SECURITY-AS-A-SERVICE

SECURITY-AS-A-SERVICE

HOW YOUR MSP CAN HELP CLIENTS MANAGE THEIR SECURITY

INTRO

On May 12th 2017, an unknown hostile actor wreaked havoc on the British government's National Health Service, FedEx, Telefonica and Deutsche Bahn with its WannaCry worm. While the attack was eventually disarmed, it was not before it crippled institutions in Europe and Asia.

How did the worm attack its victims? WannaCry worked by taking advantage of these companies failing to install a necessary Microsoft security update put out two months prior. By exploiting this weakness, hackers were able to find a backdoor capability that allowed them to use the Eternal Blue SMB exploit.

The scary part of the whole scenario is that if multimillion dollar companies that have thousands of dollars to spend on security and consultants can get hacked, how can small and medium sized businesses possibly keep themselves safe? Moreover, as many small and medium sized businesses (SMBs) rely on MSPs to keep them safe, what should MSPs do to stay ahead of security threats and keep their clients safe?

The answer is that SMBs need to become security conscious. As one MSP noted:

> As far-reaching attacks like WannaCry receive national media coverage, SMB owners are beginning to accept that it is now mission-critical to have a meaningful security strategy in place.[1]

THE GOAL OF THIS WHITEPAPER IS TO:

- Highlight approaches to managed security
- Highlight ConnectWise's value in aiding MSPs' security management
- Indicate why critical alerting is a necessary integration

APPROACHES TO MANAGED SECURITY

The FIRST STEP an MSP should take is to encourage clients to adopt a culture of security. This means that clients understand they are not an island and that they run a good chance of being attacked by a virus or worm or ransomware. As such, they need to learn to practice proper security hygiene and manage their users more carefully.

Practically, this means that clients realize they cannot just implement anti-virus protection such as Webroot and consider themselves protected. Instead, clients need to be willing to invest in antivirus, malware, internet security, firewalls, email protection and backups in order to be somewhat secure.

[1] http://mspmentor.net/managed-security-services/ceo-forum-three-pillars-successful-managed-security-services-offering

Additionally, this means that clients realize that users also need to be managed. Every worker will not have access to every file. Instead, owners will practice the principle of least privilege and only provide users with the access they need to do their job. Since users are the overwhelming cause of viruses being introduced into the system, users must be managed and limited so that they don't accidentally bring the whole system down.

The SECOND STEP to managing security is realizing that you need to be proactive and constantly monitor your clients' security profile. This is because no matter how strict you are with privileges and ensuring you have the proper software to monitor the client's stack, your client has a good chance of becoming a target. The best way to manage clients, keep track of software updates and alerts is through a ticketing system like ConnectWise Manage.

HOW CONNECTWISE CAN HELP MANAGE SECURITY AND YOUR CLIENTS

ConnectWise Manage becomes a robust tool when MSPs look to improve their management of clients' security profile as it allows them to receive ticket updates when issues are spotted. As an MSP using ConnectWise, you can learn that your client's version of the Windows OS was updated. You can also learn of something more sinister.

The point is, that by using ConnectWise you can keep track of your client's security and make sure that necessary updates were made to their system. You will have a record of changes made rather than having to guess at them.

However, as a busy MSP, you probably have multiple clients whose security you are monitoring. Ideally, all your clients would use the same level of security and back-up and you could keep them synchronized. The reality is that this is probably not the case. More likely, you have multiple clients on multiple platforms and keeping track of all their updates can create a lot of noise.

While it is important to know that they had their latest backup completed successfully, do you really want to get alerted to this fact? Probably not. Therefore it is important to have a way to differentiate when a ConnectWise ticket represents an incident that requires your attention and when you can simply file the ticket. To achieve this result, you need an alerting tool that can fit into ConnectWise's rule based ticketing.

WHY CRITICAL ALERTING IS A CRITICAL ALLY

When a critical incident is ticketed by ConnectWise, it is imperative that the MSP receive an alert. Upon receiving an alert, the MSP can spring into action and implement proper remediation. Yet implementing this remediation process is more complex that simply connecting tickets to alerts. For alerting to be effective, MSPs need to ensure that their alerting platform has the following characteristics:

- The alert comes with specific information as to which device is having trouble and the nature of the incident.
- A persistent alert is sent to the on-call engineer apprising them of the event. The alert needs to continue until it is responded to.
- If the alert is not responded to within a given time span, it needs to escalate to the next engineer on call.
- When the incident is responded to, this action is updated in the ticketing database
- Both MSP and client need real-time updates on an incident's status.

- Management should be able to monitor and audits response times by its engineers to ensure your MSP meets SLAs

Once the alert is received proper remediation can begin. This remediation can be actions such as ensuring a virus is eradicated, helping the client restore the proper back-ups or reformatting drives that have been effected.

The important conclusion to draw here is that it is not enough to simply have cybersecurity software. This software needs to be integrated with tickets and the tickets need to be given a voice. The strongest and clearest voice possible is provided by a robust alert management platform.

CONCLUSION

Adding security to an MSP practice is a difficult proposition. In addition to providing the proper software, MSPs must encourage a security based culture that has proper security hygiene, security workflows and alerting. In addition to offering firewall and endpoint protection software, MSPs need to consider how they will be alerted when an incident occurs.

The job of a good MSP is to act as a trusted advisor. When MSPs offer true vulnerability management and remediation through providing layers of security, they become trusted advisors.

ABOUT ONPAGE

OnPage is a cloud-based, industry leading smartphone application for high-priority, real enterprise messaging. OnPage provides critical alerts to Managed Service Providers based on notifications from RMM or PSA system for faster incident resolution.

Using OnPage you get instant visibility and feedback on alerts. As part of your IT service management, you can track alert delivery, ticket status, and responses.

As a result, you will improve MTTR and better manage your clients’ ecosystem by decreasing service interruptions. As an organization, you will improve responsiveness to SLAs and lower your and your clients’ costs.

TO LEARN MORE, VISIT OUR WEBSITE OR CALL: ONPAGE.COM/CONTACT-US 781-916-0040

Visit iTunes or Google Play from your smart phone or tablet to download the OnPage app.

Available on the App Store

Get it on Google play