IT 365

BEST PRACTICE GUIDE

Effective Perimeter Security

How to build a secure digital fence

It’s easy to feel powerless in the face of a rising tide of cybercrime. But by taking some relatively simple actions, your business can significantly improve its defences against this new threat.

Hardly a day goes by without a shocking cybercrime story hitting the news headlines. Hospitals are forced to shut down all their IT due to a ransomware attack. Major companies suffer the theft of customer data. Online services are put out of action by massive digital assaults.

The stories you don’t read about are the millions of attempts at cybercrime that are thwarted. They are usually prevented by someone having carried out a little planning and preparation, which includes erecting and maintaining a digital security fence around their organisation.

The components in detail...

A virtual fence, also known as digital perimeter security, is made up of various elements. To provide the best possible protection, all these elements need to be working together to close all the possible gaps.

ROUTERS

Router security is hugely important, because a router marks the digital boundary between your IT network and the outside world. Every router has its own security settings, that can be configured in line with the rest of your network. Incredibly, many organisations install routers without changing the default settings, making it much easier for a hacker or rogue software to break in.

FIREWALLS

Your firewall is essentially a piece of software that analyses all the digital traffic that your routers don't turn away. It filters everything and only allows legitimate activity to keep coming through. Again, a poorly configured or out-of-date firewall is likely to have many holes in it.

ANTIVIRUS & ANTISPAM SOFTWARE

This scans all incoming data, such as emails and their attachments, for known virus and malware threats, and for spam. It's essential that it's kept up to date, because new threats are discovered daily. While much of spam is harmless junk that simply clogs up email systems, some of it carries malware.

SYSTEM ARCHITECTURE

Once a threat finds its way into your organisation's IT network, the design of that network will affect how fast it spreads, and what data is affected. A poorly designed system could allow ransomware to destroy your firm's entire database, effectively killing the business.

WE CAN HELP YOU BUILD A SECURE DIGITAL PERIMETER

By keeping ourselves up to date with the latest best practices and tools for digital security, we're well positioned to advise our clients on the current trends and the threats they're likely to face.

If you would like to know more about the cybersecurity issues facing your business, or how to protect yourself from the growing risks from cybercrime, give us a call on 0808 168 9135 or email enquiries@itsupport365.co.uk. We would be pleased to have a no-obligation conversation with you.

Alternatively, follow us as we share news updates and information on Twitter, Facebook or LinkedIn.

It's impossible to create an IT network that's 100% secure. But it's relatively easy to significantly increase security by implementing the right tools, configuring them to work together, and keeping them up to date.