CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 22.05.2020 г.

Как криптирането може да помогне за защита на вашите чувствителни данни

22 май 2020 г.

Ето как криптирането може да ви помогне да запазите данните си, дори ако устройството ви е откраднато или вашият облачен акаунт е хакнат.

Вероятно съхранявате всякакъв вид чувствителна информация на вашия личен компютър, смартфон или в облака. Вероятно сте си осигурили достъп до устройствата си с парола, биометрични данни или дори комбинация от двете. Това е добре, но какво ще стане, ако загубите устройството си или то бъде откраднато? Именно тогава шифроването е полезно, добавяйки допълнителна защита.

Криптирането не е ограничено само до съхраняване на вашите данни; можете да шифровате и вашите комуникации и уеб трафик, както и паролите си. Всичко това може да се счита за най-добри практики за осигуряване на вашите лични данни. Ето и някои от тях:

Шифроване на диска

Повечето компютри все още имат сменяеми твърди дискове, които не са запоени за дънната платка; или като допълнително място за съхранение хората използват външни дискове. Ето защо шифроването на цял диск е чудесен допълнителен защитен слой; ако вашият диск бъде откраднат, тогава никой няма да има достъп до информацията на него. Дискът ще е напълно криптиран, включително всичките ви данни, софтуер и операционната система, която използвате. Ако не въведете ключа при зареждане, целият ви компютър по същество става неизползваем.

Що се отнася до смартфоните и таблетите, еквивалентната функционалност, която трябва да се търси, е криптиране на устройството и обикновено тази опция е активирана по подразбиране на съвременните устройства.

Облачно криптиране

Повечето от нас използват облачно хранилище заради лесния достъп - можете да го достъпите от всяка точка по всяко време, стига да имате интернет връзка. За съжаление, тази достъпност въвежда набор от предизвикателства. През годините услугите за съхранение в облак претърпяха нарушения в сигурността, дължащи се на

човешка грешка или на целенасочена атака. Следователно, криптирането на вашите файлове, преди да ги качите в облака, е препоръчително.

Дори ако има нарушение или системата на облачния доставчик е компрометирана, данните, които нападателите могат да получат, ще бъдат безполезни за тях без ключа за декриптиране. Можете да избирате от различни продукти въз основа на вашите нужди и предлаганите функции за криптиране. Вижте най-малко тези, които предлагат AES криптиране.

Шифровайте вашия уеб трафик

Един от най-лесните начини да започнете с това е да настроите виртуална частна мрежа (VPN). Нека да кажем, че работите от кафене и ще споделяте някои чувствителни данни с клиент. VPN ще ви позволи да споделяте тези данни в криптирана мрежа, без никой да ги прихваща.

Друг начин да защитите вашата поверителност включва използване на мрежа за анонимност, като Tor. Идеята е, разбира се, да защитите вашата самоличност и навиците си за сърфиране от недоброжелатели.

Друго нещо, за което също трябва винаги да внимавате, е, уебсайтът, до който имате достъп, да използва протокола HTTPS. S означава сигурно и означава, че цялата комуникация между посетителя (вас) и уеб сървъра е криптирана. Повечето от най-добрите световни уебсайтове вече използват HTTPS по подразбиране.

Шифровайте съобщенията си

Що се отнася до приложенията за криптиране на съобщения, имате възможност да избирате и докато най-популярните предлагат криптиране от край до край, не във всички от тях то е активирано по подразбиране.

Можете да шифровате своите имейл съобщения, като изпращачът се нуждае от вашия публичен ключ, за да криптира съобщение, така че само вие да можете да го декриптирате и прочетете, като използвате личния си ключ, и имате нужда от неговия публичен ключ, за да можете да декриптирате шифрованите съобщения, които изпращате на него.

Също така си струва да се обмисли използването на сигурна платформа за електронна поща, като ProtonMail и други, която осигурява криптиране на имейлите от край до край.

Шифровайте паролите си

Мениджърите на пароли са популярен избор за хора, които не искат (или не могат) да запомнят всичките си пароли. Мениджърът на пароли функционира като трезор, който съхранява всичките ви пароли.

Повечето облачни услуги поддържат копие от трезора ви на сървърите си, защитено с надеждно криптиране и за допълнителна сигурност позволяват на потребителите да използват многофакторна автентификация (MFA).

За повече информация:

https://www.welivesecurity.com/2020/05/22/how-encryption-can-help-protect-sensitive-data/