**Výsledky průzkumů ČBA, ESET a SC&C:**

**Většina Čechů o kyberhrozbách ví, nedokáže je ale odhalit**

**Uživatelé v České republice si nebezpečí na internetu začínají uvědomovat, dvě třetiny ale nepoznají pokus o podvod.**

**Praha, 8. prosince 2020 – Index Kyberbezpečnosti, který každoročně sestavuje Česká bankovní asociace (ČBA), dosáhl v letošním roce opět průměrných výsledků, celkem 61 %. Češi stále nečtou informační zprávy od bank a nevěnují pozornost upozorněním svého mobilního telefonu, polovina navíc neřeší ani jeho zabezpečení, vyplývá z průzkumu ČBA. Jak však ukázal Kybertest uskutečněný v listopadu ve spolupráci ČBA, ESET a agentury SC&C, realita v oblasti kyberbezpečnosti je ještě horší. Češi v testu, který simuloval rizikové situace a hrozby, dosáhli pouze 43% úspěšnosti. Zkušenost s pokusem o kyberútok přitom v průzkumu ČBA deklaruje více než polovina Čechů**

Index Kyberbezpečnosti se v letošním roce vrátil na 61 %, což je průměrný výsledek. Necelá třetina Čechů získala dokonce méně něž 50 bodů. Problém zůstává v tom, že Češi stále nečtou informační zprávy zasílané bankami, často je jen odkliknou; nevěnují pozornost bezpečnostním upozorněním svého telefonu, a polovina neřeší ani jeho zabezpečení. Každý desátý je navíc ochoten připojit se ke svému internetovému bankovnictví přes jakoukoli Wi-Fi síť, aniž by zjišťoval, zda je připojení bezpečné. Na druhou stranu při tvorbě hesel jsou ale Češi oproti loňsku obezřetnější.

„*Vzhledem ke stagnujícímu Indexu Kyberbezpečnosti jsme se ve spolupráci se společností ESET a agenturou SC&C rozhodli prověřit znalosti Čechů v praxi. Připravili jsme modelovou situaci, v níž se respondenti stali klienty fiktivní Rodinné banky a zároveň řešili některé z běžných činností v online prostoru. Šlo nám o to zjistit, zda lidé poznají podezřelé prvky, které v kyberprostoru mohou naznačovat, že se jedná o práci podvodníků. V reálném světě by totiž v takovém případě mohli přijít o svá data, peníze či kontrolu nad svým zařízením,*“ říká Helena Brychová, gestorka finančního vzdělávání ČBA, ke Kybertestu.

Češi v Kybertestu uspěli pouze na 43 %, což je vzhledem k jejich deklaracím v průzkumu asociace alarmující výsledek. Navíc pouhé 1 % Čechů dosáhlo v testu výsledku nad 81 %. Úspěšnost se odvíjí od věku i vzdělání – mladí a vzdělaní lidé dosahují o něco lepších výsledků (54 % a 51 %), naopak lidé se základním vzděláním dosáhli 37 %.

**Počet hackerských útoků stále roste, pandemie tomu napomohla**

Situace je o to horší, že počty kyberútoků stále rostou a nějakou zkušenost s nimi má podle průzkumu asociace více než polovina Čechů. Svoji roli v tom sehrála i stávající omezení a přesun velké části aktivit do online prostoru, neboť v 9 % případů šlo o situace, které se odehrály v letošním roce během první vlny koronavirové pandemie*.* Tento trend zároveň potvrzují i statistiky společnosti ESET, podle kterých počet phishingových útoků, oproti minulému roku vzrostl o 100 %. Mnoho z nich se přitom vydává za zprávy a výzvy bank.

„*I v rámci Kybertestu jsme simulovali e-mailovou komunikaci, ve které respondenti obdrželi e-mail od Rodinné banky s výzvou o aktualizaci údajů na přiloženém odkazu. V e-mailu byly celkem tři podezřelé prvky, které mohly naznačovat, že se jedná o podvod. Jednalo se typicky o podvrženou e-mailovou adresu odesílatele, kterou odhalilo jen 57 % respondentů, dále pak podvržený odkaz v těle e-mailu, který odhalilo více než tři čtvrtiny dotázaných a apel na čas, který za podezřelý označilo pouze 34 % respondentů,“* komentuje výsledky Pavel Matějíček, manažer technické podpory společnosti ESET. Podle něj se přes 90 % různých trojských koní šíří právě prostřednictvím e-mailu.

Podle průzkumu asociace byly nejčastějším cílem útoků počítače a notebooky (84 %). „*V tomto zjištění se jistě odráží* *mohutný rozvoj digitálních služeb a současný překotný přechod do online světa. Podstatné ale je, že rapidně stoupá i počet aktivit, k nimž dnes využíváme své mobilní telefony, a přesně tam budou další útoky hackerů směřovat,*“ odhaduje Helena Brychová z ČBA, a odkazuje se přitom na výsledky průzkumu, který nárůst počtu útoků na mobilní telefon ukázal již nyní (z loňských 11 % na letošních 17 %). „*Naštěstí se v drtivé většině jedná jen o pokus, který není úspěšný. Obecně jsou podle respondentů kyberútoky vedeny prostřednictvím podvodných e-mailů a zacíleny jsou na získání osobních dat, anebo přímo finančních prostředků,*“ upřesňuje výsledky Jana Hamanová, ředitelka výzkumné agentury SC&C.

V poslední době se rozmáhají podvody formou tzv. hlasového phishingu označovaného jako vishing. Obdobně jako u phishingu jde o snahu získat údaje potřebné k přihlášení do uživatelských, anebo přímo bankovních účtů, kdy se útočníci vydávají za instituce a předstírají, že tyto údaje potřebují. Rozdíl je jen v provedení. U vishingu je typicky používán přímý telefonický rozhovor místo podvodného e-mailu či zprávy. Klienti bank by neměli zapomínat, že banky tímto způsobem nejednají a v žádném případě nebudou požadovat sdělení takto citlivých údajů.

**Zabezpečení nám stále moc neříká**

Podle průzkumu asociace má vědomě zabezpečený mobilní telefon jen polovina Čechů a pětina si myslí, že je jejich přístroj chráněn díky samotnému operačnímu systému.

„*I když se v porovnání s předchozími lety výsledky zlepšily, není to důvod k radosti. Právě s ohledem na široké spektrum činností, které z mobilu provádíme, musíme věnovat zvýšenou pozornost i jeho zabezpečení, jinak můžeme rychle přijít o peníze či osobní údaje,*“ komentuje Helena Brychová z ČBA a dodává, že neustálá osvěta v tomto směru je nezbytná. Nejrizikovějším článkem v oblasti zabezpečení jsou totiž často sami uživatelé či klienti, kteří svou vlastní nepozorností podvodníkům práci usnadňují. Z průzkumu asociace mimo jiné vyplynulo, že Češi v ochraně dat před jakýmkoli možným únikem nejvíce (v 70 %) důvěřují bankám.

*„Zabezpečení mobilního zařízení přitom není nikterak složité. Především je třeba pravidelně aktualizovat operační systém telefonu, stahovat důvěryhodné aplikace z důvěryhodných zdrojů a používat bezpečnostní software,“* vysvětluje Pavel Matějíček z ESETu.

**Na sílu hesel začínáme dbát, jedno univerzální heslo však používá každý desátý**

V letošním roce došlo k podstatnému zlepšení chování Čechů ve vztahu k tomu, jaká hesla používají. Stále platí, že ta nejsilnější používá většina z nás především v prostředí internetového bankovnictví (85 %, oproti 71 % v roce 2019) a pro přihlášení se ke svému e-mailu (69 %, oproti 48 % v roce 2019). Narostl však také počet těch, kteří sofistikované heslo volí i pro přístup k sociálním sítím, e-shopům a v případě stahovaní aplikací.

„*Hesla fungují jako první obranný val. Pokud nejsou kvalitní, nemusí ty ostatní bezpečnostní vrstvy zafungovat podle očekávání. Doporučil bych uživatelům využívat fráze, nikoli náhodný shluk písmen. Fráze může vycházet z nějaké vzpomínky uživatele, aby byla zapamatovatelnější. Pokud bude fráze delší než 16 znaků, stačí použít malá a velká písmena a číslice,“* radí Pavel Matějíček z ESETu.

I přes výše uvedená zlepšení uvedl každý desátý, že využívá jedno univerzální heslo bez ohledu na danou aplikaci či službu. Na 30 % pak využívá hesla odlišná. V tomto ohledu jsou obezřetnější především starší lidé, u mladých šlo pouze o pětinu respondentů.

Co se týče uchovávání hesel stále jasně dominuje jejich uchovávání v paměti, a to pro různé typy účtů. Zhruba každý desátý si přitom heslo zapisuje na místo, které je podle něj bezpečné. *„To, jestli si heslo Češi pamatují nebo ho mají zapsané souvisí podle průzkumu s věkem respondenta – s věkem roste i tendence hesla zapisovat. Zajímavé zjištění z pohledu věkové struktury je u speciálních aplikací, resp. správce hesel. Tyto aplikace, i přesto, že jsou podle průzkumu využívané v malém množství, jsou používané napříč generacemi poměrně vyrovnaně,*“ doplňuje Jana Hamanová z výzkumné agentury SC&C.

*„Bezpečnost hesel výrazně zvyšuje i to, pokud uživatel pro každou službu využívá heslo unikátní. Pochopitelně tolik hesel je složité si pamatovat z hlavy. Lidé se tak uchylují k jejich zapisování nebo ukládání v prohlížečích. Ani jeden postup nelze doporučit. V Česku jsou dlouhodobě nejvýraznější hrozbou trojské koně, které kradou hesla uložená v prohlížečích. Vhodnější variantou je využívat speciální program pro správu hesel. Stačí si zapamatovat jednu vstupní frázi a pak už program dokáže všechna hesla vyplňovat automaticky. Přihlašovací údaje se ukládají v zabezpečené šifrované podobě,“* uzavírá Pavel Matějíček ze společnosti ESET.

**O průzkumu: Index Kyberbezpečnosti ČBA**

Průzkum zaměřený na chování Čechů na internetu a jejich názory spojené s on-line prostředím realizovala pro Českou bankovní asociaci výzkumná agentura SC&C. Průzkumu, který probíhal ve dnech 22. května až 8. června letošního roku, se zúčastnilo 1 010 respondentů z celé ČR starších 18 let s přístupem k internetu.

**O Kybertestu**

Společný projekt České bankovní asociace, společnosti ESET a výzkumné agentury SC&C, jehož cílem bylo otestovat znalosti Čechů. On-line test obsahoval otázky (resp. obrázky), které představovaly situace, do kterých se uživatel internetu běžně dostává. V každé otázce byly ukryty podezřelé prvky, které naznačovaly, že se může jednat o práci podvodníků a cílem bylo tyto prvky odhalit. Kybertest probíhal od 16. listopadu do 22. listopadu letošního roku a zúčastnilo se ho 1826 respondentů starších 18 let s přístupem k internetu.

**Další informace obdržíte na adrese:**

|  |  |  |
| --- | --- | --- |
| Monika Petrásková,  Manažerka PR a komunikace ČBA  [monika.petraskova@cbaonline.cz](mailto:monika.petraskova@cbaonline.cz)  tel: +420 733 130 282 | Ondřej Šafář,  Manažer PR a komunikace ESET  [ondrej.safar@eset.cz](mailto:ondrej.safar@eset.cz)  tel: +420 776 234 218 | Jana Hamanová,  Ředitelka výzkumné agentury SC&C  [jhamanova@scac.cz](mailto:jhamanova@scac.cz)  tel: +420 732 150 284 |