IBM Czech Republic News Room

IBM Report: Co se kyberkriminality týče, největší škody firmám působí nabourané uživatelské účty zaměstnanců

V 80 procentech analyzovaných případů došlo k únikům osobních informací; umělá inteligence (AI) a automatizace výrazně snižují náklady

Cambridge, 29. července 2020 – Společnost IBM oznámila výsledky celosvětové studie mapující finanční dopad úniků dat. Vyplývá z ní, že události tohoto druhu stojí napadenou firmu v průměru 3,86 milionu dolarů, tedy přes 86 milionů korun. Největší škody přitom způsobilo prolomení uživatelských účtů zaměstnanců. V 80 procentech případů došlo k úniku osobně identifikovatelných informací (PII), které jsou také druhem uniklých dat, ze kterých firmám vznikly největší škody. Studie je založená na hloubkové analýze případů, ke kterým došlo ve více než 500 organizacích po celém světě.

Protože zaměstnanci stále větší měrou přistupují k citlivým datům vzdáleně, ať už při práci z domova, nebo používáním cloudových uložišť a aplikací, soustředila se studie na finanční dopad úniků dat na firmy. Podle jiné studie IBM nebyla více než polovina zaměstnanců, kteří v důsledku pandemie pracovali z domova, poučena o bezpečném nakládání s PII zákazníků při využívání vzdáleného přístupu k nim. A to přesto, že se s přesunutím práce z kanceláří domů proměnila také bezpečnostní rizika.

Studie 2020 Cost of a Data Breach Report provedená výzkumníky z Ponemon Institute vychází ze zevrubného dotazování více než 3 200 profesionálů na poli bezpečnosti dat působících v organizacích, ve kterých došlo k únikům dat v období od srpna 2019 do dubna letošního roku. Více k metodologii lze nalézt ve studii samotné, přičemž její hlavní zjištění jsou tato:

- **Chytré technologie omezují škody na polovinu:** Firmy, které mají plně nasazeny automatizované bezpečnostní technologie, tedy využívají AI, analytiku a automatizovanou orchestraci dat, zaznamenaly méně než poloviční náklady na vypořádání následků úniku dat. Ty v průměru činily 2,45 milionu dolarů oproti průměrným 6,03 milionu v případě organizací bez těchto nástrojů.
- **Nejdražší je únik přihlašovacích dat**: V případech, kdy útočníci pronikli do firemních sítí pomocí zcizených přihlašovacích údajů, firmám vznikla v průměru o 1 milion dolarů vyšší škoda ve srovnání s celkovým průměrem, konkrétně 4,77 milionu průměrně. Zneužití zranitelnosti třetích stran byla druhá nejnákladnější příčina úniků dat s průměrnými náklady 4,5 milionu dolarů.
- **Obří průlom:** Studie také samostatně analyzovala největší incidenty tohoto druhu, které měly za následek únik milionu a více datových sad.
- **Škody letí nahoru**: Ztráta více než 50 milionů datových sad se firmám meziročně průměrně prodražila z 388 milionů na 392 milionů dolarů a úniky o objemu 40 až 50 milionů datových množin o 19 milionů na 364 milionů dolarů.
- **Útoky ze strany států jsou nejškodlivější**: Úniky dat, u kterých lze odůvodněně předpokládat zapojení národních států, způsobují největší škody. Vypořádat vládami provedené či iniciované útoky si vyžádalo náklady o průměrných 4,43 milionech dolarů, tedy více než úniky způsobené finančně motivovanými zločinci či hacktivisty.

„Co se schopnosti firem předcházet únikům dat týče, vidíme jasnou výhodu organizací, které investovaly do automatizovaných technologií," říká Wendi Whitmore, viceprezidentka IBM X-Force Threat Intelligence. „V době,

kdy firmy rozšiřují svoji prezenci v digitálním prostoru a zároveň přetrvává nedostatek talentů v oboru IT bezpečnosti, zaměstnanci a týmy již nemusí být s to zajistit bezpečnost stále dalších zařízení, systémů a dat. Automatizace těchto procesů jim v tomto ohledu může výrazně ulevit. Reakci na únik nejen urychlí, ale také zlevní.

Přihlašovací údaje zaměstnanců a špatně nakonfigurovaný cloud tvoří nejčastější zdroj problémů: Přihlašovací údaje ve špatných rukou byly nejčastějšími příčinami průniků do firemních systémů s podílem 40 procent. V roce 2019 z firem uniklo 8,5 miliardy datových sad, a to v pětině ze zkoumaných případů pomocí ukradených mailů a hesel. Firmy by proto měly přehodnotit svoje obranné strategie proti kyberzločincům ve smyslu přísnější autentifikace uživatelů a jejich práv v rámci svých systémů.

Stejně tak se firmy potýkají se složitostí bezpečnostních opatření, které tvoří největší část nákladů v případě prolomení jejich systémů. To pravděpodobně přispívá k okolnosti, že bezmála pětina zkoumaných úniků dat byla způsobena špatným nastavením cloudových uložišť a služeb. Takto způsobené škody se ukázaly být v průměru o více než půl milionu dolarů vyšší, se 4,41 miliony dolary jsou zdrojem úniku dat vedoucí k třetím nejvyšším škodám.

Útoky ze strany států mívají nejhorší dopad

Přestože způsobily pouhých 13 procent incidentů analyzovaných v rámci studie, jsou útoky s vládním pozadím nejškodlivější, zatímco finančně motivovaní útočníci (53 procent případů) výrazně nadprůměrné škody nezpůsobují. Vysoce promyšlené, dlouhodobě prováděné a dobře skryté útoky vládních organizací, navíc zpravidla na významnější cíle, často vedou k vážnějším důsledkům pro napadené a zvyšují tak způsobené škody na průměrné 4,43 miliony dolarů.

Respondenti ze Středního východu, kde podle žebříčku IBM 2020 X-Force Threat Intelligence Index dlouhodobě dochází k vyššímu počtu kyberútoků s vládním pozadím, zaznamenali meziroční nárůst škod s nimi spojených průměrně o 9 procent. Tyto náklady v průměrné výši 6,52 milionu dolarů byly druhé nejvyšší ze všech 17 zkoumaných regionů. Výrazný nárůst útoků, meziročně o 14 procent na průměrně 6,39 milionu dolarů, zaznamenala také energetika, jeden z nejčastěji napadaných sektorů hospodářství.

Pokročilé technologie se firmám vyplácí

Studie také odhaluje narůstající rozdíl ve výši způsobených škod mezi firmami, které investují do moderních bezpečnostních nástrojů, a těmi, které rizika vnímají méně naléhavě. V průměrném konečném účtu za napáchanou škodu obě skupiny již dělí 3,58 miliardy dolarů, které organizace s nejpokročilejším zabezpečením ušetřily. Tento rozdíl meziročně narostl o 2 miliardy dolarů, přičemž loňská studie oproti roku 2018 zaznamenala nárůst 1,55 milionu dolarů.

Firmy plně využívající automatizované bezpečnostní nástroje navíc těží z výrazně rychlejšího reakčního času na hrozby, což je faktor největší měrou určující konečné náklady úniku dat. Ze studie vyplývá, že AI, strojové učení, analytika a další formy automatizace bezpečnostních procesů firmám umožňují reagovat na průnik do jejich systémů o více než 27 procent rychleji než v případě organizací bez nejpokročilejšího zabezpečení. Posledně zmiňované potřebují průměrně o 74 dní více, aby útok rozpoznaly a překazily.

Celková připravenost organizace na útok určuje jeho následky i v dalším smyslu. Jak ukazuje studie, firmy bez specialistů na bezpečnost dat a ozkoušených postupů pro případ kyberútoku stojí ztráta dat v průměru 5,29 milionu dolarů. Zatímco společnosti, které ve svých řadách mají patřičné odborníky a testují bezpečnostní procesy, se v případě útoku potýkají s v průměru o 2 miliony nižšími škodami. Připravenost na tyto situace se tedy obrovsky vyplácí.

Mezi další zjištění letošní studie patří:

- **Špatně zabezpečená práce na dálku se nevyplácí** – Takzvaně hybridní modely práce v prostředích s nižší mírou zabezpečení s sebou nese rizika. Ze studie vyplývá, že 70 procent společností, které během pandemie přešly na práci z domova, očekává zvýšené riziko škod způsobených únikem dat.
- **Za problémy firmy viní specialisty na bezpečnost dat, přestože je nevybavily dostatečnými rozhodovacími pravomocemi**: 46 procent respondentů uvedlo, že za únik dat v konečném důsledku zodpovídají jejich vedoucí pro IT bezpečnost (CISO/CSO), přestože jen ve 27 procentech případů jsou tito pracovníci těmi, kdo mají skutečné pravomoci na tomto poli. Studie dále ukázala, že firmy, které mají obsazenu pozici odpovídající CISO, v případě úniku dat zaznamenaly v průměru o 145 tisíc dolarů nižší škody.
- **Většina firem pojištěných proti kyberzločinu využívá pojistné plnění pro náklady třetím stranám:** Zkoumané firmy s pojištěním proti úniku dat zaznamenaly průměrně o 200 tisíc dolarů nižší škody ve srovnání se společnostmi bez pojištění. 51 procent z nich přitom vyplacené pojištění použilo pro pokrytí nákladů na konzultační a právnické služby z třetích stran a 36 procent pro vypořádání se s oběťmi kyberútoku. Jen 10 procent dotázaných z nich zaplatilo vyděračům, kteří na ně nasadili ransomware a podobné nástroje.

Více informací najdete: zde.

Pro další informace kontaktujte:

IBM Česká republika
Vladislav Doktor
External Communications Manager
Tel.: + 420 733 149 624
E-mail: vladislav.doktor1@ibm.com

---

https://cz.newsroom.ibm.com/2020-07-29-IBM-Report-Co-se-kyberkriminality-tyce-nejvetsi-skody-firmam-pusobi-nabourane-uzivatelske-ucty-zamestnancu