IMAGINE IT

Imagine: Happ(i)ness in Business.

The Q4 2020 State of SMB CYBER SECURITY

Peter Durand, Chief Technical Officer

(We purposely skipped Q3. We want to spend less time looking back and more time in the now and future).

www.imagineiti.com

The Q4 2020 State of SMB Cyber-Security

It has been another very interesting quarter in terms of breach activity, and how the U.S. Govt is finally taking a stand.

U.S. GOVT SANCTIONS FOR FACILITATING RANSOMWARE PAYMENTS

This is big news! Effective October 1, 2020, the Department of the Treasury posted an advisory that "…Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations."

Bottom line, in some situations your insurance company will be putting themselves at risk of sanction, and therefore may choose to NOT pay a ransom.

You can skim through the advisory here:
https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

THE 3 TOP CYBER-THREATS

1. Impersonation

A hacker will pretend to be a trusted person and ask for confidential information to be passed along (HR records, for example). Using this information, the hacker can then attack other users and/or perform identity theft.

2. Mailbox Breaches

Mailbox breaches lead to user impersonation, which then causes unsuspecting users to perform money transfers or provide confidential information. And commonly, recipients are asked to change bank deposit information, leading to significant lost dollars. These breaches also often spread malware and allow a foot in the door for Ransomware.

3. Ransomware

Due to the easy access to Ransomware deployment tools, Ransomware has become the preferred money-making activity for organized crime and nation-states. The average Ransomware payment is well over $100,000 and is going up significantly each quarter.

Of note: in late October the U.S. Cybersecurity & Infrastructure Security Agency posted an alert about HEALTHCARE currently under attack. If your org is in this industry you need to take action NOW…

https://us-cert.cisa.gov/ncas/alerts/aa20-302a. Has your clinic taken the Imagine IT "HIPAA Posture Self-Assessment" yet?

Pete's Insight

As long as there is Bitcoin there will be Ransomware. As long as millions of orgs continue to ignore the threats there will be Ransomware. Bitcoin allows the bad actors to collect money in an untraceable way, and poor security posture just feeds the beast.

WHAT YOU CAN DO TO PROTECT YOUR ORG

If your org is like many these days, you are likely not sure what to do, or maybe think you are "good to go" or "under the radar". You have a

Firewall, Antivirus, and Passwords, but modern attacks easily get around decades-old protections. And the hackers are attacking EVERYONE.

When you are ready to take Cyber-Security seriously, please engage with Imagine IT. We have developed an easy to follow process to take your cyber-security from the outhouse to the penthouse.

The 4-Step Process To Protect Your Org

1. **Develop a real security strategy**
   It all starts with a strategy. What is your current security posture (have you taken the Imagine IT "Security Posture Self-Assessment")? What are you aiming for, and when? How will you get there, and fast? What is the strategy for continual security posture improvement? Who is responsible for seeing this through?

2. **Deploy strong security protection technologies**
   For example, unhackable backup (including for O365/G-Suite), Two-Factor Authentication deployed everywhere, permissions locked down, email spoofing locked down, etc…

3. **Deploy breach detection technologies**
   The average time to breach detection is 200 days. Once breached, lateral hacker movement can't be stopped if undetected. Intrusion Detection technologies can alert to malicious traffic inside the network, on endpoints, on cloud servers, and even in Microsoft 365.

4. **Enroll users in Security Awareness Training**
   90-95% of all breaches are caused by human error. And most of these are due to end-users falling victim to phishing and online scams. Even with awesome protection technologies in place, it is critical to keep security front of mind at all times.

WHAT IMAGINE IT IS CURRENTLY DEVELOPING THAT PROTECTS OUR PARTNERS

Here is a list of security technologies we have recently gone live with or are currently in the R&D process…

Threat Hunting
The latest revision of Security Shield now includes a breach detection agent to identify malicious files and settings that were missed by antivirus and other security technologies. This can be an extremely useful tool against Ransomware and other malicious software, especially in this "work from anywhere" world.

Cloud Data Backup
Microsoft 365 and G-Suite include very rudimentary backups, and it can take many days to restore data with the potential for data loss. And Ransomware is now a threat to this type of data. The latest revision of Security Shield now includes a 3rd party backup to allow for fast and easy granular restores of this type of data.

Data Loss Protection (DLP)
One of the most common types of breaches is when a hacker impersonates a trusted person and asks for confidential data to be provided. The success rate for this type of attack is mind-boggling, likely due to the human nature of instinctively trusting others. To solve for this, Imagine IT can now optionally deploy Microsoft subscription-based technologies that can block the accidental or intentional leakage of confidential data.

Mobile Device Management (MDM)
Imagine IT is currently performing R&D on a Microsoft solution that will allow much stronger administration of remote computers. Just a few of the features included are remote wipe, encryption enforcement, policy enforcement, and remote software deployments. Considering the new norm of remote work, the ability to secure remote endpoints has become extremely critical.

Application Allow-List System (AAL)
Imagine IT is currently performing R&D on a solution that could for the most part render malware useless. In the current way of protection systems, antivirus software vendors are forced to play "whack-a-mole". An AAL system complements antivirus by only allowing pre-approved software to run, thereby blocking malware. And the AAL system restricts "allowed" applications to only perform in their designed manner, called "Ringfencing".

Breach Attack Simulation (BAS)
Imagine IT is currently performing R&D on a solution that will simulate a breach attack from inside the network. BAS is not a penetration test, but instead is a way to automate breach attack testing of systems. This will allow us to continually uncover vulnerabilities in a way that Vulnerability Assessments might miss.

PRO TIP OF THE QUARTER

Password Management
Do you or your users store passwords in Word, Excel, text files and/or sticky notes? You probably know this is not a good idea. Even password protected Office files are not truly secure. Besides the security aspect, maintaining secure passwords can be cumbersome, and having to look them up each time can be frustrating.

A Password Manager application allows users to login to sites faster, using longer and more complex passwords that they will not need to remember, and that are wildly different from other passwords. Encryption and Two-Factor Authentication are integrated into these systems. Imagine IT can deploy a centrally managed system that is easy for an onsite admin to administer, and ultimately improves the security posture of your org.

CONCLUSION

The U.S. Govt has finally decided to take Ransomware policy seriously. Why on Earth would any U.S org feel OK about paying a ransom to a state-sponsored hacker org that will use that money to fund their military objectives? Well hopefully between policy and actual security we can all work together to stop this terrible threat to our businesses and country.

Please stay diligent and do everything you can to protect your users and data. Thank you for reading, and we wish for a safe and successful 2021!