Kaseya 365 USER

5 THREATS TO USERS THAT DEMAND IMMEDIATE ACTION

Employees are among an organization's most valuable assets. However, they are also the weakest link and a vulnerable gateway for attackers seeking to compromise business security. Simply taking precautions is not an option!

The first step to protecting your organization is to identify and understand the threats likely to plague the business so you can take steps to stop them. The second, and most critical step, is investing in modern tools and best practices that enable you to prevent, respond and recover should that weakest link break.

This infographic provides an overview of the top five threats to look out for and how to stop them before they stop you.

1 PHISHING & SOCIAL ENGINEERING ATTACKS

Email is simultaneously an essential service and the biggest vulnerability for any business. About 90% of all cyberthreats start with an email,[1] and phishing attacks are the most common.

Although phishing attacks most often come in the form of email messages, they can also occur through text messages, phone calls or fraudulent websites. Regardless of medium, the objective of a phishing attack is to trick users into sharing sensitive information, like passwords or payment details, or click malicious links that install malware. These attacks often impersonate trusted entities, such as banks or company executives.

Fortunately, with the right tools and best practices, phishing attacks are easy to stop.

Anti-phishing filtering blocks phishing emails before they reach users, thwarting the risk at the source.

Employee awareness training helps ensure that users have the education and skills needed to identify a potential attack.

Phishing simulations deliver realistic mock attacks to determine which users are properly trained and able to recognize a potential attack and which need more training or a refresher.

2 CREDENTIAL COMPROMISE

The dark web is big business for bad actors, offering a lucrative marketplace to sell credentials stolen through phishing, malware and data breaches. Attackers can then use these credentials to impersonate employees or gain unauthorized access to systems.

With an estimated more than 36 billion credentials available on the dark web,[2] it's highly likely that your users' credentials can also be found there.

Here, too, the right tools and best practices are critical to protect your users and your business.

Dark web monitoring is proof that knowledge is power. After all, you can't plug a gap if you don't know it's there. Dark web monitoring tools scan the dark web for compromised user accounts, and many allow you to set your scans to a regular schedule, providing you with the information you need to stay proactive.

Alerts for exposed credentials allow you take immediate action, empowering you to respond swiftly when it matters most.

Automated password resets force affected users to change passwords quickly, mitigating or stopping a potential breach.

3 RANSOMWARE ATTACKS

Phishing emails and compromised credentials are the gateway to a more disruptive problem: ransomware attacks. Ransomware encrypts critical files and demands payment for decryption. Paying the ransom, however, doesn't always result in data being returned. It's a costly problem without an easy solution — unless you have a tested and proven backup and recovery plan in place.

SaaS backups performed regularly ensure that the most recent version of cloud-based critical business data (e.g., Microsoft 365) is accessible for easy recovery.

Rapid recovery options quickly restore the most recent backup of the encrypted files to reduce downtime.

User awareness training, when conducted regularly, helps prevent users from clicking phishing emails, making it more difficult for bad actors to gain a foothold in your environment and deploy ransomware.

4 SAAS MISCONFIGURATIONS AND UNAUTHORIZED ACCESS

Configuring your SaaS platforms is far from just being a one-and-done. Even flawless initial configuration and permissions have the potential to age poorly with users leaving the company or access needs changing. Misconfigured SaaS platforms and inadequate access control allow unauthorized users to obtain sensitive information or modify business systems, whether inadvertently or deliberately. Having a solution in place that detects and automatically remediates SaaS security threats will mitigate these vulnerabilities.

Automated SaaS management ensures proper configuration and permissions from the get-go and aggregates and analyzes user behavior, keeping an eye out for unusual user activity that may require action or changes.

Real-time alerting detects and flags unusual activity across SaaS applications, notifying you of unusual, high-risk behavior.

Automatic account locking disables compromised accounts and blocks any new login attempts to contain the potential risk.

5 BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) attacks trick employees into making wire transfers or sharing sensitive information through fraudulent emails from a bad actor impersonating executives or trusted partners. BEC has become an increasingly popular tactic, with 21,489 attacks in the United States in 2023 that cost $2.3 billion.[3] Here again, prevention, with the right tools and training, reduces the risk.

Anti-phishing filtering identifies and blocks suspicious emails by removing them (and their potential risk) before they reach users.

User susceptibility testing evaluates employee awareness and knowledge and improves vigilance. Simulations are a risk-free and cost-effective way to establish who needs additional training.

Alerts for unusual email behavior flags account takeovers or suspicious activity, allowing you to stop a BEC before its impact is felt.

KASEYA 365 USER: COMPREHENSIVE PROTECTION BEYOND THE ENDPOINT

The importance of the ability to **prevent, respond and recover from threats** to users cannot be understated. Kaseya 365 User provides an integrated solution that protects users from cyberthreats. Our holistic approach ensures comprehensive protection for users, data and business operations.

LEARN MORE

Sources

1. https://www.idagent.com/resources/mid-year-cyber-risk-report-2024/
2. https://www.reliaquest.com/resources/research-reports/annual-threat-report-2024/
3. https://www.ic3.gov/PSA/2024/PSA240911