Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- Преглед
- Изтегляне на мобилни приложения
- Разрешения
- Актуализиране на приложения

Безопасно използване на мобилни приложения

Преглед

Мобилните устройства като таблети, смартфони и часовници се превърнаха в основната технология, която ползваме в личния и професионалния ни живот. Това, което прави мобилните устройства толкова гъвкави е наличието на избор от милиони приложения. Тези приложения ни помагат да сме по-продуктивни, незабавно да комуникираме или споделяме с другите, да преподаваме и учим, или просто да се забавляваме повече. Освен възможностите обаче, с всички тези мобилни приложения идват и рискове. Тук ще намерите няколко стъпки, които може да следвате, за да използвате безопасно и пълноценно мобилните си приложения.

Гост-редактор

Джошуа Райт е техническият директор на Counter Hack и старши инструктор на института SANS. Той е авторът на SEC575: Mobile Device Security and Ethical Hacking, както и на Hacking Exposed: Wireless. Намерете Джош в Twitter **@joswr1ght**.

Изтегляне на мобилни приложения

Първата стъпка е да се уверите, че винаги сваляте мобилни приложения от безопасен и доверен източник. Кибер престъпниците са се специализирали в създаването и разпространението на заразени мобилни приложения, които изглеждат като всички други. Ако инсталирате едно от тези заразени приложения, престъпниците могат да получат пълен контрол над мобилното ви устройство. Използвайки приложения само от добре известни и доверени източници намалявате риска от инсталиране на заразено приложение. Нещо, което може би не знаете е, че марката на мобилното ви устройство определя опциите ви за сваляне на приложения. За Apple устройства като iPad или iPhone, сваляйте мобилни приложения само от Apple App Store. Предимството на това е, че Apple проверява сигурността на всички мобилни приложения, преди да ги направи достъпни. Въпреки че Apple не може да хване всички заразени мобилни приложения, тази наблюдавана среда помага рискът от инсталиране на заразено приложение да се намали драстично. Освен това, ако Apple открие приложение в своя магазин, което смята, че е заразено, то ще бъде бързо премахнато. Windows Phone използва подобен подход за управление на приложенията.

Мобилните устройства с Android са различни. Android ви дава повече гъвкавост като ви позволява да изтегляте мобилно приложение от където и да в Интернет. С тази гъвкавост обаче идва и повече отговорност. Трябва да бъдете по-внимателни относно това кои мобилни приложения изтегляте и инсталирате, тъй като не всички биват преглеждани. Google поддържа управлявано хранилище за мобилни приложения подобно на това на Apple,

Безопасно използване на мобилни приложения

което се казва Google Play. Мобилните приложения, които сваляте от Google Play са преминали някакви основни проверки за безопасност. В този смисъл ние препоръчваме да изтегляте своите мобилни приложения за Android устройства само от Google Play. Избягвайте изтеглянето на мобилни приложения с Android от други уебсайтове, тъй като който и да е, включително кибер престъпници, могат лесно да създадат и разпространят зловредни мобилни приложения и да ви подмамят да заразите мобилното си устройство. Като допълнителна защита, когато е възможно, инсталирайте антивирусна програма на мобилното си устройство.

Ключът към сигурното използване на мобилни приложения е да се инсталират такива само от доверени източници, да се актуализират когато е възможно, и да се дават само необходимите за приложението разрешения.

Независимо от това кое устройство използвате, една допълнителна стъпка, която можете да направите, е да избягвате чисто нови приложения, които малко хора са изтеглили или които имат много малко положителни коментари. Колкото по-дълго едно приложение е било достъпно, колкото повече хора са го използвали и колкото повече положителни коментари има то, толкова по-голяма е вероятността това приложение да е надеждно. В допълнение, инсталирайте само приложения, които са ви необходими и които използвате. Запитайте се – трябва ли ми наистина това приложение? Всяко приложение носи не само потенциални нови уязвимости, но също така и нови проблеми с конфиденциалността на информацията ви. Ако спрете да използвате дадено приложение, махнете го от мобилното си устройство (винаги можете да го добавите обратно, ако установите, че имате нужда от него. И последно, никога не правете т.нар. jailbreak или root на мобилното си устройство. Това е процесът на проникване в него и инсталиране на неодобрени приложения или промяна на съществуващи вградени функционалности. Това не само заобикаля или елиминира много от контролите за сигурност, които са вградени в мобилното ви устройство, но често също анулира гаранции и договори за поддръжка.

Разрешения

Веднъж инсталирали мобилно приложение от доверен източник, уверете се, че то е безопасно конфигурирано и защитава поверителността на вашите данни. Винаги премисляйте преди да позволите на мобилно приложение да има достъп: искате ли да дадете на приложението разрешението, което то иска, наистина ли е му необходимо това? Например, някои приложения използват услуги за гео-локация. Ако позволите на дадено приложение винаги да знае къде се намирате, възможно е да позволявате на създателя на това приложение да следи движенията ви, и дори да позволите на автора на приложението да продава тази информация на други. Ако не желаете да дадете разрешенията, откажете искането за разрешение или потърсете друго приложение, което отговаря на изискванията ви. Помнете, имате богат избор.

Безопасно използване на мобилни приложения

Актуализиране на приложения

Мобилните приложения, точно като операционната система на компютъра ви и на мобилното ви устройство, трябва да бъдат актуализирани, за да са в крак с настоящето. Престъпниците постоянно търсят и намират слабости в приложенията. След това разработват планове за атака, за да използват тези слабости. Разработчиците, които са създали приложението ви също създават и публикуват актуализации за отстраняване на слабостите и защитаване на устройствата ви. Колкото по-често проверявате за актуализации и ги инсталирате, толкова по-добре. Повечето устройства ви позволяват да конфигурирате системата си, за да актуализирате мобилните приложения автоматично. Ние препоръчваме тази настройка. Ако това не е възможно, тогава ви препоръчваме да проверявате на всеки две седмици за актуализации на мобилните ви приложения. И накрая, когато приложенията бъдат актуализирани, винаги проверявайте всички нови разрешения, които може да изискват.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Социално инженерство:	https://securingthehuman.sans.org/ouch/2017#january2017
Безопасна раздяла с мобилно устройство:	https://securingthehuman.sans.org/ouch/2016#december2016
Защитете своя нов таблет:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Архиви & Преводи:	https://securingthehuman.sans.org/ouch/archives
Курс по сигурност на мобилните устройства:	https://sans.org/sec575

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова

