Q-News

November 2019

A Word from Jack

Things have been very busy this month. I have been very active with sharing my views on where the IT industry is heading and the challenges of meeting legal and regulatory requirements, when it comes to protecting your clients' data. I have been putting out weekly blogs loaded with information and I've also started posting videos about how to keep data safe and how the criminals are being effective.

Over 18 months ago, we started talking and writing about the end of extended support for Windows 7 and Windows 2008R2 Server. Microsoft will no longer support these products after January 13, 2020. Also note; the end of extended support for Office 2010 is October 2020.

With these deadlines looming, it is safe to guess that exploits are being developed today and won't be released till after the January 13th date. This is because the criminals know that many systems will not be updated by the deadline. After the deadline, the criminals will be able to use these newly developed exploits for a long period of time because Microsoft will not release fixes to these new-found vulnerabilities. If you cannot update your systems by the deadline, there are mitigating controls that can be put in place to help protect your environment.

When companies get compromised and have their data ransomed or stolen, we have found there were multiple things that could have been done to prevent the incident. In the article "Layered Security Simplified", I discuss a layered security model that is proven to minimize the risk of an incident. Keeping your operating systems properly updated is one of several key items in a layered security model. If the other layers are preforming properly, the chance of an incident is greatly reduced. This should buy companies a little time if they cannot update their systems before the deadline. This by no means should be considered a permanent or even semi-permanent reason for not upgrading.

Layered Security Simplified

I have been talking about layered security for a long time now. Lately, I have been asked, "If I have a limited budget and can only do a few things, what should I do first". My response is this, "When you think about security, how do you personally protect what is important to you, starting with your house and valuables". It is safe to say, that most everyone keeps their door locked, to prevent someone from breaking in. Second, it is safe to also say that most everyone has insurance to protect themselves in case of a break in. Insurance provides a means to replace the items you consider valuable. Next, people living in the home know that they are to lock the doors, and the homeowner knows that they must purchase the insurance and keep the policy premiums paid.

Taking this analogy to a computer network is straight forward. You lock the doors. This is typically done with a business class, next generation firewall (NGFW). It can be argued that a good endpoint solution can be used in place of a firewall, but that will be a topic for another blog posting. You buy insurance to be able to recover from a loss. To recover a loss of your data, you need to have a reliable backup solution. And just as important as the firewall and backup solution, you have the people element. People need to be trained and know what the expectations are, e.g. doors are to be locked, insurance premiums are to be paid. Users of computers need to be trained on what the company policies are and how to behave while on the network, and just as importantly, how to identify if something is not working correctly and how to report an issue.

These three items are just the absolute minimum starting point. Using the home analogy, it is safe to guess that none of you leave all your money, jewelry and other valuables on the kitchen table. At minimum, these valuables are in a drawer or in a safe. These additional controls are like implementing a patch management and antivirus solution.

To sum up, the absolute minimum security items to implement are:
- **Next generation firewall**
- **Reliable backup solution**
- **User training**

Quanexus™

571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com

Is My Business too Small to get Hacked?

It is hard to believe, but there is a myth still shared by many small businesses and individuals. The myth is "I'm too small for anyone to attack my business." This myth is far from reality. A review of the target distribution data provided by hackmageddon.com shows that for 2019, the number one group being attacked is the individual (27%) and the number two group is multiple industries (14.3%), which is the small business group.

31% of all the cyber-attacks are designed for the individual and small business. There is a logical reason for this. Big business is taking cybersecurity seriously. They have made it difficult for the criminals to break into their systems. Criminals typically don't want to work hard. They have developed easily deployable tools to find those organizations that believe they are too small to be attacked (I call them "the low hanging fruit"). At minimum, even if you don't think you have anything worth stealing, your data has value to you. Imagine not being able to access the data on your computer system. That is the goal of ransomware, which continues to be one of the greatest threats to most organizations. The reason for the steady increase in ransomware attacks is because it is an extremely successful tool to exploit money from their victims. Implementing the best security tools won't guarantee you will not experience some type of a cyber-event, but ignoring the facts and doing nothing, guarantees you are more likely to experience a bad day.

There is a minimum number of things that every business should implement that will minimize the threat of a cyber-attack such as ransomware. The cost of these security tools has continued to drop and is now affordable for most small and medium sized businesses. Quanexus has developed our Q-Stack which is a layered security approach to protect against cyber-threats.

Have You Been Hacked? Indicators of Compromise (IOC)

How do you know if you have been hacked? Organizations often find out they have been hacked 3 to 6 months after the initial incident. Typically, they learn of the hack from an outside source. There are many items that should be monitored in a network to determine if there is a potential incident. Below is a list of a few key items for monitoring Active Directory (AD) and your firewall.

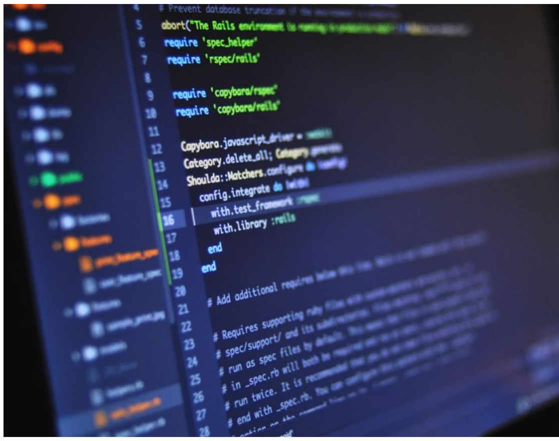
In AD monitor these key items:

- **Any network login from a user with privileged (administrative) access. Privileged accounts should only be used to manage the network. Users with administrative accounts should have a regular user account to perform normal business functions. The use of privileged accounts must be justified.**
- **The creation and deletion of user accounts.**
- **The modification of user access rights – escalation or de-escalation.**
- **Failed logins. Many failed logins can indicate the account is at risk.**

On your firewall monitor these key items:

- **Top users by bandwidth and sessions. These metrics should be used to create a baseline to detect anomalies.**
- **Outbound firewall traffic that is being blocked. This indicates that a user or their computer is trying to reach unauthorized sites.**

The items suggested above are the minimum key indicators that can be monitored to help you if you have a potential incident.



Security Awareness Training

If you work in any regulated industry, medical, finance, energy, transportation, government, etc. your company is required to provide ongoing security awareness and training (SAT). Often this is misidentified as security awareness training without the "and". Security awareness is typically provided through on-going emails, newsletters and posters that address different aspects of security. The training part is more formal, it often includes a lecture and a basic test required to prove that employees understand security topics that apply to their organization. For many years, we have been recommending the SANS.org OUCH! Newsletter, to fulfill part of the awareness function. The OUCH! Newsletter is free. As an additional control, we recommend that one person be responsible to distribute the newsletter to all employees. Employees are then required to respond back via email that they have read the newsletter. The replies are then logged. It is important to log the acknowledgments as proof that your organization is in compliance with its policies.

New Android Malware xHelper Infects 131 Devices Per Day

A new malware app has been identified, and infected users are not able to remove it from devices. Over the past six months, Android users have been complaining about a piece of malware called xHelper. The app hides itself from users, can download additional malicious software, and display ads and popups. Currently the malware is only directing users back to the Play store to download other apps. The real problem with xHelper is once a device is infected, there is no known way to remove it. If the app is uninstalled, it reinstalls itself quickly. Even if the user performs a factory reset on the device, xHelper will reinstall itself after a few minutes. It is not believed xHelper comes preinstalled on devices, so it's still a mystery how the malware can reinstall itself after a factory reset. It is believed the malware is picked up from third party Android sites. Sites like these often instruct users on how to install unofficial Android apps from outside the Play store.

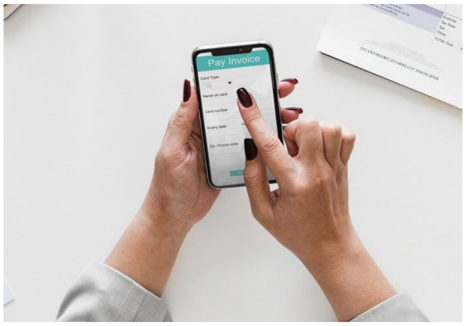
The malware continues to evolve and receive updates after finding its way onto a device. There were some reports early on that antivirus software was able to remove xHelper, but the malware continues to be updated so that currently no antivirus are known to be effective against it.

The cybersecurity company Symantec observed the malware changing over time and taking over more of the device's operating system since they've been tracking it. Even though currently xHelper is only showing ads, they believe the malware is capable of data theft and a complete takeover of the device. They also found many references to "Jio" in the source code. Jio is the largest 4G network in India. Symantec believes India is the hackers next target. Currently xHelper is being seen on devices in Russia, the US, and India.

Now that Symantec has shined a light on the problem and severity of xHelper, the hope is Google will put more resources against a solution. In the meantime, here are some tips to make sure your devices don't fall victim:

- **Keep the operating system and apps up to date on all devices**
- **Don't "sideload" or download and install apps from unknown sources**
- **Pay attention to permission requests by apps**
- **Make frequent backups of critical data**

Practicing good data retention habits is part of our Q-stack. It normally takes more than one thing to go wrong to have a piece of malware find its way onto your devices. Contact us today if you have questions on data security or malware.



Can't We All Play in the Same Sandbox?

This was the title from one of the breakout sessions I attended last month at the Northern Kentucky University Cybersecurity Symposium. Currently every organization that has any client information is having to deal with a patchwork of many requirements ranging from industry based, regulatory based, state and federal laws, and even the laws of other countries. All these different requirements are just making compliance an unreasonable task.

An example of how different states are choosing to treat companies can best be illustrated by looking at two extremes, California v. Ohio. I am proud to say that Ohio has taken the high road on this issue. On November 2, 2018 the Ohio Data Protection Act became effective. Ohio is the first state to give organizations an affirmative defense should they suffer a data loss or breach. The affirmative defense is based on the organization's voluntary implementation of an approved framework. If an organization can prove that they have taken appropriate measures through an approved frame work, and they do suffer a loss the company can be protected against potential liability.

California recently passed the California Consumer Protection Act (CCPA) which goes into effect January 1, 2020. This Act creates stringent penalties for theft/breach of data, while offering no guidance on how an organization should protect consumer data.

What makes things even more complicated is the fact that if you do business in any state such as California, you must abide by their state laws. Each state has a vested interest in protecting their consumers and are reluctant to let any other agency take over this obligation. The reality is, this patchwork of endless requirements is becoming a huge burden for any organization too keep up with. The big question is, "Is it time to come up with a common standard"?

Government agencies, regulatory bodies, and states, etc., don't want to lose political control over the privacy issue. I believe we are at the tipping point that if something doesn't change soon, organizations will not be capable of meeting the onerous compliance requirements and will be forced or fined out-of-business. My opinion on this is, compliance is necessary and should be required. Politics need to be set aside, and reasonable guidance needs to be published and updated as necessary, so organizations have a clear and reasonable understanding of the requirements.

Security Checklist

Over the last few months, I have shared many tips and suggestions on how to protect the data in your network environment. This week, I am providing a basic checklist with the minimum items that every organization needs to implement.

To put things in the proper perspective, policies and procedures are the foundation of a successful security program. The reality is most organizations today are extremely vulnerable and need to start a defensive program immediately vs. taking the time to build strong policies and procedures. This checklist is not a substitute for a good security program, it is only presented as a starting point. Once these items have been implemented, you need to proceed with developing your security program.

□ All operating systems need to be patched on a regular basis. This includes items such as routers, firewalls, and anything that has access to or can be accessed from the Internet.

□ All servers and workstations need to have a current anti-virus/malware solution implemented and updated regularly.

□ A business class firewall must be installed and updated regularly. Business class firewalls are not the devices you plug into your network and then to the Internet. They need to be properly configured to assure maximum benefit.

The features included in a business class firewall are:

□ Antivirus Engine: AV protection at the edge of your network.
□ Intrusion Detection and Intrusion Prevention Services (IDS/IPS)
□ DNS Filtering: The ability to stop users from going to known, bad sites that contain malware or inappropriate material.
□ Application Filtering: Prevent unauthorized applications' access to the Internet.
□ Network Segmentation: Ability to create multiple internal networks for wireless and wired connections. Devices connected to your network that do not need access to your internal resources, such as your server, should be on their own network segment. Examples of networks that should be segmented are: guest wireless access, environmental control systems, such as your heating and air conditioning system, postage meters, etc.

□ Backup Solution: The backup solution should include two key items. The first is for a quick recovery of data. The other consideration should be for a catastrophic event, such as if your server or your facility is no longer avail able, where your backup data will be stored (on site/ Off site) and how fast you can recover from an event. Several event scenarios should be considered.

□ Develop a culture of security. Your users need to understand the important role they play in protecting your business's and your clients' data.

Follow Quanexus on Social Media!

Find Quanexus on Facebook, Twitter, LinkedIn and Instagram! We share blog posts, useful articles, and pose questions to our followers. We also like to share pictures of our team to give you a glimpse of what's going on in the office!

Also, subscribe to our email list to regularly receive tech news, cybersecurity alerts, and information on upcoming events. **Visit Quanexus.com to sign up!**

@Quanexus571 **@Quanexus** **@Quanexus** **@Quanexus571**

Quanexus™

**571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com**