Forrás: https://www-geeksforgeeks-org.translate.goog/introduction-to-physical-security/?_x_tr_sl=auto&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=wapp

Bevezetés a fizikai biztonságba

Napjainkban minden újabb kibertámadás bejelentését követik a kiberbiztonság megerősítésére vonatkozó tippek. Ne felejtsen el biztonsági másolatot készíteni adatairól, javítsa a sebezhetőséget, figyelje a tűzfalakat stb. Nagyon fontos észben tartani, hogy a szoftver nem az egyetlen fegyvere a kiberbiztonság terén. A fizikai kiberbiztonság egy másik szint a védelmi vonalában.

Goldstein (2016) szerint a fizikai biztonság kritikus fontosságú, különösen a kisvállalkozások számára, amelyek nem rendelkeznek sok erőforrással a biztonsági személyzetre és eszközökre, szemben a nagyobb cégekkel. Amikor a fizikai biztonságról van szó, itt is ugyanazok az elvek érvényesek:

- Azonosítsa és osztályozza eszközeit és erőforrásait.
- Azonosítsa a valószínű fenyegetéseket.
- Azonosítsa azokat a lehetséges sebezhetőségeket, amelyeket a fenyegetések kihasználhatnak.
- Határozza meg a várható költségeket támadás esetén.

Tényezők, amelyektől a fizikai biztonság függ

- Hány munkahely, épület vagy telephely van egy szervezetben?
- A szervezet épületének mérete?
- Hány alkalmazottat foglalkoztat a szervezet?
- Hány belépési és kilépési pont van a szervezetben?
- Adatközpontok és egyéb bizalmas információk elhelyezési pontjai.

A fizikai biztonság rétegei

A fizikai biztonság rétegei a kerületen vannak megvalósítva, és egy eszköz felé haladnak. A rétegek a következők:

1. Elrettentés

Az Elrettentés módszereinek célja, hogy meggyőzzék a potenciális támadót arról, hogy az erős védekezés miatt nem lehetséges sikeres támadás. Például: Ha kulcsait nehézfémből, például acélból álló, rendkívül biztonságos kulcsvezérlő rendszerbe helyezi, megakadályozhatja, hogy a támadók hozzáférjenek az eszközökhöz. Az elrettentő módszerek 4 kategóriába sorolhatók:

- **Fizikai akadályok**: Ide tartoznak a kerítések, falak, járműsorompók stb. Pszichológiai visszatartó erőként is működnek, mivel meghatározzák a létesítmény kerületét, és megnehezítik a behatolást.

- **Kombinációs korlátok**: Ezek a meghatározott fenyegetések legyőzésére szolgálnak. Ez az építési szabályzat és a tűzvédelmi szabályzat része.
- **Természetes megfigyelés**: Ebben az építészek arra törekednek, hogy nyitottabb és láthatóbb helyeket építsenek a jogosult felhasználók és biztonsági személyzet számára, hogy a támadók ne tudják végrehajtani a jogosulatlan tevékenységet anélkül, hogy látnák őket. Például a sűrű és magas növényzet mennyiségének csökkentése.
- **Biztonsági világítás**: Az ajtóknak, kapuknak vagy a bejárat egyéb elemeinek jól megvilágítottnak kell lenniük, mivel a behatolók kisebb valószínűséggel lépnek be jól megvilágított területekre. Ügyeljen arra, hogy a világítást nehezen manipulálható módon helyezze el.

2. Észlelés

Ha a kézi kulcsvezérlő rendszert használja, nem tudja pontosan megtudni, hogy mikor kért egy jogosulatlan felhasználó kulcsot, vagy mikor lépte túl annak időtartamát. Az észlelési módszerek a következő típusúak lehetnek:

- Riasztórendszerek és érzékelők: Riasztórendszerek telepíthetők a biztonsági személyzet figyelmeztetésére jogosulatlan hozzáférési kísérlet esetén. Érzékelőkből állnak, mint például kerületérzékelők, mozgásérzékelők stb.
- Videó megfigyelés: A térfigyelő kamerák segítségével észlelhető, ha már megtörtént a támadás, és a támadás helyén kamera van elhelyezve. A rögzített videó felhasználható

3. Hozzáférés-vezérlés

Ezeket a módszereket az adott hozzáférési pontokon keresztüli forgalom figyelésére és ellenőrzésére használják. A hozzáférés-vezérlés a következő módszereket tartalmazza:

- Mechanikus beléptetőrendszerek: Ide tartoznak a kapuk, ajtók, zárak stb.
- Elektronikus hozzáférés-vezérlés: Nagyobb populációk figyelésére és vezérlésére szolgálnak, a felhasználói életciklusok, dátumok és egyéni hozzáférési pontok vezérlésére.
- Azonosítási rendszer és hozzáférési szabályzatok: Ezek magukban foglalják a szabályzatok, eljárások és folyamatok használatát a korlátozott területre való hozzáférés kezelésére.

4. Biztonsági személyzet

A biztonság minden rétegében központi szerepet játszanak. Számos funkciót látnak el, például:

- Elektronikus beléptetés-ellenőrzés adminisztrálása.
- Riasztásokra reagálva.
- Videófelvételek figyelése és elemzése és még sok más

Ellenintézkedések és védelmi technikák

1. Védelem a Dumpster Diving ellen

A Dumpster Diving egy olyan folyamat, amely során hasznos információkat találunk az adott személyről vagy vállalkozásról a szemétből, amelyet később feltörésre használhatnak fel. Mivel az információ a kukában van, nem a tulajdonos számára hasznos, hanem a válogató számára hasznosnak. A védekezés érdekében bizonyos intézkedéseket be kell tartania:

- Győződjön meg arról, hogy minden fontos dokumentumot feldaraboltak, és továbbra is biztonságosak.
- Semmisítse meg a személyes adatokat tartalmazó CD-t/DVD-t.
- Győződjön meg arról, hogy senki sem léphet be az épületbe, és egyszerűen ellophatja a szemetet, és gondoskodjon a biztonságos ártalmatlanításról.
- A tűzfalak segítségével megakadályozható, hogy gyanús felhasználók hozzáférjenek az eldobott adatokhoz.

2. Munkavállalói tudatosságnövelő tréning

Egy gondatlan alkalmazott lehet a kiberbiztonság megsértésének egyik fő oka. Ilyen esetekben segíthetnek a munkavállalói figyelemfelkeltő tréningek. A munkavállalói tudatosságnövelő tréningnek egy mögöttes témára kell összpontosítania – kerülje el a szeptemberi – Valaki más problématerületét.

3. Site Access Control

A hozzáférés-szabályozás hiánya nagyon pusztító lehet, ha rossz személy kerül be és jut hozzá érzékeny információkhoz. Szerencsére manapság számos modern eszköz áll rendelkezésére, amelyek segítenek optimalizálni a hozzáférés-szabályozást.

- Az Envoy egy olyan eszköz, amely segít szabályozott módon bővíteni a vendégek hozzáférését.
- Az Open Path egy olyan mobil rendszer, amely csak korlátozott számú ember számára teszi lehetővé a hozzáférést a címtáron belül okostelefonok és egyéb eszközök segítségével.

4. Az ablakok biztonsága

Ha rendelkezik olyan adatokkal, amelyekre a hackerek szívesen hozzájutnának, bármilyen módszert kipróbálnak, és lehet, hogy egyszerűen csak kinéznek az ablakon. Győződjön meg arról, hogy tisztában van a látószögekkel a képernyők és más eszközök elhelyezéséhez. A különböző látószögekből való kitekintést, hogy megtekinthesse hitelesítő adatait, vállszörfözésnek nevezzük .

5. Biztonságos hálózatra alkalmas nyomtatók

A hálózati nyomtatók nagyon kényelmes megoldást jelentenek, amely lehetővé teszi, hogy az irodában bárki csatlakozhasson további kábelezés nélkül. Sajnos vannak mögöttes

biztonsági kockázataik is. Néha, az alapértelmezett beállítások miatt, nyílt WiFi hozzáférést kínálnak, így bárki bejuthat, és a folyamat során sebezhetőséget nyithat meg.

- Csak azokat csatlakoztassa az internethez, amelyeknek valóban szükségük van rá.
- Nincs szükség távoli hozzáférésre olyan helyzetekben, amikor csak az Ön irodájában dolgozók használják a nyomtatót.
- Szükség esetén jelszavakat adhat hozzá a kapcsolathoz.

6. A biztonsági másolatok biztonsága

A fizikai biztonsági mentések létfontosságúak az üzletmenet folytonossága szempontjából, mivel segítenek megelőzni az adatvesztést katasztrófák, kimaradások és egyebek esetén. A legtöbb vállalkozás védi szervereit, de elfelejtik, hogy a biztonsági mentések ugyanolyan fontosak. Ugyanolyan érzékeny adatokkal rendelkeznek, mint a szerverek. Úgy kezelje biztonsági másolatait, mint érzékeny adatait, és védje azokat.

7. Secure Guest Wifi kiépítése

A vendég WiFi természetes megoldás, ha vendégei vagy látogatói vannak. Íme néhány trükk, amelyek segítségével megvédheti erőforrásait a külső felhasználóktól:

- Szegmentálja a hálózatot – Ily módon elkülöníti a vendég WiFi-t a belső eszközöktől és adatoktól.
- Titkosítsa vezeték nélküli jeleit, és módosítsa a hálózaton lévő összes eszköz alapértelmezett jelszavát.

8. A szerverek lezárása

A szervezet minden olyan területét, ahol adatokat tárolnak, védeni kell. Az ajtók zárása és a szerverterület extra védelmet biztosít.

9. Elveszett vagy ellopott eszközök elszámolása

Ahogy az eszközök egyre mobilabbak, egyre gyakrabban előfordul, hogy ellopják őket, vagy kiesnek valakinek a zsebéből. A Mobileszköz-kezelés segíthet az ilyen helyzetek kezelésében és a szükséges óvintézkedések megtételében. Ilyen esetekben a legjobb megoldás az, ha egyszerűen zároljuk, és távolról töröljük az elveszett vagy ellopott eszközöket a szervezetből.

10. Videó rendszerek megvalósítása

A biztonságosabb helyiségek elérése érdekében célszerű Video Surveillance rendszert használni.

- A kamerák puszta jelenléte elriaszthatja a potenciális támadókat.
- A videofelvételek elérhetősége lehetővé teszi a folyamatos megfigyelést az egész helyiségben.
- Ha támadás történik, ellenőrizheti a rögzített videót, könnyen összeegyeztetheti a folyamatot és elkaphatja az elkövetőt.