Pitfall4: Failure to address known vulnerabilities

Bookmark this page

High-profile breaches in enterprises have often resulted from known vulnerabilities that went unpatched even after the release of patches. Failure to quickly patch known vulnerabilities puts your organization's data at risk because cybercriminals actively seek these easy points of entry.

However, many businesses find it challenging to quickly implement patches because of the level of coordination needed between IT, security and operational groups. Furthermore, patches often require testing to see if they don't break a process or introduce a new vulnerability.

In cloud environments, sometimes it's difficult to know if a contracted service or application component should be patched. Even if a vulnerability is found in a service, its users often lack control over the service provider's remediation process.

"51% of breaches recorded in 2019 were caused by malicious attacks. Malicious Attacks are the most common and expensive leading causes of breaches"

Solution: Establish an effective vulnerability management program with the appropriate technology to support its growth.

Vulnerability management typically involves some of the following levels of activity:

- Maintain an accurate inventory and baseline state for your data assets.
- Conduct frequent vulnerability scans and assessments across your entire infrastructure, including cloud assets.
- Prioritize vulnerability remediation that considers the likelihood of the vulnerability being exploited and the impact that event would have on your business.
- Include vulnerability management and responsiveness as part of the SLA with third-party service providers.
- Obfuscate sensitive or personal data whenever possible. Encryption, tokenization and redaction are three options for achieving this end.
- Employ proper encryption key management, ensuring that encryption keys are stored securely and cycled properly to keep your encrypted data safe.

Even within a mature vulnerability management program, no system can be made perfect. Assuming intrusions can happen even in the best protected environments, your data requires another level of protection. The right set of data encryption techniques and capabilities can help protect your data against new and emerging threats.