IS YOUR DATA SECURE?

8 Best Practices for Vetting Vendors

naglotech.
IT SOLUTIONS FOR BUSINESS

An effective way to bolster your business's data security is to work with a Managed Service Provider (MSP).

We address network vulnerabilities to prevent cyber criminals from exploiting them.

Besides monitoring and organising your servers, an MSP plays a pivotal role in the cyber security programme of your business.

We implement several strategies to shield your network from attacks and protect your data.

For instance, many providers use email authentication protocols to monitor your server's vulnerabilities.

This results in enhanced system security.

Another common practice is training your employees to ensure they follow the highest security standards.

This is especially important if you have remote team members since it's more difficult to keep track of their activities.

To tackle this issue, we teach your staff how to operate safely to avoid harm to your company's infrastructure and reputation.

On top of that, we neutralise various threats due to our proactive approach.

We offer several tools such as firewalls and endpoint detection to control the traffic and stave off cyber attacks. We also install antivirus software and email security to stop intrusion attempts.

Needless to say, we can shield you from a wide array of cyber security issues. But it's vital to work with the right provider.

To ensure this happens, you should look for these 8 best practices in an MSP.

Using & Enforcing Multi-Factor Authentication (MFA)

Cyber criminals are becoming proficient at accessing your credentials, so it’s critical to enable MFA for all your users.

It consists of three elements: a password, security token, and biometric verification.

Consequently, if attackers breach one security layer, they’ll still have to do a lot of digging to access your information.

01

02

Making Patching A Priority

Application and operating system exploits are common. Hackers target them to access your system and compromise your data, but you can prevent this through regular patching.

Making sure your system is up-to-date with the latest security standards decreases the risk of exploitation.

03

Conducting Regular Cyber Security Audits

An MSP must be aware of onboarding, offboarding, and lateral movements within an organisation.

This warrants frequent audits to assess the competency of your team.

Conducting regular audits mitigates this risk. It enables us to implement some of the most effective access privilege limitations.

Backups are crucial for tackling malicious activities and ensuring operational continuity after cyber attacks.

They also help address whether you can access the latest version of your data and applications. This feature is vital for enterprises that must adhere to compliance requirements, including PCI-DSS and GDPR.

But besides implementing on-site backups, we also set up off-site versions. If attackers compromise the Remote Monitoring & Management software, they can most likely reach on-site backups, too.

So, to avoid disasters, businesses should have an off-site backup accessible to only a few people. It should also be offline for greater security.

04

Have an Off-Site Backup

Incorporating Log Monitoring

Log monitoring is analysing your logs for potential glitches.

As we scrutinise your records, we can detect traffic from harmful sources and provide a clear idea of threat patterns. And over time, we deploy countermeasures to seal these gaps.

For example, we use reliable security information and event management (SIEM) tools. They facilitate scanning through piles of information to enable faster threat detection.

Launching Phishing Campaigns

Phishing criminals target your team members, posing as legitimate institutions to steal your data.

Unfortunately, most attacks succeed because of human error, meaning we are aware of and monitor employees' behaviour.

Setting up fake phishing campaigns is a great way to test your team's ability to respond to phishing attacks. It allows us to pinpoint and improve inadequate responses, bolstering data security.

Choose Your Software Carefully & Secure Endpoints

From small browser plugins to large-scale business systems, we take data protection and cyber security seriously. Learn about software creators' commitment to these aspects before using applications. Cyber Essentials and ISO 27001 certifications are good indicators.

Furthermore, we employ web filtering tools, antivirus software, and email authentication to fend off ransomware attacks through malicious emails. We ensure each endpoint and your virus definition library are secure and up-to-date with the latest standards.

Set Alerts & Document Everything

We configure our systems to receive alerts upon system changes, so we can work proactively and tackle threats early on. Many platforms automate this process through rules, templates, personalisation, and direct tickets to the system. This eliminates manual digging, saving precious time.

Another useful strategy is to document your cyber security information, such as your defence mechanisms, emergency guidelines, and disaster recovery plans. You should also review it regularly to help pre-empt cyber attacks.

While digitalisation has significantly streamlined your operations, it’s also made you more susceptible to data theft.

To ensure criminals don’t get their hands on valuable information and ruin your reputation, your MSP needs to adopt well-established security practices.

If your provider hasn’t introduced off-site backups, regular patches, and employee training, you’re not getting your money’s worth. Hence, you may be frustrated since your provider isn’t delivering the necessary results.

We can help you. Reach out to us for a quick 15-minute chat, and our tech experts will do their best to show you a way out of your cyber security crunch.