Bezpečnostný audit technikami sociálneho inžinierstva

„Kým správanie sa systémov pri útoku sa dá z pohľadu IT bezpečnosti pomerne exaktne predikovať, monitorovať a vyhodnocovať, myslenie a konanie ľudí v krízových situáciách je značne ovplyvnené okolnosťami a prostredím. Na našich ľudí sa však potrebujeme 100% spoľahnúť v každej situácii. Preto našich zamestnancov nielen školíme v oblasti informačnej bezpečnosti, ale aj pravidelne testujeme úroveň ich bezpečnostného povedomia. Bezpečnostný audit od ESET Services preveril ich schopnosť využiť teoretické poznatky v praxi. Konzultanti ESET testovanie našej organizácie zvládli profesionálne a na jednotku."

Jaroslav Lompart, IT security manager, Poštová banka

ZÁKAZNÍK

Poštová banka je najrýchlejšie rastúca banka na slovenskom trhu, čoho dôkazom je, že v rokoch 2008 až 2011 získala za svoje produkty a služby množstvo prestížnych ocenení od nezávislých organizácií a odbornej verejnosti. Vďaka partnerstvu so Slovenskou poštou a širokej predajnej sieti má ku svojim klientom veľmi blízko. Okrem klasických bankových služieb pre občanov a podnikateľské subjekty pôsobí Poštová banka prostredníctvom dcérskych spoločností aj na trhu podielových fondov (Prvá penzijná správcovská spoločnosť Poštovej banky), v poisťovníctve (Poisťovňa Poštovej banky) a v oblasti dôchodkového sporenia v druhom pilieri (Dôchodková správcovská spoločnosť Poštovej banky).

ZADANIE

Zistiť úroveň bezpečnostného povedomia zamestnancov, znalosť interných predpisov a v reálnych situáciách preveriť správanie sa zamestnancov, keď je na nich vyvíjaný psychický nátlak. Ako metóda testovania bol použitý „black-box" - to znamená, že sa simuluje reálny útok a testovaný subjekt nespolupracuje na príprave testovania a neposkytuje vopred žiadne interné informácie (napr. informácie o poskytovaných službách, štruktúre organizácia a dôležitosti spracovávaných dát).

RIEŠENIE

Prvý krok bol zistiť všetky užitočné informácie z verejne dostupných zdrojov (oficiálne internetové stránky, publikované informácie, sociálne siete, ...). Zamerali sme sa hlavne na informácie o zamestnancoch, predmet podnikania a na obchodné vzťahy. Na zber dát sme použili automatizované vyhľadávacie a korelačné nástroje, ktoré sme doplnili ručným zberom dát. Všetky získané informácie sme podrobili kontrole na platnosť a aktuálnosť.

Následne sme informácie použili na zostavenie testovanej vzorky, výber testovacích metód a na prípravu testovacích scenárov. Do testovanej vzorky sme zaradili zamestnancov rôznych vekových kategórií, na rôznych pozíciách, v rôznych lokalitách, tak aby vzorka štatisticky čo najlepšie reprezentovala testovanú organizáciu. Vzhľadom na poskytované služby a štruktúru organizácie Poštovej banky sme sa zamerali na phishingové techniky a ako komunikačné kanály sme zvolili email a telefón. V rámci emailovej kampane sme rozposlali 50 cielených phishingových správ. V rámci telefonickej kampane sme oslovili 10 zamestnancov, pričom na každého testovaného zamestnanca sme si pripravili individuálny scenár, ktorý zohľadňoval informácie, ktoré sa nám podarilo zistiť v úvodnej fáze projektu.

Po ukončení všetkých testov sme vypracovali výslednú správu, ktorá obsahovala zoznam zistení a odporúčania na ich odstránenie, popis realizovaných scenárov, postup pri výbere testovanej vzorky a podrobný popis celého priebehu testovania.

„Výsledky testovania nám pomôžu presnejšie a adresnejšie zacieliť náš vzdelávací program a prispievajú tak k zvýšeniu bezpečnostného povedomia v našej organizácii", hovorí manažér pre informačnú bezpečnosť Jaroslav Lompart.