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

МОДЕЛ ЗА ПРИЛАГАНЕ НА CSI

GO CLOUD GO SECURE

Фаза 1: АНАЛИЗ

- Стъпка 1: Регистър на облачните услуги
- Стъпка 2: Картографиране на рисковете
- Стъпка 3: Съответствие

Фаза 2: ОПРЕДЕЛЯНЕ

- Стъпка 4: Роли и отговорности
- Стъпка 3: Определяне на целите на контролите
- Стъпка 2: Приоритизиране на рисковете
- Стъпка 1: Разработване на политики

Фаза 3: ПЛАНИРАНЕ

- Стъпка 1: Мерки за ограничаване на риска
- Стъпка 2: Свързване на контролите
- Стъпка 3: Документация
- Стъпка 4: Програма за обучение

Фаза 4: ПРИЛАГАНЕ

- Стъпка 2: Обучение и повишаване на осведомеността
- Стъпка 1: Технически мерки

Фаза 5: ПРОВЕРКА

- Стъпка 1: Тестване
- Стъпка 2: Наблюдение
- Стъпка 3: Обратна връзка

Съфинансирано от Европейския съюз

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

МОДЕЛ ЗА ПРИЛАГАНЕ НА CSI

GO CLOUD GO SECURE

Фаза 1: АНАЛИЗ

Стъпка 1: Регистър на облачните услуги

Съставете пълен списък на всички облачни услуги, използвани от вашата организация. Преди да започнете оценката, е важно да знаете какви услуги използвате и кои от тях са критични за дейността ви.

Стъпка 2: Картографиране на рисковете

Матрицата CSI идентифицира заплахите, уязвимостите и рисковете за всяка облачна услуга и предоставя ясна представа за основните слабости на вашата организация.

Стъпка 3: Съответствие

Проверете дали организацията ви спазва приложимите регламенти на ЕС и международните стандарти, за да избегнете санкции, загуба на данни и увреждане на репутацията. Някои изисквания налагат конкретни мерки, като регистриране на достъпа, криптиране и докладване на инциденти.

Фаза 2: ОПРЕДЕЛЯНЕ

Стъпка 1: Разработване на политики

Изгответе Политика за сигурност в облака, която определя правилата за безопасно използване на облачните услуги, управление на достъпа и защита на данните. Тя ще служи като основа на вашата рамка за сигурност.

Стъпка 2: Приоритизиране на рисковете

Използвайте Матрицата CSI, за да оцените рисковете според вероятността от настъпване и възможното въздействие. Съсредоточете се първо върху най-неотложните рискове, за да насочите правилно мерките за тяхното ограничаване.

Стъпка 3: Определяне на целите на контролите

За всеки високоприоритетен риск в Матрицата CSI определете ясни цели за ограничаването му, така че установените проблеми да бъдат превърнати в конкретни и подходящи планове за действие.

Стъпка 4: Роли и отговорности

Разпределете ясно ролите:Администраторът на облачните услуги управлява платформите., Собственикът на данните управлява достъпа до тях., Отговорникът по сигурността следи средата и реагира при инциденти., Мениджърът по съответствието следи за спазването на нормативните изисквания.

Фаза 3: ПЛАНИРАНЕ

Стъпка 1: Мерки за ограничаване на риска

За всеки високоприоритетен риск в Матрицата CSI определете конкретни и изпълними мерки. Това позволява бързо и последователно прилагане, особено в МСП, които не разполагат с постоянен специалист по сигурността.

Стъпка 2: Свързване на контролите

Създайте таблица, която свързва мерките за ограничаване на риска с конкретните облачни услуги. Така ясно ще се вижда какво се защитава и по какъв начин се прилагат съответните контроли.

Стъпка 3: Документация

Подгответе образци и контролни списъци, например: контролни списъци за прилагане; образци за реакция при инциденти; формуляри за преглед на журналите за одит. Те ще подпомогнат прилагането на политиките, извършването на одити и непрекъснатото подобрение.

Стъпка 4: Програма за обучение

Разработете практическа програма за обучение по CSI, която обхваща основите на облачните технологии, основните уязвимости и неправилните конфигурации. Целта е служителите да бъдат подготвени ефективно и да се предотвратят до 80% от проблемите, свързани със сигурността в облака.

Съфинансирано от Европейския съюз

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

МОДЕЛ ЗА ПРИЛАГАНЕ НА CSI

GO CLOUD GO SECURE

Фаза 4: ПРИЛАГАНЕ

Приложете техническите мерки, определени в плана от Фаза 3, например: активиране на многофакторна автентикация; криптиране; политики за управление на идентичности и достъп; контрол на достъпа въз основа на роли. Използвайте вградените инструменти на платформи като AWS Config и Azure Security Center. Започнете с мерки, които могат да бъдат приложени бързо и да дадат незабавен резултат, като активирането на MFA и RBAC.

Стъпка 1: Технически мерки

Приложете плана за обучение, разработен във Фаза 3. Използвайте Матрицата CSI и съответните учебни материали, като организирате кратки и практически модули, съобразени с техническата среда и рисковия профил на вашата организация.

Стъпка 2: Обучение и повишаване на осведомеността

Фаза 5: ПРОВЕРКА

Стъпка 1: Тестване

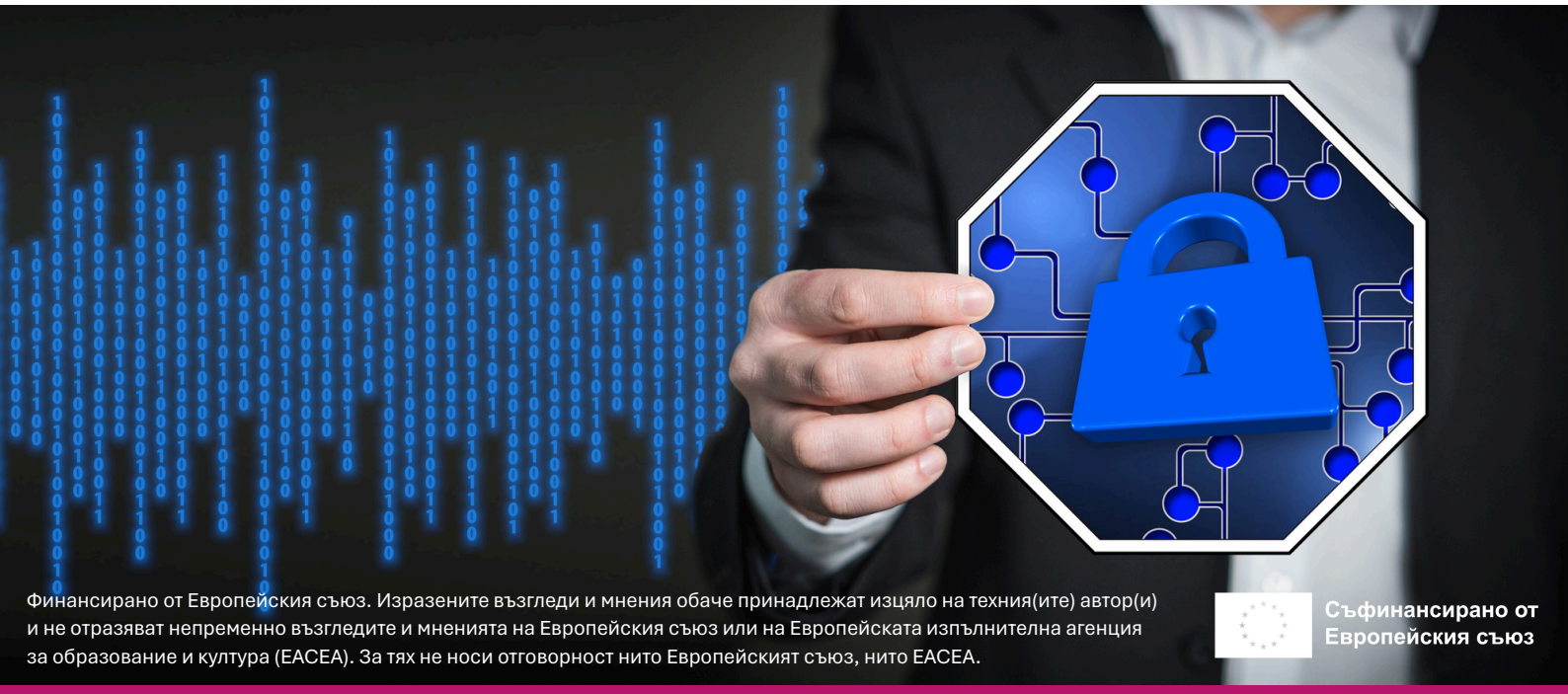
Провеждайте тестове за устойчивост чрез практически упражнения, симулирани атаки, проверки на контролите и оценки на сигурността. Целта е да се потвърди, че мерките за ограничаване на риска са приложени правилно, работят ефективно и са актуални, така че организацията да бъде подготвена за реални заплахи.

Стъпка 2: Наблюдение

Определете ключови показатели за ефективност, чрез които да следите сигурността на облачната среда, да управлявате рисковете проактивно и да отчитате напредъка. Подходящи показатели са например: неуспешни опити за влизане; сигнали за неправилна конфигурация; неактуализирани корекции и системни обновявания. Показвайте резултатите в лесно разбираемо табло с основни показатели

Стъпка 3: Обратна връзка

Създайте регистър на инцидентите, в който се записват подробностите за всяко събитие, причините, последствията и предприетите мерки. Използвайте тази информация, за да: актуализирате оценките на риска; подобрявате политиките; адаптирате обученията; поддържате рамката за сигурност актуална и развиваща се.



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 Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

Съфинансирано от Европейския съюз