WEI INSIGHTS TECH BRIEF

THE BLUEPRINT FOR PREVENTING, DETECTING, AND BEATING RANSOMWARE

59% of IT decision makers indicated their Firewall/VPN technologies need to be upgraded over the next two years.[1]

The world is at war with ransomware. It is a threat that every business with a digital presence must contend with. Like any war, you must have a strategy to win against it. The attackers that launch these extortion campaigns certainly do. That's why they keep winning victories on the field of battle. It can be hard to understand how so many enterprises fall victim to ransomware attacks with all the money that has been spent on cybersecurity in the past decade. After all, doesn't every internet connected organization have a firewall? The truth is, you can have an entire arsenal of best of breed cybersecurity tools at your disposal and still fall victim to ransomware. Yes, having the right defensive tools is critical but beating ransomware first requires a well-conceived multi-layer strategy based upon an established framework and implemented by the proper mindset to successfully implement it.

A GROUNDED FRAMEWORK

You can't just create arbitrary cybersecurity policies and expect consistent results. You need a framework core that establishes your cybersecurity activities and desired outcomes that are communicated across all levels of the organization. Fortunately, there are several reputable and established frameworks out there that you can freely utilize. At WEI, we like to suggest the NIST Cybersecurity Framework that touches on all the things you need to secure your organization. The NIST framework is written in common language to bridge the technical gap between internal IT and business leadership. It can be used to help educate stake holders from across the organization to understand, manage and reduce cybersecurity risk by properly aligning cybersecurity policies with business objectives. At the center of this framework lies the core functions that include identify, protect, detect, respond, and recover. Each function plays a critical role in the war against ransomware.

The truth is, you can have an entire arsenal of best of breed cybersecurity tools at your disposal and still fall victim to ransomware.

WHICH FRAMEWORK TIER IS YOUR ORGANIZATION OPERATING FROM?

In actual war, the army needs the support of its leaders and citizenry over the long haul. The same is true of today's cyberwars. The NIST Framework Tiers provide context

WEI

into how an organization approaches cybersecurity when managing its risk exposure. Each tier describes the priority and effort allotted its cybersecurity risk management practices and how it deals with current threat environments and regulatory requirements. Collectively, the tiers represent a progression of mindset ranging from an informal reactive response to approaches that are agile, and risk informed. While most organizations are a tier 1 or tier 2, the objective is to be at least a tier 3 and eventual tier 4. The tiers are outlined as follows.

- **Tier 1** – There is little semblance of a formalized approach to organizational cybersecurity management. Risk is managed in an ad hoc case by case basis. This mindset typically exemplifies a reactionary approach to risk, which stems from the limited awareness of cybersecurity risk at the organizational level.
- **Tier 2** – It is here that an awareness of cybersecurity risk begins to be realized at the organizational level as well as the establishment of risk objectives to govern security initiatives. While management takes more of an active role in prioritized risk management efforts, the initiatives still lack an established organizational-wide policy and cybersecurity information is shared within the organizations on an informal basis.
- **Tier 3** – A formal approach begins to take hold as risk management practices are now expressed as established policies that follow an organization-wide approach. This tier is characterized by repeatable processes as policies are defined and regularly reviewed and cybersecurity practices are regularly updated to address the inevitable changing threat and technology landscapes.
- **Tier 4** – Organizations have reached the top of the summit from a risk management perspective. Not only is the organization able to rapidly adapt to new and evolving sophisticated threats, but leadership has also now fused a relationship between cybersecurity risk and organizational objectives. A totally proactive approach to cybersecurity permeates throughout the organization with user education being a priority.

You can have the best security tools in the industry supported by experienced personnel teams, but without the support of management across the entire organization, your cybersecurity protection will be spotty and vulnerable. While you will win skirmishes from time to time, ransomware will eventually win the day.

USING MULTIPLE SECURITY LAYERS TO COMBAT RISK

Nearly every organization is exposed to cyberattacks today. That is the risk we take in a digitally connected world. Cybersecurity is all about the management and mitigation of risk. That starts with identifying where your risks lie, determining which risks are you willing to accept and prioritizing the risks you choose to mitigate. Every enterprise is exposed to attack avenues. The biggest avenue is your

internet connection, but singularly focusing your efforts to defend this gate would be a mistake. There are many avenues into your network, and that number has vastly increased with the dramatic growth of remote work. Remote work architectures now represent a large attack vector that companies must contend with. For instance, remote access solutions now offer remote users to copy and paste between

their consumer grade laptop and their on-premise corporate desktop. These small but permissive attack avenues are but one example of how the challenge of securing your IT estate has been greatly augmented in recent year.

The truth is that everybody in your workforce represents an attack vector, and that realization is critical in establishing an effective cybersecurity plan. Your users are connected to your enterprise through multiple attack avenues, which is why you need multiple security layers to protect against them. One layer would be an email security solution that would eradicate phishing attacks that target user inboxes. Of course, no email security solution is failsafe, which is why another supplementary layer is an educated user that can identify a suspicious embedded link or attachment and know not to click on it. Another layer would be an enforced configuration policy that denies access to removable drives, preventing users from transferring infected files using USB sticks. Organizations should also consider bringing their firewall inside the organization. Rather than treating the firewall exclusively as a perimeter tool, additional firewalls can be strategically placed to segment, analyze and scrub traffic crisscrossing VLANs or traveling between sites, thus creating more security layers.

To maximize your investment in your next generation firewall, you need to enable all the features and functionality that it already has.

LAYERS THAT WORK COHESIVELY TOGETHER

The effectiveness of your multiple security layers to mitigate ransomware threats and other risk types is further augmented if these layers can work in conjunction with one another. For instance, a user decides to download a file from the internet that contains malicious code. Because the code is part of a zero-day attack that is part of a zero-day threat, the firewall mistakenly lets it through. That's why you have an EDR client serving as another layer that then detects that something isn't right about the file and contains it. While the immediate threat has been avoided, the containment doesn't deter other users from downloading the file. This means the battle might be fought a thousand times, increasing the chances of a successful infiltration. What if instead, the EDR sent the file to a sandbox where it was detonated and identified as malicious. The Sandbox could then forward the code signature to the firewall where it then blocks it from that point on, preventing anyone within the organization from downloading the code ever again. Under this scenario, the EDR clients work as sensors, digital sentries that alert central command, ensuring that the battle only be fought once. That is the power of layered security working in unison together under a united front.

MAXIMIZING THE RESOURCES YOU ALREADY HAVE

Many organizations fail to realize the integrated firewall tools they already have at their disposal while others ignore the treasure trove of information contained within the internal logs of these devices. To maximize your investment in your next generation firewall, you need to enable all the features and functionality that it already has. These untapped features provide additional security layers. Besides the ability to block potentially malicious traffic from infiltrating or leaving the network, firewalls today provide visibility into your traffic patterns. Integrated heuristic tools can actively monitor and analyze incoming traffic for abnormal packet activity, allowing you to act on them. The firewall dispersed throughout your IT estate also contain extensive logging information that can be aggregated and correlated into a historical record, allowing you to discern how an attack occurred in order to contain it. This visibility can be enhanced with an external analyzer or SIEM that can generate actionable reports in real time, giving you the necessary time to react.

LET WEI AID YOU IN THE FIGHT AGAINST RANSOMWARE

Getting to where you need to be is an evolving process. Transitioning from a tier 1 level organization to a tier 3 or 4 doesn't happen overnight on your own. There's also a learning curve when it comes to multilayer security strategy design, strategical firewall placement and logging interpretation. That's where the value of an external cybersecurity partner comes into play. We can help flatten the learning curve and accelerate the implementation of your risk management action plans. Our experienced SMEs can help you access where you are right now, and determine where you need to be, providing you the guidance and expertise to create an effective multilayer cybersecurity strategy, utilizing tools sets that match your risk environment and objectives. Let WEI help you create the blueprint you need to win the war against ransomware.

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.

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.

WEI Dedication meets innovation.

info@wei.com
www.wei.com
43 Northwestern Drive | Salem, NH 03079
800.296.7837