek közti (site-to-site) VPN. Állandó kapcsolat kialakítására alkalmas megoldás, ahol két hálózat biztonságos összeköttetése valósul meg. Ezt a típust az OT általában egy másik szervezet (például beszállító, partnerszervezet, anyavállalat) hálózatával való összekötése miatt alkalmazhatja.
- Gépek közti (machine-to-machine) VPN. Titkosított, biztonságos adatcsatorna hozható létre gépek, eszközök vagy szolgáltatások között. Egyes szolgáltatók előszeretettel kötik össze a privát felhőjüket az OT-s eszközükkel, ilyen módon menedzselhetővé teszik őket.[4]

[4] Kocsis 2025.

Távelréssel összefüggő támadási technikák

A különböző OT-ra jellemző technikák (*tactics, techniques and procedures,* TTP) megismerésére a MITRE Corporation saját OT-s mátrixszal[5] rendelkezik, amelyben ismerteti az OT-környezetek támadási technikáit. Ezt felhasználva a szervezet megvizsgálhatja a távoli elérésekkel kapcsolatos támadási technikákat, taktikákat és eljárásokat. A mátrix több technikát is tartalmaz, ami közvetlenül a távoli elérést biztosító szolgáltatásokkal, így a VPN-nel is összefüggésbe hozható.

Kezdeti hozzáférés *(initial access)* kategória

Exploitation of remote services. Ebben az esetben a cél, hogy valamilyen sérülékenységet kihasználva a támadó hozzáférjen az OT-környezethez. A technikával kapcsolatban a MITRE zsarolóvírus-támadásokat hoz fel példaként, ahol az eredetileg a szervezet irodai informatikai környezetébe (IT-ba) bejuttatott vírussal, az OT kompromittálása után sikerült megfertőzni az ipari környezetet is, ami egy újabb példa annak igazolására, hogy a legtöbb támadás az IT-zónából szivárog át az OT-ba.[6]

External remote services. A technika lényege, hogy a távelérést biztosító szolgáltatások feltörése útján szereznek hozzáférést a felügyeleti rendszerekhez, és hajtanak végre támadásokat. Erre a MITRE példaként hozza fel a VPN-hozzáférések felderítését és kompromittációját, főként valamilyen külső, a szervezet által nem ellenőrzött gépről való elérés vagy nem megfelelő konfiguráció esetén. Ennek megfelelően a célpontok között felsorolták a VPN-szervert is.[7]

Remote services. A fenti technika a külső távelérésre, ez viszont már a belső hálózaton belüli távelérésre is jellemző, és példaként hozza fel a távoli asztali protokollokat (például *remote desktop protocol,* RDP), a *server message block* (SMB) protokollt, vagy a *secure shell* (SSH) protokollt is. A MITRE példaként hozza fel ezen megoldások kihasználását fájlátvitelre és kódfuttatásra az IT-zónában kompromittált eszközről az OT-környezetbe. A technika egyik fontos tanulsága, hogy ne használjunk olyan *dual-home* megoldást, amelyen keresztül a távelérési megoldást kihasználva támadják az ipari rendszereket.[8]

Discovery kategória

Remote system discovery. A hálózaton lévő eszközök valamilyen (például IP-cím, *hostname*) logikai azonosító alapján felderíthetők, így további eszközök kompromittálódhatnak. A MITRE a statikus hálózati konfigurációt javasolja kockázatcsökkentő

[5] Alexander–Belisle–Steele et al. 2020: 7.
[6] MITRE 2025.
[7] MITRE 2025.
[8] MITRE 2025.

intézkedésként, ami az OT-környezet esetében még egyszerűbben is megvalósítható, hiszen ott gyakoribbak a statikus eszközök.[9]

Remote system information discovery. A távoli elérést biztosító megoldások és azok konfigurációjának feltérképezésével a támadók információt gyűjthetnek a különböző szabályozásokkal, viselkedési mechanizmusokkal kapcsolatban. Ezen keresztül látható a támadó számára, hogy a céljainak megfelelő célpontot talált-e.[10]

Lateral movement kategória

Amikor a támadó érvényes felhasználónévvel és jelszóval (például egy VPN-fiókhoz) bejut a vállalati hálózatba, az elsődleges célja, hogy minél mélyebbre jusson, és minél magasabb jogosultságokat szerezzen. Ezt a folyamatot nevezik oldalirányú mozgásnak *(lateral movement)*. A CrowdStrike 2025-ös Globális Fenyegetettségi Jelentése[11] szerint a támadók rendkívül gyorsak: a kezdeti behatolást követően átlagosan mindössze 48 perc alatt megkezdik az oldalirányú mozgást a hálózaton. A leggyorsabb mért *breakout time* pedig mindössze 51 másodperc volt. Ez a szűk időablak hatalmas nyomást helyez a védelmi csapatokra, hogy a behatolást szinte azonnal észleljék, és megállítsák.[12]

Az oldalirányú mozgás kategóriába eső technikák általánosságban a távelérést biztosító rendszerek kompromittációjának lehetőségeit tartalmazzák, amelyet kihasználva a támadó képes továbbmenni a környezetben, további zónákban lévő eszközök elérése érdekében, ezért a MITRE ICS mátrixában szereplő összes ilyen technikát felsorolom.[13]

Default credentials. Az alapértelemezett jelszavak gyakoriak, főként a programozható logikai kontrollerek (*programmable logic controller,* PLC) és ember-gép interfészek (*human-machine interface,* HMI) esetében. Ezeket a kockázatokat hozzáférés-kezeléssel és jelszószabályok *(policy)* megfelelő kialakításával csökkenteni lehet.

Exploitation of remote services. Azonos az *initial acces* kategóriában lévő azonos nevű technikával.

Hardcoded credentials. A szoftverek vagy *firmware*-ek kódjai tartalmazhatnak olyan alapértelmezett jelszavakat, kriptográfiai kulcsokat, vagy API-kulcsokat *(API-token)*, amelyeket felfedve a támadó jogosulatlanul szerezheti meg a felhasználói munkamenetet *(session)*. Ezeket gyakran az adatgazdák sem ismerik, vagy nehéz módosítani azokat, mert ez rossz hatással lehet az üzemmenetre. Ezek az azonosítók a gyártók, modellek esetében ugyanazok szoktak lenni. Ezért a hozzáférés-menedzsment részévé kell tenni ezen kulcsok, azonosítók kezelését is.

Lateral tool transfer. A támadók a fájlmegosztó-protokollok sérülékenységeit vagy rossz konfigurációt kihasználva képesek fájltranszfereket végezni, amivel támadó

[9] MITRE 2025.
[10] MITRE 2025.
[11] Crowdstrike 2026.
[12] Frész 2025.
[13] MITRE 2025.

kódokat is képesek átültetni további rendszerekbe. Ennek végrehajtására a támadók a távoli elérések sérülékenységeit is kihasználják.

Program download. Protokollsérülékenység kihasználásával a támadó képes programletöltésre vagy -módosításra az eszközökön (például PLC-ken és kontrollereken). Kockázatcsökkentő intézkedés az alkalmazás naplózása, illetve a letöltések és módosítások monitorozása.

Remote services. Azonos az *initial access* kategóriában lévő azonos nevű technikával.

Valid accounts. A támadók valósnak hitt felhasználókként képesek a távoli elérést biztosító megoldáson keresztül bejutni a belső hálózatba. Ennek egyik megelőzési lehetősége többek között a többtényezős hitelesítés (*multi-factor authentication,* MFA), a felhasználói fiókok megfelelő menedzsmentje vagy a hálózati forgalom szűrése is.

A cikk további részében azt is megvizsgálom, hogy a fenti támadási technikák alkalmazhatók-e a ZTNA-megoldások használata esetén.

A ZTNA-megoldások rövid története

A *soha ne bízz, mindig ellenőrizz* (*zero trust,* ZT) elv régóta ismert, gyakorlati megvalósítására számos technológiai megoldás lehetőséget adott az utóbbi évtizedekben. Ezek a technológiák alapvetően egy-egy informatikai terület esetében biztosították ezt az elvet, így számos különálló megoldást kellett párhuzamosan implementálni és üzemeltetni ahhoz, hogy a szervezet a lehető legtöbb területen elérje a *zero trust* elv szerinti működést.

A hálózati szegmentációval a szervezet jelentősen csökkentette annak kockázatát, hogy egy támadó több szervezeti egység gépeit is elérje, például nem jutott át más virtuális helyi hálózatokba (*virtual local area network,* VLAN), így kevesebb kárt tudott okozni. Azonban így is, az adott hálózati szegmensen belüli felhasználói tevékenységek ezzel még nem kontrolláltak, legfeljebb naplózottak.

A *zero trust* architektúra (*zero trust architecture,* ZTA) is egy adott területre összpontosít – a hálózati forgalmon valósítja meg a *zero trust* elvet –, amivel a hálózati szegmentációnál is egy magasabb szintre emeli a biztonságot és az elvnek való megfelelést. A *zero trust* architektúra szerint „semmilyen felhasználó vagy eszköz nem tekinthető alapértelmezetten megbízhatónak, függetlenül attól, hogy a hálózaton belül vagy kívül található. Minden egyes hozzáférési kísérletet szigorúan ellenőrizni és hitelesíteni kell."[14]

A ZTA-elvnek való megfelelést a NIST SP 800-207 számú publikáció[15] is segíti (a továbbiakban, ahol külön nem hivatkozom, ebből a munkából indulok ki), amely meghatározza a ZTA kialakításához szükséges követendő alapelveket. Az alpontokban lévő magyarázatok a távelérések kapcsán is fontos követelmények, akár az OT-ban is.

- Minden adatforrást és szolgáltatást erőforrásként kell kezelni:
  - például a magánkézben lévő vagy külső harmadik félnél, például külső szerződéses karbantartóknál lévő eszközök is ilyen erőforrások, amennyiben

[14] Frész 2025.
[15] Rose et al. 2020: 6.

azokkal szervezeti erőforrások érhetők el. Az OT-ban gyakori a tranziens eszközök használata, amelyek felett a szervezet nem gyakorol kontrollt, nincs nyilvántartva, ezért nem kontrollálandó erőforrásként kezeli, pedig támadási felületet jelent az OT-hálózat számára.

- A hálózattól függetlenül minden kommunikációt biztonságossá kell tenni:
  - attól, hogy egy eszköz a szervezet által menedzselt hálózatban van vagy azon kívül, nem tekinthető megbízhatónak, minden kommunikációs csatornán védeni kell az adatok bizalmasságát és sértetlenségét. Az OT-ban a kommunikációs csatornákkal kapcsolatos legfőbb probléma a titkosítatlan kommunikációs protokollok használata.
- Munkamenet (session) alapon kell megadni a hozzáférést az egyes erőforrásokhoz:
  - a távelérések kapcsán is fontos követelmény a session alapú hozzáférés engedélyezése, ilyenkor a rendszer csak egy adott szolgáltatásához adunk hozzáférést, amivel szintén szűkíthetjük a jogosultságokat.
- Dinamikus szabályokkal kell kezelni az erőforrásokhoz való hozzáféréseket:
  - a dinamikus szabályok esetében (policy) az eszköz olyan tulajdonságait kell figyelembe vennie, mint az idő, szoftververzió, lokáció vagy különböző viselkedési tulajdonságok. Ezek az OT távelérésében is szerepet játszhatnak a külső hálózatokból csatlakozó eszközök tulajdonságainak megfigyelésére.
- Minden eszköznek monitorozni és mérni kell az integritásra, rezilienciára vonatkozó képességeit:
  - a távoli felhasználók esetében más típusú tulajdonságokat lehet szükséges meghatározni, mint a belső hálózaton lévők esetében, például egy, a szervezet által nem menedzselt külső karbantartó eszközéről a végpontvédelmi rendszer frissítéseit is javasolt felülvizsgálni, hiszen az eszközön nem a szervezet kezeli a vírusadatbázis frissítéseit.
- Dinamikus autentikációs és authorizációs folyamatokat kell kialakítani minden erőforrás esetében:
  - ennek megvalósítását segítik az IAM *(identity and access management)* rendszerek és eszközmenedzsment-rendszerek, a többtényezős hitelesítés (MFA), amelyek közül a külső felek távelérése esetében korlátozottak a lehetőségek – a nem menedzselt eszközök a legtöbb esetben nem rendelkeznek a szervezet által használt rendszerek klienseivel.
- Adatgyűjtés és -elemzés:
  - a lehető legtöbb adatot be kell gyűjteni annak érdekében, hogy minél pontosabb szabályokat (policy) lehessen meghatározni, és folyamatosan fejleszteni az egyes erőforrásokra, ami a távoli felhasználók esetében a lokációra vonatkozó tulajdonságok esetében már nehezebben használható.

Zero trust network access (ZTNA)

Az OT fejlődése megköveteli a biztonságának fejlesztését is. Egyre nagyobb az igény a felügyeletre, az adatvezérelt gyártásra (ipar 4.0, IIoT) egyre több IT/OT-kapcsolat

kiépítését követeli meg, a szakértők, karbantartók egyre többször használnak távelérést. Ezek a fejlesztések biztonsági szempontból támadási felületként jelentkeznek, amelyekre egyre több és hatékonyabb védelmi intézkedést kell kialakítani. Az OT számára is egyre fontosabb lesz a jelenleg még inkább csak az IT-ban alkalmazott kiberbiztonsági elvek, gyakorlatok alkalmazása. Ugyanakkor az IT/OT-konvergencia megteremtése segíti a szervezetben összhangba hozni a két terület kiberbiztonsági képességeit is. Ezért fontos vizsgálni a távoli elérések fejlesztési lehetőségeit is az OT-ban, akár egy *zero trust network access* (ZTNA-) megoldás implementációs lehetőségeinek vizsgálatán keresztül.

A *zero trust* architektúra elvére építve a *zero trust network access* (ZTNA-) megoldások gyakorlati megvalósítását kínálják a biztonságos távelérésnek. A ZTNA nemcsak egy szoftveres funkció, hanem architekturális megoldás is, amely megvalósítja a távoli felhasználók beléptetését, validálja azok biztonsági állapotát *(security posture)*, elrejti az erőforrásokat a felderítéstől *(discovery)*, megakadályozza az oldalirányú mozgásokat *(lateral movement)*, kikényszeríti a felügyeleti szabályokat *(policy)*.

A ZTNA-megoldások nem VPN-alapon működnek, hanem a távoli kliens egy felhős vagy helyi *(on-premise)* brókerhez csatlakozik *(trust broker)*, amelyen keresztül megtörténik az autentikáció, a jogosultságok kiosztása, a protokoll kiválasztása, az időintervallum megadása stb. A bróker egy ZTNA-útválasztóval *(gateway)* kommunikál.

A ZTNA tulajdonságai, előnyei

A jelenleg széles körben használt VPN és annak kiváltási lehetőségeként vizsgált ZTNA-megoldások megismerése után vizsgáljuk meg a ZTNA főbb tulajdonságait és előnyeit, illetve vessük össze a VPN funkcionalitásával!

- Míg a VPN perimeter védelmi megközelítésen alapul, és a teljes hálózathoz enged hozzáférést, addig a ZTNA a zero trust elvre építve biztosítja a mikroszegmentációt, illetve a legkisebb jogosultság *(least privilege)* elvnek való megfelelést.[16]
- A VPN IP-alapú autentikációt, a ZTNA identitás alapú autentikációt valósít meg.[17]
- Legkisebb jogosultság elvének való megfelelés: alkalmazásra korlátozva, adott munkamenetre ad jogosultságot a távoli felhasználónak.[18]
- Folyamatos ellenőrzés *(continous verification)* a távoli eszközön is: operációs rendszer (*operating system,* OS) verzió, antivírusprogram utolsó frissítése, titkosítás alkalmazása (például bitlocker), rosszindulató szoftver *(malicious software, malware)* detekció stb.[19]
- Mivel a szervezet által nem felügyelt eszközök esetében nagyobb a kockázata annak, hogy kompromittált eszközről csatlakoznak a szervezet hálózatába, ezért a ZTNA által nyújtott funkcionalitás mellett a szervezet által nem menedzselt (például BYOD, tranziens) eszközök használatának is kisebb a kockázata.

[16] Mavroudis 2024: 1.
[17] Mavroudis 2024: 3.
[18] Mavroudis 2024: 3.
[19] Mavroudis 2024: 3.

Természetesen VPN-használat esetében is lehetősége van a szervezetnek valamilyen szintű felügyeletre, például ellenőrizheti az eszközön futó legutóbbi vírusellenőrzés dátumát, de ez többletmunkával és feltételekkel jár.[20]

- Auditálhatóság és megfelelés *(compliance):* a központi menedzsmenten keresztül könnyebben és hatékonyabban kezelhetők, felügyelhetők és ellenőrizhetők a szabályok.
- Központi naplógyűjtő- és elemző (*security information and event management,* SIEM) / Műveleti központ (*Security Operational Center,* SOC) integráció: a ZTNA naplói szintén beköthetők központi naplógyűjtő és -elemző (SIEM-) rendszerbe, így hatékonyabbá tehető az incidenskezelés is.
- *Agent* és *agentless* működés is támogatott: a kialakítás lehet felhős vagy *on-prem* is.[21]
- Felhasználóbarát: ZTNA-val nem kell kliensszoftvert telepíteni a gépekre, nem kell kiépíteni a kapcsolatot, mint a VPN esetében, elegendő böngészőn keresztül bejelentkezni a felhős szolgáltatásba.

1. táblázat: A VPN és ZTNA főbb különbségeinek összefoglalása

	VPN	**ZTNA**
Biztonsági funkciók	Biztonságos alagutat biztosít a felhasználó eszköze és a vállalati hálózat között	Testreszabható hozzáférés-vezérlési szabályok
Bizalmi modell	Egyszeri ellenőrzés, perimeter védelem	Dinamikus ellenőrzés, nemcsak a perimeteren, hanem a teljes belső hálózaton belül is
Hozzáférés-biztonsági modell	Az egész hálózathoz való hozzáférés biztosítása	Hozzáférés adott alkalmazásokhoz munkamenetalapon; testreszabhatóság a felhasználói viselkedések alapján (az eszköz állapota és az alkalmazás érzékenysége alapján)
Hitelesítés	Hagyományos módszerek (pl. felhasználónév és jelszó)	A felhasználó hitelesítése hagyományos módszerekkel, az eszközé pedig tanúsítványokkal

Forrás: Fortinet 2025

A ZTNA-architektúra megvalósítási lehetőségei

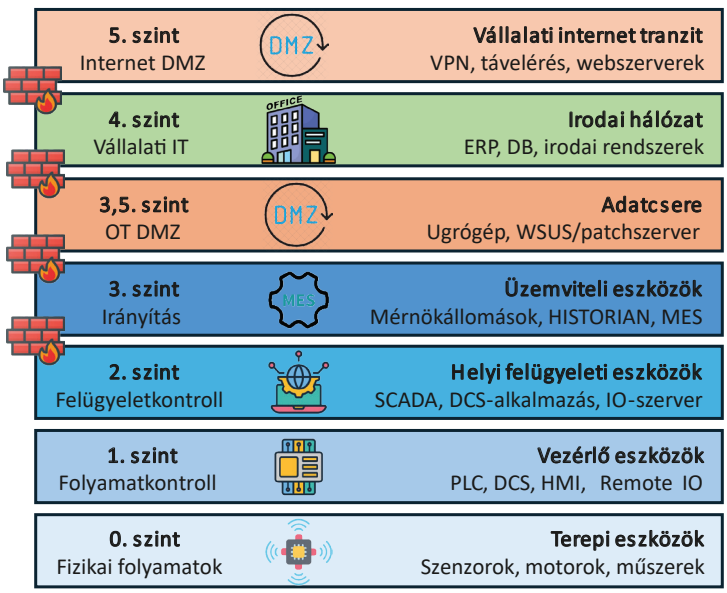
A fejezet egyik célja kideríteni, hogy a jelenleg elérhető, alapvetően IT-infrastruktúrára tervezett ZTNA-megoldások OT-ba való implementálása milyen kihívásokkal járhat, akkor, ha az OT-környezetet valamilyen mértékben a PERA-modell szerint építették ki.

[20] Mavroudis 2024: 7.
[21] Mavroudis 2024: 5.

Implementáció PERA-modell szerint épített architektúrába

Az OT-ban hálózati architektúra kialakításánál követendő modell a *Purdue Enterprise Reference Architecture* (PERA). A *Purdue*-modell szerinti szabályokat az OT-infrastruktúrát távolról elérni kívánó felhasználóra is vonatkoztatni kell. A megvalósítás többféleképpen történhet, de az alapvető szabályok, amelyekre törekedni kell, az alábbiak:

- A távoli elérést közvetlenül az OT-környezetbe végződtetni nem javasolt.
- Zónaátlépések ellenőrzése: a zónák közötti átjárásokat kontrollálni kell.
- Egyet le, egyet fel szabály: egyszerre csak egy zónába lehet fel- vagy lelépni. Ennek vonatkozása a távelérés tekintetében az, hogy a távoli felhasználót nem terminálhatjuk, érkeztethetjük közvetlenül egy alsóbb zónába.



1. ábra: PERA-modell
Forrás: The Claroty Team 2023

A napjainkban javasolt kialakítás demilitarizált zóna (*demilitarized zone,* DMZ) használatával javasolt, ahol a PERA szerinti 3,5. (OT DMZ) és/vagy az 5. zónában (IT-internet DMZ-je) van kialakítva DMZ. A DMZ alkalmazása többféleképpen is történhet, de az alapvető előnye, hogy a távoli elérést ide lehet végződtetni. A két tűzfal között elhelyezett DMZ-be lehet elhelyezni azt az ugrógépet *(jump host)*/terminálszervert, amelyen keresztül a felhasználó az alsóbb zónákba ugorhat. A DMZ tartozhat az OT-hoz, de az IT DMZ-n keresztül is megvalósítható a távelérés. Az alábbi két példa szemlélteti a DMZ kialakításának lehetőségeit:[22]

[22] Andersson 2023: 7.

- OT DMZ: amikor az OT-nak saját DMZ-je van, akár külön a távelérésre dedikáltan *(remote access DMZ).* Javasolt ide végződtetni a VPN-t, és elhelyezni azt az ugrógépet, amelyen keresztül elérhető a hármas zóna. A hármas zónából szintén ugrógéppel javasolt elérni a kettes zónában lévő felügyeleti eszközöket.
- IT (internet) DMZ: ebben az esetben az ötös zónában lévő IT DMZ tölti be az OT DMZ szerepét. Az IT DMZ-t külön tűzfal választja el a hármas zónától, amelyben szintén ugrógépeken keresztül juthatunk le a kettes zónába.

ZTNA-implementációs lehetőségek architekturális szempontból

Természetesen az infrastruktúra adottságaitól függően többféleképpen is megvalósítható az implementáció, az alábbiakban bemutatok néhány szcenáriót.

OT DMZ. Az OT implementáció legvalószínűbb architekturális megvalósítása, hogy a ZTNA *gateway* az OT DMZ-ben (*industrial* DMZ, L3,5) kap helyet, vagyis:

- a felhasználó VPN-n helyett ZTNA-megoldással terminálódik a DMZ-be.
- A DMZ-ből az OT-hálózatba már a megszokott módon, például ugrógépeken keresztül érheti el az alsóbb zónákat.
- Amennyiben az IT-ból való elérést is távoli elérésnek tekintjük, úgy lehetséges a ZTNA gateway-en keresztül elérni az IT-ból is az OT DMZ-t.

Előnyök:

- A VPN helyett egy jobban kontrollált és könnyebben menedzselhető megoldást használhat az OT, miközben az OT-hálózati működés nem változik, így kisebbek a működési és implementációs kockázatok, illetve költségek is.
- Nem szegjük meg a PERA-modell szerinti szabályokat.

Internet DMZ. Amennyiben a szervezet nem rendelkezik OT DMZ-vel, úgy az IT-internet DMZ-jébe is telepíthető a ZTNA *gateway,* ahonnan ugrógépen érhető el a 3. zóna (L3). Ez esetben egyszerre az IT és OT használatra is alkalmazható a megoldás, ami kedvezőbb lehet a szervezet számára.

DMZ-to-DMZ. A szervezet az internet DMZ-ben lévő *gateway-nek* ad elérést az OT DMZ-ben lévő ugrógéphez, vagy egy ott lévő másik *gateway-hez.*

OT belső hálózat. A fenti példák mellett egy másik megközelítés, hogy a *gateway-eket* az OT-hálózatba is implementáljuk: az alsóbb zónákban lévő *gateway-ek* kommunikálnak egymással, így az OT-hálózaton belül az ugrógépeket váltjuk ki ZTNA-eszközökkel. Ehhez hasonló megoldással már rendelkezik a Cisco, amely a saját ipari útválasztóiba *(switch)* integrálta a ZTNA-alkalmazást.[23]

[23] Lobo 2023.

ZTNA-implementációs kihívások az OT-ban, ZTA-implementációs követelményeken keresztül vizsgálva

A NIST SP 800-207 publikáció alapján a ZTA kialakításának támogatásához az alábbi hálózati követelményekkel kell rendelkeznie az OT-nak. A ZTNA-megoldások implementálásának tekintetében az alábbi szempontok szintén fontosak. Az alpontokban az OT sajátosságaiból eredő problémákon keresztül lehet képet kapni a ZTNA implementációjának kihívásairól az OT-ban:

- Az objektumoknak *(enterprise assets)* alapvető hálózati kapcsolattal kell rendelkezniük.[24]
  - Az OT-eszközök hálózati kapcsolataival kapcsolatos probléma lehet, hogy nem képesek TCP/IP-protokoll szerinti *(transmission control protocol)* kommunikációra, például csak ModBUS-protokollon vagy egyéb módon érhetők el, IP-címük nincs.
- A szervezetnek meg kell tudnia különböztetni, hogy mely eszközök tartoznak a vállalathoz, és fel kell mérnie azok biztonsági állapotát.[25]
  - Az OT-nak részletes eszközleltárral kell rendelkeznie, amelynek olyan tulajdonságokat is tartalmaznia kell, amely alapján megállapítható, hogy az eszköz képes-e a ZTNA-megoldással való együttműködésre. Az elavult *(legacy)* eszközök és alkalmazások nem képesek megfelelően kommunikálni a ZTNA-*gateway-jel*.[26]
- A hálózaton le kell tudni követni minden adatforgalmat.[27]
  - A szabályok *(policy)* pontosabb létrehozása érdekében minél több metaadatot ki kell tudni nyerni az eszközökből és a velük történő kommunikációból. Ez OT-ban gondot okozhat a szűkös erőforrásokkal rendelkező eszközök esetében, és növelheti a késleltetést *(latency)* is.[28]
- A vállalati erőforrások nem érhetők el anélkül, hogy szabályokat kikényszerítő megoldáson (*policy enforcement point* [PEP], ami a ZTNA esetében a gateway) keresztül történne a hozzáférés.[29]
  - Ehhez minden távoli felhasználónak a ZTNA-*gateway-en* keresztül kellene haladnia. OT-ban egyes gyártók gyakran saját távoli menedzsmentmegoldást adnak a termékeikhez, *machine-to-machine* VPN-megoldással. Ezek PEP-en keresztüli megvalósítása akadályokba ütközhet.
- Az adatsík és a vezérlési sík logikailag el kell legyen választva.[30]
  - Az OT-menedzsment interfészeket külön menedzsment VLAN-ban kell szeparálni az OT tényleges üzemi rendszereinek interfészeitől.
- Az objektumoknak el kell érniük a PEP komponensét.[31]

[24] Rose et al. 2020: 6.
[25] Rose et al. 2020: 6.
[26] Mavroudis 2024: 7.
[27] Rose et al. 2020: 6.
[28] Mavroudis 2024: 6.
[29] Rose et al. 2020: 6.
[30] Rose et al. 2020: 6.
[31] Rose et al. 2020: 6.

  - A távolról elérni kívánt OT-eszköznek el kell érnie a ZTNA-*gateway-t,* és tudnia kell vele kommunikálni. Ez esetben is problémát okozhat az OT-ban gyakran jelen lévő elavult eszköz, amely nem feltétlenül lesz képes kapcsolatot kiépíteni a *gateway-jel*.
- A PEP az egyetlen komponens, amely hozzáfér a *policy administratorhoz (trust brokerhez)* az üzleti folyamat részeként.[32]
  - A ZTNA-megoldások kialakításukból fakadóan teljesítik a követelményt. Ezért a jelen szempontokat figyelembe véve adott a követelmény teljesítése.
- A távoli vállalati eszközöknek hozzá kell férniük a vállalati erőforrásokhoz anélkül, hogy előbb a vállalati hálózatot kellene használniuk.[33]
  - A ZTNA-megoldások esetében a távoli felhasználónak nem kell először a belső hálózatot elérnie, és onnan elérnie egy felhőszolgáltatást (például e-mail), mintha *full-tunnel* VPN-t használna. Ehelyett a ZTNA-*gateway* hitelesíti a távoli felhasználót, ahonnan egyből a privát felhőbe terminálható, a belső hálózat érintése nélkül.
- A ZTA-hozzáférési döntési folyamatot támogató infrastruktúrának skálázhatónak kell lennie a változó terhelési igényekhez.[34]
  - A ZTNA-megoldást alkotó komponenseket úgy kell tervezni, hogy képesek legyenek kiszolgálni a nagyobb számban érkező kéréseket. Mivel a távoli hozzáférések tekintetében ezek a komponensek szűk keresztmetszetek *(bottleneck)*, ezért biztosítani kell a magas rendelkezésre állásukat.
- Bizonyos esetekben a vállalati eszközök nem érhetnek el bizonyos PEP-eket a szabályzat vagy megfigyelhető tényezők miatt.[35]
  - A ZTNA esetében a szabályok beállítása révén bármilyen feltétel szabható, például külföldi lokáció esetén a *gateway* megszakítja a kommunikációt.

Tehát a fenti szempontok figyelembevételével megállapítható, hogy az OT-környezetbe való implementáció gyakran költséges akadályokba ütközhet, ami miatt a szervezeteknek érdemes átgondolniuk egy ilyen projekt elindítását.

Következtetések

A kutatás alapján megállapítható, hogy az OT távoli elérésére jelenleg biztonságosnak tartott és gyakorlatban gyakran használt megoldás a VPN. Azonban a VPN-megoldások számos sérülékenységgel rendelkezhetnek, amelyekkel támadási felületet adnak a támadók számára, így releváns kérdésként merül fel a VPN kiváltására alkalmas megoldás keresése és vizsgálata.

A ZTNA-megoldások a vizsgálat alapján valóban képesek a VPN-megoldások kiváltására, és nagyobb biztonságot képesek nyújtani a távoli elérés biztosítására.

[32] Rose et al. 2020: 6.
[33] Rose et al. 2020: 6.
[34] Rose et al. 2020: 6.
[35] Rose et al. 2020: 6.

Mindez az OT-környezetben ugyanakkor jelentős kihívásokat tartogathat az OT-környezetben lévő eszközök, és általában az OT technológiai lemaradottsága miatt.

A ZTNA-megoldás bevezetése hatékonyabb szegmentációt, erősebb autentikációt, nagyobb vizibilitást, könnyebb kezelhetőséget jelenthet az OT számára. Azonban a szervezetnek mérlegelnie kell a bevezetéssel kapcsolatos OT-működtetési kockázatokat, költséghatékonyságot. Az alábbiakban összefoglaltam a főbb szempontokat.

Fokozatos bevezetés. Javasolt fokozatosan bevezetni: egyszerre csak egy gyártó egy-két eszközének elérésével javasolt tesztelni az implementációt. Közben pedig fokozatosan le kell építeni a VPN-megoldásokat, törekedni kell arra, hogy a ZTNA-*gateway* legyen az egyetlen bejárat az OT-hálózat felé.

Ár-érték arány. Meg kell vizsgálni, hogy a jelenleg kiépített infrastruktúra milyen kockázatokat rejt magában, és ezeken milyen költségek árán, mennyit segíthet az implementáció. Egy jól kialakított és felügyelt környezet esetében nem biztos, hogy a ZTNA-bevezetés a költségeket is figyelembe véve kockázatarányos döntés lenne.

Az implementációt lehetővé tevő körülmények vizsgálata. A szervezetnek meg kell vizsgálnia, hogy a jelenlegi környezetben működő eszközök/megoldások rendelkeznek-e azokkal a tulajdonságokkal, amelyek lehetővé teszik az implementációt – egy elavult megoldásokat tartalmazó infrastruktúrát nagymértékben fejleszteni kellene ahhoz, hogy képes legyen a ZTNA-funkciók támogatására, ami aránytalanul magas költségeket eredményezhet.

Felhasznált irodalom

Alexander, Otis – Belisle, Misha – Steele, Jacob (2020): *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. Bedford, MA, USA: The MITRE Corporation.

Andersson, Niklas (2023): *The Effect of the IT/OT Gap on the NIS 2 Implementation*. Szakdolgozat. Stockholm: Stockholm University Department of Computer and Systems Sciences. Online: https://su.diva-portal.org/smash/record.jsf?pid=diva2%3A1784461&dswid=5127

CrowdStrike (2026): *CrowdStrike 2026. Global Threat Report.* Online: www.crowdstrike.com/en-us/global-threat-report/

Dragos (2025): *2025 OT. Cybersecurity Action Guide.* Online: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos_2025_OT_Cybersecurity_Global_Action_Guide.pdf?hsLang=en

Fortinet (2025): *ZTNA vs VPN – What's The Better Cybersecurity Solution?* Online: www.fortinet.com/resources/cyberglossary/ztna-vs-vpn

Frész Ferenc (2025*):* Milliárdnyi kiszivárgott hitelesítő adat. *Substack,* 2025. június 19. Online: https://substack.com/@ferencfresz/p-166319450

Kocsis Tamás (2025): *Ipari (OT) kiberbiztonsági szakember képzés*. Óbudai Egyetem Neumann János Informatikai Kar, prezentáció.

Lee, Robert M. – Conway, Tim (2022): *The Five ICS Cybersecurity Critical Controls.* SANS. Online: https://sansorg.egnyte.com/dl/R0r9qGEhEe

Lobo, Ruben (2023): Zero Trust Network Access (ZTNA) – Revolutionizing Remote Access Security Across OT Environments. *Industrial Cyber,* 2023. december

3. Online: https://industrialcyber.co/zero-trust/zero-trust-network-access-zt-na-revolutionizing-remote-access-security-across-ot-environments/
MAVROUDIS, Vasilios (2024): Zero-Trust Network Access (ZTNA). *arXiv:2410.20611*. Online: https://doi.org/10.48550/arXiv.2410.20611
MITRE Corp. (2025): *ICS Matrix*. Online: https://attack.mitre.org/matrices/ics/
ROSE, Scott et al. (2020): *Zero Trust Architecture*. NIST Special Publication 800–207. Online: https://doi.org/10.6028/NIST.SP.800-207
The Claroty Team (2023): *ICS Security: The Purdue Model.* Online: https://claroty.com/blog/ics-security-the-purdue-model
ZAYTSEV, Alexey (2023): OT Remote Access: Can You Trust Your Technician's Laptop? *Cisco Blogs,* 2023. november 9. Online: https://blogs.cisco.com/industrial-iot/ot-remote-access-can-you-trust-your-technicians-laptop