Case Study: Интегрирана имплементация на системи за киберсигурност в съответствие с DORA

Въведение

За финансови институции, подчинени на регулациите на DORA, изграждането на надеждна и интегрирана система за киберсигурност е от съществено значение. Този случай разглежда как една организация успя да интегрира няколко специализирани решения – защита на крайни устройства, управление на уязвимости, Dark Web мониторинг, SIEM, управление на ИТ активи и ИТ риск, както и управление на трети доставчици – за да гарантира оперативната си устойчивост и съответствие с DORA.

Предизвикателството

Организацията се сблъска с редица критични въпроси:

- **Защита на крайните точки:** Осигуряване на надеждна защита за всички работни станции и мобилни устройства.
- **Управление на уязвимости:** Идентифициране и коригиране на слабости в ИТ инфраструктурата.
- **Проследяване на Dark Web:** Откриване на компрометирана информация и потенциални заплахи извън традиционните канали.
- **Централизация на логове:** Необходимост от интегрирана SIEM система за бърза реакция при инциденти.
- **Управление на ИТ активи и риска:** Пълна видимост и контрол върху хардуер, софтуер и връзки с трети доставчици.

Решението

За да отговори на тези предизвикателства, екипът по киберсигурност разработи стратегия за цифрова оперативна устойчивост, включваща:

- Имплементиране на EDR и антивирусни решения за защита на крайни устройства.
- Автоматизиран процес за сканиране на ИТ активи и управление на уязвимости, който предлага препоръки за корективни мерки.
- Платформа за Dark Web мониторинг, която позволява навременна идентификация на изтичане на чувствителна информация.
- SIEM система за централизация и анализ на логове, което улеснява корелацията на инциденти и бързата им реакция.
- Система за управление на ИТ активи, интегрирана с процеси за оценка и управление на ИТ риска, включително оценка на трети доставчици.

Имплементация

Първоначално бе извършена пълна инвентаризация на ИТ активите и оценка на текущото ниво на сигурност. След това:

- **Защитата на крайни устройства** бе разпределена към всички устройства чрез внедряване на антивирусен и EDR софтуер.
- **Управлението на уязвимости** автоматизира процеса на сканиране, като идентифицира слабости и предоставя препоръки за тяхното отстраняване.
- **Dark Web мониторингът** позволи своевременно проследяване на потенциални заплахи и компрометирани данни.
- **SIEM системата** централизира логовете от всички решения, осигурявайки възможност за корелация на инциденти и навременна реакция.
- **Управлението на ИТ активи и риска** се интегрира с оценките на трети доставчици, гарантирайки, че външните услуги отговарят на изискванията на DORA.

Резултати

Интегрираната платформа осигури:

- Подобрена оперативна устойчивост и бърза реакция при инциденти.
- Повишено ниво на защита на критичната ИТ инфраструктура.
- Пълно съответствие с изискванията на DORA чрез редовни одити, мониторинг и актуализации.
- Засилено управление на риска, включително прозрачност при работата с трети доставчици.

Изводи

Този случай подчерта важността от холистичен подход към киберсигурността, при който интеграцията на множество системи е ключът към цялостна защита. Регулярната актуализация на решенията, тясното сътрудничество между екипите и ефективното управление на външните доставчици са от съществено значение за успешното посрещане на съвременните киберзаплахи и за осигуряване на дългосрочна оперативна устойчивост в съответствие с регулаторните изисквания.