V aktuálním IT Kompasu jsme pro Vás připravili:

158. číslo

Vybrané aktuality ze světa IT
Tipy – Triky
Soutěž
Vtip pro dobrou náladu

Vybíráme zajímavé aktuality:

Pět nejčastějších technik sociálního inženýrství
Naprostá většina úspěšných kybernetických útoků zneužívá nechtěné spolupráce napadeného a stojí na technikách sociálního inženýrství. Více...

Ukládáte hesla do prohlížečů?
V téměř pětině všech případů kybernetických hrozeb pro operační systém Windows v Česku se v červenci objevil spyware Agent Tesla. Více...

Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na Facebooku .

Tipy a triky

Co je bezkontaktní NFC platba a je její používání bezpečné?

Bezkontaktní platby NFC se velice rychle stávají oblíbenou metodou placení, a to nejen mezi mladými lidmi, kteří již vyrůstali v "digitální ekonomice". Spousta uživatelů se ale stále obává o bezpečnost svých platebních transakcí, přestože bezkontaktní NFC platby jsou z principu velice bezpečné. Pro bezpečné NFC platby jsou klíčové tři prvky - zařízení s podporou NFC (mobilní telefon, chytré hodinky...), transakční aplikace (Google Pay, Apple Pay...) a také platební terminál u obchodníka.

Nejprve si povíme něco o technologii NFC jako takové. Počátky technologie NFC sahají až do roku 1983, kdy byl registrován první patent, který byl asociován se zkratkou RFID (Radio Frequency Identification, identifikace na rádiové frekvenci). RFID čipy se používají dodnes například k identifikaci zboží (hezky má identifikaci řešen například Decathlon - z košíku přemístíte zboží "do boxu" u pokladny, která snímá RFID čipy umístěné ve štítcích na zboží a pokladna tak automaticky zboží rozpozná a namarkuje) nebo pro ochranu zboží před zcizením (pípající rámy jsou dnes téměř v každém obchodě). Pod zkratkou NFC se skrývá název Near Field Communication, což česky znamená doslovně "komunikace v blízkém poli". Ono "blízké pole" v praxi znamená vzdálenost mezi komunikujícími zařízeními maximálně 4 cm. Mezi první zařízení s podporou NFC patřily například již stařičké mobily Nokia 6131, to se psal rok 2006. V praxi se NFC využívalo například k výměně dat mezi telefony (soubory či kontakty), kdy se telefony doslova přitiskly zády k sobě. Až v roce 2013 ale došlo k prvním smysluplným pokusům o bezdrátové NFC platby, a to spoluprací firem Samsung a VISA (bezkontaktní platební karty), které byly o rok později následovány firmou Apple, která představila transakční aplikaci Apple Pay na jejich nových zařízení iPhone 6/6 Plus. Pak se teprve začali dít věci :).

Je bezkontaktní NFC platba skutečně bezpečná?

Jak již bylo zmíněno, princip NFC spočívá v komunikaci mezi dvěma zařízeními na velmi krátkou vzdálenost. Tento aspekt je z hlediska bezpečnosti velice důležitý - kdyby Vám chtěl někdo ukrást informace z platební karty, mobilu či hodinek, musel by se na Vás doslova nalepit, aby dostal čtečku NFC do potřebné blízkosti. A i v takovém případě by byl schopen načíst možná tak údaje z platební karty, protože v chytrých zařízeních se funkce NFC platby musí nějakým způsobem aktivovat, což je druhý podstatný aspekt zabezpečení NFC. K ochraně bezkontaktních platebních karet existují různé pouzdra, většinou kovové - ostatně by stačilo platební kartu hezky zamotat do alobalu :). K dalším důležitým bezpečnostním prvkům NFC komunikace patří:

1. Platby jsou odesílány zabezpečeným připojením, které je sdíleno pouze s obchodníkem a přenos dat je šifrován 256 bitovou šifrou AES. Odposlech takové transakce je víceméně nereálný, a dešifrování komunikace by i tak bylo velice obtížné.
2. Při platbě obchodník nevidí žádné údaje ani o platební kartě, ani o zařízení použitým k platbě.
3. Při placení nemusíte vůbec používat platební kartu (klidně ji nechejte doma), takže ani nehrozí riziko "odečtení" čísla platební karty, bezpečnostního kódu CVC (také CCV či CVC2) ani údaje o držiteli platební karty.
4. Zařízení komunikují na velmi krátkou vzdálenost (4 cm), takže kdyby chtěl útočník v reálu načíst údaje z Vašeho telefonu či hodinek, musel by svou loupežnickou čtečku přiložit přímo k Vašemu zařízení. A toho byste si velice pravděpodobně všimnuli.
5. Pokud máte podezření, že došlo ke zneužití či krádeži údajů přes NFC, po nahlášení bance dojde k zablokování platební karty a velice pravděpodobně byste také dostali peníze zpět. Zde je nutno zdůraznit, že i když platíte pomocí telefonu či hodinek, stále tato zařízení předávají přes NFC údaje o platební kartě autorizované v transakční aplikaci (Apple Pay, Google Pay).

Možné útoky cílící na NFC

Přesto, že je tedy NFC z principu velice dobře zabezpečeno, lze se teoreticky setkat se třemi možnými typy útoků. Prvním možným typem útoku je zachycení a změna dat. Tento útok předpokládá, že útočník zachytí NFC komunikaci, dešifruje ji a následně pošle příjemci upravenou verzi dat. V praxi je to vlastně nereálné - to spíše vyhrajete v EuroJackpotu hlavní cenu :).

Druhým typem útoku je rušení NFC komunikace. Tento útok nemá za úkol získat a následně zneužít data, ale znemožnit NFC komunikaci. Důsledky takového útoku jsou nasnadě - pokud by se v nějakém supermarketu pohyboval útočník s "rušičkou NFC", jistě byste si všimli zmatku na pokladnách :). V praxi je tento útok ale také víceméně nereálný.

Dalším teoreticky možným útokem je zneužití zcizených či ztracených mobilů či chytrých hodinek. Zde přichází ke slovu zabezpečení transakční aplikace, kterou musíte v zařízení nejprve "zavolat". Což znamená, že se jakožto útočník musíte do telefonu či hodinek nejprve nějak dostat (otisk prstu, obličej, PIN) a následně překonat i zabezpečení samotné transakční aplikace (opět třeba otisk prstů, obličej, nebo další PIN). Z čehož logicky plyne, že používat NFC v totálně nezabezpečeném mobilu je zásadní chybou.

Co mohu udělat pro ještě lepší zabezpečení NFC plateb?

Pokud chcete ještě zvýšit bezpečnost NFC plateb, můžete teoreticky udělat pár věcí. V prvé řadě můžete v zařízení preventivně vypnout NFC :). Není NFC, není datový přenos, není únik dat. Samozřejmě Vás to bude trošku omezovat v tom, že před platebním terminálem nejprve budete muset NFC funkci zapnout, což Vás zdrží asi tak na tři vteřinky.

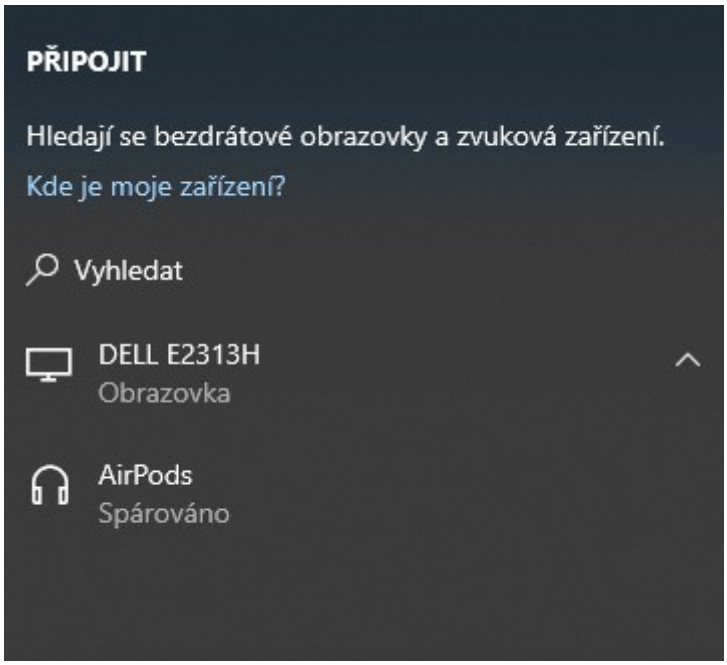
Pokud k placení nepoužíváte mobil či hodinky, ale přímo bezkontaktní platební kartu, pořiďte si na ni speciální pouzdro či obal, který blokuje bezdrátový signál. Někteří uživatelé v závislosti na typu bankovního účtu a/nebo platební karty mohou také relativně jednoduše a pohodlně pro placení používat oddělený bankovní účet či virtuální jednorázovou platební kartu. Dobře vymyšlené to má například britský Revolut - v jejich mobilní aplikaci si jednorázovou virtuální kartu vytvoříte okamžitě a převod peněz z hlavního účtu na ten, který máte vyhrazený pro placení kartou je také "instantní".

Rozhodně nezkoušejte manipulovat s telefonem, hodinkami či dokonce přímo s platební kartou v blízkosti podezřelých či nedůvěryhodných NFC čipů (jinak také NFC tagů) nebo NFC čteček.

A samozřejmě si také dávejte pozor na různé ne zcela standardní platební možnosti, které se poslední dobou rozšiřují - například menší restaurace či bary, které z jakéhokoliv důvodu nemají standardní platební terminál, umožňují provést platbu pomocí mobilního telefonu s aplikací, který tak nahradí klasický platební terminál. V případě, že obsluha (nebo bar či restaurace jako taková) a ve Vás nebudí důvěru, použijte buď jednorázovou virtuální platební kartu, nebo si raději zajděte do bankomatu pro hotovost :).

Jaká klávesová zkratka se ve Windows 10 a 11 může hodit?

Zejména při vzdálené komunikaci se připojují k notebooku nebo stolnímu počítači i bezdrátové přístroje jako jsou například Bluetooth sluchátka (případně jiné zařízení). Použitím klávesové zkratky **Win+K** spustíte v bočním panelu možnosti připojení k bezdrátovým zařízením typu obrazovka (lze tak vysílat obraz na podporovaném monitoru či televizoru) nebo zvuková zařízení (již zmiňovaná sluchátka apod.).



Soutěž

Vyhodnocení minulé soutěže:

Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděla správně a ze správných odpovědí byla vylosována slečna/paní L. Ž., které tímto gratulujeme k výhře softwaru AVG PC TuneUp pro 1 PC na rok zdarma.

Otázka zněla:

Co znamená pojem "Racketeering"?

Správná odpověď měla být:

Tento pojem označuje vydírání (druh organizovaného zločinu), ve kterém pachatelé vytvářejí donucovací, podvodné, vyděračské nebo jinak nezákonné koordinované činy, aby opakovaně nebo konzistentně z toho měli zisk.

Více informací naleznete zde.

Nová otázka:

Co znamená pojem "Sharenting"?

Ze správných odpovědí vylosujeme výherce, který od nás získá Norton 360 Standard pro 1 PC na rok zdarma.

Odpovědi pište do 20. 9. 2022 na e-mail amenit@amenit.cz.

Správnou odpověď a výherce uveřejníme v příštím čísle. Pokud se chcete co nejdříve dozvědět, zda jste vyhráli, staňte se našimi přáteli na Facebooku. Tam se informace o výherci objeví jako první.

Vtip pro dobrou náladu

Co mají společného víly, vodníci a nefrustrovaní informatici?
Všichni se vyskytují jenom v pohádkách.

Vydání IT Kompasu od 1. čísla naleznete zde.