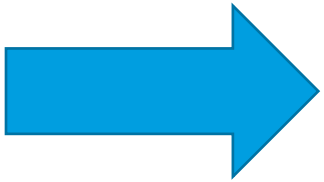
A ZERO TRUST MODEL AZ MNB IT AJÁNLÁSAINAK TÜKRÉBEN

MI A ZERO TRUST MODEL?

Bízz, de ellenőrizz!



Ne bízz senkiben, mindig ellenőrizz!

John Kindervag - Forrester Research Insitute 2010

Forrester Research, Inc. by John Kindervag: No More Chewy Centers: Introducing The Zero Trust Model Of Information Security
Forrester Research, Inc. by John Kindervag: Build Security Into Your Network's DNA: The Zero Trust Network Architecture

A ZERO TRUST MODEL ALAPELVEI

1) Minden erőforráshoz kizárólag biztonságos módon (hitelesítés, megfelelő jogosultság kiosztás, titkosítás) lehet hozzáférni, helytől függetlenül (külső, belső hálózat).

2) Az erőforrásokhoz való hozzáférés a legkisebb jogosultság elvén alapul, és minden alkalommal ellenőrzésre kerül.

3) Az összes forgalmat valós időben és folyamatosan naplózni kell és széleskörű analitikai vizsgálatoknak alávetni.

Forrás | MNB

NIST - ZERO TRUST ARCHITECTURE (ZTA)

NIST Special Publication 800-207 - **Zero Trust Architecture**

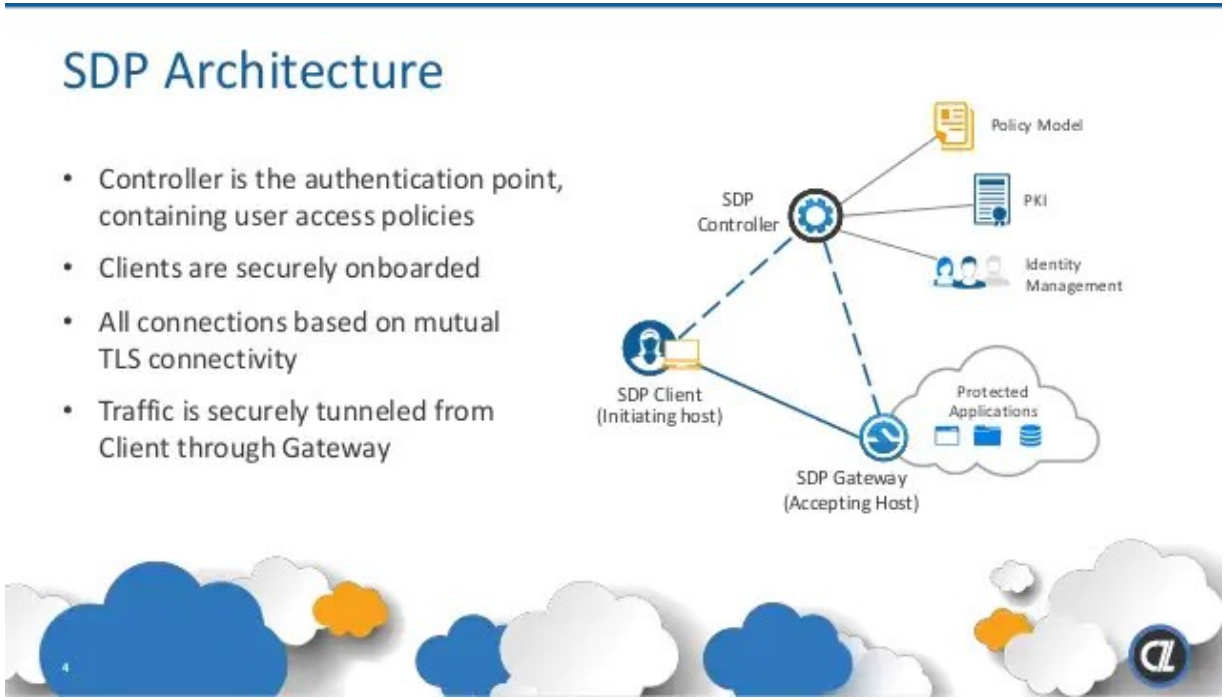
1. Minden adatforrást és informatikai szolgáltatást azonosítani kell.
   - Adatok, eszközök, szolgáltatások nyilvántartása, osztályozása

2. Minden kommunikációt biztonságossá kell tenni a hálózati helyétől függetlenül.
   - Külső és belső hálózatok egyenrangúak (megbízhatatlanok)
   - Minden kommunikáció titkosított
   - Integritás ellenőrzés

3. Az egyes vállalati erőforrásokhoz való hozzáférés munkamenet alapon történik.
   - Még a hozzáférés megadása előtt szükséges megvizsgálni annak jogosságát
   - Software Defined Perimeter (SDP)/Zero Trust Network Access (ZTNA) (CSA SDP Architecture Guide)

Forrás | MNB

NIST - ZERO TRUST ARCHITECTURE (ZTA)



Forrás:Cryptzone

- A szolgáltatások, alkalmazások csak a jogosultaknak láthatók/elérhetők
- Személyazonosság ellenőrzés (több faktoros, MFA)
- Eszköz hitelesítés (kölcsönös)

Forrás | MNB

NIST - ZERO TRUST ARCHITECTURE (ZTA)

3. Az egyes vállalati erőforrásokhoz való hozzáférés munkamenet alapon történik. (folyt.)
   - Legkisebb jogosultság elve
   - Mikroszegmentáció
     - Alkalmazások, szervizek csoportosítása
     - Software Defined Network (SDN) alkalmazása
     - A támadó belső mozgásának korlátozása
   - Minden egyes hozzáféréskor a kiosztandó jogok teljeskörű újbóli ellenőrzése szükséges
   - Az egyik erőforrás elérése nem jelenthet egy másikhoz való automatikus hozzáférést
4. A vállalati erőforrásokhoz való hozzáférést a dinamikus házirend - beleértve az ügyfél, az alkalmazás/szolgáltatás és a kérelmező eszköz megvizsgált és kiértékelt állapotát -, valamint egyéb viselkedési és környezeti jellemzők határozzák meg.
   - Felhasználó viselkedés analitika (UBA)
   - Kliens/szolgáltatás által indított ZTNA

Forrás | MNB

NIST - ZERO TRUST ARCHITECTURE (ZTA)

5. A vállalat monitorozza és méri az összes saját- és harmadik fél tulajdonában lévő eszköz integritását és biztonsági állapotát.
   - SIEM, IPS/IDS, CASB …
   - Folyamatos diagnosztika és IT biztonsági ellenőrzés
   - Eszköz biztonsági állapotának vizsgálata (vírusvédelem, biztonsági javítások)

6. Minden erőforrás-hitelesítés és engedélyezés dinamikus, és szigorúan kikényszerítésre kerül a hozzáférés engedélyezése előtt.
   - Eszköz hitelesítés (kölcsönös)
   - Újbóli hitelesítés (reauthentication)

7. A vállalat a lehető legtöbb információt gyűjti össze az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és felhasználja azokat az informatikai biztonsági helyzetének javítására.
   - Mesterséges Intelligencia (AI) és gépi tanulás (ML)alkalmazása
   - Fenyegetettségi információk (Threat Intelligence) alkalmazása
   - Valós idejű monitorozás a kapcsolat létrejötte után is

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

1. Minden adatforrást és informatikai szolgáltatást azonosítani kell.

MNB ajánlás	Megjegyzés
5.2. - Az intézmény rendelkezik naprakész szoftver és hardver nyilvántartással	Az MNB erőforrásokra és szolgáltatásokra vonatkozó ajánlásai lefedik a Zero Trust követelményeit.
5.4. - Az intézmény gondoskodik rendszerei legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról.	
7.2. - Elvárt az üzleti folyamatok adatáramlásainak nyomon követése, a folyamatot támogató kapcsolatok (interfészek) és eszközök azonosítása.	

8/2020 - A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről (továbbiakban 8/2020)
12/2020 - A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről (továbbiakban 12/2020)

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

2. Minden kommunikációt biztonságossá kell tenni a hálózati helyétől függetlenül.

MNB ajánlás	Megjegyzés
7.4 Az intézmény gondoskodik az adatok biztonságáról az adatátvitel során.	A Zero Trust követelményei erősebbek, mivel teljes titkosítást várnak el. Az MNB titkosításra vonatkozó ajánlásainak szélesebb körű alkalmazásával ez teljesíthető.

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

3. Az egyes intézményi erőforrásokhoz való hozzáférés munkamenet alapon történik.

MNB ajánlás	Megjegyzés
9.2. – 9.3 Az intézmény gondoskodik az adatok hozzáférésének szabályozottságáról és rendjéről.	A legkisebb jogosultság elvének a használata, és a hozzáférés szigorú szabályozása és ellenőrzése az MNB ajánlások részei. A hálózat szegmentáció bizonyos mértéke az MNB ajánlásokban megkövetelt, ugyanakkor az erőforrás láthatósága/elérhetősége, illetve az erőforráshoz való kapcsolódás tiltása a jogosultság kiosztása előtt a Zero Trust modell sajátossága, ami az MNB ajánlásokban nem szerepel.
7.4.4. a) Az intézmény a belső hálózatán lévő informatikai rendszereihez (beleértve a virtuális privát hálózati vagy levelező rendszereket is) történő csatlakozást csak engedélyezett felhasználók és eszközök számára, csak központi megoldáson keresztül, csak a szükséges mértékig és a szükséges eszközök eléréséhez biztosítja.	
7.5.1. Az MNB elvárja, hogy a hálózati kapcsolatok – beleértve a hálózati szegmensek közötti átjárásokat – úgy kerüljenek kialakításra, hogy azokon mindenkor csak az üzletileg indokolt és engedélyezett forgalom haladjon át.	

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

4. Az erőforrásokhoz való hozzáférést a dinamikus házirend - beleértve az ügyfél, az alkalmazás/szolgáltatás és a kérelmező eszköz megvizsgált és kiértékelt állapota -, valamint egyéb viselkedési és környezeti jellemzők határozzák meg.

MNB ajánlás	Megjegyzés
9.4. Az intézmény szabályozza, nyilvántartja, ellenőrzi a végfelhasználói hozzáférést.	A távoli hozzáférésnél a viselkedés alapú vizsgálat és a dinamikus környezeti változók változásainak figyelése az MNB 12/2020 ajánlása 7.f) pontjában már megtalálható.
7. e) az intézmény határozza meg a távolról csatlakozó eszközök hozzáférésének módját a belső hálózaton található erőforrásokhoz (pl. terminál szerver, nyomtatók) – és a szükséges mértékben határozzon meg különböző biztonsági szinteket és kapcsolódási típusokat;	
7. f) az intézmény előzetesen határozza meg és rendszeresen vizsgálja felül a működés során elvárt paramétereket (adatkapcsolatok száma, adatkapcsolatok eloszlási ideje és helye, forgalmazott adatmennyiség stb.);	
16. j) az intézmény technikai megoldásokkal is gondoskodjon arról, hogy a belső hálózathoz, illetve erőforrásokhoz hozzáférést biztosító kapcsolat csak az intézmény által jóváhagyott és regisztrált eszközről legyen felépíthető;	

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

5. Az intézmény monitorozza és méri az összes saját- és harmadik fél tulajdonában lévő eszköz integritását és biztonsági állapotát.

MNB ajánlás	Megjegyzés
7.6.3. Az intézmény gondoskodik a védelmi rendszer folyamatos monitorozásáról a támadások mielőbbi - lehetőség szerint automatikus - észleléséről és kezeléséről.	Az eszközök és a kapcsolatok folyamatos monitorozása és figyelése szerves része az MNB ajánlásainak, ami megfelel a Zero Trust model elvárásainak.
28. Az intézmény folyamatosan monitorozza a távoli hozzáféréssel felépített hálózatikapcsolatokat és a rajtuk átfolyó adatfolyamot, és folyamatosan biztosítsa a távoli hozzáféréshez szükséges kapacitásokat;	
11. f). Elvárás, hogy külső hálózat közvetlen elérése csak a távoli kapcsolat kialakításának idejére legyen megengedett (pl. autentikációt igénylő szállodai vagy otthoni WiFi hálózat elérése esetén), vagy indokolt esetben a távoli hozzáféréshez elvárt technikai feltételek teljesítéséhez szükséges kapcsolatok biztosításáig (pl. kártékonykód elleni védelmi rendszer vírusdefiníciós állományok frissítéséhez, biztonsági javítócsomag letöltéséhez);	

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

6. Minden erőforrás-hitelesítés és engedélyezés dinamikus, és szigorúan kikényszerítésre kerül a hozzáférés engedélyezése előtt.

MNB ajánlás	Megjegyzés
9.4.9. Távoli hozzáférések esetében az intézmény a felhasználói fiók mellett legalább még egy további, a felhasználót hitelesítő faktort – például dinamikus kódot, tanúsítványt – is használ.	A kapcsolódó eszközök vizsgálata és a kapcsolódás feltételekhez kötése elvárás az MNB ajánlásaiban. A távoli elérések esetében az MNB elvárja a kapcsolódó eszközök hitelesítését is. Az eszközhitelesítés kiterjesztésének követelménye az összes eszközre összhangban van a Zero Trust elvárásaival.
7. f) az intézmény előzetesen határozza meg és rendszeresen vizsgálja felül a működés során elvárt paramétereket (adatkapcsolatok száma, adatkapcsolatok eloszlási ideje és helye, forgalmazott adatmennyiség stb.);	
26. i) az MNB elvárja: a kockázatokkal arányos mértékben a megbízhatóbb hitelesítés érdekében a távoli eszközök hitelesítését is.	

Forrás | MNB

NIST ZTA vs. MNB IT AJÁNLÁSOK

7. Az intézmény lehető legtöbb információt gyűjti össze az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és felhasználja azokat az informatikai biztonsági helyzetének javítására.

MNB ajánlás	Megjegyzés
7.4.4. f) Az intézmény gondoskodik a távelérések folyamatos monitorozásáról, valamint a biztonsági események - lehetőség szerinti automatikus - észleléséről és kezeléséről.	Az MNB ajánlások rendelkeznek az adatforgalom folyamatos figyeléséről. Az analitikai vizsgálatok és egyéb IT biztonsági információk használata a NIST ZTA és a Zero Trust fejlettebb követelménye.
8.3.3. Az intézmény gondoskodik a virtuális környezeti rendszerelemek működésének folyamatos monitorozásáról, illetve az események - lehetőség szerinti automatikus - észleléséről és kezeléséről.	
28. folyamatosan monitorozza a távoli hozzáféréssel felépített hálózatikapcsolatokat és a rajtuk átfolyó adatfolyamot, és folyamatosan biztosítsa a távoli hozzáféréshez szükséges kapacitásokat;	

Forrás | MNB

KÖSZÖNÖM A FIGYELMET!

Kállai László
vezető felügyelő

INFORMATIKAI FELÜGYELETI FŐOSZTÁLY

1013 Bp., Krisztina krt. 39.
Telefon: +36 (1) 489 9722
Mobil: +36 (30) 214 2340
Email: kallail@mnb.hu

MNB Informatikai Felügyelet aloldal, ajánlások, szakmai anyagok:
https://www.mnb.hu/felugyelet/szabalyozas/informatikai-felugyelet