Virtual Patching

Virtual Patching (známý také jako externí patchování) je bezpečnostní mechanismus, který vytváří ochrannou bariéru kolem aplikace nebo systému. Tato bariéra zachycuje a blokuje provoz, který se pokouší zneužít známou zranitelnost, dříve než tento provoz dosáhne samotného cíle.

1. Princip fungování

Na rozdíl od tradičního patchování, které mění binární soubory aplikace, Virtual Patching implementuje pravidla na síťových prvcích. Funguje v několika krocích:

```
1. **Identifikace zranitelnosti:** Je objevena chyba (např. pomocí skeneru zranitelností nebo hlášení CVE).
2. **Analýza exploitace:** Bezpečnostní experti určí, jak vypadá síťový provoz, který se tuto chybu pokouší zneužít.
3. **Vytvoření pravidla:** Do bezpečnostního nástroje (WAF, IPS) je přidáno pravidlo (signatura), které tento specifický provoz rozpozná a zahodí.
4. **Ochrana:** Systém je chráněn, i když aplikace pod ním je stále technicky zranitelná.
```

—

2. Kdy se Virtual Patching používá?

Tato technika je nepostradatelná v situacích, kdy nelze aplikovat standardní opravu:

- **Legacy systémy:** Staré systémy, pro které výrobce již nevydává aktualizace (End of Life).
- **Critical Uptime:** Servery, které nemohou být restartovány mimo plánovanou údržbu.
- **Vlastní aplikace:** Oprava chyby ve vlastním kódu může trvat týdny; virtuální patch zajistí ochranu během několika minut.
- **Zero-day útoky:** Rychlá reakce na nově objevené hrozby, pro které ještě neexistuje oficiální oprava.

—

3. Nástroje pro implementaci

Virtual Patching se nejčastěji realizuje pomocí:

- **WAF (Web Application Firewall):** Specializované na HTTP/HTTPS provoz, chrání před útoky jako SQL Injection nebo XSS (např. ModSecurity, Cloudflare, F5).
- **IPS (Intrusion Prevention System):** Hloubková kontrola paketů na síťové vrstvě (např. Snort, Suricata).
- **NGFW (Next-Generation Firewall):** Kombinují firewall s detekcí průniků.

—

4. Výhody a nevýhody

Výhody	Nevýhody
Rychlost: Ochrana může být nasazena během minut.	**Není to trvalé řešení:** Skutečná chyba v kódu stále existuje.
Bez restartu: Nevyžaduje odstávku systému.	**Falešná pozitiva:** Příliš přísné pravidlo může blokovat legitimní uživatele.
Snížení rizika: Překlenuje období „Window of Exposure“.	**Výkon:** Kontrola provozu může mírně zvýšit latenci sítě.

—

5. Virtual Patching vs. Tradiční Patching

Virtual Patching by neměl být vnímán jako náhrada, ale jako **komplementární strategie**. V ideálním případě organizace nasadí virtuální patch okamžitě po zjištění hrozby a následně v rámci plánované údržby provede řádné otestování a instalaci oficiální systémové záplaty.

Související články:

- Kybernetické hrozby a prevence
- WAF a síťová bezpečnost
- Hledání zranitelností a QA

Tagy: security virtual-patching waf ips cve exploits devops