JAK SE BRÁNIT PHISHINGU

Manuál pro administrátory

OMEZTE PŘÍSTUP ÚTOČNÍKŮ K UŽIVATELI

V sofistikovaných spearphishingových kampaních útočníci falšují adresu odesílatele tak, aby vypadala stejně jako adresa konkrétní osoby v rámci organizace. Tomuto postupu se říká spoofing.

Doporučujeme proto využívat antispoofingové nástroje. Jmenovitě jde o technologie:

- **SPF** (Sender Policy Framework) ověřuje, zda zpráva dorazila od legitimního odesílatele. Funguje tak, že vlastník domény vytvoří speciální TXT záznamy, díky kterým SMTP server na základě adresních rozsahů rozhodne, zda je zařízení, které zprávu posílá, oprávněno odesílat zprávu pod hlavičkou dané domény.
- **DKIM** (DomainKeys Identified Mail) je specifický digitální podpis v hlavičce zprávy. Poštovní server zašifruje privátním doménovým klíčem část hlavičky zprávy. Přijímací server si následně z DNS záznamu domény stáhne veřejný klíč, dešifruje hlavičku zprávy a ověří, zda zpráva skutečně pochází z dané domény a nebyla cestou změněna.
- **DMARC** (Domain Message Authentication Reporting and Conformance) vyhodnocuje výstup z mechanismů SPF a DKIM.

Všechny tyto nástroje využívá řešení ESET Mail Security při detekci podezřelých zpráv a spamu.

Čím méně informací útočníci budou mít tím lépe. Je na zvážení, zda zveřejnit přesnou strukturu firmy, životopisy managementu a další údaje, které by šlo zneužít.

Podobně by také zaměstnanci měli zvažovat, jaké služební informace budou sdílet na internetu. Můžete například informovat zaměstnance o tom, jak si nastavit profily na sociálních sítích jako soukromé. V rámci pracovních smluv a směrnic můžete také vyžadovat, aby zaměstnanci nesdíleli interní informace. Lze to doporučit především v oblastech kritické infrastruktury, státních úřadů a strategických podniků, které bývají terčem APT útoků.

NAUČTE UŽIVATELE IDENTIFIKOVAT SPEARPHISHING

Důležité je vytvořit prostředí, ve kterém se zaměstnanci nebojí zeptat. Doporučujeme vytvořit jednu e-mailovou adresu nebo kontaktní osobu, na kterou se mohou lidé s dotazy obrátit. Důležité je, aby se takto dedikovaný člověk skutečně dotazům věnoval.

Méně sofistikované útoky dokáží proškolení zaměstnanci rozpoznat sami. Doporučujeme proto pravidelně školit tým a ukazovat na příkladech, jak podezřelé e-maily a další hrozby poznat.

Společnost ESET nabízí služby školení vašich zaměstnanců v oblasti IT bezpečnosti.

CHRAŇTE FIRMU PŘED DOPADY SPEARPHISHINGU

Doporučujeme dodržovat tyto univerzální zásady kybernetické bezpečnosti:

- Instalujte na všechny koncové stanice anti-malware řešení
- Využívejte výhradně legální a aktuální software
- Omezte využití maker pro Microsoft Office;
- Zvažte využívání správce hesel a dvoufaktorového přihlašování
- Mějte nastavenou politiku pro zálohování
- Kontrolujte, zda mají uživatelé správně nastavená přístupová práva a mažte nepoužívané účty
- Administrátorské účty využívejte jen pro nutné potřeby, nikoli pro e-mailovou komunikaci či surfování po internetu
- Vytvořte interní proces pro hlášení incidentů, který budou všichni zaměstnanci znát
- Vytvořte scénář, jak postupovat v případě rozsáhlého útoku, aby všichni zaměstnanci věděli, jak v případě různých incidentů postupovat.

Zdroj: ESET a Národní úřad pro kybernetickou a informační bezpečnost