Mely levelezési protokollok számítanak elavultnak a 7/2024 (VI.24) MK rendelet követelményei szempontjából?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/14

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A jogszabály nem név szerint tilt levelezési protokollokat, hanem elvárja, hogy minden adatátvitel titkosított legyen, és erős hitelesítést használjon a szervezet. Elavultnak tekintendők mindazon protokollok és beállítások, amelyek ezt nem teljesítik, így a titkosítatlan POP3/IMAP, a sima felhasználónév–jelszó alapú bejelentkezés, valamint a Telnet, FTP, HTTP, SMBv1, SSL 2.0/3.0, TLS 1.0/1.1, SNMPv1/v2c. Vállalati környezetben POP3/IMAP csak TLS-alapú titkosítással és – ahol lehetséges – modern, OAuth2-alapú hitelesítéssel fogadható el; az MFA-követelmény miatt a régi kliensek többsége kivezetendő. A modern e-mail biztonság része az SPF, DKIM és DMARC kötelező alkalmazása is; ezek hiánya vagy gyenge beállítása ma már nem tekinthető megfelelőnek jelentős és magas biztonsági osztályban. Legacy rendszerek ideiglenesen védhetők VPN-nel, SSH tunnellel és szegmentálással, de ehhez dokumentált kockázatelemzés és ütemezett kivezetési terv szükséges.

2. A VIZSGÁLANDÓ KÉRDÉS

Mely levelezési protokollok számítanak elavultnak a 7/2024 (VI.24) MK rendelet követelményei szempontjából? Pl.: POP3, IMAP elavultnak számít?

3. VÁLASZ

A hatályos magyar kiberbiztonsági jogszabályok nem tartalmaznak egy kimerítő, tételes „feketelistát” az elavult (legacy) protokollokról név szerint. Ehelyett funkcionális biztonsági követelményeket határoznak meg (bizalmasság, sértetlenség, titkosítás), amelyek alapján egy adott protokoll használata nem megfelelőnek vagy kockázatosnak minősülhet.

A protokollok elavultsága jogi és szakmai szempontból elsősorban akkor állapítható meg, ha azok nem képesek teljesíteni a modern titkosítási és hitelesítési elvárásokat. A 7/2024. (VI. 24.) MK rendelet 2. melléklete több ponton is előírja a nem biztonságos funkciók és protokollok letiltását, valamint az adatátvitel titkosítását.

A jogszabály előírja a „Legszűkebb funkcionalitás” elvét, amely alapján a szervezetnek azonosítania kell a nem biztonságos protokollokat:

> *„6.27. A szervezet:*
> *6.27.1. Meghatározott gyakorisággal átvizsgálja az EIR-t, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.*

6.27.2. Kikapcsolja vagy eltávolítja azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyeket szükségtelennek vagy nem biztonságosnak ítél."

Továbbá Jelentős és Magas biztonsági osztálynál elvárt követelmény az adatátvitel során a kriptográfiai védelem (titkosítás) alkalmazása, amely automatikusan kizárja a titkosítatlan (cleartext) protokollok használatát:

„17.40. Az EIR megvédi a továbbított információk bizalmasságát és sértetlenségét.
17.41. Az EIR kriptográfiai mechanizmusokat alkalmaz az adatátvitel során, hogy megelőzze az információk jogosulatlan felfedését, illetve kimutassa az információk módosításait."

- POP3 és IMAP státusza

A POP3 (Post Office Protocol version 3) és az IMAP (Internet Message Access Protocol) megítélése attól függ, hogy milyen formában és milyen hitelesítési mechanizmussal alkalmazzák őket.

A POP3 és IMAP elavultnak és nem biztonságosnak számít, amennyiben:

- Titkosítatlan formában használják, az alapértelmezett POP3 (110-es port) és IMAP (143-as port) egyszerű szöveges formában (cleartext) továbbítja a felhasználónevet és a jelszót a hálózaton. Ez sérti a 7/2024. (VI. 24.) MK rendelet 17.40. és 17.41. pontjában foglalt, a bizalmasságra és titkosításra vonatkozó követelményeket.
- Alapvető hitelesítést használnak, még titkosított csatornán (SSL/TLS) belül is elavultnak tekinthető az egyszerű felhasználónév/jelszó páros használata, mivel nem támogatja a többtényezős hitelesítést (MFA) és modern személyazonosság-kezelést.

A POP3 és IMAP elfogadhatónak tekinthető, amennyiben:

- Titkosított csatornán futnak (POP3S, IMAPS): Ha a kommunikáció SSL/TLS csatornába van csomagolva (jellemzően a 995-ös és 993-as portokon), az adattovábbítás titkosított.
- Modern hitelesítést alkalmaznak (Modern Auth / OAuth2): Ha a protokoll implementációja támogatja az OAuth 2.0 szabványt (pl. Microsoft Exchange Online vagy Gmail esetében), akkor nem számítanak elavultnak, bár funkcionalitásban (pl. szinkronizáció hiánya POP3 esetén) elmaradnak a modernebb megoldásoktól (pl. MAPI/HTTP, ActiveSync).

Bár szigorúan véve nem adatátviteli protokollok, a modern levelezésbiztonság elválaszthatatlan részét képezik a feladó hitelesítését szolgáló mechanizmusok. A 7/2024. (VI. 24.) MK rendelet 17.40. pontja előírja az információk sértetlenségének védelmét. Ennek hiányában a levelezőrendszer kiszolgáltatott a hamisításnak (spoofing) és adathalászatnak.

Ma már elavultnak és nem megfelelőnek tekinthető az olyan levelezőrendszer-konfiguráció, amely nem alkalmazza az alábbi védelmi szabványokat:

- SPF (Sender Policy Framework), megakadályozza, hogy illetéktelen szerverek küldjenek levelet a szervezet nevében.
- DKIM (DomainKeys Identified Mail), kriptográfiai aláírással biztosítja, hogy az üzenet tartalmát útközben nem módosították (sértetlenség).
- DMARC (Domain-based Message Authentication, Reporting, and Conformance): Összefogja az SPF és DKIM ellenőrzést, és házirendet kényszerít ki. A DMARC hiánya vagy "none" házirend tartós alkalmazása a jelentős és magas biztonsági osztályokban nem javasolt.

A kiberbiztonsági auditok és a jogszabályi megfelelés vizsgálata során az alábbi táblázatban szereplő protokollok minősülnek jellemzően elavultnak ("legacy"), mivel nem felelnek meg a titkosítási és hitelesítési követelményeknek.

Protokoll	**Leírás és kockázat**	**Helyettesítő, biztonságos protokoll**
Telnet	Távoli hozzáférést biztosít, de minden adatot (beleértve a jelszavakat is) titkosítatlanul (cleartextben) továbbít. Kifejezetten tiltott a legtöbb biztonsági szabályzatban.	SSH (Secure Shell)
FTP	A File Transfer Protocol titkosítatlanul küldi a hitelesítési adatokat és a fájlok tartalmát.	SFTP (SSH File Transfer Protocol) vagy FTPS (FTP-SSL)
HTTP	A titkosítatlan webes forgalom nem védi az adatok bizalmasságát és sértetlenségét.	HTTPS (HTTP Secure)
SMBv1	A Server Message Block 1.0 verziója számos kritikus sérülékenységet tartalmaz (pl. WannaCry zsarolóvírus terjedése).	SMBv2 vagy SMBv3
SSL 2.0 / 3.0, TLS 1.0 / 1.1	Ezek a titkosítási protokollverziók elavultak, kriptográfiai gyengeségeik miatt könnyen feltörhetők.	TLS 1.3
TLS 1.2	Már csak kompatibilitási célból használják, minden más esetben a TLS 1.3 használata javasolt erősen.	TLS 1.3
SNMPv1 / v2c	A hálózatmenedzsment protokoll korai verziói titkosítatlanul, (cleartext) "community string"-ekkel kommunikálnak.	SNMPv3

A 7/2024. (VI. 24.) MK rendelet alapján a szervezetnek rendszeres felülvizsgálatot kell végeznie (6.27. pont), amelynek során azonosítania kell a fenti protokollokat.

Amennyiben a szervezetnél POP3 vagy IMAP protokollt használnak:

1. Ellenőrizni kell, hogy kényszerítve van-e a titkosított kapcsolat (SSL/TLS).
2. Vizsgálni kell, hogy alkalmazható-e a modern hitelesítés (OAuth2), mivel az "Alap", "Jelentős" és "Magas" biztonsági osztályokban is elvárás a többtényezős hitelesítés (MFA) támogatása, amit a régi POP3/IMAP implementációk gyakran nem tesznek lehetővé.

> *„8.4. A szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.”*

Ez a követelmény (MFA) teszi a gyakorlatban elavulttá a hagyományos POP3 és IMAP használatát a legtöbb vállalati környezetben.

A gyakorlatban előfordulhatnak olyan örökölt (legacy), de üzletileg kritikus alkalmazások, amelyek nem támogatják a modern titkosítást vagy hitelesítést. Ilyen esetekben a protokoll önmagában nem biztonságos, de a kockázat műszaki intézkedésekkel csökkenthető:

Alagút technológiák (Tunneling): a nem biztonságos protokollt (pl. Telnet, POP3) egy titkosított csatornába csomagoljuk. Tipikus megoldás a VPN (Virtual Private Network) vagy az SSH Tunnel használata. Ebben az esetben a titkosítást nem az alkalmazás, hanem az átviteli csatorna (alagút) biztosítja.

Hálózati szegmentálás: a sérülékeny eszközök elszeparálása dedikált VLAN-ba, szigorú tűzfal szabályokkal, hogy csak a szükséges végpontok érhessék el.

Fontos, ezen megoldások alkalmazása esetén a dokumentációnak tartalmaznia kell a kockázatelemzést és az indoklást, hogy miért nem lehetséges a natívan biztonságos protokoll használata.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről