

HOGYAN VÉDHETJÜK MEG A KRITIKUS INFRASTRUKTÚRÁNKAT?

Dr. Bányász Péter
egyetemi docens, Nemzeti Közszolgálati Egyetem

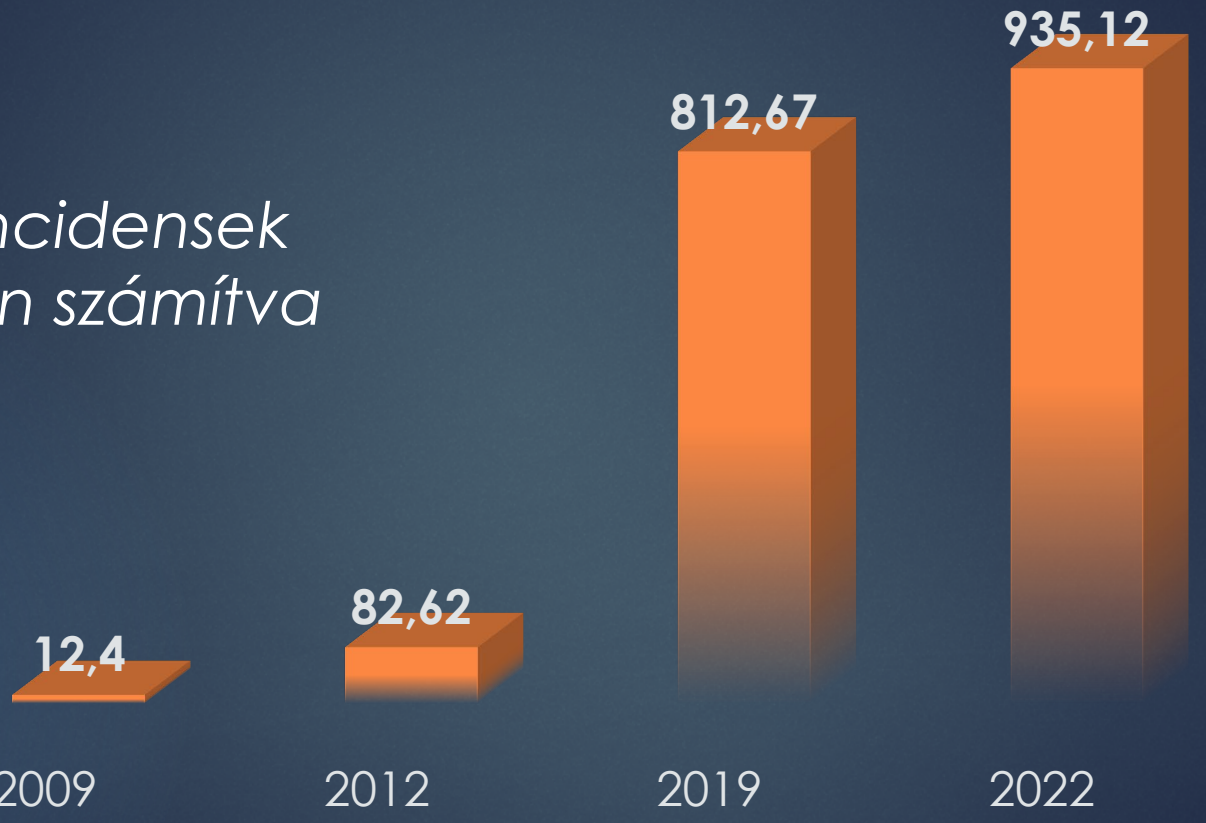
BELÜGYI ALAPOK
Méltányosság és biztonság
Az Európai Unió támogatásával
BELSŐ BIZTONSÁGI ALAP

TARTALOM

1. A KIBERTÁMADÁSOK HELYREÁLLÍTÁSI KÖLTSÉGEI ÉS A LEHETSÉGES KÁROK
2. KOCKÁZAT- ÉS KÖVETKEZMÉNY-MENEDZSMENT
3. AZ ELLÁTÁSI LÁNC, MINT KIBERBIZTONSÁGI KOCKÁZAT
4. AZ ELLÁTÁSI LÁNC VÉDELME

A KIBERTÁMADÁSOK HELYREÁLLÍTÁSI KÖLTSÉGEI

Kibervédelmi incidensek száma millióban számítva



A KIBERTÁMADÁSOK HELYREÁLLÍTÁSI KÖLTSÉGEI

Egy kisebb kibertámadás is átlagosan 15 000 – 25 000 dollárba kerül, és 279 napba telik teljesen visszaállni utána



Zsarolóvírusok
170 404 USD

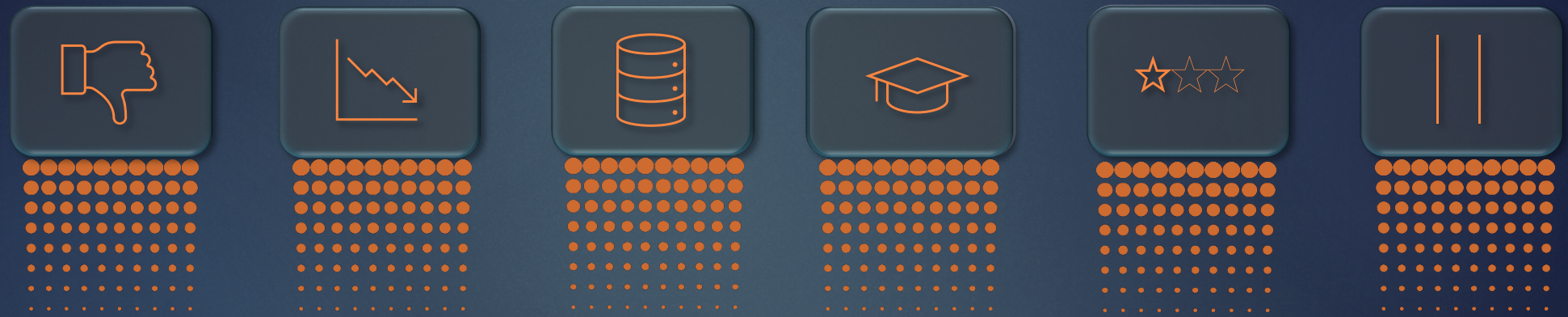


Adathalászat
71 000 USD



Adatszivárgás
4.35 millió USD

A kibervédelmi incidensekből fakadó károk:



- Reputációs kár vagy veszteség
- Pénzügyi veszteség
- Adatszivár-gás vagy adatvesztés
- Szellemi tulajdon elvesztése
- Ügyfelek elvesztése
- Szolgáltatás, termelés leállása

KOCKÁZAT- ÉS KÖVETKEZMÉNY-MENEDZSMENT

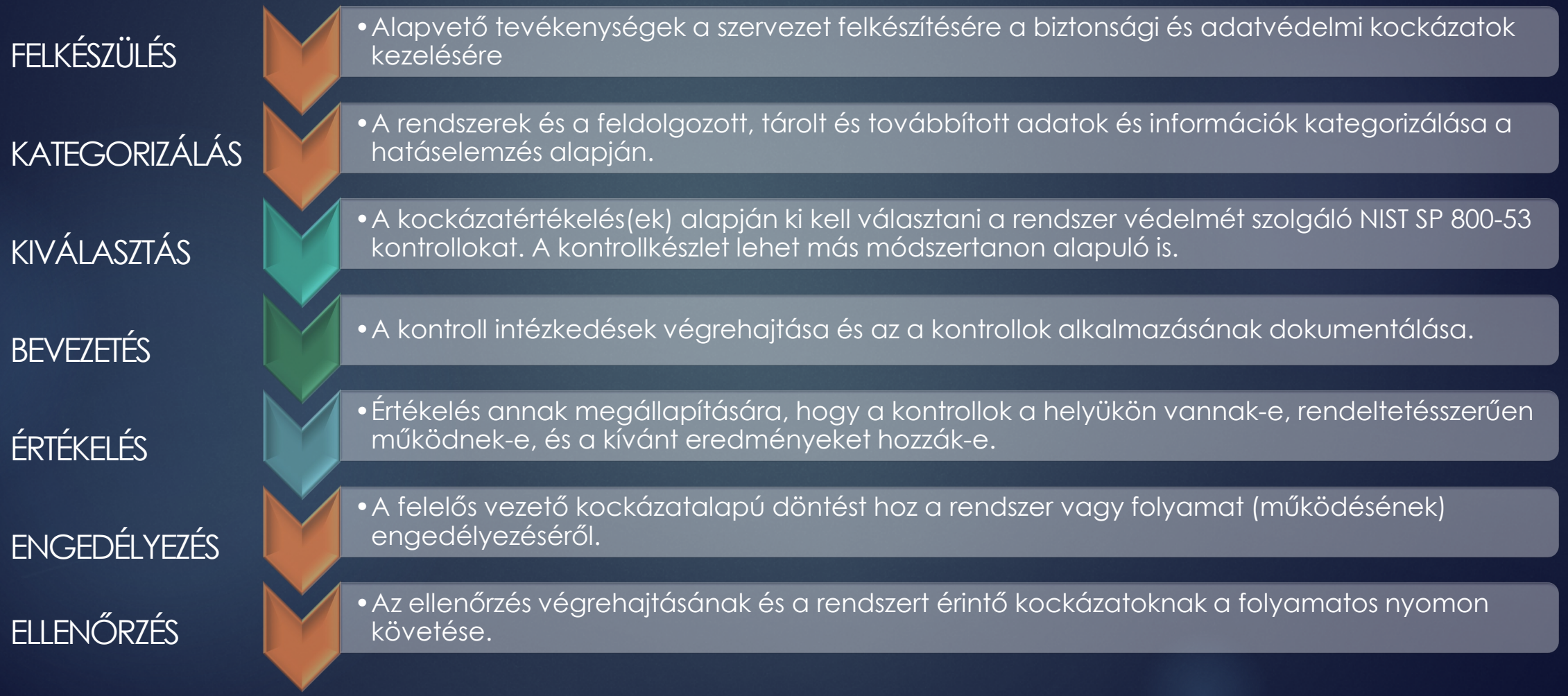
Jó gyakorlatok



A kiberbiztonsági kockázatmenedzsment:

- A szervezet digitális eszközeinek **azonosítása**
- A meglévő biztonsági intézkedések **rendszeres felülvizsgálata**
- Olyan **megoldások bevezetése**, amelyek vagy folytatják, ami működik, vagy mérséklik a vállalkozást fenyegető biztonsági kockázatokat.




FELKÉSZÜLÉS
Alapvető tevékenységek a szervezet felkészítésére a biztonsági és adatvédelmi kockázatok kezelésére
KATEGORIZÁLÁS
A rendszerek és a feldolgozott, tárolt és továbbított adatok és információk kategorizálása a hatáselemzés alapján.
KIVÁLASZTÁS
A kockázatértékelés(ek) alapján ki kell választani a rendszer védelmét szolgáló NIST SP 800-53 kontrollokat. A kontrollkészlet lehet más módszertanon alapuló is.
BEVEZETÉS
A kontroll intézkedések végrehajtása és az a kontrollok alkalmazásának dokumentálása.
ÉRTÉKELÉS
Értékelés annak megállapítására, hogy a kontrollok a helyükön vannak-e, rendeltetésszerűen működnek-e, és a kívánt eredményeket hozzák-e.
ENGEDÉLYEZÉS
A felelős vezető kockázatalapú döntést hoz a rendszer vagy folyamat (működésének) engedélyezéséről.
ELLENŐRZÉS
Az ellenőrzés végrehajtásának és a rendszert érintő kockázatoknak a folyamatos nyomon követése.

Sérülékenység-menedzsment:

- **Célja:** a sérülékenységmenedzsment célja, hogy folyamatosan azonosítsa, osztályozza, értékelje, kezelje és jelentse a szervezet rendszereiben található sérülékenységeket.

- **Eszközei:** a sérülékenységmenedzsment eszközei közé tartoznak a sérülékenység- ellenőrző szoftverek, sérülékenységi adatbázisok, a biztonsági információ- és eseménykezelő (SIEM) rendszerek és a kockázatkezelési platformokból származó adatok.
  - Az Automatizált Sérülékenységvizsgálati Rendszer (továbbiakban: ASR) célja azonosítani a nyilvántartásába rögzített internetről elérhető szolgáltatások sérülékenységeit, valamint monitorozni ezen weboldalak elérhetőségeit.

- További információk, kapcsolódó nyomtatványok, valamint Gyakran Ismételt Kérdések az **NKI honlapján érhetőek el.**

Következmény-menedzsment:

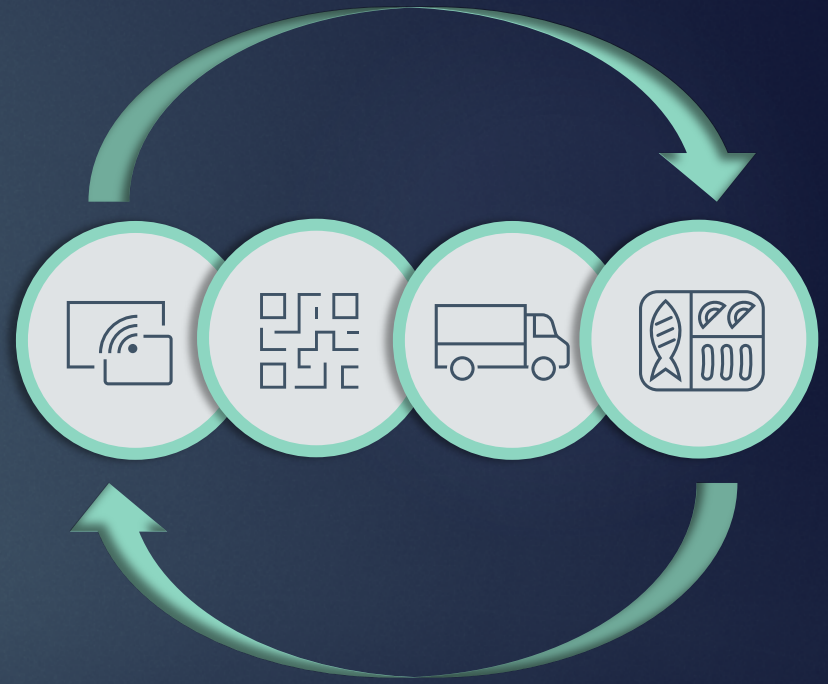
A biztonsági incidenskezelés a biztonsági fenyegetések vagy incidensek valós idejű azonosításának, kezelésének, rögzítésének és elemzésének folyamata.

1. A biztonsági incidenskezelési folyamat jellemzően az incidens bekövetkeztére vonatkozó **riasztással és az incidenskezelő csoport bevonásával kezdődik.**
2. Ezt követi az azonosított **incidensek értékelése** a kockázat mérséklésére irányuló megfelelő következő lépések meghatározása érdekében.
3. Majd **reagálás az incidensre** az incidens behatárolásával, kivizsgálásával és megoldásával.

AZ ELLÁTÁSI LÁNC, MINT KIBERBIZTONSÁGI KOCKÁZAT

Az **ellátási lánc** azokra az emberekre, folyamatokra és technológiákra utal, amelyek az áruk vagy szolgáltatások egyik csoporttól a másikhoz történő szállításához kapcsolódnak.

- A hálózati ellátási lánc megtámadása
- A szoftver-ellátási lánc megtámadása
- A hardver ellátási lánc megtámadása
- Kibertámadás az ellátási láncban működő vállalkozások ellen



Supply-chain támadások (SCA)

- Solaarwinds
- Világgazdasági fórum: a vizsgált szervezetek ért kibertámadások során 39-62%-ában érintett harmadik fél.
- Jövő: egyre nagyobb mértékű harmadik fél függőség
- NIS2 megfelelőségi kérdés

Hazai helyzetkép:

1. A harmadik fél függőségek kezelése általánosan egy gyengén menedzselt terület.
2. A külső fejlesztők felé specifikus biztonsági elvárások meghatározása nem elterjedt gyakorlat.
3. A biztonságos fejlesztési kompetencia korlátozottan áll rendelkezésre.
4. A harmadik fél függőségek nyilvántartása és kezelése korlátozottan valósul meg.

AZ ELLÁTÁSI LÁNC VÉDELME

- A kockázatkezelési stratégiának ki kell térnie az ellátási láncra is
- Egy incidenskezelési forgatókönyv létrehozása az ellátási láncot érintő incidensek esetére
- Legyenek összeszedve a rendszerhez hozzáféréssel rendelkező személyzetet, vállalkozót, szállítót és beszállítót
- Beszállítók/szállítók bevonása a kiberreziliencia, az incidensreagálási vagy a katasztrófa-helyreállítási tevékenységekbe
- Rendszeres ellenőrzések elvégzése

BIZTONSÁGI INTÉZKEDÉSEK

- A minimális jogosultság elvének bevezetése
- Kerüljenek törlésre a nem használt email címek
- Biztonságos jelszavak használata
- Többfaktoros hitelesítés használata
- Biztonsági másolatok készítése és biztonságos tárolása
- Szoftverek telepítésének és használatának korlátozása

Módszerek a kockázatok csökkentéséhez:

- **1. év, 1. félév:** *Harmadik fél kockázatértékelés*
  - A harmadik felekkel való kapcsolatok feltérképezése és a függőségek értékelése. Ez magában foglalja az adatmegosztást, a rendszerhálózatok elérését és más kölcsönös függőségeket.
  - A harmadik felek kiberbiztonsági értékelése. Ez tartalmazza a harmadik fél kiberbiztonsági politikájának és gyakorlatának értékelését, valamint a kiberbiztonsági incidensek kezelésére vonatkozó eljárásokat.

- **1. év, 2. félév:** *Harmadik fél kiberbiztonsági nyomon követés*
  - A harmadik felek kiberbiztonsági állapotának nyomon követésére szolgáló rendszer bevezetése. Ez magában foglalja a harmadik fél kiberbiztonsági állapotának folyamatos monitorozását és jelentését.
  - Az adatbiztonsági incidensek kezelésére vonatkozó eljárások kidolgozása és bevezetése, amely folyamatok magukban foglalják a harmadik féllel való együttműködést is.

- **2. év, 1. félév:** *Kockázatcsökkentő intézkedések*
  - Kockázatcsökkentő intézkedések bevezetése a harmadik felekkel. Ez magában foglalja a kiberbiztonsági képzéseket, a kiberbiztonsági politikák fejlesztését és bevezetését, valamint a harmadik féllel közös kiberbiztonsági gyakorlatokat.
  - A harmadik fél kiberbiztonsági állapotának folyamatos felülvizsgálata és értékelése. Ez magában foglalja a harmadik fél kiberbiztonsági állapotának folyamatos monitorozását és jelentését, valamint az adatbiztonsági incidensek kezelésére vonatkozó eljárások felülvizsgálatát és frissítését.

- **2. év, 2. félév:** *Folyamatos felügyelet és javítás*
  - Kiberbiztonsági auditok és ellenőrzések rendszeres végrehajtása a harmadik feleknél. Ezek az ellenőrzések segítenek felmérni a harmadik felek kiberbiztonsági helyzetét és azonosítani az esetleges kockázatokat.
  - A harmadik fél kiberbiztonsági állapotának nyomon követésére szolgáló rendszer folyamatos fejlesztése és frissítése, hogy mindig naprakész információkat szolgáltasson a harmadik felek kiberbiztonsági helyzetéről.

- **3. év, 1. félév:** *Kockázatkezelési stratégiák továbbfejlesztése*
  - Új kockázatkezelési stratégiák kidolgozása és bevezetése, amelyek a harmadik felekkel való kapcsolatokra és a harmadik felek kiberbiztonsági állapotára összpontosítanak.
  - A harmadik felek kiberbiztonsági képzésének és tudatosságának továbbfejlesztése. Ez magában foglalja a kiberbiztonsági képzések és tudatosságnövelő programok rendszeres frissítését és továbbfejlesztését.

- **3. év, 2. félév:** *Folyamatos felügyelet és javítás*
  - Folyamatos felülvizsgálat és frissítés a harmadik felek kiberbiztonsági állapotának monitorozására szolgáló rendszerben, hogy mindig naprakész információkat szolgáltasson a harmadik felek kiberbiztonsági helyzetéről.
  - Folyamatos kiberbiztonsági auditok és ellenőrzések végrehajtása a harmadik feleknél, hogy felmérjék a harmadik felek kiberbiztonsági helyzetét és azonosítsák az esetleges kockázatokat.

Felhőszolgáltatások bevezetése

- **1. év, 1. félév:** *Felhőszolgáltatások értékelése és kiválasztása*
  - Különböző felhőszolgáltatások értékelése, amelyek megfelelnek a szervezet igényeinek és követelményeinek.
  - Ez magában foglalja a szolgáltatások költségének, teljesítményének, biztonsági képességeinek és kompatibilitásának értékelését.

- **1. év, 2. félév:** *Biztonsági infrastruktúra tervezése és bevezetése*
  - Biztonsági infrastruktúra tervezése a felhőszolgáltatások védelmére. Biztonsági infrastruktúra bevezetése a felhőszolgáltatásokban.

Felhőszolgáltatások bevezetése

- **2. év, 1. félév:** *Felhőszolgáltatások bevezetése és felhasználói képzés*
  - Felhőszolgáltatások bevezetése a szervezetben.
  - Felhasználói képzés a felhőszolgáltatások használatáról és biztonsági gyakorlatokról.

- **2. év, 2. félév:** *Folyamatos felügyelet és javítás*
  - Folyamatos felügyelet és biztonsági incidensek kezelése a felhőszolgáltatásokban.
  - Biztonsági infrastruktúra továbbfejlesztése és frissítése.

Felhőszolgáltatások bevezetése

- **3. év, 1. félév:** *Incidenskezelési terv kidolgozása és bevezetése*
  - Incidenskezelési terv kidolgozása és bevezetése a felhőszolgáltatásokban.
  - Felhőstratégia továbbfejlesztése, ami magában foglalja a szolgáltatások skálázását, a biztonsági infrastruktúra fejlesztését és a felhőszolgáltatóval való kapcsolatok kezelését.

- **3. év, 2. félév:** *Átállási stratégia kidolgozása*
  - Átállási stratégia kidolgozása, amely lehetővé teszi a szervezet számára, hogy gyorsan és hatékonyan átálljon egy másik felhőszolgáltatóra vagy visszatérjen a földi infrastruktúrába, ha szükséges.
  - Az átállásistratégia tesztelése, hogy biztosítsa a folyamat simaságát és hatékonyságát.

Biztonsági naplóelemzés bevezetése

- **1.év, 1.félév:** *Infrastruktúra auditálás és igényfelmérés*
  - Egy mélyreható infrastruktúra audit szükséges, hogy meghatározzuk a szervezet jelenlegi állapotát.
- **1. év, 2. félév:** *Eszközök implementációja és konfigurálása*
  - Be kell vezetni és tesztelni kell azokat az eszközöket, amelyeket a naplóelemzéshez kiválasztotta szervezet.
  - Meg kell tervezni a rendszer architektúráját, kapcsolódási pontjait, hardver-és hálózatigényét, licenszelést, mentést és archiválást és nem utolsó sorban a riasztási és incidenskezelési folyamatokat.
  - Az implementáció folyamán követni kell a gyártók és szállítók biztonsági útmutatóit.

Biztonsági naplóelemzés bevezetése

- **2.év, 1.félév:** *Naplóelemzési rendszer élesítése és finomhangolása*
  - Sikeres tesztelés után élesíteni kell a naplóelemzési rendszert, és meg kell kezdeni a gyakorlati alkalmazást.
  - Az eseményeket a MITRE ATT&CK keretrendszerrel összhangban kell bekategorizálni.

- **2. év, 2. félév:** *Személyzet képzése és folyamatos edukáció*
  - Képzési programokat kell kialakítani a munkatársak számára a biztonsági naplóelemzésről és az új eszközök használatáról.

Biztonsági naplóelemzés bevezetése

- **3.év, 1.félév:** *Naplóelemzési rendszer továbbfejlesztése és finomítása*
  - Új szabályok, szűrők és riasztások bevezetése, valamint a naplózási politikák és protokollok felülvizsgálata kerül sorra.

- **3. év, 2. félév:** *Személyzet képzése és folyamatos edukáció*
  - A naplóelemzési eszközök és technológiák piaci trendjeit figyelemmel kell kísérni, hogy naprakész legyen a rendszer és a kapcsolódó munkafolyamatok.
  - Folyamatosan értékelni kell a szervezet biztonsági helyzetét és a naplóelemzési rendszer hatékonyságát, és ahol szükséges, frissíteni és továbbfejleszteni a rendszert.

Köszönjük a figyelmet!

edt@nki.gov.hu

nki.gov.hu

nki.gov.hu

facebook.com/nki.gov.hu

KIBERTÁMADÁS! PODCAST

1996

Fortes fortuna adiuvat

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET