StaySecure
Leden 2020

Vyšetřování kybernetických útoků

Když dojde například ke vloupání, policie ohledává místo činu za účelem rekonstrukce dané události, nalezení viníků a sběru důkazů. Takto podobně probíhá i vyšetřování, kde je objektem zkoumání počítač nebo jiná digitální zařízení s cílem najít stopy, jak se útočník do systému dostal, co v něm udělal a co získal.

Jak probíhá takové vyšetřování?

Identifikace incidentu

Nejprve je nutné určit rozsah technického prostředí – může se jednat o jeden počítač, několik serverů či o kompletní síť. Velmi důležitý je klid. Pokud se rozhodnete příliš rychle, riskujete vymazání důležitých prvků (zálohy nutné k identifikaci původu útoku) a dat.

Získávání evidence

Pro vyšetřování jsou využívané záznamy, jako například obsah paměti (cache, RAM), stav internetového připojení, stav běžících procesů, obsah disku a další záznamy v podobě logů.

Uchování evidence

Další fází je vytvoření kopie stávajících důkazů, které jsou dále zkoumány a sestaveny do chronologické dokumentace (Chain of Custody).

Analýza evidence

Analytik pokračuje s rozborem dat, které má k dispozici. Nejčastějším případem analýzy bývají ztracená či odstraněná data poškozeného harddisku (ať nehodou či úmyslně útočníkem). Tyto soubory se však dají v reálu zachránit, neboť vymazáním souboru odstraníte pouze jeho cestu. Volné místo je potom označeno jako „dostupné“ a později je zastoupeno jiným souborem.

Vyhodnocení výsledků

V této fázi se vyvozují výsledky z předešlých kroků a identifikují se podezřelé aktivity z počátku útoku. Výsledky jsou reportovány s podrobným popisem podniknutých kroků zadavateli. To umožnuje následně implementovat ochranná opatření, aby se incident již neopakoval.

Jak usnadnit práci expertům.

- Neobnovujte vaše zařízení do továrního/dřívějšího nastavení bez důkladného sběru všech důležitých dat.
- Pravidelně zálohujte nejen vaše soubory, ale i logy ze systémů. Pomůžete tak rychleji obnovit data pro analýzu.

Jak vám můžeme pomoci?

Pokud vás zajímají detaily forenzního vyšetřování, neváhejte se na mne obrátit. Rád vám poradím i v jiných oblastech kybernetické bezpečnosti.

Oddělení IT Bezpečnosti

Cyber & Privacy

pwc