Phishingový test

Východiska služby

Zasměstnanci jsou považováni za nejslabší článek v ekosystému kybernetické bezpečnosti a útočníci toho využívají. Poštovní schránky vašich zaměstnanců jsou zaplavovány denně podvodnými emaily, ti ztrácí ostražitost či reagují zbrkle. Hrozí tak jednoduché napadení vaší organizace, ztráta či zašifrování dat, únik informací. Je jen otázkou času, kdy někdo z vašich uživatelů na takový email zareaguje!

Chcete vědět, jak na tom jste a jak velká je to pro vás hrozba?

Obsah služby

Společnost Chranimdata s.r.o. je připravena otestovat vaše zaměstnance pomocí simulovaného phishingového útoku. Díky testu můžete bez jakéhokoliv rizika sledovat jejich reakci a trénovat jejich chování. Ve spolupráci s vámi získáme potřebné informace pro výběr vhodných témat a obsahu cílených podvodných zpráv.

Poté jsou v dohodnutých termínech připravené zprávy rozeslány ze zfalšované adresy definovanému vzorku vašich uživatelů. Náš link nebo příloha samozřejmě nebude obsahovat škodlivý kód. Jediné, co budeme potřebovat je, aby váš antispamový systém neblokoval domluvené adresy.

Phishingové testy provádíme buď jednorázově, nebo dle potřeby zákazníka. V případě, že se bude jednat o „vzdělávací“ kampaň bude v rámci daného scénáře zobrazena stránka se zprávou, že se jedná o phishing. Dále zde budou poskytnuty informace, jak takové e-maily v budoucnu rozpoznat.

Na základě našich rozsáhlých zkušeností jsme vyvinuli řadu úspěšných scénářů. Například:

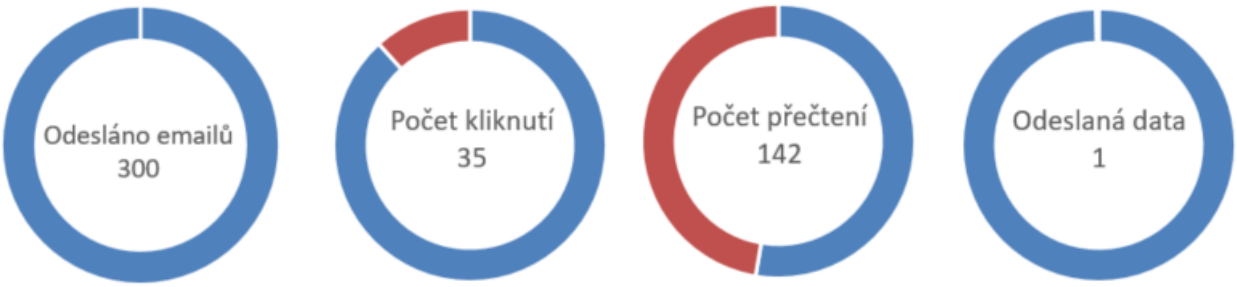
- **Uživatelské**
  - Varianty phishingových zpráv, které běžně člověk dostává. Např. falešná oznámení ze sociálních sítí, COVID-19 novinky, podvržené informace o kompromitovaných účtech, nově získané odměny atd.
- **Firemní**
  - Napodobují styl firemní komunikace, jako jsou vydané faktury, HR zprávy, zprávy o umístění e-mailu v karanténě, upozornění na firemní výhody atd.
- **Komerční**
  - Zprávy související s podnikáním a nákupy, který ale není typicky firemní. Patří sem oznámení o příchozí zásilce, žádosti o bankovní převod atd.
- **Cloudové**
  - Falešná upozornění, která nutí uživatele stahovat soubory z veřejného cloudového webu, upravovat dokument hostovaný v cloudu, resetovat heslo v cloudové službě atd.

Rozesílané zprávy mohou být následujícího typu:

Název	Popis
Odkaz na podvodnou webovou stránku	Zpráva obsahuje odkaz, který vede na podvodnou stránku imitující reálnou stránku.
Odkaz na podvodnou webovou stránku s žádostí o zaslání přihlašovacích údajů	Zpráva se snaží uživatele přesvědčit, aby zareagoval a vložil své přihlašovací údaje.
Závadná příloha	Zpráva obsahuje závadnou přílohu a snaží se uživatele přesvědčit, aby ji otevřel a spustil.

Výstup služby

Výstupem testů bude Závěrečná zpráva v elektronické formě obsahující popis jednotlivých testů, celkové vyhodnocení testu a návrh doporučení na základě analýzy výsledků. Výsledky budou zpracovány do přehledné zprávy s těmito statistikami:



Přínosy služby

- Snížení rizik pro vaši organizaci díky zvyšování bezpečnostního povědomí uživatelů
- Ověření, zda bezpečnostní školení vašich zaměstnanců jsou skutečně účinná
- Prověření reakcí zaměstnanců na pokusy o získání citlivých údajů
- Praktickými ukázkami upozornit uživatele na reálné nebezpečí phishingu
- Nepředstavuje riziko žádné skutečné škody pro vaši organizaci