Dahua – Kiberbiztonsági ajánlások

Az eszközök alapvető hálózatbiztonságához szükséges intézkedések

1. Erős jelszavak használata

A jelszavak beállításakor az alábbi szempontokat javasolt figyelembe venni:

– A jelszó legalább 8 karakterből álljon.

– Legalább kétféle karaktertípust tartalmazzon: kis- és nagybetűket, számokat vagy szimbólumokat.

– Ne tartalmazza a felhasználónevet, sem annak fordítottját.

– Ne használjon egymást követő karaktereket, például 123 vagy abc.

– Ne használjon ismétlődő karaktereket, például 111 vagy aaa.

2. A firmware és a kliensszoftver időben történő frissítése

– Az iparágban követett általános gyakorlatnak megfelelően javasoljuk, hogy az eszközök (például NVR, DVR, IP-kamera) firmware-e mindig naprakész legyen, így a rendszer megkapja a legújabb biztonsági javításokat és hibajavításokat. Ha az eszköz nyilvános hálózathoz csatlakozik, javasolt engedélyezni az „Automatikus frissítéskeresés” funkciót, hogy időben értesüljön a gyártó által kiadott firmware-frissítésekről.

– Javasoljuk a kliensszoftver legújabb verziójának letöltését és használatát.

További ajánlott intézkedések az eszközök hálózatbiztonságának növeléséhez

1. Fizikai védelem

Javasoljuk az eszközök, különösen az adattároló berendezések fizikai védelmét. Például helyezze az eszközöket külön gépterembe vagy zárható szekrénybe, gondoskodjon a megfelelő belépési jogosultságokról és kulcskezelésről. Ezzel megakadályozható, hogy illetéktelen személyek fizikailag hozzáférjenek a berendezésekhez, megrongálják azokat, vagy engedély nélkül külső eszközöket (például USB-adathordozót vagy soros porton csatlakozó eszközt) kapcsoljanak hozzájuk.

2. Jelszavak rendszeres módosítása

Javasoljuk a jelszavak rendszeres módosítását a kitalálásukból vagy feltörésükből eredő kockázatok csökkentése érdekében.

3. A jelszó-visszaállítási adatok beállítása és naprakészen tartása

Az eszközök támogatják a jelszó-visszaállítást. Időben állítsa be az ehhez szükséges adatokat, például a végfelhasználó e-mail-címét és a biztonsági kérdéseket. Ha ezek az adatok megváltoznak, frissítse őket. A biztonsági kérdések esetében kerülje a könnyen kitalálható válaszokat.

4. Fiókzárolás engedélyezése

A fiókzárolás alapértelmezés szerint engedélyezett; a fiókok biztonsága érdekében javasolt bekapcsolva hagyni. Ha egy támadó egymás után többször hibás jelszóval próbál bejelentkezni, az érintett fiók és a forrás IP-címe zárolásra kerül.

5. Az alapértelmezett HTTP- és egyéb szolgáltatásportok módosítása

Javasoljuk, hogy az alapértelmezett HTTP- és egyéb szolgáltatásportokat változtassa meg egy 1024 és 65535 közötti portszámra, ezzel csökkentve annak kockázatát, hogy külső személyek kitalálják a használt portokat.

6. HTTPS engedélyezése

Javasoljuk a HTTPS engedélyezését, hogy a webes felületet biztonságos kommunikációs csatornán keresztül lehessen elérni.

7. Engedélyezési lista (Allow List) használata

Javasoljuk az engedélyezési lista használatát: így csak a megadott IP-címekről lehet elérni a rendszert. Ügyeljen arra, hogy a saját számítógépének és a kapcsolódó berendezéseknek az IP-címe is szerepeljen a listán.

8. MAC-cím hozzárendelése

Javasoljuk az átjáró IP- és MAC-címének hozzárendelését az eszközhöz, amellyel csökkenthető az ARP-hamisítás (ARP spoofing) kockázata.

9. Felhasználói fiókok és jogosultságok megfelelő kiosztása

Az üzleti és üzemeltetési igényeknek megfelelően hozzon létre felhasználókat, és számukra csak a feladataikhoz szükséges minimális jogosultságokat adja meg.

10. Felesleges szolgáltatások kikapcsolása és biztonságos üzemmódok használata

Ha nincs rájuk szükség, a kockázatok csökkentése érdekében javasolt kikapcsolni egyes szolgáltatásokat, például az SNMP-t, az SMTP-t vagy az UPnP-t.

Amennyiben szükséges e szolgáltatások használata, különösen ajánlott a biztonságos megoldások alkalmazása, többek között az alábbiak szerint:

– SNMP: válassza az SNMP v3 verziót, és állítson be erős titkosítási és hitelesítési jelszavakat.

– SMTP: a levelezőszerver eléréséhez használjon TLS-t.

– FTP: válassza az SFTP-t, és állítson be erős jelszavakat.

– AP-hotspot: használjon WPA2-PSK titkosítást és erős jelszavakat.

11. Hang- és videoadatok titkosított továbbítása

Ha a hang- és videoadatok különösen fontosak vagy érzékenyek, javasoljuk a titkosított adatátvitel használatát, hogy csökkenjen a továbbítás közbeni adatszerzés kockázata.

Megjegyzés: a titkosított továbbítás csökkentheti az adatátvitel hatékonyságát.

12. Biztonsági ellenőrzés és naplózás

– Bejelentkezett felhasználók ellenőrzése: rendszeresen vizsgálja meg, hogy nem jelentkezett-e be valaki jogosulatlanul az eszközre.

– Eszköznaplók ellenőrzése: a naplókból megállapítható, milyen IP-címekről történt bejelentkezés, és milyen fontos műveleteket hajtottak végre.

13. Hálózati naplózás

Az eszközök korlátozott tárkapacitása miatt a helyben tárolható naplók mennyisége is korlátozott. Ha hosszú távon szükséges megőrizni a naplókat, javasolt a hálózati naplózási funkció engedélyezése, hogy a fontos naplóbejegyzések egy hálózati naplószerverre is továbbításra kerüljenek, és később visszakereshetők legyenek.

14. Biztonságos hálózati környezet kialakítása

Az eszközök jobb védelme és a lehetséges kiberbiztonsági kockázatok csökkentése érdekében javasoljuk:

– Kapcsolja ki a router porttovábbítási funkcióját, hogy a belső hálózati eszközök ne legyenek közvetlenül elérhetők külső hálózatból.

– A hálózatot a tényleges igények szerint ossza szegmensekre és különítse el. Ha két alhálózat között nincs szükség kommunikációra, VLAN, hálózati leválasztás (network gap) vagy más technológia alkalmazásával valósítsa meg az elkülönítést.

– Alakítson ki 802.1X hálózati hozzáférés-hitelesítést az illetéktelen belső hálózati hozzáférés kockázatának csökkentésére.