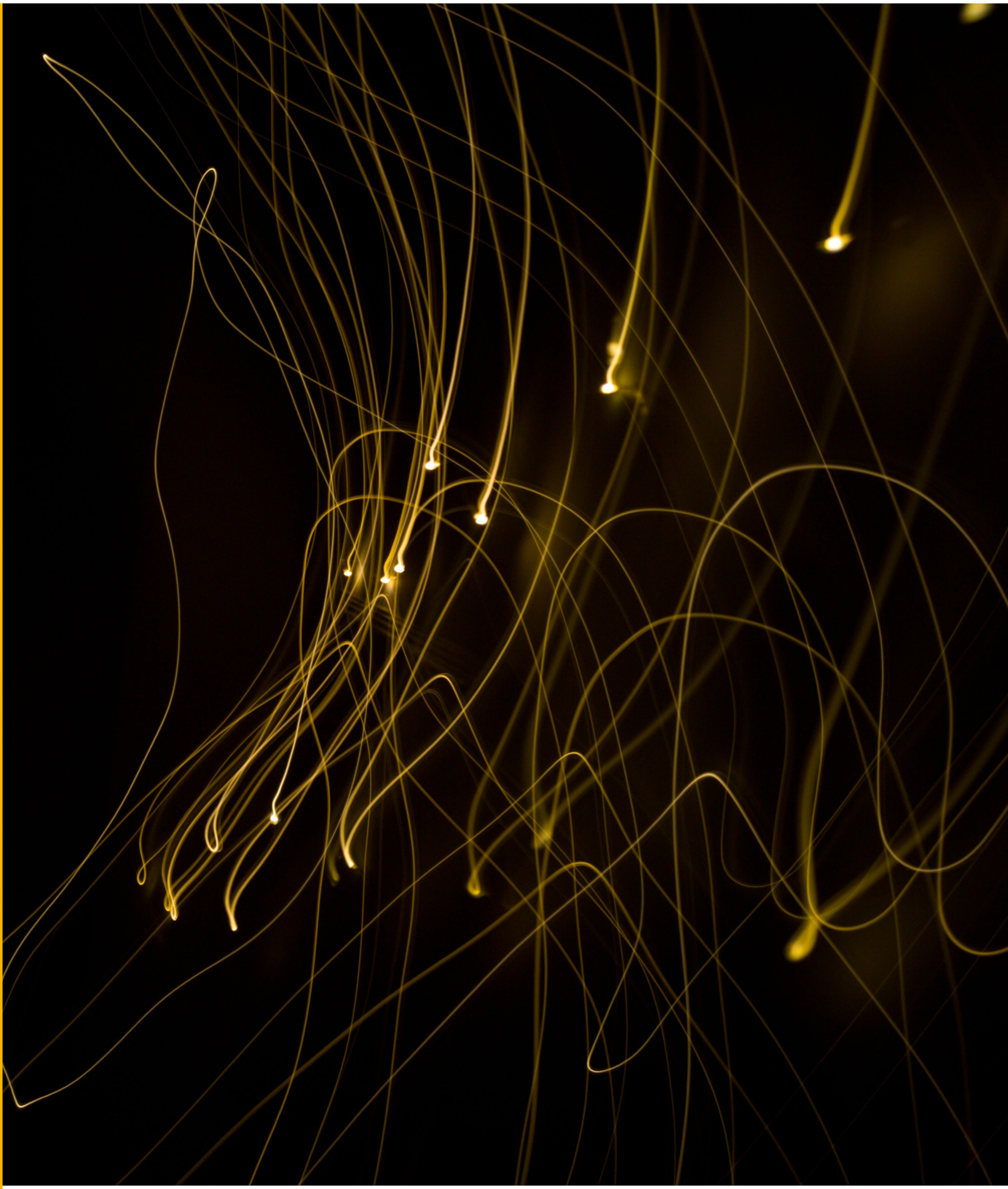
Petri IT Knowledgebase Resource
A BWW Media Group Brand

PETRI
WE GET IT



Petri Whitepaper
August 09, 2022

Top Challenges for IT Security Professionals in 2022

Sponsored by

Devolutions

Overview

Cybersecurity has been a top priority for IT professionals for the past several years. Even so, there continues to be an ever-increasing incidence of malware, hacking, and other cybersecurity breaches that include many high-profile targets.

Today's security attacks are becoming more sophisticated, more damaging, and not surprisingly more costly with each passing year. Defending against these attacks and securing the organization's critical data is the number one job for today's IT security professionals. Let's have a closer look at some of the biggest challenges for today's IT security professionals.

Ransomware

There's no doubt that ransomware is one of the biggest security threats for businesses of all types and sizes. Ransomware can cripple a business by encrypting its essential data and services, rendering them inaccessible, until either a ransom is paid or until the business can recover using its own data protection capabilities.

Ransomware has only become more sophisticated, more widely available, and more convenient for hackers over time. Cybercriminals can now use **Ransomware-as-a-Service (RaaS) providers** to create ransomware attacks with little technical knowledge or expertise.

Research done by the security firm Sophos showed that **66% of organizations were hit by ransomware in 2021, up from 37% in 2020**. In the same timeframe, the study also showed that ransom payment demands have also increased. The average ransom payment came in at $812,360 USD, a 4.8X increase from the 2020 average of $170K.

Even if the organization does not pay the ransom, a ransomware attack still has significant costs. Loss of income and interruption of operations amounted to an average cost of $1.4M. The average length of time to recover from a ransomware attack was one month.

Phishing and social engineering

Phishing and social engineering exploits are two of the most common methods of spreading ransomware, largely because these methods rely on human error rather than technical vulnerabilities. Research from Veeam's Ransomware Trends Report 2022 showed that **44% of ransomware infections came from phishing emails or malicious links** on websites. It's technologically easier to entice a human to click on an infected link than it is to breach a multi-layer security system.

Who is at risk?

Effective ransomware protection requires a combination of:

1. End user training
2. Regular software updates
3. Reliable and protected backup procedures
4. Protection of privileged accounts

End user training can help prevent initial exposure by educating users about the types of dangers to avoid.

Restoring from **backups** has proven to be the best way to recover from ransomware attacks.
The Sophos State of Ransomware 2022 report showed that 73% of organizations used backup to restore encrypted data. IT security professionals need to make sure that backups are not only working and current but also immutable, air-gapped, and incorruptible to ransomware.

Patching ensures that a business is protected from known exploits.

Finally, protecting and **restricting access to privileged accounts** can help limit the spread of a ransomware attack.

Supply chain vulnerabilities

Before 2022, supply chain vulnerabilities weren't considered a frontline security risk. However, after the SolarWinds exploit in December 2020, and the Kaseya attack in July 2021, the possibility and potential damage caused by supply chain vulnerabilities hit the top of most IT security professional's radar.

These attacks show that very sophisticated security attacks are becoming more common. The SolarWinds attack involved nation-state level actors who exploited a vulnerability in SolarWinds Orion, a widely used IT performance monitoring system. Using a backdoor exploit called Sunburst, cybercriminals were able to gain access to systems of **more than 30,000 SolarWinds customers and partners**, including the U.S. Departments of Treasury, Commerce, Homeland Security, and other high profile private companies like Intel, VMware, and Cisco.

Solarwinds created a patch for the software exploit and the company itself underwent a massive security overhaul to prevent similar attacks in the future.

Kaseya VSA

Likewise, the Kaseya breach exploited vulnerabilities in Kaseya VSA (Virtual System Administrator) IT Management software. VSA is used for managing networks, systems, and information technology infrastructure. VSA is popular among managed service providers (MSPs) that use it to remotely administer IT systems for their customers.

The MSP business has boomed during the coronavirus pandemic. Along with a substantial increase in remote work. **Exposures in MSP tools can be hard for customers to detect and defend**. An authentication bypass vulnerability in the Kaseya VSA software allowed the REvil ransomware gang to distribute a malicious payload through hosts managed by the VSA software. The payload spread ransomware to the customers' endpoints.

According to Kaseya, there were about 50 direct customers, and between 800 and 1,500 other businesses, that were impacted by this breach. After involvement from the U.S. and Russian governments, the REvil websites vanished from the Internet. And Kaseya announced it had created a patch for the VSA software. And that it had received a universal decryptor tool that it used to help businesses recover their data.

Spotlight on supply chain vulnerabilities

High profile and far-reaching exploits really put a spotlight on supply chain vulnerabilities. These types of exploits can be hard to detect. And protecting against this type of threat requires a cooperative multi-company approach. You need make sure that all your software partners and suppliers follow security best practices. As well as keeping all your software updated with the latest security patches.

Remote access management

Remote access management has always been a critical concern for IT security professionals. Windows Remote Desktop Protocol (RDP) is a standard service available in all current versions of Windows. RDP gives IT administrators, IT professionals, and end users the ability to log into a remote computer that's connected across the network.

Likewise, remote Linux systems often use VNC (Virtual Network Computing) or one of its many open-source derivatives like RealVNC, TightVNC, or TigerVNC to provide this type of remote access.

RDP and VNC have always been widely used for remote administration. But the increases in the remote workforce driven by the pandemic have really pushed the usage of these remote access technologies to a new level. Unfortunately, remote access services are often a focus for attacks on the network perimeter. Internet-facing servers, running Windows or Linux, often receive many brute-force login attempts, which is a tactic that is typically associated with ransomware attacks.

Lateral movement using compromised account credentials

Weak passwords and stolen credentials are also some of the primary ways that hackers and cybercriminals can breach your remote access technologies. Once a hacker has breached your network, they can also use these remote access technologies for lateral system access within your networks.

A remote access management solution, like Devolutions ***Remote Desktop Manager,*** can combine the ability to perform remote access, using RDP or VNC, with password and security management. It enables you to unify, centralize, and control access to all the systems on your network.

Remote access management solutions can harden security and network perimeter protection by:

- **Enforcing strong passwords** - Security starts by making sure that all your users have strong passwords. Strong passwords that can't be easily guessed provide a core protection for your organization's sensitive data, and can provide a strong layer of protection from brute-force and password spraying attacks.

- Tools like Devolutions ***Remote Desktop Manager (RDM)*** can ensure that your remote desktop passwords are strong by supporting password policies requiring length, levels of complexity, and enforcing password reuse history. A password generator and password analyzer make it easier for users to create and use strong passwords.

- **Providing centralized password management** – Remote access managers centrally and securely store all your remote connection passwords in one secure location. They eliminate the need for users to come up with their own haphazard password storage schemes. RDM can store company-wide passwords in an on-premises encrypted database, helping users to quickly access the connection information they need, and to share information between and across teams, eliminating the need for users to store passwords and remote credentials in unsecured files or even Post-it notes.

- **Enabling secure on-demand remote sessions** – Remote connections can be encrypted, protecting them from man-in-the-middle attacks. You can set RDP connection security to ***high***. And VNC can be upgraded to 256-bit AES by a configuration setting in the VNC Server.

- **Providing real-time session tracking** – When it comes to remote access, keeping track of who accessed what, when, and for how long is essential for security and compliance requirements. Regular monitoring helps you to detect if there are any unusual activities like unauthorized failed login attempts. A remote access manager also provides a centralized consolidated view of all your organization's remote desktop activity. RDM can track the connection system, date, time, user, and machine for all remote sessions.

Privileged access

Managing privileged access, and reducing the risks associated with the use of privileged accounts, is another one of the top challenges for IT security professionals. According to the Verizon Data Breach Investigations Report (DBIR) for 2022, in the past year ***"82% of breaches involved the human element. Whether it is the Use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike."***

Protecting credentials, and especially privileged credentials, is essential for protecting your network and systems. Cybercriminals rely on access to vulnerable privileged accounts to breach networks, access critical systems, and steal confidential data.

Privileged accounts can do more damage to the organization than accounts that only have standard user rights or outsider guest access. Because in addition to data, they can also access services and even system configurations.

Microsoft has stated **that privileged access should be the top security priority at every organization**. Planning around the principle of least privilege, where accounts are only assigned the rights that they need to perform a given task, is one of the best ways to limit the exposure of privileged accounts.

Privileged Access Management

Privileged Access Management (PAM) solutions, like Devolutions Server, address privileged access exposures by securing, controlling, managing, and monitoring privileged access to critical assets. PAM solutions monitor and control access to highly privileged accounts. And they not only protect against external cyber threats, but they can also prevent insider threats like the accidental or deliberate misuse of privileged accounts.

To prevent these types of threats, PAM solutions enable you to restrict, revoke, and monitor the access of highly privileged accounts. When privileged accounts are created, PAM solutions can provide protection for the credentials for those accounts. A credential storage solution or password management system is used to securely store the privileged account authentication information, preventing possible theft or mismanagement.

To access these privileged accounts, PAM users must use their PAM solution for authentication. Each time these accounts are accessed, the PAM solution logs the session and tracks the actions performed. A complete record of the privileged account access will include:

- the name of the user
- the time the session began
- how long the session lasted
- and the actions performed using those credentials

PAM solutions also provide you with vital information about your privileged accounts that you might not be aware of. For example, you can discover things like how many privileged accounts you have that never expire, or how many privileged accounts exist that should have been deprovisioned.

While some businesses may view PAM solutions troublesome or difficult to implement, these solutions help streamline the management and monitoring of privileged users. PAM makes it easier to effectively secure the most important parts of your changing IT infrastructure.

Emerging challenges for 2022 and beyond

In addition to these top challenges that IT security professionals face in 2022, there are a several emerging challenges that are sure to grow in significance over the coming year. **One of the biggest emerging security challenges for 2022 and beyond is IoT (Internet of Things) security**. All sorts of different IoT devices are rapidly being deployed to address computing requirements in everything from process control to edge computing, and even home automation.

Internet of Things

IoT devices don't rely on human intervention to function. IoT devices automatically use sensors to collect, analyze, and process information. However, this automation can create a significant security risk as IoT devices can be comprised without anyone knowing about it. Data and services from IoT are often shared with other IoT devices. As well as server and cloud services, making the risks of a security exposure very significant.

Because of their autonomous nature, IoT devices must be kept up to date with all security patches and OS updates required by the devices to be properly secured. It's also important to use strong passwords or multi-factor authentication whenever possible for all connected devices.

Linux and Mac security

A couple of other emerging concerns for IT security are sure to be Linux and Mac security. While Windows ubiquitous deployments have long made it the biggest target for malware, Linux and macOS have been getting more attention from cybercriminals.

A Crowdstrike report looking into the attack data from 2021, showed that there was a **35% rise in malware targeting Linux systems compared to 2020**. Likewise, Mac use in enterprises has also increased – especially for laptops, which have now become quite mainstream. According to IDC, **macOS devices were used in 23% of U.S. enterprises in 2021**, up from 17% in 2019, making them a more attractive target for hackers than they were in the past.

Here again, regular software updates and strong passwords provide a sound basis for securing these platforms. Making sure that all privileged accounts are protected also helps limit any exposure from possible Linux or Mac attacks.

Security is the highest priority for IT professionals

There's no doubt that security will continue to be one of the highest priorities for IT professionals for the foreseeable future. Tackling challenges like ransomware, supply chain attacks, remote access management, and privileged access requires a combination of user education, best practices, and security solutions like Devolutions Remote Access Management and the PAM support in Devolutions Server. Remote Access Management can ensure that your users have strong and secure centrally managed passwords, while PAM can safeguard access to your privileged accounts, which have the deepest levels of access into your organization's information structure.

Additional Information

For more detailed information about SMB cybersecurity challenges and solutions, be sure to check out Devolutions State of Cybersecurity in SMBs in the 2021 report.