V aktuálním IT Kompasu jsme pro Vás připravili:

123. číslo

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

Vybíráme zajímavé aktuality:

Hackeři napadli třetinu malých firem
Okolo 36 % malých firem se v průběhu tohoto roku stalo obětí úniku dat. Více...

Některé značky mobilů lze hacknout pomocí podvodných SMS zpráv
Společnost Check Point odhalila nový druh phishingových útoků, které kradou e-maily z mobilních zařízení s operačním systémem Android vyrobených společnostmi Samsung, Huawei, LG a Sony. Více...

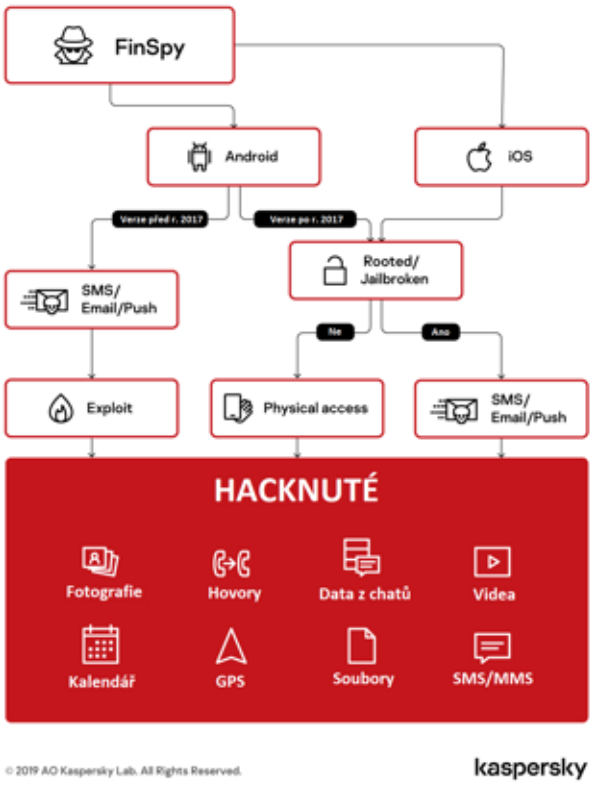
Více aktualit naleznete na www.AntiviroveCentrum.cz nebo na Facebooku .

Tipy a triky

Jak můžete přispět k ochraně svého mobilního zařízení?

- Nikdy nenechávejte nezamčený mobil nebo tablet bez dohledu a ujistěte se, že se nikdo nedívá, když zadáváte svůj bezpečnostní kód pro odemčení obrazovky.
- Neprovádějte u svých zařízení jailbreak nebo rootování – hackerům byste tím velmi usnadnili práci.
- Instalujte si aplikace pouze z oficiálních obchodů Google Play a App Store.
- Neklikejte na podezřelé odkazy, které vám přišly od neznámého čísla/odesilatele.
- Neotvírejte neznámé SMS zprávy.
- V nastavení svého zařízení si zablokujte instalace programů z neznámých zdrojů.
- Pokud to není nutné, nesdílejte s nikým přístupové heslo nebo PIN svých mobilních zařízení.
- Neukládejte si na svá zařízení žádné neznámé soubory nebo aplikace, protože mohou ohrozit vaše soukromí.
- Nainstalujte si na své zařízení účinné bezpečnostní řešení určené pro mobilní zařízení.

Ukázka schématu, jak se dostane malware FinSpy do Vašeho zařízení a jaká data krade:



Více informací naleznete zde.

Jak vyzrát na bezpečná hesla?

V dnešní "internetové době" se uživatel musí téměř stále někam přihlašovat. Začíná to Seznamem či Googlem, pokračuje Facebookem, Twitterem a dalšími sociálními sítěmi a končí zpravodajskými portály nebo internetovým bankovnictvím. V mnoha případech si uživatelé zjednodušují život tím, že do více online služeb používají stejná hesla. Což je samozřejmě velmi, velmi špatný nápad, protože v případě úniku uživatelských dat z jedné služby mají kyberzločinci usnadněnou práci a velice jednoduše se pak mohou nabourat i do dalších služeb založených na kombinaci e-mailová adresa - heslo.

Otázka tedy zní - jak vymýšlet silná hesla, která si lze zapamatovat a aby se neopakovala? Při tvorbě hesla vezměte v potaz, že je musíte snadno napsat na jakékoli klávesnici. Můžete použít i českou diakritiku, což rozhodně zvýší bezpečnost, na druhé straně je ale možné, že na klávesnici v zahraničí heslo nedokážete napsat. Tvořte si sousloví, které bude obsahovat různé znaky, číslovky i velká písmena. Optimální délka je okolo 7 slov. Skvělým příkladem mohou být například takováto spojení:

Kazde-p0ndeli-ctu-bl0g-0d-Petra-N0vaka

Nepoužívejte ale přísloví nebo třeba části písňových textů. Takto populární fráze ve slovníkových databázích bývají.

Sílu hesla si můžete ověřit online pomocí testovacího nástroje HowSecureIsMyPassword.net. Uvedené heslo v příkladu by potenciální útočník luštil miliardy let.

Zda byl Váš uživatelský účet kompromitován, tedy zda byl obsažen v některé z již uniklých databází, můžete ověřit na stránce HaveIBeenPwned.com. Pokud Vás systém na kompromitaci hesla upozorní, změňte si jej co nejdříve.

Dobrým pomocníkem jsou také programy pro správu hesel. Správce hesel přihlašovací údaje ukládá v zašifrované podobě a přístup do programu je chráněn například jedním silným hlavním heslem (možností ochrany může být v závislosti na použitém programu více). Díky správci hesel můžete vymýšlet unikátní a bezpečná hesla, aniž by bylo nutné si je psát na papír. Správce umí také sledovat práci ve webovém prohlížeči a pokud narazí na registrační formulář, nabídne vygenerování a uložení silného hesla a zároveň si přihlašovací údaje uloží do své databáze.

Programů, které umí takto spravovat přihlašovací údaje (a nejen je) existují desítky, je tedy určitě z čeho vybírat. Password Manager ostatně obsahuje například bezpečnostní balíček ESET Smart Security Premium, o který si můžete tentokrát také zasoutěžit.

Soutěž

Vyhodnocení minulé soutěže:

Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a z mnoha správných odpovědí byl vylosován pan J. Š., kterému tímto gratulujeme k výhře softwaru AVG PC TuneUp pro 1 PC na rok zdarma.

Otázka zněla:

Co je v IT bezpečnosti označováno pojmem "Whaling"?

Správná odpověď měla být:

Phishingový útok, který se specificky zaměřuje na vrcholové manažery společnosti, se nazývá whaling (lov velryb), protože jsou oběti považované za vysoce hodnotné, a lze jim tak odcizit cennější informace, než má k dispozici běžný zaměstnanec.
Přihlašovací údaje patřící výkonnému řediteli otevřou více dveří než informace zaměstnance na základní úrovni. Cílem je ukrást data, údaje o zaměstnancích a finanční prostředky.

Nová otázka:

Co je v IT bezpečnosti označováno pojmem "Snowshoeing"?

Ze správných odpovědí vylosujeme výherce, který od nás získá ESET Smart Security Premium pro 1 PC na rok zdarma.

Odpovědi pište do 20. 10. 2019 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

"Všichni mi říkají, že jméno kocoura se jako heslo pro roota nehodí,"
stěžuje si kamarádovi programátor.
"Ale když já jsem si tak zvykl na mého Qzb7kw_2et!"

Vydání IT Kompasu od 1. čísla naleznete zde.

Tým Antivirového Centra
Amenit s.r.o.

ANTIVIROVÉ CENTRUM
www.AntiviroveCentrum.cz

ANTIVIROVÉ CENTRUM - MÁTE SE KAM OBRÁTIT

Amenit s.r.o. - jsme s vámi již od roku 1998, tel.: 556 706 203, 222 360 250

Nezobrazuje-li se vám e-mail správně, klikněte prosím zde.