# **Zaměstnanci jsou nejslabším článkem zabezpečení firem a rizikem pro jejich data. Nejnověji na ně útočí AI**

**Praha, 16. května 2023** - **Nejslabším článkem zabezpečení firem jsou, ať už úmyslně nebo neúmyslně, zaměstnanci. Mohou vědomě vynášet citlivé informace, ale i bez špatného úmyslu klikat na nebezpečné odkazy nebo otevírat zavirované přílohy. Či bez uvážení předávat firemní data nedůvěryhodným zdrojům, v krajním případě i hackerům či šmejdům posílat firemní finanční prostředky. A nejnověji na ně útočí i AI v podobě naprogramovaných chatbotů či musí čelit zcela novým rizikům ChatGPT.**

**Nebezpečné klikání stále vede**

Podle výsledků simulovaných útoků v rámci testování odolnosti firem, pětina zaměstnanců klikne na odkaz ve zprávě, aniž by si prověřila, kam směřuje. Únik nebo poškození dat, falešné platební příkazy nebo phishingové léčky mohou způsobit firmám katastrofální škody. Zacílení na jednotlivce je velmi účinná technika, mnoho zaměstnanců stále kliká na phishingové e-mailové odkazy a stahuje přílohy se škodlivými soubory.

„Riziko pro firemní data a celkovou bezpečnost, které přichází od zaměstnanců je stále velmi vysoké. A phishingové útoky, které hackeři vedou přes zaměstnance jsou velmi účinné. Firmy mají stále ve vzdělávání svých zaměstnanců zejména v bezpečném chování na internetu rezervy,“ říká Ondřej Ševeček, odborník na bezpečnost a etický hacking z Počítačové školy GOPAS.

**Nezabezpečená komunikace**

Velkým rizikem jsou v době BYOD a častého home office i programy a platformy, na kterých probíhá komunikace na dálku. Pokud nejsou například videokonference stoprocentně zabezpečeny a výslovně určeny pro práci s citlivými informacemi, firemní data jsou pak vystavena obrovskému nebezpečí.

„IT specialisté mnoha firem pod tlakem okolností dělají ústupky a unáhlená rozhodnutí a volí často snadná a levnější řešení bez ohledu na bezpečnostní rizika. To se jim může velmi nevyplatit,“ říká Michal Černý ze společnosti Audiopro.

**Personalizované útoky a CEO Fraud**

Podvodných metod napodobujících vnitrofiremní komunikaci je mnoho. Existují konkrétní příklady, kdy zaměstnancům přišly podvodné zprávy, které oznamovaly údajné změny dovolených a rodičovských, jiné informovaly příjemce o jeho propuštění a nabízely vyplacení dvouměsíčního platu po vyplnění přiloženého dokumentu. Vše hackeři dělali s cílem získat od obětí citlivé osobní informace. Útočníci zneužívají i komunikaci směrem k HR oddělení – zde můžeme zmínit případ, kdy ukradenou identitu zaměstnance zneužil útočník tak, že jeho jménem poslal HR oddělení zprávu s novým číslem účtu, kam mají nadále posílat výplatu. A než dotyčný podvod odhalil, připravil jej řádově o desítky tisíc korun.

Oblíbenou metodou je i tzv. CEO fraud, kdy podvodníci zjistí díky automatické odpovědi nepřítomnost člena managementu společnosti a jeho jménem pak vydají podvržený příkaz – například účtárně podniku pokyn k vyplacení určité částky.

**Zneužitelní chatboti**

Chatboti se stále více stávají standardním nástrojem zákaznických služeb pro mnoho společností. Jako každá technologie jsou však potenciálně zranitelní – hackeři totiž mohou snadno vytvořit roboty, kteří se budou vydávat za nákupčí nebo dodavatele a navázat konverzaci s interními pracovníky firem. V průběhu chatu může tento „podvodný bot“ přesvědčit zaměstnance, aby sdíleli citlivé údaje nebo se přihlásili k odběru neautorizovaného, škodlivého obsahu. Zabaveného chatbota lze použít také k phishingu.

„Chatboti jsou v zásadě zranitelní vůči stejným druhům útoků jako jakákoli jiná technologie. Pokud útočník získá přístup k síti, data, se kterými chatbot pracuje, mohou být ohrožena. Pokud mohu upravit data, mohu také nakrmit chatbota dezinformacemi. Nebo firmu vydírat na základě odcizených dat. Případně je možné přístup k získaným údajům rovnou zneužít a obeslat například databázi klientů nabídkou se škodlivým kódem,“ říká Michal Merta, ředitel Cyber Fusion centra společnosti Accenture.

**Nové riziko AI a pokročilé verze Chat GPT**

Zcela nová rizika s sebou nese překotný vývoj na poli ChatGPT. Ten umí být i velmi šikovným pomocníkem i hackerům a zlodějům. Umí naprogramovat i škodlivý kód, ale může ohrozit i zaměstnance, který se jej snaží nevědomky použít pro svou práci. Existují již případy, kdy zaměstnanec využívá ChatGPT k vyřešení interního úkolu a nevědomky tak poskytuje v rámci zadání úkolu citlivá firemní data, která se tím stala de facto veřejnými.

Podle serveru DigiTimes došlo díky tomuto nástroji například k úniku dat ze společnosti Samsung, Zaměstnanci totiž s ChatGPT sdíleli informace, které neměli. V jednom případě se zaměstnanec pokusil vyřešit problém se zdrojovým kódem tím, že jej do ChatGPT vložil a požádal umělou inteligenci o řešení, přičemž si neuvědomil, že kód se tak stal součástí interních tréninkových dat chatbota. Druhé pochybení se týkalo optimalizace vytvořeného kódu a ve třetím případě požádal zaměstnanec ChatGPT o vytvoření zápisu z jednání, ve kterém také samozřejmě bylo množství citlivých informací.

Firmy, které využívají chatboty, by měly mít přísné zabezpečení dat a důslednou informační bezpečnostní politiku, která se prolíná celou firemní kulturou. Zaměstnanci by měli být školeni v této oblasti a měli by se řídit bezpečnostními postupy. Tyto postupy by měly být pravidelně kontrolovány a aktualizovány, aby se minimalizovala rizika ztráty dat a úniků citlivých informací.

**Pozor ale i na fyzickou bezpečnost dat ve firmě**

Zaměstnanci mohou ohrozit bezpečnost firemních dat i nezodpovědným zacházením s fyzickými nosiči dat. Například, když data a interní informace bez ohledu na předpisy kopírují na nezabezpečená přenosná zařízení, a ta pak buď nechají ve firmě bez dalšího zabezpečení nebo dokonce vynášejí mimo prostory firmy. Firmy věnují stále větší důraz na zajištění IT bezpečnosti, ale některé z nich podceňují, že je stejně důležité mít perfektně zvládnutou také bezpečnost fyzickou.

„Na pracovištích je třeba vymezit prostory, které jsou strategické z hlediska zajištění bezpečnosti informací a zajistit je proti přístupu návštěvníků, vymezit pravomoci externích zaměstnanců a přesně určit, kam a za jakých podmínek mají přístup,“ říká Ondřej Mareček ze společnosti SSI Group. „Zajištění ostrahy objektů a bezpečnosti dat a systémů firem tak musí jít ruku v ruce a vzájemně se doplňovat.“