Brno 20. 2023

**Napadení virem v důsledku phishingu přiznává 58 % zaměstnanců. Často selhává lidský faktor**

**S rostoucím využíváním digitálních platforem roste i hrozba podvodů a podvodného jednání na internetu. Mezi nejrozšířenější formy kybernetických útoků patří stále phishing – metoda, při které se zločinci snaží vylákat citlivé informace, jako jsou hesla, čísla kreditních karet nebo osobní údaje. Riziko ale často vzniká i zaměstnavateli.**

Phishingové útoky jsou v posledních letech stále sofistikovanější a podvodníci používají nejrůznější taktiky, aby nalákali oběti do svých pastí. Mezi nejběžnější cesty patří e-maily nebo zprávy na sociálních sítích. Dalšími variantami tohoto typu útoku mohou být podvodné SMS (smishing) nebo hovory (vishing).

**V ohrožení jak osobní data, tak firemní**

Podle velkého výzkumu vypracovaného pro společnost Seyfor se mezi dotazovanými zaměstnanci různých firem, kteří aktivně využívají v práci informační technologie,[[1]](#footnote-2) v loňském roce každý druhý setkal v práci s nějakou bezpečnostní hrozbou. 58 % dotazovaných uvedlo, že se jednalo o napadení škodlivým softwarem (malware) v důsledku phishingu. Ve čtvrtině případů šlo o cílený hackerský útok, v dalších 26 % o připojení zavirovaného zařízení.

Uvedené typy útoků představují nebezpečí jak pro data zaměstnavatele, tak pro soukromé informace zaměstnanců. V současnosti práci z domova využívá v Česku téměř každý třetí zaměstnanec. Zaměstnanci využívají připojení mimo firemní síť také na služebních cestách. A lidé využívají nezřídka pouze jedno zařízení.

*„Dnes už je běžnou praxí, že pokud není používání firemních zařízení pro soukromé účely přímo povoleno, bývá v organizacích často tolerováno. Zaměstnanci tak mohou firemní zařízení použít například pro přístup k soukromému e-mailu, zpracování soukromých dokumentů či pro přístup k sociálním sítím,“* říká odborník na bezpečnost ze společnosti Seyfor Milan Ryšavý a dodává: *„Je nutné řešit zabezpečení přímo na úrovni koncových zařízení, aby byla zajištěna adekvátní úroveň ochrany i mimo podnikovou síť (např. při práci z domova a na cestách).“*

**Každý čtvrtý zaměstnanec způsobil IT bezpečnostní incident. Stačí jednoduchá pravidla**

Z průzkumu také vyplynulo, že čtvrtina respondentů už někdy v zaměstnání způsobila IT bezpečnostní incident. *„Otevřít podezřelou přílohu může omylem i zkušený uživatel. I když se technické možnosti zabezpečení zlepšují, své praktiky vylepšují také útočníci,“* uvádí Ryšavý a doplňuje: *„Je zřejmé, že nestačí použít pouze bezpečnostní technologie, ale je nutné zaměřit se i na vzdělávání uživatelů, aby věděli, co je bezpečné chování v kyberprostoru.“* Konsekvence vůči vzniklým problémům by měly být podle něho přizpůsobené konkrétní společnosti a povaze její práce.

Jiná pravidla a interní zvyklosti platí u technologických start-upů, jiné v silně regulovaném prostředí, jakým je vojenské zpravodajství. Je vhodné interním předpisem jasně definovat, za jakých podmínek a jakým způsobem je možné firemní zařízení používat
k soukromým ​​účelům. *„V praxi bývá častá situace, že interní předpis toto využití zakazuje, ale používání pro soukromé ​​použití je tiše tolerováno. V tomto režimu je těžké vymáhat zodpovědnost za případné škody, které vyplynuly z porušení pravidel,“* říká Ryšavý.

**Jak správně uchopit bezpečnost?**

Zabezpečení je potřeba řešit na úrovni každého koncového zařízení zvlášť, protože ochrana v rámci firemní sítě už nebývá dostatečná (zaměstnanci s koncovými zařízeními cestují, pracují z domova apod.). Základem je moderní a průběžně aktualizovaný antimalware nástroj s centrální správou. Přidat například správně zabezpečený a pravidelně aktualizovaný operační systém, a to i pro aplikace. A zajištění vícefaktorové autentizace (kombinace hesla a nějaké další informace často v podobě biometriky, jako je otisk prstu či rozeznání obličeje) pro přístup k aplikacím a datům. Za nástavbu, ale důležitou funkcionalitu potom můžeme považovat oddělení firemních dat a dokumentů od těch soukromých, čímž lze zajistit vyšší úroveň ochrany pro citlivá firemní data.

**O společnosti Seyfor**

Seyfor se řadí k velkým evropským dodavatelům ICT řešení. Společnost má přes 1 600 zaměstnanců v osmi zemích a celosvětově obsluhuje zákazníky ve 38 státech. Dlouhodobě patří k nejrychleji rostoucím IT společnostem v regionu. Je největším výrobcem účetních, ERP a mzdových a personálních systémů v České republice, v roce 2022 přesáhly konsolidované výnosy 3 miliardy korun. Společnost uskutečnila v posledních letech desítky významných akvizic IT firem v České i Slovenské republice a také na Balkáně. Ovládajícími vlastníky společnosti jsou slovenská private equity společnost Sandberg Capital a Martin Cígler. Firma byla založena v roce 1990 jako Cígler Software, v letech 2017–2022 působila pod značkou Solitea.

**Kontakt pro média:** Havas PR Prague**,** Petr Kubíček, petr.kubicek@havaspr.com**,** +420 602 388 970

1. Zdroj dat: Agentura MNFORCE, 1 000 respondentů 18–60 let, kteří používají v práci informační technologie. Reprezentativní vzorek české populace dle pohlaví, věku a krajů. Dotazování probíhalo 8.–15. 11. 2022. [↑](#footnote-ref-2)