

Ochrana dodavatelů tiskových řešení

“Odbornost a zkušenosti konzultantů společnosti ESET v oblasti testování technikami sociálního inženýrství přispěly ke zvýšení bezpečnostního povědomí našich zaměstnanců a k budování bezpečného prostředí v naší organizaci”.

Pavel Kmoníček, Security manager,
GMC Software Technology s.r.o.



ZÁKAZNÍK

GMC Software Technology je špičkou mezi dodavateli tiskových řešení a personalizovaných dokumentů pro komunikaci se zákazníky. Společnost se zabývá vývojem softwaru pro návrh, kompozici a produkci personalizovaných dokumentů v oblasti komunikace firem se zákazníky. Produkty GMC Software Technology (dále jen GMC) používá řada firem etablovaných v českém a zahraničním finančním sektoru. GMC je globální společnost se sídlem ve Švýcarsku a pobočkami v Evropě, Asii, Severní a Jižní Americe.

HLAVNÍ POŽADAVKY

Zadání bylo vyspecifikováno následujícím způsobem.

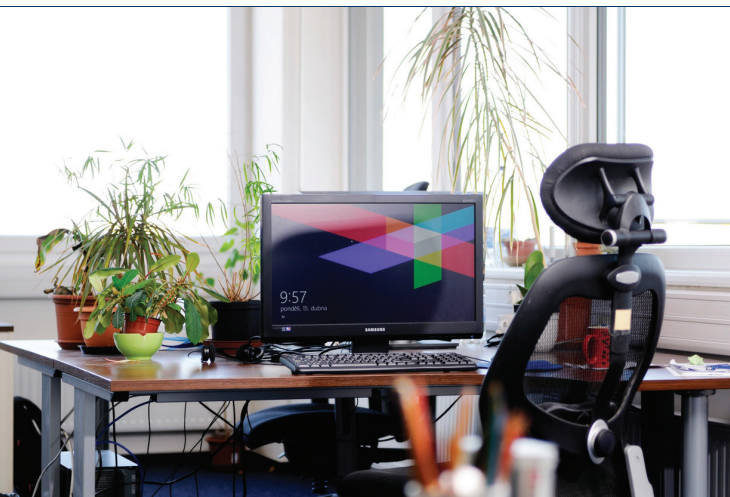
- Metodami sociálního inženýrství prověřit bezpečnostní povědomí zaměstnanců a účinnost implementovaných bezpečnostních opatření v rámci poboček GMC v České republice.
- Ověřit reakce zaměstnanců primárně na:
 - phishingové emaily s potenciálně možným zavedením škodlivého kódu;
 - telefonáty s žádostí o zaslání/sdílení chráněných informací;
 - nalezená/obdržená přenosná media z neznámého zdroje a s neznámým obsahem s potenciálně možným zavedením škodlivého kódu.
- Testovat tzv. „black-box“ přístupem – to znamená, že testovaná organizace neposkytne před testováním žádné interní informace o svém fungování. Součástí testování je tedy i sběr potřebných informací z veřejných zdrojů. Zvolený typ testu simuluje útočníka z vnějšího prostředí bez jakýchkoliv interních informací o testované organizaci.
- K ohodnocení rizik použít metodiku zavedenou v GMC tak, aby bylo možné výsledky testování jednoduše zahrnout do celkového řízení rizik.

REFERENCE

„Pomocí realizovaných testů jsme získali informace o aktuálních slabínách v chování zaměstnanců a zavedených bezpečnostních opatření. Už samotná realizace testů přispěla ke zvýšení bezpečnostního povědomí u zaměstnanců, zejména díky tomu, že nyní mají osobní zkušenost s možným útokem pomocí sociálního inženýrství. S výsledky testování současně získáváme cenný materiál pro interní školení, do něhož můžeme nově zakomponovat konkrétní příklady možného útoku z prostředí GMC SW”.

Pavel Kmoníček, Security manager, GMC Software Technology s.r.o.





ŘEŠENÍ

Úvodním krokem při black-box testování je získání co nejdetailnějšího obrazu o testované organizaci pomocí sběru informací z veřejně dostupných zdrojů, jako jsou např. webové stránky společnosti, sociální sítě a různé vyhledávače. Sběr byl zaměřený na informace o zaměstnancích, předmětu podnikání, obchodní vztahy, kontakty či získaná ocenění. Použito bylo ruční vyhledávání i automatizované nástroje pro sběr, vizualizaci a vyhodnocování informací z Internetu.

Na základě získaných informací navrhl testovací tým scénáře a seznam cílových osob, na které byly tyto scénáře zaměřené. Do testovacího vzorku byli zařazeni zaměstnanci z různých oddělení, na různých pozicích a v různých lokalitách tak, aby vzorek co nejlépe pokrýval různé části organizace. Scénáře pro jednotlivé testy byly následně projednány a odsouhlaseny zástupcem GMC.

Telefonické testy zahrnovaly scénáře, při kterých byli kontaktováni vybraní zaměstnanci GMC s cílem získat chráněné firemní informace. Telefonické testy byly podpořeny i emailovou komunikací. Při emailových testech použil tým scénáře, při kterých rozeslal různé phishingové emaily na několik desítek zaměstnanců testované organizace. Cílem těchto emailů bylo ověření reakcí uživatelů na vložený link nebo připojenou přílohu. Při testu s přenosnými médii byla do prostor organizace roz distribuována přenosná média s cílem ověřit chování zaměstnanců v případě, že se dostanou k CD nebo USB klíči s neznámým obsahem. Při žádném z provedených testů nebyl použitý škodlivý kód.

Po ukončení výkonu testů vypracoval testovací tým komplexní zprávu, která obsahovala popis realizovaných scénářů, podrobný průběh testování, výsledky, vyhodnocení rizik a navržená doporučení. Zpráva také obsahovala stručné shrnutí pro management GMC s nejdůležitějšími závěry z testování.

KONTAKT

Pavel Kmoníček, Security manager, GMC Software Technology s.r.o.

