Jak účinně chránit obchodní značku před kyberhrozbami

26.9.2023 - | PROTEXT

Podle Olgy Svistunové, analytičce webového obsahu ve společnosti Kaspersky, kyberzločinci zneužívají k páchání svojí trestné činnosti dobrého jména obchodních značek, na jejichž vybudování tvrdě pracovali jiní lidé.

Na podvodné webové stránce, která velmi dobře kopíruje stránku zavedené značky nebo online služby, zveřejňují promyšlený obsah, aby vylákali od lidí cokoli od přihlašovacích údajů přes osobní a profesní identitu až po citlivé firemní nebo finanční informace. Může to vést ke ztrátě dat a peněz, ale také k velkému riziku poškození pověsti firmy, protože zpráva o takovém případu může způsobit negativní vnímání značky ze strany veřejnosti.

Chcete-li svoji obchodní značku ochránit před potenciálními kybernetickými riziky, měli byste dodržovat několik jednoduchých pravidel:

1. Poučte zaměstnance i zákazníky o tom, jak rozpoznat podvodný e-mail nebo webovou stránku. Nedostatečné povědomí o kybernetické bezpečnosti mezi zaměstnanci firmy může vést k narušení důležitých obchodních procesů a úniku dat. Kyberzločinci mohou získat kontrolu nad účty firmy na sociálních sítích a provádět jejím jménem škodlivé aktivity.

2. Vaši zákazníci jsou vystaveni stejnému riziku – měli by si být vědomi možných hrozeb, aby je dokázali rozpoznat. K dosažení tohoto cíle mohou firmy provádět specializovaná školení o kybernetické bezpečnosti pro zaměstnance a vytvářet speciální příběhy nebo série e-mailů s informacemi o bezpečnosti, které zákazníkům vysvětlují, jak rozpoznat phishingové aktivity.

3. Pokud pracujete ve finanční nebo jiné citlivé oblasti, která často přitahuje kyberzločince, upozorněte svoje klienty na zvýšené riziko podvodu. Požádejte je, aby věnovali větší pozornost e-mailům a zprávám, které dostávají.

4. Požádejte svoje zákazníky, aby nahlásili všechny neobvyklé aktivity prováděné pod vaší značkou. Poproste je také o poskytnutí snímků obrazovky a dalších důkazů, abyste mohli včas zachytit podezřelé akce.

5. Věnujte pozornost nastavení zabezpečení svých účtů na sociálních sítích. Firmy zpravidla zveřejňují informace a komunikují se svými příznivci nejen na vlastních, ale také na externích platformách. Dávejte si pozor na nastavení soukromí na těchto platformách, důkladně si je prověřte, vytvořte si silná komplexní hesla a nastavte si dvoufaktorové ověřování, pokud je to možné.

6. Používejte nástroje pro sledování hrozeb, například Kaspersky Digital Footprint Intelligence, k včasnému odhalení útoků zneužívajících vaši obchodní značku. Taková řešení vás mohou v reálném čase informovat o cíleném phishingu a falešných účtech na sociálních sítích a pomáhat sledovat výskyt phishingových webových stránek zaměřených na firemní značku, stejně jako monitorovat a odstraňovat falešné účty na sociálních sítích a aplikace na mobilních tržištích.

ČTK ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/jak-ucinne-chranit-obchodni-znacku-pred-kyberhrozbami/2418343