PODCAST KDP ČR

DAŇOVÝ SVĚT JINAK NEŽ JEJ ZNÁTE.

Audiočlánek / 28.6.2022

Střípky z digitálního světa 4 / 4
Odvrácená tvář

MVDr. Milan Vodička, vedoucí sekce IT KDP ČR

Odvrácená tvář

Pokud procházíme digitálním světem, nelze se vyhnout ani hrozbám, které se v něm vyskytují a které nemohou být nikdy zcela eliminovány. Cílem je proto minimalizovat rizika a především ochránit, jak vlastní, tak i klientská data.

Aktivity hackerů zesílily adekvátně tomu, jak se do digitálního prostředí přesunují další a další činnosti i uživatelé. Základní postupy jsou přitom víceméně stále stejné, snahou je donutit uživatele, aby o sobě sdělil citlivé údaje (včetně platebních), otevřel infikovanou přílohu zprávy anebo navštívil konkrétní webovou stránku, kde proběhne pokus nainstalovat mu do zařízení škodlivý software. Co se v čase proměňuje, jsou prostředky používané hackerskou komunitou, kdy dochází k hledání nových, daleko více individualizovaných cest, zaměřených na konkrétní osobu. Reálné údaje budící zdání legitimity jsou přitom často získány z internetu a sociálních sítí (tzv. scrapping).

Falešné e-shopy a phishing

Čím dál vynalézavěji se snaží nepovolané osoby dostat k osobním údajům nebo finančnímu profitu. V předvánočním čase se vyrojilo nemalé množství falešných internetových obchodů s atraktivními slevami a cenami. Autor je nucen přiznat, že byl také nachytán podvrženými stránkami e-shopu, který nabízel za skvělé ceny výrobky známého producenta zimního oblečení. Falešné byly nejen stránky samotného e-shopu, ale i pod odkazem otevřený web „originálního“ výrobce, včetně seznamu ověřených prodejců a zprostředkovatelů a rozsáhlého katalogu zboží. Digitální stopy končí na území Číny.

Nedávno se s podobnými problémy setkali i zákazníci známé a v Čechách rozšířené dodávkové služby Zásilkovna.[1] Falešné webové stránky obsahovaly také zdařilou napodobeninu platební brány sbírající zadané informace, které byly následně nelegálně použity k pokusu o zpronevěru finančních prostředků.

[1] Zdroj https://cyberblog.cz/zasilkovna-upozornuje-na-phishingove-praktiky/

Scam call a vishing

Možná jste absolvovali telefonát s podvodným operátorem, který nabízel skvělou investici, např. do akcií některé renomované společnosti. Jeho legenda bývá vylepšena tím, že se jedná o nabídku veřejně neobchodovatelných cenných papírů, které jsou dostupné pouze prostřednictvím speciálního fondu, jehož zástupce tuto příležitost právě vám nabízí. Vše potřebné k realizaci obchodu přitom vyřeší volající, podmínkou ale je, že si uživatel stáhne a nainstaluje software, kterým následně předá vládu nad svým počítačem vzdálenému operátorovi. Ten tuto šanci ovšem zneužije k pokoutným účelům, jako je vydolování osobních údajů, hesel apod.

Na podobném principu funguje vishing (zkratka slov voice phishing), který zneužívá metody sociálního inženýrství. Volající se vydávají za nějakou důvěryhodnou osobu, jako osobního bankéře, zástupce známé instituce, operátora poskytovatele mobilních služeb apod. Důvodem telefonátu bývá nějaká fiktivní „naléhavá“ záležitost, kterou je potřeba neodkladně řešit. Jednat se může o podezřelé platby v exotické destinaci, bezpečnostní riziko nacházející se údajně v počítači, problémy s plněním objednávky, dluhy na daních, ale třeba také cennou výhru v soutěži. Cílem je navodit stresovou situaci, ve které uživatel poleví v ostražitosti a sdělí citlivé údaje, včetně čísla účtu, bankovní karty nebo CVV kódu. Pokus bývá někdy doprovázen předchozí falešnou SMS zprávou (smishing) avizující následný kontakt ze strany operátora, identita volajícího bývá skryta nebo může dokonce podvodně simulovat reálné číslo nějaké známé a důvěryhodné instituce (spoofing).

QR kódy

Tyto obrázkové kódy doznávají čím dál většího rozmachu díky jednoduchosti a rychlosti použití mobilními prostředky. Stále častěji se lze setkat i s platebními QR kódy pro rychlou mobilní platbu nejen faktur, daní ad., ale např. také v restauracích.

A díky masovosti použití roste i snaha o zneužívání tohoto způsobu komunikace určeného k pohodlnému placení anebo k navigaci na konkrétní webové stránky.[2] V podvrženém QR kódu může být ukryt odkaz na web obsahující škodlivý software ke stažení, objevily se i falešné kódy pro vybírání charitativních příspěvků, které ale skončily na účtech podvodníků, v Čechách např. v souvislosti se sbírkami na pomoc obětem tornáda na jižní Moravě nebo k podpoře zooparků během lockdownu.

Obrana existuje

Minimalizovat rizika pohybu v digitálním prostředí je možné a žádné zásadně nové doporučení v souvislosti s výše uvedenými novinkami neexistuje. Stále platí, že nejlepší obranou je důsledné využívání aktualizovaných operačních systémů a antivirových programů, správné užívání a obměna hesel, nestahování software či aplikací z neoficiálních zdrojů, neotevírání neznámých příloh, nesdělování platebních údajů mimo prověřená prostředí apod. Nedílnou součástí této obrany ale musí být i obezřetnost uživatele, nikoli přehnaná, ale adekvátní. Ano,

[2] Podrobnosti viz např. https://spajk.cz/bezpecnost-qr-kodu/

respektování bezpečnostních zásad je někdy otravné a zdržující, ale virtuální svět jedniček a nul to vyžaduje.

Česká bankovní asociace ve spolupráci se společností ESET a Policií ČR připravila hezky zpracovaný test kybernetické ostražitosti,[3] na němž si můžete prakticky vyzkoušet, jak dalece je platné pořekadlo, že ďábel bývá skryt v detailu. Ale právě včasné rozeznání takových drobných odlišností od „běžných“ situací nás může ušetřit následných komplikací a problémů.

A když jsme u těch zásad, tak jedna univerzální na závěr: „Pokud je na internetu nabízeno něco zdarma, zbožím jste vy a vaše údaje.“

[3] Dostupný online na https://kybertest.cz/