CYREBRO

The Real Cyber Threats: Common Attacker Entry Points

5 CYBER-ATTACK INCIDENTS FROM AVOIDABLE COMMON ENTRY POINTS

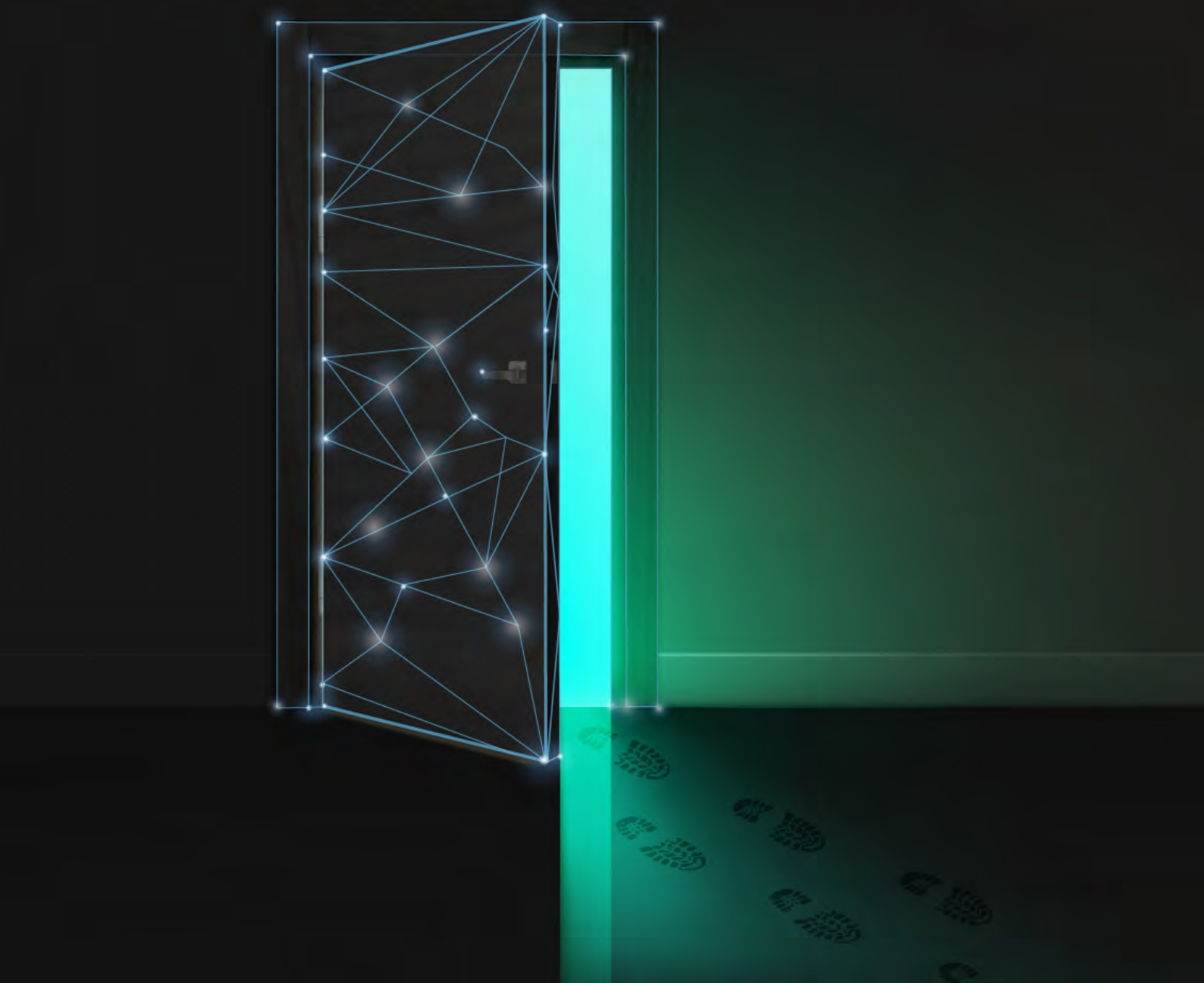
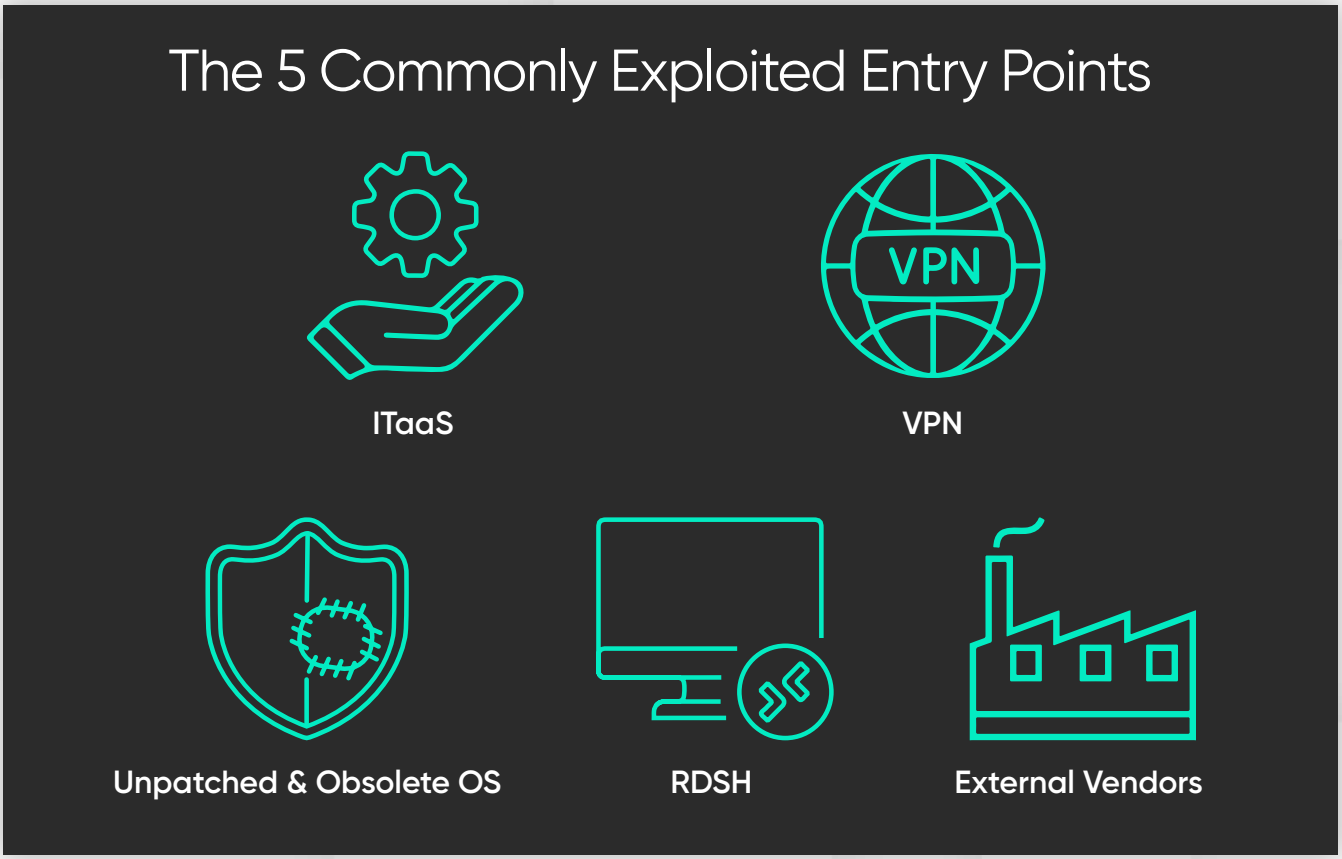


TABLE OF CONTENTS

An Attackers Mindset – Maximum Gain Minimum Effort

A rigid dichotomy is at play in today's cloud-first, technology-driven world. On one side are the cybersecurity professionals tasked with protecting organizations' complex infrastructures and managing ever-expanding attack surfaces with growing toolsets. On the other side, sit threat actors who keep it simple by launching minimal-effort attacks that yield maximum gains.

Unlike what we see in Hollywood movies or the stories that make headlines, your SMB likely won't be breached by state-sponsored actors who use the best tools and have the best expertise. Instead, you'll experience standard and avoidable breaches due to overlooked and unsecured common entry points.



Being unaware of these easily exploitable entry points, which include IT-as-a-Service providers (ITaaS), VPNs, unpatched and obsolete operating systems, remote desktop session host platforms (RDSH), and external vendors, or failing to see them as potential vulnerabilities can spell disaster for your company.

The Impacts of a Single Breach for SMBs

Another interesting but alarming paradox is happening in cybersecurity: the well-known statistics of attacks against SMBs tell a frightening tale, yet the overwhelming majority of SMBs still lack cybersecurity awareness and preparedness.

Of the SMBs with no cybersecurity protections, 59% have made that choice because they believe they are too small to be attacked. However, in 2021, 46% of all cyber breaches and 82% of ransomware attacks were against companies with fewer than 1,000 employees.

The impact of a breach can have far-reaching consequences, as an attack can cost an SMB anywhere from $826 and $653,587. That wide range depends on several factors.

Downtime: Over half of SMBs experienced 8-24 hours of downtime, while nearly 20% were down for over 24 hours, costing $137 - $427 per minute. That outage will have a waterfall effect on the business, given that 50% of customers will move on after experiencing just 5 minutes of downtime.

Legal Obligations: Organizations without cyber insurance, monitoring tools, or an in-house security team must hire external forensics or IT service providers to investigate and eradicate the threat or negotiate a ransom payment. If sensitive customer data is stolen, businesses may need to pay for credit and fraud monitoring services for impacted customers. Lawyers and compliance experts will also need to be hired, and the list goes on.

Reputation Restoration: Since over half of an organization's customers will shift to a competitor, damage control is imperative. Regaining public trust is a challenging and time-consuming process that requires SMBs to hire PR firms to handle customer communications and complaints as well as monitor and respond to negative news stories and reviews.

Product Pricing: After paying the costs associated with an attack, companies must find ways to refill their depleted coffers. Although they may risk pushback, 60% percent of businesses pass their cyberattack costs onto customers by raising product prices.

Any or all of those factors can result in a business shutting its doors, not to mention that a single ransomware payment would push 75% of SMBs to close permanently. Given that 2022 saw a 38% increase in attacks compared to 2021, a steep upward trend likely to continue, SMBs must prioritize cybersecurity.

cyber-attack growth from 2021-2022

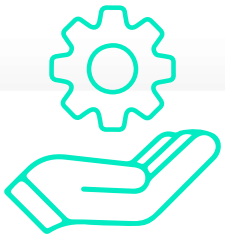
As mentioned earlier, we know the most common attack vectors for attackers, and at a minimum, businesses should do what's necessary to harden those soft targets

5 Common Entry Points

Threat actors will always attack a business' weakest point. Why would they work hard when so many organizations make it easy?

Knowing the most common entry points, why they are attractive to attackers, and how to harden your defenses with best practices can significantly reduce the chances of becoming a victim.

Common Entry Point 1: ITaaS (IT-as-a-Service)



SMBs contract third-party providers for various IT services because they lack the in-house expertise and funds to acquire and maintain the level of IT innovation and infrastructure needed today. Through ITaaS models, providers offer IT as a commodity, which usually includes customized packages of bundled hardware, software, and support for a subscription fee.

Besides the advantage of predictable OPEX budgeting, minimal upfront investment costs, and tax advantages, organizations get access to expert technical support, regular software upgrades and hardware refresh cycles, and continuous monitoring. However, being digitally connected to service providers also opens you up to your provider's risk exposure.

WHY IS ITAAS A COMMON ENTRY POINT?

IT service providers are high on the target list for attackers. A significant risk lies in the potential for cross-contamination through various vectors, including technician laptops, USB drives, shared folders, servers, and other means. Once compromised, attackers can skillfully exploit these avenues to infiltrate the provider's clients, granting them unauthorized access and enabling potentially substantial consequences.

REAL-WORLD INVESTIGATION: ITAAS

CYREBRO has recently investigated a case involving three insurance firms that utilized the same IT provider. When external threat actors gained access to one of the firms due to a ransomware attack, they quickly moved onto the IT providers' management server to gain access to their other customers. This proved ridiculously easy as the provider used an 11-year-old operating system and a portfolio of obsolete and outdated software rampant with vulnerabilities. Through this single management server, the attackers were able to gain access to the networks of multiple companies with ease.

BEST PRACTICES FOR WORKING WITH ITAAS PROVIDERS

Just because your IT provider may be an authority to you doesn't mean they aren't taking shortcuts that may expose your company to unnecessary risks. Here are a few best practices to follow if you have an ITaaS provider.

1. ADOPT A ZERO-TRUST FRAMEWORK

IT managers should follow a "never trust, always verify" mindset regarding all connection requests, even those originating from within the network. Zero implicit trust also includes your IT providers, especially those who provide the components and services that permeate your network.

2. FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

Your ITaaS provider should only be granted the exact privileges needed to do their job. There is no reason for network admin accounts to have read access to the HR employee records file directory or other sensitive information. If an internal or governing administrator needs to perform a task on a select folder that holds sensitive data, rather than having privileged access to the folder, the admin should be required to first take control of the folder, triggering an alert that can be logged for future inquiry if necessary.

3. SECURITY NEEDS TO BE POLICY DRIVEN

A decentralized approach to security is no longer viable; every computer must be safeguarded using the same protection measures, and all users must adhere to a minimum-security standard. You can achieve that through policy deployments that deliver mandated configuration settings or enforce security and compliance restrictions. For on-premise domain networks, this is usually done using Windows Group Policy. An MDM such as Microsoft Endpoint Manager is a better choice for mobile or remote machines.

Common Entry Point 2: VPNs

VPNs offer significant and extensive benefits for organizational security by enhancing endpoint protection. Instead of connecting via an ISP, VPNs create an impenetrable tunnel between your IT environment and your employees.

You can use a VPN to better control system access, granting it to employees regardless of their device or location while preventing unwanted access to protect sensitive data. VPNs can also help you gain more network visibility and alert you to anomalies, making it easier to identify possible intrusions.

WHY ARE VPNS A COMMON ENTRY POINT?

As its name suggests, a Virtual Private Network is an interface to the internal organizational network, a very attractive target. Attackers can use simple brute-force attacks or gain control through compromised credentials or lazily constructed logins and passwords, which are no match for savvy attackers. Once inside the network, the damage the business will experience can be devastating.

REAL-WORLD INVESTIGATION: POOR VPN SECURITY

One of CYREBRO's clients was doing everything right, requiring employees to use a VPN and multi-factor authentication (MFA) to access its network. However, one day the company's Head of QA received an MFA push notification on his mobile device out of the blue. Without much thought, he clicked "Allow" instead of ignoring or denying it. CYREBRO's investigation revealed that when the user approved the MFA, he unknowingly allowed an attacker to access the company VPN through his account. Once in the system, the attacker immediately began scanning the network, eventually entering through a remote desktop protocol (RDP) to an AWS EC2 instance with administrative credentials and stealing a role's secret key.

BEST PRACTICES FOR SECURING VPNS

VPNs are critical for security, but harnessing their true power and eliminating their risk comes down to implementing minor behavioral and policy tweaks.

1. STRUCTURE MFA CORRECTLY

MFA should force users to enter an OTP (one-time password) or a refreshing code from a third-party authentication application. Requiring direct user interaction and input should bring the person's attention to the task at hand, causing them to think about their actions and dramatically reducing the chance of an accidental click.

2. RESTRICT GEOLOCATIONS

Although dispersed and remote teams make it tricky, you must know all employees' locations. Using that as a resource, you can set your VPN parameters, only allowing specific geolocations that correspond to employees. Any suspicious IP addresses or geolocations should trigger an alert, be blocked immediately, and then investigated.

Common Entry Point 3: Unpatched and Obsolete Operating Systems

Software updates are rigorously tested before release, but vulnerabilities are constantly discovered. Each new verified vulnerability is published to a list of known Common Vulnerabilities and Exposures (CVE) – a list accessible to you as well as threat actors.

While you are stuck waiting for the vendor to release a vulnerability patch, attackers are planning and launching their attacks, scanning for these vulnerabilities within 15 minutes of being published. Because CVEs are so prevalent today, organizations struggle to apply every patch in a timely manner, making them an attractive target.

Operating systems that have been deprecated and are no longer supported by the vendor represent one of the most blatant examples of vulnerability. Unfortunately, businesses continue to use these obsolete systems instead of incurring the cost of replacing them. Although Microsoft stopped supporting Windows 7 in January 2020, 18 months later, 16% of all Windows PCs were still running the unsupported OS, sending attackers an open invitation to their environment.

WHY ARE UNPATCHED AND OBSOLETE OPERATING SYSTEMS A COMMON ENTRY POINT?

You are pulled in different directions on any given day, putting out security fires, attending to IT needs, and reviewing protocols. Likely, your small team doesn't have the bandwidth to constantly check the CVE list or test and apply patches as soon as they are available and most businesses don't have software updating policies.

However, cybercriminals can spend all day tracking newly published CVEs and writing code and tools to exploit them. This imbalance leaves you vulnerable and makes your unpatched or obsolete systems easy prey for threat actors. To add to the challenge, outdated software and obsolete operating systems stay as they are due to the "if it don't work – don't touch it" mentality many organizations assume. Often when a tenured developer leaves the workplace, adjusting old software to new operating systems without them can be too difficult to be bothered with.

REAL-WORLD INVESTIGATION: NEGLECTING UPDATE AND PATCH SECURITY

In 2019, the CYREBRO SOC team responded to a major incident in which dozens of a client's POS (Point of Sale) endpoints were infected with the WannaCry virus, one of many malware strains that exploited the CVE-2017-0144 vulnerability, also known as EternalBlue.

At the time of the attack, a patch for this known exploit had already existed for over two years, but the POS machines, which were running Windows 7, hadn't been updated since their initial deployment. To make matters worse, the POS devices were exposed to the internet and were assigned external static IP addresses. The combination of these factors can be lethal for any company.

BEST PRACTICES FOR UNPATCHED AND OBSOLETE OPERATING SYSTEMS

In addition to active monitoring, which gives you visibility into what is trying to connect to your internet-exposed systems, you should implement a few other best practices.

1. GET FAMILIAR WITH PATCHING SCHEDULES

Security patches are typically released according to a regular schedule, such as Microsoft's infamous' Patch Tuesday.' That means there is a gap between when a vulnerability is first discovered and the release of its patch, plus the days or months that go by before you apply the patch. Creating a patching routine or schedule for yourself is imperative to remain secure and to eradicate exploitable weak points quickly.

2. HARDEN ALL SYSTEMS

Because patching isn't perfect, it's essential to harden all your systems by disabling unnecessary ports, services, and features. Only authorized applications should be allowed, and they should be locked down using allow lists. Privileged account users should use separate accounts to check email and surf the web from the accounts utilized to perform privileged tasks on critical systems. If a malware outbreak does occur, workstations and IoT devices should be segmented from critical systems using VLANs and a next-generation firewall.

3. REPLACE OBSOLETE SYSTEMS

Stop using operating systems that have been deprecated and are no longer supported. While you'll need to invest in an updated operating system, the cost of a breach will likely be far higher than the software investment – which you'll have to purchase anyway after you're attacked.

Common Entry Point 4: RDSH (Remote Desktop Sessions Host)

RDSH is a Remote Desktop Service (RDS) role. It holds session-based desktops and apps shared with users who access them through remote desktop clients or a web client and supported browser. Once users have access, they have control over the connected device.

In the wake of the pandemic and companies shifting to work-from-home structures, RDSH went from a nice-to-have to a must-have so employees could work productively and access what they needed. Although RDP has been around for decades, the pandemic caused many companies to start using it, likely triggering attackers' interest in exploiting it. A joint US-UK alert in 2020 noted that a 127% increase in exposed RDP endpoints had led to RDP becoming the most common attack vector for cybercriminals and ransomware gangs.

WHY IS RDSH A COMMON ENTRY POINT?

Any time you add new tools, you open yourself up to more vulnerabilities, especially when they aren't correctly secured because businesses rush to implement them. RDSH, just like VPN, is a gateway to the internal network. If RDSH is not properly hardened, upon successful infiltration, an attacker can escalate local privileges and extract domain credentials, especially administrative credentials of user used to manage the server.

REAL-WORLD INVESTIGATION: LOOSE RDSH RESTRICTIONS

A CYREBRO client deployed an RDSH platform, so its employees could interactively connect to a gateway server connected to the internet and the internal network. However, the client's domain was completely compromised by an attacker who had gained access to Domain Controllers and managed to generate a "Golden Ticket."

Two points of failure led to severe consequences. First, the server had cached credentials of a domain admin, so after the attacker managed to breach the server and extract the credentials, they could connect to any server they wished. Second, the RDSH server wasn't isolated from the company's server network, allowing attackers to use the harvested credentials and connect to any server.

This breach resulted in the client having to rebuild their domain entirely from scratch, which took several months and caused significant downtime.

BEST PRACTICES FOR RDSH PLATFORMS

As employees continue with remote and hybrid work schedules, RDSH platforms are here to stay so it makes sense to implement them correctly and ensure they are secure.

1. SET A GPO

If domain admins have cached credentials on servers, you must immediately change that via Microsoft's Group Policy Object (GPO). You can use the Group Policy Management Console (GPMC) to create a GPO that defines security options, registry-based policies, software and script options, and more.

2. GROUP POLICY SECURITY

Group Policy settings can provide security by limiting access to Control Panel to protect data and systems, preventing software installations that could include malware or other undesirable applications, and triggering a refusal message if someone attempts to open a command window.

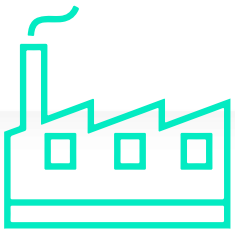
3. SAFEGUARD AND MONITOR SYSTEMS

RDSH and other remote services connected to the internet should be blocked from all critical assets and be tightly monitored. Monitoring needs to be continuous so that should assets be compromised, the attack can be stopped or mitigated when first detected.

4. USE AN EDR SOLUTION

To bolster security further, ensure that your company has installed a reliable endpoint detection and response (EDR) or other endpoint protection solution. These solutions will alert you to malicious activity, so you can investigate incidents quickly and contain endpoint attacks.

Common Entry Point 5: External Vendors and OEMs



Running a business and staying 'in the black' is a delicate balancing act. To save money, many businesses contract with external vendors for various services or to secure affordable alternatives to expensive software and hardware.

Companies may purchase computers, phones, or other original equipment manufacturer (OEM) devices which come preinstalled with some services and functionalities and are managed, updated, and maintained by the OEM provider.

WHY ARE EXTERNAL VENDERS AND OEMS A COMMON ENTRY POINT?

Original Equipment Manufacturer (OEM) devices are appealing targets for attackers because they often lack proper security measures. They tend to run older operating systems with known vulnerabilities, and attackers know that OEM providers often fail to update and patch vulnerabilities. Companies reasonably assume that their OEM provider will carry out the work, so they do not attend to it, leaving them exposed.

To make matters worse, too often OEM devices have unnecessary open ports and unnecessary internet access, enabling an attacker to preform a scan and preform lateral movement. As a point-of-service, the organization faces significant financial risks when attackers exploit vulnerabilities in the OEM, compromising the integrity of their services.

REAL-WORLD INVESTIGATION: IMPROPER VENDOR SUPERVISION

A few years ago, CYREBRO investigated a case in which a client was hit with the WannaCry virus. When the CYREBRO team conducted a full investigation, it was revealed that the virus entered the client's system when an OEM technician plugged into the OEM network using his WannaCry-infected laptop. As was typical with this virus, WannaCry spread using the EternalBlue exploit and managed to infect all of the OEM devices connected to the network.

BEST PRACTICES FOR WORKING WITH EXTERNAL VENDORS AND OEMS

The benefits of external vendors and OEMs are undeniable. If you use them, take extra precautions by following these good-sense practices.

1. QUESTION VENDOR'S SECURITY

Ask every external vendor about their security policies, including what proactive steps they take to maintain security, how often they conduct internal cybersecurity audits, and whether or not they have cyber insurance.

Verify that technicians aren't permitted to use their own devices and that even devices like USB drives are securely managed. Ensure OEMs are as up-to-date as possible when installed, and ask your provider for a regular update routine.

2. SEPARATION IS CRITICAL

Lower your risk by placing OEMs in a network separate from your organizational network. Take additional steps to harden the OEM network by denying unnecessary ports and internet access. Do not use domain users on the OEMs or put them inside the organization's domain; never log in with Administrative Domain accounts.

3. SCAN AS OFTEN AS POSSIBLE

Run scheduled malware scans at least quarterly, if not monthly. That will allow you to quickly identify and address security flaws that could put your organization at significant risk. If possible, scan for malware and malicious traffic with a traffic analyzer, intrusion detection system (IDS), or intrusion prevention system (IPS).

Solve Common Entry Points With Common (Security) Sense

The entry points discussed above, although incredibly common attack vectors, don't have to be. The first step to securing your organization is realizing where your weak links exist and taking steps to strengthen them. By properly configuring systems and solutions and achieving greater visibility, you can significantly reduce the chances of an attack. Without an easy way in, attackers are likely to move on to a softer target.

However, as the sophistication and frequency of cyber threats increase, you'll need to harden your defenses even more. A security operations center (SOC) platform provides a range of capabilities that can level the playing field by allowing you to detect and respond to cyber threats proactively.

ENTERPRISE-GRADE SECURITY WITH CYREBRO'S SOC PLATFORM

The 24/7 monitoring, proactive threat intelligence, and threat-hunting capabilities offered by CYREBRO's SOC Platform allow rapid and thorough identification and mitigation of threats before they can cause significant damage.
CYREBRO's SOC Platform incident response and forensic investigation capabilities enable you to quickly and effectively respond to security incidents as well as gather evidence to support legal or regulatory requirements.

These capabilities, combined with the expertise and support provided by the SOC platform, will help you improve your overall security posture and reduce the risk of a damaging cyberattack. Ultimately, with a SOC platform, you'll be able to focus on your core business activities while leaving the security monitoring and incident response to experts.

Learn more here