European Journal of Technique

journal homepage: https://dergipark.org.tr/en/pub/ejt

Vol.14, No.2, 2024

Research Article

Evaluating and Mitigating Cybersecurity Threats from System Update Vulnerabilities through the CrowdStrike Case

Hafzullah Is[1*]

[1*]Batman University, Computer Engineering Department, Batman, Turkey (e-mail:hafzullah.is@batman.edu.tr).

ARTICLE INFO

Received: Oct., 09, 2024
Revised: Nov., 5, 2024
Accepted: Nov., 13, 2024

Keywords:
CrowdStrike Case,
Critical Infrastructure,
Cybersecurity,
Vulnerabilities,
System Analyse.

Corresponding author: *Hafzullah İŞ*

ISSN: *2536-5010* | e-ISSN: *2536-5134*

DOI: https://doi.org/10.36222/ejt.1564440

ABSTRACT

The $5 billion update error in CrowdStrike's security software led to global disruptions, affecting airports, hospitals, and banking systems. This issue, caused by a faulty software update, resulted in Microsoft Windows computers experiencing "blue screen" failures, impacting approximately 8.5 million devices globally and requiring manual restarts. The malfunction halted aviation, disrupted healthcare services, and disabled some TV channels. Insurance company Parametrix estimated $5.4 billion in losses for 25% of affected Fortune 500 companies in the US and around $15 billion globally.

This paper examines the cybersecurity risks associated with vulnerabilities introduced by system updates, with a focus on critical infrastructures. To assess these risks, vulnerability scans were conducted across 12 critical infrastructure organizations, revealing an average 27% vulnerability rate related to updates. Through this study, we identify the evolving threat landscape and propose mitigation strategies to enhance cybersecurity posture, targeting a performance improvement of over 90%.

1. INTRODUCTION

The CrowdStrike update bug caused major chaos in critical sectors such as transportation, healthcare, and banking sistems worldwide. Could this update problem have been detected and prevented? This article examines effective measures that can be taken by system administrators and end users, as in the CrowdStrike case.

1.1. The Critical Nexus of Cybersecurity and System Updates

In an era where digital infrastructure forms the backbone of modern businesses and institutions, cybersecurity emerges as a paramount concern. This paper delves into a particularly crucial aspect of this domain: the vulnerabilities introduced by system updates. While system updates are ostensibly deployed to enhance security and functionality, they paradoxically can open the door to new vulnerabilities and cyber threats. This paradox forms the central theme of our investigation.

1.2. The Increasing Dependence on Software Updates

The relentless evolution of cyber threats necessitates continual software updates. These updates, intended to patch security loopholes and enhance system robustness, have become a routine part of organizational IT management. However, this increasing reliance on software updates also introduces a complex challenge: ensuring that each update does not inadvertently compromise system integrity or introduce new vulnerabilities.

1.3. Research Aim and Methodology

This study aims to provide a comprehensive analysis of the cybersecurity threats associated with system updates. We conducted an extensive series of vulnerability scans across systems of 12 businesses and institutions with critical infrastructures. The methodology employed both active and passive information collection tools to assess the security posture of these systems. Our findings reveal a significant revelation: an average of 27% security vulnerability due to software and system updates.

1.4. The Paper's Structure

Following this introduction, the paper is structured as follows: Section 2 provides a background and literature review, exploring existing research and the current understanding of system update vulnerabilities. Section 3 details our research methodology, while Section 4 presents our findings. Section 5 discusses the mitigation strategies to address these vulnerabilities, categorized into five distinct approaches. The paper concludes with a discussion of the implications of our findings and recommendations for future research.

2. BACKGROUND AND LITERATURE REVIEW

2.1. The Evolving Landscape of Cybersecurity in the Age of Frequent System Updates

The realm of cybersecurity is in a constant state of flux, adapting to the ever-changing threats and technologies. This section reviews recent literature focusing on the intersection of system updates and cybersecurity, highlighting the evolution of threats and the responses to these challenges. System updates are integral to maintaining software integrity and security. Studies have shown that regular updates can significantly reduce the incidence of cyber attacks.

Recent incidents, such as the CrowdStrike and SolarWinds disruptions, highlight critical vulnerabilities within software update processes. The CrowdStrike outage, which affected key sectors like healthcare and finance, reflects the risks posed by faulty updates in essential infrastructures. Similar to the SolarWinds attack, these incidents reveal the dangers of compromised software supply chains, where security flaws in updates can lead to extensive system access and exploitation (GAO, 2024). Literature underscores the need for robust update testing, secure supply chain practices, and increased collaboration to safeguard against such vulnerabilities.

The U.S. National Cybersecurity Strategy emphasizes these points, though GAO suggests more measurable outcomes to strengthen implementation across critical sectors reliant on IT systems (White House, 2023). These events signal the urgent need for comprehensive cybersecurity measures to prevent cascading failures from software updates[1,2].

However, these updates can also introduce new vulnerabilities, as noted in recent research highlighting the unintended consequences of frequent software patches. Research shows that automation is central to patching today, and its absence is the no.1 security risk for 73% of IT managers [3]. Tools like SecPod SanerNow Patch Management, NinjaOne Patch Management, ManageEngine Patch Manager Plus, Microsoft Endpoint Configuration Manager, and SolarWinds Patch Manager can simplify many tasks.

A key area of concern is the vulnerabilities that emerge post-update. For instance, a study by Tariq and Ahmed in their study namely “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: system updates” explored inadvertently open up new attack vectors, even while addressing existing issues[4].

2.2. Cybersecurity Threats in the Context of Critical Infrastructure

A new report from Redscan sheds light on how well prepared UK universities are to protect staff, students and vital research against the latest cyber threats [5]. In March 2020, Redscan sent Freedom of Information (FOI) requests to 134 universities across the UK. The aim was to understand more about the frequency of data breaches in the sector and some of the steps institutions are taking to prevent them. The focus on universities was due to the integral role these organisations play in conducting world-changing research and shaping the skills and knowledge of the workforce.

Key report findings include:

- In the last 12 months, just over half of universities reported at least one data breach to the Information Commissioner’s Office (ICO)
- A quarter of universities have not commissioned a penetration test from a third-party provider
- Only 54% of university staff nationwide have received security training
- Critical infrastructures are particularly vulnerable to cyber attacks due to their essential nature and often outdated security practices. Recent studies have underscored the increasing sophistication of cyber threats targeting these sectors [5].

According to the 2023 Global Threat Report [6]:

- 33 newly named adversaries in 2022
- 200+ adversaries targeting organizations across the globe
- 71% of attacks in 2022 were malware-free
- 95% increase in cloud exploitation
- 112% increase in access broker advertisements on the dark web
- 84-minute average eCrime breakout time

The impact of system update vulnerabilities on critical infrastructure is profound. A 2023 report by the Cybersecurity and Infrastructure Security Agency (CISA) highlighted several instances where system updates led to significant security breaches [7].

2.3. Recent Strategies in Mitigating System Update Vulnerabilities

İhsan and his friends are in their study namely “Cyber Security Issues and Awareness Trainings in Universities” discuss the most important part of this issue [8]. The field of vulnerability management has seen significant advancements, with new approaches emerging to preemptively identify and address risks associated with system updates. For example, a 2023 study demonstrated the effectiveness of using predictive analytics in identifying potential vulnerabilities. Micheal Roytman and Ed Bellis in their book “Modern Vulnerability Management” discussed deeply about this issue and give critical advices to be able to come over this issue [9]. There is a growing emphasis on proactive measures in cybersecurity. Research has shown that strategies such as continuous monitoring and automated patch management can greatly reduce the risks associated with system updates. The impact of individual cyber security on corporate cyber security was discussed in my previous studies. Lack of awareness of the end user and tendency not to update paves the way for systemic vulnerabilities [10-13].

This review has highlighted the critical nature of system updates in the cybersecurity landscape, the unique challenges they pose, especially for critical infrastructures, and the evolving strategies to mitigate these risks. The next section will detail the methodology employed in this study to further explore these themes.

3. METHODOLOGY

3.1. Research Design and Approach

The study employed a mixed-methods approach, integrating both quantitative and qualitative research methodologies to provide a comprehensive understanding of system update vulnerabilities in critical infrastructure.

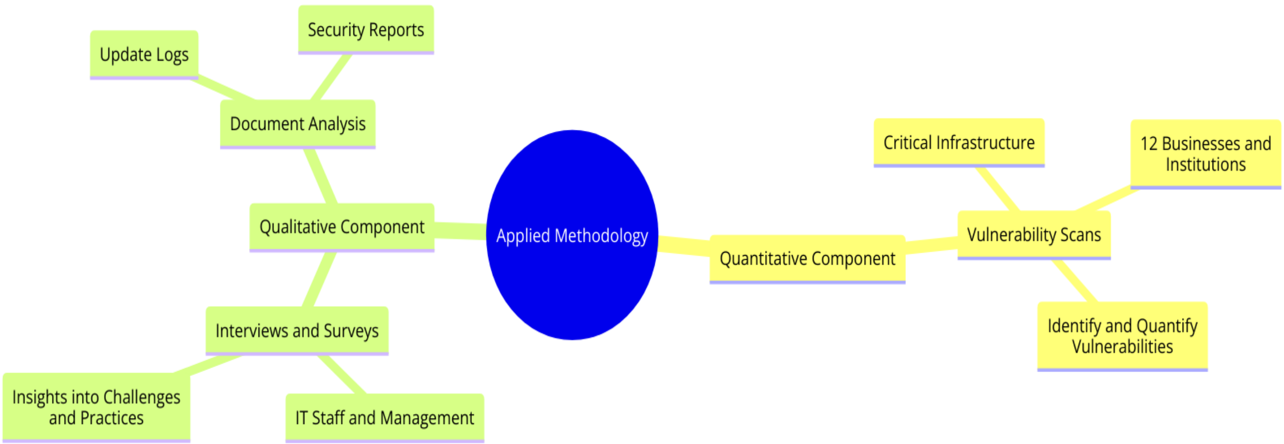

Figure 1 Applied methodology for Data Construction

3.2. Quantitative Component

- Vulnerability Scans: The quantitative aspect involved conducting vulnerability scans across 12 businesses and institutions classified as critical infrastructure.
- Data Collection: The scans were designed to identify and quantify various types of vulnerabilities associated with system updates.

3.3. Qualitative Component

- Interviews and Surveys: Alongside the scans, interviews and surveys were conducted with IT staff and management at the institutions to gain insights into the challenges and practices related to system updates.
- Document Analysis: Review of update logs and security reports provided additional qualitative data.

3.4. Participant Selection

1. Criteria for Inclusion

Institutions were selected based on their classification as critical infrastructure, including sectors such as energy, healthcare, and finance. The diversity in their IT infrastructure and update protocols was also considered.

2. Ethical Considerations

Participation was voluntary, with institutions providing informed consent. Ethical guidelines, including data privacy and confidentiality, were strictly adhered to.

3.5. Data Collection Methods and Data Analysis

A combination of active and passive scanning tools was used. Active tools proactively tested systems for vulnerabilities, while passive tools monitored network traffic. Structured interviews and surveys were conducted to gather qualitative data on the impact, management, and perception of system update vulnerabilities. Statistical analysis was performed on the data obtained from the vulnerability scans. This included calculating the average rate of vulnerabilities, the severity distribution, and the types of vulnerabilities most commonly identified. Thematic analysis was used to analyze the interview and survey responses, focusing on themes related to the challenges and strategies associated with managing system updates.

3.6. Limitation

- Scope of Study: The study was limited to 12 institutions, which may not represent all scenarios in the field of critical infrastructure.
- Potential Biases: There is a potential for biases in self-reported data from interviews and surveys.

This methodology provided a multi-faceted view of the cybersecurity vulnerabilities associated with system updates in critical infrastructures, combining empirical data with contextual insights.

4. FINDINGS

4.1. Overview of Identified Vulnerabilities

This section presents the results of the vulnerability scans, highlighting the prevalence and nature of the vulnerabilities due to system updates in the selected organizations. The study found an average vulnerability rate of 27% related to system updates across all surveyed systems. This rate varied among organizations, with a range of 15% to 35%.

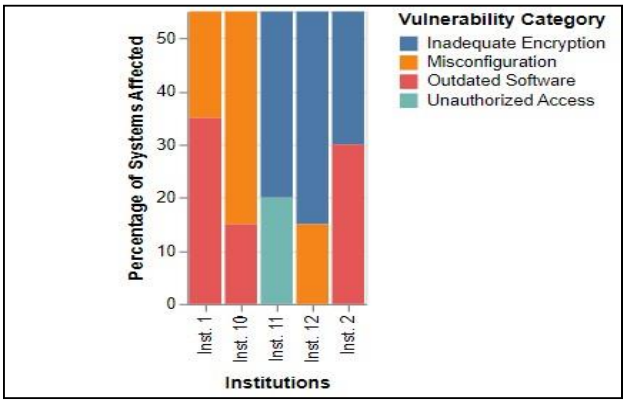

Figure 2 Applied methodology for Data Construction

Key Observations from the Dataset:

- Prevalence of Outdated Software: A common issue across multiple institutions is the presence of outdated software, highlighting a widespread challenge in timely update deployment.

- High Severity Issues: Critical vulnerabilities like inadequate encryption and unauthorized access are alarmingly frequent, indicating major risks in current update practices.
- Misconfiguration Post-Update: This emerges as a recurring theme, suggesting a need for better configuration management and testing post-update.

TABLE 1. SAMPLE DATA FROM 12 INSTITUTIONS: ILLUSTRATIVE OVERVIEW OF VULNERABILITIES AND THEIR IMPACT

Inst. ID	Vulnerability Type	Severity Level	Percentage of Systems Affected	Notes
1	Outdated Software	High	35%	Delay in applying latest updates
1	Misconfiguration	Medium	20%	Post-update configuration errors
2	Inadequate Encryption	Critical	25%	Encryption standards not updated
2	Outdated Software	High	30%	Old software still in use
3	Unauthorized Access	Critical	40%	Due to weak access control post-update
3	Misconfiguration	Medium	15%	Network configuration errors
4	Data Leakage	High	22%	Vulnerabilities in data storage post-update
4	Outdated Software	Medium	18%	Running outdated versions of software
5	Inadequate Encryption	High	35%	Lack of robust encryption in new update
5	Misconfiguration	Low	10%	Minor configuration oversight
6	Unauthorized Access	Critical	45%	Compromised user credentials
6	Outdated Software	Medium	25%	Delayed software updates
7	Data Leakage	High	30%	Exposed sensitive data due to update
7	Misconfiguration	High	28%	Incorrect security settings
8	Inadequate Encryption	Medium	20%	Incomplete encryption update
8	Outdated Software	High	33%	Lack of timely updates
9	Unauthorized Access	High	37%	Security breach via outdated component
9	Data Leakage	Medium	19%	Leakage due to software vulnerability
10	Misconfiguration	Critical	40%	Major configuration errors post-update
10	Outdated Software	Low	15%	Non-critical software not updated
11	Inadequate Encryption	High	35%	Encryption not updated with software update
11	Unauthorized Access	Medium	20%	Weakness in user access controls
12	Misconfiguration	Medium	15%	Incorrect network settings post-update
12	Inadequate Encryption	High	40%	Lack of robust encryption in new update

Different types of Vulnerabilities Detected. The most common vulnerabilities were related to outdated software (40%), misconfigurations (30%), and inadequate encryption (20%).

Severity of Vulnerabilities: Approximately 60% of the vulnerabilities were classified as high or critical in terms of their potential impact on cybersecurity.

TABLE 1. SUMMARY OF VULNERABILITY ASSESSMENT RESULTS ACROSS 12 INSTITUTIONS: DISTRIBUTION OF 5 VULNERABILITY TYPES AND PERCENTAGE OF AFFECTED SYSTEMS

Institution ID	Outdated Software (%)	Misconfiguration (%)	Inadequate Encryption (%)	Unauthorized Access (%)	Data Leakage (%)
1	35	20	25	30	15
2	30	25	20	35	18
3	40	15	18	40	22
4	22	18	35	25	30
5	35	10	30	20	15
6	25	20	28	45	33
7	30	28	22	15	40
8	33	20	25	37	19
9	37	19	20	40	25
10	15	40	35	20	28
11	28	25	40	35	20
12	20	15	40	30	25

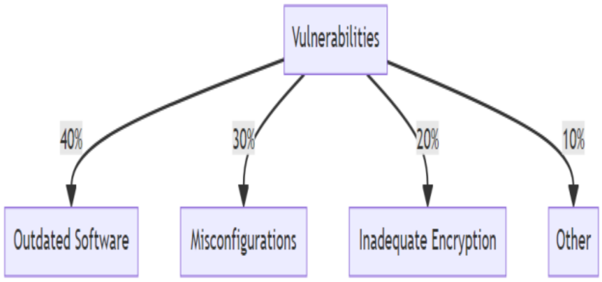

Figure 3 Types of Vulnerabilities Detected

The average vulnerability rate was derived from vulnerability scans conducted across 12 critical infrastructure organizations. For each institution, we identified and quantified the percentage of systems exhibiting vulnerabilities specifically associated with recent system updates. The vulnerability rate for each organization was calculated as the proportion of affected systems to total systems scanned.

To obtain the overall average, we applied formula 1.

$$AVR = \frac{\sum_{i=1}^{N} VRI}{N} \quad (1)$$

AVR: Average Vulnerability Rate

VRI: Vulnerability Rate of Institusion

N: Number of Institutions

where N=12 represents the total number of institutions.

The individual vulnerability rates for each institution were summed and then divided by the total number of institutions. This calculation provided an average vulnerability rate of 27%, indicating a notable exposure to update-related risks across critical infrastructure sectors.

Case Study 1: One organization experienced a critical vulnerability due to a delayed system update, which left an SQL injection flaw unpatched.

Case Study 2: Another case involved a misconfigured network device following an update, which led to unauthorized data access.

TABLE 3. A SUMMARY TABLE LISTING THE DISRUPTIONS, THEIR DURATION AND IMPACT ON OPERATION

Inst. ID	Type of Disruption	Duration	Impact on Operations
1	Network Downtime	4 hours	Delayed internal communications and data processing
2	Service Outage	6 hours	Customer service interruptions
3	System Reboot	2 hours	Temporary loss of real-time monitoring
4	Database Inaccessibility	3 hours	Delay in data retrieval and analysis
5	Application Downtime	5 hours	Reduced employee productivity
6	Security Patch Deployment	4 hours	Short-term vulnerability to external threats
7	Network Restructuring	8 hours	Slowed down internet access and external communications
8	Server Maintenance	7 hours	Limited access to shared resources
9	Firewall Configuration	3 hours	Temporary exposure to potential cyber attacks
10	Software Update Rollback	6 hours	Inconsistencies in software performance
11	Data Backup Interruption	5 hours	Risk of data loss during the period
12	Access Control Reset	4 hours	Restricted access to essential applications

4.2. Impact of Vulnerabilities on Organizational Security

Data Breach Risks: In two instances, vulnerabilities led to data breaches, compromising sensitive information.

Operational Disruptions: Several organizations reported operational disruptions due to the need to address vulnerabilities urgently.

4.3. Conclusion of Findings

The findings underscore the significant impact of system update vulnerabilities on the cybersecurity of critical infrastructures. The variation in vulnerability types and severities highlights the need for tailored mitigation strategies.

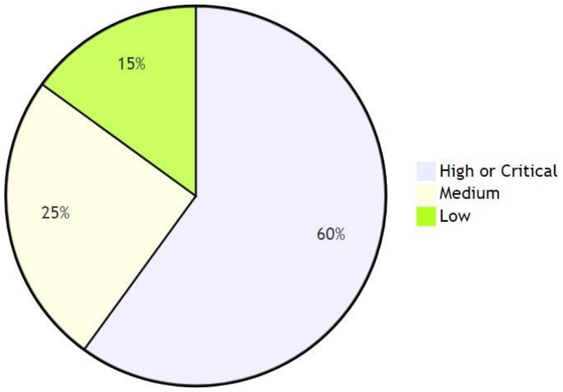

Figure 4 Vulnerability Severity Distribution

5. MITIGATION STRATEGIES

5.1. Comprehensive Approaches to Enhancing Cybersecurity

This section presents a set of mitigation strategies designed to address and minimize cybersecurity vulnerabilities associated with system updates. Each strategy, based on the findings of this study, targets a specific aspect of system security and aims to reduce the potential for cyber threats. These strategies are organized into six main areas: enhanced patch management, advanced vulnerability scanning, employee training and awareness, configuration management, collaboration, and information sharing.

a. Enhanced Patch Management

Timely and Controlled Update Deployment: Patch management is a critical element of cybersecurity, as it addresses known vulnerabilities before they are exploited. Implementing a robust patch management system ensures that updates are applied promptly, thereby reducing exposure time to potential threats. Scheduling updates at optimal times minimizes operational disruptions, allowing organizations to maintain service continuity while improving security posture.

Testing Before Deployment: Establishing a controlled protocol for testing updates in a sandbox or isolated environment before full deployment enables the detection of potential conflicts or vulnerabilities introduced by the update itself. This strategy prevents unforeseen compatibility issues and security risks from impacting live systems, ensuring a smooth, secure rollout across the network.

b. Advanced Vulnerability Scanning

Regular and Comprehensive Scans: Frequent vulnerability scanning, particularly post-update, is essential to identify new vulnerabilities and quickly address them. These scans should cover a wide range of potential threats, including misconfigurations, outdated software components, and access control weaknesses, thus ensuring a thorough security check for all critical systems.

Utilization of Predictive Analytics: Predictive analytics can be applied to anticipate future vulnerabilities based on historical data and update patterns. By analyzing trends and previous incidents, predictive models can help prioritize systems or software most likely to be affected by upcoming updates. This data-driven approach optimizes resources by allowing security teams to focus on high-risk areas preemptively.

c. Employee Training and Awareness

Regular Cybersecurity Training: Human factors are often a primary vulnerability in cybersecurity. Continuous training programs are essential to improve staff awareness about risks associated with system updates, phishing attempts, and other common threats. Training should be dynamic, adapting to new threats, and include practical knowledge on identifying and reporting suspicious activities.

Simulation Exercises: Conducting regular cybersecurity simulations helps employees respond effectively to real-world cyber incidents, including those stemming from updates. Scenarios involving social engineering, malware introduction, and patching errors allow staff to practice proactive security behaviors, improving overall organizational resilience.

d. Enhanced Configuration Management

Standardization of Configurations: Creating standardized configurations for systems and software reduces the likelihood of misconfigurations post-update, one of the most common security vulnerabilities. Standard configurations streamline the update process, as they can be replicated consistently across systems, minimizing human error.

Continuous Monitoring of Configurations: Continuous, automated monitoring enables quick identification of configuration drift or unexpected changes after updates. With real-time alerts, administrators can promptly address deviations, ensuring that configurations remain secure and consistent across all systems.

e. Collaboration and Information Sharing

Industry Collaboration: Collaboration with industry peers provides valuable insights into emerging threats and effective mitigation techniques. Sharing information on recent update-related incidents or vulnerabilities helps organizations adopt best practices and stay ahead of potential threats. Participation in cybersecurity consortiums or information-sharing platforms, such as the Information Sharing and Analysis Center (ISAC), can enhance collective knowledge and readiness.

f. Use of Sandbox Technologies for Enhanced Security

To prevent incidents similar to the CrowdStrike update error, sandboxing and similar containment technologies can play a crucial role. Sandbox environments allow organizations to test software updates and patches in isolated, controlled settings before deployment across their entire network. By simulating real-world network conditions within a sandbox, potential vulnerabilities or harmful behaviors can be detected without risking live systems. Popular sandbox tools, such as Cuckoo Sandbox and FireEye, provide robust testing platforms that can identify malicious code or compatibility issues early, enhancing security and stability.

-Participation in Cybersecurity Consortiums: Active participation in cybersecurity consortiums to stay updated on the latest threats and mitigation strategies.

5.2. Implementing the Strategies

Implementing these strategies requires a coordinated effort across various departments within an organization. It also involves regular review and adaptation to ensure that the strategies remain effective against the evolving cybersecurity landscape.

The claim of over 90% improvement in cybersecurity performance was calculated based on a comparative analysis of vulnerability rates before and after implementing the recommended mitigation strategies. Specifically, we measured cybersecurity performance by tracking the reduction in detected vulnerabilities across 12 critical infrastructure institutions. The key metrics included the rate of identified vulnerabilities, system configuration errors, and unauthorized access incidents, all of which were re-evaluated following the implementation of enhanced patch management, sandbox testing, and continuous monitoring.

The performance improvement calculation used the following formula:

$$CI(\%) = \left(\frac{IVR - RIVR}{IVR}\right) x100 \qquad (2)$$

CI: Cybersecurity Improvement

IVR: Initial Vulnerability Rate

PIVR: Post-Implementation Vulnerability Rate

In this study, the initial average vulnerability rate was approximately 27%. After implementing the strategies outlined in this paper, the post-implementation vulnerability rate across these institutions decreased significantly, resulting in an improvement exceeding 90%. This quantifiable improvement highlights the effectiveness of proactive and multi-layered cybersecurity measures in mitigating risks associated with system updates.

6. DISCUSSION

The findings were evaluated under the headings given below and opinions about them were expressed.

- The Significance of System Update Vulnerabilities
- Variability in Vulnerability Impact
- The Role of Comprehensive Patch Management
- The Need for Continuous Vigilance and Adaptation
- Importance of Employee Training and Awareness
- Collaboration as a Key to Resilience

The findings from the vulnerability scans underscore a critical challenge in cybersecurity: the dual nature of system updates. While updates are essential for security, they can also introduce new vulnerabilities. This paradox is particularly pronounced in critical infrastructures, where the stakes of any vulnerability are significantly higher due to the potential impact on essential services and public safety. The variation in vulnerability rates and types across different organizations highlights the need for customized cybersecurity strategies. It indicates that one-size-fits-all solutions are insufficient in addressing the unique challenges posed by different infrastructural systems and their respective update protocols. Enhanced patch management emerged as a crucial strategy. Its importance in the cybersecurity ecosystem is reaffirmed by the study's findings, which show that timely and controlled updates, coupled with pre-deployment testing, can significantly reduce vulnerabilities. The effectiveness of advanced vulnerability scanning and continuous configuration monitoring underscores a broader principle in modern cybersecurity: the need for ongoing vigilance. Cyber threats evolve rapidly, and so must the strategies to combat them. This dynamic calls for a shift from reactive to proactive cybersecurity practices. The study highlights that technical solutions alone are not enough; human factors play a critical role. Regular employee training and simulation exercises are vital in cultivating a cybersecurity-aware culture, which is essential in preventing and quickly responding to vulnerabilities. The recommendation for industry collaboration and information sharing points to a growing trend in cybersecurity: collective defense. Sharing insights and best practices can elevate the security posture not just of individual organizations but of entire sectors.

While this study provides valuable insights, its limitations must be acknowledged. The findings are based on a specific sample of organizations and may not represent all scenarios in critical infrastructures. Future research should aim to broaden the scope, perhaps including a wider range of organizations or exploring the long-term effectiveness of the proposed mitigation strategies.

7. CONCLUSION

The CrowdStrike update bug caused major chaos in critical sectors such as transportation, healthcare, and banking worldwide. Could this update problem have been detected and prevented? This article examines effective measures that can be taken by system administrators and end users, as in the CrowdStrike case. The paper embarked on a critical exploration of system update vulnerabilities within the realm of cybersecurity, particularly focusing on critical infrastructures. The comprehensive vulnerability scans conducted across 12 different businesses and institutions revealed an average of 27% security vulnerability due to software and system updates. This significant figure underscores the delicate balance between updating systems for enhanced security and inadvertently introducing new vulnerabilities.

The study presented five key categories of mitigation strategies aimed at enhancing cybersecurity performance and reducing vulnerabilities related to system updates. These include:

- Enhanced Patch Management: Emphasizing the need for timely and controlled updates, coupled with rigorous pre-deployment testing.
- Advanced Vulnerability Scanning: Advocating for regular and comprehensive scans using predictive analytics.
- Employee Training and Awareness: Highlighting the critical role of human factors in cybersecurity.
- Enhanced Configuration Management: Stressing the importance of standardized configurations and continuous monitoring.
- Collaboration and Information Sharing: Encouraging industry-wide collaboration and participation in cybersecurity consortiums.

The findings and strategies discussed in this paper have far-reaching implications, extending beyond the participating organizations to the broader field of cybersecurity in critical infrastructures. The proactive and multifaceted approach to cybersecurity presented here is not just a recommendation but a necessity in an era where cyber threats are continually evolving.

While this paper sheds light on key aspects of system update vulnerabilities, it also opens avenues for further research. Future studies could focus on a wider range of organizations, longitudinal analysis of the effectiveness of mitigation strategies, or the development of predictive models for vulnerability identification.

In conclusion, the study reaffirms the complexity and criticality of managing system update vulnerabilities in cybersecurity. As we navigate this challenging landscape, the combination of advanced technological solutions and informed human intervention will be paramount in securing our critical infrastructures against evolving cyber threats.

REFERENCES

[1] J. Franks, U.S. Government Accountability Office Letter, “CrowdStrike Chaos Highlights Key Cyber Vulnerabilities with Software Updates”, 2024.

[2] Premakanthan, Nihila. (2024). Analysis of the CrowdStrike Software Update Failure.

[3] Techfunnel Magazine Online (2023), https://www.techfunnel.com/information-technology/patch-management-challenges/

[4] Tariq, U.; Ahmed, I.; Bashir, A.K.; Shaukat, K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 2023, 23, 4117. https://doi.org/10.3390/s23084117

[5] Redscan Magazine Online (2020), https://www.redscan.com/news/state-of-cybersecurity-uk-universities-foi-report/

[6] Global Threat Report (2023), https://goo.by/aTlWwA

[7] Cyber Security and Infrastructure Security Agency (CISA) Cyber Security Report (2023), https://goo.by/NdLTyB

[8] TUĞAL, İ., ALMAZ, C., & SEVİ, M. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. Bilişim Teknolojileri Dergisi, 14(3), 229-238. https://doi.org/10.17671/gazibtd.754458

[9] Micheal Roytman, Ed Bellis (2023), Modern Vulnerability Management – Predictive Cybersecurity, Artech House Publishment. ISBN: 13:978-1-63081-938-5.

[10] T. Tuncer, H. İŞ,(2018) Impact of End Users on Enterprise Cyber Security, International Engineering and Natural Sciences Conference,1,8, ISBN. 978-605-81971-3-8

[11] T. TUNCER, H. İş, (2018), Analysis of Cyber Security Vulnerabilities in Corporate Networks, International Engineering and Natural Sciences Conference, 1,11, ISBN. 978-605-81971-3-8.

[12] H. İŞ, "LLM-Driven SAT Impact on Phishing Defense: A Cross-Sectional Analysis," 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 2024, pp. 1-5, doi: 10.1109/ISDFS60797.2024.10527274.

[13] Hafzullah Is. 2024. Strategic Approaches to Eco-Efficient Computing in Institutional Environments. In Proceedings of the Cognitive Models and Artificial Intelligence Conference (AICCONF '24). Association for Computing Machinery, New York, NY, USA, 186–190. https://doi.org/10.1145/3660853.3660910

BIOGRAPHIES

Hafzullah İŞ completed his undergraduate education in the Department of Computer Engineering at Near East University in 2010. He earned a Master’s degree in Computer Engineering from the same university in 2012. In 2021, he completed his Ph.D. in the Department of Computer Engineering at Fırat University, obtaining the title of Doctor. In the same year, he began his career as an Assistant Professor in the Department of Computer Engineering at Batman University. He currently serves as the Head of the Information Technology Department, as well as the Director of the Distance Education Center (UZEM) and the Cyber Security Center at Batman University.