A megfelelő hitelesítésre és jogosultságra vonatkozó szabályok

Külső szerződött fél informatikai rendszereivel a kapcsolatot csak az iparág által mindenkor bizonyítottan biztonságosnak ítélt protokollokon keresztül és a bizonyítottan biztonságos kulcsmélység mellett lehet kialakítani. Alapvetően az ún. Zero Trust Architecture-t (ZTA) kell alkalmazni.

Tilos az elavult és titkosítással nem rendelkező protokollok használta (pl. telnet, ftp, http stb.)

Tilos az elavult és gyenge kriptográfiai titkosítások használata:

1. MD2, MD4, MD5, 3DES titkosítás
2. SHA-1
3. TLS 1.2 alatti verziók
4. SSL
5. HTTPS 2048 bit alatti kulcsok
6. IPMI protokoll,
7. SMB1 protokoll,
8. stb.

Tekintve, hogy a kriptográfiai eljárások megbízhatósága az idő múlásával folyamatosan gyengül, ezért a külső rendszerrel történő összekapcsolódás lehetséges paramétereit már a tervezés fázisában ismertetni kell az ITTI vezetővel, az Informatika igazgatóval és az Információbiztonsági Felelőssel.

Referenciaoldalak:

https://www.nist.gov/cryptography
https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2
https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html
https://ciphersuite.info/