**Hackeři zvyšují aktivitu. Mezi jejich nové triky patří zlodějské nabíječky, vysoce propracované falešné e-maily i sociální inženýrství. Nahrává jim nezodpovědnost, zbrklost či naivita**

**Praha, 10. září 2021 – Vynalézavost hackerů byla vždy velká, ale poslední dobou se ještě stupňuje. Jejich útoky jsou stále propracovanější a intenzita se zvyšuje. Stále více tak ohrožují zaměstnance, firmy, i běžné lidi. Neopatrnost lidí přináší útočníkům velké výhody. Statistiky firem a institucí zaměřených na bezpečnost i Policie ČR potvrzují, že meziročně přibylo rizik až čtyřnásobně.**

**Velké cíle – firmy a nemocnice**

„Máme vaše data. Pokud nezaplatíte, přijdete ok ně.“ Tak často začínají vyděračské, takzvané ransomwarové útoky. Hackeři mohou zašifrovat data v soukromém počítači, tedy fotografie a další soubory, ale podobné útoky se týkají i firemních dat nebo třeba nemocnic. Pak letí rizika a škody raketově nahoru.

„Ransomware útok si dnes lze objednat na míru, třeba jako součást nekalého konkurenčního boje. I to přispělo k boomu této kriminality,“ říká Michal Merta, odborník na bezpečnost a ředitel Cyber Fusion Centra v Accenture ČR. A mnoho lidí situaci hackerům navíc ulehčuje. Téměř čtvrtina zaměstnanců například podle průzkumu připouští, že často odkládá a zdržuje aktualizace softwaru na svých pracovních počítačích a dalších zařízeních,“ dodává.

**Pozor na podvržené žádosti o platbu**

Útoky, které ještě nedávno byly neumělé a snadno odhalitelné, již dnes mají vysokou míru profesionality. Hackeři si často dají práci pomocí sociálního inženýrství zjistit mnoho osobních údajů o člověku, a pak zaútočí. „Jednu naši klientku kontaktovala přes Facebook ‚příbuzná‘ a požádala ji o pomoc. Chtěla ofotit platební kartu a následně posílat autorizační kódy transakcí. Údajně se účastnila důležité hry. Klientce až později došlo, že jde o podvod a obrátila se na Policii,“ zmiňuje konkrétní případ Viktor Houška z BNP Paribas Cardif, která mimo jiné poskytuje i pojištění takovýchto hrozeb plynoucích z kyberprostoru.

**Podvodné e-maily nejen od kurýrních služeb ale i videoték**

Dalším příkladem věrohodně vypadajících podvržených emailů je příběh člověka, který obdržel emailovou zprávu, která se tvářila jako od přepravce s tím, že má zaplatit za služby. Vzhledem k tomu, že se jednalo velmi věrohodnou formu komunikace, poslal peníze a až poté zjistil, že e-mail byl podvodný.

„Tyto případy se opakovaly a k části lidí informace o těchto rizicích dorazily. Hackeři ale stále hledají nové možnosti a zkouší využít dalších, na první pohled seriózních a známých, služeb. Nejen služeb pošty a kurýrních společností, finančních institucí, ale nově také například online videoték,“ upozorňuje Ondřej Ševeček z Počítačové školy GOPAS.

**Pozor na nový kanál, zprávy na WhatsApp a evegreen: výhry v loterii či soutěži**

V dalším případě klient při nákupu na internetu zaplatil převodem za objednané zboží z druhé ruky. Zásilka nedorazila, a prodávající přestal komunikovat. Jiným novým trikem internetových podvodníků jsou v poslední době zprávy zasílané přes WhatsApp, jimiž požadují pod různými záminkami uhrazení malé částky. Tyto podvody mají několik různých podob. I zde pak bohužel funguje naivní nadšení příjemců zpráv, kteří se chytnou na podvržené informace s tématem výhry v loterii či soutěži, které se nezúčastnili.

**Zlodějské nabíječky**

Ještě před časem by nás nenapadlo, že nám data z telefonu může někdo odcizit pomocí podstrčeného nabíjecího kabelu. Díky dramatickému zlevnění k tomu potřebných technologií můžeme nyní sledovat kauzy úniku informací způsobené například kabelem O.MG Lightning, tak dokonalou replikou originálního kabelu od Applu, že nemáte šanci poznat rozdíl. Pokud si jej ke svému zařízení připojíte, otevřete hackerovi cestu do vašeho mobilu a dobíjení zdarma tak může skončit vysátím vašeho účtu.

**Nepodceňovat školení a osvětu**

Firmy ani jednotlivci by neměli zanedbávat ani osvětu a bezpečnostní školení. „Pokud člověk má solidní povědomí o základních pravidlech online bezpečnosti, a navíc sleduje aktuální informace o nových hrozbách, pak může sám identifikovat naprostou většinu podvržených e-mailů a při sebemenším podezření si před otevřením neváhá ověřit jeho pravost,“ říká Ondřej Ševeček z Počítačové školy GOPAS.