

KIEGÉSZÍTŐ MEGVALÓSÍTÁSI ÚTMUTATÓ

A CSI felhőbiztonsági modell alkalmazása az Ön szervezetében

A „Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs” projekt kísérő útmutatója (Erasmus+ 2024-1-AT01-KA220-VET-000245093).

Tananyagok és interaktív eszközök: gocloudsecure.eu

1. Az útmutató célja

Az ötszakaszos CSI-modell segít a kis- és középvállalkozásoknak (kkv-knak) felhőszolgáltatásaik biztonságosabb használatában, legyen szó szoftverről (SaaS), platformról (PaaS) vagy infrastruktúráról (IaaS).

Ez az útmutató kiegészíti a CSI-modell hivatalos dokumentációját. Röviden bemutatja az egyes szakaszokat, és gyakorlati példán keresztül segít megérteni a megvalósítás lépéseit, amelyeket a vállalkozások saját igényeikhez igazíthatnak.

További információkat, sablonokat és részletes útmutatást a CSI-modell öt szakaszához tartozó dokumentumokban talál.

Az útmutatót a CSI két alapvető eszközével együtt használja:

- **CSI Mátrix:** Interaktív eszköz, amely feltárja a felhőszolgáltatások fenyegetéseit, sérülékenységeit és kockázatait, és az OWASP Top 10 alapján értékeli őket. Az 1–3. szakaszban használható.
- **CSI-önértékelés & CSI-kurzus:** Önértékelés és tananyag a felhőtechnológia alapjairól, a kiberfenyegetésekről, a biztonságos tervezésről és az irányításról. A 3–4. szakasz képzéseinek előkészítését és megtartását támogatják.

Tipp: Az 1–3. szakasz során tartsa nyitva az útmutatót és a CSI Matrix eszközt. Kövesse az utasításokat, végezze el az értékelést, majd használja fel az eredményeket a következő szakaszokban.

2. A CSI-modell áttekintése

A CSI-modell öt egymásra épülő szakaszból álló, folyamatos ciklus. Minden szakasznak világos célja, fő lépései és a következő szakaszban felhasználható eredményei vannak.

Szakasz	Cél	Fő lépések	Eredmények
1. Elemzés	A felhőhasználat, a fenyegetések és az előírások áttekintése.	Szolgáltatások felmérése · CSI Matrix kockázatértékelés · Megfelelőség	Szolgáltatásjegyzék, kezdeti CSI Matrix értékelés, vonatkozó előírások.
2. Meghatározás	Biztonsági szabályok, kockázati sorrend és védelmi célok.	Szabályzat · Kockázatok rangsora · Védelmi célok · Felelősök	Felhőbiztonsági szabályzat, prioritások, célok és felelősségi körök.
3. Tervezés	Kockázatok és célok konkrét megvalósítási tervvé alakítása.	Kockázatcsökkentés · Hozzárendelés · Dokumentáció · Képzés	Intézkedési terv, táblázat, sablonok, listák és képzési terv.
4. Megvalósítás	Intézkedések bevezetése és a munkatársak képzése.	Műszaki lépések · Képzés és tudatosság	Bevezetett intézkedések, képzés és biztonságosabb, szabályos környezet.
5. Ellenőrzés	Hatékonyágvizsgálat és folyamatos fejlesztés.	Tesztek · KPI-k követése · Incidensek és visszacsatolás	Ellenőrzött intézkedések, irányítópult, tanulságok és fejlesztett szabályzatok.

3. Lépésről lépésre

Az öt szakaszt sorrendben hajtsa végre, mert mindegyik eredménye a következő szakasz kiindulópontja.

1. szakasz – Elemzés

Cél: Felmérni, milyen felhőszolgáltatásokat használ a vállalkozás, milyen fenyegetéseknek és sérülékenységeknek van kitéve, és milyen megfelelőségi követelmények vonatkoznak rá.

- **Felhőszolgáltatások felmérése:** Vegye számba az összes használt szolgáltatást (IaaS, PaaS, SaaS, tárhely, adatbázisok, hálózatok, biztonsági szolgáltatások). Jelölje a működés szempontjából kritikus elemeket.
- **Kockázatértékelés:** A CSI Matrix segítségével azonosítsa az egyes szolgáltatások fenyegetéseit (pl. adatszivárgás, DDoS-támadás), sérülékenységeit (pl. gyenge hitelesítés) és lehetséges következményeit (pl. adatvesztés, fiókfeltörés).
- **Megfelelőség ellenőrzése:** Tekintse át a vonatkozó uniós előírásokat (GDPR, DORA, NIS2) és a már alkalmazott vagy bevezetni kívánt szabványokat (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

Eredmény: Felhőszolgáltatás-jegyzék, kitöltött CSI Matrix értékelés és a megfelelőségi követelmények listája.

2. szakasz – Meghatározás

Cél: Biztonsági szabályokat kialakítani, rangsorolni a kockázatokat és meghatározni a vállalkozás védelmi céljait.

Az Európai Unió finanszírozásával. Az itt szereplő vélemények és állítások a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az OeAD-GmbH hivatalos álláspontjával. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem vonható felelősségre miattuk.

Projektazonosító: 2024-1-AT01-KA220-VET-000245093.

- **Biztonsági szabályzat:** Készítsen felhőbiztonsági szabályzatot a szolgáltatások biztonságos használatáról, a hozzáférések kezeléséről és az adatvédelemről.
- **Kockázatok rangsorolása:** A CSI Matrix minden kockázatát értékelje a bekövetkezés valószínűsége és a várható hatás alapján. A legfontosabbakra összpontosítson.
- **Védelmi célok:** Minden kiemelt kockázathoz rendeljen egyértelmű célt. Például a „gyenge hitelesítés” esetén a cél lehet a „felhasználói fiókok védelmének megerősítése”.
- **Szerepek és felelőségek:** Határozza meg, ki felel a felhőszolgáltatásokért, az adatokért, a biztonságért és a jogszabályi megfelelésért. Kisebb vállalkozásnál egy személy több feladatot is elláthat.

Eredmény: Felhőbiztonsági szabályzat, rangsorolt kockázatok, meghatározott védelmi célok és egyértelmű felelősségi körök.

3. szakasz – Tervezés

Cél: A kockázatokat és a védelmi célokat konkrét intézkedéseket, dokumentációt és képzést tartalmazó megvalósítási tervvé alakítani.

- **Kockázatcsökkentő intézkedések:** Minden védelmi célhoz rendeljen konkrét teendőt. A „fiókok védelmének megerősítése” például többtényezős hitelesítés (MFA) bevezetésével érhető el.
- **Intézkedések hozzárendelése:** Készítsen táblázatot arról, hogy az egyes intézkedések melyik felhőszolgáltatást védik.
- **Dokumentáció:** Készítsen megvalósítási ellenőrzőlistát, incidenskezelési sablont és az auditnaplók ellenőrzésére szolgáló űrlapot.
- **Képzési program:** Tervezzen rövid, gyakorlati modulokat a CSI tananyagai alapján, a csapat tudásához és igényeihez igazítva.

Eredmény: Kockázatcsökkentő intézkedések listája, hozzárendelési táblázat, megvalósítási dokumentumok és képzési terv.

4. szakasz – Megvalósítás

Cél: A tervezett biztonsági intézkedések bevezetése az érintett felhőszolgáltatásokban és a munkatársak képzése.

- **Műszaki intézkedések:** Hajtsa végre a 3. szakasz tervét: kapcsolja be például az MFA-t, a titkosítást és az identitás- és hozzáféréskezelési szabályokat (IAM, RBAC). Kezdje a gyorsan megvalósítható lépésekkel, és használjon beépített eszközöket, például az AWS Configot vagy az Azure Security Centert.
- **Képzés és tudatosság:** Tartsa meg a képzéseket, különös tekintettel a CSI Matrix által feltárt kockázatokra. Használja a CSI tananyagait.

Eredmény: Bevezetett biztonsági intézkedések, képzett munkatársak és a végrehajtást igazoló dokumentumok.

5. szakasz – Ellenőrzés

Cél: A bevezetett intézkedések hatékonyságának értékelése és a vállalkozás védelmének folyamatos fejlesztése.

- **Tesztelés:** Végezzen szimulált támadásokat, kontrollvizsgálatokat és biztonsági felméréseket.

- **Nyomon követés:** Figyelje a fő teljesítménymutatókat (KPI-eket), például a sikertelen bejelentkezéseket, a hibás konfigurációkra figyelmeztető jelzéseket és az elmaradt biztonsági frissítéseket. Ehhez egyszerű irányítópult is elegendő.
- **Visszacsatolás:** Vezessen incidensnyilvántartást arról, mi történt, miért, milyen hatással járt és hogyan kezelték. A tanulságokat építse be az 1. és 2. szakaszba.

Eredmény: Ellenőrzött intézkedések, KPI-eredmények, helyesbítő lépések és tanulságok a következő CSI-ciklushoz.

4. Gyakorlati példa

Képzelt vállalkozás: NordicCraft Handicrafts

A NordicCraft 25 fős, kézműves termékeket online értékesítő e-kereskedelmi kkv.

A példa bemutatja a CSI-modell öt szakaszának gyakorlati alkalmazását. Az adatok és eredmények szemléltető jellegűek.

1. szakasz – Elemzés: Felhőszolgáltatások és kockázatok feltérképezése

Felhőszolgáltatás	Szolgáltatási modell	Üzleti felhasználás
Shopify	SaaS	Webáruház, rendelések, ügyfelek személyes adatai, fizetések továbbítása.
Google Workspace	SaaS	Céges e-mail, megosztott fájlok és naptárak.
AWS S3	IaaS / Tárhely	Termékfotók és a rendelésadatok napi biztonsági mentése.
Azure App Service	PaaS	Egyedi rendeléskezelő webalkalmazás, amely összeköti a Shopify-t a raktárral.

A CSI Matrix eredményei (részlet):

Szolgáltatás	Fenyegetés	Sérülékenység	Kockázat	Prioritás
Shopify adminfelület	Fiókfeltörés / adathalászat	Nincs MFA a rendszergazdánál.	Illetéktelen módosítások, ügyfeladatok kiszivárgása.	Magas
AWS S3	Adatok nyilvánossá válása	Az S3-bucket nyilvánosan olvasható.	Ügyfélképek és mentések kiszivárgása.	Magas
Azure rendeléskezelő	Kódbefecskendezés / ismert sérülékenység (CVE)	Elavult könyvtárak, nincs WAF.	Adatszivárgás, szolgáltatáskiesés.	Közepes
Google Workspace	Céges e-mail-fiók kompromittálása	Gyenge vagy ismételt jelszavak, nincs kötelező MFA.	Adatvesztés, hamis fizetési felszólítások.	Közepes

Az Európai Unió finanszírozásával. Az itt szereplő vélemények és állítások a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az OeAD-GmbH hivatalos álláspontjával. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem vonható felelősségre miattuk.

Projektazonosító: 2024-1-AT01-KA220-VET-000245093.

Megfelelőségi ellenőrzés:

A NordicCraft ügyfelei személyes adatait kezeli, ezért a GDPR vonatkozik rá.

A DORA és a NIS2 közvetlenül nem érinti a céget, de az önként követi az ISO/IEC 27001 bevált gyakorlatait.

2. szakasz – Meghatározás: Szabályzat, prioritások és szerepek

A NordicCraft egyoldalas felhőbiztonsági szabályzatot készített a fiókhozzáférésről, az adatok besorolásáról és a biztonsági mentésekről.

A két magas prioritású kockázat – a Shopify rendszergazdai fiókjai és a nyilvánosan elérhető AWS S3-tárhely – azonnali kezelést kapott.

A felelősségi köröket így osztották fel:

- **Felhőadminisztrátor:** IT-vezető – az összes felhőplatform beállítása és kezelése.
- **Adatgazda:** Üzemeltetési vezető – az ügyfeladatok besorolása és a hozzáférési szabályok meghatározása.
- **Biztonsági felelős:** IT-vezető, külső informatikai partner támogatásával – felügyelet, incidenskezelés és szabályzatfrissítés.
- **Megfelelőségi felelős:** Ügyvezető igazgató – a GDPR és az ISO/IEC 27001 szerinti megfelelés biztosítása.

3. szakasz – Tervezés: Kockázatcsökkentő intézkedések

Kockázat	Védelmi cél	Intézkedés	Felelős
Shopify-adminfiókok gyenge védelme	Fiókvédelem erősítése	Kötelező MFA minden Shopify-adminfióknál.	IT-vezető
Nyilvános AWS S3-tárhely	Csak a szükséges hozzáférés engedélyezése	Privát bucket, hozzáférési szabályok és naplózás.	IT-vezető
Elavult Azure-könyvtárak	Támadási felület csökkentése	Könyvtárfrissítés, Azure WAF és automatikus frissítések.	Külső IT-partner
Nincs MFA a Google Workspace-ben	Fiókvédelem erősítése	Kötelező MFA mindenkinek és bejelentkezési riasztások.	IT-vezető

Elkészült dokumentumok:

- Felhőbiztonsági szabályzat.
- Megvalósítási ellenőrzőlista, intézkedésenként egy sorral.
- Incidenskezelési sablon.
- Auditnapló-ellenőrző űrlap (Audit Logs).

Képzési program:

A CSI tananyagára építve két 45 perces képzést terveztek:

- „MFA és a jelszavak biztonságos kezelése”
- „Az adathalászat felismerése és az incidensek bejelentése”

Az Európai Unió finanszírozásával. Az itt szereplő vélemények és állítások a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az OeAD-GmbH hivatalos álláspontjával. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem vonható felelősségre miattuk.

Projektazonosító: 2024-1-AT01-KA220-VET-000245093.

4. szakasz – Megvalósítás: Műszaki lépések és képzés

A NordicCraft az alábbiakat valósította meg:

- Kötelezővé tette az MFA-t minden Shopify- és Google Workspace-rendszergazdai fióknál. Ez az első héten elkészült.
- Priváttá tette az AWS S3-tárhelyet, és engedélyezte a hozzáférési szabályzatot és a naplózást.
- Frissítette az Azure App Service függőségeit, és az Azure WAF-ot állította a rendeléskezelő alkalmazás védelmére.
- Mindkét képzést megtartotta mind a 25 munkatársnak. A részvételt közös táblázatban követték.

5. szakasz – Ellenőrzés: Tesztelés, nyomon követés és visszacsatolás

Egy hónappal a bevezetés után a külső IT-partner szimulált adathalásztesztet és alapvető sérülékenységvizsgálatot végzett az Azure-alkalmazáson.

Egy táblázatban egyszerű KPI-irányítópultot is létrehoztak.

Mutató (KPI)	Mérés módja	Riasztási küszöb
Sikertelen bejelentkezések (minden platform)	Heti adatkinyerés az adminfelületekről.	Több mint 10 próbálkozás fiókonként hetente.
MFA-val védett adminfiókok aránya	Havi beállításellenőrzés.	100% alatt.
Az utolsó könyvtár- vagy biztonsági frissítés óta eltelt napok (Azure)	Havi frissítési napló.	Több mint 30 nap.
Nyitott biztonsági incidensek	Folyamatos nyomon követés.	Bármely incidens több mint 14 napja nyitott.

Incidensnyilvántartás készült, amely rögzíti az eseményeket, azok okait, hatásait és a megtett intézkedéseket.

Az ellenőrzés eredményeit és a tanulságokat felhasználják a CSI Matrix, a szabályzatok, a védelmi intézkedések és a képzések frissítéséhez.

Így a vállalkozás az 1. szakasszal új CSI-ciklust kezdhet, és folyamatosan javíthatja biztonságát.

5. Indulás előtti ellenőrzőlista

A CSI-modell első alkalmazása előtt gondoskodjon a következőkről:

- Jelöljön ki egy felelőst a teljes bevezetés koordinálására. Kisvállalkozásnál ehhez nem kell külön biztonsági pozíció.
- Szánjon időt a csapat közös CSI-önértékelésére, hogy felmérje a kiinduló tudásszintet.
- Biztosítson hozzáférést a CSI Matrixhoz az 1. szakasz kockázatértékeléséhez.
- Hozzon létre közös mappát a felhőbiztonsági szabályzathoz, az ellenőrzőlistákhoz és az incidensnyilvántartáshoz.

Az Európai Unió finanszírozásával. Az itt szereplő vélemények és állítások a szerző(k) álláspontját tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az OeAD-GmbH hivatalos álláspontjával. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem vonható felelősségre miattuk.

Projektazonosító: 2024-1-AT01-KA220-VET-000245093.



- Állítson be rendszeres emlékeztetőt az 1. szakasz megismétlésére, például 6–12 havonta vagy jelentős felhőszolgáltatás-változás után.

6. Hasznos források

Az útmutatóban szereplő összes eszköz elérhető a **gocloudsecure.eu** oldalon.

- [CSI megvalósítási modell](#): A CSI-modell mind az öt szakaszának teljes dokumentációja.
- [CSI Mátrix](#): Interaktív eszköz a felhőbiztonsági fenyegetések és kockázatok felismerésére és értékelésére.
- [CSI-önértékelés](#): A csapat felhőbiztonsági ismereteinek felmérésére szolgáló eszköz.
- [CSI-kurzus](#): Tananyag a felhőbiztonsághoz szükséges gyakorlati ismeretek és készségek fejlesztéséhez.

Megjegyzés az útmutatóhoz

Ez a nem hivatalos kiegészítő útmutató a CSI-modell alkalmazását támogatja.

Nem helyettesíti a „Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs” című hivatalos kiadványt (Erasmus+ 2024-1-AT01-KA220-VET-000245093), amely CC BY-NC-ND 4.0 licenc alatt jelent meg.