MDR (Managed Detection and Response)

MDR řeší největší problém současné kyberbezpečnosti: nedostatek kvalifikovaných lidí. Zatímco software (antivirus) vám oznámí, že máte problém, MDR služba ten problém za vás vyřeší – odhalí útočníka, zastaví ho a vyčistí následky.

1. Hlavní rozdíl: Software vs. Služba

Mnoho firem má moderní nástroje, ale nikdo se nedívá na jejich varování. MDR tento prázdný prostor vyplňuje:

Vlastnost	EDR / XDR (Nástroj)	MDR (Služba)
Kdo to ovládá?	Váš interní IT tým.	Externí tým bezpečnostních expertů.
Pracovní doba	Obvykle 8:00–16:00.	24 hodin denně, 7 dní v týdnu.
Výsledek	„Máte v síti virus.“	„Zablokovali jsme útok a izolovali napadený PC.“
Údržba	Musíte nástroj sami ladit.	Dodavatel se stará o vše, vy dostáváte reporty.

2. Co MDR zahrnuje?

- **SOC (Security Operations Center):** Tým analytiků, kteří neustále sledují výstrahy ze všech vašich zařízení.
- **Threat Hunting (Lov hrozeb):** Experti nečekají na alarm, ale aktivně v síti hledají skryté stopy útočníků, které software přehlédl.
- **Vyšetřování incidentů:** Pokud dojde k útoku, MDR tým zjistí, jak se tam útočník dostal a co všechno viděl.
- **Řízená reakce:** Přímý zásah (např. odpojení serveru od sítě, smazání škodlivého kódu) prováděný na dálku experty MDR.

[Image showing a security analyst in a modern SOC environment with multiple screens]

3. Pro koho je MDR určeno?

- **Středně velké firmy:** Které si nemohou dovolit platit vlastní tým 5–10 drahých bezpečnostních expertů pro nepřetržitý provoz.
- **Kritická infrastruktura:** Kde i pětiminutové zpoždění v reakci na ransomware může znamenat miliónové škody.
- **Firmy pod útokem:** MDR se často nasazuje „za pochodu“, když už firma čelí aktivnímu průniku a potřebuje profesionální pomoc.

4. Přínosy MDR

```
1. **Rychlost (MTTR):** Průměrná doba do vyřešení incidentu (Mean Time to Respond) klesá z dnů na minuty.
```

```
2. **Kvalita detekce:** Lidé dokáží rozpoznat kontext (např. "proč se
administrátor přihlašuje z Číny o půlnoci?"), který software může vyhodnotit
jako povolenou akci.
3. **Compliance:** Pomáhá splnit zákonné požadavky na ochranu dat (např.
NIS2 nebo GDPR).
```

5. Evoluce: MSSP vs. MDR

Dříve existovaly **MSSP** (Managed Security Service Providers). Ti se ale starali hlavně o správu firewallů a logování. **MDR** jde dál – neřeší jen „správu krabiček“, ale zaměřuje se na aktivní „lov a likvidaci“ útočníka uvnitř sítě.

> **Zajímavost:** Podle statistik dochází k nejničivějším částem kybernetických útoků v pátek večer nebo během svátků, kdy interní IT týmy většiny firem nepracují. Služby MDR vznikly právě proto, aby tuto slabinu „víkendových útoků“ eliminovaly.

Zpět na Bezpečnost