WHAT IS THREAT REMEDIATION? THREAT REMEDIATION EXPLAINED

With the recent onset of ransomware plaguing the Internet, threat remediation has become an important piece of the cybersecurity puzzle for businesses who wish to protect their digital assets.

But what exactly does threat remediation mean? What are the most effective methods for successful threat remediation? And how can organizations know if they have adopted the right way for optimal protection?

Now more than ever, threat remediation will have a tremendous impact on the future of cybersecurity.

What is Threat Remediation?

Threat remediation refers to the process by which organizations identify and resolve threats to their systems. A threat is anything that can infiltrate your system to steal information, hurt operations or damage your software and hardware. In 2016, top threats were machine-to-machine attacks, headless worms, cloud jailbreaking, ghostware and two-faced malware.

Today, one of the biggest threats to enterprise businesses happens to be ransomware, a form of malware that seizes your operations until you pay exorbitant costs that increase over time. Ransomware, if not paid, can permanently lock you out of important files that are critical for business operations.

Organizations who are yet to embrace the principles of threat remediation -- such as implementing virus prevention software -- have higher risk of infections like ransomware or cloud jailbreaking.

Out with the old method of defense

In simpler times, if you owned a PC and ran antivirus software, you were usually all set. But in today's complex landscape of cybersecurity, this is no longer the case.

While it is still advisable that all organizations run anti-virus software on any device connected to a network, they must also understand that no connected computer is immune to certain threats. And that remediation is critical.

Another common line of defense involves keeping computer operating systems and software updated. While Microsoft Windows computers running the newest version of software can often withstand threats like WannaCry, clever hackers are always working on ways to get around newly updated systems and into cloud systems that are essential to business operations.

Threat remediation: the way forward

The most effective way to handle cybersecurity is to be proactive. This can be achieved in two important steps:

- **Step 1:** Run a thorough Risk Assessment
- **Step 2:** Deploy a Vulnerability Management System

Sounds easy enough but threat remediation may not be as simple as it looks on paper. Implementing the following steps will ensure your organization takes further control of its cybersecurity needs.

Step 1: Risk Assessment

A risk assessment refers to the process by which a business can gather intelligence about potential vulnerabilities in their systems and operations that may leave them susceptible to cyber threats. It's the first essential piece of the puzzle for coming up with any threat remediation strategy.

When preparing to conduct a risk assessment for your organization, be sure to consider these nine key areas:

1. **Third Party Vendors:** How secure are their operations? How much visibility and insight do you have? Who is the cybersecurity point of contact for each vendor you work with?
2. **Security Management:** Who is in charge of implementing strategy? What strategy is being implemented? Has it been effective? What changes should be made?
3. **Security Architecture:** What programs are currently in place? How effective are they? What measures can be added? What tools are available to teach employees about the current architecture?
4. **Emerging Technologies:** What can be added to enhance security? How secure are new technologies that are currently in place? Where are these technologies applied - physical server, virtual server, cloud?
5. **Regulations and Policy:** What is the current security policy? How does it impact overall security? What updates can be made?

6. **Incident and Crisis Management:** How are you monitoring for incidents currently? How well is it working? How are incidents resolved today?
7. **Identity Management:** What authentications are in place? What password protections are available?
8. **Awareness & Education:** What programs are in place to educate employees about cybersecurity? What tools and guidelines are given to employees?
9. **Threat & Vulnerability Management:** What systems are there to identify and remediate vulnerabilities and threats?

There are numerous goals of a risk assessment. Some include assisting IT departments in a total inventory of assets, determining a standard for cataloging risk and vulnerabilities and making it easier to prioritize which vulnerabilities should be tackled first.

It is important to note that the best way to prioritize risk data is in a way that is easily actionable. A long list of vulnerabilities on a spreadsheet is not the most functional document. However, creating actionable data means developing a system where easily digestible information can be shared among key stakeholders, typically the essential members of security and operations teams.

Risk assessments can be conducted by in-house IT departments and members of executive management, or by a third-party cybersecurity partner, equipped to handle the needs of your business.

Step 2: Deploy a Vulnerability Management System

After conducting a thorough risk assessment and learning each vulnerability, you can now begin to implement a vulnerability management system. With vulnerabilities and risks prioritized, companies can focus on protecting the most important assets first.

This can be achieved utilizing a vulnerability management system (VMS) which actively monitors risk and responds to threats.

Active Network Monitoring

The process of active monitoring for network security includes the collection and examination of security data and escalation for remediation if necessary. This security data comes in the form of indicators that serve as warnings of potential vulnerabilities.

Indicators & Warnings

Indicators & Warnings (I&W) form a process by which networks are monitored to increase the likelihood of identifying threats. Having vulnerabilities, alone, does not necessarily translate into threats that are trying to intrude on your system. However, the I&W process will provide the requisite guidance.

Indicators are observable actions that suggest there may be an issue. In a system of I&Ws, these indicators produce a warning. A VMS alerts stakeholders of the warning signs, and automates remediation processes.

Vulnerability Detection and Remediation

According to Gartner, over 99% of the successful exploits will be from vulnerabilities that were known for at least a year. Thus, it's critically important to reduce these vulnerabilities before bad actors get into your system, forcing you to try and catch them in the act. This is akin to locking your front door, rather than leaving it open and waiting for a burglar to come in.

BMC's SecOps Response Service, offers quick identification, planning and remediation of vulnerabilities helping to reduce the attack surface and overall risk to the business.

Some examples of automated vulnerability remediation include:

- Providing prioritized to-do lists
- Identifying and closing blind spots
- Patching vulnerable software and network devices
- Changing configurations
- Removing connections
- Changing workflows and rules
- Integrating with other programs and protocols to offer full protection

How do you know if your threat remediation strategy is working?

Context

A lack of understanding of context within the threat remediation process poses a concern when it comes to evaluating effectiveness. For instance, your automated VMS can return thousands of potential vulnerabilities in your system. Some may be big and others small. Without proper context,that will help in prioritizing your indicators and warnings, the process of threat remediation can become overwhelming at best.

Understanding context means knowing not only which threats are flagged as high-risk, but also the location and the potential ripple effect of each threat. A VMS that only identifies threats without telling you how to locate them is doing only half the job.

Training

Apart from conducting risk assessments and deploying a VMS, organizations cannot overlook the importance of training across all departments. Promoting a culture where employees are empowered against threats is another effective tool within the threat remediation arsenal. What does this entail?

Cybersecurity awareness means providing quick reference guides, training and IT support that will ensure employees are prepared to identify issues and escalate them if needed. In addition, understanding the organization's awareness of cybersecurity processes should be a part of your risk assessment even though it's not something that can be addressed with an automated VMS program.

Threat remediation: The future of cybersecurity

Threat remediation should be viewed as an active approach to cybersecurity measures. It refers to the process by which risk is assessed, indicators are identified, and warnings are flagged, prioritized

and resolved in a cyclical fashion. Effective threat remediation considers context, makes available actionable data and is part of an overall cybersecurity program that includes more traditional measures like preventive anti-virus software and raising employee cybersecurity awareness.

Threat remediation processes can be automated with a Vulnerability Management System and the most valuable threat remediation software must provide relevant information about threats in a way that can be easily distributed and consumed. It should be able to resolve priorities without human interaction.

BladeLogic Server Automation

As more and more businesses move to the cloud; the landscape of cybersecurity continues to change in drastic ways. And even those organizations who may have already implemented some form of vulnerability remediation, are left asking how to protect all their digital assets.

BMC offers digital enterprise management solutions that automate and integrate all of your cloud, virtual and physical servers with built in security measures. To learn more about how BMC's BladeLogic Server Automation can help you improve security as well as compliance for your enterprise, contact us today.