Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI MEGVALÓSÍTÁSI MODELL

GO CLOUD GO SECURE

1. fázis: ELEMZÉS

1. lépés: Felhőszolgáltatások jegyzéke
2. lépés: Kockázatok feltérképezése
3. lépés: Megfelelőség

2. fázis: MEGHATÁROZÁS

4. lépés: Szerepek és felelősségek
3. lépés: Kontrollcélok meghatározása
2. lépés: Kockázatok rangsorolása
1. lépés: Szabályzat kidolgozása

3. fázis: TERVEZÉS

1. lépés: Kockázatcsökkentő intézkedések
2. lépés: Kontrollok hozzárendelése
3. lépés: Dokumentáció
4. lépés: Képzési program

4. fázis: MEGVALÓSÍTÁS

2. lépés: Képzés és tudatosság
1. lépés: Technikai intézkedések

5. fázis: ELLENŐRZÉS

1. lépés: Tesztelés
2. lépés: Felügyelet
3. lépés: Visszacsatolás

Az Európai Unió társfinanszírozásával

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI MEGVALÓSÍTÁSI MODELL

GO CLOUD GO SECURE

1. fázis: ELEMZÉS

1. lépés: Felhőszolgáltatások jegyzéke

Készítsen teljes listát a szervezet által használt felhőszolgáltatásokról. Az értékelés előtt fontos tisztázni, mely szolgáltatások vannak használatban, és melyek üzletileg kritikusak.

2. lépés: Kockázatok feltérképezése

A CSI-mátrix szolgáltatásonként azonosítja a fenyegetéseket, sérülékenységeket és kockázatokat, így világos képet ad a szervezet legfontosabb gyenge pontjairól.

3. lépés: Megfelelőség

Ellenőrizze, hogy a szervezet megfelel-e az uniós előírásoknak és a nemzetközi szabványoknak, hogy elkerülhetők legyenek a bírságok, az adatvesztés és a hírnévkárosodás. Egyes követelmények külön ellenőrzéseket írnak elő, például hozzáférési naplózást, titkosítást és incidensjelentést.

2. fázis: MEGHATÁROZÁS

1. lépés: Szabályzat kidolgozása

Készítsen felhőbiztonsági szabályzatot, amely rögzíti a felhő biztonságos használatára, a hozzáférés-kezelésre és az adatvédelemre vonatkozó szabályokat, és megalapozza a szervezet biztonsági keretrendszerét.

2. lépés: Kockázatok rangsorolása

A CSI-mátrix segítségével értékelje a kockázatokat valószínűségük és hatásuk alapján, és összpontosítson a legsürgősebbekre.

3. lépés: Kontrollcélok meghatározása

Minden kiemelt CSI-kockázathoz határozzon meg egyértelmű mérséklési célokat, hogy a felismerésből konkrét intézkedési terv szülessen.

4. lépés: Szerepek és felelősségek

Jelölje ki egyértelműen a szerepeket: a felhőadminisztrátor kezeli a platformokat, az adattulajdonos az adathozzáférést, a biztonsági felelős a felügyeletet és az incidenseket, a megfelelőségi felelős pedig a szabályozási követelmények betartását.

3. fázis: TERVEZÉS

1. lépés: Kockázatcsökkentő intézkedések

Minden kiemelt CSI-kockázathoz határozzon meg konkrét és végrehajtható intézkedéseket, hogy azok gyorsan és következetesen megvalósíthatók legyenek, különösen olyan KKV-knál, ahol nincs külön biztonsági szakember.

2. lépés: Kontrollok hozzárendelése

Készítsen táblázatot, amely összekapcsolja a kockázatcsökkentő intézkedéseket az egyes felhőszolgáltatásokkal, és egyértelművé teszi, mit és hogyan védenek.

3. lépés: Dokumentáció

Készítsen sablonokat és ellenőrzőlistákat, például bevezetési ellenőrzőlistát, incidenskezelési sablont és auditnapló-ellenőrző űrlapot a szabályzatok végrehajtásához, az auditokhoz és a folyamatos fejlesztéshez.

4. lépés: Képzési program

Dolgozzon ki gyakorlati CSI-képzési programot a felhő alapjairól, a fő sérülékenységekről és a hibás beállításokról, hogy a munkatársak felkészültek legyenek, és csökkenjen a biztonsági hibák kockázata.

Az Európai Unió társfinanszírozásával

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI MEGVALÓSÍTÁSI MODELL

GO CLOUD GO SECURE

4. fázis: MEGVALÓSÍTÁS

1. lépés: Technikai intézkedések

Valósítsa meg a 3. fázisban meghatározott technikai intézkedéseket, például az MFA-t, a titkosítást, az IAM-szabályokat és az RBAC-ot, olyan beépített eszközökkel, mint az AWS Config vagy az Azure Security Center. Kezdje a gyorsan megvalósítható intézkedésekkel, például az MFA és az RBAC bekapcsolásával.

2. lépés: Képzés és tudatosság

Hajtsa végre a 3. fázis képzési tervét a mátrix és a tananyagok felhasználásával, rövid, gyakorlati modulokban, a szervezet technikai környezetéhez és kockázati profiljához igazítva.

5. fázis: ELLENŐRZÉS

1. lépés: Tesztelés

Végezzen ellenálló képességi teszteket gyakorlatokkal, szimulált támadásokkal, kontrollvizsgálatokkal és biztonsági értékelésekkel. Így ellenőrizhető, hogy az intézkedések megfelelően működnek, hatékonyak és naprakészek, valamint hogy a szervezet felkészült-e a valós fenyegetésekre.

2. lépés: Felügyelet

Határozzon meg KPI-ket a felhőbiztonság nyomon követésére, a proaktív kezelésre és a fejlődés mérésére. Ilyen mutató lehet a sikertelen bejelentkezések száma, a hibás konfigurációkra vonatkozó riasztások és az elavult javítócsomagok, egyszerű irányítópulton megjelenítve.

3. lépés: Visszacsatolás

Hozzon létre incidensnyilvántartást, amely tartalmazza az események részleteit, okait, hatásait és a megtett intézkedéseket. Ezek alapján frissíthetők a kockázatértékelések, pontosíthatók a szabályzatok és módosítható a képzés, így a biztonsági keretrendszer folyamatosan fejlődik.

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 Európai Oktatási és Kulturális Végrehajtó Ügynökség (EACEA) hivatalos álláspontjával. Sem az Európai Unió, sem az EACEA nem vonható felelősségre miattuk.

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης