

PODVOD ZVANÝ BOSS SCAM, CEO/BEC PODVOD

Kamil KOPECKÝ

Boss scam (či CEO/BEC fraud, fake president) je druhem podvodu, ve kterém pachatelé předstírají, že jsou vaši nadřízení (např. ředitelé), kteří chtějí, abyste převedli na jejich pokyn peníze z firemního účtu na účet jiný, např. na zafinancování konkrétního projektu, případně proplatili fiktivní fakturu či fiktivní platební příkaz. Podvod využívá především nepozornosti zaměstnanců, kteří jsou zvyklí se svým nadřízeným běžně e-mailem komunikovat a již si neověřují, od koho příkaz ve skutečnosti přišel.

Podvod začíná nenápadně, na firemní e-mail nám dorazí **zpráva, která se tváří, jako kdyby ji odeslal váš nadřízený** - odesílatel se skutečně "jmenuje stejně". Na první pohled se tedy může zdát, že skutečně pochází od našeho nadřízeného.

(Běžná e-mailová stránka se seznamem zpráv, pachatel využívá jméno Kamil Kopecký)

V našem příkladu se zaměříme na e-mail s předmětem: Platba. Ten se tváří, jako by byl odeslán Kamilem Kopeckým. V tento moment je velká část zaměstnanců přesvědčena, že e-mail skutečně pochází od jejich vedoucího. Po otevření e-mailu se nám objeví následující zpráva.

Na první pohled vidíme, že náš nadřízený chce ověřit stav firemního účtu, protože bude chtít provést finanční operaci. Na což má jistě oprávnění. Pokud se ale zaměříme na e-mail podrobněji, zjistíme, že **e-mailová adresa odesílatele neodpovídá skutečné firemní či soukromé adrese našeho šéfa**. Pokud jsme ale zvyklí takto s vedoucím komunikovat, snadno tento zásadní detail přehlédneme. V dalším e-mailu nám pak náš “fiktivní šéf” pošle konkrétní čísla účtu s detailním platebními informacemi, požaduje potvrzení o odeslání apod. Pokud pak peníze převedeme, velmi rychle zmizí jak účet, tak i pachatel.

Přestože je podvod poměrně jednoduchý, i v České republice nalezneme řadu případů, ve kterých skutečně pracovníci administrativy finanční prostředky na zahraniční účty převedly. O téměř půl milionu korun např. [přišla firma na Zlínsku](#), která uvěřila podvodníkovi. Účetní firmy dostala e-mailem od svého šéfa pokyn, aby odeslala peníze. Jenže se ukázalo, že e-mail byl falešný. Policie takových pokusů o podvod vyšetřuje celou řadu.

“Jedná se o poměrně rozsáhlou trestnou činnost, která je Policií ČR prověřována. Velmi často jsou poškozenými právnické osoby, v jejichž firmách je účetní agenda složitá a objemná. Pak se lehce stane, že je některý z takto podvržených podvodných e-mailů vyslyšen a dojde k převodu finančních prostředků. Problémem je, že finanční prostředky jsou zasílány v cizí měně na zahraniční účty a škoda bývá opravdu vysoká. Sledování finančního toku bez rychlé reakce poškozeného, případně zajištění finančních prostředků na podvodném účtu, je pak cestou velmi komplikovanou a složitou. Přitom by stačilo jen více pozornosti při kontrole příchozí e-mailové pošty, ověření u nadřízeného který transakci zadal, nebo měl zadat. Způsob páchání u podvodů “boos scam” není totiž nějak moc sofistikovaný,” uvádí Pavel Schweiner, vyšetřovatel oddělení kyberkriminality KŘPOL.

Na tento typ podvodu pravidelně upozorňují české i zahraniční banky, včetně ministerstva financí a dalších institucí ([Česká spořitelna](#), [Komerční banka](#)). Podle statistik pak zhruba 20-30 % firem oslovených tímto podvodem částku skutečně zaplatí. Na

podvod upozorňuje také Europol, který k problematice ve spolupráci s českou policií vydal přehlednou infografiku (k dispozici v češtině [zde](#)).

Základní pravidla ochrany:

Ochranou je především **správně nastavený způsob předávání informací uvnitř firmy** (firemní komunikace), kdy jsou veškeré platební žádosti skutečně ověřeny. To však platí i mimo firemní sektor - vždy si ověřme, zda v případě online plateb skutečně komunikujeme s oprávněnou osobou. Toto lze snadno provést třeba telefonicky.

Pro E-Bezpečí
Kamil Kopecký
Univerzita Palackého v Olomouci