Network Security is an Essential Piece of Your IT Strategy

stasmayer.com

Stasmayer INCORPORATED 20 YEARS

Network security is a complex combination of factors that work together to keep users, companies, and their information secure. It involves multiple layers of defenses, each with their own policies and controls that operate both within and on the edges of the network.

“According to Juniper Research, cybercrime will cause over $5 trillion in losses globally in 2024.”

These controls allow authorized users to access the network while blocking unauthorized users such as malicious actors. Essentially, this allows people to have the benefits of using online networks while protecting their rights and interests.

The internet is a public network, a huge online system that connects millions of other networks and individual computers. Network security, therefore, is not only critical for companies with their own internal networks, but for anyone who uses the internet.

More people are using the internet than ever before and online technologies are being increasingly integrated into our daily lives. At the same time, cyber-attacks have emerged as a major issue: according to Juniper Research, cybercrime will cause over $5 trillion in losses globally in 2024.

Network breaches can be detrimental to companies, leading to loss of data, loss of customers, and significant damage to their reputation. Network threats can be internal too, and businesses need to protect themselves from dishonest staff members and other malicious insiders through internal network controls.

Network security is indispensable to businesses in order to protect themselves from these threats, whether internal or external. It should be a central part of any company's IT strategy.

Common Network Threats

One of the most common threats to networks is caused by malware such as computer viruses. There are reportedly over 1 billion types of malware in existence today. Online virus attacks are all too common, and these can be devastating to networks in a number of ways. Viruses attack network assets, corrupting files and destroying data.

For employees, this can be at best, frustrating, and at worst, make it impossible for them to do their jobs, as important information is deleted or inaccessible. In turn, this lowers productivity on a business-wide level, making companies less profitable.

If your network is insecure, you can also be vulnerable to data breaches from hackers. Hackers are malicious actors that break into your network from anywhere in the world in order to access your data. They generally do this for their own financial gain, for example by stealing financial information or trade secrets that they can sell to your competitors.

Breaches can occur internally also, sometimes due to malicious insiders who deliberately steal, misuse or leak information. In other cases, data may be compromised by staff members accidentally, such as when they connect to an unsecured WiFi network, send an email to the wrong person, or misplace a work device. Whatever the reason, these problems represent a huge financial cost to businesses. According to IBM, the averge data breach cost US companies $4.24 million per incident in 2021..

“According to IBM, the averge data breach cost US companies $4.24 million per incident in 2021.”

Other issues that networks can experience include software vulnerabilities caused by not updating software to the latest version. This can put users and companies at risk, as out-dated software slows down computers and the network overall. This, in turn, makes employees less efficient. It could also cause the entire network to crash, meaning potential lost business and income.

How Network Security Monitoring Can Protect Businesses

Network security risks have the potential to cause businesses significant damage through loss of productivity, data, clients, and reputation. Furthermore, these threats are immense. Cybercrime is estimated to put a total value of $5.2 trillion at risk globally over the next five years.

It is, therefore, cause for concern that many businesses are underprepared to deal with these threats and do not have adequate network security in place. According to a 2018 Minerva Labs survey, the majority of IT professionals reported that their organization was not secure enough against cyber attacks.

Network security monitoring can help to protect your network and your business interests in a variety of ways. Firstly, it keeps your network secure against cyber attackers and data breaches. Network security monitoring allows you to keep on top of threats and issues, remotely from anywhere, even if you don’t have a dedicated in-house cybersecurity team.

What Makes a Good Network Security Strategy?

A strong network security strategy that is implemented effectively is a company’s best protection against cybersecurity threats. It is critical that every organization has a centralized network strategy that manages upgrades, the distribution of policies and other network concerns so that these aspects can be tightly controlled, thus ensuring the network stays secure.

Strong networks are also segmented, keeping different parts of the network separate for distinct purposes. Networks should be interconnected only as much as they need to be, to limit the potential for data breaches as much as possible.

A good network strategy will also accommodate both on-site and cloudbased use of the network. Modern employees are increasingly working remotely for at least part of the time, and the network needs to allow for this while maintaining security at the same time.

Finally, it is important that any network strategy incorporates network security training at all levels. Each member of an organization is responsible for network security, and every employee could potentially jeopardize that security. It is therefore critical that all staff members are thoroughly briefed on the importance of network security, as well as trained in best practices.

A managed service provider can help to implement this strategy by ensuring the best tactics are used in order to strengthen the network and guarantee the highest level of protection against threats. Managed service providers allow businesses that lack the internal resources of large, multinational corporations to manage their networks, and detect and address threats.

Take Action

In the context of ever-growing cybersecurity threats with the potential to devastate companies of all sizes, network security is critical to all businesses. Every company should effectively address network security as part of their IT strategy, with a centralized approach that comprehensively protects the network against internal and external threats.

A managed service provider is an invaluable asset in helping you to implement this strategy. An MSP can give you the best level of protection against hackers, malware, and accidental data breaches. Contact us today to learn how we can help you implement the best possible network security strategy to protect your business.

Contact Us

stasmayer.com

843-724-3440

2420 Mall Drive, Suite 201
North Charleston, SC 29406