Kaseya 365
User

Building cyber resilience

Key considerations for protecting users

As phishing, ransomware, BEC and other sophisticated cyberattacks rise, protecting end users is no longer optional, but a business necessity. True cyber resilience starts with securing user identities, data and privacy through proactive strategies and layered security solutions.

To help you stay ahead, we've created a comprehensive checklist with practical steps and insights to strengthen defenses, secure accounts, reduce risks and recover quickly from disruptions. Discover how the right measures can help your business not only withstand today's threats but thrive amid tomorrow's challenges.

1 Educate and empower users

According to the 2026 Kaseya Cybersecurity Outlook Report, nearly 30% of businesses expressed concern that human error may become a significant threat vector, potentially enabling a successful cyberattack within the next 12 months.

A well-informed workforce is critical to building a cyber-resilient business. Users who have a good understanding of emerging threats can help to reduce the risks of cyberattacks. Follow these steps to cultivate a security-aware culture and empower end users:

- [ ] **Conduct regular security awareness training**

  Equip your end users with the knowledge and skills to reduce the likelihood of human error and recognize cyberattacks like phishing and social engineering with scheduled periodic training.

- [ ] **Use phishing simulations**

  Conduct realistic phishing simulations to test your organization's resilience. These exercises not only assess user readiness but also help identify patterns of high-risk behavior, paving the way for tailored training solutions.

- [ ] **Provide tailored training content**

  It is important to understand that cybersecurity threats vary depending on job functions. Provide customized training materials to address specific risks associated with different roles, such as the human resource department handling sensitive employee data or the finance teammanaging payment systems.

2 Protect user accounts and credentials

The 2025 Data Breach Investigations Report found that over 20% of breaches involved the use of stolen credentials.[1] User accounts and credentials are the gateway to an organization's network and systems. Therefore, they are among the most sought-after targets for attackers. With billions of compromised credentials circulating on the dark web, the need to safeguard accounts has never been more critical. Here's how to stay ahead of the threat:

- [ ] **Implement anti-phishing defenses**

  Deploy robust anti-phishing solutions to prevent threat actors from gathering user credentials. Use email filtering technologies to block malicious emails before they reach user inboxes and leverage powerful technology like machine learning and AI.

- [ ] **Use dark web monitoring solutions**

  Leverage dark web monitoring tools to detect exposed credentials associated with your organization. Early detection minimizes the risk of attackers exploiting stolen credentials to cause further damage.

- [ ] **Mandate the use of MFA**

  Making MFA mandatory adds a critical layer of defense, significantly reducing the risk of account compromise by requiring an additional verification step, such as a one-time code, biometric authentication or hardware token.

3 Detect and respond to threats in SaaS applications

Cloud-based Software-as-a-Service (SaaS) applications have become a core component of business productivity today. More than 60% of business data is now stored in the cloud.[2] Although the rapid adoption of SaaS applications has revolutionized business productivity, they also introduced new vulnerabilities and threats. Here are some key strategies to address the new vulnerabilities SaaS applications have introduced:

- [ ] **Regularly review and adjust permissions in SaaS apps**

  Your IT team must ensure that users only have access to the files and features required for their roles by conducting periodic reviews of SaaS application permissions. Apply the principle of least privilege to restrict access to sensitive data and reduce the risk of insider threats or accidental deletions, learning and AI.

- [ ] **Set up real-time alerts to flag unusual user behavior or misconfigurations**

  Implement monitoring tools to constantly track user activity and SaaS configurations. Configure real-time alerts to notify your security team of suspicious behavior, such as attempts to access restricted areas, data downloads exceeding normal thresholds or unexpected changes to configurations. This is critical to detecting anomalies early and preventing potential breaches.

- [ ] **Automate remediation actions when threats are detected**

  Use automation to respond to detected threats swiftly before they can escalate. For example, configuring systems to lock compromised accounts and block unauthorized IP addresses automatically when threats are detected.

4 Prepare for ransomware attacks

More than 50% of businesses surveyed in the 2026 Kaseya Cybersecurity Outlook Report anticipate experiencing a ransomware breach within the next 12 months. These attacks can cause irreparable damage and, in some cases, shut down businesses for good. Proactively preparing for ransomware threats is essential to safeguarding your organization and ensuring rapid recovery in the event of a crisis. Follow these steps to build resilience against ransomware:

- [ ] **Test recovery plans regularly**

  Develop a detailed disaster recovery plan that outlines steps to respond to disruptive incidents efficiently. Test this plan regularly to ensure business continuity with minimal downtime when the need arises. Testing also helps identify gaps in the recovery process, enabling you to make improvements before a real incident occurs.

- [ ] **Have flexible recovery options**

  Implement robust backup and recovery solutions that allow you to restore data with ease and precision. Flexible options, such as point-in-time restores, enable you to recover data exactly as it was before the attack.

- [ ] **Ensure frequent, automated backups of critical SaaS data**

  Regularly back up critical data from SaaS applications like Microsoft 365 and Google Workspace. Use automated solutions to ensure backups are consistent, up to date and stored securely.

5 Protect against business email compromise attacks

The 2026 Kaseya Cybersecurity Outlook Report found that about 30% of organizations experienced BEC attacks in the past 12 months. BEC attacks are highly targeted and often involve sophisticated social engineering to exploit unsuspecting users and gain unauthorized access to sensitive information or resources. To protect your end users against BEC attacks, follow these strategies:

- [ ] **Use email protection solutions with AI-based detection**

  Implement advanced email security solutions that utilize artificial intelligence (AI) and ML to analyze email patterns, detect anomalies and identify suspicious activity. They provide an essential layer of defense against phishing, BEC and ransomwar attacks by intercepting threats before they reach your end users.

- [ ] **Monitor executive and privileged accounts for targeted attacks**

  Protect critical, high-value accounts, such as those belonging to executives and finance personnel, which are often prime targets for BEC attacks. Ensure these accounts are carefully and consistently monitored to detect unusual activity, such as login attempts from unfamiliar locations, unauthorized forwarding rules or changes to account permissions.

Sources:
1 https://www.verizon.com/business/resources/reports/dbir/
2 https://www.g2.com/articles/cloud-computing-statistics