DIGITÁLIS BIZTONSÁG ELLENŐRZŐ LISTA

A hálózathoz kapcsolt eszközök száma folyamatosan növekszik. Így a kibertámadók számára is egyre könnyebb azonosítani és kihasználni a gyenge hálózati biztonsági intézkedéseket, hogy hozzáférést nyerjenek a kritikus adatokhoz. Ellenőrizze hálózatát ezzel az ellenőrző listával.

Lásd: Egy betekintésből láthatja, hogy milyen adatok vannak már védve, és mik azok amik még nincsenek.

Vegye végig lépésről lépésre az összes fontos biztonsági pontot. Minden kipipált jelölőnégyzet egy pontnak felel meg. Minél több pontja van, annál jobban vannak védve adatai és eszközei. Összesen 44 pontot érhet el.

Védelem számítógépek és mobil eszközök számára

Pontok /4

- ☐ Tartsa operációs rendszerét naprakészen
- ☐ Telepítsen megbízható vírusirtó szoftvert, és rendszeresen futtasson teljes körű ellenőrzést
- ☐ Csak akkor engedélyezze a távoli asztali protokollt (RDP), ha a távoli hozzáférés feltétlenül szükséges, hogy védelmet nyújtson a protokollt kihasználó támadások ellen
- ☐ Ha nyilvános WiFi-t használ, mindig titkosítja a kapcsolatot VPN csatlakozással

Az IoT-eszközök védelme

Pontok /4

- ☐ Használjon erős jelszót
- ☐ Az eszközök (pl. IP-kamerák, nyomtatók, telefonok stb.) internet-hozzáférésének blokkolása, kivéve, ha szükséges az eszköz csatlakoztatása. Internet-kiszolgálóval való kommunikáció a működéshez
- ☐ Csatlakoztassa az IoT-eszközöket a vendéghálózathoz, és válassza le őket a felhasználó tulajdonában lévő eszközökről, például a számítógépekről, okostelefonokról és NAS-okról, hogy megakadályozza az IoT-eszköz feltörését és az ugyanazon a hálózaton lévő más eszközök megtámadását.
- ☐ Azonnal blokkoljon egy eszközt, ha az gyanús tevékenység jeleit mutatja. Vizsgálja ki az eseményeket, és szükség esetén állítsa vissza/telepítse újra az eszközt

A NAS védelme

Pontok /12

- ☐ Használjon egyéni rendszergazdafiókot és deaktiválja az alapértelmezett admin és vendégfiókokat
- ☐ 2 lépéses hitelesítés engedélyezése
- ☐ Alkalmazzon erős jelszószabályokat az összes felhasználónál
- ☐ Korlátozza a felhasználók hozzáféréseit a számukra nem szükséges megosztott mappákhoz és szolgáltatásokhoz
- ☐ Módosítsa a rendszer alapértelmezett portjait, pl. B. Port 5000/5001 a NAS operációs rendszer kezelőfelületéhez (DiskStation Manager, röviden DSM) a magasabb 5 számjegyű tartományban lévő új egyéni portokra
- ☐ Ha a NAS-on engedélyezve van a port-továbbítás, használjon egyéni portokat a jól ismert portok helyett (pl. 5000/5001).nyilvános portok az routeren
- ☐ Automatikus IP-blokkolás engedélyezése a brute force támadások ellen
- ☐ HTTPS engedélyezése a DSM-en futó szolgáltatások számára érvényes SSL-tanúsítvánnyal
- ☐ E-mail, SMS vagy push értesítések engedélyezése, hogy mindig értesüljön a kritikus eseményekről
- ☐ Automatikus frissítés engedélyezése a DSM számára
- ☐ A Security Advisor rendszeres futtatása a rendszer sebezhetőségének feltárására és a rosszindulatú programok azonosítására
- ☐ Telepítsen vírusirtó csomagot, és rendszeresen futtasson teljes körű vizsgálatot

Kerületi védelem routerek számára

Pontok /14

Rendszerbiztonság

- ☐ Használjon egyéni rendszergazdai fiókot, és tiltsa le az alapértelmezett admin és vendég fiókokat
- ☐ Aktiváljon 2 lépéses hitelesítést
- ☐ Módosítsa a rendszer alapértelmezett portjait, pl. a kezelési interfész 8000/8001-es portját új egyéni portokra, ha Ön a Synology Router Manager (SRM) szolgáltatást használja.
- ☐ Automatikus IP-blokkolás engedélyezése a brute force támadások ellen
- ☐ HTTPS engedélyezése az SRM-en futó szolgáltatások számára érvényes SSL-tanúsítvánnyal
- ☐ E-mail, SMS vagy push értesítések engedélyezése, hogy mindig értesüljön a kritikus eseményekről
- ☐ Az router firmware és az összes beépített biztonsági adatbázis automatikus frissítésének engedélyezése

Hálózatbiztonság

- ☐ Hozzáférés az irodai vagy otthoni eszközökhöz VPN-en keresztül
- ☐ A Synology Safe Access engedélyezése a rosszindulatú domainek és IP-címek blokkolásához
- ☐ Engedélyezze a fenyegetések megelőzését és az alapos csomagátvizsgálást
- ☐ A DNS HTTPS-titkosítás engedélyezése a DNS feltörésének megakadályozására
- ☐ GeoIP tűzfal szabályok engedélyezése
- ☐ A Mac szűrés és az ismert eszközök fehérlistázásának engedélyezése a WiFi használatához
- ☐ Rendszeresen ütemezett forgalmi jelentések engedélyezése a hálózati használat nyomon követése érdekében

Adatvédelem biztonsági mentéssel

Pontok /10

PC biztonsági mentés

- ☐ A Synology Drive engedélyezése a fontos fájlok és mappák biztonsági mentéséhez
- ☐ Az Active Backup for Business engedélyezése a teljes rendszer biztonsági mentéséhez

NAS biztonsági mentés

- ☐ A Hyper Backup engedélyezése a megosztott mappák, LUN-ok és rendszer-/csomagkonfigurációk biztonsági mentéséhez
- ☐ A Hyper Backup alkalmazásban konfiguráljon figyelmeztető értékhatárt a két biztonsági mentési verzió közötti fájlváltozásokra vonatkozóan, hogy
  automatikusan értesítést kapjon a rendellenes viselkedésről, és így megakadályozhassa az esetleges adatvesztést
- ☐ Pillanatfelvétel-replikáció engedélyezése a fontos megosztott mappák pillanatfelvételeinek létrehozásához
- ☐ A Cloud Sync engedélyezése a fájlok és mappák folyamatos átviteléhez egy biztonságos nyilvános felhőszolgáltatóhoz, például a Synology C2 biztonságos tárhelyére

Külső eszközök biztonsági mentése (pl. USB merevlemezek)

- ☐ Az USB másolás használatával központilag mentheti az összes külső eszközt a NAS-ra

Egyéb fontos biztonsági mentési beállítások

- ☐ Tartson legalább egy külső másolatot a katasztrófa utáni helyreállításhoz
- ☐ Ütemezze az összes biztonsági mentési feladat automatikus futtatását
- ☐ Az első biztonsági mentés után tesztelje, hogy vissza tudja-e állítani az adatokat a biztonsági másolatról. Ezt a későbbiekben rendszeresen ismételje meg, hogy hiba esetén mindig teljes helyreállítást tudjon végezni