**Kyberútoky: Firmám se do ochrany nechce investovat. Česko je hlavním evropským cílem**

**PRAHA, 24. ŘÍJNA 2024 – Počet digitálních útoků v Česku roste. Tuzemské společnosti patří k nejčastějším cílům v Evropě. Hackeři nejčastěji cílí na oblasti školství, zdravotnictví nebo vládní a vojenský sektor. Kyberútokům čelí ale čím dál častěji i jednotlivci.**

Z pohledu kyberbezpečnosti patří Česká republika k nejméně bezpečným zemím v Evropě. Navíc počet kybernetických útoků v zemi dramaticky stoupá, meziročně se jejich počet zvýšil o více než 30 procent. Podle dat americko-izraelské IT skupiny Check Point Software Technologies je evropský průměr kyberútoků 1367 týdně na jednu společnost, ty české ale čelí týdně více než dvěma tisícům. „Hlavním cílem kybernetických útoků je získat citlivá data, finanční prostředky nebo narušit provoz organizací. Kyberútoky směřují především na firmy, státní instituce a finanční sektor, stále častějšími terči jsou ale i malé a střední podniky. Přibývá také útoků na jednotlivce, zejména prostřednictvím e-mailu nebo sociálních sítí. Podle dostupných dat byla někdy napadena počítačovým virem více než polovina Čechů, kolem 20 procent těchto obětí přišlo při útoku o finanční prostředky,“ uvedla Denisa Janatová, ředitelka společnosti smitio. Její slova potvrzuje i Tomáš Holomek ze společnosti CDC Data, která se zaměřuje na kybernetickou bezpečnost. „Útoků každoročně přibývá. Zároveň se rozšiřuje seznam cílů, kdy jsou pro útočníky zajímavé už i menší organizace nebo jednotlivci. Předpokládat, že na vás nikdo nezaútočí, protože nejste dostatečně perspektivním cílem, se již delší dobu nevyplácí,“ upozornil.

Nárůstu počtu kybernetických útoků napomohla pandemie, kdy spousta společností, organizací, ale i jednotlivců začala fungovat převážně v online prostředí. „Nárůst kybertické kriminality je způsoben několika faktory, včetně rostoucí digitalizace, většího množství propojených zařízení, zvyšující se závislosti na cloudových službách a technologiích a také stále sofistikovanějšími metodami útočníků. Pandemie covidu-19 navíc urychlila digitalizaci a přechod k práci na dálku, což vedlo ke zvýšení zranitelnosti firemních sítí a osobních zařízení, a tím i k nárůstu útoků. Hackeři také stále častěji využívají nové techniky, jako jsou ransomware útoky nebo phishing,“ popsala Vladimíra Tesková z TeskaLabs, která vyvíjí pokročilé softwarové produkty pro kybernetickou bezpečnost.

Forma útoků se liší podle cíle. Nejčastějšími typy útoků jsou podle odborníků phishing, ransomware a Distributed Denial of Service (DDoS) útoky. „Phishingové útoky míří na lidskou chybu, hackeři se jejich prostřednictvím pokouší ukrást vaše peníze nebo vaši identitu tak, že vás přimějí odhalit osobní údaje – například čísla kreditních karet, bankovní údaje nebo hesla. Právě tento typ útoků nejčastěji cílí na jednotlivce například v podobě e-mailu. Alarmující je, že přes 40 procent Čechů uvádí, že někdy otevřeli podezřelý e-mail, i když věděli, že se může jednat o hrozbu. Ransomware blokuje například prostřednictvím stažené aplikace přístup k systémům a požaduje výkupné, takový útok může mít výrazný dopad na fungování celé firmy. DDoS je forma kybernetického útoku, při kterém se útočníci snaží narušit nebo poškodit webovou stránku, síť nebo jinou online službu tím, že ji přetíží velkým množstvím falešných nebo nevyžádaných požadavků. Takové útoky pak velmi často cílí na poskytovatele veřejných služeb,“ popsala Denisa Janatová.

Takzvané spamy ohrožují data v počítači nejčastěji – někdy jsou snadno rozpoznatelné, jindy se ale tváří jako věrohodná e-mailová zpráva od poskytovatele služeb. „Ke každé zprávě od neznámého odesílatele je třeba přistupovat opatrně, zkontrolovat e-mail, ze kterého byla zpráva odeslána, to bývá první indicií, že nezní jako obvyklé formální adresy. Sdělení bývá naléhavé, nutí adresáta, aby rozklikl přílohu nebo odkaz, to je další indicie. Pokud se navíc jedná o služby, které v posledních dnech adresát nijak nepoptával, nabídku peněz, zázračného produktu nebo naopak výzvu k zaplacení dluhu či zadání osobních údajů, je vhodné zprávu ihned označit jako nevyžádanou a smazat,“ popsal Martin Vodička, ředitel Soukromé střední školy výpočetní techniky.

Hlavním cílem útočníků je finanční profit, jedním vydařeným kybernetickým útokem mohou vydělat miliony. „Útočník je buď cíleně zaplacen další osobou, nebo předpokládá zisk po úspěšném provedení ransomwarového útoku, a tedy následném vyplacení výkupného. I v dnešní době je bohužel poměrně časté, že infrastruktura obětí není v takovém stavu, aby dokázala útokům odolat. Oběť má pak dvě možnosti – srovnat se se ztrátou dat, nebo zaplatit výkupné. První možnost bývá často likvidační, na to útočníci spoléhají, proto počítají se ziskem. Časté jsou i pokusy o prodej ukradených citlivých dat,“ uvedl Tomáš Holomek.

Přestože je Česká republika jedním z hlavních evropských cílů kybernetických útoků, dosahuje v oblasti kybernetické bezpečnosti solidních výsledků. „Přibližně 70 až 80 procent kybernetických útoků je dnes úspěšně odraženo díky moderním bezpečnostním technologiím, jako jsou firewally, antiviry a systémy detekce narušení. Útoky se ale vyvíjejí, a proto je důležité neustále aktualizovat technologie a postupy. Průměrné náklady pro firmy po úspěšném kybernetickém útoku se mohou pohybovat od statisíců až po miliony korun, v závislosti na rozsahu škod. Náklady zahrnují nejen přímé ztráty, ale i obnovu systémů, ztrátu důvěry zákazníků a pokuty spojené s porušením pravidel o ochraně dat,“ vyjmenovala Denisa Janatová.

Jedním z důvodů, proč je Česko terčem množství kybernetických útoků, je fakt, že kybernetická bezpečnost českých společností je silně podfinancovaná. Podle letošního průzkumu agentury Ipsos více než polovina oslovených společností investuje do zabezpečení firemních sítí a koncových bodů částku do 100 tisíc korun ročně. „Klíčové technologie pro kybernetickou bezpečnost dnes zahrnují Zero Trust Architecture, která vyžaduje neustálé ověřování uživatelů a zařízení, a automatizaci s umělou inteligencí, která umožňuje rychlou detekci a reakci na hrozby. Ochrana cloudových služeb je důležitá kvůli přesunu dat do cloudu, roste i význam kybernetické odolnosti, tedy schopnosti rychle se zotavit z útoků. Taková opatření s sebou ale samozřejmě nesou určité finanční náklady, které rozhodně nejsou v řádech desítek tisíc korun,“ uvedla Vladimíra Tesková.

Problémem nejsou pouze finance, které se zatím firmám do ochrany jejich dat nechtějí investovat. Česku chybějí i odborníci, kteří s potřebnými technologiemi umí pracovat. „Česko, stejně jako mnoho jiných zemí, čelí nedostatku kvalifikovaných odborníků na kybernetickou bezpečnost. Tento problém je jedním z hlavních důvodů, proč je nutné investovat do vzdělávání a tréninku specialistů. Hlavní trendy v oblasti kybernetické bezpečnosti zahrnují rostoucí využití umělé inteligence a strojového učení pro detekci hrozeb, rozvoj Zero Trust modelů a posílení cloudových bezpečnostních technologií. To logicky vyžaduje i nárůst odborníků, kteří budou umět tyto systémy do firem zavádět,“ uzavřela Denisa Janatová.

**KONTAKT PRO MÉDIA:**

**Mgr. Petra Ďurčíková\_mediální konzultant**

****

**+420 733 643 825,** **petra@pearmedia.cz**

[**pearmedia.cz**](http://www.pearmedia.cz)

**SMITIO,** [**smitio.com/cs**](https://smitio.com/cs)

Na začátku bylo smitio kariérní platformou pro IT komunitu, která klade důraz na transparentnost a otevřenou komunikaci. V rychle se měnícím a dynamickém trhu se smitio neustále rozvíjelo a přizpůsobovalo se novým potřebám a trendům. Postupně rostlo a reagovalo na výzvy trhu, až dosáhlo své současné podoby jako komplexní služby pro nábor, včetně recruitmentu.

Smitio vychází ze zkušeností a potřeb IT komunity a spojuje je s projektovými týmy. Jeho vývoj je důkazem toho, jak se dokáže adaptovat a inovovat v souladu s potřebami a dynamikou trhu. Smitio je nejen prostředkem pro efektivní nábor IT specialistů, ale také platformou, která posiluje propojení a spolupráci mezi jednotlivci a týmy v oblasti IT.