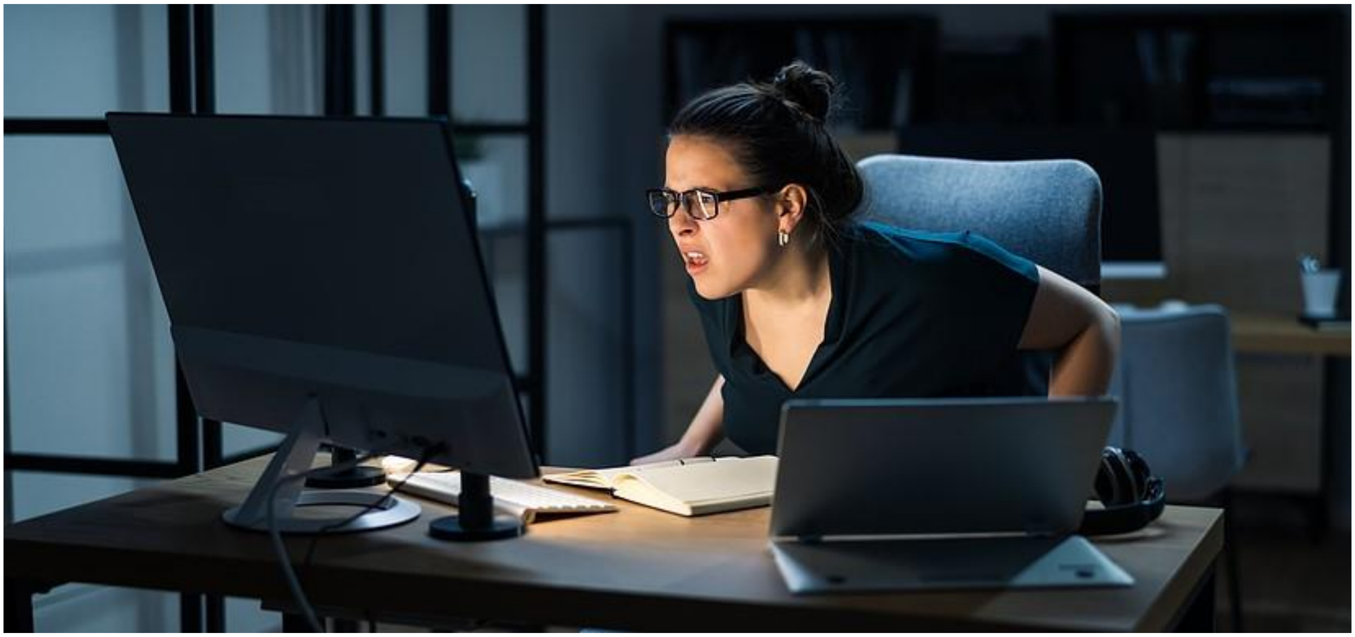
Kaseya Ransomware Attack, Lessons to Learn



Over the July 4th weekend, IT solutions provider Kaseya fell victim to a cyber-attack. Cybercriminal gang REvil exploited a vulnerability in Kaseya’s remote monitoring tool, using the update process to push ransomware further downstream. The Kaseya ransomware attack provides yet another cautionary tale for businesses across the spectrum.

Kaseya represents the trend of small to medium businesses (SMBs) using managed services providers (MSPs) to manage their IT environments. These critical services allow SMBs to focus on their core business while benefiting from enterprise-level IT services. But the convenience, while essential, does pose some risk.

Kaseya Ransomware Attack Highlights Supply Chain Vulnerabilities

In the current attack, REvil infected Kaseya with malicious code attached to its virtual system administrator software. That infection spread to approximately 60 Kaseya customers, all MSPs. And those 60 customers unwittingly passed the infection downstream to up to an additional 1,500 businesses.

While incredibly ambitious, the Kaseya ransomware attack is hardly an isolated instance. It joins a recent spate of similar attacks, including SolarWinds and Colonial Pipeline. In supply chain attacks like these, hackers can compromise thousands of organizations and millions of devices with a single breach.

In this case, Kaseya acted quickly, obtaining a universal decryption key and minimizing the damage somewhat. However, organizations should take note of critical best practices to mitigate the risks they face in their own supply chains.

Update Business Continuity Plans

No matter how diligently an organization addresses cybersecurity, the chances of experiencing an attack run high. Ironically, Kaseya won several cybersecurity excellence awards just months before the attack. Consequently, businesses should take time to regularly update their business continuity and incident response plans.

First and foremost, every business continuity plan must include running and testing backups regularly. Adhere to the 3-2-1 rule. This implies keeping three copies of the backup. Store two of those backups locally, but on different types of media. Store the remaining copy off-site. Automate backups where possible.

Incident response plans work in conjunction with business continuity plans to define a response team and communication plan in advance of an incident. With a plan in place, organizations can respond quickly, minimizing damage and interruptions to the business at hand.

Conduct Security Assessments and Monitoring

The Kaseya attack happened very quickly. Only two hours lapsed between the time servers were infected and the time the ransomware deployed on individual devices. The speed and sophistication of the attack underscores the need for continuous monitoring.

Organizations should run initial risk assessments to pinpoint vulnerabilities. This will identify gaps and help security teams formulate a plan for strengthening the security posture. But a single assessment provides only minimal protection. On the other hand, continuous, automated monitoring will provide real-time alerts to any suspicious activity.

Implement Zero Trust Strategy

A zero trust security strategy means that the system verifies every access request before granting access to data and resources. Thus, every time a user or device attempts to access information, the system requires validation. This can take the form of multi-factor authentication, endpoint security, identity, and access management and so forth.

Secure the Supply Chain

When hackers identify an attractive target with tight security, they turn their focus to vendors with more lax security measures. For instance, a hospital may boast formidable security. However, if hackers can breach the vendor that supplies telecommunications software to the hospital, they can often compromise their main target.

Because supply chain attacks can originate with any third party, organizations must develop transparency up their supply chain. This involves knowing what security measures vendors have implemented and identifying a communication plan in case a breach occurs. Incorporate strict security standards into vendor contracts.

Improve Your Security Posture with Expert Help

At eMazzanti, we take cybersecurity seriously. We hold ourselves to the highest security standards, and we stay abreast of cybersecurity tools and best practices. We can provide an initial risk assessment to identify areas of weakness. Then, we will help you implement a comprehensive data security plan, including continuous monitoring.