**Prezentace Trend Micro – Jak pomocí technologie XDR zlepšit detekci útočníků, bránit se jim a ochránit svou hybridní infrastrukturu.**

**Co je to XDR?**

* XDR je obecný termín pro „Extended Detection and Response“
* Jedná se o další evoluční krok systémů EDR, XDR se začalo prosazovat výrazněji v roce 2019/2022. Oproti EDR systémům, které hledí zejména na koncové zařízení se systém XDR dívá na oblast celé infrastruktury a veškeré drobné a na první pohled třeba nesouvisející události dává automaticky do souvislostí aby dokázal lépe identifikovat pokusy o kompromitaci a případně dokázal identifikovat celý příběh bezpečnostního incidentu i s přehledem všech dotčených aktiv.

**Proč je detekce důležitá?**

* I dnešní doporučení NÚKIB a dalších organizací nehovoří pouze prvcích ochrany infrastruktury, ale o potřebě umět útočníka v infrastruktuře detekovat.
* Dogma jako 100% kybernetická bezpečnost neexistuje a je potřeba neustále vyhodnocovat stav infrastruktury a aktivity v ní.

**Jaké personální úskalí mají dnes IT týmy?**

* Mnoho firem má dnes problém s plným obsazením týmů kvalifikovanými IT pracovníky - na trhu jich je nedostatek a jejich ohodnocení je pro mnoho firem mimo jejich možnosti. Zároveň v situaci, kdy zákazník chce vybudovat interní response tým s provozem 24x7, musí přemýšlet o naddimenzování a dalších investicích zvyšující nákladnost oddělení.
* Trend Micro XDR naopak díky automatizaci a komplexnosti umožňuje realizovat proaktivní ochranu a ušetřit velké množství interních zdrojů.

**Co je zranitelnost a jak se dotýká softwarových záplat?**

* Označení v informatice pro programátorskou chybu, která v software nebo v hardware způsobuje bezpečnostní problém. Jednoduše řečeno - Slabé místo v infrastruktuře, které má vysoké riziko zneužití pro narušení bezpečnosti.
* Vývojáři operačních systémů, aplikací a dalších nástrojů tak v pravidelných cyklech vydávají balíčky opravující tyto zranitelnosti, kterým se říká Softwarové záplaty.
* Zero Day zranitelnost („Zranitelnost nultého dne“)
  + Dosud nezveřejněná softwarová chyba, kterou útočníci objevili dříve, než se o ní dozvěděl výrobce. Jelikož o ní výrobce nevědí, neexistuje pro ni ani žádná záplata a takové útoky mají vysokou úspěšnost.

**Proč by měl firmy zajímat virtuální patching?**

* Problém plnohodnotných softwarových záplat je jejich časová náročnost od doby objevení až po vydání záplat vendorem systémů, otestování v infrastruktuře zákazníků a nasazení je po celou dobu zákazník zranitelný proti útokům zneužívající zranitelnosti v jeho infrastruktuře.
* Virtuální záplaty naopak fungují na úrovni operačních systémů, aplikací a síťové komunikace, kdy vytvoření jejich expertních pravidel a politik blokujících pokusy o zneužití zranitelností, ale i závažných Zero-day zranitelností jsou otázkou mnohem kratšího času a poskytují tak zákazníkům výrazně rychlejší reakci na rizika v infrastruktuře. Zároveň má virtuální patching výhodu minimálního dopadu na provoz infrastruktury a není potřeba servery při jejich instalaci restartovat – tak je zachována i kontinuita provozu.
* Virtuální záplaty však nejsou plnohodnotnou náhradou a jsou spíše odstíněním dočasného problém. Zákazník by i tak měl v pravidelných intervalech provádět plnohodnotné aktualizace verzí operačních systémů, ale celá proces se stává pro něj výrazně flexibilnějším.