WEI INSIGHTS WHITE PAPER

THE MANDATORY COMPONENTS OF AN EFFECTIVE RANSOMWARE STRATEGY

51% of IT decision makers indicated 'security and compliance concerns' as a top driver of digital transformation.[1]

Here's a great trivia question for your IT department. What year did the first confirmed ransomware attack occur? Many may place the birth of ransomware to be somewhere in the previous decade, but even if you presumed the 21st century you would be wrong. If you guessed 1989, you got it right. It was that year that a biological researcher named Dr. Joseph L. Popp created the first cryptor that is referred to today as the AIDS Trojan. Dr. Popp distributed a floppy disk to a list of subscribers to WHO sponsored AIDS conference. The floppy was programmed to deliver malware to the victim's computer that encrypted any file names located on the system drive. A message then appeared on the screen, requesting the victim to send a $378 licensing fee for the floppy disk. Dr. Popp was arrested but the court ruled him mentally unfit to stand trial.[2]

RANSOMWARE IS EXTORTION

We wanted to mention that milestone not because it makes a good trivia question, but because it establishes a simple truth. While ransomware as we know it may seem to have appeared on the global radar in only recent year, the idea of encrypting someone's computer to extort money is more than thirty years old. Let's be clear, ransomware is extortion. It is a crime, and a costly one at that. It destroys businesses and lives. It's far more than a crime, however. According to DHS Secretary Alejandro Mayorkas, "Ransomware is a national security threat."[3]

WEI

A TOTAL EMPHASIS ON FIGHTING RANSOMWARE

Here's another trivia question. How many attempted ransomware attacks were launched on targets within the United States in 2020? According to a 2021 report by Sophos, it was a mind blowing 227,266,604 times?[4] And it's only projected to get worse. The frequency of ransomware attacks increased more than 93% in the first half of 2021 compared to the same period the year prior.[5] If the regularity of the attacks seems astounding, the associated costs of remediation from a ransomware attack are even more staggering. In 2019, the global average costs of remediation from a ransomware attack were approximately $761,000.[6] In one year that figure doubled to $1.85 million. In the U.S., ransomware victims spent an average of more than $2 million.[6] Note that figure doesn't include the cost of downtime which on average in 2020 encompassed 21 days.[7]

These figures haven't gone unnoticed by Washington. According to the current NSA director in October of 2021, The public can expect ransomware attacks' every single day; for the next five years.[8] So serious is the threat of ransomware to the country at large, that the U.S. government through a collaborative effort between the DHS and DOJ launched a website to combat ransomware. The website titled, StopRansomware.gov is to serve as a central hub for ransomware resources for individuals, businesses, and other organizations.[9] Says DHS Secretary Mayorkas, "As ransomware attacks continue to rise around the world, businesses and other organizations must prioritize their cybersecurity,"[10]

At WEI, we recognized the seriousness of Ransomware years ago, and are responding to the recent battle cry heard to overcome the ransomware menace with even more resources than ever. Our technical team includes some of the leading subject manner experts when it comes to ransomware strategies. In this paper we have condensed some of the leading strategies recommended by our team of experts in order to help our customers combat what the head of Britain's National Cyber Security Center refers to as the #1 cyber risk.[11]

EASY TO LAUNCH, DIFFICULT TO PROTECT AGAINST

Despite the publicized success that ransomware organizations have had, this malware threat is too often underestimated. Traditionally, ransomware attacks were implemented through some type of phishing attack and launched via the clicking of an embedded hyperlink or email attachment. While this generic type of attack characterized ransomware early on, ransomware attack methodologies have greatly advanced recently. Attacks today are growing more targeted and include hands-on-keyboard hacking. Attacks are implemented with methodical precision and patience as hackers often quietly traverse and observe the infiltrated network for weeks or months to learn how best implement the attack. These precision attacks are the most difficult to combat and recover from.

Although hacking experience may improve the odds of a successful ransomware payment for the attackers, one doesn't need an extensive knowledge base in IT to implement a campaign thanks to Ransomware-as-a-Service (RaaS) subscription models. Under these affiliate-based models, the RaaS developer receives a cut of each ransom paid to the subscriber. It is estimated that nearly two-thirds of ransomware campaigns in 2020 utilized a RaaS service.[12]

NEW RANSOMWARE GANGS AND ATTACK METHODS

Stopping ransomware gangs is kind of like the arcade game, Whac-a-Mole. As soon as one gang goes by the wayside, another one takes its place. Two of the most infamous ransomware service organizations, Darkside and REvil, recently retired after feeling the heat from their much-publicized attacks on Colonial Pipeline and Kesaya. The void left by these organizations was quickly filled by a new Russian based ransomware gang called BlackMatter. With new organizations, come new attack methodologies. In the case of BlackMatter, the hackers actively seek what they refer to as Initial Access Brokers (IABs). According to HHS Security, IABs are financially motivated individuals who trade RDP credentials, VPN login details or other access information for a fee. BlackMatter promises IABs up to $100,00 for a successful attack on organization's network.[13] The group also utilizes a new encryption strategy called partial encryption, an attack methodology that is growing popular amongst other organizations as well. As its name implies, partial encryption only encrypts a small portion of the file, yet still renders the file inaccessible. This dramatically speeds up the attack, allowing the attack to spread before its presence can be detected. It also leaves the file partially readable, making its compromise harder to detect by the naked eye.

BACKUP EXTORTION METHODS

Ransomware today isn't just about encryption. While the inaccessibility of one's data remains the primary motivator to extort money from victims, ransomware criminals no longer solely rely on it to close the deal. Many ransomware attacks use a two-pronged approach in which an organization's files are exfiltrated to a secure third-party site prior to the encryption process. Should the victim be able to successfully thwart the attack and recover its data, the criminals can then threaten to publish or sale the confiscated data on the dark web. More recently, ransomware gangs have used the threat of bricking computers as a third option. The term bricking, literally means to turn the computer into a brick, rendering it useless as a machine as the BIOS and internal motherboard components are damaged.

THE NIST FRAMEWORK TO COMBAT RANSOMWARE

Because ransomware is constantly evolving as new criminal innovators advance their attack methodologies to gain the upper hand, there is no magic pill to combat ransomware.

You cannot rely on a single tool such as an email security solution, a signature-based endpoint solution or a perimeter firewall. You need a strategy that centers around a framework that utilizes a multi-layer strategy. One of the more popular frameworks and endorsed by WEI is the NIST Cybersecurity Framework which centers on five core functions.

1. **Identify** - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2. **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
3. **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4. **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
5. **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Every cybersecurity strategy begins with the Identifying phase. The activities involved in this exercise are foundational for effective use of the framework. This is where a company identifies the risks it may be exposed to, determining the likelihood of those risks occurring and what the impact would be. It is at that point that leadership decides what their accepted and unacceptable risk levels and what their due-of-care level is to protect all stakeholders.

The recovery phase often involves some type of incident response team. This team can be internal to the organization or contracted out to third-party experts in their field. Whatever the makeup of your incident response team happens to be, your team needs to be ready at a moment's notice. You should not be sitting down with your cyber attorney for the first time or familiarizing yourself with the small print involving your cyber insurance policy during the aftermath of an attack. All involved parties need to be familiar with your organization and its key operations. Your incident response plan should have been rehearsed more than once to ensure its success.

PROTECT, DETECT AND RESPOND

At the conclusion of the Identifying phase comes the realization that the internet is no longer the sole attack avenue. Every user across your organization is a threat point, as is every VPN and RDP connection. And that's where WEI comes in. No organization can be everything. At WEI, our expertise lies in three of the NIST core functions: protect, detect, and respond. The most effective cybersecurity tool to secure these threat points is a Next Generation Firewall. This doesn't denote a single perimeter firewall, however. First off, many geographically dispersed companies have multiple perimeters due to the propagation of edge computing utilizing

SD-WAN architectures. But its more than just multiple internet points. We recommend bringing firewalls inside the organization in order to separate users in the environment from getting to the data center. This allows cybersecurity teams to create firewall policies for traffic that traverses internal VLANs, segmenting your vulnerable IoT infrastructure and other LAN based traffic from your core network.

Today's NGFW appliances not only block traffic that is known to be malicious, they also constantly analyze and appraise allowed traffic, looking for anomalies and abnormalities. While the firewall may not be able to identify the traffic at hand, such as a zero-day attack, it can deem it suspicious and send it to another component within the security ecosystem such as a sandbox where it can be detonated and studied within a controlled isolated environment. If deemed malicious, a signature is then generated automatically, alerting all connected firewalls. Visibility is the key. Only a visible threat can be acted on. The more you can see, the faster you can react to a threat, which allows you to move from a reactionary stance to a proactive one. With the speed at which ransomware can encrypt files throughout the IT estate, the ability to have multiple firewalls working intelligently and cohesively in automated fashion is imperative in containing a ransomware attack.

If your organization has a firewall, then it has logs, and those logs contain valuable information. However, while your firewalls may generate tons of valuable logging data, the recorded information is of little value if it is ignored. Logs can play a critical role in gaining visibility of your digital traffic patterns when they can be integrated with some type of analytics reporter to stop an attack before it gains momentum. Your logs also serve as a historical record that provide the clues outlining how the crime was committed. Did you know that 80% of ransomware victims suffer repeat attacks?[14] The UK's National Cyber Security Centre (NCSC) often uses the example of a company that paid 6.5 million pounds to recover their files from a ransomware attack but didn't make the effort to identify the root cause of the attack in order to protect against similar attacks. Less than two weeks later, the company was hit once again by the same attackers and once again, forced to pay a similar ransom.[15] No details whether the company learned its lesson.

SECURING YOUR BACKUPS IS ABSOLUTELY ESSENTIAL

There was a time in which overcoming a ransomware attack was as easy as 3-2-1; 3 copies of your data on two different media with one copy offsite. While the traditional 3-2-1 backup strategy is still relevant as a foundational approach to backups, it is no longer that simple. Ransomware organizations know that the one thing standing between them and getting paid is a systemized backup solution. Just as the first target of a surprise attack is often the airfields of an opposing military force, the first objective of an attack is to disable your backup system. Whether that means it deleting it, corrupting it, or modifying it, once it is out of the way, the way is clear for the real attack to commence.

One of the reasons why a ransomware attack may take place weeks or months after being successfully infiltrated is to give the attackers time to learn your backup operations. By examining your backup architectures and the actions of those who manage your backups, they can find exploitable weaknesses. That is why it is imperative to ensure that your backups systems follow best practice methodologies. Some of them include the following.

- Many organizations place their backup server on a VM located in the same virtual environment it is supposed to protect. Once a vCenter or Hyper-V cluster is compromised, the backup server probably is too. That's why you should consider placing your backup server on a physical machine or host it in the cloud.
- Do not allow RDP connections to your backup server. Use a backup solution with remote console software that offers remote access over a secure and proprietary protocol.
- Don't join your backup server to active directory. The premise is simple. If attackers gain access to your local AD, they then have access to your backup server. Use local accounts with very strong passwords that are then reinforced by multifactor authentication. Never secure your backup environment with password protection alone.

HOW WEI CAN HELP

Complying with regulatory mandates does not always equal security. Cybersecurity is a moving target and the inability to stay ahead of the transforming threat landscape can have severe consequences. Many organizations currently reside below what is referred to as the security poverty line.[16] While one may equate this with budgetary pressures, it also refers to a lack of expertise in the field of cybersecurity. With internal IT departments already stretched, few organizations have the time and resources to stay ahead of the cyber threat curve. That's why you need a partner that can educate you about how to protect yourself against today's ransomware attacks as well as other threats. Our staff includes some of the most prominent SMEs in the industry. We also aren't about selling you a bunch of tools. Instead, we sell strategical, cohesive solutions to create a united front to secure all threat points. Let us share with you our vast knowledge of ransomware, as well as the proven ways to protect against it.

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.

info@wei.com

800.296.7837

www.wei.com

43 Northwestern Drive
Salem, NH 03079

TALK TO WEI TODAY

Contact the security experts at WEI to find out how you can combat cybersecurity within your organization.

Sources:
1. IDG Research commissioned by WEI, January 2021.
2. Ransomware: From blockers to cryptors and beyond | Kaspersky official blog
3. DHS: Ransomware Is National Security Threat - Breaking Defense Breaking Defense - Defense industry news, analysis and commentary
4. Record-breaking ransomware attempt spike in 2021 - Tech Monitor
5. Ransomware attacks increase dramatically during 2021 (computerweekly.com)
6. With Ransomware Costs On The Rise, Organizations Must Be More Proactive (forbes.com)
7. Ransomware Payments Decline in Q4 2020 (coveware.com)
8. NSA Chief Says Ransomware Threat to Remain for Years - WSJ
9. Stop Ransomware | CISA
10. United States Government Launches First One-Stop Ransomware Resource at StopRansomware.gov | Homeland Security (dhs.gov)
11. Analysis: Why Ransomware Is No. 1 Cyberthreat (bankinfosecurity.com)
12. Ransomware as a service is the new big problem for business | ZDNet
13. HHS Security Report on BlackMatter 9/02/2
14. 80% of ransomware victims suffer repeat attacks, according to new report - CBS News
15. Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again | ZDNet
16. The Security Poverty Line, Part 1 - Wendy Nather - SCW #60 - Security Weekly