IMAGINE IT

Imagine: Happ(i)ness in Business

The Q2 2020 State of SMB DATA SECURITY

Peter Durand, Chief Technical Officer

www.imagineiti.com

The Q2 2020 State of SMB Data Security

It has been another very interesting (and sad) quarter in terms of breach activity, downtime, and loss of revenue.

The most noticeable change is that organized crime is getting, well, more organized. "Ransomware as a Service" is now a real thing, and some very mature hacking organizations have published offerings where they provide the tools and processes. The smaller hacker organizations that pay for the service then give out a percentage of the profits in return. They are even developing some ethical Ransomware standards – crazy world!

The 3 Top Cyber-Threats In Q2 2020

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. We were just made aware of a small, local organization that was asked to pay a $200,000 ransom.

Pete's Insight

My take is, it's all about the Benjamins. With the current poor state of online security, businesses are just low-hanging fruit to hackers. And it is EXTREMELY easy for hackers to carry on their activities without detection. I worry that too many of the world's brightest minds are being converted into organized hackers due to the lure of easy money and glamour.

Why is it getting so easy to successfully breach a company?

Many companies still think they are under the radar and that "*this only happens to other companies*." Unfortunately, it isn't until they are breached that they finally take security seriously. Others tell their staff to "*not click on anything stupid*." Both of these are examples of flawed security strategies. It's like driving a car without insurance… feeling pretty confident that "*I will probably never get into an accident*."

The 4 core reasons for successful breaches

1. Lack of a real security strategy
   It all starts with a strategy. What is your current security posture? What are you aiming for, and when? How will you get there, and fast? What is the strategy for continual security posture improvement?

2. Lack of 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. Lack of breach monitoring technologies
   The average time to breach detection is 200 days. Once breached, lateral hacker movement can't be stopped if undetected.

4. Lack of user training
   According to KnowBe4's recent study, 37.9% of untrained end-users will fail a phishing test. The phishing test was administered to organizations with no prior security awareness training. The study included 4 million users, 17,000 organizations of all sizes, and 19 different industries

What is Imagine IT doing about these threats?

It starts with a Security Strategy that has two main components, each with a Roadmap:

1. To continually educate and improve our *customers'* security posture
   99% of the security R&D that we perform is for our Security Shield customers. Our Security Shield program is now at version 2, and if you have not yet enrolled, your security posture is getting farther and farther behind, creating significant risk.

2. To continually improve our *internal* security posture.
   We know we can NEVER experience an undetected breach, and we have a strategy in place to achieve that goal. I would be happy to share a high-level overview of our internal security posture upon request.

IMAGINE IT

Imagine IT SMB Security Predictions for 2020/2021

Ransomware attacks against cloud storage

Expect to start hearing about successful Ransomware attacks against cloud storage, like Office365, Azure, AWS, DropBox, etc.

Data Loss Protection (DLP) technologies will gain wide adoption

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.

Breach Attack Simulation

(BAS) will gain some early adoption. BAS is not a penetration test but is a way to automate breach attack testing of systems.

Ransomware impacts on non-Security Shield Partners

20% of our non-Security Shield customers will be impacted by either Ransomware and/or a significant data breach.

Remote worker's personal devices

Remote workers on personally-owned devices will be the root cause of 10% of all breaches.

National Threat Reports

It starts with a Security Strategy that has two main components, each with a Roadmap:

1. To continually educate and improve our *customers'* security posture. 99% of the security R&D that we perform is for our Security Shield customers.
2. To continually improve our *internal* security posture. We know we can NEVER experience an undetected breached, and we have a strategy in place to achieve that goal. We would be happy to share a high-level overview of our internal security posture upon request.

According to the July 2020 McAfee Threats Report:

- McAfee Labs observed 375 threats per minute. And since the previous quarter:
    - New PowerShell malware increased by 689% (see comment below).
    - New mobile malware increased by 71%.
    - New IoT malware increased by 58%.
    - New macOS malware increased by 51%.
    - New coin minder malware increased by 26%.

Regarding PowerShell

Only skilled IT staff (or hackers) use PowerShell. If PowerShell commands are being run on your systems, you need security technologies in place to immediately detect that activity. Very few organizations have such technologies deployed.

According to the Sophos July 2020 State of Cloud Security Report:

Almost three-quarters of organizations hosting data or workloads in the public cloud experienced a security incident in the last year. 70% of organizations reported they were hit by malware, Ransomware, data theft, account compromise attempts, or crypto-jacking in the previous year.

Data loss/leakage is the number one concern for organizations. Data loss and leakage topped our list as the biggest security concern, with 44% of organizations seeing data loss as one of their top three focus areas. 96% of organizations are concerned about their current level of cloud security.

Conclusion:

As the security threat landscape gets more dangerous, I hope that organizations of all sizes start to take the security of their confidential data more seriously. Until there is broad adoption of strong security posture strategies, the statistics are going to continue to go in the wrong direction.