Kiberbiztonságra való felkészülés lépései

Útmutató a NIS2 által érintett cégek beszállítóinak

Készítette Nagy Imre Gábor
Elektronikus Információbiztonsági vezető, ISO 27001 auditor
Verzió: 2.0

Tartalom

1. Bevezetés

Az ma már senkinek nem kell magyarázni, hogy kiberbiztonság nem olyan teendő, mely csak a legnagyobb cégeket érinti. Ezt a problémát felismerve 2022-ben az EU elfogadta a NISD2/NIS2 irányelvet, amit minden tagálammban saját jogrendjébe átemelve egységesen 2024 október 18-tól alkalmaznia kell. Ennek az irányelvnek van egy fontos, de kevésbé tárgyalt része a beszállítói lánccal kapcsolatos követelmények. A jelen dokumentum ebben a témakörben kíván segítséget nyújtani.

2. Kinek szól a kézikönyv?

A NIS2 sok feladatot fog jelenteni olyan cégeknek, melyek nem tartoznak a NIS2 hatálya alá, de beszállítói olyan cégnek, amelyek azonban a NIS2 hatálya alá tartoznak.

Két fajta beszállítói kört lehet elkülöníteni

1. Az informatikai cég, aki valamilyen informatikai megoldást szállít be
2. Egyéb beszállító

Jelen dokumentum olyan beszállítóknak próbál segítséget nyújtani, akik a második körbe tartoznak és átlagos informatikai felkészültséggel rendelkező a társaságok.

3. Alapvető dolgok

Van néhány dolog, amit attól függetlenül el kell végeznie minden cégnek, hogy érintett-e vagy sem a az új kiberbiztonsági előírások által.

3.1 Erős jelszavak kialakítása és kezelése

Az egyik legnagyobb gond a legtöbb KKV-nál, hogy a jelszavakat szükséges rossznak tartják és csak annyit foglalkoznak vele, amennyi szükséges. Pedig a jelszavak az első védelmi vonalat jelentik. Egy erős jelszó nehezen kitalálható, és betűk, számok, valamint speciális karakterek kombinációjából áll.

3.1.1 Jelszavak kezelése

- Ne használja ugyanazt a jelszót több fiókhoz!
- Használjon jelszókezelő programokat a jelszavak biztonságos tárolásához és kezeléséhez.
- Rendszeresen legyen megváltoztatva a jelszó

3.1.2 Mitől lesz erős a jelszó?

- Használjon legalább 12 karakterből álló jelszót.
- Kombinálni kell a nagy- és kisbetűket, számokat és szimbólumokat.
- Kerülni kell a könnyen kitalálható információkat, mint például a születési dátumokat vagy a kedvenc sportcsapat nevét.

3.2 Kétfaktoros hitelesítés (2FA) alkalmazása

3.2.1 Mi az a kétfaktoros hitelesítés?

A kétfaktoros hitelesítés egy olyan biztonsági folyamat, amely két különböző hitelesítési módszert igényel a felhasználó személyazonosságának igazolására. Ez lehet egy jelszó és egy email címre küldött kód kombinációja. De ilyen, amikor valaki egy applikáció segítségével azonosítja magát felhasználó.

3.2.2 Miért van erre szüksége egy cégnek?

A védelem miatt. A legtöbb CRM már képes kezelni a kétfaktoros azonosítást. Ennek segítségével ki lehet védeni az illetéktelen hozzáférést – többek között – üzleti titkokhoz

3.2.3 Hogyan lehet beállítani a kétfaktoros hitelesítést?

- Keressük meg a fiók beállításaiban a kétfaktoros hitelesítés lehetőségét.
- Vagy beállításra kerül egy email cím, vagy un. autentikátor programot kell letölteni a mobiltelefonra és azt kell összepárosítani a programmal.
- Aktiváljuk a kétfaktoros hitelesítést, és győződjünk meg róla, hogy működik.

4. Szoftverek/programok/applikációkkal kapcsolatos teendők

Sokan azt hiszik, hogy ezek különböző dolgokat takarnak, de valójában mind ugyanazt jelenti S mindegyik esetében a legfontosabb, hogy **legálisan** szerezze be a KKV. Legálisan is lehet ingyenes szoftverez jutni, de az egyik leggyakoribb informatikai kockázatot az illegálisan beszerzett programok használata okozza egy cég életében.

4.1 Miért fontosak a szoftverfrissítések?

A legtöbb felhasználó tart a frissítésektől. Sajnos az egyik legelterjedtebb operációs rendszer esetén – MS Windows – az elmúlt években többször is megtörtént, hogy a felhasználók egy részénél elromlottak a program egyes funkciói. De ettől függetlenül a szoftverfrissítések tartalmazzák a legújabb biztonsági javításokat, amelyek védelmet nyújtanak az újonnan felfedezett sebezhetőségekkel szemben.

4.1.1 Hogyan végezzen rendszeres frissítéseket a cég?

- Legyen bekapcsolva az automatikus frissítések opció az operációs rendszeren és az alkalmazásokon.
- Rendszeresen legyen ellenőrizve a frissítések elérhetősége, és telepítése.
- Csak megbízható forrásokból származó szoftverek használjon mindenki a társaságnál.

4.2 Vírusirtó és kémprogram-elhárító szoftverek

4.2.1 Miért van szükség ezekre a programokra?

A vírusirtó és kémprogram-elhárító szoftverek védelmet nyújtanak a rosszindulatú programokkal szemben, amelyek károsíthatják a számítógépet vagy ellophatják az adatainkat.

4.2.2 Hogyan lehet megfelelő vírusirtót választani?

- Válasszunk olyan vírusirtót, amely teljes védelmet nyújt. Legyen felvértezve valós idejű védelemmel és rendszeres frissítésekkel.
- Több operációs rendszert támogasson pl PC, Android, iOS
- Figyeljünk az ismert biztonsági cégek termékeire és olvassunk felhasználói véleményeket.
- Telepítsünk kémprogram-elhárító szoftvert is, amely kifejezetten a kéretlen programok felderítésére és eltávolítására specializálódott.

4.3 Biztonsági mentések készítése

4.3.1 Miért fontos a biztonsági mentés?

Az egyik legnagyobb érték az adat és információ egy cég életében. A rendszeres biztonsági mentések védelmet nyújtanak az adatvesztés ellen, legyen szó hardverhiba, vírusfertőzés vagy emberi hiba következményéről.

4.3.2 Hogyan végezzen biztonsági mentéseket egy KKV?

- Használjon külső merevlemezt pl NAS rendszert, vagy felhőalapú tárhelyet a fontos adatok mentésére.
- Állítson be az automatikus mentést, hogy rendszeresen és zavartalanul történjen az adatmentés.
- Ellenőrizze rendszeresen a mentések épségét és hozzáférhetőségét.

5. Biztonságos internethasználat

5.1 Biztonságos böngészési szokások

- Kerülni kell az ismeretlen vagy gyanús weboldalakat.
- Ne kattintson senki ismeretlen linkekre vagy mellékletekre e-mailekben.
- Használjon mindenki böngésző kiterjesztéseket, amelyek figyelmeztetnek a potenciálisan veszélyes weboldalakra.

5.2 Biztonságos letöltések

- Csak biztos forrásokból töltsön le bárki szoftvereket és fájlokat.
- Használjon letöltéskezelő szoftvert, amely ellenőrzi a fájlok biztonságát még a letöltés előtt.

5.3 Biztonságos hálózati beállítások

Ez elsőre bonyolultnak tűnhet, de pár egyszerű megoldással biztonságosabbá lehet tenni a céges hálózatokat.

5.3.1 Wi-Fi hálózatok védelme

- Erős jelszó használata a Wi-Fi hálózaton.
- Vendég hálózat kialakítása a külsősök számára
- Legyen bekapcsolva a WPA3 titkosítást, ha elérhető a routeren.

- Legyen korlátozott a hozzáférés a hálózathoz a megadott MAC címek alapján.

5.3.2 VPN használata

A VPN az online adatvédelem alapvető biztonsági eszköze. VPN nélkül mások könnyen lehallgathatják és megtekinthetik az internetes tevékenységeidet. Ebbe beletartoznak a böngészési előzmények, a letöltött fájlok, az online banki adatok és a jelszavak.

A VPN segítségével az adatok védve lesznek, de pl lassíthatja az internetes sávszélességet

- Megbízható VPN szolgáltatást érdemes választani, amely erős titkosítást és adatvédelmet biztosít.
- Nyilvános Wi-Fi hálózatokhoz való csatlakozáskor javasolt VPN használata.

6. Humánerőforrás

A támadások 90%-a az emberi tényező alapján talál be egy cég életébe. Létfontosságú, hogy a munkatársak tudatossága és felismerő képessége naprakész legyen.

6.1 Kiberbiztonsági tudatosság növelése

6.1.1 Oktatás és képzés

- Legyen szervezve oktatás kiberbiztonsági támban
- Rendszeresen legyen ezzel kapcsolatos tudatosság-növelés legalább évente egyszer.
- Ha van erre lehetőség, akkor a KKV kövesse a kiberbiztonsági trendeket és fenyegetésekről.

6.1.2 Gyakorlatok és próbatámadások

Ha van erre lehetőség a cég életében, akkor javasolt, hogy részt vegyen a cég szimulált támadásban és gyakorlaton. Így a cég teszteli a rendszerei biztonságát és felkészíti kollégáit, hogy miképp cselekedjenek egy valós helyzetekben.

- Érdemes szakértőket hívni, hogy végezzenek penetrációs teszteket és auditokat.
- A cég vezetése értékelje a biztonsági irányelveinket a tesztek eredményei alapján.

7. Haladó szint

A NIS2 itt nem áll meg, és megrendelő cég, aki érintett NIS2-ben szintén nem fog itt megállni. Szüksége lesz dokumentációr, ami alapján látja, hogy a beszállítója nem jelent számára kiberbiztonsági fenyegetést.

7.1 Milyen dokumentációk lehetnek ezek?

7.1.1 Informatikai Információs Szabályzat

A legalapvetőbb dokumentáció, amely Magyarországon is elérhető számos helyen, az Informatikai Biztonsági Szabályzat (IBSZ). Ez nagy vonalakban összefoglalja a cég informatikai kiberbiztonsági tevékenységét és irányelveit. Ez alapján már be lehet mutatni, hogy mivel is rendelkezik a cég. Egy minta IBSZ a 11. fejezetben is megtalálható.

7.2 További dokumentumok

Rengeteg dokumentáció segítheti a kiberbiztonság munkát. Néhány felsorolásszerűen

- Adatvagyonleltár
- Kockázatelemzési javaslatok
- Incidenckezelési terv
- Üzletmenet-folytonossági Terv (BCP)
- Katasztrófa utáni helyreállítási terv (DRP)

7.3 Incidenskezelés

Ez az a tevékenység, amire valószínűleg rá fog kérdezni a NIS2 általérintett cég, ezért érdemes pár szót említeni róla.

7.3.1 Mi az incidenskezelés?

Az incidenskezelés a kiberbiztonsági támadások vagy más biztonsági események kezelésére és megoldására irányuló folyamatok összessége.

7.3.2 Hogyan lehet felkészülni az incidenskezelésre?

- A cég alakítson ki világos eljárásokat és szabályokat az incidensek jelentésére és kezelésére.
- Tartson rendszeres gyakorlatokat, hogy a csapat felkészültségét fenntartsa a vállalat.

8. Szabványok

Két nemzetközi szabvány is segít, hogy ha tényleg időt és pénz tud áldozni a cég a kiberbiztonsági felkészülésre. Azonban mindkettő bevezetése már külső szakértőt igényel. Ezek a szabványok:

- NIST 800-53 ver5 – a 7/2024-es MK rendelet ez alapján készült, amit a NIS2 által érintett cégeknek be kell tartani.
- MSZ ISO 27001:2023 – a jól ismert ISO család tagja

9. Jogszabályi hattér

2024 év végére majdnem az összes jogszabály megszületett, ami a NIS2 megfelelés kapcsán szükséges. A legfontosabbak a következők:

- 2024. évi LXIX tv. Magyarország kiberbiztonságáról
- 418/2024 (XII. 23) Kormány rendelet. Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

10. Gyakran Ismételt kérdések (GYIK)

Az alább felsoroltak olyan rövid magyarázatok, melyek KKV munkatársaktól érkeztek be.

- *Tárhelyek/felhő*
  Az EU-n belűl szigorúan vannak szabályozva a felhőszolgáltatások. Több közül lehet választani pl Google, Microsoft, Amazon, Apple –
  Felhőszolgáltatás esetén végig kell gondolni, hogy mire akarom használni a felhőt. Egyénileg vagy cégben? Tárhelyre van csak szükségem, vagy több szolgáltatást is használni akarok felhőben? Nincs két ugyanolyan megoldás. Ha tárhelyet akarok és Androidot használok a Google Drive lehet megoldás. Ha Office csomagom van, akkor Onedrive előfizetés lehet az ideális megoldás. Ez cégenként és egyénenként eltérő lehet.
- *Apple (iOS) vs Android –*
  Alap biztonság kérdésében nincs különbség a két eszköztípus között.
- *Verziókövetés – kell-e cserélnem telefont újra, ha lejár a biztonsági frissítés?*
  A Apple hivatalos közleménye szerint 5 évig ad ki frissítéseket egy adott verziójú iPhone-hoz. A legnagyobb Android gyártó a Samsung és maga a Google is 7 évet vállal. Ezt követően biztonsági szempontból kockázatos a telefonokat használni.
- *Hol tudom ellenőrizni, milyen biztonsági verziós a telefonom (Apple / Android) ÉS hol teszik közzé hivatalosan a verziókövetés határidejét (Apple / Android)?*
  A beállításokban található meg az aktuális verzió.
- *Bankolás telefonon applikációval*
  Mivel legalább 2 faktoros ellenőrzés van hozzá szükség, ezért alapvetően biztonságos
- *E-mailezés telefonon*
  A legtöbb ember csak olvassa az emailjeit. Javasolt megbízható email kliens használata és a jelszavak megváltoztatása időnként.
- *Applikációk a telefonon, mire figyeljünk telepítés esetén (Google Play / App Store) – (PRO licence, vélemények, letöltésszám stb.)*
  Több alkalmazásbolt is van, ahonnan le lehet tölteni egy programot. A telefonokon az alapbeállítás az operációs rendszertől függően A Google Play vagy az App Store. De ilyen alkalmazásboltja van pl az Amazonnak is. Néhány szempont amire figyelünk letöltésnél
    - A legfontosabb, hogy direktbe ismeretlen weboldalról ne töltsön le senki semmilyen alkalmazást.
    - mielőtt letölt bármilyen programot nézze meg, hogy hányan töltötték le
    - milyen vélemények vannak a programhoz kapcsolódóan
    - honnan vannak a vélemények pl mindenki Bangladesből szól hozzá, az elég gyanús
    - mikor frissítették az alkalmazást legutoljára
    - ha az van odaírva, hogy vásárlási lehetőség az appban, akkor ott nagy valószínűséggel reklámmal fogunk találkozni
- *DÁP (Megkerülhetetlen lesz.)*
  Az állam mindenképp bevezeti a Digitális Állampolgárság feltételeit. Jelenleg a DÁP törvény alapján megvan a kötelezettek köre és megvan, aki opcionálisan kell biztosítania az alkalmazását.
- *Mac vs PC; szoftverfrissítések (operációs rendszer, programok)*
  Mindig a legfrissebb operációs rendszer használata javasolt.

Az iMacek frissítése ritkán jár jelentős hardverberuházással és a gépek hardware-e kevésbé avul el. Egy akár 10 éves iMac gép is normál használatra tökéletes lehet.
A Windowsos gépek elavulása sokkal gyorsabb, mert sokszor gyenge hardware-rel rendelkeznek és az újabb és újabb verziók egyre nagyobb teljesítmény írnak elő.

- *Webáruház üzemeltetés.*
  Nem lehet mindenhez érteni. A webáruházakkal kapcsolatban rengeteg szabály van, amit be kell tartani. Javasolt vagy külsős üzemeltetésű webáruházat használni, vagy saját embert felvenni hozzá, vagy megbízni egy céget vele
- *Adataink biztonsági mentése eszközökről és tárhelyekről (telefon, számítógép, webáruház, ERP-rendszer, saját szerver, felhő szerver) – honnan, mit, hova, hogyan?*
  Az egyik legalapvetőbb dolog, hogy védeni kell az adatokat. Azt kell végig gondolni, hogy mely eszközöket és az ezeken található adatokat hogyan akarja a vállalkozás lementeni. Mentési megoldások alapvetően a következők lehetnek
    - Helyi adathordozóra pl NAS
    - Felhőbe

  A felhő mindenkinek kézenfekvő megoldás, de ott olyan szolgáltatás érdemes választani, amit be lehet állítani telefonra és PC/laptopra is pl OneDrive.
- *Meghajtó titkosítása - Bitlocker*
  A felhasználók számára, különböző segédprogramok segítséget nyújtanak, hogy az összes adatot titkosítsák a merevlemezen. A BitLocker Drive Encryption egy Microsoft Windows biztonsági és titkosítási funkciója. Ilyen lehetőségek az okostelefonon is rendelkezésre állnak.
- *Régi eszközök, háttértárak eladása, megszüntetése (data recovery!)*
  Rendkívül kritikus probléma a háttértárak eladása. A bankok pl. kifejezetten tiltják. Az egyre fejlettebb visszaállító programok miatt könnyen kerülhetnek az adataink illetéktelen kezekbe
- *Vírusirtók*
  Minden évben kiadnak különböző listákat, amiben tesztelik a virusírtókat. 2024-ben El kell dönteni, hogy mire akarjuk használni. Tud-e komplett védelmet adni, pl. több operációs rendszerre, vagy csak egyre. Ez egyénenként és cégenként is változhat. Az biztos, hogy legyen vírusírtó minden eszközünkön a telefonon is!
- *VPS-szolgáltatók,*
  A VPS (Virtual Private Server) szolgáltatás egy olyan erőforrás szolgáltatás, amely lehetővé teszi, hogy saját, elkülönített szerveren futtassuk weboldalainkat és alkalmazásainkat.
- *VPN csatlakozás*
  A VPN az online adatvédelem alapvető biztonsági eszköze. VPN nélkül mások könnyen lehallgathatják és megtekinthetik az internetes tevékenységeidet. Ebbe beletartoznak a böngészési előzmények, a letöltött fájlok, az online banki adatok és a jelszavak.
  A VPN segítségével az adatok védve lesznek, de pl lassíthatja az internetes sávszélességet
- *Szerverkérdés: saját szerver vs. hazai VPS vs. külföldi VPS (ott is melyik)*
  Ez a cégmérettől függ. Ha van dedikált munkatárs, aki ért hozzá és karban tudja tartani, csak akkor érdemes saját szervert üzemeltetni. Ha nincs, akkor érdemes virtuális szervert használni. Ebben az esetben olyat érdemes használni, ami garantálja, hogy adataink az EU-n belül maradnak. Vagy Svájcban pl TresorIT
- Saját szerver / VPS esetén: elérési, biztonsági kérdések
  Itt már haladó ismeretek szükségesek. Ha weboldalról lépünk be, akkor mindenképp csak https protokollt használó oldalról. Ha nem weboldalról, akkor FTPS-en keresztül lépjünk be
- *Jelszavak: erős jelszóhasználat; jelszókezelési program használata*
  Alapvető kérdés, hogy erős, egyedi jelszavakat használjon a cég és ezeket meghatározott időközönként cserélje le. Mivel nem lehet minden jelszót fejben tartani érdemes jelszókezelőt használni pl KeePassXC.
- *Nyílt forráskódú vs. fizetős szoftverek. Megbízható szoftverek.*

A kérdés, hogy mit használunk és erre hajlandóak vagyunk-e áldozni. Pl LibbreOffice egy megbízható és jól működő program. Az MS Word azonban jóval elterjedtebb. Ez egy üzleti döntés. Ha szükségem van IT támogatásra, akkor érdemes fizetős software-t használni. Ha azonban ritkán használok egy programot akkor pl egy GIMP tökéletes választás lehet a Photoshop helyett.

- *Humán tényező (gyerek; én; kollégák; kollégák gyerekei; takarítónő; stb.)*
  A legnagyobb veszélyfaktor a humán tényező. Egy módon lehet elkerülni. A folyamatos tudatosítással, oktatással.
- *IT-szolgáltató cégek megbízhatóságának ellenőrzése (ISO 27001; más?)*
  Minden ISO szabvány annyit ér, amennyit betartanak belőle. Egy ISO 27001-es szabvány egy jól jel, de nem garancia semmire.

í

11. Informatikai Biztonsági Szabályzat minta

1. Bevezetés Az informatikai biztonság elsődleges célja, hogy megvédje a vállalat informatikai rendszereit, adatait és erőforrásait az illetéktelen hozzáférésektől, adatvesztéstől, visszaélésektől és egyéb fenyegetésektől. Jelen szabályzat az informatikai biztonság fenntartására vonatkozó alapelveket, szabályokat és eljárásokat tartalmazza.

2. Alapelvek

- **Adatvédelem:** Az érzékeny adatok védelme elsődleges fontosságú.
- **Hozzáférés-szabályozás:** Csak a megfelelő jogosultsággal rendelkező személyek férhetnek hozzá az informatikai rendszerekhez és adatokhoz.
- **Folyamatosság biztosítása:** Az üzletmenet-folytonosság érdekében az informatikai rendszerek megbízható működését biztosítani kell.
- **Tudatosság:** Minden munkavállalónak ismernie kell az informatikai biztonsági alapelveket és be kell tartania azokat.

3. Hatály Ez a szabályzat minden munkavállalóra, alvállalkozóra, partnereinkre, valamint a vállalat által használt összes informatikai eszközre és rendszerre vonatkozik.

4. Felelősségi körök

- **Informatikai vezető:** Felelős a szabályzat karbantartásáért és betartásáért.
- **Munkavállalók:** Kötelesek betartani a szabályzatban foglaltakat, jelenteni az esetleges biztonsági incidenseket.
- **IT csapat:** Felelős az infrastruktúra védelméért, karbantartásáért és a jogosultságok kezeléséért.

5. Hozzáférés-kezelés

- **Hitelesítés:** Az informatikai rendszerekbe való belépéshez egyedi azonosítók és jelszavak szükségesek.
- **Jelszókezelés:** Jelszavak minimális hossza 12 karakter, amelyek tartalmaznak kis- és nagybetűket, számokat, valamint speciális karaktereket.
- **Korlátozott hozzáférés:** Minden felhasználó csak azokhoz az adatokhoz és rendszerekhez férhet hozzá, amelyek aí munkakörének ellátásához szükségesek.

6. Adatvédelem és adatkezelés

- **Adatmentés:** Naponta automatikus adatmentés történik, amelyeket biztonságos helyen tárolunk.
- **Adatmegsemmisítés:** Az adatok megsemmisítése biztonságos és visszaállíthatatlan módon történik.
- **Titkosítás:** Érzékeny adatokat titkosítani kell az átvitel és tárolás során.

7. Biztonsági incidensek kezelése

- **Jelentési kötelezettség:** Minden biztonsági incidenst azonnal jelenteni kell az IT osztálynak.
- **Incidenskezelési folyamat:** Az IT csapat kivizsgálja az incidenst, dokumentálja az esetet, és meghatározza a szükséges lépéseket.

8. Oktatás és tudatosság

- Az új munkavállalók számára kötelező informatikai biztonsági oktatást biztosítunk.
- Évente rendszeres képzéseket tartunk a legfrissebb fenyegetésekről és védelmi mechanizmusokról.

9. Fizikai biztonság

- Az irodai helyiségekbe való belépés kizárólag belépőkártyával vagy engedéllyel lehetséges.
- Az informatikai eszközöket zárt, biztonságos helyen kell tárolni.

10. Szankciók A szabályzat megsértése fegyelmi eljárást, szerződésbontást vagy jogi lépéseket vonhat maga után.

11. Záró rendelkezések Ez a szabályzat a közzététel napjától lép hatályba, és az itt foglaltakat rendszeresen felül kell vizsgálni a technológiai és jogi változások figyelembevételével.

Mellékletek

1. Jelszókezelési szabályzat
2. Adatvédelmi eljárások
3. Példák biztonsági incidensekre és azok kezelésére

12. Jelszókezelési szabályzat minta

1. Cél

A jelen szabályzat célja, hogy meghatározza a jelszókezeléssel kapcsolatos alapelveket és követelményeket annak érdekében, hogy a vállalkozás információi és rendszerei biztonságban legyenek. Az itt foglaltakat minden alkalmazottnak, alvállalkozónak és partnereknek kötelező betartani.

2. Alapelvek

2.1. **Jelszók titkossága**

A jelszavakat szigorúan titokban kell tartani. Tilos azokat harmadik személynek kiadni vagy nem biztonságos módon megosztani.

2.2. **Erős jelszavak alkalmazása**

Az alkalmazott jelszavaknak meg kell felelniük az alábbi követelményeknek:

- Legalább 12 karakter hosszú legyen.
- Tartalmazzon kis- és nagybetűket.
- Legyen benne legalább egy szám és egy speciális karakter (pl. @, #, $).
- Ne tartalmazzon könnyen kitalálható információt (pl. születési dátum, évszámok, cégnév).

2.3. **Egyedi jelszavak**

Minden rendszerhez, alkalmazáshoz vagy szolgáltatáshoz egyedi jelszót kell használni.

3. Jelszókészítés és -kezelés

3.1. **Jelszók létrehozása**

- Az alkalmazottak jelszavait erősített jelszógeneráló eszközzel érdemes elkészíteni.
- A jelszókat soha ne jegyezzék fel papírra vagy ne tárolják nem biztonságos módon.

3.2. **Jelszókezelési eszközök**

- Az alkalmazottak használjanak jóváhagyott jelszókezelő alkalmazásokat (pl. KeyPass, Bitwarden, LastPass, Dashlane), hogy a jelszavakat biztonságosan tárolják.
- A jelszókezelő eszközökön belüli mesterjelszó erőssége kulcsfontosságú; ezt ugyancsak szigorú biztonsági szabályok szerint kell kezelni.

4. Jelszóvédelmi gyakorlatok

4.1. **Jelszók megosztása**

- Tilos jelszavakat e-mailben, chatalkalmazásban vagy bármely nem biztonságos módon megosztani.

- Ha jelszó megosztása elkerülhetetlen, azt kizárólag a jelszókezelő eszközök biztonságos megosztási funkciójával szabad elvégezni.

4.2. **Jelszócsere**

- Az alkalmazottak legalább 6 havonta cseréljék le a fontos rendszerekhez tartozó jelszavaikat.
- Ha gyanú merül fel arra, hogy egy jelszó kompromittálódott, azonnal cserélni kell.

4.3. **Automatikus kijelentkezés**

- Az eszközökön és alkalmazásokban automatikus kijelentkezést kell alkalmazni, ha hosszabb ideig nem használják azokat.

4.4. **Kétszintű hitelesítés (2FA)**

- A jelszóval védett rendszereken lehetőség szerint engedélyezni kell a kétszintű hitelesítést.
- A kódok generálására használjanak hitelesítő alkalmazásokat (pl. Google Authenticator, Microsoft Authenticator).

5. Oktatás és ellenőrzés

5.1. **Kiberbiztonsági oktatás**

- Minden alkalmazott vegyen részt rendszeres kiberbiztonsági oktatáson, amely tartalmazza a jelszókezeléssel kapcsolatos ismereteket is.

5.2. **Jelszóauditálás**

- Az IT csapat vagy rendszergazda időközönkként auditot végez a rendszerekben használt jelszavak megfelelőségének ellenőrzésére.
- Az auditok során kiemelten vizsgálják a gyenge jelszókat és a jelszócsere elmaradását.

6. Felelősség

6.1. **Munkavállalók**

- Az alkalmazottak felelősek az általuk használt jelszavak titkosságáért és biztonságáért.

6.2. **IT osztály vagy rendszergazda**

- Felelős az irányelv betartásának ellenőrzéséért, valamint az alkalmazottak tájékoztatásáért és oktatásáért.

A jelen szabályzat hatályba lépésének dátuma: **[dátum]**. A szabályzatot időközönként felül kell vizsgálni, hogy megfeleljen az aktuális biztonsági követelményeknek és legjobb gyakorlatoknak.

13. Adatvédelmi Szabályzat Minta

1. Bevezetés

Ez a szabályzat meghatározza a vállalat adatvédelmi eljárásait, amelyek célja az ügyfelek, partnerek és munkavállalók személyes adatainak biztonságos és jogszerű kezelése.

2. Adatkezelési alapelvek

A vállalat az alábbi alapelvek szerint kezeli a személyes adatokat:

- **Jogszerűség, tisztesség és átláthatóság:** Az adatok kezelése jogszerűen, tisztességesen és átlátható módon történik.
- **Célhoz kötöttség:** Az adatokat csak előre meghatározott, jogszerű célokra használjuk.
- **Adattakarékosság:** Csak a szükséges és releváns adatokat gyűjtjük és tároljuk.
- **Pontosság:** Gondoskodunk arról, hogy az adatok pontosak és naprakészek legyenek.
- **Tárolás korlátozása:** Az adatokat csak a szükséges ideig tároljuk.
- **Integritás és bizalmas kezelés:** Megfelelő technikai és szervezési intézkedésekkel védjük az adatokat.

3. Személyes Adatok Kezelése

3.1. Adatgyűjtés

A személyes adatokat kizárólag a szükséges célok érdekében gyűjtjük, beleértve az ügyfélkapcsolatok fenntartását, szerződéses kötelezettségek teljesítését és jogszabályi előírások betartását.

3.2. Adattárolás és Védelem

- Az adatokat biztonságos szervereken, titkosított formában tároljuk.
- Az adatkezeléshez csak az arra jogosult munkatársak férhetnek hozzá.
- Rendszeres adatmentést végzünk, és védelmi intézkedéseket alkalmazunk a jogosulatlan hozzáférés ellen.

3.3. Adattovábbítás

Személyes adatokat csak törvényes keretek között és megfelelő garanciák mellett továbbítunk harmadik feleknek.

4. Adatkezelési Jogok és Kérelmek

Az érintettek jogosultak:

- Tájékoztatást kérni az adataik kezeléséről,
- Hozzáférni a tárolt adataikhoz,
- Helyesbíteni vagy töröltetni az adataikat,
- Tiltakozni az adatkezelés ellen,

- Az adatkezelés korlátozását kérni.

5. Incidenskezelés

Adatvédelmi incidens esetén az alábbi lépéseket követjük:

1. Az incidens azonosítása és bejelentése.
2. Az érintett adatok körének meghatározása.
3. A szükséges védelmi intézkedések végrehajtása.
4. Az illetékes hatóság és az érintettek értesítése, ha szükséges.
5. A jövőbeni incidensek megelőzésére irányuló intézkedések bevezetése.

6. Felelősségek és Betartás

- Az adatvédelemért felelős személy folyamatosan ellenőrzi az adatvédelmi szabályok betartását.
- Az alkalmazottak számára rendszeres képzéseket biztosítunk az adatvédelmi előírásokról.
- A szabályzat megszegése esetén fegyelmi intézkedések lépnek életbe.

7. Záró rendelkezések

Ez a szabályzat minden munkavállalóra és partnerre vonatkozik, és rendszeresen felülvizsgálatra kerül az aktuális jogszabályoknak megfelelően.

14. Kiberbiztonsági Incidensek kezelési szabályzata minta

1. Adatszivárgás

Leírás: Egy illetéktelen fél bizalmas adatokhoz fér hozzá, vagy érzékeny információk kerülnek nyilvánosságra.

Problémamegoldás lépései:

1. Az incidens bejelentése az IT biztonsági csapatnak.
2. Az érintett rendszerek és adatok azonosítása.
3. Az illetéktelen hozzáférés megszüntetése (például jelszavak cseréje, hozzáférések korlátozása).
4. Az esemény forrásának és mértékének vizsgálata.
5. Az érintett felek értesítése (jogi, üzleti és ügyféloldali kommunikáció).
6. Helyreállítási és megelőző intézkedések végrehajtása.

2. Zsarolóvírus (Ransomware) támadás

Leírás: Egy rosszindulatú program titkosítja az adatokat és váltságdíjat követel azok visszaállításáért.

Problémamegoldás lépései:

1. A fertőzött rendszer leválasztása a hálózatról.
2. A támadás bejelentése a biztonsági csapatnak.
3. A támadás terjedésének megakadályozása más rendszerek védelmével.
4. A fertőzés forrásának azonosítása.
5. Az adatok visszaállítása biztonsági mentésekből.
6. A rendszer megtisztítása és a sebezhetőségek kijavítása.
7. Oktatás és megelőző intézkedések bevezetése.

3. DDoS (Distributed Denial of Service) támadás

Leírás: Nagyszámú kéréssel történő támadás, amely túlterheli a rendszert és elérhetetlenné teszi a szolgáltatást.

Problémamegoldás lépései:

1. Az anomális hálózati forgalom észlelése.
2. Az érintett szolgáltatások azonosítása.
3. A forgalom elemzése és a támadás azonosítása.

4. A támadás csökkentése forgalomszűrőkkel vagy DDoS-védelmi eszközökkel.
5. Együttműködés az internetszolgáltatóval a forrás korlátozására.
6. Az esemény elemzése és a további védekezési intézkedések meghatározása.

4. Adathalász (Phishing) támadás

Leírás: Egy támadó hamis e-mailt vagy weboldalt használ az érzékeny információk megszerzésére.

Problémamegoldás lépései:

1. Az adathalász e-mail vagy üzenet azonosítása és jelentése.
2. Az érintett dolgozók figyelmeztetése.
3. Az e-mail rendszeren és tűzfalakon keresztüli szűrési beállítások felülvizsgálata.
4. A kompromittált fiókokhoz tartozó jelszavak azonnali megváltoztatása.
5. A támadási minták elemzése a jövőbeni védekezéshez.
6. Oktatási kampány az alkalmazottak részére.

5. Belső fenyegetés

Leírás: Egy alkalmazott vagy belső személy szándékosan vagy véletlenül veszélyezteti a rendszer biztonságát.

Problémamegoldás lépései:

1. Az incidens észlelése és dokumentálása.
2. Az érintett személy azonosítása és a hozzáférésének korlátozása.
3. A jogi és HR osztály bevonása az eset kezelésébe.
4. A rendszer és adatok állapotának ellenőrzése.
5. A belső hozzáférési szabályok felülvizsgálata és megerősítése.
6. A biztonságtudatosság növelése az alkalmazottak körében.

Összegzés: Minden incidens esetén kulcsfontosságú a gyors beavatkozás, az esemény alapos kivizsgálása és a megfelelő megelőző intézkedések bevezetése a hasonló esetek elkerülése érdekében.