Imagine: Happ(i)ness in Business.

The Q1 2020 State of SMB DATA SECURITY

Peter Durand, Chief Technical Officer

www.imagineiti.com

The 2020 State of SMB Data Security

We are more than one-third of the way through a very unusual year-in-the-life. And as I ponder how life has changed, considering my business purpose in the world, I also ponder how small businesses are coping with the ever-increasing threat to the security of their data.

Here is what our recent research has led us to…

The Threat

According to the Q1 2020 Coveware Ransomware Report:

- The median victim company size was 62 employees.
- The average business ransomware payment in Q1 2020 was $111,000 – a 33% spike compared to the previous quarter.
- The average days of downtime was 15.
- 96% of the time the hacker delivered decryption tool worked after payment.

And that's just Ransomware. According to Cybersecurity Ventures,

Cybercrime is expected to grow to a whopping $6,000,000,000,000 (Trillion) in 2021.

IMAGINE IT

What are the 3 most common Cybercrimes Imagine IT discovered over the past 12 months?

1. **Mailbox breaches**: This leads to user impersonation, which then causes unsuspecting users to perform money transfers or provide confidential information (like HR records). 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.
2. **Phishing for logins:** This is often how a hacker obtains user login credentials. This also spreads malware and allows a foot in the door for Ransomware.
3. **Gift card scams**: Often these start with a phishing email, and end with a user being bilked out of $.

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

Two-Factor Authentication missing from Remote Desktop or VPN, and user Phishing are the two main ways into the system. Once in, the hackers now have a plethora of tools at their disposal that can be purchased for as little as $50 on dark web marketplaces. When companies are only protected by traditional security solutions, these marketplace tools allow for easy, undetected lateral movement inside the system, and significantly reduce the amount of time and effort required to get to the prize.

Organized hackers continue to get smarter. For example, in early 2020 it became common practice that shortly before planting Ransomware the hackers first download all of the data. That way if the victim recovers from backup and chooses not to pay, the hackers threaten to post the data online (intellectual property, confidential data, customer data, and PII/PHI) causing compliance violations, lawsuits, and damaged reputation… thereby forcing payment.

350% increase in reported cybersecurity complaints, much of this originating from hostile nation-states.

How are traditional network security strategies holding up against the onslaught?

According to the Mandiant 2020 Security Effectives Report, which compiles data for "Enterprise" security penetration testing:

- 53% of penetration tests successfully infiltrated without detection.
- 26% of penetration tests successfully infiltrated but were detected.
- 68% of the time, organizations reported their controls did not prevent or detect Ransomware detonation within their environment.
- 48% of the time, controls in place were not able to prevent or detect the delivery and movement of malicious files.

Those metrics are terrible, especially for so-called highly secure "Enterprise" companies. At the SMB level (with lower security budgets) we would expect the metrics to be significantly worse. According to Verizon, 43% of breach victims were SMB.

How has COVID-19 impacted the threat landscape?

Organized hacking will always try to take advantage of bad situations. Case in point… COVID-19. Since March 1, 2020, the FBI is reporting an enormous 350% increase in reported cybersecurity complaints, much of this originating from hostile nation-states.

Imagine IT SMB Security Predictions for 2020/2021

- Expect to start hearing about successful Ransomware attacks against cloud storage, like Office 365, Azure, AWS, G-Suite, DropBox, etc…
- Data Loss Protection (DLP) technologies will gain wide adoption.
- 20% of our non-Security Shield customers will be impacted by either Ransomware and/or a significant data breach.
- Remote workers on personally owned devices will be the root cause of 10% of all breaches.
- 0% of our Security Shield v2 customers will be impacted by Ransomware and/or a significant data breach. This is not to say there won't be breaches, but that any breaches will be quickly discovered and locked down before damage is done.

What is Imagine IT doing about this?

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.

What is on the Customer Security Roadmap?

- Continual customer education about security and why the Shield is so critical.
- Continual security improvements for Security Shield customers. Your security posture can never stand still as the hackers are continually finding more and more ways to attack. New for Q2 2020: Security Shield v2 and "Transform Security Teams".
    - Security Shield v2 continually improves customer security posture by building into the monthly cost the labor to deploy many security improvements each year. For example, Microsoft provides an additional subscription that can block the accidental or intentional user leakage of confidential information. This subscription would have averted many recent incidents within our customer base, including our Shield v1 customers.
    - "Transform Security Teams" are small security collaboration groups with customer leadership participation. These groups are not tactic-focused security groups, but instead will focus on business security strategy, education, and aligning security with the corporate mission.

We will reach out to you over the course of 2020 to discuss "Security Shield v2" and "Transform Security Teams".

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 2020!