The Changing Cyber Security Landscape

The cyber security landscape is always evolving.

As an MSP, you need to prepare an effective defence to protect your customers. By looking back at the cyber threats of 2021, and ahead to those of 2022, we will help your MSP to deliver the strongest possible cyber security services.

The Effect of COVID-19 on Cyber Crime

Since the beginning of the pandemic, cyber crime has increased by:

600%

Cyber attacks using previously unseen malware/methods have risen from:

25% to 35%

66%

of small businesses have experienced a cyber attack in the past 12 months

A Year in Cyber Crime: The Threats of 2021

Phishing

Phishing attacks account for over 90% of all data breaches.

Ransomware

There were more than 500M ransomware attacks attempted globally in 2021.

DDos Attacks

Ransom DDos attacks increased by 29% over the course of 2021.

Network Hijacking

VPN attacks rose by almost 2000% in 2021.

Cyrptojacking

Nearly 500,000 people were victims of cryptojacking in Q1 of 2021.

Looking Ahead: The Predicted Threats of 2022

Modern Ransomware

Targets enterprises using human operated scripts and malware to encrypt and exfiltrate data.

Internet of Things Attacks

IoT commonly exploited by cyber criminals wishing to gain access to secure digital systems.

Man in the Middle Attacks

A cyber criminal intercepts data being transferred through a connection between two points/people.

Deep Fake Threats

Hackers use deep fake technology to bypass multi-factor and biometric authentication and access confidential data.

Supply Chain Attacks

Aimed at software developers and suppliers: cyber criminals attempt to infect legitimate code, updates or applications with malware.

Insider Threats

Current and ex-employees with access to the corporate network pose insider threats. Can be malicious or accidental.

Prepare for The Threats of 2022

Audit and inventory

Targets enterprises using human operated scripts and malware to encrypt and exfiltrate data.

Configure and monitor

Configure software, hardware and network infrastructure. Monitor network ports, protocols and services.

Patch and update

Conduct patching and update operating systems and applications.

Protect and recover

Enforce data protection, backup, and recovery measures and implement multifactor authentication.

Secure and defend

Perform sandbox analysis with Trend Micro Email Security, and enable advanced detection technologies (like Vision One).

Train and test

Perform security skills assessments and training regularly and conduct red-team exercises and penetration tests.

Selling Cyber Security Services: Demonstrating Your Value

Establish
A strong client relationship

Maintain
Transparent communication

Share
Your security expertise

Remain
Responsive to evolving needs

Book a meeting with one of our representatives today to discover how our unique products and services can optimise your MSP's cyber security offering.

BOOK A MEETING