ARTICLE

Dropsuite

5 Key MSP Cybersecurity Threats of 2022

MSPs are a hot target for cybercriminals. They handle highly sensitive information for tens, hundreds, or even thousands of private businesses. Bad actors know this, and they will exploit a range of vectors – from ransomware to social engineering, to DDoS attacks – to steal data and conduct attacks. In this article, we discuss the top five MSP cybersecurity threats of 2022, and how MSPs can best protect themselves and their clients from these threats.

It's a Digital Jungle Out There

Cybercriminals will exploit any vulnerability that will enable them entry into an IT network. If they cannot infiltrate an organization directly, they will find a backdoor in their supply chain.

For businesses in the tech industry, this backdoor is often their managed services provider (MSPs). MSPs work with multiple clients, holding massive amounts of information and data. Gaining access to their systems means a high chance of obtaining access to thousands of business systems.

Clients of MSPs typically rely on them to bring a full stack of IT services – including security. If MSP cybersecurity threats become a reality, the effects could impact their entire client roster – leading to financial loss, legal consequences, and serious reputational damage.

The reality is: No-one wants to use a provider that they think could put them at digital risk.

Here are the top five categories of MSP cybersecurity threats and digital risks that businesses need to be aware of as we head through 2022 – and how MSPs can protect themselves and their clients.

1. Ever-Evolving Ransomware Threats

Ransomware evolves with the times. What started as petty crime has become a major problem for businesses everywhere. Previously, ransomware attackers had to jerry-rig their own payment collection methods or employ retail shopping cards, prepaid cash cards, and even cash payments sent to PO boxes across the country. The effort versus reward kept ransomware attacks from spreading out of control.

Recently, ransomware threats have become more frequent and more lucrative, spurred by the growth of cryptocurrencies.

This new payment method is virtually untraceable and very attractive to criminals as it allows ransomware attackers to wield the swiftness and anonymity of crypto-transactions. This development has made life much harder for MSPs: 73% of companies **identify ransomware as the top threat method** used to infiltrate their systems.

Connectwise's 2021 MSP Threat Report revealed that 60% of MSP client incidents were related to ransomware.

The report also predicts that attackers will continue exploiting the lack of visibility or understanding across the multiple cloud-based solutions and programs that MSPs use. Threat actors will be "banking on the fact that [the cloud] is a source of poor visibility for us," said one MSP. It is likely they will continue to focus on cloud-based attacks against MSPs going forward.

Ransomware threats have become more focused as well, due to a technique called **Big Game Hunting (BGH)**. This is a targeted, complex, low-volume, high-return cyberattack through ransomware. Once attackers gain entry, they make lateral movements across the network to observe it before exfiltrating files and deploying the ransomware.

For MSPs, BGH attacks are extremely damaging. Part of this is due to the patience that big game hunters display when performing this attack method. It typically takes a considerable amount of time for an attacker to understand, steal from, and infect the compromised network. But once they do, they can single out the 'big shots' within the MSPs' systems and exploit them without anyone the wiser.

By the time the MSP and their clients realize what has happened, a huge amount of data will have been damaged or stolen, and the provider's reputation suffers.

Other types of ransomware threats that will most likely be common in the near future include:

1. **Crypto-malware** – a malware attack that is almost impossible to undo without the malefactor's decryption key.
2. **Scareware** – "scares" users into believing a virus has invaded their system and asks users to pay money to "fix" it.
3. **Lockers** – prevent access to the entire system by "locking" the user out completely.
4. **Doxware/Leakware** – comes with a threat to release encrypted personal/sensitive data to the public.
5. **RaaS (Ransomware as a Service)** – people without the tools or expertise can "order" a ransomware attack on a business/individual's systems.

2. Social Engineering Exploits

Social engineering refers to a broad range of malicious activities performed by human interaction. Psychological manipulation is often utilized to trick users into breaching security protocols and giving away sensitive or personal data.

The perpetrator first investigates the intended victim to gather necessary background information such as potential points of entry and weak security protocols.

The attacker then moves to **gain the victim's trust and bait them for subsequent actions that break security practices**, such as revealing sensitive information or granting access to critical resources.

98% of cyberattacks rely on social engineering; on the rapport and connection that is established as the attack progresses. Moreover, social engineering exploits are effective about 80% of the time.

That's how convincing social engineers are – and there is no indication of that changing anytime soon.

MSPs need to educate everyone in the organization, as well as their customers, on how these MSP cybersecurity threats start, how to identify them, and how to deal with them appropriately. Online cybersecurity courses, awareness training, and seminars will go a long way in keeping teams up to date about social engineering exploits and tactics.

Some social engineering forms and examples are as follows:

1. **Baiting** – uses a false promise to pique a victim's greed or curiosity to steal personal information or inflict their system with malware.
2. **Pretexting** – starts by establishing trust with their victim by impersonating co-workers or authority figures, then asks questions that allow them to gather sensitive data.
3. **Phishing** – one of the most popular social engineering forms; often email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.
4. **Spear phishing** – a more targeted version of the phishing scam, where an attacker tailors their messaging to a specific individual or business.

3. DDoS Attacks in Cloud Computing

A **Distributed Denial of Service (DDoS) attack**, also known as a Distributed Network Attack, is a cybersecurity threat that leverages the limits of network infrastructures. Cybersecurity provider Kaspersky summarizes a DDoS attack as follows:

"The [attacker] will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly."

Microsoft reports they've mitigated an **average of 1,392 DDoS attacks per day (as of May 2021), and more than 251,944 unique attacks** in total during the first half of 2021.

Hackers tend to launch coordinated DDoS attacks in cloud computing with multiple devices that have already been compromised, either through hacking or malware. This allows every machine involved to perform criminal activity without the owner's knowledge.

Examples of these MSP cybersecurity threats are the Equifax hack in 2017 and the TaskRabbit app attack the year after. Even tech giant Amazon declared that its AWS Shield service successfully mitigated such an attack in February 2020 – a 2.3 Tbps DDoS attack – the largest by far.

DDoS-for-hire services have also spurred in number due in part to the pandemic and shelter-in-place setup, and every business should be on the lookout for this new wave of attacks.

In Q1 of 2021, there were approximately 2.9 million distributed denial-of-service (DDoS) attacks, which is a 31% increase from 2020 Q1.

4. Remote Work Risks

In recent years, remote work has also seen an unprecedented rise. During the pandemic, businesses had no choice but to rely on digital services and online communication tools to keep connected, whether for work or for personal reasons.

Work-from-home vulnerabilities have arisen due to the remote work setup. CISO's Benchmark Report revealed that businesses have been struggling to manage phones and other mobile devices that remote workers use.

Employees have blurred the lines between their professional and personal lives – this creates serious headaches for the CISO.

Personal devices are being used to access workspace tools like Slack, Zoom, and Teams. Work devices, on the other hand, are being used to send memes to colleagues, share posts on social media and other personal purposes. This crossover introduces new remote work threats, as it expands the risk surface of an organization and puts sensitive information in jeopardy. In fact, the report further reveals that **52% of businesses find mobile devices to be a major cybersecurity challenge**.

It's not only the technological element of the business that should be closely monitored. Studies have found that:

- 35% of employees reported feeling tired or having little energy while working from home. (Society of Human Resources Management)
- 50% of workers, particularly in the UK, have cited a lack of motivation while working remotely. (Velocity Smart Technology Market Research Report 2021)
- Despite the distractions, remote employees tend to have worked five hours a week more on average than those who worked in the office; also doing six hours of unpaid overtime on average per week, compared to 3.6 hours for those who never work from home. (Office of National Statistics)

As admirable as it is, putting in extra hours constantly may affect the quality of an employee's work and induce remote work risks. Worst case scenario, it may cause them to unintentionally divulge sensitive information and jeopardize the security of the business.

5. IoT Threats and Vulnerabilities

Security services provider Kaspersky revealed that Internet of Things (IoT) cyberattacks have more than doubled compared to the previous year, in the first half of 2021.

From 639 million attacks in Q1 of 2020, some 1.51 billion IoT breaches have been reported just within January to June 2021.

A majority of these (58%) utilized the telnet protocol. The intent of these MSP cybersecurity threats ranges from crypto mining to DDoS to data theft.

The most glaring of these IoT threats and vulnerabilities include:

1. **Weak password protection** – Hard-coded, guessable credentials are a blessing to hackers. For example, the Mirai malware of 2016 successfully logged in to and infected a significant amount of IoT devices using a table of **61 common hard-coded default usernames and passwords**. Ever since then, various botnets have infected IoT devices worldwide, with **Mozi** being the most active botnet in 2021.

2. **Lack of regular patches/updates and/or weak update mechanisms** – A responsible manufacturer will always provide security updates on their embedded software/firmware, but that's not always the case. Without constant and regular security patches and updates, an IoT device becomes vulnerable to hacking over time.

3. **Insecure interfaces** – The interfaces that IoT devices use can become vulnerability points due to insufficient device authentication and authorization, as well as weak or non-existent encryption. Without a solid device authentication protocol and digital certificates, bad actors will be able to connect to the exposed interface.

4. **Insufficient data protection** – Securing data storage and networks cannot be understated. Data encryption can help solve this, in the event of data theft or unauthorized access. Even basic cryptography systems can go a long way in protecting users from eavesdropping or "man-in-the-middle" attacks.

5. **Poor IoT device management** – This study published some disturbing information about how poorly IoT devices in certain industries are being managed.

6. **The IoT skills gap** – It's not always possible to hire new talents and personnel. The only option is to conduct training and upskilling programs for the existing employees. Train team members to be prepared and capable of managing IoT devices, and they will be all the more effective for it.

> "I've found that more than 51 percent of IT teams are unaware of what types of devices are touching their network. But perhaps what is more disconcerting is that the other 49 percent often find themselves guessing or using a 'Frankenstein'd' solution to provide visibility into their network security..."
>
> **Zeus Kerravala,**
> **founder and Principal Analyst, ZK Research**

Furthermore, according to the report:

- About 15% of devices were unauthorized or unknown.
- 75% of the deployed devices violate VLAN protocols.
- 5-19% are still attached to and using unsupported legacy systems.

How Can MSPs Protect Themselves?

An MSP needs to have the drive to improve their overall network security. Aside from educating employees on social engineering exploits and other MSP cybersecurity threats, as well as keeping software and firmware patched and updated, here are some other steps to achieve a more secure system.

- **Have a multi-layered, in-depth security system to defend the business**. This security system should protect not only against ransomware attacks, but also social engineering, DDoS attacks, and system vulnerabilities.
- **Extended threat detection and response solutions** can help identify potential risks that bad actors may exploit.
- **Security tabletop exercises** – sessions where team members discuss their roles and responses during emergencies are handy to keep personnel prepared and ready to respond to any breach or cybersecurity attack. These security tabletop exercises will also help in discovering possible security gaps and vulnerabilities, not just within the systems, but also in policies and protocols.
- **Frequently back up data**. This tip is paramount for an MSP. Deploying an automated backup system and securing reliable backups mitigates the risks of data loss.

An ongoing, cloud-based, automated backup solution is one of the best ways to guarantee data safety and security.

Ensure complete backups of emails, attachments, tasks and calendars are in a separate, secure system. Many solutions exist in the market, but it's often difficult to find the right fit. Fortunately, Dropsuite provides these services with the following benefits:

1. **An automated backup solution** for Microsoft 365, Google Workspace and/or email files.
2. **Incremental backups** that include **unlimited storage and retention options** to ensure MPSs never run out of space.
3. **Single-pane-of-glass admin panel** with role-based access levels that enable **easy access**.
4. **Secure storage** with TLS or SSL, plus data is encrypted using military-grade 256-bit AES
5. **1-Click Restore and Download** in case of accidental deletions.

Technology constantly evolves, and as long as bad actors exist, digital threats will evolve as well.

These five MSP cybersecurity threats may not be the only ones that MSPs like yours will face going forward. It's up to businesses to counter this evolution by being proactive with protecting their data and preparing for the worst-case scenario as best they can.

Dropsuite allows you to effortlessly and securely backup, restore, and migrate all business-critical data. This is a great first step in preparing for whatever digital tempest comes your way.

To discover more about Dropsuite's automated backup solution and capabilities, contact us here for a demo.

> Just like everyone knows they have and will endure cyber attacks and yet have no insurance, cloud issues and loss are bound to happen. Dropsuite is the insurance they should have for that loss"
>
> **Matt Lee,**
> **Director of Technology and Security, Iconic IT**

> Now, thanks to Dropsuite, if our customers do become compromised or something happens to their data, it doesn't represent serious data loss or a security incident for them."
>
> **Daniel Johnson,**
> **CEO, machineLOGIC**

CONTACT US

For more information, please contact us:
www.dropsuite.com | sales@dropsuite.com