Q-News

July 2022

A Word from Jack

Cyber insurance, a moving target. Each month we get many requests from our clients to assist with completing a cyber insurance questionnaire. The request for this type of assistance has more than tripled since last year. What has also drastically changed is the number of clients that are being turned down for coverage. We are seeing about one in six applications denied. We are often able to remediate the issue that caused the denial of coverage, but it is a rush job. We are happy to assist with completing the applications, but we do ask that you are timely in sending them to us. The key items that insurance companies are looking for are:

- **Multi-factor authentication for remote access, local administrative access, and remote email access.**
- **Ability to recover data in a timely manner (backup solution)**
- **Patch management solution**
- **A managed endpoint detection and response (EDR) solution**
- **A next generation firewall (NGFW)**
- **Enforced password policy**
- **Security awareness training**

The two biggest reasons I have seen for policy denials are not having MFA implemented and not having a clearly defined data recovery solution.

A Future Without Passwords

Apple, Google, and Microsoft are on the road to eliminating passwords for all online services. The three tech giants committed to adding or enabling the technology needed to allow users to choose their phone as the main authentication device for websites and digital services. A user would be able to unlock their smartphone, as they do now, with a PIN, face ID, or fingerprint, and that action would take the place of entering a password on a website. The authentication would work through a cryptographic token called a passkey. The new authentication method would also make phishing more difficult because login would require a physical device.

Passwords are an ineffective way to authenticate for a service. Users are bad at password management. About 25% of people re-use passwords, and an equal 25% use weak, easily guessable passwords. But we can relate to these users. Passwords are a pain, and we are expected to remember a different password for every service. There are password managers, but they have low usage rates because users don't know what they are, or don't trust them.

The FIDO (Fast Identity Online) Alliance is the group behind the higher-level authentication technology. To maximize adoption FIDO was looking for something end-users already have and making the process as user-friendly as possible. The FIDO Alliance takes authentication out of the hands of the individual service and moves it to a higher-level security mechanism.

"This shift from letting every service fend for themselves with their own password-based authentication system to relying on the higher security of the platforms' authentication mechanisms, is how we can meaningfully reduce the Internet's over-reliance on passwords at a massive scale," FIDO said.

The FIDO Alliance has been working on a password-free workflow for a decade now. This latest announcement is the largest step we have seen in the quest to zero passwords.

Quanexus™

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

Small Business Not Prioritizing Cybersecurity

A recent small business survey showed only 5% of small business owners viewed cybersecurity as the biggest risk to their business. This is the first survey since the Russian invasion of Ukraine, and the cybersecurity risks and warnings that came from the conflict. The warnings that came from numerous government agencies seem to have no impact on the small business community. The same 5% level of concern was found in the previous survey from the first quarter of 2022, before the conflict began.

Less than half of the small business owners say they use an antivirus, complex passwords, or external backups which affirms the statistic that cybersecurity is not a priority. The number falls even lower when we get into software updates and multi-factor authentication.

The NSA and the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on Weak Security Controls Exploited for Initial Access. The advisory, in part, highlights many of the security controls small business owners admit to not using. Multi-factor authentication, software updates, and strong passwords are among the weak controls highlighted by the NSA advisory.

Customers disagree with small business owners regarding cybersecurity. About 75% of customers think businesses they use, will suffer a cybersecurity incident over the next 12 months, and 55% say they would be less likely to continue doing business with a company after a security breach.

Even if a company can recover data from a cybersecurity incident like ransomware, there is the added cost of paying the ransom, company downtime and loss of productivity, and the loss of public trust in the business. The most recent data available shows about 31% of US businesses that suffered a cyber-attack ultimately went out of business as a result of the incident.

Back to Basics – What is Zero Trust?

Zero trust is a security strategy based on the concept “never trust, always verify.” The idea of zero trust was a response to traditional perimeter network security that assumed everything inside the network was safe. A perimeter security network puts all of its defenses at the edge of the network. This means if a criminal gets inside, they are able to move around freely and access any applications or data on the network. Additionally, with remote work and cloud-based data and applications, it’s more difficult to define that perimeter. Zero trust changes the model and requires verification for each user and device accessing each application and element of data.

The zero trust model works generally on three tenets. First, the framework must identify and authorize the user. Users are no longer automatically authorized simply because they are on the office network. Authorization typically includes multi-factor authentication (MFA).

Once a user is authorized, they only have access to the data and applications they need to perform their job. This policy is known as ‘least privilege’ and helps to limit the data accessible to a hacker in the event of a breach. With the least privilege policy, an employee in marketing would not have access to personally identifiable information from human resources. Conversely, human resources would not have access to the latest confidential marketing presentation.

Lastly, the zero trust model sets device requirements that must be met in order to access the data or applications. Device requirements could be as simple as an approved antivirus must be installed, or could be much more complex depending on the business need.

In addition to these three tenets, network segmentation and monitoring are often implemented to further prevent lateral movement and to log unusual activity. Zero trust does not trust any users or applications by default. After a user, application, and device are approved, the zero trust model continues to monitor the criteria and discontinues access if any of the criteria change.

Businesses are turning to cyber insurance as ransomware and other cyberattacks continue to increase. Cyber insurance policies typically will help a compromised business contact customers in accordance with state laws, recover data, and repair damaged computers. However, the increase in costly ransomware has forced insurance companies to make policies more difficult to get approved.

How War Impacts Cyber Insurance

A court decision earlier this year on an insurance claim from 2017 is raising questions about what cyber insurance looks like during times of war. A malware attack on Ukraine in 2017 quickly spread and destroyed data from thousands of companies around the world. The pharmaceutical company Merck was one of the businesses impacted by the malware which destroyed data on 40,000 of their computers. Merck estimated the cost of new equipment, personnel, and production downtime was $1.4 billion and submitted a claim against their insurance policy. The insurance company denied the claim citing the malware originally was an attack on Ukraine from Russia and was, therefore, an act of war. Most insurance policies have an "act of war" exclusion clause. The case spent three years in court and was finally decided in Merck's favor.

Today we have a conflict between Russia and Ukraine where cybercrime is a large concern. Cyber insurance companies have had five years since this incident to understand the risk of the current climate and write policies appropriate for the risk. Attribution is another factor when a company tries to make a claim on an insurance policy. The origin of a cyberattack is purposefully difficult to attribute. With a conflict going on where cyberattacks have been part of the conflict, an "act of war" exclusion could play a large part in an insurance claim today.

There are many factors to consider when shopping for cyber insurance. Click here for our latest cyber insurance update video where we discuss more factors for a business owner to consider when selecting a policy. It's important to understand what is covered in a policy, and even more importantly, what is not covered. Also, cyber insurance should be used as a last resort. Protecting your data with quality best practices is the best way to reduce risk.

Hackers are Getting Around MFA

Multi-factor authentication is an extra layer of security beyond a password that requires an authenticator or often a one-time password sent via text message. Any form of two-factor authentication (2FA) or multi-factor authentication is better than only relying on a password, but hackers are finding ways to get around MFA, and users should be aware of the signs of those attack vectors.

Hackers are bombarding users with MFA push notifications or phone calls, and it's working. Attackers shared how they used the technique commenting, "No limit is placed on the amount of calls that can be made. Call the employee 100 times at 1 am while he is trying to sleep, and he will more than likely accept it. Once the employee accepts the initial call, you can access the MFA enrollment portal and enroll another device." Criminals reportedly used this technique to breach Microsoft and Nvidia recently. In the case of Microsoft, hackers were able to log into the company's VPN from Germany and the US at the same time.

The bombardment technique works best in disruptive MFA requests like phone calls or push notifications. Criminals can continually push requests making users' phones unusable until they accept. Attackers can also intercept SMS notifications, we covered SIM swapping on a previous blog post you can read here.

In all of these cases, the user's password has been compromised. In order to make MFA requests, the hacker must already have the user's password. Employees should be educated on this new hacking tactic to get around MFA, and also understand their password has been compromised and needs to be changed.

A new authentication technology called FIDO would fix this problem because the login requires a physical device. Most web services are not there yet, but a future without passwords is coming.

CISA Outlines Three Critical IT Failures

The deputy associate director at the Cybersecurity and Infrastructure Security Agency (CISA), Donald Benack, gave a presentation along with Joshua Corman at the RSA convention last week where they outlined three critical cybersecurity failures, they are seeing exploited in the wild.

The pair called out the healthcare industry specifically as a sector with limited IT knowledge and skill focused on security. The nature of patient records, personally identifiable information (PII) including SSN, and financial information, make the healthcare sector a particularly desirable target for ransomware and phishing attacks. These factors are paired with limited budgets or a lack of cybersecurity priority in the sector.

The presentation was titled, “Bad Practices” to highlight a contradiction to ‘best practices.’ “The uncomfortable truth is that we can’t just say do best practices,” Corman said. Benack outlined three “terrible tactics” in an attempt to change the language of cybersecurity. If ‘best practices’ are too much for some businesses, CISA is thinking about other ways they can have a positive influence on cybersecurity.

The three terrible tactics:

Use of unsupported or stop-of-existence software program
A business should not use unsupported or end-of-life software. When software is not being patched and updated consistently, it becomes an easy target for attack. Hackers follow end-of-life software, find vulnerabilities, and then search the web for systems using the easily hacked software.

Use of recognized/preset/default credentials
Many industry-specific hardware comes with default credentials for easy setup. If the credentials are not changed, the devices can be easily accessed remotely. Some credentials are so easy to find, they are printed in the product manual. Hackers can use the credentials and search the web for devices still using the default credentials.

Use of single-variable authentication for remote or administrative access
Remote and admin privileges are the most sensitive login credentials. No user should use admin privileges as their normal login. Additionally, this higher-level access should never use only a password, they should always have some form of multi-factor authentication (MFA).

“All of these procedures are not dependent on theory, they are dependent on evaluation of all the incident experiences and accessibility to info CISA has all-around what’s being exploited in the wild,” Benack stated.

Podcast

We have two new short Podcasts out this month. Jack and Chuck discuss cyber insurance for small business, and actions taken by the FBI to remove Russian Malware.

Cyber Insurance Updates for Small Business

Click Here for Podcast- Cyber Insurance Update for Small Business

FBI Secretly Removed Russian Malware

Click Here for Podcast- FBI Removed Russian Malware from Network Devices

Quanexus™

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

Follow Quanexus on Social Media!

Find Quanexus on Facebook, Youtube, LinkedIn, and Instagram! Click on the buttons below to access our social media pages. Like, comment and subscribe!

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 @Quanexus571