V aktuálním IT Kompasu jsme pro Vás připravili:

161. číslo

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

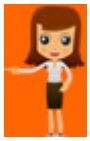
Vybíráme zajímavé aktuality:

Hrozby pro Android
Útočníci se zaměřují na uživatele, kteří stahují software z veřejných internetových úložišť. V pravidelné statistice kybernetických hrozeb pro platformu Android se objevila tři aktuálně největší rizika pro české uživatele – adwary Andreed a Hiddad a nový dropper Agent.KEQ. Více...

V říjnu šířily spyware falešné faktury
Podle poslední statistiky nejčastějších hrozeb pro operační systém Windows v Česku je s téměř pětinou všech detekcí největším rizikem spyware Agent Tesla. Více...

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

Tipy a triky



Jak bezpečně provozovat IP kamery?

Stále více uživatelů si domů pořizuje bezpečnostní kamery, které jim v nepřítomnosti umožní lépe chránit a kontrolovat jejich majetek či rodinné příslušníky. Jakožto každá užitečná věc ovšem i bezpečnostní kamery mohou být v případě nevhodného zabezpečení zneužity k narušení soukromí, nebo k útoku na další zařízení v domácí síti. Na internetu jsou dostupné databáze online dostupných kamer, přičemž je víceméně jisté, že ne všichni uživatelé svoje kamery sdílí s celým světem dobrovolně a ví o tom. Zranitelné kamery lze ovšem zneužít nejen v rámci narušení soukromí, mohou také být zapojeny do rozsáhlé sítě "zotročených zařízení", (tzv. botnetu), která může být zneužita k dalším útokům typu DDoS a podobně.

Co tedy před pořízením IP kamery zvážit a o vyhlédnuté kameře zjistit? V žádném případě nelze doporučit pořízení nejlevnějších "neznačkových kamer" z různých neprověřených webových obchodů, a je jedno, zda se jedná o e-shop čínský či český. Důležité je, aby výrobce vydával nové aktualizace firmware kamery a reagoval na zjištěné případné bezpečnostní problémy svých výrobků - a to u těch nejlevnějších kamer nelze moc očekávat. Pokud chcete pořídit kameru připojenou přes Wi-Fi, je vhodné zjistit, zda kamera používá stejné zabezpečení jako Vaše Wi-Fi síť (kterou máte jistě správně nastavenou a zabezpečenou :)). Pamatujte, že kamera se musí přizpůsobit Vaší Wi-Fi, nikoliv naopak - nechcete si přece kvůli ušetřeným pár korunám snížit zabezpečení své bezdrátové sítě jen proto, aby s ní komunikovala nějaká levná kamera.

Dále by Vás mělo zajímat, jakým způsobem se k datům z kamery přistupuje. Obecně vzato jsou zde dvě možnosti, jak se ke kameře připojit, a to buď prostřednictvím cloudových služeb výrobce či speciální aplikace, nebo přímo na kameru skrz internetový prohlížeč (k tomu budete patrně potřebovat pár dalších drobností, jako je veřejná IP adresa apod.). V obou případech je důležité, aby přenos dat probíhal šifrovaně.

Dalším oříškem může být ukládání dat z kamer v případě, kdy Vám prostý online přenos či ukládání dat do cloudových služeb výrobce z nějakých důvodů nebude vyhovovat. Kamery dokáží vygenerovat poměrně velký objem dat a je tedy potřeba zvážit, kam data ukládat. Některé kamery umí data ukládat na SD kartu, nicméně objem uložených záznamů je pak pochopitelně limitován velikostí SD karty. Častější formu ukládání dat jsou síťová disková úložiště typu NAS, z nichž mnohá disponují funkcí NVR (network video recorder) a dokážou data z kamer jednoduše ukládat a zpřístupnit. Krom toho disponují také například funkcí detekce pohybu včetně upozornění uživatele e-mailem.

Důležité je také fyzické umístění kamery. Kamera by měla být umístěna mimo dosah dětí či domácích mazlíčků a rozhodně ji nedávejte do míst, kde by Vám bylo nepříjemné, kdyby Vás pozoroval v případě narušení někdo cizí. Takže kamera v koupelně, na toaletě či v ložnici asi není úplně nejlepší nápad :)

Pro minimalizování možných rizik narušení je důležité, abyste co nejdříve po zprovoznění kamery změnili výchozí hesla pro přihlášení a pokud to lze, použijte neutrální název kamer, kupříkladu název "Cam1" je určitě méně zajímavý a bezpečnější, než například "Franta Novák kamera obývací pokoj". Pro přístup přes mobilní aplikaci či cloudové služby výrobce použijte silné heslo a použijte také dvou faktorové zabezpečení, pokud to výrobce umožňuje. Zkontrolujte také aktualizaci firmware kamery či mobilní aplikace.

Co dělat s nechtěně aktivovanou klávesou CapsLock při psaní textu?

Pokud nepatříte mezi uživatele, kteří píšou všemi deseti prsty, aniž by se přitom museli dívat na klávesnici, jistě jste již zažili situaci, kdy vesele píšete s aktivovanou klávesou CapsLock. Výsledkem bývá kus textu napsaný velkými písmeny, což by samo o sobě možná nemuselo nijak zvlášť vadit, ale... Text psaný velkými písmeny je hůře čitelný a navíc v "počítačštině" velké písmena znamenají kromě zdůraznění slova či věty také rozhořčení či naštvání. Je tedy určitě namístě text přeformátovat na malá písmenka.

Jak na to? Většina uživatelů svou chybu napraví tak, že text smaže a napíše ho znovu. Existuje ale jednodušší a také podstatně rychlejší řešení. To spočívá ve využití klávesové zkratky **Shift+F3**. Pokud text napsaný velkými písmeny označíte a následně použijete klávesovou zkratku **Shift+F3**, dojde ke změně textu na malá písmena. Po dalším stisknutí klávesové zkratky se přeformátuje text tak, že první písmena ve větě budou velkými písmeny. Po dalším stisknutí bude celý text opět velkými písmeny a tak stále dokola :)

Na závěr zdůrazníme, že tato funkce je použitelná například v aplikaci Word či Outlook, není ale dostupná například při psaní e-mailu na Seznamu či Google.

Soutěž

Vyhodnocení minulé soutěže:

Na otázku z minulého vydání elektronického magazínu IT Kompas odpověděl správně a ze správných odpovědí byl vylosován pan J. O., kterému tímto gratulujeme k výhře softwaru Sticky Password Premium pro 1 uživatele na rok zdarma.

Otázka zněla:

Co je v počítačové bezpečnosti "Anti-stealth"?

Správná odpověď měla být:

Anti-stealth chrání před tzv. stealth viry, které mohou v systému utajeně škodit (stealth = neviditelný). Anti-stealth je tedy technologie antivirového programu pro rozpoznání a odstranění těchto virů.

Nová otázka:

Co znamená v počítačové terminologii pojem "Deepfake"?

Ze správných odpovědí vylosujeme výherce, který od nás získá AVG Internet Security pro 1 PC na rok zdarma.

Odpovědi pište do 20. 12. 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

Kdybys potkal medvěda, jaké kroky bys podniknul?

Co nejdelší...

Vydání IT Kompasu od 1. čísla naleznete zde.