■ Kyberbezpečnost

Firmy se bojí, že hackery pustí do systémů jejich vlastní zaměstnanci

Adam Mašek
adam.masek@hn.cz

Povědomí o kybernetické bezpečnosti ve svých podnicích hodnotí více než čtvrtina malých a středních firem jako nízké. To je problém, protože pak se pravděpodobnost úspěšného kyberútoku výrazně zvyšuje. Obzvláště v situaci, kdy více než polovina z těchto společností vnímá největší riziko právě v tom, že jeden z jejich pracovníků kvůli své nepozornosti pustí hackery do interních systémů firmy. Základní prevence proti kyberzločinu přitom není zas tak složitá.

Zmíněná čísla vyplývají z průzkumu výzkumné agentury Ipsos zpracovaného pro Asociaci malých a středních podniků a živnostníků ČR a její partnery. Data dále ukazují, že jako vůbec největší hrozbu firmy vnímají phishingové útoky. Tedy například e-maily odkazující na podvržené stránky internetových bankovnictví, které mají za cíl vylákat ze zaměstnanců přístupové údaje k firemním kontům. Anebo viry typu ransomware, malware či trojský kůň, jež dokážou z firemních počítačů dostat citlivá data, uzamknout je a přístup k nim poskytnout pouze výměnou za peníze.

„Z průzkumu víme, že kyberbezpečnost je pro malé a střední podniky veliké téma. Takřka třetina z dotázaných uvedla, že se s nějakým typem kyberútoku už setkala," říká Petr Šmíd, marketingový ředitel Googlu pro Česko, Slovensko, Maďarsko a Rumunsko.

Více než třetina firem pak mezi největší hrozby zařadila slabá hesla a 28 procent podniků uvedlo jako primární riziko nedostatečnou edukaci zaměstnanců. Právě ta je podle expertů největším problémem v zabezpečení malých a středních firem. „Kromě komplexní ochrany (například antiviru a dalších bezpečnostních softwarů) by mělo být prioritou také vzdělávání zaměstnanců v oblasti kyberbezpečnosti – poměrná část útoků cílí hlavně na chybu lidského faktoru," říká Jiří Homola, manažer vývoje byznysu ve Vodafonu.

Kvalitním proškolením zaměstnanců lze podle něj navýšit obranu proti kybernetickým hrozbám. Právě takové vstupní školení, které dá podnikatelům základní přehled, jak se před hrozbami bránit, nabízí Google v rámci školení, které prezentovalo na konferenci AMSP na téma digitalizace a kybernetická bezpečnost. HN vám z přednášky přinášejí několik základních tipů a rad.

~

Experti radí, aby si pracovníci pozorně hlídali překlepy a chyby ve formátování e-mailů, které jsou znakem podvodu. A také, z jaké adresy mail přichází – zdali sedí s běžným formátem, který firma používá.

Vytvářejte silná hesla

Úplně ideální je vytvářet hesla pro každý účet zvlášť. Vyloučí se tím situace, kdy dojde k prolomení hesla, díky němuž se útočník může dostat prakticky všude. To je ovšem náročné, protože v řadě firem se musí její zaměstnanci hlásit hned k několika službám najednou. Odborníci proto doporučují nainstalovat si jednu z aplikací pro správu hesel. Na výběr jich je celá řada, kromě Google Password Manageru, který spravuje hesla v internetovém prohlížeči Chrome, jsou velmi oblíbené NordPass, RoboForm či KeePass. První dvě jmenované jsou placené, například prémiová verze NordPassu ale stojí v přepočtu přibližně 42 korun za měsíc, RoboForm je ještě levnější a například KeePass je pak zcela zdarma.

„U hesel se obecně vyplácí dodržovat základní pravidlo, kdy by každé mělo obsahovat alespoň jedno velké a malé písmeno, číslici a speciální znak, například hvězdičku či křížek," říká Filip Holec, certifikovaný školitel Googlu a spoluzakladatel vzdělávací platformy v oblasti kyberbezpečnosti Engeto.

Základem je aktualizovaný software

Ve firmách by také neměli zaměstnanci nikdy používat aplikace a softwary, které jsou zastaralé a nenabízejí bezpečné verze. Jinými slovy – pokud používaný software daná společnost, která jej provozuje, nadále neaktualizuje a nevydává její vylepšené verze, je pro hackery takový software vstupní branou do interních systémů firem. Jako prevence mohou sloužit na trhu dostupné platformy pro správu firemního hardwaru, který se zaměstnancům nedovolí přihlásit, pokud není systém aktualizovaný. Současně platí, že staré a nepoužívané aplikace by měli uživatelé průběžně mazat.

Pozor na podezřelé e-maily

Jeden z nejčastějších způsobů, jak se hackeři nabourávají do firemních systémů, je prostřednictvím podvržených e-mailů. Útočníci malwary a ransomwary schovávají například do příloh e-mailů, které budí dojem, že se v nich skrývají firemní dokumenty. Časté také je, že se kyberútočníci snaží zmocnit bankovních údajů k firemním účtům, a to prostřednictvím zaslání falešných faktur. V těle e-mailu se většinou nachází odkaz, který vede na podvržené platební brány. Když pracovník či pracovnice v účtárně platbu zadá, peníze jsou nenávratně pryč.

Text samotného e-mailu je pak psán tak, aby vyvolal dojem, že příkaz k platbě zadává například finanční ředitel dané společnosti – pomocí umělé inteligence útočníci dokážou napodobit styl jeho psaní a do e-mailu vkládají i hlavičku s podpisem. Kyberzločinci v tomto případě sází primárně na nepozornost zaměstnanců. Experti radí, aby si pracovníci pozorně hlídali překlepy a chyby ve formátování e-mailů, které jsou znakem podvodu. A také, z jaké adresy e-mail přichází – zdali sedí s běžným formátem, který daná firma používá nejběžněji: jmeno.prijmeni@nazevfirmy.cz a podobně. „Pakliže adresa obsahuje znaky, číslice nebo slova navíc, jedná se většinou o podvod," říká Holec. „Červenou vlaječkou" také je, když u e-mailu chybí fotka, přestože ji pracovník dříve u účtu měl.

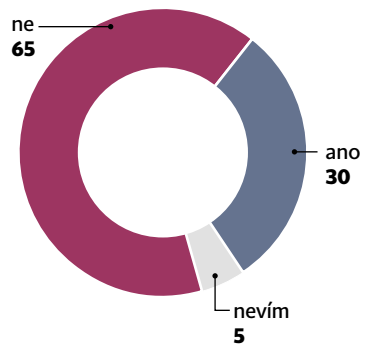
Zaměstnance průběžně školte

Vzhledem k tomu, že nejsnazší cesta do IT „střev" společnosti vede přes nepozorné pracovníky, je jejich průběžné vzdělávání a školení klíčové. Bezplatný on-line kurz s názvem „Dávej kyber!", který absolventy učí základům bezpečného pohybu v kyberprostoru, nabízí Národní úřad pro kybernetickou a informační bezpečnost. Kurz má osm okruhů, na konci účastníci procházejí testem a při jeho splnění získají certifikát.

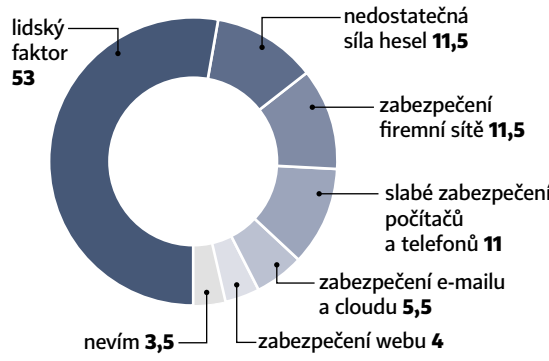
Svou nabídku profesních certifikátů o oblast kybernetické bezpečnosti nedávno rozšířil i Google. Ty slouží primárně k rozvinutí dovedností, které účastníkům posléze pomohou s uplatnění přímo v oboru kyberbezpečnosti, který se dlouhodobě potýká s nedostatkem kvalifikované pracovní síly. V Česku bude moci až 500 uchazečů získat stipendium prostřednictvím neziskové organizace Czechitas, jež se zaměřuje na IT vzdělávání.

Čeho se obávají malé a střední podniky v souvislosti s kyberbezpečností?

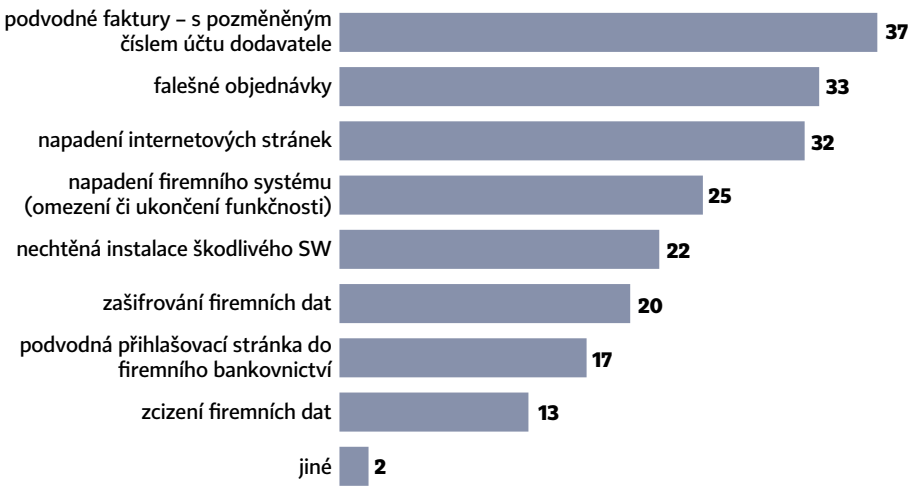
Kolik firem se setkalo s kyberútokem?
(v procentech)



Největší rizika z hlediska zabezpečení firem
(v procentech)

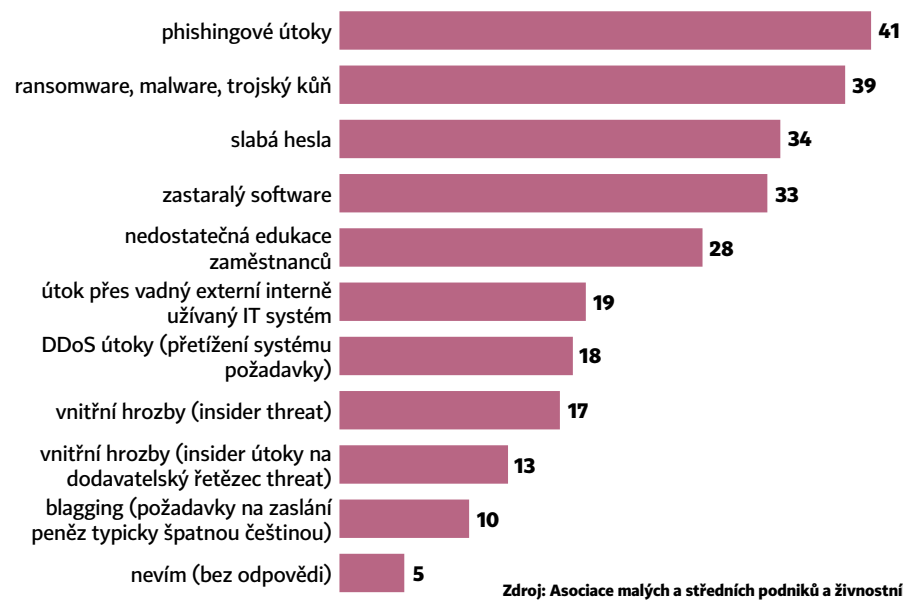


Konkrétní typy kyberútoků, se kterými se firmy setkaly
(v procentech)



Poznámka: Pouze dotazovaní, kteří uvedli, že se někdy setkali s kyberútokem na jejich firmu.

Největší hrozby pro kybernetickou bezpečnost firem
(v procentech)



Zdroj: Asociace malých a středních podniků a živnostníků ČR