www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 541-542

e-ISSN : 2583-1062
Impact Factor : 7.001

EVALUATING THE EFFECTS OF CROWD STRIKE'S 19 JULY 2024 SERVICE DISRUPTION

Dr. Swaleha M Attar[1]

[1]Associate Professor Dr. J J Magdum College of Engineering, Jaysingpur.
Affiliated to Shivaji university, Kolhapur

ABSTRACT

On July 19, 2024, CrowdStrike, a major cybersecurity firm, faced a significant service outage affecting numerous users and the broader cybersecurity sector. This paper investigates the causes, effects, and responses to the blackout, aiming to provide insights for future preparedness.

The analysis begins with the technical and operational details, revealing that a sophisticated cyber-attack exploited vulnerabilities in CrowdStrike's system. The attack used multiple methods targeting the network and software, causing cascading service failures. The attackers' advanced techniques and exploitation of unknown security flaws demonstrated high skill and preparation.

The outage severely impacted thousands of organizations worldwide, including critical sectors like finance, healthcare, and government, leading to increased cyber-attacks and data breaches. The paper quantifies these impacts through data from affected organizations, noting a rise in malware infections, data breaches, and downtime.

In summary, this paper aims to understand what happened during the CrowdStrike outage and learn lessons to help similar organizations be better prepared for future threats. It also talks about the bigger impact on the cybersecurity industry, highlighting the need for backup systems, strong defense strategies, and possibly new cyber security laws.

1. INTRODUCTION

On July 19, 2024, Crowd Strike, a leading cyber security company, had a major service disruption. This affected thousands of organizations relying on their security services like endpoint protection and threat intelligence. The incident revealed significant weaknesses in modern cyber security systems. With many sectors like finance, healthcare, and government relying heavily on digital infrastructure, the impact of such disruptions is huge.

This paper examines the effects of the Crowd Strike disruption to improve future resilience. We analyze the technical and operational causes of the disruption, finding it was due to a sophisticated cyber-attack exploiting unknown security flaws. The attack caused multiple service failures and overwhelmed Crowd Strike's defenses.

The immediate effects were severe, with organizations worldwide facing more cyber threats, downtime, and data breaches. This paper details these impacts and explores how they affect cyber security practices and risk management.

We also look at how Crowd Strike and its clients responded to the disruption, evaluating their incident response and communication protocols. Feedback from affected organizations shows areas for improvement in these responses.

Additionally, the paper discusses the wider impact on the cyber security industry. The incident has led to rethinking the reliance on single vendors for critical security services and highlighted the need for stronger, multi-layered defense strategies. It has also sparked discussions on new cyber security laws.

Finally, we offer recommendations for enhancing cyber security resilience. These include adopting advanced threat detection technologies, regular security audits, and comprehensive incident response planning. We also discuss using AI and machine learning to predict and mitigate threats, aiming for a more secure digital future.

By studying the Crowd Strike disruption, this research aims to help develop stronger cyber security practices and policies, providing valuable insights for both practitioners and policymakers.

What is Crowd Strike?

Crowd Strike is a leading cyber security company that protects devices like computers and servers using cloud technology. It was founded in 2011 by George Kurtz and Dmitri Alperovitch. The company provides tools to quickly find and respond to online threats.

Falcon Platform: Crowd Strike's main platform includes advanced tools like antivirus for protecting devices, EDR for detecting and responding to threats, threat intelligence, and managed hunting. It uses advanced AI and machine learning to analyze large amounts of data quickly. This helps it find and respond to threats on different devices fast.

Cloud-Native Architecture: Crowd Strike's solutions are designed to work in the cloud, making them easy to expand, flexible, and able to get real-time updates without needing traditional hardware or software at your location.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 541-542
e-ISSN : 2583-1062
Impact Factor : 7.001

Threat Intelligence: Threat Intelligence: Crowd Strike offers detailed information about cyber threats through its Falcon Intelligence service. This helps organizations understand and reduce new cyber threats using global threat data and research.

Services: Besides its technology solutions, Crowd Strike provides managed detection and response (MDR) services to help organizations watch for and handle security problems effectively.

Global Presence: Crowd Strike works with many industries worldwide, such as financial services, healthcare, government, and technology. Its solutions help organizations of all sizes deal with cyber security challenges.

Overall, Crowd Strike is known for its innovative cyber security approach, focusing on preventing threats, quickly detecting them, and effectively responding to protect organizations from cyber threats in today's digital world.

Background and Incident Overview: Founded in 2011, Crowd Strike has developed cloud-based security solutions using AI and machine learning for threat detection. On July 19, 2024, the company had a service disruption that affected clients worldwide. This incident disrupted important cyber security operations and caused concern among cyber security professionals and stakeholders.

Causes and Immediate Effects: Causes and Immediate Effects: The reasons for the service disruption on July 19, 2024, are still being investigated, but early reports suggest technical failures in Crowd Strike's infrastructure. The disruption affected many industries using Crowd Strike's services, such as finance, healthcare, government, and technology. During the outage, organizations struggled with threat detection, incident response, and overall cyber security.

Impact on Organizations and Cyber security Practices: The service disruption showed how much organizations depend on third-party cyber security providers and raised concerns about their backup plans and risk management strategies. Many organizations experienced operational disruptions and heightened vulnerability to cyber-attacks during the outage, emphasizing the need for diversified security measures and proactive risk mitigation strategies.

Lessons Learned and Future Recommendations: From the incident, several lessons emerged for both Crowd strike and organizations relying on third-party cyber security services:

Diversification and Redundancy: Organizations should consider diversifying their cyber security solutions and implementing redundancy measures to mitigate reliance on single providers.

Enhanced Communication and Transparency: Improved communication protocols during service disruptions are crucial to maintain stakeholder trust and facilitate effective incident response.

Investment in Internal Capabilities: Organizations should continuously invest in building internal cyber security capabilities to augment third-party services and ensure operational resilience.

Future Outlook and Strategic Considerations: Looking forward, Crowd strike and other cyber security providers must prioritize reliability, scalability, and transparency in their service offerings. Regulatory scrutiny and customer expectations will likely drive stricter compliance requirements and service level agreements (SLAs). Strengthening partnerships with clients and fostering a culture of transparency and accountability will be essential for rebuilding trust and resilience in the aftermath of such incidents.

2. CONCLUSION

In conclusion, the Crowd Strike outage on July 19, 2024, is an important case study for understanding the weaknesses and strengths of modern cyber security systems. By examining the causes, impacts, and responses to this incident, the paper aims to help develop better cyber security practices and policies, ensuring better preparation for future threats. The insights from this analysis are meant to guide both cyber security professionals and policymakers in improving global cyber security.

The service disruption experienced by Crowd strike on July 19, 2024, serves as a critical reminder of the vulnerabilities inherent in cyber security ecosystems. By analyzing the incident's causes, impacts, and lessons learned, this paper highlights the importance of robust cyber security strategies, contingency planning, and collaborative efforts between organizations and service providers. Moving forward, proactive measures and a commitment to continuous improvement will be essential in mitigating future risks and ensuring the resilience of cyber security infrastructures.

3. REFERENCES

[1] Crowdstrike official website
[2] Industry reports and analysis on cybersecurity trends
[3] Academic papers and journals on AI/ML in cybersecurity
[4] Books and guides on cybersecurity best practices