TREND MICRO™

The Changing Cyber Security Landscape

As cyber threats continue to evolve, ensure your MSP's security offering delivers a comprehensive defence

COVID-19: a golden opportunity for cyber criminals

Since March 2020, the way businesses work has changed dramatically and, potentially, for good. As the pandemic swept the globe and employees were confined to their homes, organisations became increasingly reliant on technology solutions to support them through the transition to remote working.

Unfortunately, as emails supported enterprises and laptops became lifelines, cyber criminals were presented with a significant opportunity to capitalise on businesses struggling to adapt.

Since the beginning of the pandemic, cyber crime has increased by 600% and has manifested itself in a variety of destructive ways.

47% of individuals fall for a phishing scam while working from home.

The average cost of a data breach was $1.07 million higher where remote work was a factor in causing the breach.

Between February and May 2020, more than half a million people were affected by personal video conferencing data breaches.

Cyber attacks using previously unseen malware or methods have risen from 25% prior to the pandemic to 35%.

(Sources: Deloitte and IBM)

In 2022, as new strains of COVID continue to rear their ugly heads, and businesses continue to uphold remote or hybrid working procedures, the opportunities for cyber criminals remain expansive. As an MSP, you must ensure that your cyber security offering is robust and comprehensive to defend your customers from the negative impacts of cyber crime.

Effective preparation is your strongest defence

In 2021, cyber criminals continued to capitalise on the gains they had made in 2020, and the resulting substantial increase in attacks had devastating effects for businesses across the globe, financially, legally and operationally.

Small and medium-sized businesses, those who make up the majority of your MSP's client base, are the most at risk.

43%
of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

66%
of small businesses have experienced a cyber attack in the past 12 months.

69%
of small businesses say that cyber attacks are becoming more targeted.

(Source: Ponemon Institute)

When it comes to cyber security, we believe that knowledge is power. To help your MSP prepare effectively for the ever-evolving cyber threat, we have created a comprehensive guide to the changing security landscape. By looking back at the cyber threats of 2021, and ahead to those of 2022, we will help your MSP to prepare the strongest possible cyber security services.

TREND MICRO

Looking back: a year in cyber crime

To prepare your MSP for the security landscape of 2022, you must assess the security trends that dominated 2021 and learn from the patterns that emerged. In particular, five cyber threats wreaked havoc over the course of the last year.

Phishing

The actor

Phishing emails are an increasingly common, extremely pervasive and unfortunately successful form of cyber attack, founded on the principles of social engineering. Cyber criminals masquerade as official, legitimate or trusted correspondents, and send targeted messages designed to trick victims into divulging sensitive information or downloading malware onto their device. 96% of phishing attacks are sent via email, but these scams can also take the form of text messages or malicious websites.

According to a 2021 report from CISCO, Phishing attacks account for over 90% of all data breaches. In 2021, they reported that at least one person clicked on a phishing link in around 86% of all organisations. The Anti-Phishing Working Group reported that the number of monthly phishing attacks broke all known records in Q3 2021. These alarming statistics highlight the increased need for phishing awareness training and advanced email security measures.

Over the course of 2021, phishing attacks became more advanced. The volume of spear phishing attacks increased dramatically last year, with 65% of the known groups on online attackers reporting spear phishing as their primary method of infection. In contrast to phishing which targets the masses, spear phishing is directed at specific individuals or organisations via personalised content designed to inspire trust. This method of attack can be extremely effective, with the average impact of a successful spear phishing attack costing $1.6 million.

Ransomware

The salesman

Ransomware is a form of malware that encrypts data until the owner pays a ransom to retrieve it. In essence, cyber criminals steal your data and sell it back to you for an extortionate price. Cyber criminals know the value of sensitive data, and exploit victims' fear of either losing it, or, if they are targeted by double-extortion ransomware, having it breached for the world to see.

In 2021, there were more than 500 million ransomware attacks attempted globally, an increase of 134% from 2020. Furthermore, the expense of ransomware increased, with GRC World Forums reporting that the average ransomware payment rose from $312,000 in 2020, to a record $570,000 in 2021.

The evolution of ransomware was highlighted by the volume of high-profile attacks that dominated global news in 2021. One of the USA's largest fuel companies, Colonial Pipeline Company, suffered one of the largest ransomware attacks in history, and the largest to ever affect an oil company. The attack resulted in CPC paying the DarkSide group $4.4 million in ransom.

Distributed Denial of Service (DDoS) attacks

The bouncer

Distributed Denial of Service attacks block access to the targeted website, application, server or network by overwhelming it with connection requests from compromised computer networks, or botnets. By disrupting the regular traffic, any actual users are restricted. DDoS attacks can overlap with ransomware attacks, as the victim is sometimes forced to pay a ransom to reclaim access.

In mid-2021 a new botnet, called Meris botnet emerged and targeted thousands of organisations around the world with some of the largest HTTP attacks on record. In addition to this, ransom DDoS attacks increased by 29% over the course of 2021, rising by 175% each quarter. There were the most DDoS attacks in the final quarter of 2021, with more attacks in December alone than there were in Q1 and Q2 combined.

Network Hijacking

The spy

Virtual Private Networks (VPNs) were one of the most commonly used remote working solutions of 2021, allowing employees to access their corporate network from home with a hidden IP address and location. However, the increase in the implementation of VPNs came with a whole host of security vulnerabilities to exploit, including, but not limited to, poor password security and missing patches. By taking advantage of these, cyber criminals were able to gain access to corporate networks and monitor for sensitive information to steal, planting ransomware or exfiltrating data.

VPN attacks rose by almost 2000% in 2021, with a 1,527% rise in attacks against Pulse Connect Secure VPN, and a shocking 1,916% increase in attacks against Fortinet's SSL-VPN. These concerning statistics highlight the continued negative impact of the COVID-19 pandemic and remote working on cyber crime.

Cryptojacking

The accountant

The purpose of cryptojacking is to generate cryptocurrency illegally on another person's device. Cryptojackers typically use social engineering techniques to gain access to a victim's device, following which they trick them into installing malicious code. Typically, this is done completely insidiously, without the victim being aware of the cyber criminal's presence. After gaining access, hackers use a malware called coin miner to generate cryptocurrency.

Cyber threats tend to follow and respond to evolutions in the use of technology. Therefore, it is natural that cryptojacking has increased over the past year, as the use of cryptocurrency has become more popular among the public. In the first quarter of 2021 alone, code changes to cryptomining malware quadrupled. In this period, nearly 500,000 people were the victims of cryptojacking. It is now estimated that 25% of all businesses have encountered miners on their devices.

Looking ahead: the encroaching threats of 2022

While these threats are not completely new to the security landscape, they are becoming more notable and dangerous as we move through 2022. Without a strong cyber security strategy in place, your customers will be at risk of six key forms of attack this year.

Modern ransomware

Ransomware is an ever-evolving form of cyber attack. Traditional ransomware has developed significantly in recent years, advancing far beyond exploiting individual victims for a ransom. Modern ransomware targets entire enterprises using human operated scripts and malware to encrypt and exfiltrate data. Ransomware was already on an impressive growth trajectory in 2021, and as we enter 2022, this shows no signs of stopping.

Ransomware as a Service (RaaS) is becoming a more prevalent threat in 2022. RaaS is a particularly dangerous form of cyber crime as it opens ransomware to the masses, not just those with technical expertise. Cyber criminals sell or offer subscriptions to their malware, allowing anyone who can afford to buy it to launch a ransomware attack. RaaS allows malware to spread across the cyber sphere extremely quickly, making it very difficult to track down the original perpetrators.

Internet of Things attacks

The Internet of Things (IoT) refers to a system of physical objects embedded with the capabilities to exchange data with other devices on the internet. IoT devices could include anything from smartwatches to printers to smart refrigerators. The IoT is expanding at a rapid rate, being estimated to reach 18 billion objects by the end of 2022. When implementing cyber security measures, the IoT can often be overlooked, but it is commonly exploited by cyber criminals wishing to gain access to secure digital systems. In 2022, 5G is set to expand its rollout, increasing cellular bandwidth and facilitating the growth of IoT networks. As this expansion takes place, MSPs need to be on the lookout for the resulting increase in IoT attacks.

Man in the Middle attacks

During a man-in-the-middle attack, a cyber criminal intercepts a connection between two points. This connection is most commonly an exchange between two players on a network. The 'Man in the Middle' is then able to intercept the data being transferred through the connection and manipulate or compromise it. This form of attack is developing rapidly – cyber criminals are now even able to assume the identity of one user and mine for data under this guise. This technique is known as 'eavesdropping'. It is relatively simple for cyber criminals to launch man-in-the-middle attacks; even an unsecured WiFi connection can be a golden ticket to data interception.

Deep fake threats

A report from Duo Security found that in 2021, 79% of people stated that they used two-factor authentication, up from 53% in 2019. This increase has been responded to by cyber criminals, who need to find a way to bypass the additional security measures users are implementing. Their solution? Deep fakes. Hackers can harness deep fake technology to bypass multi-factor and biometric authentication, to gain access to confidential data. Deep fake attacks have increased by 43% since 2019, demonstrating that cyber criminals are hot on the heels of cyber security experts, finding new ways to overcome their preventative measures. There is speculation that in the next few years, deep fake attacks will follow the trajectory of ransomware, and be monetised as a service, allowing this threat to spread yet more widely across the globe.

Supply chain attacks

Supply chain attacks are aimed at software developers and suppliers. Cyber criminals attempt to infect legitimate code, updates or applications with malware. The hope is that the infection will go undetected, and the vendor will release the app or update to the general public, spreading the malware widely. In 2021, supply chain attacks on open-source software increased by 650%. If this growth is not curbed in 2022, supply chain attacks could continue to cause major disruptions, particularly if a popular application is targeted.

Insider threats

Did you know that the employees within a company can be just as much of a threat to it as those outside it? Access to confidential data and the corporate network places team members in a powerful position. Whether they are acting out of resentment, malice or financial coercion from an outsider, all employees and any ex-hires who retain access to a corporate network pose a significant security threat. As the job market remains uncertain in 2022, these threats are set to increase.
However, not all insider threats are malicious. The majority occur due to human error, lack of training or cyber security ignorance. In 2022, you should encourage your customers to invest in their human firewall, and support them through the process of strengthening this first line of defence.

How to prepare for the threats of 2022

As an MSP, it is crucial that you are able to effectively protect your customers from the cyber threats of 2022. With a clear cyber security strategy, like the one laid out below, and the intelligent utilisation of industry-leading security products and solutions from Trend Micro, you can offer your clients a comprehensive and up-to-date defence against the cyber security landscape of 2022.

Audit and inventory

Taking an inventory of assets and data when you first begin working with a customer allows you to identify authorised and unauthorised software and devices, as well as any vulnerabilities. Penetration testing and phishing simulation software like Phish Insight from Trend Micro will help you to accurately assess their existing security posture.

Configure and monitor

Monitoring your customers' IT infrastructures can help to proactively prevent threats. The industry-leading XDR capabilities of Trend Micro Vision One give you greater visibility and power to detect and limit cyber attacks, across email, endpoints, networks, servers and Cloud workloads. You can also implement security configurations such as firewalls and routers to limit threats.

Patch and update

Out of date software can be a major security vulnerability for your customers. As part of the regular vulnerability assessments you carry out, you should conduct patching or virtual patching for operating systems and applications, and ensure that software and applications are updated to their latest versions.

Protect and recover

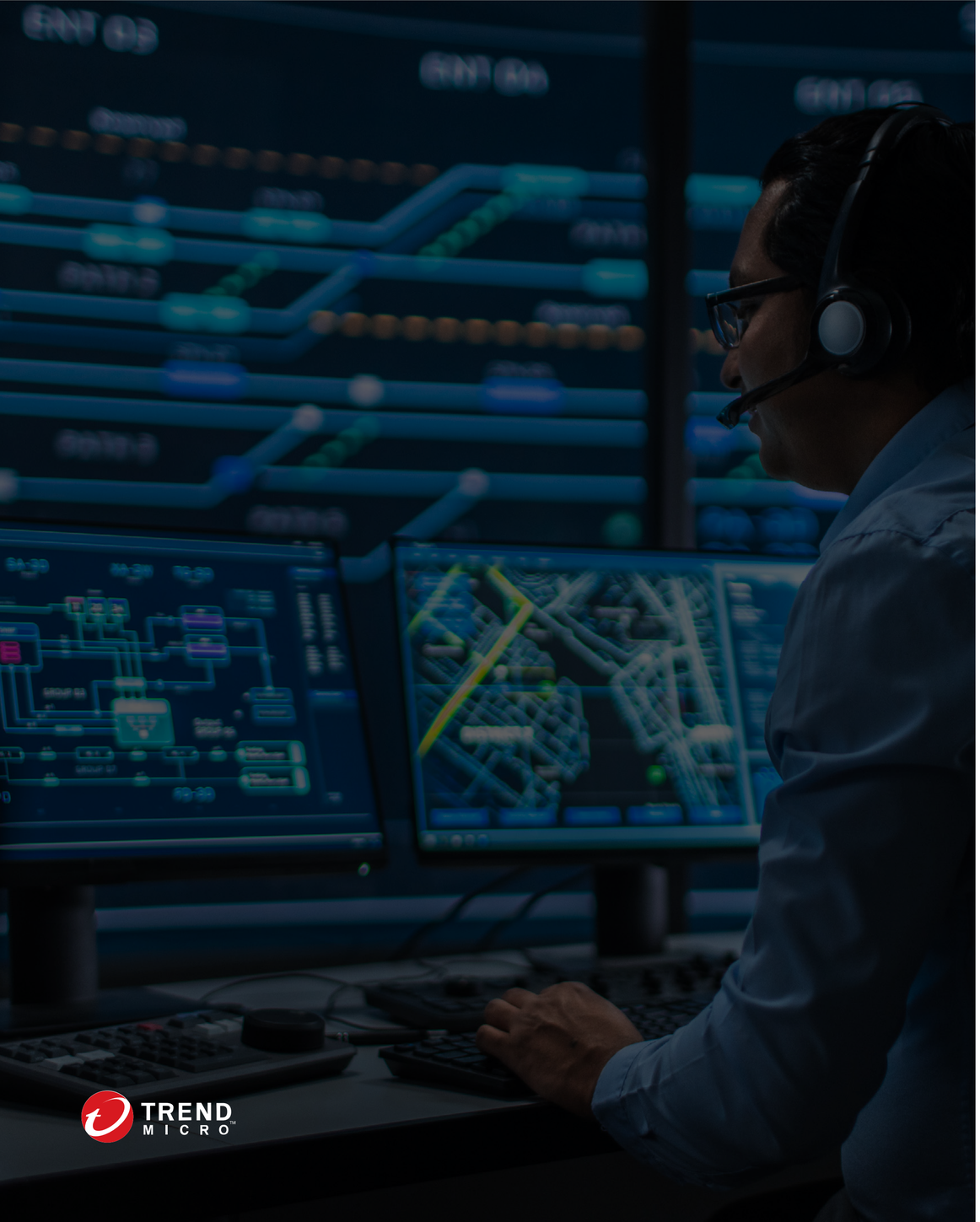
As an MSP, you should encourage your customers to enforce stringent password policies and multi-factor authentication to ensure secure access to corporate networks. In case of disaster, you should also implement data protection, backup and recovery measures to ensure that your customers are never faced with the loss of valuable data.

Secure and defend

Ensure that you are employing the latest version of all security solutions to all layers of your customer's IT system, including email, endpoint, web and network. With Trend Micro Email Security, you can perform sandbox analysis to examine and block malicious emails, minimising the impact of phishing, which is responsible for 90% of all data breaches.

Train and test

Training your own team is just as important as ensuring your customers have strong cyber security awareness. Implement regular training programmes within your MSP, to ensure that the entire team are kept up to date and informed on the latest developments in the security landscape. Armed with specialist knowledge, your technicians will be prepared to tackle any and all cyber threats head on.



Selling your cyber security services: demonstrating value to customers

As an MSP, you must be able to demonstrate your value to your potential and existing customers. When selling cyber security services, you must be able to express your capacity to adapt, demonstrate the specific value of your services, and explain why prospects should choose to partner with you in an ever-changing security landscape.

This can be a challenging feat. That's why we have compiled four key ways to demonstrate the value of your MSP and your cyber security offering to customers.

Establish a clear client relationship

It is essential to establish strong relationships with your clients, based on trust. Don't over promise at the beginning of your working relationship, and then underdeliver. You should set clear goals and expectations, and lay these out in an SLA which expresses not only the levels of service you will provide, but the value these services will bring.

Maintain transparent communication

As an MSP, you should never leave your customers in the dark, particularly when it comes to the state of their cyber security. You should maintain clear and transparent communication with them at all times. An excellent way to do this is to deliver value driven cyber security reports, which will update them on the state of their security posture.

Share your security expertise

A company's team are their first line of defence against cyber threats. An effective way to demonstrate your value is to share your cyber security expertise with your clients. This could take the form of security skills assessments or regular training. Trend Micro offer Phish Line, a phishing simulation software that you can use to begin training. The impact of this assistance will be undeniable and long-lasting for your customers.

Remain responsive to evolving needs

As businesses grow, their cyber security requirements evolve alongside them. You need to demonstrate that the solutions and services you provide are scalable and can continue to meet their changing needs. By regularly reviewing a customer's goals and expectations, you can adapt your cyber security provisions appropriately, ensuring that you continue to demonstrate value throughout your working relationship.

Take cyber security in 2022 by storm

The cyber security landscape is always evolving and posing new and more dangerous threats. As we settle into a new year, it's the ideal time to review your security protections, provisions and procedures, to ensure that you can offer your customers the best possible defence.

Trend Micro are a global security leader, with decades of security expertise, global threat research, and continuous innovation already under our belt. With our specialist security solutions by your side, the cyber threats of 2022 will be no match for your MSP.

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

TREND MICRO™