COMPUTER NEWS from the

Titusville Computer Community

TCC

Titusville, FL

AUGUST 2015 Volume 3 NO. 8

As found on the web and other sources

NOTE from the editor, A little heavy on security this month

4 Ways Cloud Usage Is Putting Health Data At Risk

By *Jai Vijayan in Darkreading.com*

A huge shadow IT problem is just one of the risks of uncontrolled cloud usage in healthcare organizations, new study shows.

The prolific manner in which healthcare workers use cloud services for storage and collaboration purposes poses a huge and growing threat to health data.

An analysis of cloud service usage of over 1.6 million employees at healthcare providers and payers by Skyhigh Networks shows that a vast majority of healthcare organizations are only dimly aware of the extent of cloud service usage by employees.

Even though healthcare organizations are tightly regulated and the risks to patient health information are well understood, employee behavior with regard to cloud usage is no different from any other sector, says Rajiv Gupta, CEO of Skyhigh.

"You might think because an industry is regulated, things are more locked down," he says. But the opposite is true, he says. Healthcare workers use un-vetted cloud services to share and collaborate with sensitive health information on a scale that most organizations are completely unaware of, he says.

"The amount of data going from an average healthcare organization to the cloud each month is more than the amount of data in all of Wikipedia's databases."

Here are four ways the trend is putting sensitive patient health data at risk:

The Shadow IT Problem

A lot of the cloud services used at healthcare organization happens outside the IT group's purview or their knowledge. The Skyhigh analysis showed that workers at the healthcare organization use over 920 cloud services in the workplace. Yet, the IT organization itself is typically aware of only about 60 of them.

That means on average over 860 cloud services are being used to share, store, and collaborate on health data that IT has no idea about. The risk posed by such shadow cloud services is enormous, Gupta says. "It's surprising how far the industry is in their understanding and assessment of the potential for compromise."

Consumer Grade Services

A vast majority of the cloud services that healthcare employees use for work-related purposes is consumer grade and offers little to none of the security controls needed to properly protect sensitive patient health information (PHI).

Skyhigh found that the average healthcare organization uses over 180 collaboration services, including those like Office 365, Evernote, and Gmail. Other popular services include those used for development purposes like GitHub and SourceForge, content sharing services like LiveLeak, and file-sharing services like Dropbox and Google Drive. On average each employee uses 26 distinct cloud services.

Yet, a bare 7 percent are enterprise ready, less than 15 percent support two-factor authentication, and 9.4 percent support encryption of data at rest.

Huge data volumes

The healthcare organizations that Skyhigh considered for its analysis uploaded an average of 6.8 terabytes of sensitive data to the cloud each month, a lot of it without IT's knowledge.

Such data is increasingly of interest to malicious attackers. The intrusions at Anthem, Community Health Services and Premera Blue Cross over the past several months have highlighted the growing value of healthcare data to cybercriminals. A complete health record with a social security number in fact now can fetch 20 times the price of a stolen credit card, according to Skyhigh.

In addition to the risks posed by malicious attackers, organizations may be at risk in other ways as well, Gupta says. Some cloud services, for example, require users to consent to terms and condition that basically give ownership of the data to cloud providers. Many cloud services also track users for targeted ad delivery purposes. Such services can sometimes be co-opted by cybercriminals and used for more malicious purposes, he notes.

Hiding Risky User Behavior

The massive use of cloud services by healthcare workers makes it relatively easy for malicious insiders to conceal illegal behavior, Skyhigh said in its report. In many cases, healthcare organizations have no way to detect intentional or unintentionally risky behavior in the cloud. Not surprisingly, though, 79 percent of healthcare organizations had behavior indicative of an insider threat, only 33 percent actually detected it.

The incidence of potentially malicious, negligent or risky behavior by users in the cloud is much higher than organizations assume, Gupta says.

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio

---

Lock Down Your WiFi Router

Category: Security From "askbobrankin.com".

While we've been focusing on the security of our desktop PCs, laptops, and mobile devices, malware-manufacturing miscreants have been exploiting the most overlooked computer in most homes and businesses: the router. Here's what you need to know…

Is Your Router Secure?

For those who have high-speed Internet, the router is the little box that connects your home or office to the Internet. And they are the latest target of the online criminal classes.

A legion of hacked consumer-grade routers were used to launch distributed denial-of-service (DDoS) attacks that brought Sony and Microsoft gaming networks to a halt over the last holiday season.

And now, according to researchers at the Fujitsu Security Operations Center, hundreds of hacked routers are being used to distribute malware that steals login credentials by redirecting browsers to rogue websites that imitate financial institutions.

AskBobRankin.com

A router can be compromised by changing its settings. For instance, substituting a hacker's rogue DNS server address for that of a legitimate DNS server would redirect browser requests to a fake website. But a router can also be remotely reprogrammed with firmware that includes malware and instructions for distributing it, turning the router into a slave in a botnet.

It's unsettling that the researchers are not sure how bad guys are gaining control of routers. They speculate that users are to blame for not changing the factory default administrator login credentials when they set up their routers. Most often, the default credentials are published online; always, they're simple and easily guessed. But I can't lay all the blame on users.

Configuring the Router

Hardening your router's security is important, but don't neglect the other machines on your network. You may want to review my earlier article, Avoid These Five WiFi Security Mistakes.

Certainly, the first thing you should do when installing a new router is change the administrator's use rid and password to something that only the administrator (which is probably you) knows. Conventional wisdom says the password should be long and complex, but that really isn't necessary if you make one other simple change to the router's settings.

Most routers are shipped with “remote administrative access” or “remote management access” enabled by default. That means the administrator can log in to the router from any device connected to it. That’s convenient for admins but dangerous.

Disabling remote administration means that the admin must log in via a hardwired connection between the admin’s computer and the router’s Ethernet port. It doesn’t matter if your use rid is “admin” and your password is “password.” Only someone who has physical access to the router can log in and fiddle with its settings or install new firmware.

In a home or small office, it should be easy to control who can plug an Ethernet cable into the router. But to protect against an “inside job,” the admin’s login credentials should still be changed to something non-obvious. I've visited coffee shops and motels with wifi routers that were completely unprotected. If I was malicious or mischievous, I could have logged into the router and changed the settings so that anyone who tried to access a website would be redirected to an inane cat video on Youtube.

Even if you doubt that your family, guests, or employees might hack your router, it’s entirely possible for their devices to be infected with malware that will attack a router. Denying admin access to the router foils such attacks, even if they come from machines that are connected to your local network.

I can't give specific instructions on exactly how to login to your router and change settings, because each model has a different interface. But the first step in every case is to find the address of your router. On Windows, open a Command Prompt, then enter the **ipconfig** command. The output will look something like this:

```
IP Address. . . . . . . . . . . . : 192.168.1.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . : 192.168.1.1
```

Look for the "Default Gateway" line, and you'll find the router address there. (Mac users can click the Apple icon, then “System Preferences” and “Network”. Your default gateway will appear next to “Router”.) So in this case, you'd open your browser and enter http://192.168.1.1 in the address box. You should be greeted with a prompt to enter your router's login and password. If you don't know the router's username and password, check with your Internet service provider.

NOTE: Your router's username and password is NOT THE SAME as your wifi password. The former allows access to your router's configuration screens, while the latter allows you (and others who know the password) to access the Internet via wifi.

For Extra Credit…

Here are a few other steps you can take to improve the security of your wifi router:

Switch to OpenDNS, an alternative to the DNS servers from your Internet provider. See my article OpenDNS - Faster and Safer Internet for details on how this can improve security, and how to make the change.

Change the router's SSID (network name) to something of your own choosing. Your router's SSID is broadcast to others nearby who are searching for wifi networks. Often the default name is "linksys" or something else that gives away the make or model of your router. That only makes a hacker's job easier.

Consider updating your router's firmware. Think of this as the operating system that controls your router. After logging into your router, look for an option called "Firmware Upgrade" or similar. On my Verizon FIOS router, there's an option to automatically check for available firmware upgrades, and even install them automatically. But those are turned off by default. Check with your Internet provider first if you have questions about where to download updated firmware.

Is YOUR wifi router secure?

..

Facial Recognition: Should Permission be Required?

BY John Lister on June, 17 2015 in “infopackets.com”.

Plans to draw up guidelines for how firms use facial recognition technology have fallen apart after civil liberties groups withdrew from talks. They say businesses aren't making a serious offer at an acceptable compromise.

Businesses and consumer groups have been taking part in facial recognition guideline talks since early last year. They've been organized by the National Telecommunications and Information Administration (NTIA), a government agency. The idea behind the talks was to avoid the need to draw up and implement legislation, something that could be politically tricky.

The talks have covered a range of issues dealing with how companies store, use and share information they've gathered by using facial recognition, whether from photographs such as on social media sites, or from images captured by security cameras.

Facial Recognition Now Very Viable

The debate has become much more important in recent years because of the growth in computer processing power. While humans are hard-wired to recognize faces, **it's a surprisingly difficult task for computers**. That's because, while a computer can carry out tasks extremely quickly and meticulously, they aren't as good at humans at using instinct and intuition to take "shortcuts" when assessing imagery.

That's changed with both faster computers generally and the ability to use remote **"cloud" processing** that makes it much more efficient to access immense computing power only as and when its needed. It's now much more practical for a business to scan security footage and identify somebody on the spot. One company that works with casinos says each of its servers can check images at a rate of one million comparisons per second. (Source: **bostonglobe.com**)

Point Of Principle Divides Sides

Despite the lengthy discussions, it appears the process has collapsed over a central issue: whether or not organizations should have to get explicit consent before using a person's image for facial recognition with the purpose of identifying them by name.

Businesses argue that in some circumstances this simply isn't practical, for example when trying to identify a known shoplifter when they enter a store.

The consumer groups argue that getting permission in every case is a basic principle and the absolute minimum they could accept from any agreement. They note that Illinois and Texas already have laws to this effect.

The groups also say that the businesses refused to even agree to a compromise of requiring them to get permission in specific circumstances such as where security wasn't an issue. (Source: **nytimes.com**)

What's Your Opinion?

Are you concerned about companies being able to almost instantly identify people by their face using security camera footage? Should they have to get permission before doing so, or would this undermine security? Do you think this issue can be resolved through further talks and, if not, should legislators take action?

What is a SIM CARD?

Subscriber Identity Module (SIM)

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking.

Though for the month

We are here on earth to do good unto others. What the others are here for, I have no idea.
~ W.H. Auden