Parallels® Browser Isolation

Parallels®

WHITEPAPER

The evolution of cyber threats: Actionable tips from the last three-year review

Table of contents

Introduction to cybersecurity challenges

In recent years, the frequency and severity of cybersecurity breaches have significantly increased, affecting various sectors, including banking, healthcare, and consumer services. These breaches result in financial losses and damage the reputation and trustworthiness of the affected organizations.

This paper examines significant cybersecurity breaches from 2021 to 2023, identifies common vulnerabilities exploited by cybercriminals, and proposes technical fixes that could have mitigated the risks or reduced the impact of these attacks. Emphasis is placed on simple yet effective measures such as browser isolation and password management.

Human errors have been a significant contributor to security breaches in cybersecurity. Phishing attacks, for example, exploit human vulnerabilities by tricking individuals into divulging sensitive information or clicking malicious links. A study by Verizon's 2019 Data Breach Investigations Report highlights that 33% of data breaches involved social engineering attacks, predominantly phishing.

Moreover, the COVID-19 pandemic has seen a surge in phishing attacks, exploiting the widespread uncertainty and reliance on digital communications, as noted by a 2020 report from the World Health Organization.

Another example is the use of weak passwords. Despite widespread awareness campaigns, the use of easily guessable passwords remains prevalent. According to a 2019 report by the UK's National Cyber Security Centre, millions of users continue to use passwords like "123456" or "password", making it trivial for attackers to gain unauthorized access.

Misconfiguration of cloud services is another area where human error plays a critical role. The Capital One breach in 2019 is a case in point. A misconfigured web application firewall allowed a hacker to access the personal data of over 100 million individuals. This incident underscores the importance of thorough security configurations and regular audits.

Major breaches and their impact

The banking sector's significant increase in cyberattacks in 2021, with a 1300% rise in blackmail virus incidents, underscores a critical vulnerability to cyber threats. These attacks were characterized by sophisticated methods such as ransomware, phishing, and advanced persistent threats (APTs), which targeted millions of customers' financial assets and confidential data.

- **Banking sector vulnerabilities:** The banking sector experienced a significant rise in cyberattacks in 2021, with blackmail virus attacks increasing by over 1300% compared to the previous year. These incidents highlight the sector's vulnerability to sophisticated cyber threats (Gulyas & Kiss, 2022).
- **Technical actions and challenges:** The attacks exploited weaknesses in the banks' cybersecurity defenses, including outdated firewalls, insufficient endpoint detection, and lack of employee training on cyber hygiene.
- Hackers used phishing emails as a primary vector for installing ransomware on bank networks. Once inside, they escalated privileges to gain access to sensitive areas, deploying ransomware to encrypt data and demand ransom for its release.
- **Broader context and implications:** This surge in cyber-attacks revealed systemic issues within the banking sector's approach to cybersecurity. Many banks were found to rely on legacy systems that needed more agility to respond to new threats.
- Furthermore, the sector's slow adoption of cloud services, partly due to regulatory concerns, left it vulnerable to attacks that cloud-based security measures could have mitigated. The incidents led to financial losses, erosion of customer trust, and regulatory scrutiny, highlighting the need for banks to adopt a more proactive and comprehensive cybersecurity posture.

- **Capital One data breach analysis:** The Capital One data breach of 2019 exposed the personal information of over 100 million individuals. A detailed analysis reveals that the violation was not only due to technical vulnerabilities but also managerial and organizational failures, suggesting a need for a comprehensive approach to cybersecurity (Khan et al., 2022).

  This is a stark reminder of the multifaceted nature of cybersecurity vulnerabilities. The incident was not solely a technological failure but highlighted significant human error.

- **Technical vulnerabilities:** At the heart of the breach was a misconfigured web application firewall that allowed unauthorized access to the data stored on a cloud server. The attacker exploited a server-side request forgery (SSRF) vulnerability to access the server's role credentials and, subsequently, sensitive data.

  This was compounded by insufficient data encryption and inadequate real-time detection mechanisms, failing to identify and mitigate the breach promptly.

- **Managerial and organizational failures:** The breach underscored the lack of a comprehensive cybersecurity framework that included technological solutions and organizational policies—a robust system for continuously monitoring and updating cybersecurity measures also needed to be implemented.

  Additionally, the incident revealed a gap in employee training regarding the latest cybersecurity threats and best practices, contributing to the breach's severity.

- **Broader implications:** Beyond the immediate financial and reputational damage, the breach has had wider implications for the industry. It prompted a reevaluation of cloud security practices and the importance of a holistic approach to cybersecurity that integrates technological, managerial, and organizational measures.

  Regulatory bodies and other financial institutions have taken note, leading to stricter cybersecurity guidelines and a push for greater transparency and accountability in handling customer data.

How cybersecurity lapses led to notable breaches and how to fix it

Over the last three years, the cybersecurity landscape has witnessed a proliferation of attacks exploiting various vulnerabilities and underscoring the critical role of human factors in security breaches. Below are expanded discussions on these topics, supplemented with specific use cases and breakdowns of technical failures:

- **Vulnerabilities and exploits:** Common vulnerabilities exploited in the breaches include insufficient endpoint protection, lack of timely patch management, and inadequate access control and privileges.

SolarWinds Orion platform compromise (2020)

A sophisticated supply chain attack affected the SolarWinds Orion platform, impacting thousands of public and private sector organizations. Attackers managed to insert malicious code into the software's updates, leading to the distribution of a backdoor Trojan among its users.

- **Technical failures:** The breach was facilitated by insufficient endpoint protection against sophisticated malware and inadequate access control measures in software development and distribution processes.

  Moreover, the lack of timely patch management allowed the malicious code to remain undetected and operational for months.

Colonial Pipeline ransomware attack (2021)

This attack temporarily shut down the largest fuel pipeline in the United States, causing widespread fuel shortages and a spike in gas prices.

- **Technical failures:** A compromised password and insufficient network segmentation primarily enabled the ransomware attack. Attackers accessed the network through a VPN account that did not have multi-factor authentication enabled, demonstrating inadequate access controls and privilege management.
- **Human factor:** A significant proportion of breaches were facilitated by human error, emphasizing the need for improved security awareness training among employees (Oka & Hromada, 2022).

Verkada camera hack (2021)

Hackers accessed the live feeds of 150,000 surveillance cameras installed in various facilities, including hospitals, schools, police departments, and prisons. The breach was facilitated using a "super admin" account found exposed on the internet.

- **Human error:** This incident underscored the risks of inadequate security training and poor cybersecurity hygiene, such as the improper handling of access credentials and the failure to implement the principle of least privilege in access controls.

Technical fixes

- **Browser isolation:** Implementing browser isolation could have prevented attackers from exploiting web-based vulnerabilities to access internal systems.
- **Password management:** Enhanced password management policies, including multi-factor authentication (MFA) and password managers, could significantly reduce the risk of unauthorized access.
- **Patch management:** Regular and timely application of security patches would address known vulnerabilities, minimizing the window of opportunity for cybercriminals.

Introduction

Cybersecurity is ever evolving, with attackers constantly finding new vulnerabilities to exploit. Over the last three years, the world has witnessed significant cybersecurity breaches, highlighting the importance of robust security measures. This paper analyzes major breaches, identifies where security measures failed, and discusses specific technical fixes that could have mitigated these risks.

Case study 1: SolarWinds Orion platform breach— a deep dive into supply chain vulnerabilities

Overview: A sophisticated supply chain attack compromised the SolarWinds Orion platform, affecting thousands of public and private organizations globally. The SolarWinds Orion platform compromise, discovered in December 2020, stands out as one of the recent most sophisticated and impactful cyber espionage campaigns.

It affected not only a wide array of private companies but also crucial government agencies in the United States and around the world. The breach was primarily executed through a supply chain attack, which involved inserting malicious code into the platform's software updates.

This incident provides a critical case study in understanding the complexities of cybersecurity in a globally interconnected environment. Here is an expanded insight into the specific technical factors and the after-action analysis.

What went wrong: The attackers inserted malicious code into the software's updates, which went undetected for months. The breach resulted from compromised credentials and a lack of secure software development practices.

- **Trojanized updates:** The attackers inserted a backdoor, SUNBURST, into legitimate software updates for the SolarWinds Orion platform. This was achieved by compromising the software's build environment, highlighting a critical vulnerability in the software development and distribution process.
- **Stealth and longevity:** The malicious code was designed to operate stealthily, with the capability to stay dormant for weeks. It avoided detection by only executing malicious payloads after a delay. It used obfuscated blocklists to prevent running on machines that could detect it, including those belonging to cybersecurity firms.
- **Command and control (C2) traffic mimicry:** The malware communicated with command-and-control servers, mimicking legitimate SolarWinds traffic, which allowed it to exfiltrate data without raising alarms. The sophistication of its evasion techniques was a crucial factor in the duration and impact of the campaign.

Technical fix: Implementing secure software development lifecycle (SDLC) practices could have significantly reduced the risk. Additionally, more robust password management and multi-factor authentication (MFA) for developers and administrative accounts would have made credential compromise more difficult.

- **Software supply chain security:** The attack exploited organizations' trust in their software suppliers. It underscored the need for enhanced security measures in software development and distribution processes, including the use of secure and isolated build environments and verification of software integrity before deployment.
- **Detection and response mechanisms:** The delay in detecting the breach highlighted limitations in existing cybersecurity detection and response frameworks. Many organizations lacked the necessary endpoint detection and response (EDR) solutions and network monitoring tools to identify and mitigate such sophisticated threats.
- **Access and privilege management:** Once inside the network, attackers could escalate privileges and move laterally across it. This points to a need for better access controls, including enforcing the principle of least privilege and segmenting networks to limit lateral movement.

Case study 2:
Colonial Pipeline ransomware attack— analyzing infrastructure security breaches

Overview: A ransomware attack on Colonial Pipeline, a major fuel pipeline in the USA, led to significant fuel shortages. The attackers gained access through a compromised VPN password.

What went wrong: The compromised VPN account did not enable MFA, allowing attackers easy access once they obtained the password. The ransomware attack on Colonial Pipeline, one of the most critical infrastructure systems in the United States, disrupted fuel supply across the Eastern Seaboard and marked a significant escalation in the cyber threat landscape targeting vital national infrastructure. This event underscored several technical vulnerabilities and operational oversights.

Expanding on the overview and what went wrong, here are more technical details and insights into the event:

Initial access and exploitation

- **Compromised VPN password:** The attackers obtained a legacy VPN password that was no longer in use but still provided access to Colonial Pipeline's network. This password was reportedly found in a batch of leaked passwords on the dark web, suggesting it may have been reused across multiple services, a common security oversight.
- **Lack of multi-factor authentication (MFA):** The critical failure in this case was the absence of MFA for the VPN account. MFA is a security enhancement that requires two or more proofs of identity to grant access, significantly reducing the risk of unauthorized access even if a password is compromised.

Lateral movement and escalation

- **Network segmentation:** Once inside the network, the attackers likely exploited the lack of adequate network segmentation. Proper segmentation would have limited their ability to move laterally across the network and access critical operational systems.
- **Privilege escalation:** The attackers used techniques to escalate their privileges within the network. This could involve exploiting network software vulnerabilities or leveraging compromised administrative credentials, allowing them to gain broader access and control over the system.

Ransomware deployment and impact

- **Ransomware payload:** The specific ransomware known as DarkSide is a type of ransomware-as-a-service (RaaS) sold or leased to cybercriminals. It encrypts files on infected systems, making them inaccessible, and demands a ransom for the decryption key.
- **Operational shutdown:** Faced with the encryption of critical operational IT systems, Colonial Pipeline proactively shut down its pipeline operations to prevent the ransomware from affecting operational control systems. While necessary for security reasons, this decision led to significant fuel supply disruptions.

The company confirmed it paid the ransom demanded by the attackers (approximately $4.4 million in cryptocurrency) to expedite the restoration of its systems. This controversial decision underscored the challenging position companies find themselves in during such crises.

Technical fix: Enabling MFA on all remote access systems and employing browser isolation to access sensitive systems can prevent similar attacks. Additionally, implementing a robust password management system would mitigate risks related to password theft.

Case study 3:
The Facebook data breach—
understanding the exploitation of social network vulnerabilities

Overview: Personal data from over 530 million Facebook users was available on a hacking forum, originating from a vulnerability exploited in 2019. The breach involving personal data from over 530 million Facebook users, which became publicly available on a hacking forum, highlights critical vulnerabilities and lapses in Facebook's security controls.

This incident was traced back to exploiting the platform's "Add Friend" feature in 2019. By delving deeper into the technical issues and the modern security controls that could have mitigated these vulnerabilities, we can gain insights into how such a significant breach occurred and what measures are essential to prevent similar incidents in the future.

What went wrong: Attackers exploited a vulnerability in Facebook's "Add Friend" feature, which was not appropriately secured against scraping. The attackers took advantage of the "Add Friend" feature's functionality, which allowed users to connect with others on the platform.

Specifically, the vulnerability was in the feature's phone number lookup function, where entering a phone number would reveal the associated user's profile. This functionality was not intended for mass data extraction but was exploited to scrape user data on a large scale.

One of the primary technical shortcomings was the lack of effective rate limiting for the "Add Friend" feature. Rate limiting is a crucial security control that restricts a user's requests to a service within a specific timeframe. Without strict rate limits, attackers could automate requests to the feature, enabling them to scrape data at scale.

The platform's monitoring systems failed to detect the abnormal, large-scale use of the "Add Friend" feature for grinding purposes. Effective anomaly detection systems could have identified and flagged the unusual patterns of requests, leading to early detection of the scraping activity.

Technical fix: Regular vulnerability scanning, immediate patching, and rate limiting and monitoring unusual access patterns could have prevented the exploitation. Implementing better access controls and encrypting sensitive data would also reduce the impact of such breaches.

Fixes for common risks in cybersecurity

Browser isolation

Browser isolation is a technology that isolates internet browsing activity from the local machine and the corporate network. It prevents malware, ransomware, and other threats from reaching end-user devices or the corporate environment.

For instance, in the case of the Colonial Pipeline, if administrative tasks were performed within an isolated browser session, it would have been much more challenging for attackers to exploit the VPN password.

Browser isolation technology offers a promising solution to mitigate the risks associated with human errors. This technology isolates the browsing activity from the local machine and network, effectively containing malicious content in a secure, remote environment. Here is how browser isolation negates risks from human errors:

- **Phishing protection:** By isolating the browsing session from the end-user's device, even if a user inadvertently clicks on a phishing link, the malicious payload is contained within the remote environment. This prevents any malware from reaching the user's device or network.
- **Secure web gateways:** Browser isolation serves as a secure web gateway, scrutinizing and filtering out malicious content before it reaches the user. It can block access to known malicious sites or quarantine suspicious downloads for further inspection.
- **Reducing surface attack:** The attack surface is significantly reduced since the isolated browsing session. Attackers cannot exploit browser vulnerabilities to access the user's device or internal networks.
- **Privacy and compliance:** Browser isolation helps maintain privacy and compliance with data protection regulations by ensuring that sensitive data is not inadvertently leaked through the browser.

For instance, an institution's adoption of browser isolation could prevent a scenario like the Capital One breach. Even if an employee were to misconfigure an application or click on a phishing link, the isolated browser environment would contain the threat, preventing data exfiltration.

Password management

The importance of strong password policies and management must be balanced. Using a password manager can help generate and store complex passwords, reducing the risk of password-related breaches.

Furthermore, enforcing MFA adds a layer of security. For example, the SolarWinds and Colonial Pipeline breaches could have been averted, or their impacts would have been significantly reduced if robust password management and MFA had been implemented.

Parallels Browser Isolation

Parallels Browser Isolation strengthens your Zero Trust security approach by providing a secure path to web browsing and access web applications, including Software as a Service (SaaS) applications right from your preferred web browser.

Ready to start, continue, or further enhance your Zero Trust journey?

If you or your organization are looking to address any of the above complexities associated with delivering secure web access solutions, learn more by signing up our free 7-day trial:

Get your free trial of Parallels Browser Isolation now.

References

- Microsoft Security Response Center. (2020). A moment of reckoning: the need for a robust global cybersecurity response. [Blog Post]. Retrieved from https://msrc-blog.microsoft.com/2020/12/13/a-moment-of-reckoning-the-need-for-a-strong-and-global-cybersecurity-response/
- Kolochenko, I. (2021). Understanding the SolarWinds Hack and its Security Implications. Infosecurity Magazine. Retrieved from https://www.infosecurity-magazine.com/opinions/understanding-solarwinds-hack/
- CISA. (2021). Alert (AA21-131A) - DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/uscert/ncas/alerts/aa21-131a
- Newman, L. H. (2021). The Facebook Data Leak: What Happened and What is Next. WIRED. Retrieved from https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/
- Burt, T. (2021). Turning the page on Solorigate and opening the next chapter for the security community. Microsoft On the Issues. Retrieved from https://blogs.microsoft.com/on-the-issues/2021/02/18/solorigate-security-community/
- FBI. (2021). Colonial Pipeline Cyber Attack. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
- Gallagher, S. (2021). How SolarWinds hacked back: Details on their proactive response. Ars Technica. Retrieved from https://arstechnica.com/gadgets/2021/01/how-solarwinds-hacked-back-details-on-their-own-proactive-response/
- Alperovitch, D. (2021). The Truth About the SolarWinds Hack and Complex Cyber Intrusions. CrowdStrike Blog. Retrieved from https://www.crowdstrike.com/blog/the-truth-about-solarwinds-hack/
- LastPass. (2022). The Guide to Modern Password Security. LastPass. Retrieved from https://www.lastpass.com/learn/password-security
- Verizon 2019 Data Breach Investigations Report https://www.verizon.com/business/resources/T279/reports/2019-data-breach-investigations-report.pdf
- WHO reports fivefold increase in cyberattacks, urges vigilance (2020) https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
- Most hacked passwords revealed as UK cyber survey exposes gaps in online security (2019) https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security
- Information on the Capital One cyber incident (2019) https://www.capitalone.com/digital/facts2019/
- Attacks Surge in H1 2021 as Trend Micro Blocks 41 Billion Cyber Threat https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats