EDR (Endpoint Detection and Response)

Zatímco klasický antivirus funguje jako „vrátný“, který do budovy nepustí známé kriminálníky, **EDR** funguje jako síť bezpečnostních kamer a detektivů uvnitř budovy, kteří sledují podezřelé chování každého, kdo se dostal dovnitř.

1. Proč EDR vzniklo?

Tradiční antiviry (EPP - Endpoint Protection Platform) spoléhají na tzv. **signatury** (otisky prstů známých virů). Moderní útočníci však používají techniky, které signaturu nemají:

- **Fileless útoky:** Škodlivý kód běží pouze v operační paměti a nezapisuje se na disk.
- **Zneužití legitimních nástrojů:** Útočník použije vestavěné nástroje systému (např. PowerShell) k nekalé činnosti.
- **Zero-day útoky:** Zcela nové hrozby, které ještě nikdo nepopsal.

2. Čtyři pilíře fungování EDR

```
1. **Sběr dat (Monitoring):** Agent nainstalovaný na počítači sleduje procesy, síťová spojení, změny v registrech a přístupy k souborům.
2. **Detekce (Analýza):** Data jsou odesílána do cloudu, kde umělá inteligence hledá anomálie (např. "Proč program Kalkulačka najednou stahuje data z internetu?").
3. **Vyšetřování:** EDR ukládá historii událostí, takže administrátor může zpětně vidět celou cestu útočníka systémem (tzv. //Kill Chain//).
4. **Reakce:** Pokud EDR zjistí hrozbu, může napadený počítač okamžitě izolovat od sítě, ukončit podezřelý proces nebo smazat infikovaný soubor.
```

3. Srovnání: Antivirus vs. EDR

Vlastnost	Klasický Antivirus	EDR
Zaměření	Prevence (zabránit vstupu)	Detekce (najít útočníka uvnitř)
Způsob práce	Hledání známých virů (signatur)	Hledání podezřelého chování
Viditelnost	Vidí jen útok	Vidí celou historii aktivit na PC
Hlavní cíl	Smazat soubor	Pochopit útok a zastavit ho

4. Co je to XDR a MDR?

Technologie EDR se dále vyvíjí do širších konceptů:

- **XDR (Extended Detection and Response):** Propojuje EDR s daty z firewalů, e-mailů a cloudu pro komplexní ochranu celé firmy.
- **MDR (Managed Detection and Response):** Služba, kde EDR nástroje obsluhují profesionální

bezpečnostní experti externí firmy 24/7.

5. Přínos pro firmy

EDR dramaticky zkracuje dobu, po kterou se útočník v síti nachází (tzv. **Dwell Time**). Bez EDR trvá odhalení průniku průměrně přes 200 dní; s kvalitním EDR řešením se tato doba zkracuje na minuty či hodiny.

> **Zajímavost:** Termín EDR zavedl v roce 2013 Anton Chuvakin ze společnosti Gartner, aby popsal nově vznikající třídu nástrojů, které se nezaměřují jen na „blokování“, ale na „pochopení“ toho, co se v systému děje.

Zpět na Bezpečnost