Q-News

A Quanexus Publication

June 2016

The Quanexus Newsletter

by Jack Gerbs

Ransomware continues to grow and we have seen a few clients suffer from it. Fortunately, all of them had good backups and we were able to quickly recover the infected workstation and the affected servers. In this newsletter, I have written several articles addressing ransomware and what can be done to minimize your chance of it getting into your systems. The key to keeping your systems safe is to keep them patched, prevent potentially malicious email from getting to your users and keeping your users trained on how to identify emails that might contain malicious code. Quanexus has recently partnered with KnowBe4 to offer social engineering security awareness training. Last month MySpace, a very popular on-line social network (similar to Facebook), was hacked and 427 million passwords were stolen. This breach highlights the scary issue of password reuse. Companies should have a policy that states "Users are not permitted to use a password that they use for personal accounts".

Ransomware and Social Engineering

We are seeing more and more companies being affected by ransomware. If you have not heard of ransomware, it is bad stuff. Ransomware will encrypt files on the infected computer. If the infected computer is attached to a network, it can also infect all the files on the server. These encrypted files cannot be accessed unless you pay a ransom (fee) to unencrypt your files.

The most common way computers get ransomware is by opening or previewing attachments in emails. These files contain macros (scripts) that download and execute the malicious code. If you use a mail filtering service, which we offer as part of our Q-Works platform, it can be configured to filter out many of the potentially dangerous files. There are tradeoffs when applying mail filtering rules. Emails that are sent to you from outside organizations may be blocked as a result of this technology. Our email filtering recommendations are:

- Executable files attached in emails should be treated as SPAM.
- Image files should be treated as normal files.
- Video files should be treated as normal files.
- Archived (e.g. zipped) files should be treated as SPAM.
- Password protected files should be treated as normal files.
- Macro-enabled files should be treated as a virus.
- Scripting files should be treated as a virus.

Description of email filtering:

- Normal files are those files that get delivered to the user's email inbox.

(Continued on page 2)

Quanexus – DBJ Best Places to Work Honoree

The Dayton Business Journal recently celebrated Dayton's 2016 Best Places to Work at the Schuster Center, and named Quanexus as an Honoree. This recognition is especially meaningful because results are based on surveys returned by our most important assets, our employees. Quanexus was honored to be recognized as one of the top area companies with some of the best office culture and best talent in the region. On top of those traits, we also know how to have fun!

Inside Q-News

Social Engineering Training

With so many threats out there, it is becoming extremely important that your users be trained on how to recognize potentially harmful emails. Quanexus has recently partnered with KnowBe4 to offer a social engineering security awareness training product. This training consists of on-line videos that users watch and are tested on the material. The service also includes a phishing tool kit that we use to send out a monthly phishing email to test which users are opening up suspicious emails. From data gathered from the phishing tests, we can then adjust the training to assist users on how to recognize and report suspicious activity.

What makes this solution very effective is the monthly, or if needed more often, phishing attempts directed toward the user. This brings heightened awareness of the threat landscape through continuous training. For more information on pricing and to determine if this might be a good fit for your organization, please give us a call.

KnowBe4
Human error. Conquered.

Ransomware and Social Engineering

(Continued from page 1)

- Spam files are stored in the user's on-line quarantine folder. Users get a daily email with a description of email that has been quarantined. Users can go to the quarantine and release the specific messages. It is extremely important that the user understand that opening attachments from the SPAM quarantine most likely is some form of malicious code.
- Treat as virus, these messages are dropped and the user gets no notification of the message ever existing.

Before implementing this type of filtering, it is important to understand that emails with attachments may be dropped or put into your quarantine box, and they will not show up in your inbox.

If you have a need to share files with clients, we recommend using other services such as Box.com, ShareFile or Dropbox.

Even with the best technology implemented, there is a chance of ransomware getting into your network. It is essential that you have a solid backup solution to be able to recover lost files.

427 Million Passwords Leaked

Late last month, MySpace was breached and had 427 million passwords stolen. If you ever had a MySpace account, you could be one of the many victims, even if you have not logged into MySpace for many years. In my security awareness trainings and in previous articles, I preach the issue of password reuse. You should not use personal passwords for your business accounts. Ideally you should not use a password for more than one account, but that is too challenging for most of us.

The significance of this breach brings to light the tremendous issue with password reuse. Password reuse is the use of one password for multiple accounts. With the bad guys now having access to your old MySpace account means, if you are still using that same password on other accounts, the bad guys now have your password. For example, if you use the same password for MySpace as you use for Amazon, banking or other on-line sites, you are now vulnerable. The password database is being sold on the black market underground. The bad guys buying the list will be using social media sites such as Facebook, LinkedIn etc. to learn more about you. From information that we freely share, they can determine who you work for, what city you live in, your shopping habits and what banks are in your neighborhood.

If you ever had a MySpace account and you still use that same old password, it is now time to change your password on all your accounts, especially for on-line banking, Amazon & PayPal accounts, etc.

(Continued to page 4)

Upgrade Your Operating System, Replace Your Computer and other Tough Questions

The never ending question, should I upgrade my computer to Windows 10? What I still find pretty amazing is there are many users who are still using Windows XP. Windows XP was officially dropped by Microsoft on April 8th, 2014. That is over two years ago. As I've mentioned many times, running an obsolete operating system makes that computer vulnerable to malicious code (viruses and malware). For the small business and the end user, the worst type of malware you may be hit with is ransomware. Ransomware encrypts the data on your system and requires you to pay a ransom (fee) to get your data back. If you don't have a complete backup and you don't pay, there is an excellent chance you will lose all the data on that system. Even worse, if the infected computer is connected to a network, it is very likely the files on the server will be encrypted. Many users fear that if they do pay the ransom, they might not get their data back. I have not heard of an instance where the data was not returned to the victim. If it got out that the bad guys were not making good on their promise to restore your files, the effectiveness of their whole scheme would lose value. ***I do not advocate paying any ransom!***

I do advocate running current operating systems and current versions of software, and keeping them properly patched. What is of most value is not the computer, but the data on the computer. The computer is just a box of hardware and can easily be replaced. On the other hand, the data on the computer is what users really care about and often times, might be very difficult if not impossible to replace.

Determining if you should upgrade your computer involves a few simple questions:

- How old is your computer?
- How much memory and what is the processor in your computer?
- Is the computer experiencing any issues?

If your computer is over 4 years old, it has most likely served you well and you should consider replacing the computer vs. upgrading it. If it is a home computer, this may cost you about $500. If it is a business class computer, you could expect to spend about $850 for a new system with a new operating system and application suite.

If your computer has less than two gigabytes of memory or a slow processor, you should consider replacing the system.

If the computer is having issues, you need to determine if the issues are hardware related or software related. If they are hardware related, replace the system. If they are software related considering installing a clean version of the new operating system vs. performing an upgrade.

A few words of caution; while our experience has been very successful with upgrading clients to Windows 10,

(Continued to page 4)

Frustrated with your Home Computer?

We have had many inquiries about providing IT support for home users. Consumers become frustrated with attempting to call an 800 number somewhere in the world, hanging on the phone for long periods of time and still not getting the help that they need.

Quanexus has come up with a solution for home users that want to deal with a trusted local company - **Q-Works for Home**.

Whether you are looking to set up, secure or repair your computer, Quanexus has the know-how to help. With 24 years in business and an A+ rating with BBB, you can trust and count on our knowledgeable IT technicians for in-home service.

- Computer Set-up
- Data Backup or Transfer
- Email/Printer Set-up
- Wireless Set-up
- Hardware installation or repair
- Data Recovery
- Virus/Spyware removal

If you prefer ongoing support, for a low monthly fee **Q-Works for Home** offers an option that includes:

- Remote Support by phone
- AVG Anti-Virus
- Unlimited monthly updates
- Discounted in-home service

Give us a call at **937 885-7272** to discuss pricing or schedule a visit.

Upgrade Your Operating System, Replace Your Computer and Other Tough Questions

(Continued from page 3)

there are a few things that must be considered. The applications on the computers must be supported by Windows 10. We have seen a few applications not supported by Windows 10. We have also seen a few applications that need to be fully uninstalled, before an upgrade is performed and then reinstalled.

There is always a risk of a system crashing during the upgrade process. It is highly recommended that the computer system be backed up before performing any upgrades. It is also suggested that the system be connected to an uninterruptable power supply while performing an upgrade.

The other benefit to keeping your software current, is that if all users are running the same version of an operating system, it makes it easier for the vendor to support and improve the platform.

If you are considering upgrading your Windows 7 or Windows 8 systems to Windows 10 and you qualify for the free upgrade, time is running out. The free upgrade offer is valid until July 29th, 2016.

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.

427 Million Passwords Leaked

(Continued from page 2)

There is some good news. Many banks and on-line services are starting to use two-factor authentication. Two factor authentication makes it extremely difficult for the bad guys to access your information. Two factor authentication is two out of the following three:

- Something you know (password)
- Something you have (fob that changes numbers every 30 to 90 seconds)
- Something you are (biometric fingerprint, retina scan etc.)

If your bank or other on-line sites offer two-factor authentication, you should seriously consider taking advantage of the technology.

Quanexus
We make *IT* easy.
571 Congress Park Dr.
Dayton, Ohio 45459
937 885-7272
info@quanexus.com

Here We Grow Again

We are pleased to announce that three, new data technicians have joined our Data Team. Jeff Massie, Adrian Rush and Josh Mirisciotti will be assisting clients with remote support, building workstations and servers and troubleshooting and repairing equipment. Quanexus now has 19 members of our company team spanning across Data, Voice, Security and administration. If you are in the area of our new location, please stop in and say hi! We will be proud to give you the grand tour.