RSM: HELPING SMALL BUSINESSES BUILD A SCALABLE SECURITY ARCHITECTURE

Middle market businesses are facing many challenges when it comes to meeting cybersecurity demands. The transition to a hybrid workforce, for example, has created new risks by expanding the attack surface, and ransomware continues to be a major threat.

Compared to large enterprises, middle market companies simply do not have the same time, budget, and resources to defend against cybercrime. The absence of the right tools and the lack of a dedicated security team often force these smaller companies to take a reactive approach to attacks.

With rising cybersecurity insurance premiums, midsized businesses must find ways to meet both higher costs and broadened insurance requirements. Security solutions that can scale as the business grows, such as cloud-based solutions, are essential.

Here's an overview of five aspects of IT security your organization should be aware of when assessing your security posture.

DOMAIN NAME SERVICES SECURITY

Domain name services, or DNS, security is a method of web filtering that blocks malicious traffic on the internet. DNS traffic often flows through firewalls, making a different approach to security necessary.

Without DNS inspection and filtering, workers may click on malicious website links and phishing emails, infecting your systems with malware. In this era of hybrid work, DNS security is especially important because it enforces the same security policies for remote workers as for in-office employees.

MULTI-FACTOR AUTHENTICATION

Multifactor authentication—MFA—strengthens identity and access management by using a secondary method of authentication. Passwords are a notoriously ineffective method of controlling access, so MFA adds one or more extra layers of protection, such as a token, a single-use code, or a biometric verification.

Middle market companies need MFA for access and authority management when remote users are accessing the network.

BACKUP STRATEGY

Ransomware is one of the biggest threats in today's risk landscape, making a backup strategy indispensable for middle market businesses. When a ransomware attack hits, it encrypts all company files and sometimes deletes on-site backup files.

Middle market companies need a way to recover files, network equipment, and hardware configurations after an attack. An effective backup and recovery strategy involves making several copies of data on different storage mediums and storing these backups both on-site and off-site, which can be accomplished with the cloud. Companies should also make regular backup and recovery testing a part of their strategy.

PATCH MANAGEMENT

Cybercriminals often exploit unpatched applications, servers, and devices to stage attacks. After an attack, malware may spread, moving laterally to unpatched parts of the system. Exploit attacks can also originate at the unpatched asset when cybercriminals use code to gain access and unleash malware through the vulnerability.

Workstations and hybrid servers need to be protected with patch management that conducts regularly scheduled scans to uncover and eliminate any vulnerabilities.

NEXT-GENERATION FIREWALL

When middle market companies apply for or renew their cybersecurity insurance policies, many insurance providers now require a next-generation firewall, or NGFW, to issue a policy.

NGFWs provide additional features that aren't included in traditional firewall solutions, such as application awareness and control, an integrated intrusion prevention system, and cloud-delivered threat intelligence. A top NGFW enables full visibility across the network and offers accelerated threat detection.

CHECK ALL THE BOXES FOR IT SECURITY

If your organization is missing any of the items on this IT security checklist, working with a managed services provider (MSP) for security will help you overcome the challenges of strengthening your security on a budget. An MSP can also work with you to assess your security further to uncover additional gaps.

HOW RSM CAN HELP

As a Cisco Certified Gold Partner, RSM provides managed services for leading security solutions. Our team has certified experience in Cisco solutions and takes a holistic approach to understanding your company's security requirements.

Our advisors have a wide variety of skills; they can assist you with the solution that best fits your needs. With RSM, your company will have access to a large team of experienced consultants who can augment your internal IT staff and ensure you take a proactive approach to security.

+1 800 274 3978
rsmus.com

RSM