

# Honeypot (Vábnička)

**Honeypot** je bezpečnostní prostředek (počítač, data nebo síťová služba), který je záměrně nastaven tak, aby vypadal zranitelně a lákal útočníky. Protože tento systém nemá žádný legitimní účel ani skutečné uživatele, jakákoliv aktivita na něm je automaticky považována za podezřelou nebo útočnou.

Honeypoty slouží především k **detekci útoků**, odvedení pozornosti od skutečných serverů a ke studiu metod, které hackeři používají.

## Typy Honeypotů podle úrovně interakce

Honeypoty se dělí podle toho, kolik volnosti útočníkovi poskytnou:

- Low-interaction (Nízká interakce):** Simuluje pouze základní služby (např. webový server nebo SSH port). Útočník nemůže ovládnout operační systém, ale správce získá informaci o pokusu o připojení a použitých heslech.
- High-interaction (Vysoká interakce):** Skutečný operační systém s reálnými službami. Útočník se může v systému pohybovat, instalovat software a provádět příkazy. Poskytuje nejvíce informací o postupech útočníka, ale je rizikovější na správu (útočník by se mohl pokusit napadnout zbytek sítě).

## Typy podle účelu nasazení

### 1. Produkční Honeypoty

Slouží k ochraně konkrétní firemní sítě. Jejím cílem je:

- Odlákat útočníka od skutečných databází.
- Zpomalit útočníka (marní čas na falešném cíli).
- Poskytnout včasné varování (pokud někdo „sáhne“ na honeypot, v síti je útočník).

### 2. Výzkumné (Research) Honeypoty

Používají je bezpečnostní experti a vládní agentury ke studiu nových hrozeb a trendů. Získávají data o tzv. **Zero-day** útocích a o tom, jaké nástroje hackeři aktuálně vyvíjejí.

## Další formy vábniček

- **Honeynet:** Celá síť složená z honeypotů. Simuluje komplexní podnikovou infrastrukturu.
- **Honeytoken:** Falešný soubor, záznam v databázi nebo e-mailová adresa. Pokud někdo soubor otevře nebo na adresu pošle e-mail, systém vygeneruje poplach.
- **Honeycred:** Falešné přihlašovací údaje (hesla) uložené v paměti nebo v souborech, které

útočník často hledá.

## Výhody a nevýhody

Výhody	Nevýhody
<b>Minimum falešných poplachů:</b> Každý kontakt je útok.	<b>Úzké zorné pole:</b> Vidí jen útočníky, kteří na něj přímo narazí.
<b>Detekce neznámých hrozeb:</b> Nepotřebuje signatury.	<b>Riziko průniku:</b> Špatně izolovaný honeypot může ohrozit zbytek sítě.
<b>Nízké nároky na data:</b> Nesbírá miliony logů, jen záznamy o útocích.	<b>Odhalitelnost:</b> Zkušení útočníci dokáží poznat, že jsou v pasti.

**Zajímavost:** Honeypoty jsou často součástí tzv. **Deception Technology**, která v celé síti rozmisťuje tisíce drobných pastí (kreditní údaje, konfigurační soubory), aby útočník při jakémkoliv kroku stranou okamžitě odhalil svou přítomnost.

— **Viz také:** [IDS/IPS](#), [SIEM](#), [SOC](#), [Zero-day útok](#)

From:  
<https://serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:  
<https://serviceit.cz/doku.php?id=honeyopot>

Last update: **2026/01/06 17:52**

