BEST PRACTICES: TOP 10 TIPS FOR SELECTING AN MSSP

Most organizations and businesses have trouble keeping up with today's constant barrage of cyber threats. Many are turning to MSSPs (managed security services providers) to protect their networks cost-effectively and reliably. But choosing an MSSP requires thought and research. Not all offer the same levels of protection, so you should focus your search on a provider with a solid track record and reputation. Here are 10 best practices to follow when selecting an MSSP.

1. GETTING TO KNOW YOU

The first clue that you're talking to the right MSSP is that the provider asks about your organizational needs and strategic goals. A provider needs to understand your IT environment to properly secure it. If a provider doesn't ask enough questions about what's in place, how it's used and which users need what level of access, you probably should find another.

2. REPUTATION MATTERS

Handing over IT security to a third party requires trust. Ask for references and get feedback from existing customers about the MSSP's reliability and expertise, and how responsive it is when clients need support. Find out if the MSSP has stopped any threats and, if remediation was required, how effective it was.

3. CLOUD? COVERED

Just because your organization is moving to the cloud, you can't take your eyes off the ball. You'll want an MSSP that understands cloud security. Do you need to protect SaaS applications, infrastructure, or both? Your provider should offer a cloud-native solution that fully integrates with data from your network, endpoints and SIEM to detect threats and misconfigurations quickly and remediate any issues.

4. MENU, PLEASE

Security requires more than firewalls, patch updates and antivirus software. These days, you need functions such as asset discovery, vulnerability assessments, intrusion detection, log management, threat intelligence and behavior monitoring. If an MSSP doesn't deliver these functions, it may not be able to fully protect you in a business environment where 1 million new malware threats are released every day.

5. TECHNICAL KNOW-HOW

Some MSSPs focus on specific security areas or do little more than monitor your environment. That may not meet your needs. Be sure to check on the MSSP's levels of expertise and experience. Ask about its technical team – how much experience it has and what certifications its members hold. A well-rounded MSSP should have experts in multiple areas of IT security, and they should attend regular training to keep up with new and evolving threats.

6. THERE FOR YOU

It's one thing to have the best technology and a well-trained staff, but what happens when you need support? An MSSP needs to be responsive and ready to respond to any inquiries you may have about their service or new threats. Considering what's at stake – your organization's data – you need a provider that responds promptly to your calls, especially if you believe an attack or breach is underway.

7. KEEPING IT TOGETHER

An MSSP, like any other provider of remote and cloud-based services, functions better by leveraging automation and repeatable processes as much as possible. All processes and procedures should be documented and clearly defined. If the provider is unclear or unable to explain its services, take that as a sign it might struggle to deliver on promises.

8. HUMAN FACTOR

So, you've done your homework and contracted an MSSP that secures your data. But who secures the users? Human action, malicious or otherwise, plays a major role in security incidents, which explains why cybercriminals rely so much on tactics like ransomware and phishing. Find out if your MSSP offers exercises and red teaming to help your security team and other departments prepare for insider threats and avoid risky practices that could result in a security incident.

9. IT'S THE LAW

Aside from protecting your IT environment, your MSSP must have the tools and know-how to help you comply with all applicable privacy and security laws. The MSSP must know what laws apply to your particular organization, and, from a technology standpoint, offer functionality such as endpoint protection, vulnerability assessment, intrusion detection and log management. The MSSP should also provide the ability to integrate data from legacy security tools to ensure compliance.

10. VALUE VS. COST

When contracting an MSSP, you'll want to know upfront how much the provider charges and exactly what you're paying for. Try to get the best possible rates but avoid basing decisions strictly on cost. Keep in mind the value of the security services, and how much it can cost to recover from a security incident, especially when valuable private records and business data are stolen.

MOTOROLA SOLUTIONS - YOUR TRUSTED PARTNER

As a leading provider of mission-critical solutions, we understand your mission can only be as secure as your partners enable you to be. Our goal is to provide you with transparency, accountability and security that's built-in from the start.

We believe that our set of highly knowledgeable people with industry certifications, best-in-class organizational policies and procedures and state-of-the-art automation and analytics tools enables us to uniquely deliver enhanced cybersecurity solutions that address your needs today and in the future.

For more information on managed security services, contact your Motorola Solutions representative or visit us at **www.motorolasolutions.com/cybersecurity**

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**