Zero-day útok

Zero-day útok je kybernetický útok, který zneužívá softwarovou chybu dříve, než má vývojář šanci ji opravit. Název „Zero-day“ (nultý den) odkazuje na počet dní, které měl vývojář na přípravu opravy od chvíle, kdy se o chybě dozvěděl – tedy nula dní.

Tento typ útoku je extrémně nebezpečný, protože proti němu nefungují tradiční obranné mechanismy založené na signaturách (antiviry, IDS), jelikož útok je zcela nový a neznámý.

Klíčová terminologie

V rámci tohoto tématu rozlišujeme tři stádia:

- **Zero-day Vulnerability (Zranitelnost):** Skrytá chyba v kódu, o které výrobce neví.
- **Zero-day Exploit:** Software nebo kód vytvořený útočníkem, který konkrétně tuto chybu využívá k průniku.
- **Zero-day Attack (Útok):** Samotný akt zneužití exploitu k infikování systému nebo krádeži dat.

Časová osa Zero-day incidentu

Proces od vzniku chyby po její opravu obvykle probíhá následovně:

```
1. **Vznik chyby:** Programátor nechtěně vytvoří zranitelný kód.
2. **Objevení:** Útočník (nebo bezpečnostní výzkumník) chybu najde.
3. **Vytvoření exploitu:** Útočník napíše kód pro zneužití chyby.
4. **Útok:** Probíhají útoky, zatímco výrobce o chybě stále netuší.
5. **Odhalení:** Výrobce je informován (nebo útok detekuje).
6. **Vydání opravy:** Vývojář vydá bezpečnostní záplatu (patch).
```

Proč jsou Zero-day útoky tak cenné?

Existuje obrovský černý trh s těmito zranitelnostmi. Ceny za funkční exploit pro populární systémy (iOS, Windows, Android) se mohou pohybovat v řádech **milionů dolarů**. Kupci bývají:

- **Kyberkriminální skupiny:** Pro ransomware a špionáž.
- **Státní aktéři:** Pro účely kybernetické války a sledování.
- **Vládní agentury:** Pro účely vyšetřování.

Jak se bránit neznámému?

Protože neexistuje patch, obrana se musí spoléhat na jiné metody:

- **Heuristická analýza:** Antiviry, které hledají podezřelé chování, nikoliv známé vzorky.

- **Sandboxing:** Spouštění podezřelých souborů v izolovaném prostředí.
- **Využití Honeypotů:** Chytání útočníků do pastí, kde lze pozorovat jejich nové metody.
- **WAF (Web Application Firewall):** Může blokovat podezřelé dotazy, i když nezná konkrétní chybu.
- **Virtuální patching:** Dočasná pravidla na IPS/Firewallu, která blokují cestu k chybě dříve, než vyjde oficiální oprava.

> **Zajímavost:** Existují i tzv. „White-hat“ výzkumníci, kteří hledají zero-day chyby a zodpovědně je hlásí výrobcům za odměnu (tzv. **Bug Bounty** programy). Tím pomáhají internet dělat bezpečnějším dříve, než chybu najdou zločinci.

— **Viz také:** IDS/IPS, Honeypot, Firewall, Ransomware