Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- Какво е криптиране?
- Какво може да се криптира?
- Как да го използваме правилно

Криптиране

Какво е криптиране?

Сигурно сте чували хората да използват термина „криптиране“ и как то може да се употреби за да защитите себе си и информацията си. Въпреки това, криптирането може да е объркващо, и трябва да сте запознати с ограниченията му. В този бюлетин обясняваме с прости думи какво е криптиране, как ви защитава и как да се използва правилно.

Гост-редактор

Франческа Боско (**@francibosco**) е изследовател, ръководител и участник в проекти в областта на кибер-престъпленията, кибер-сигурността и злоупотреби с технологии.Тя работи в Междурегионалния Изследователски Институт по Криминология и Правораздаване на Обединените Нации и е съосновател на Tech and Law Center.

В устройствата ви има огромно количество поверителни данни, като лични документи, снимки и съобщения. Ако едно от устройствата ви бъде изгубено или откраднато, всичката ви поверителна информация може да бъде достъпна за хората, сдобили се с него. В допълнение, възможно е да изпълнявате поверителни транзакции онлайн, като банкиране или пазаруване. Ако някой е в състояние да наблюдава тези ви действия, той би могъл да открадне информацията ви, включително банкови данни или детайли за разплащателни карти. Криптирането ви предпазва в тези случаи, като гарантира, че неоторизирани хора не могат да виждат или променят информацията ви.

Криптирането съществува от хиляди години. В наши дни криптирането е доста по-сложно, но се използва за същата цел – да се предаде тайно съобщение от едно място на друго, като се гарантира, че само този, за който е предназначено съобщението, ще има достъп до него. Когато информацията не е криптирана, се нарича обикновен текст. Това означава,че всеки може да я прочете или да има достъп до нея. Криптирането преобразува тази информация в нечетим формат, наричан шифриран текст. Съвременното криптиране използва сложни математически операции и уникален ключ, с който преобразува информацията ви в шифриран текст. Ключът е това, което заключва или отключва информацията ви. В повечето случаи, ключът е вашата парола.

Какво може да се криптира?

По принцип съществуват два вида данни за криптиране – данни в покой (като например данните на мобилното ви устройство) и данни в движение (като изтегляне на електронна поща или изпращане на съобщение на приятел).

Криптирането на данните в покой е важно за защита на информацията ви в случай че компютърът или мобилното ви устройство бъдат изгубени или откраднати. Съвременните устройства са изключително мощни и съхраняват

Криптиране

огромни количества информация, но също така е много лесно да бъдат изгубени. В допълнение, други видове мобилни носители могат да съдържат поверителна информация, като например USB устройства за съхранение или външни твърди дискове. Криптирането на целият диск (Full Disk Encryption - FDE) е широко използван метод за криптиране, който криптира цялото устройство в системата ви. Това означава, че всичко в системата бива автоматично криптирано, и не се налага да решавате какво да криптирате и какво не. В днешно време повечето компютри идват с FDE, но на вас може да ви се наложи сами да го включите или активирате. На Мак компютрите се нарича FileVault, докато на Уиндоус компютри, в зависимост от версията, можете да използвате Bitlocker или Device Encryption. Повечето мобилни устройства също поддържат FDE. iOS на iPhone и iPad автоматично активира FDE щом бъде зададена парола. Започвайки от Андроид 6.0 (Marshmallow), Гугъл изисква FDE да бъде включен по подразбиране, стига устройството да покрива определени минимални изисквания.

Криптирането е мощен начин да защитите информацията си, но е толкова сигурно, колкото е сигурен ключът ви.

Информацията е също уязвима докато е в движение. Ако данните не са криптирани, те могат да бъдат подслушвани, променяни и записвани онлайн. Ето защо трябва да се уверите, че всяка поверителна онлайн транзакция и комуникация е криптирана. Обичаен метод за криптиране е HTTPS. Това означава, че всичкият трафик между браузъра ви и уеб сайта е криптиран. Следете за https:// в адреса, иконка на катинарче в браузъра, или адресното поле да е оцветено в зелено. Още един пример е когато изпращате или получавате електронна поща. Повечето програми предоставят възможности за криптиране, които вие трябва да активирате. Друг пример за криптиране на данни в движение е между двама души разменящи си съобщение, например в iMessage, Wickr, Signal, WhatsApp или Telegram. Приложения като изброените използват криптиране от край до край, което не позволява на трети лица да имат достъп до данните докато те се трансферират от едно крайно устройство или система до друго. Това означава, че само вие и човека с който си комуникирате може да прочете какво е изпратено.

Как да го използваме правилно

За да сте сигурни, че сте защитени при употребата на криптиране, изключително важно е то да се употребява правилно.

- Криптирането ви е толкова силно, колкото е силен ключът му. Ако някой налучка или се сдобие с ключа, ще има достъп до данните. Пазете ключа. Ако използвате парола за ключа, уверете се че тя е добра и

Криптиране

уникална. Колкото е по-дълга паролата, толкова по-трудно е за злосторник да я отгатне или налучка. Не забравяйте паролата си, без нея ключът ви няма как да декриптира информацията ви. Ако не можете да помните всичките си пароли, ви препоръчваме да използвате мениджър за пароли.

- Криптирането ви е толкова силно, колкото силна е сигурността на устройствата ви. Ако устройството ви е компрометирано или заразено със зловреден софтуер, кибер престъпниците могат да заобиколят всякакво криптиране. Ето защо е толкова важно да се погрижите за това устройството ви да е сигурно, което включва потреба на антивирусен софтуер, добри пароли и редовно обновяване на устройствата.
- Много мобилни и компютърни приложения вече предлагат силно криптиране, за да защитят данните и комуникацията ви. Ако приложението, което смятате да ползвате не поддържа криптиране, помислете си за алтернативно такова.

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

Криптирането обяснено:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Пароли:	https://securingthehuman.sans.org/ouch/2015#april2015
Мениджъри на пароли:	https://securingthehuman.sans.org/ouch/2015#october2015
Какво е зловреден софтуер:	https://securingthehuman.sans.org/ouch/2016#march2016
Защитете новия си таблет:	https://securingthehuman.sans.org/ouch/2016#january2016

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