Kyberkriminalita na vzestupu. Počet napadených klientů bank vzrostl o 37 procent

18.9.2024 - Petr Lesenský | Dýcháme

Během prvních sedmi měsíců tohoto roku bylo prostřednictvím kyberútoků napadeno 49 436 klientů bank. Meziročně tak jejich počet vzrostl o 37 procent.

Jednou z aktuálně nejrozšířenějších metod podvodníků je takzvaný smishing. Jeho princip spočívá v rozesílání klamavých SMS zpráv, které se z obětí snaží vylákat citlivé údaje. Útočníci se přitom maskují za oficiální instituce, jako jsou banky, pojišťovny či přepravní společnosti. Snížit počty okradených pomáhají moderní technologie i edukativní kampaně.

Česká bankovní asociace (ČBA) upozorňuje na pokračující nárůst kybernetických útoků, které cílí na klienty bank po celé České republice. Jen za prvních sedm měsíců tohoto roku bylo napadeno 49 436 klientů, což představuje nárůst o 37 procent oproti stejnému období loňského roku. Podle **Marka Macháčka**, experta na prevenci platebních podvodů v Komerční bance, je právě Česko s počtem podvodů na předních místech. *„Je to proto, že stojíme na špičce v oblasti bankovních technologií a podvodníci si u nás své metody zkoušejí. Co bude fungovat u nás, bude pak fungovat i jinde,“* dodává expert.

Jednou z aktuálně nejpopulárnějších metod podvodníků, s níž se pravděpodobně alespoň jednou setkal každý vlastník mobilního telefonu, je takzvaný smishing. Jedná se o podvodnou techniku založenou na phishingu, která využívá SMS zprávy k získání citlivých informací od uživatelů. *„Útočníci posílají falešné smsky nebo zprávy na různých chatovacích platformách typu WhatsApp, které často vypadají jako od důvěryhodných institucí a snaží se oběti přimět k vyzrazení osobních údajů či přihlášení na podvodné weby,“* popisuje **Jan Nedělník**, CEO společnosti Konecta Czech, Hungary a Slovakia, která působí v oblasti zákaznického servisu

Podvodné SMS typicky obsahují aktivní odkaz, jenž člověka přesměruje na falešné stránky konkrétní instituce. Zde je nucen přihlásit se prostřednictvím své bankovní identity či zadat citlivé údaje o svojí kartě. Uvedením daných informací však otevírá dveře čekajícím podvodníkům. Ti následně mohou proniknout do internetového bankovnictví oběti, ukrást její údaje o platební kartě, pokusit se provést platbu nebo citlivá data vyzkoušet pro přístup do jiných služeb či je prodat na černém trhu.

Podvodníci využívají sezónnost

K zefektivnění svých pokusů se kyberpodvodníci často snaží využít různé sezónní příležitosti. Před Vánocemi se například vydávají za e-shopy či přepravní společnosti. V čase odevzdávání daňových přiznání se zase maskují za Finanční správu ČR. Vůbec nejčastěji si však přisvojují identitu zástupců bank a pojišťoven.

Řadu podvodných smishingových útoků na své klienty řeší v letošním roce například VZP ČR. Podvodníci nejčastěji lákají oběti prostřednictvím odkazů na falešné weby, kde se má příjemce prostřednictvím formuláře registrovat pro získání finanční odměny. *„Vyplněním údajů se vystavujete vysokému riziku, že budou vaše osobní data zneužita k odčerpání prostředků z vašeho účtu. Jediným správným postupem je takové zprávy zcela ignorovat a odesílatele klidně zablokovat,“* doporučuje **Jan Svoboda**, šéf bezpečnostního úseku VZP ČR.

Rychlá reakce může úspory zachránit

Smishingové útoky byly dříve rozeznatelné podle krkolomné stylistiky a špatné gramatiky. Dnes jsou však texty řady falešných zpráv mnohem propracovanější. Rovněž falešné stránky institucí, na které se útočníci snaží své oběti nalákat, jsou mnohdy téměř k nerozeznání od oficiálních. Varovným signálem může být například cizí telefonní číslo, z něhož je zpráva adresována. I to však má svůj háček. *„Propracovanější smishingové útoky dnes mnohdy využívají i metodu zvanou spoofing. V rámci ní dokážou napodobit jiné telefonní číslo. Člověku se tak na mobilním telefonu skuteční zobrazí, že mu píše jeho banka, pojišťovna, či dokonce policie,“* upozorňuje Jan Nedělník.

Častým znakem, podle kterého je možné smishing odhalit, je snaha pisatele vyvolat pocit naléhavosti. Podvodníci často lákají na výhodné nabídky, odměny či naopak smyšlená nebezpečí v podobě kupříkladu napadených účtů. Podezření může rovněž vzbudit nestandardní podoba samotných odkazů, jež mnohdy obsahují zkrácená či cizí slova nebo čísla.

Obecně platí, že pokud má adresát SMS jakékoli podezření, neměl by žádné aktivní prokliky ve zprávách používat a vše si raději ověřit u dané instituce. V momentě, kdy si uvědomí, že naletěl na podvod, měl by pak co nejrychleji kontaktovat svoji banku. V některých případech lze rychlou reakcí peníze na účtu ještě ochránit.

Banky zdokonalují zabezpečení

Ačkoli se techniky podvodníků neustále zdokonalují, na místě rozhodně nezůstávají stát ani bankovní instituce. Díky efektivním zásahům se jim podařilo od počátku roku uchránit svým klientům více než 4 miliardy korun, přičemž nejvyšší doposud zachráněná částka na jednoho klienta činila 13 milionů korun. Přesto škody způsobené e-šmejdy dosáhly 845 milionů korun. V meziročním srovnání se jedná o nárůst o 9 procent.

Průměrná škoda na klienta se oproti loňsku snížila na 17 083 Kč z předchozích 21 439 Kč. *„Tento pokles je výsledkem efektivních kontrolních procesů bank. Moderní technologie, do kterých banky investují významnou část svých rozpočtů, umožňují rychle identifikovat a zastavit podezřelé transakce dříve, než mohou způsobit výraznější škody,“* uvádí **Radek Šalša**, vedoucí PR a komunikace České bankovní asociace.

Odpovědnost však podle něj není jen na bankách, ale především na klientech samotných, kteří se v důsledku neznalosti stávají snadným terčem pro podvodníky. Výraznou roli tak hraje i pokračující edukace veřejnosti. Příkladem může být rozsáhlá informační kampaň #nePINdej!, kterou organizuje Česká bankovní asociace ve spolupráci s Policií ČR, Národním úřadem pro kybernetickou a informační bezpečnost, Vysokým technickým učením v Brně a dalšími partnery z řad bank a významných zástupců českého byznysu.

https://www.dychame.cz/kyberkriminalita-na-vzestupu-pocet-napadenych-klientu-bank-vzrostl-o-37-procent