CYBER RISKS & LIABILITIES_
NEWSLETTER

October / November 2014

IN THIS ISSUE

Securing Your Files in Cloud Storage
Storing files in the cloud is easy and convenient—but definitely not risk free.

Shellshock Bug Poses Serious Threat
A new software bug has been discovered with the potential to harm half-a-billion machines.

Recent Cyber Security Fines
Do not make the same mistakes as these cyber security slackers.

Securing Your Files in Cloud Storage

Cloud storage—a service that allows you to upload documents, photos, videos and other files to a website in order to share those files with others or for backup storage—is proliferating across the Internet. Users can access their files stored in the cloud from any location on any type of device. The ease of use is unrivalled. But a quick glance at recent newspaper headlines shows that storing files in the cloud—especially sensitive files—is not without risks.

For example, in late August, an anonymous hacker extracted private, nude photos of several major celebrities from Apple's online iCloud storage service. Because the celebrities had synced their iPhones with their iCloud storage, any photos they took on their phones were automatically saved in the cloud. Apple believes that the hacker either correctly answered security questions or used a phishing scam to breach the celebrities' accounts.

The message is clear: anything saved in the cloud is vulnerable. After all, storing files in the cloud just means that you are storing them on servers controlled by the service provider (such as Apple, in the case of the celebrity photo leak). Therefore, if you choose to store your business' files in the cloud, check that the security and availability is right for the types of files you want to upload. When considering whether to upload files to a cloud storage service, ask yourself the following questions:

- **Who can access my files?** Cloud storage services will usually allow users to set one of three privacy controls: private (only you can view the files, although the cloud storage provider may be able to view them, too), public (everyone can view the files without any restriction) and shared (only people you invite can view them). Choose the privacy control that matches the sensitivity of your files.
- **What is my password?** Access to your files will be controlled by your username and password, so choose a strong, unique password. Never use the same password across more than one site, as this severely compromises your security.
- **What are the storage provider's terms and conditions?** Reputable cloud storage providers should have clear, transparent information describing how they secure your information. If you cannot find it or feel the terms are unclear, shop around with other providers.
- **What types of encryption does the provider offer?** Encryption adds a further layer of security, rendering your files illegible unless the user has the decryption key. Some cloud storage providers encrypt files on your behalf.

Packetts

Shellshock Bug Poses Serious Threat

Cyber security experts recently discovered a new software bug with the potential to harm millions of computers, servers and devices around the world. The bug, named Shellshock, has been found in a software component known as Bash (Bourne Again Shell), which is a part of many Linux systems, as well as Apple's Mac operating system.

Hackers can use Shellshock to remotely take control of almost any system that uses Bash, including potentially commandeering the operating system, accessing confidential information and making unauthorised changes, according to industry researchers. And these same researchers are warning that Shellshock is much more serious than the Heartbleed bug, which caused a huge stir after being discovered in April 2014.

According to the BBC, about 500,000 machines were estimated to have been vulnerable to Heartbleed. This pales in comparison to Shellshock's reach—industry experts' early, conservative estimates suggest that Shellshock could strike at least 500 million machines.

As of 25 September 2014, there have been no reports of attacks exploiting the Shellshock bug, but experts believe it is only a matter of time until they emerge—numerous cyber security experts have rated the Shellshock bug a severe threat for its ability to inflict damage, but 'low' for its complexity, meaning it is a serious but relatively easy vulnerability for hackers to exploit.

In the meantime, industry experts recommend that anybody with systems that use Bash should deploy patches immediately. For business owners with small networks or home users, experts recommend monitoring the websites of their machines' manufacturers for updates and patches. Manufacturers will often seek to provide customers with the latest news and patches to lessen their machines' vulnerability.

However, some security researchers are warning that the current patches are incomplete and cannot fully secure systems. Therefore, a constant monitoring of the situation is the key to discovering effective patches.

£180,000 fine for the Ministry of Justice

The Information Commissioner's Office (ICO) fined the Ministry of Justice £180,000 for serious and repeated failings in properly handling prisoners' information. The latest failing stems from the May 2013 loss of a backup hard drive at HMP Erlestoke prison in Wiltshire. The hard drive contained sensitive and confidential information about almost 3,000 prisoners, including details of links to organised crime, health information, history of drug misuse and material about victims and visitors. The device was not encrypted. A similar case happened in October 2011, when another unencrypted hard drive containing the details of 16,000 prisoners at HMP High Down prison in Surrey was lost.

Racing Post signs undertaking after breach

The ICO is warning businesses that they must be prepared for a targeted cyber attack, using the Racing Post, a daily horse racing newspaper, as an example. In October 2013, the Racing Post's lax cyber security allowed a hacker to penetrate the newspaper's online customer database and compromise 677,335 accounts. The information compromised included names, addresses, passwords, dates of birth and telephone numbers. An ICO investigation discovered that the Racing Post had carried out security testing on its website in 2007, but it failed to apply security patches since then, leaving a gaping security hole easily exploited by the hacker. The Racing Post has since signed an undertaking committing the company to improve its compliance with the Data Protection Act.

Reading colleagues' bank accounts prove costly

A Birmingham banker was fined £880, plus £440 in costs and an £88 victim surcharge after he admitted to reading his colleagues' bank accounts. The 29-year-old banker worked in Santander UK's suspicious activity reporting unit in Leicester. His role investigating allegations of money laundering meant he was able to view customer accounts. But he also used his access to spy on 11 colleagues' accounts to learn how much their salaries and bonuses were.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Packetts
Salts Wharf, Ashley Lane
West Yorkshire, BD17 7DB
01274 206 500
http://www.packetts.com