Ako sa vyhnúť firemným podvodom?

Počet sofistikovaných digitálnych podvodov, ktoré sú spojené s finančnými stratami vo firmách, neustále narastá. Obeťou sa môže stať každý. Prečítajte si užitočné rady, ako ich spoznať, a tipy, ako sa im vo firme vyhnúť.

Známou formou digitálnych útokov vo firmách sú **autorizované podvody**, v ktorých sa obetiam manipuluje s realizáciou firemných platieb. Podvodníci používajú na vykonanie podvodu rôzne taktiky, najčastejšie:

1. Podvod s úhradou faktúry

V tomto type podvodu sa **útočník môže vydávať za dodávateľa firmy** – či už za bývalého, alebo súčasného.

Zaslaná faktúra od útočníka **vyzerá identicky s reálnou faktúrou** (logo, adresa, IČO), no sú **pozmenené platobné údaje** (IBAN). Túto zmenu je možné veľakrát prehliadnuť. Útočník sa spolieha, že pracovník firmy nebude overovať správnosť údajov, keďže ide o kontakt s dlhodobou spoluprácou.

Rovnako sa využívajú aj **manipulatívne techniky**, ako je naliehanie na úhradu platby z dôvodu nedodržania termínu alebo priame oznámenie zmeny v platobných údajoch. V takýchto prípadoch **je potrebné preveriť si každú zmenu aj cez iný kontakt, ako je odosielateľ e-mailu**.

2. CEO fraud

Pri CEO fraude ide o naliehavé platby na podvodné účty, v ktorých sa **útočník vydáva za nadriadeného osoby, ktorej je mail zaslaný**. Páchateľ vystupuje ako CEO firmy alebo finančný riaditeľ. Využíva sa tak **manipulácia cez autoritu v danej firme**.

Môže ísť o **písomný, telefonický alebo dokonca zmanipulovaný videohovor**. Páchateľ vie vďaka pokročilým technikám veľmi vierohodne **napodobniť identitu reálnej osoby**. Telefónne číslo môže byť veľakrát **„spoofnuté"**, čo znamená, že ide o predstieranie identity reálnej osoby či firmy (napr. na displeji mobilného telefónu sa zobrazí meno nadriadenej osoby alebo názov spoločnosti).

Aj v takýchto prípadoch je opäť **nevyhnutné zabezpečiť viacúrovňové preverenie požiadavky** alebo **využiť na preverenie aj iný kontakt** ako ten, z ktorého podnet prichádza.

Spôsoby podvodnej komunikácie:

Podvodná komunikácia môže byť doručená z reálnej e-mailovej adresy, pretože je napadnutá „malvérom". Alebo útočník používa e-mailovú adresu či doménu, ktorá pôsobí ako od reálneho dodávateľa (napr. je pozmenené 1 písmeno: *namiesto „emerald" je uvedené „ernerald" alebo sa v závere mailu doplní písmeno „s" – napr. namiesto „holding.com" sa uvedie „holdings.com")*.

TATRA BANKA
Member of RBI Group

Čo je malvér?

Ide o škodlivý softvér, ktorého cieľom je poškodiť alebo zneužiť programovateľné zariadenie, službu či sieť. Môže ísť aj o **phishingové útoky na získanie prístupu k e-mailovému účtu** alebo počítačovému systému obete. Keď podvodníci získajú takýmto spôsobom prístup, môžu monitorovať komunikáciu a identifikovať platobné príležitosti na zacielenie daného podvodu.

Ako sa šíri malvér?

Malvér sa šíri primárne cez prílohy v e-mailoch, škodlivé reklamy na populárnych webových stránkach (malvertising) či falošné inštalácie softvéru. Rovnako však aj cez infikované jednotky USB, infikované aplikácie alebo textové správy.

Rozdiel medzi malvérom a phishingovým útokom:

Na rozdiel od phishingových útokov ide o **podvod s presmerovaním platieb zameraný na jednotlivcov** alebo malé počty zamestnancov (oddelenie vo firme), kde je nie adresátom celá firma. Tento spôsob podvodu zameraný na jednotlivcov môže zvýšiť jeho úspešnosť, lebo ak pracovník zrealizuje platbu podľa pokynov, v celom procese nie je zapojený ďalší zamestnanec, ktorý by si mohol všimnúť podvodnú a neštandardnú aktivitu.

Odporúčania, ako sa vyhnúť autorizovaným podvodom:

1. Edukácia

Veľmi dôležitou prevenciou predchádzania autorizovaným podvodom je **pravidelná edukácia zamestnancov** o tejto téme. Práve vďaka dostatočným informáciám o spôsoboch podvodnej komunikácie môžu pracovníci zabrániť podvodným útokom vo firmách.

2. Priame overenie

Vždy je potrebné **dostatočne overiť akúkoľvek zmenu súvisiacu s platbou aj cez iný komunikačný kanál**, ako je ten, z ktorého požiadavka prichádza. Odkazy alebo kontaktné údaje uvedené v e-maile alebo v liste so žiadosťou o zmenu môžu byť podvodné. Tie určite **nie je vhodné používať**.

3. Viacúrovňové kontroly

Účtovníci a zamestnanci s prístupom k platbám by mali vykonávať **viacúrovňové kontroly**:

- Overenie obchodného partnera cez oficiálny podnikový systém.
- Kontrola e-mailovej adresy, z ktorej požiadavka prichádza.
- Overenie spôsobu neštandardnej komunikácie iným kanálom, ako prichádza komunikácia (napr. telefonické overenie).

4. Čo najskôr autorizovaný podvod nahlásiť

Vyšetrovanie takejto trestnej činnosti je nesmierne náročné, keďže finančné prostriedky sú presúvané veľmi rýchlo. Pravdepodobnosť návratu finančných prostriedkov späť poškodeným je nízka, najmä ak je incident nahlásený s časovým odstupom. Preto je dôležité pravidelne edukovať zamestnancov a zabezpečovať preventívne kontroly v oblasti platieb, vďaka ktorým sa dá vyhnúť nežiaducemu podvodu.

Viac informácií nájdete
na https://www.tatrabanka.sk/predigitalnubezpecnost/bezpecnost-a-firmy/

TATRA BANKA
Member of RBI Group