Zkroťte práva aplikací

Smartphony a tablety by byly bez dodatečně instalovaných aplikací mnohem méně užitečné. Problém je, že si aplikace často nárokují podstatně více oprávnění, než je zdrávo.

Manuel Schreiber, Radek Kubeš

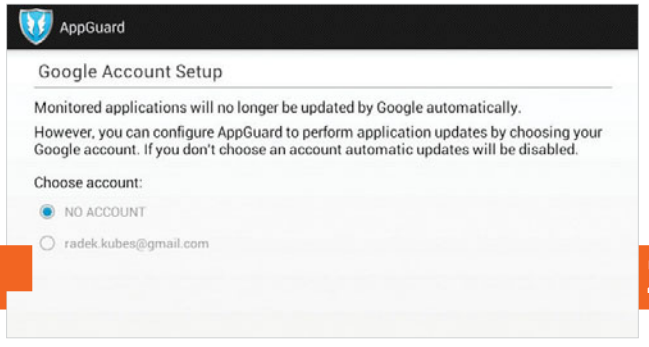
Aplikace pro zařízení s operačním systémem Android se nechovají právě vzorně. Přes třicet pět procent bezplatných aplikací z Google Play sleduje uživatele, více než devět procent aplikací požaduje přístup ke kontaktům a přes šest procent z nich si vyžádá přístup k vašim e-mailům. Lepší není ani situace s aplikacemi pro iOS, kde navíc ani uživatel netuší, jaká oprávnění má konkrétní aplikace přidělena. Tato alarmující zjištění vyplývají z průzkumu společnosti Bitdefender, která vyvíjí stejnojmenný antivirový software. Ptáte se, jaký k tomu mají tvůrci těchto aplikací důvod? Nejčastěji jde o prodej dat získaných ze zařízení uživatele, který při instalaci bez dlouhého zkoumání potvrdí špehovacím aplikacím práva v požadovaném rozsahu. Aplikace samy získaná data většinou k ničemu nevyužívají, pouze je sbírají, aby je mohli jejich tvůrci zpeněžit.

Aplikace za osobní data

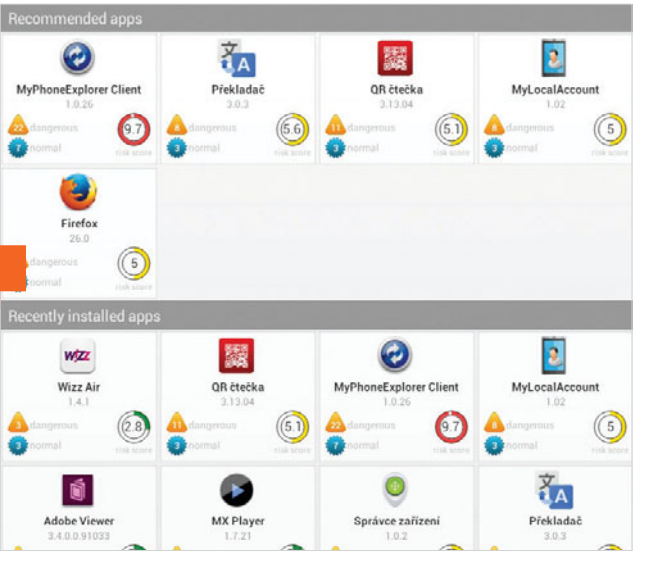
Použití bezplatné aplikace nebo služby za cenu částečné ztráty soukromí je dnes na internetu běžnou praxí. Vývojáři některých aplikací jsou však často tak daleko, že předávají obsah e-mailů pochybným serverům, prodávají adresy spammerům a nabízejí na trhu i detailní informace o zařízeních. Každý, kdo chce takovou aplikaci používat a nebere přitom ohled na oprávnění, která aplikace požaduje, zaplatí svými osobními daty. Zdarma dostupných aplikací je na Google Play obrovské množství a každým dnem přibývají další. Nelze tedy říci, kterým konkrétním aplikacím se vyhnout. Pomocí vhodných nástrojů však můžete sami určit, jaká oprávnění instalovaným aplikacím přidělíte.

Android 4.3: Dobře ukrytá správa oprávnění

V Androidu 4.3 se skrývá nová funkce App Ops, prostřednictvím které lze řídit práva instalovaných aplikací. App Ops však nemá žádné ovládací rozhraní, kde by bylo možné s právy aplikací pracovat. Proto je třeba instalovat aplikaci, jako je například Permission Manager, která nabídne přehledné uživatelské rozhraní a funkce pro správu oprávnění. Navíc k tomu nepotřebuje ani odemknutý administrátorský účet ve vašem zařízení (tzv. root). Bohužel funkce App Ops nepracuje vždy stoprocentně, a tak se může stát, že aplikace s pozměněnými právy přestane fungovat.



1



2

Permission Manager

SRT AppGuard

Kontrola nad aplikacemi

V minulém Chipu jsme se podrobně věnovali alternativní verzi operačního systému Android (tzv. custom ROM) Paranoid Android, která, podobně jako například CyanogenMod, obsahuje funkce pro kontrolu oprávnění instalovaných aplikací. Na rozdíl od nástrojů jako SRT AppGuard však tyto funkce neupravují samotné aplikace, ale podstrkují jim falešné informace, u kterých nevadí, že jsou vyneseny ze zařízení. Pokud chce nějaká aplikace například přístup ke kontaktům, nahlásí jí funkce CyanogenMod, že žádné kontakty nejsou k dispozici. Výhodou je, že tento způsob ochrany osobních dat uživatele nemá vliv na funkčnost aplikací, které se snaží získat informace k prodeji.

Správa aplikací ve starších verzích Androidu

Jak jsme zmínili, funkci App Ops najdete pouze v Androidu 4.3 nebo novějším. Aktuálním Androidem je ale vybaveno jen málokteré zařízení, pokud se nejedná o smartphone či tablet řady Nexus přímo od Googlu nebo prémiový přístroj značkových výrobců. Existuje však způsob, jakým spravovat oprávnění aplikací i v zařízeních se starší verzí operačního systému Android.

Aplikací použitelných za tímto účelem je celkem hodně, většina z nich však vyžaduje odemknutý administrátorský účet v Androidu. Světlou výjimkou je aplikace SRT AppGuard, která ale není k dispozici na Google Play. Stáhnout si ji můžete v podobě APK balíčku z odkazu skrytého pod QR kódem u tohoto článku. Základní verze SRT AppGuard je k dispozici zdarma, může však monitorovat chování a nastavovat oprávnění nejvýše čtyř aplikací. Za plnou verzi SRT AppGuard Pro je třeba zaplatit asi 110 korun.

Po instalaci vás SRT AppGuard nejprve stručně provede svými funkcemi a pak vám nabídne využití vašeho účtu Google pro pozdější automatické aktualizace instalovaných aplikací (obr. 1). Pokud byste s tímto nastavením nesouhlasili, museli byste všechny aplikace aktualizovat manuálně.

SRT AppGuard provede analýzu všech instalovaných aplikací a posoudí jejich rizikovost z hlediska oprávnění, která mají přidělena. Automaticky vám pak nabídne čtyři nejrizikovější aplikace, které vám doporučí sledovat (ve verzi Pro můžete samozřejmě sledovat všechny instalované aplikace) (obr. 2).

Sledování aplikace zahájíte použitím tlačítka »Monitor« v jejím detailním popisu (obr. 3). SRT AppGuard vás přitom ještě upozorní na skutečnost, že byste správně neměli upravovat oprávnění aplikace, jejíž licenční podmínky použití takovou změnu zakazují. Záleží na vás, zda budete varování respektovat. SRT AppGuard analyzuje aplikaci a provede její reinstalaci. Zároveň vás informuje, že tento postup povede ke ztrátě uživatelských dat a nastavení v této aplikaci.

Když je aplikace instalovaná prostřednictvím SRT AppGuard, můžete upravovat její oprávnění (obr. 4). Podobně jako v případě funkce App Ops je zde ovšem jisté riziko, že aplikace s pozměněnými právy přestane fungovat správně. autor@chip.cz

Permission Manager

Permission Manager využívá funkci App Ops v Androidu a umí detailně spravovat oprávnění instalovaných aplikací.