

Co je honeypot

Poslední aktualizace 15 listopadu, 2024

Honeypot je termín používaný v oblasti počítačové bezpečnosti, který označuje past na hackery a další neautorizované uživatele. Jde o server, službu nebo data, záměrně vystavené na internetu, jež se **maskují jako relevantní cíl pro útočníky**, ale ve skutečnosti jsou od zbytku infrastruktury izolované a bedlivě monitorované.

Cílem honeypotu je přilákat útočníky, aby se pokusili o průnik nebo útok, což umožní správcům sítě identifikovat a analyzovat používané nástroje, metody a techniky.

Na základě těchto cenných dat pak společnosti mohou lépe zabezpečit svou infrastrukturu.

Honeypoty se rozlišují podle zaměření a složitosti na:

- **Mízkou interakci:** Tyto honeypoty obvykle simulují pouze určité síťové služby a protokoly, aby přilákaly základní útoky. Jsou relativně snadné na nasazení a správu.
- **Vysokou interakci.** Tyto systémy poskytují realističtější a komplexnější prostředí, jež může zahrnovat celé operační systémy a aplikace. Cílem je přilákat pokročilejší útočníky a získat podrobnější informace o jejich metodách.
- **Spam traps:** Tento typ honeypotu je navržen k zachycení nevyžádané pošty ([spamu](#)). Poskytuje falešné e-mailové adresy, které by měly být používány pouze spamery.

Honeynets: Jde o sítě obsahující více honeypotů, které společně simulují realistické síťové prostředí, aby přilákaly sofistikovanější útočníky.