Preparing for the Unpredictable: Proactive Measures Against Cyber Threats

In the last year, we've battled with the cyber security and operational challenges of transitioning to work-at-home. We've also witnessed exponential growth in phishing attacks and ransomware attacks targeting work-at-home users, the healthcare industry, government agencies, educational institutions – and really when you get down to it – targeting everyone.

Just when we thought it couldn't get any worse, we witnessed and are still working through the aftermath of two large-scale and devastating nation state cyber-attacks – SolarWinds and the Microsoft Exchange attacks. We don't know what might be coming next!

With this unprecedented level of cyber activity, we thought it would be a good time to take a step back, gather some lessons learned, and work to prepare ourselves for the next "big cyber-attack" – and since we really don't know where the next big cyber-attack will come from, we need to be prepared to rapidly respond to whatever the attackers throw at us.

We recommend focusing your efforts to prepare for the "next big attack" in three areas:

- Improve your cyber hygiene with the goal of raising the work factor for the attackers. Let's make them pull out something a little more exotic than the exploitation of an unpatched vulnerability to gain access to your infrastructure.
- Deploy active defense capabilities that enable your security team to detect, hunt for, assess, and respond to not only known threats (e.g., known vulnerabilities and attack techniques) but also the more sophisticated and stealthy attack techniques used by nation-state attackers and increasingly by Ransomware gangs (e.g., zero-day exploits, "living off the land" attack techniques, supply chain attacks, etc.). Active defense capabilities are critical to not only helping your organization defend itself from advanced threats, but also helping your organization quickly determine, as details of a new attack become available, if you were breached and how badly.
- Finally, have a well thought out and well-rehearsed incident response plan in the event that you become a victim of the next big attack.

Cyber Hygiene

While the importance of good cyber hygiene is well known, organizations struggle to keep up with the endless stream of CVEs, security patches, and software updates. And attackers continue to take advantage of poor cyber hygiene to gain access to networks though Phishing attacks, drive by attacks, credential compromise, and exploitation of unpatched vulnerabilities.

Our guidance here is not to try and boil the ocean, but instead focus on your most critical and most exposed assets. If you have a large and complex infrastructure, automation is key to keeping these devices secure. For example, automated discovery, inventory, and categorization of the IT assets connected to your networks (i.e., what's on my networks – IT, OT, and IoT), automated tracking of vulnerabilities, and automation to help you assess the risk of assets based on vulnerabilities present on the asset, their criticality to your business operations, and their level of exposure to the Internet and 3rd parties. Fidelis has some great terrain mapping and risk management solutions in this space, so if this is something you continue to struggle with, we suggest you look at what we have to offer. Some other things to consider:

Robust endpoint protection

This is particularly important as we continue to work from home and our endpoints are directly exposed to the Internet through our employees' home networks. We recommend a combination of automated vulnerability management software to keep endpoints up to date with the latest software and patches, anti-virus software to catch signature-based threats, and Endpoint Detection and Response capabilities (EDR) to catch the stealthier attacks.

EDR provides additional benefits for remote employees by enabling your security operations team to quarantine a device that is misbehaving, remotely diagnose the device to determine if and how it was compromised, return the device to a secure state, and apply global policy updates to all your remote devices to ensure other devices are not compromised in a similar way. Fidelis Endpoint, our Endpoint Detection and Response (EDR) platform is another Fidelis offering that is worth a look.

Network segmentation

The end goal here is to create some firebreaks within your architecture to contain an attack by limiting an attacker's ability to move laterally throughout your enterprise. They key here is to group "like" systems that must communicate with each other into a separate network segment (e.g. VLANs) and limit the communication between that network segment and other network segments. The chokepoints created between network segments now become convenient points within your architecture to deploy internal monitoring capabilities. Taking network segmentation a step further, many organizations are moving towards a zero-trust architecture that combines network segmentation with risk aware access controls and transaction-based security monitoring.

Log Retention

Based on the long dwell time associated with the SolarWinds attack, we would suggest revisiting your log retention policy to determine if you are capturing sufficient logs for your critical and exposed systems and if you are retaining the logs long enough. Logs enable you to perform retrospective analysis to determine if you have been compromised by an attack that occurred in the past. Many did not have logs that covered the timeframe of the initial SolarWinds exploit (nine months prior to when the SolarWinds attack was discovered and exposed) and were forced to go down the much harder path of analyzing their networks for signs of post compromise IOCs. Continual reinforcement of cybersecurity best practices: Humans continue to be the weak link in cyber security and require continual reminders about your organization's security policy, procedures, and best practices. The key here is to ensure that employees understand the risks associated with Phishing and Social Engineering attacks, can identify Phishing and Social engineering attacks, and know how to report it.

Active Defense Capabilities

As you may have read in our past blogs about the need to move beyond protective and reactive defense (i.e., passive defense) to proactive, predictive, and retrospective defense (i.e., active defense) in order to defend your enterprise against the full spectrum of cyber threats. Fidelis Elevate is an extended Detection and Response platform purpose-built for Active Defense (per MITRE SHIELD). It helps users "shift left" and engage with and defeat adversaries earlier in the attack lifecycle. Fidelis has been an innovator in this market segment since its inception. Fidelis Elevate XDR unifies detection and response across endpoint (EDR), network (NDR), and cloud with decoys and deception technologies. By coupling XDR with deception technologies, we enable your security operations team to quickly detect and block attacks from sophisticated

threat actors, perform deep inspection/analysis of the environment to assess what if any systems have been compromised, and return compromised systems to normal business operations as quickly as possible.

In a recent blog post, we distilled active defense down to its core elements – an iterative and continuous process of investigation and discovery using threat intelligence, analytics, machine learning, and threat hunting to gain insights into threats impacting your environment. These insights enable your security team to continually tune your defenses and neutralize threats before they can cause damage to your business operations.

Have a Response Plan

Be prepared in case you become the next victim of a big attack by having a response plan in place. Document how business continuity would take place in the event of a disaster or breach. Strategize disaster recovery and how to respond to an attack with supporting playbooks. And take that next step of preparedness by rehearsing your plan on a regular basis through tabletop exercises based on real world threats like a ransomware attack. Additionally, set up offline backups for business-critical data and systems to ensure that you can reconstitute your business-critical systems should a disaster or cyber-attack occur. We also recommend that you have an in-house cyber incident response team in place or have an outside team on retainer, to allow you to take immediate action in the event of an attack. And finally, coordinate your response plan with your organization's General Council as cyber-attacks can often involve a data breach, which carry a number of privacy and reporting requirements.

With these strategies in mind and in play, your enterprise will be safer and more secure against the full spectrum of threats impacting our networks. While we gave a general overview of these solutions, we provide more details and strategies in our Global CISO Playbook for the New Normal.

Ultimately, we're here to help you detect, hunt and respond to sophisticated threat actors targeting your environment, so you don't become a victim of the next big attack. If you'd like to know more about our cybersecurity solutions, contact us.