Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

Сигурност в Облака

В този брой

„Облакът“ може да означава различни неща за различни хора, но обикновено означава използване на услуга, предоставена чрез Интернет за съхранение и управление на изчислителни системи и/или данни. Предимството на Облака е, че може лесно да се синхронизират данните между различни устройства навсякъде по света, и също така информацията може да се споделя с когото поискате. Тези услуги се наричат „Облак“, защото често дори не се знае къде точно се съхраняват данните. Примерите за Облачни услуги включват създаване на документи в Google Docs, споделяне на файлове в Dropbox, изграждането на собствени сървъри в Amazon Cloud, съхранение на клиентски данни в Salesforce или архивиране на музика и снимки в Apple's iCloud. Тези облачни услуги могат да ви направят далеч по-продуктивни, но те също така идват със своите специфични рискове. В този бюлетин ще разгледаме как можете да запазите сигурността и да се възползвате максимално от Облака.

Гост-редактор

Дейв Шакълфорд (**@daveshackleford**) е професионален консултант и собственик на Voodoo Security, както и автор на множество SANS курсове, включително SANS Security 579: Virtualization and Private Cloud Security и Security 524: Cloud Security Fundamentals.

Избор на доставчик на Облачни услуги

„Облакът“ не е нито добър нито лош; той е инструмент с който се извършват дейности, както на работа, така и в къщи. Съществото е, че използвайки тези услуги предоставяте собствените си данни на някой друг, като очаквате от този някой да ги съхранява сигурно и достъпно за вас. Именно затова трябва изборът на доставчик на Облачни услуги да бъде направен внимателно. За работните ви компютри или данни, допитайте се до прекия си ръководител, за да разберете дали компанията ви позволява да ползвате Облачни услуги. Ако това е разрешено, проверете кои услуги точно могат да се ползват, и каква е политиката на компанията за ползването им. Ако смятате да използвате Облачна услуга за лична употреба, имайте в предвид следното:

1. **Поддръжка**. Колко лесно е да получите помощ или отговор на въпрос? Има ли имейл адрес на който да пишете, публични форуми за въпроси или секция за Често Задавани Въпроси на уебсайта на доставчика на услугата?
2. **Простота**: Колко лесно е да се използва услугата? Колкото е по-сложна услугата, толкова по-вероятно е да се допуснат грешки и без да искате да изложите информацията си на показ или да я изгубите. Изберете доставчик,

Сигурност в Облака

чиято услуга ви изглежда лесна за разбиране, настройване и употреба.

3. **Сигурност**. Какви данни се изискват относно вас самите? Как данните ви ще бъдат пренесени от вашия компютър към Облака и как се съхраняват в Облака – криптирани ли са, и ако да, кой може да ги де-криптира?
4. **Условия за ползване**: Отделете време да прегледате Условията за Ползване (те са често изненадващо лесни за четене). Проверете кой може да има достъп до данните ви и какви са законовите ви права, както и какви са отговорностите на доставчика относно сигурността – предоставени от доставчика или като ваше изискване.

Облакът може да направи информацията ви по-достъпна и вас самите по-продуктивни, но бъдете внимателни как ползвате и споделяте информацията си.

Защита на данните ви

След като веднъж изберете Облачен доставчик, следващата стъпка е да се уверите, че употребявате услугата правилно. Това как достъпвате или споделяте данните си често може да има много по-голямо влияние върху сигурността на файловете ви отколкото всичко друго. Някой ключови стъпки, които можете да предприемете, включват:

1. **Удостоверяване**: Използвайте силна, уникална парола за удостоверяване в облачния си акаунт. Ако доставчика предлага удостоверяване в две стъпки, силно ви препоръчваме да го включите. Това е една от най-важните стъпки, които можете да предприемете, за да защитите акаунта си.
2. **Споделяне на файлове/папки**: Облакът прави споделянето много лесно, понякога твърде лесно. В най-лошия случай, може да си мислите, че споделяте данните с определен човек, но може по погрешка да направите файловете или дори цели папки публично достъпни за целият Интернет. Най-добрият начин да се защитите е да не споделяте нищо с никого по подразбиране. В този случай давате само на специфични хора (или групи от хора) достъп до конкретни папки само ако имат нужда от това. Когато няма повече нужда от нечии достъп до файловете, премахнете достъпа. Доставчикът на услугата трябва да предоставя лесен начин да следите кой има достъп до файловете и папките.
3. **Споделяне на файлове/папки с връзки**: Една обичайна функция на някои облачни услуги е възможността да създавате уеб връзки, сочещи към данните или папките ви. Тази функция ви позволява да споделяте тези файлове с всеки, като просто предоставяте адреса на връзката. Този начин предоставя много малко сигурност, тъй като всеки, на когото е известна връзката може да получи достъп до файловете или папките. Ако изпратите връзката на само един човек, този човек може да я сподели с други, или връзката може

Сигурност в Облака

да се появи в резултати от търсене. Ако споделяте данни с връзка, уверете се, че връзката ще бъде спряна, когато вече не е нужна, като зададете срок на годност или защитите връзката с парола.

4. **Настройки**: Разучете добре настройките за сигурността, предоставени от доставчика на услугата. Например, ако споделите папка с някой друг, този някой може ли да я сподели с някой друг без вие да знаете? Също така проверете дали има начин да проследите кой и кога е преглеждал споделеното от вас. Можете ли да ограничите споделянето да е „само за четене“ вместо „четене и писане“, където второто би означавало, че други ще могат да ви променят файловете?
5. **Антивирус**: Уверете се, че имате последната версия на антивирусния си софтуер инсталирана на компютъра си, както и на всеки компютър, използван за споделяне на данните ви. Ако споделен от вас файл бъде заразен, други компютри с достъп до този файл могат също да бъдат заразени.

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

Удостоверяване в 2 стъпки:	https://securingthehuman.sans.org/ouch/2015#september2015
Пароли:	https://securingthehuman.sans.org/ouch/2015#april2015
Управление на пароли:	https://securingthehuman.sans.org/ouch/2015#october2015
Зловреден софтуер:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

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

