Q-News

A Quanexus Publication

November 2016

Yahoo is Dealing with a Lot of Security Issues

Yahoo recently suffered a breach that exposed over a 500,000 email addresses, user IDs and passwords. They removed their email forwarding feature and have been caught scanning users emails.

Yahoo had a breach and over 500,000 email user IDs and passwords were stolen back in 2014. It is also estimated that the actual number may be closer to 1 billion accounts that were compromised. Yahoo performed

(Continued to page 2)

Inside Q-News

The Quanexus Newsletter

by Jack Gerbs

Ransomware continues to be an issue for many companies. While it is important for companies to implement technical controls and try to prevent ransomware from getting into their environment, it is just as important to train staff on how to identify and prevent the organization from becoming a victim. A large Urology group based in Central Ohio was recently hacked. Over 300,000 employee and patient records were stolen. Yahoo in the news! Yahoo had over 500,000 user email addresses, ID's and passwords stolen. If that wasn't bad enough, they blocked their email forwarding feature and was caught scanning their clients email. The Internet of Things (IoT) continues to grow. It is estimated that there will be over 6.4 billion devices connected by the end of 2016 and over 60 billion by the end of 2020. Many of these IoT devices are built and sold with poor or no security implementation. There were two recent, major attacks that leveraged IoT devices, and the latest, took down the Internet for a major part of the East Coast. Compliance continues to create new challenges for many of our clients. Depending on the industry you are in, privileged access to the network either currently or soon, will require two-factor authentication.

Central Ohio Urology Group Hacked

Central Ohio Urology Group (COUG), based in central Ohio, is one of the largest urology groups in Ohio. They have 28 urologists working with major hospitals. COUG reported that they were breached in early August. The breach affected 300,000 victims. Information stolen includes: complete patient medical records, complete employee records and internal emails. Detailed information includes: name, address, telephone number(s), email, birthdate, Social Security numbers, driver's license/state identification numbers, patient identification numbers, medical and health plan information, account information, diagnosis and treatment information, health insurance information and identifiers, employment-related information, and internal information including risk assessments, policies, etc.

The attack came from a group of Ukrainian hacktivists (activists) who moved the files to a Dropbox account and then to a Google Drive account where they freely distributed all of the stolen information. A total of 223 GB of data was stolen.

The group claims the reason for the attack was for retaliation against alleged drug experiments conducted in several Ukrainians cities. The attack was to serve as a warning to the US that this type of behavior won't be tolerated. What is strange about this breach is, COUG allegedly has no connection with the experiments the hacktivists are claiming.

Yahoo is Dealing with a Lot of Security Issues

(Continued from page 1)

major updates to their systems. One of those updates removed the ability to have your yahoo emails forwarded to another email account. This feature is often used if you have multiple accounts and want to forward mail from one account to another to make life easier. This feature is also often used when someone wants to change email service providers and maintain the old account until everyone has had a chance to update their new email account and contact information. After the breach, there are/were many who are considering leaving Yahoo, and without this feature it would make it difficult to easily leave. On Friday, October 14th in a blog post, Yahoo has announced that the email forwarding feature has been re-enabled.

Last year, the FBI and NSA asked Yahoo to scan all user emails for specific content. It is unknown what information was released to the two agencies. The decision was made by their CEO Marissa Mayer, without the knowledge of their Chief Information Officer (CIO) Alex Stamos. Alex left the company because of this decision and is now with Facebook. Yahoo implemented the content filtering solution without notifying their security team. The monitoring tool was quickly discovered by the security team, because it looked like they had been hacked. This is the largest broad demand for real-time web collection of data.

Verizon is in the process of acquiring Yahoo for $4.9 billion. In light of this breach, Verizon is now renegotiating the deal. Verizon believes the breach has caused a material impact on the value of Yahoo.

Ransomware Continues to be a Big Problem

As much as I write about ransomware, there still appears to be a lot of users clicking on attachments that contain files that infect their system. There is a new strain of ransomware that is getting through firewalls and email clients that contain Windows Script Files (WSF).

While there is a lot that can be done to prevent ransomware, there are no guarantees that your systems won't be affected. Ransomware is malicious software that encrypts the files on your computers and server. It then demands a ransom to be paid in order to get your files back. For small organizations, the ransom is typically $800 to $1,500. For larger organizations the ransom can be as high as $10,000 to $30,000. Some recent ransomware attacks that made the news include The University of Calgary which paid $20,000 and the Presbyterian Medical Center, based in Los Angeles, who paid $17,000.

The most effective way for criminals to spread ransomware is through email attachments. These emails appear and look like they come from legitimate organizations such as a bank, the US Postal Service, Federal Express (FedEx) and other organizations or businesses with whom you may regularly work with. Bottom line, they try to make the messages look legitimate and the goal of the email is to convince the recipient to click on a link or open an email attachment.

Malware and ransomware are now being spread with the use of USB infected memory sticks that are now being delivered through the mail, to potential victims.

To keep yourself protected from ransomware follow these basics:

- Keep your system (operating systems and applications) patched.
- Keep your Antivirus/malware solution up to date.
- Macros for Office Applications should be turned off, if not needed.
- Use a good firewall with Unified Threat Management features.
- Segment the network; isolate workstations from the server network.
- Beware of phishing attacks, don't open emails that you are not sure of.
- Train your users on network security issues including how to spot potential threats and how to report them.
- Disable the auto run feature on USB ports and do not insert unknown USB devices into your systems.

The Internet of Things (IoT) Vulnerability

The Internet of Things often referred to by people in the industry as un-patchable things, is a new category of equipment that is being installed in many homes and businesses. This includes equipment such as: video surveillance systems, home automation and security systems, routers, thermostats, garage door openers and devices that are plugged into a user's home network and are accessible via the Internet.

Gartner estimated that there will be 6.4 billion devices connected to the Internet worldwide in 2016. This is up 30% from 2015. Most IoT devices have a 12-year-old known vulnerability from OpenSSH. The vulnerability is SSHowDowN Proxy (CVT 2004-1653). This vulnerability allows attackers to take over your device and use it in distributed denial of service attacks (DDoS) against a legitimate network. Last month, there was a 620 Gb/s DDoS attack against Brian Krebs "Krebs on Security blog".

The good news is this attack runs from RAM. To remove the malicious code from the infected device, all you have to do is reboot it. The most effective way to prevent having your system infected is to change the default user ID and password. The unfortunate news is, companies that are creating these devices are not maintaining them and updating the firmware. There are also many devices out there that don't allow the user to change the default user ID and password. These types of threats were considered by the security community in the early days of IoT, and are now coming to fruition.

Two Factor Authentication Becoming More Affordable

Two-factor Authentication, also known as TFA or 2FA, is a two-step authentication process used to log into a network or network service. Single factor authentication is what most of us use every day, which is typically just a password. TFA requires two of the following: something you know (password), something you have (a token/key fob with numbers that change or a response on a smart phone) or something you are (bio-metrics, eye scan, finger print, and maybe a DNA sample in the future).

If you work in an environment that is under regulatory compliance, such as the financial industry, medical, government, etc. you are or soon will be required to have, at minimum, your privileged account users logging into the network with TFA. A privileged account user is a user with network administrative permission.

Quanexus has recently partnered with DUO Security to provide TFA solutions. DUO can work with a token device or a smartphone. When a user attempts to log into a system with their user ID and password, a message is sent to the user's smartphone and waits for a response from the smartphone before letting the user complete the login process. There are other configurations for DUO, but the Smartphone integration seems to be the most popular.

Backup Internet Access

Quanexus is partnering with a local company to provide wireless Internet access in the Dayton area. The available options are 10M/10Mb/s or 30/30Mb/s and one static IP address is included. This is an ideal solution if:

- You are unable to get Internet access at your facility because of a lack of carrier infrastructure.
- Need a backup Internet pipe, should your primary carrier go down.
- Looking for an alternative to standard cable/connected Internet access.

This service is not available in all areas.

Largest Internet Outage Caused by a Denial of Service Attack

As I am finishing up this newsletter, the East coast was hit with the largest Internet service interruption to date. DynDNS is a DNS service provider for many large organizations. DynDNS was hit on October 21st with a Distributed Denial of Service (DDoS) attack. DNS (Domain Name Services) maps URLs to IP addresses. When you surf the Internet you type in a URL that looks like, for example, www.quanexus.com, www.box.com, or www.spotifiy.com. Before your request can be fulfilled, the URL needs to be resolved to an IP address which is the job of DNS.

A distributed denial of service attack is caused by many systems on the Internet all sending an overwhelming amount of traffic to the victim. On October 21st, the victim was DynDNS. DynDNS provides services for many popular companies such as Twitter, Spotify, Reddix, Box, Github, PayPal, Wired.com, Pinterest and more.

Ironically, I had completed the previous article about known vulnerabilities with IoT devices the day before this incident with DynDNS. While the exact circumstances are not known, it is suspected that many of the devices involved in this attack were classified as IoT. The attack generated over 1 Terabit per second traffic (Tb/s) aimed at DynDNS. A Terabit is a number with 12 zeroes (1,000,000,000,000). The figure below is a screen shot of Level 3's outage map based on the attack.

For a fixed monthly fee, we are revolutionizing the IT industry with our Q-Works program. Quanexus' complete "managed services" package means that you will see increased performance, security, and reliability immediately, at an affordable price.

Your business success depends on your IT infrastructure. You need Quanexus to deliver proactive services that not only keep your network up and running, but running effectively and efficiently.

Quanexus®
We make IT easy.

571 Congress Park Dr.
Dayton, Ohio 45459
937 885-7272
info@quanexus.com

Create a Security Conscience Team

Today's employees are frequently exposed to sophisticated phishing and ransomware attacks without even realizing the consequences. More than ever, your users are the weak link in your network security.

Security Awareness Training is a formal process of educating your team about computer security. A good security awareness program should educate employees about the corporate policies and procedures for working with IT. Employees should know what to look for in emails, how to hover over a link to check who the real sender is and if a security threat has been unleashed, what is the procedure for reporting and dealing with the vulnerability?

Communicating cyber- security priorities is no longer just an IT job. It requires a tone at the top. Those of us leading the company must ensure that employees appreciate the cybersecurity risks, understand the risk tolerance, and support agreed-upon mitigation strategies. Business enablement often trumps security in the interest of going to market quickly, and only business leaders can ensure that checks and balances are in place to hold management and employees accountable.

Applying the human factor can be difficult in companies today because of the shortage of qualified information security professionals. One leading practice that many of our clients have adopted is to optimize their existing resources and outsource some of the expertise and operations to a company such as Quanexus. With a Certified Information Systems Security Professional (CISSP) on staff, Quanexus can provide training to help your team both at work and personally.