vorlon

Lessons Learned: Navigating the 2023 Data Breach Landscape

White Paper

Version 1
Published 01/03/2024

About this Paper

The year 2023 was characterized by a notable surge in third-party attacks, highlighting a critical shift in the threat landscape. This year's data breaches affected millions, leaving a trail of compromised personal, financial, and health information. From large corporations to government agencies, no sector was immune. With the average cost of a breach reaching a staggering 4.85 million USD[1], it is crucial to learn from past data breaches. This review delves into the most significant breaches of the year, extracting vital lessons to better equip us against future cybersecurity challenges.

Authors

Lauren Lee, Product Marketing Manager

Table of Contents

Major Data Breaches of 2023: A Recap.....4
Common Attack Methods.....6
Key Lessons Learned.....7
Predictions for 2024 and Beyond.....8
Conclusion.....9
Sources.....11

Major Data Breaches of 2023: A Recap

As we reflect on 2023, a year rife with cybersecurity incidents, it's important to review the major data breaches that left a significant impact. This section provides an overview of the most notable breaches, each a distinct narrative. From healthcare and finance to government and technology sectors, these breaches reveal the broad spectrum of cybersecurity challenges faced globally. By analyzing these incidents, we gain valuable insights into the evolving nature of cyber threats and the critical need for robust digital defenses.

MOVEit

The MOVEit Transfer software breach, one of the largest in 2023, began unfolding in May following the disclosure of a critical zero-day vulnerability[2]. Exploited by the Clop ransomware gang, it led to the theft of sensitive data from MOVEit Transfer servers. Affecting over 1,000 organizations and 60 million individuals, the breach had a wide-reaching impact. Among the major victims was U.S. government services contractor Maximus, with the breach compromising the health information of 11 million individuals[3], including Social Security numbers.

HCA Healthcare

In July 2023, HCA Healthcare[4] experienced a data breach after a third-party external storage location was breached. The breach affected approximately 11 million patients, compromising names, contact details, and appointment information. However, it did not include clinical, payment, or sensitive personal information like Social Security numbers. HCA Healthcare responded by disabling access to the affected storage location, reporting the incident to law enforcement, and offering credit monitoring and identity protection services to impacted individuals.

"Affecting over 1,000 organizations and 60 million individuals, the breach had a wide-reaching impact.

Duolingo

In January 2023, Duolingo suffered a data breach where information of 2.6 million users was scraped and leaked. The breach, involving both public and non-public data

such as names and email addresses, raised concerns about potential phishing risks. The leak was facilitated by an exposed API, which remained accessible even post-breach.

MGM

In September 2023, MGM Resorts suffered a cyberattack that disrupted its systems, including digital room keys and slot machines. Scattered Spider, a group skilled in social engineering, is suspected of initiating the breach through a vishing attack, impersonating an employee to gain system access. This breach exposed personal customer data, including names and identification numbers. MGM's response involved notifying affected customers and offering identity protection services.

Johnson Johnson

In September 2023, Johnson & Johnson Health Care Systems (Janssen) reported a data breach involving IBM[5] that affected numerous CarePath customers. IBM is a service provider to Johnson & Johnson, managing the application and third-party database for CarePath. This breach, part of a larger series of leaks impacting various organizations, compromised sensitive customer PHI. The exact number of affected individuals was not specified.

Okta

Okta, a key player in identity management, suffered a breach in October 2023 where unauthorized access to its support cases led to the theft of sensitive HAR files. This incident, resulting from inadequate use of multi-factor authentication, impacted Okta's reputation and financial standing. The breach affected other companies too, including 1Password, Cloudflare, and BeyondTrust, but their robust security measures prevented significant damage.

Sumologic

Sumo Logic, a cloud data analytics company, experienced a security breach in November 2023 involving unauthorized access to its AWS account. The company responded by securing its infrastructure and advising users to reset API keys and various credentials. Sumo Logic reports no evidence of wider network or system impact, and customer data remains encrypted. The extent of the breach is still under investigation, with the company committed to enhancing security measures and monitoring.

Common Attack Methods

The data breaches discussed reveal a crucial element missing in contemporary cybersecurity: the need to secure and vigilantly monitor third-party applications and APIs. These incidents underline several predominant trends:

1. **Zero-Day Vulnerabilities:** Exploited in several breaches, emphasizing the importance of rapid detection and response.
2. **Vulnerabilities in Third-Party Service Providers:** Highlighting the risks associated with external vendors and the necessity for stringent security evaluations and proactive monitoring.
3. **Exposed APIs:** Demonstrating the critical need for secure API integration and continuous data flow monitoring.
4. **Social Engineering Attacks:** Illustrating the effectiveness of human-targeted security breaches.
5. **Inadequate Multi-Factor Authentication (MFA) Usage:** Signifying the essential role of MFA in safeguarding access to systems, especially when third-party applications are involved.
6. **Compromised Credentials:** Pointing to the importance of robust credential management, particularly for systems with elevated access privileges.

These breaches, whether initiated directly through third-party apps or impacting companies using these apps, highlight the risks that can arise from external dependencies. The MOVEit and HCA Healthcare incidents demonstrate the risks of third-party service providers, where a single vulnerability can compromise vast amounts of sensitive data.

The case of Duolingo particularly highlights the critical need for monitoring APIs and the data that flows through them. An exposed API, a fundamental aspect of third-party app integration, was the point of compromise leading to a significant data leak. This incident underlines the importance of stringent security protocols around API usage, ensuring that sensitive data transmitted via these channels is constantly monitored and protected against unauthorized access.

The MGM breach, initiated by social engineering, reflects how human factors in third-party interactions can lead to security lapses. Okta's breach, resulting from inadequate MFA implementation, shows the complexities in ensuring security across integrated third-party systems. Similarly, Sumo Logic’s AWS account compromise points to the risks inherent in cloud services, a common third-party app platform.

These incidents collectively highlight that third-party apps can be both a direct and indirect conduit for cyber attacks. They reinforce the need for organizations to not only implement robust security measures in their own systems but also to rigorously assess and monitor the security postures of their third-party vendors. This approach should include regular security audits, real-time monitoring for suspicious activities, stringent access controls, and ensuring that vendors comply with the same high standards of data protection and cybersecurity.

In essence, the data breaches we saw in 2023 emphasize that effective cybersecurity strategies must extend beyond the organization's immediate digital boundaries to encompass all third-party applications and services integrated into their operations.

Key Lessons Learned

The data breaches of 2023 have provided valuable insights into cybersecurity, especially in relation to third-party applications and APIs. Here are some key lessons to keep in mind:

- **Enhanced Zero-Day Vulnerability Response:** Organizations, especially vendors of third-party services and apps, must develop rapid detection and response protocols for zero-day vulnerabilities. Staying updated with the latest security patches and having an agile incident response team are crucial.

- **Rigorous Third-Party Security Assessments:** It's essential to thoroughly evaluate the security measures of third-party service providers. Continuous regular audits and compliance checks should be part of the vendor management process, not just at the beginning, but throughout the vendor relationship.

- **Securing and Monitoring APIs:** Given the critical role of APIs in modern technology ecosystems, securing and continuously monitoring them is imperative. This includes keeping API hygiene and implementing authentication, encryption, and access control measures.

- **Strengthening Defense Against Social Engineering:** Human factors often present the biggest vulnerability. Training employees to recognize and respond to social engineering attacks, especially vishing, is vital.

- **Comprehensive Use of MFA:** Multi-factor authentication should be non-negotiable across all systems. This extends to third-party applications where data exchange occurs.

- **Effective Credential Management:** Regularly updating and monitoring credentials, especially for high-access systems, can prevent unauthorized access. Implementing a system for frequent password changes and using secure password management tools are recommended practices. Regularly updating and managing API secrets, including tokens and OAuth credentials, every 90 days should be an integral part of credential management practices.

- **Building a Culture of Cybersecurity Awareness:** Beyond technical measures, fostering a culture of cybersecurity awareness within the organization is key. This includes regular training sessions, updates on the latest cyber threats, and encouraging a proactive security mindset among all employees.

- **Creating an Incident Response Plan:** Having a well-defined and regularly tested incident response plan ensures that the organization can act swiftly and effectively in the event of a breach. Ensure that this plan is routinely reviewed and updated, and that every team member is well-acquainted with it.

- **Investing in Advanced Security Technologies:** Leveraging advanced security solutions, including AI, machine, and behavioral learning for anomaly detection, can significantly enhance an organization's ability to detect and respond to threats.

- **Collaboration and Information Sharing:** Engaging in industry collaborations and information-sharing networks can provide valuable insights into emerging threats and best practices.

By learning from these incidents, organizations can not only enhance their security postures but also prepare better for the evolving cyber threat landscape.

Predictions for 2024 and Beyond

As we move forward, the cybersecurity landscape is expected to evolve rapidly, shaped by technological advancements and emerging threats. Here are some predictions for 2024 and beyond:

- **Rise of AI-Driven Cyber Attacks:** Expect a significant increase in cyber attacks powered by artificial intelligence (AI). These sophisticated attacks will likely be more automated and targeted, posing new challenges for cybersecurity defenses.

- **Enhanced Focus on Third-Party Risk Management:** The increasing incidence of third-party breaches will drive organizations to invest more in third-party risk management solutions, focusing on continuous monitoring and real-time threat detection.

- **Greater Emphasis on API Security:** With APIs becoming central to digital infrastructure, their security will receive heightened attention. We anticipate advancements in API security technologies and standards.

- **Advancements in Quantum Computing and Cryptography:** As quantum computing advances, we predict a parallel development in quantum-resistant cryptography to protect against future quantum computing-based threats.

- **Expansion of IoT and Corresponding Threats:** The Internet of Things (IoT) will continue to grow, bringing along an expanded attack surface. Security measures specific to IoT devices will become a priority.

- **More Regulatory and Compliance Measures:** With the increasing severity of cyber threats, governments worldwide will likely introduce more stringent regulatory and compliance requirements to protect consumer and business data.

- **Growth in Cybersecurity Insurance:** As cyber risks escalate, the demand for cybersecurity insurance will rise, leading to more comprehensive coverage plans and possibly stricter requirements for insured parties.

- **Evolving Social Engineering Tactics:** Social engineering attacks will continue to evolve, becoming more sophisticated. Organizations will need to invest in regular training and awareness programs to combat these threats.

In summary, the cybersecurity landscape in 2024 and beyond will be dynamic, with emerging technologies both as tools and targets. Staying ahead of these trends will require constant vigilance, innovation, and collaboration within the cybersecurity community.

Conclusion

As we reflect on the cybersecurity landscape of 2023, the lessons learned from the numerous data breaches experienced across various sectors cannot be overstated. These incidents have served as critical reminders of the ever-present and evolving cyber threats, particularly emphasizing the importance of securing and monitoring third-party applications and APIs.

The breaches of 2023 have highlighted key vulnerabilities that organizations globally must address. From zero-day exploits to sophisticated social engineering attacks, the need for a robust, multi-faceted cybersecurity strategy is clear. As these threats continue to evolve, so too must the defenses of every organization.

Therefore, it is imperative for organizations to take these lessons to heart and continually evolve their cybersecurity strategies. This involves not only adopting the latest security technologies and practices but also fostering a culture of cybersecurity awareness and vigilance within their teams. Organizations must remain proactive, not reactive, in their approach to cybersecurity, constantly staying ahead of potential threats and vulnerabilities.

As we move into 2024 and beyond, let this be a call to action for all organizations: to learn from the past, to strengthen current security measures, and to stay vigilant in the face of new and emerging threats. The cybersecurity landscape is always changing, and staying informed and adaptable is the key to maintaining resilience in this dynamic digital world.

Sources

[1] https://www.ibm.com/reports/data-breach
[2] https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability
[3] https://techcrunch.com/2023/07/27/us-government-contractor-says-moveit-hackers-accessed-health-data-of-at-least-8-million-individuals/
[4] https://hcahealthcare.com/about/privacy-update.dot
[5] https://www.bleepingcomputer.com/news/security/johnson-and-johnson-discloses-ibm-data-breach-impacting-patients/

Make 2024 the year you crush the MTTD third-party incidents impacting your data.

Learn how at vorlonsecurity.com

Scan the QR code
to request a live demo.

vorlonsecurity.com

vorlon

vorlonsecurity.com