## Case Study: Интегрирана имплементация на киберсигурност за застрахователна компания с решения от Microsoft M365 в съответствие с DORA

**Въведение**

За застрахователните компании, които работят с огромни обеми чувствителна информация за своите клиенти, интегрираната киберсигурност е ключов фактор за оперативната устойчивост. Този казус демонстрира как една застрахователна компания внедри решения от Microsoft M365 екосистемата, за да защити крайните устройства, да управлява уязвимостите, да следи Dark Web, да централизира логовете чрез SIEM система, да контролира ИТ активите и да управлява ИТ риска и трети доставчици съгласно изискванията на DORA.

**Предизвикателството**

**Компанията се сблъска с няколко основни предизвикателства:**

- **Защита на крайните устройства:** Осигуряване на надеждна защита за офис компютри, мобилни устройства и отдалечени работни станции.
- **Управление на уязвимости:** Редовно идентифициране и отстраняване на слабости в ИТ инфраструктурата.
- **Data Leak Prevention (DLP) и Мониторинг на dark web:** Откриване на потенциални заплахи чрез изтичане на чувствителна информация**.**
- **Централизация на логове:** Необходимост от ефективно средство за събиране и анализ на сигурностни събития.
- **Управление на ИТ активи и риска:** Пълна видимост и контрол върху хардуера, софтуера и външните доставчици.

**Решението**

За да отговори на тези предизвикателства, компанията избра да се възползва от решенията в рамките на Microsoft M365 екосистемата:

- Microsoft Defender for Endpoint: За защита на крайните устройства чрез иновативна EDR технология и антивирусна защита.
- Управление на уязвимости: Автоматизирано сканиране и корекция чрез интегрираните възможности на Microsoft Defender.
- Dark web мониторинг: Използване на Microsoft Threat Intelligence за наблюдение на dark web и ранно откриване на компрометирани данни.
- SIEM система: Централизация на логовете и инцидентите чрез Microsoft Sentinel, която осигурява корелация и бърза реакция.

- Управление на ИТ активи и риска: Използване на Microsoft Endpoint Manager (Intune) за централизиран контрол върху активите, съчетано с процеси за оценка на риска и одит на трети доставчици.

**Имплементация**

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

- **Защита на крайните устройства:** Всички устройства бяха защитени с Microsoft Defender for Endpoint, осигурявайки непрекъснат мониторинг и реакция в реално време.
- **Управление на уязвимости:** Автоматизираните сканирания чрез Microsoft Defender позволиха идентифицирането и своевременното отстраняване на уязвимости.
- **Dark web мониторинг:** Чрез Microsoft Threat Intelligence компанията наблюдаваше възможни изтичания на чувствителна информация и потенциални заплахи.
- **Централизация на логове:** Microsoft Sentinel интегрира логовете от всички системи, предоставяйки централизирана платформа за анализ и реакция при инциденти.
- **Управление на ИТ активи и риска:** С помощта на Microsoft Endpoint Manager бе постигната пълна видимост върху хардуера и софтуера, като се внедриха и процеси за оценка на риска и одит на трети доставчици.

**Резултати**

Интеграцията на решенията от Microsoft M365 донесе значителни ползи:

- Подобрена оперативна устойчивост: Бърза реакция при инциденти и намаляване на потенциалните заплахи.
- Повишена сигурност: Ефективна защита на крайните устройства и редовно управление на уязвимости.
- Централизирано управление: Събиране и анализ на данни чрез Microsoft Sentinel, осигуряващо пълна видимост върху сигурността.
- Съответствие с DORA: Оптимизирано управление на ИТ активи, риск и трети доставчици, което гарантира спазване на регулаторните изисквания.

**Изводи**

Този казус демонстрира, че чрез интеграцията на решения от Microsoft M365 екосистемата, застрахователните компании могат да осигурят цялостна защита на своята ИТ инфраструктура. Пълната синергия между решенията за защита на крайните устройства, управление на уязвимости, dark web мониторинг, SIEM и управление на активи и риска дава възможност за проактивна и ефективна реакция на съвременните киберзаплахи, като същевременно отговаря на изискванията на DORA.