Průzkum Mastercard: IT odborníci očekávají v příštím roce nárůst kyberútoků. Roste význam umělé inteligence

PRAHA, 10. října 2024 – IT experti českých firem se shodují, že riziko kybernetických útoků zůstává vysoké a nejspíš dále poroste. Přičítají to z velké části nástupu umělé inteligence, která hraje stále větší roli jak při kybernetických útocích, tak i v jejich obraně. Jak vyplývá z aktuálního průzkumu společnosti Mastercard ke kybernetické bezpečnosti v českých a slovenských firmách a organizacích, mezi další výzvy v oboru patří implementace směrnice NIS2 a kybernetická bezpečnost dodavatelských řetězců.

Umělá inteligence je heslem dne. Je jedním z nejdiskutovanějších aktuálních témat v nejrůznějších oborech a kyberbezpečnost není výjimkou. Tři z pěti firemních IT expertů se ale domnívají, že pomáhá spíše útočníkům než „obráncům“ a zvyšuje úspěšnost kyberútoků.

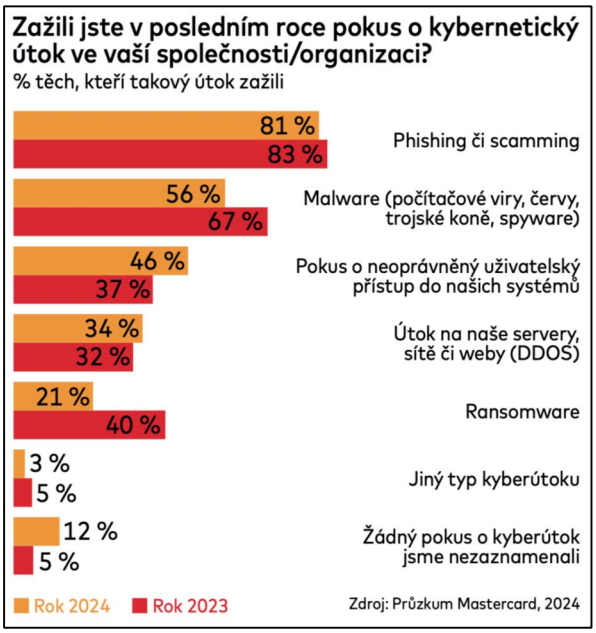
„Náš průzkum naznačil, že povědomí o tom, jak je možné využít potenciálu umělé inteligence v bezpečnosti firemních IT systémů, je stále poměrně nízké. Přitom právě tady se nabízejí nové možnosti, jak ochránit klíčová data firem i jejich zákazníků,” komentuje výsledky dotazování produktová ředitelka ve společnosti Mastercard pro Českou republiku a Slovensko Barbora Tyllová. Dodává, že AI pomáhá také například identifikovat podvodné transakce nebo dokáže rozpoznat neobvyklé vzorce chování a odhalit tak vytváření podvodných účtů.

Pro české a slovenské firmy a organizace mohou být přitom inovativní metody boje proti kyberútokům nezbytností. Přes 90 procent respondentů totiž v průzkumu uvedlo, že útoky jsou stále sofistikovanější. Dobrou zprávou naopak je, že význam kyberbezpečnosti si uvědomuje stále více firem. Zatímco loni bylo těch, pro které je kybernetická bezpečnost nejvyšší prioritou, 43 procent, letos je to již 58 procent.

Přesto v průzkumu 20 procent firem uvedlo, že nemají žádný formální plán nebo pokyny pro případ kybernetického incidentu. Formální akční plán, který popisuje, co dělat v případě útoků, může být přitom pro boj proti nim klíčový. Zatímco u firem, které ho měly pro takový případ vytvořený, se jich útoku neubránilo jen 14 procent, u těch, které ho neměly, to bylo už 24 procent. V průměru bylo úspěšných necelých 20 procent kyberútoků. To je v našich podmínkách poměrně vysoké číslo, které ukazuje, že následky útoku musela řešit každá pátá společnost v Česku nebo na Slovensku.

Největší nebezpečí? Lidská selhání

Nejčastějším typem kyberútoku byl loni phishing. Setkalo se s ním 8 z 10 podniků a organizací. To je zřejmě i důvod, proč jsou v oblasti kybernetické bezpečnosti hlavními tématy lidská selhání a edukace zaměstnanců. Naopak s ransomwarem se setkalo méně firem a organizací než loni, zde jsme zaznamenali pokles zhruba na polovinu. O něco nižší byla i evidence útoků prostřednictvím malwaru.



Nejčastější příčinou úspěšného kyberútoku je přitom podle 72 procent dotazovaných klikání na podezřelé odkazy nebo reakce na podezřelé zprávy. S tím úzce souvisí problematika krádeží digitální identity. Právě její ochrana může u důležitých lidí ve firmě předejít krádeži či zneužití dat.

Nové výzvy digitálního světa

Aby toho na správce firemních IT systémů nebylo málo, musejí se potýkat i s nárůstem administrativy, zejména v souvislosti s implementací směrnice NIS2. Ta se týká více než poloviny dotazovaných subjektů, ze kterých už tři čtvrtiny jsou na nová pravidla připraveny. Na druhé straně ale víc jak čtvrtina těch, které průzkum oslovil, zatím neví, jestli se jich bude týkat nebo o ní dokonce ještě vůbec neslyšeli. Směrnice je přitom již platná a firmy mají povinnost dodržovat stanovená pravidla.

Mezi oblasti, kterým se zatím česká a slovenská IT oddělení věnují poměrně málo, patří kybernetická bezpečnost v dodavatelském řetězci. Tato sféra je zatím poněkud podceňována. 61 procent společností a organizací se o kybernetickou bezpečnost svých dodavatelů příliš nezajímá.

Jen 19 procent jich ověřuje úroveň IT bezpečnosti u všech dodavatelů a 20 procent u svých klíčových dodavatelů. Zbytek se spoléhá na to, že jejich obchodní partneři mají bezpečnost dobře zajištěnou.

V rámci ověřovacího procesu se firmy a organizace nejčastěji spoléhají na dotazníky (52 procent), smlouvy (20 procent) nebo certifikaci ISO (10 procent). Pouze 15 procent jich má automatizovaný systém.

„Průzkum potvrdil, že nároky na kybernetickou bezpečnost neustále narůstají. Je pochopitelné, že pro část firem jde o velmi náročnou agendu, která by vyžadovala navýšení personálních stavů i financí pro jednotlivá IT oddělení. Jako logické řešení se ale v takových případech nabízí outsourcing," vysvětluje Barbora Tyllová.

Tisková zpráva

Pro další informace kontaktujte: Tomáš Jelen, mobil: +420 702 210 685, e-mail: tomas.jelen@bisonrose.cz

Příloha 1: *Proč zvolit řešení kybernetické bezpečnosti od Mastercard?*

Technologická společnost Mastercard dlouhodobě poskytuje nejbezpečnější platební transakce. S rychlým vývojem na poli finančních technologií se v posledních letech intenzivně zaměřuje i na komplexní zabezpečení všech dalších sfér podnikání. Díky desítkám akvizic a vlastnímu vývoji nástrojů pro kybernetickou ochranu je nyní Mastercard světovým lídrem v poskytování bezpečnostních řešení na míru firmám i státní správě.

- *Za posledních 5 let Mastercard investoval 7 miliard dolarů do kybernetické bezpečnosti a schopností umělé inteligence.*
- *Monitorujeme 19 milionů subjektů každých 10 dní, abychom zhodnotili míru jejich kybernetického ohrožení.*
- *V roce 2023 technologie Safety Net Mastercard zabránila potenciálním ztrátám klientů ve výši 20 miliard dolarů, které by způsobily pokusy o globální podvody a kybernetické útoky na síť Mastercard. Jedná se o rekordní částku v celé historii společnosti Mastercard.*
- *Zajišťujeme, aby více než 143 miliard transakcí v celosvětové síti bylo zpracováno rychle, bezpečně a spolehlivě.*

Příloha 2: Nástroje kybernetické bezpečnosti od Mastercard

ID Theft Protection dává koncovým uživatelům kontrolu nad jejich identitou. Nepřetržitá ochrana proti její krádeži monitoruje nejen veřejně dostupné weby, ale i tzv. deep web a dark web a vyhledává citlivé osobní údaje (emaily, čísla karet, údaje o bankovních účtech atd.). Pokud dojde k možné krádeži identity, uživatel je na nebezpečí okamžitě upozorněn.

RiskRecon umožňuje kontinuální a velmi podrobný audit kybernetické bezpečnosti kterékoli firmy. Odhaluje slabá místa v IT systémech, hodnotí rizika a dává doporučení, jaké ochranné prvky zavést, aby se zákazník co nejlépe ochránil. Zdrojem pro komplexní kybernetický audit je přitom pouhá přítomnost organizace na internetu, resp. její internetové stránky. Nástroj je určený (nejen) pro všechny společnosti působící v on-line prostředí s rozvinutým sub-dodavatelským řetězcem a v Česku ho využívají například některé nemocnice nebo pojišťovny.

NuDetect využívá pasivní biometrii pro ověřování transakcí. Jeho inteligentní algoritmus se dokáže naučit, jak konkrétní uživatel pracuje se svým telefonem nebo počítačem a na základě pohybů po obrazovce nebo úderů klávesnice rozpoznat, jestli se zařízením pracuje skutečně on. Díky zjištění odchylek od očekávaného chování uživatelů v reálném čase dokáže zamezit více než 99 procentům takových podvodů. Může fungovat buď jako náhrada nebo doplněk běžného biometrického ověření pomocí otisku prstu nebo skenu obličeje.

Ekata slouží k ověřování digitální identity pomocí umělé inteligence. Jednotlivým případům přiřazuje skóre důvěryhodnosti například podle toho, jestli osobní údaje nefigurovaly při nějakém podvodu v minulosti. Obchodníci na internetu nebo finanční instituce díky tomu dokážou rychle odhalit falešně vytvořené účty nebo neoprávněné čerpání bonusů. Nástroj využívají taky například zprostředkovatelé ubytování nebo loterijní společnosti.

Ethoca je nástroj, který již běžně využívají finanční instituce při online transakcích platební kartou. Dokáže efektivně a rychle řešit situace, kdy zákazník transakci reklamuje. Identifikuje falešné reklamace a bankám i obchodníkům tak šetří čas i peníze za celý proces vracení peněz. Snižuje vytíženost call center a zbytečné náklady na osobní řešení sporů. Vedle toho mají uživatelé a klienti bank lepší přehled o svých transakcích díky tomu, že Ethoca přiřazuje k jednotlivým nákupům detailní informace jako jméno a logo obchodníka nebo lokalitu nákupu.