



ДОПЪЛНИТЕЛНО РЪКОВОДСТВО ЗА ПРИЛАГАНЕ

Как да приложите модела CSI за сигурност в облака във вашата организация

Придружаващо ръководство към проекта „Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs“ (Erasmus+ 2024-1-AT01-KA220-VET-000245093).

Учебни материали и интерактивни инструменти: gocloudsecure.eu

1. Цел на ръководството

Моделът CSI включва пет етапа и помага на малките и средните предприятия (МСП) да повишат сигурността на облачните услуги, които използват – софтуер (SaaS), платформи (PaaS) или инфраструктура (IaaS).

Ръководството допълва официалната документация на модела CSI. То представя накратко всеки етап и показва с практически пример как предприятията могат да следват процеса и да го адаптират към нуждите си.

За повече информация, шаблони и подробни указания вижте документите за петте етапа на модела CSI.

Използвайте ръководството заедно с двата основни инструмента на CSI:

- **[CSI-Matrix](#):** Интерактивен инструмент за установяване на заплахите, уязвимостите и рисковете за облачните услуги и оценяването им според OWASP Top 10. Използва се в етапи 1–3.
- **[Самооценка по CSI](#) & [Курс по CSI](#):** Самооценка и учебни материали за основите на облачните технологии, киберзаплахите, сигурното проектиране и управлението. Подпомагат подготовката и провеждането на обучението в етапи 3–4.

Съвет: Дръжте ръководството и CSI Matrix отворени по време на етапи 1–3. Следвайте указанията, направете оценката и използвайте резултатите в следващите етапи.



2. Моделът CSI накратко

Моделът CSI представлява непрекъснат цикъл от пет етапа. Всеки има конкретна цел, основни стъпки и резултати, които служат за основа на следващия.

Етап	Цел	Основни стъпки	Резултати
1. Анализ	Разбиране на облачните услуги, заплахите и изискванията за съответствие.	Опис на услуги · Оценка с CSI Matrix · Проверка за съответствие	Списък на услугите, начална оценка CSI Matrix, приложими правила.
2. Определяне	Правила за сигурност, приоритети на рисковете и цели за защита.	Политика · Приоритети на рисковете · Цели · Роли и отговорности	Политика за сигурност, подредени рискове, цели и отговорници.
3. Планиране	Превръщане на рисковете и целите в конкретен план.	Мерки · Съпоставяне · Документация · Програма за обучение	План с мерки, таблица, шаблони, контролни списъци и обучение.
4. Прилагане	Въвеждане на мерки и обучение на персонала.	Технически действия · Обучение и осведоменост	Въведени мерки, проведено обучение и по-сигурна среда.
5. Проверка	Проверка на ефективността и постоянно подобрене.	Тестове · Наблюдение на KPI · Регистър на инциденти	Проверени мерки, панел за наблюдение, изводи и подобрени правила и обучения.

3. Указания стъпка по стъпка

Преминете през петте етапа последователно, тъй като резултатите от всеки етап са основа за следващия.

Етап 1 – Анализ

Цел: Да установите кои облачни услуги използва предприятието, на какви заплахи и уязвимости е изложено и какви изисквания за съответствие трябва да спазва.

- **Опис на облачните услуги:** Избройте всички използвани услуги (IaaS, PaaS, SaaS, хранилища, бази данни, мрежи и услуги за сигурност). Отбележете кои са критични за дейността.
- **Оценка на рисковете:** Използвайте CSI Matrix, за да определите заплахите за всяка услуга (напр. изтичане на данни, DDoS атаки), уязвимостите (напр. слабо удостоверяване) и възможните последици (напр. загуба на данни, превземане на акаунт).
- **Проверка за съответствие:** Проверете приложимите правила на ЕС (GDPR, DORA, NIS2) и стандартите, които вече прилагате или планирате да въведете (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

Резултат: Списък на облачните услуги, завършена оценка с CSI Matrix и преглед на приложимите изисквания.



Етап 2 – Определяне

Цел: Да установите правила за сигурност, да подредите рисковете по важност и да определите целите за защита на предприятието.

- **Политика за сигурност:** Изгответе политика за сигурност на облачните услуги, която обхваща безопасното им използване, управлението на достъпа и защитата на данните.
- **Приоритизиране на рисковете:** Оценете рисковете от CSI Matrix според вероятността и въздействието им. Насочете усилията си към най-значимите.
- **Цели за защита:** Определете ясна цел за всеки риск с висок приоритет. Например при „слабо удостоверяване“ целта може да бъде „по-добра защита на акаунтите“.
- **Роли и отговорности:** Определете кой отговаря за облачните услуги, данните, сигурността и нормативното съответствие. В по-малките предприятия един човек може да изпълнява няколко роли.

Резултат: Политика за сигурност на облака, приоритизирани рискове, цели за защита и ясно разпределени отговорности.

Етап 3 – Планиране

Цел: Да превърнете рисковете и целите за защита в конкретен план с технически мерки, документация и обучение.

- **Мерки за ограничаване на риска:** Определете конкретно действие за всяка цел. Например за „по-добра защита на акаунтите“ въведете многофакторно удостоверяване (MFA).
- **Съпоставяне на мерките:** Създайте таблица, която показва коя облачна услуга се защитава с всяка мярка.
- **Документация:** Подгответе контролен списък за изпълнение, шаблон за реагиране при инциденти и формуляр за преглед на одитните записи (Audit Logs).
- **Програма за обучение:** Подгответе кратки практически модули с материалите на CSI, съобразени със знанията и нуждите на екипа.

Резултат: Списък с мерки за намаляване на риска, таблица за съпоставяне, документи за изпълнение и план за обучение.

Етап 4 – Прилагане

Цел: Да приложите планираните мерки във всички съответни облачни услуги и да обучите служителите.

- **Технически действия:** Изпълнете плана от етап 3 – например MFA, криптиране и правила за управление на идентичности и достъп (IAM, RBAC). Започнете с лесни мерки с бърз ефект и използвайте вградени инструменти като AWS Config или Azure Security Center.
- **Обучение и повишаване на осведомеността:** Проведете обучението с акцент върху рисковете, установени чрез CSI Matrix, като използвате учебните материали на CSI.

Резултат: Въведени мерки за сигурност, обучени служители и доказателства за изпълнението.



Етап 5 – Проверка

Цел: Да оцените ефективността на мерките за сигурност и непрекъснато да подобрявате защитата на предприятието.

- **Тестове:** Провеждайте симулирани атаки, проверки на контролните мерки и оценки на сигурността.
- **Наблюдение:** Следете ключови показатели (KPI), като неуспешни влизания, предупреждения за грешни настройки и забавени актуализации за сигурност, например чрез обикновен панел за наблюдение.
- **Обратна връзка:** Водете регистър на инцидентите с описание на случилото се, причините, последиците и предприетите мерки. Използвайте изводите за подобряване на етапи 1 и 2.

Резултат: Проверени мерки, стойности на показателите KPI, коригиращи действия и изводи за следващия цикъл на CSI.

4. Практически пример

Примерно предприятие: NordicCraft Handicrafts

NordicCraft е малко предприятие за онлайн търговия с 25 служители, което продава ръчно изработени изделия.

Примерът показва прилагането на петте етапа на модела CSI. Данните и резултатите са илюстративни.

Етап 1 – Анализ: Опис на облачните услуги и оценка на рисковете

Облачна услуга	Модел	Приложение в предприятието
Shopify	SaaS	Онлайн магазин, поръчки, лични данни на клиенти и пренасочване на плащания.
Google Workspace	SaaS	Служебна поща, споделени файлове и календари.
AWS S3	IaaS / Съхранение	Снимки на продукти и ежедневни резервни копия на поръчките.
Azure App Service	PaaS	Собствено уеб приложение за поръчки, свързващо Shopify със склада.

Резултати от CSI Matrix (извадка):

Услуга	Заплаха	Уязвимост	Риск	Приоритет
Админ панел на Shopify	Превземане на акаунт / фишинг	Няма MFA за администраторите.	Неоторизирани промени и изтичане на данни на клиенти.	Висок
AWS S3	Излагане на данни	S3 хранилището позволява публично четене.	Изтичане на клиентски снимки и резервни копия.	Висок

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на OeAD-GmbH. За тях не носи отговорност нито Европейският съюз, нито органът, предоставящ финансирането.

Номер на проекта: 2024-1-AT01-KA220-VET-000245093.



Услуга	Заплаха	Уязвимост	Риск	Приоритет
Приложение Azure за поръчки	Инжектиране на код / известна уязвимост (CVE)	Остарели библиотеки, липса на WAF.	Изтичане на данни и прекъсване на работата.	Среден
Google Workspace	Компрометирана служебна поща	Слаби или повторно използвани пароли; MFA не е задължително.	Загуба на данни и измамни искания за плащане.	Среден

Проверка за съответствие:

NordicCraft обработва лични данни на клиенти, затова се прилага GDPR.

DORA и NIS2 не се прилагат пряко за предприятието, но то доброволно следва добрите практики на ISO/IEC 27001.

Етап 2 – Определяне: Политика, приоритети и роли

NordicCraft изготви политика за сигурност на облака от една страница, обхващаща достъпа до акаунти, класифицирането на данни и резервните копия.

Двата риска с висок приоритет – администраторските акаунти в Shopify и публичният достъп до AWS S3 – бяха определени за незабавно отстраняване.

Отговорностите бяха разпределени така:

- **Администратор на облачните услуги:** ИТ мениджър – настройва и управлява всички облачни платформи.
- **Отговорник за данните:** Ръководител операции – определя класификацията на клиентските данни и правилата за достъп.
- **Отговорник по сигурността:** ИТ мениджър с помощта на външен ИТ партньор – следи сигурността, управлява инцидентите и обновява политиката.
- **Отговорник по съответствието:** Управител – следи за съответствие с GDPR и ISO/IEC 27001.

Етап 3 – Планиране: Мерки за ограничаване на риска

Риск	Цел за защита	Мярка	Отговорник
Слаба защита на Shopify администраторите	По-сигурни акаунти	Задължително MFA за всички администратори на Shopify.	ИТ мениджър
Публичен достъп до AWS S3	Само минимално необходимите права	Хранилището става частно; правила и регистриране на достъпа.	ИТ мениджър
Остарели библиотеки на Azure	По-малко точки за атака	Актуализиране на библиотеки, включване на Azure WAF и автоматични обновявания.	Външен ИТ партньор
Без MFA в Google Workspace	По-сигурни акаунти	Задължително MFA за всички и известия при влизане.	ИТ мениджър



Подготвени документи:

- Политика за сигурност на облака.
- Контролен списък с отделен ред за всяка мярка.
- Шаблон за реагиране при инциденти.
- Формуляр за преглед на одитните записи (Audit Logs).

Програма за обучение:

Планирани бяха две обучения по 45 минути, базирани на материалите на CSI:

- „MFA и безопасно управление на паролите“
- „Разпознаване на фишинг и докладване на инциденти“

Етап 4 – Прилагане: Технически мерки и обучение

NordicCraft изпълни следните действия:

- Включи задължително MFA за всички администраторски акаунти в Shopify и Google Workspace. Мярката беше изпълнена още през първата седмица.
- Ограничи достъпа до AWS S3, като направи хранилището частно и включи правила и регистриране на достъпа.
- Актуализира библиотеките на Azure App Service и включи Azure WAF за защита на приложението за поръчки.
- Проведе и двете обучения за всичките 25 служители. Участието бе отчетено в споделена електронна таблица.

Етап 5 – Проверка: Тестове, наблюдение и обратна връзка

Месец след прилагането външният ИТ партньор проведе симулирана фишинг атака и базово сканиране за уязвимости на приложението Azure.

Създаден беше и прост панел за проследяване на KPI в електронна таблица.

Показател (KPI)	Измерване	Праг за сигнал
Неуспешни влизания (всички платформи)	Седмичен отчет от администраторските конзоли.	Над 10 опита на акаунт седмично.
Дял на администраторите с MFA	Месечен преглед на настройките.	Под 100%.
Дни от последната актуализация (Azure)	Месечен регистър на актуализациите.	Над 30 дни.
Неприключени инциденти	Постоянно наблюдение.	Инцидент, отворен над 14 дни.

Въведен беше регистър на инцидентите, в който се записват събитията, причините, последиците и предприетите мерки.

Резултатите от проверките и извлечените поуки служат за обновяване на CSI Matrix, политиките, защитните мерки и обучението.

Така предприятието може да започне нов цикъл на CSI от етап 1 и постепенно да повишава сигурността си.

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на OeAD-GmbH. За тях не носи отговорност нито Европейският съюз, нито органът, предоставящ финансирането.

Номер на проекта: 2024-1-AT01-KA220-VET-000245093.



5. Контролен списък преди началото

Преди да приложите модела CSI за първи път, уверете се, че сте:

- Определили човек, който да координира целия процес. В малко предприятие не е необходима отделна длъжност по сигурността.
- Отделили време за груповата самооценка CSI, за да установите началното ниво на знания.
- Осигурили достъп до CSI Matrix за оценката на рисковете в етап 1.
- Създали споделена папка за политиката за сигурност, контролните списъци и регистъра на инцидентите.
- Планирали редовно напомняне за повторно изпълнение на етап 1 – например на всеки 6–12 месеца или след значителна промяна в облачните услуги.

6. Полезни ресурси

Всички посочени инструменти са достъпни на gocloudsecure.eu.

- [Модел за прилагане на CSI](#): Пълна документация за петте етапа на модела CSI.
- [CSI-Matrix](#): Интерактивен инструмент за откриване и оценка на заплахи и рискове за сигурността в облака.
- [Самооценка по CSI](#): Инструмент за оценка на знанията на екипа относно сигурността в облака.
- [Курс по CSI](#): Учебни материали за практически знания и умения по сигурност в облака.

Бележка за ръководството

Това е неофициален допълнителен документ, създаден да улесни прилагането на модела CSI.

Той не заменя официалното издание „Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs“ (Erasmus+ 2024-1-AT01-KA220-VET-000245093), публикувано с лиценз CC BY-NC-ND 4.0.