Případovka

AUTOCONT

Hrozí nám ransomware? Provedení phishing testu

Statutární město Opava

PROFIL ZÁKAZNÍKA

Nad soutokem hlavních řek Opavska, Opavy a Moravice, se nachází město Opava. Včetně městských částí má cca 58 tisíc obyvatel a jeho katastrální území má rozlohu 9 061 ha. První písemná zmínka o Opavě jako o městě pochází z roku 1224.

Opava

OBDOBÍ REALIZACE

Prosinec 2015, trvání 21 dní

„Jsme si dobře vědomi hrozeb a rizik, která jsou spojena s dnes tak častými phishing útoky. Pouze připravená organizace dokáže odolat dnešním sofistikovaným útokům."

Ing. Zdenka Galgonková,
vedoucí odboru informatiky Magistrátu města Opavy

Výchozí situace a cíle projektu

Bezpečnost je základní premisou pro fungování každého informačního systému. V současné době je možné sledovat nebývalý rozmach útoků na jednotlivé uživatele prostřednictvím sociálních manipulací - phishing.

Tento typ útoků je pro potenciální útočníky jednoduchý a nebývale efektivní. Pro oběť má však na druhou stranu katastrofické dopady. Oběť může přijít o svoji identitu a peníze. Organizace pak může být vyřazena z činnosti nebo může být připravena o své know-how, zakázky nebo může dojít i k průniku na její bankovní účty.

Odbor informatiky Magistrátu města Opavy si je velmi dobře vědom těchto hrozeb a rizik a jeho cílem je jim čelit. Jedním ze základních kroků je znát své slabiny, vědět co může útočník zneužít.

To je důvod proč se statutární město Opava rozhodlo provést tzv. phishing test (neboli také PST), který ověřuje, nakolik jsou jednotliví uživatelé manipulovatelní prostřednictvím e-mailů a nakolik tedy představují zásadní hrozbu.

Cílem bylo ověřit, na jaké typy e-mailů uživatelé reagují a jestli má budování bezpečnostního povědomí odpovídající efekt.

PŘÍNOSY

Statutární město Opava:

- získalo představu o tom, jaké mají jeho zaměstnanci bezpečnostní povědomí
- získalo cenné informace o tom, jak budou jeho uživatelé odolní phishingu
- dnes ví, zdali je nutné implementovat další bezpečnostní opatření
- může opakovat provedení phishing testu, aby si opakovaně ověřilo efektivitu školení uživatelů

Zákazník si pořizuje licenci na provedení testů.

Není nutné pořizovat žádnou další technologii.

Zákazník nastavuje e-mail gateway dle instrukcí, aby se zajistil průchod testovacích e-mailů.

Popis řešení

Uživatelé zákazníka jsou testováni na odolnost vůči phishingu (cílenému útoku prostřednictvím e-mailu). Je připraven jeden nebo více e-mailů, které předstírají, že jsou legálními, legitimními e-maily, a ty jsou rozeslány na vybrané uživatele zákazníka. E-maily obsahují v těle odkaz (tak, jak je tomu u skutečných phishing e-mailů) a pokud uživatel na odkaz klikne, je zaregistrován pro další vyhodnocení. E-maily, pro hodnověrnost, mohou falšovat libovolného odesílatele včetně vizuálního stylu.

Zákazník získá představu, nakolik jsou jeho uživatelé zranitelní phishing útokem. Na základě testu může zákazník přijmout odpovídající opatření.

Klíčové charakteristiky

- je zaznamenáno otevření a kliknutí na e-mail
- je zaznamenáno jméno uživatele, prohlížeč, kterým otevíral odkaz, a IP adresa
- je možné test rozprostřít do potřebného časového okna, test je možné opakovat a tím sledovat efekt školení uživatelů

Možností je vytvořit libovolný e-mail a informační zprávu pro uživatele, který na link kliknul.

V navrženém řešení byly připraveny 3 různé e-maily, které napodobovaly dvě externí organizace, a jedna interní zpráva z fiktivního oddělení Magistrátu města Opavy.

Odeslání falešných e-mailů bylo připravováno v utajení. Po rozeslání a kliknutí na „phishing link“ byla vrácena odpověď Error 404 (uživatelé tuto zprávu znají). Rozeslání e-mailů bylo rozloženo v čase tak, aby uživatelé nepojali podezření a výsledky měly pro statutární město Opava vypovídající hodnotu.

Na základě výsledků byla zpracována zpráva, kterou Statutární město Opava využilo pro přijetí následných bezpečnostních opatření.