WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comparative Analysis Of Microsoft & Crowdstrike Outages : Cloud Security Crisis & cybersecurity Risks

Mahi Parashar

IPS business school

ABSTRACT -

This research examines the recent cloud security outages and cybersecurity risks experienced by Microsoft and CrowdStrike, highlighting the consequences of faulty updates on cloud services. This research conduct a comparative analysis of the two incidents, exploring the root causes, impact, and recovery efforts. This research reveals that the CrowdStrike outage was caused by a defective update, while Microsoft's Azure services (cloud computing platform developed by Microsoft) and Microsoft 365 (productivity tools and services) suite were affected by a separate issue. This study disclose the challenges of implementing fixes, including manual intervention and encryption complexities. This study provides insights into the importance of robust update testing, effective communication, and proactive cybersecurity measures to mitigate the risk of cloud service disruptions. This research goes to findings have significant implications for cloud service providers, cybersecurity professionals, and organizations reliant on cloud-based services.

Keywords: cloud service outage , faulty updates, cloud security, Microsoft, CrowdStrike, cybersecurity .

Introduction –

Microsoft experienced a global outage due to issues with crowdstrike's **Falcon Sensor Software** , causing widespread disruption and triggering the **Blue Screen Of Death onWindows.**

The increasing reliance on cloud services has transformed the way organizations operate, communicate, and store data. However, this shift has also introduced new vulnerabilities and risks, particularly in the realm of cybersecurity. Recent high-profile outages affecting Microsoft and CrowdStrike have highlighted the devastating consequences of faulty updates on cloud services, compromising the security and availability of critical data.

The Microsoft outage, which impacted Azure services and Microsoft 365 suite in the central U.S. region, demonstrated the far-reaching effects of a single-point failure in the cloud.

Simultaneously, CrowdStrike's defective update issue exposed the fragility of even the most robust cybersecurity systems. The impact of these outage was felt across various industries and millions like airlines, banks , media outlets , financial institution. Moreover this impact had a significant on customers and faced the loss of productivity and revenue , compromised personal data , decreased trust in cloud service and measures the cybersecurity.

This research delves into the complexities of cloud security, examining the root causes and consequences of these outages. By exploring the intersection of technology, human error, and cybersecurity, we aim to identify key takeaways and best practices for mitigating the risk of cloud service disruptions.

Through a comparative analysis of the Microsoft and CrowdStrike incidents, this research seeks to:

1. Investigate the technical and human factors contributing to the outages
2. Analyze the impact on customers, businesses, and the broader cybersecurity landscape
3. Evaluate the effectiveness of recovery efforts and communication strategies
4. Provide recommendations for cloud service providers, cybersecurity professionals, andorganizations to enhance their cloud security posture

By exploring these critical issues, this research aims to contribute to the ongoing conversation on cloud security, ultimately informing strategies for a more resilient and secure cloud computing environment.

Problem Statement –

Microsoft shut down Windows Server, Azure service, and Microsoft 365 in july 2024. This problem was caused by a software from CrowdStrike, which was named Falcon Sensor. And one reason was that crowdstrike's updated all the systems simultaneously. This research identifies the problem of single-point failures in cloud services and software updates, specifically the faulty update released by CrowdStrike, which caused global IT outages and compromised the cybersecurity of many critical systems around the world.

The Discription Of The Case –

The failure problem of Crowdstrike outage and global software's single-point
The cause of faulty update on cloud service's & software update issued by CrowdStrike, a major cybersecurity firm, triggered a significant IT outage that impacted numerous critical systems worldwide. CrowdStrike's routine update the update, designed to bolster defenses against cyber threats, was released without adequate testing. Faulty code within the Falcon sensor software, compatible with Microsoft Windows, is blamed for the disruptions, the code that caused this disruption was **kernel-level code,** impacting every computer hardware and software communication aspect.
And the second, Crowdstrike was doing to rolling out its updates software to everyone at once. And according to IT industry this a single-point failure or error in one part of a system that creates a technical disaster across industries, functions, and interconnected communications networks whosoever effected a massive domino.

- **Impact on cybersecurity** - The CrowdStrike outage highlights the vulnerability of even the most robust cybersecurity systems to single-point failures.The faulty update compromised thedefenses of numerous critical systems worldwide, leaving them exposed to cyber threats.
- **Hacking & data security** -The CrowdStrike outage created an opportunity for hackers to exploitthe vulnerability, potentially leading to data breaches and other cyber attacks.The outage compromised the security of sensitive data, potentially leading to data breaches and unauthorized access.and the additional impacts of incident is The CrowdStrike outage had a ripple effect across industries, functions, and interconnected communications networks, highlighting the interconnectedness of modern systems.
- **Impact on universe** - Banking, telecom, retail stores, courier, shipping, traffic, education and medical services were also affected in many countries.Flight cancellations and delays , airlines worked to recover from a global IT outage sparked chaos at airports and for other industries a day earlier.On the day more than 5,000 flights were canceled worldwide, with about 3,400 in the
  U.S. Nearly 13,000 U.S. flights were delayed. The next day of incident More than 2,800 flights were canceled with over 2,100 of them in the United States, More than 8,600 U.S. flights were delayed. (The data was taken flight-tracking site FlightAware). A glitch in CrowdStrike's software update caused major disruptions to Microsoft systems for businesses around the world.
- **Impact on financial stock-** CrowdStrike not only provides security software to industries, but also investigates hacks and tracks hackers.CrowdStrike stock - the disruption caused a drop in CrowdStrike's share price globally, falling by $42.22, or more than 12%, to just over $300 in trading after the incident.

Microsoft also faced problems with its Azure and Microsoft 365 products, resulting in its stock falling more than 1%. In contrast, other startups like Alto, Palo, and Fortinet have seen profitable .CrowdStrike is facing its worst week since November 2022 due to a major IT outage
that has affected businesses around the world. Shares fell 9% after the incident, totaling a decline of about 16% for the week. Despite this setback, CrowdStrike stock remains up 22.5% for 2024.

What microsoft do after this incident (Solutions)-

CrowdStrike not only provides security software to industries but also investigates hacking and tracks hackers Microsoft Corp. and CrowdStrike implemented fixes and the system was gradually restored.
Microsoft's providing a latest tool for creates a bootable USB drive that IT administrators can use to quickly repair an affected machine and a disk is protected by BitLocker encryption, the tool will prompt for a BitLocker recovery key and then continue fixing the CrowdStrike update. In additionally Also crowdstrike's focus should be on software so that updates can be released incrementally.

Suggestion -

1. Software should be updates rolled out incrementally
2. build redundancy into IT systems
3. software should have been tested in sandboxes in multiple environments before going out
4. use the SSDF (secure software development framework) with a set of protocols provide by the Government (US) already. SSDF provide the guidelines for secure and development of software . Also SSDF indicating to the companies should be prepared to adopt & implementing similar protocols to ensure the security and mitigate the risk of software .
5. Make a plan for protect against the issues of single point failure risk management andimplement the plan also covering the issues and risk .
6. Maintain the software or Software Maintenance - Software maintenance is the process of modifying and updating software to ensure it continues to meet the changing needs of its usersand to fix any issues that may arise.
7. minimize the downtime of backup systems.
8. Continuously monitor and assess the effectiveness of risk management strategy and makeadjustment as needed.
9. Consider implementing DevOps practice such as continuous integrations and delivery to improve software development and deployment process.

Conclusion -

The CrowdStrike outage highlights the vulnerability of global cybersecurity systems to single- point failures. This incident highlights the need for robust testing, quality assurance, and redundancy measures to prevent and mitigate such outages. The consequences of similar incidents can be serious, including financial losses, reputational damage, and compromised cybersecurity. To address these challenges, organizations need to prioritize

1. Rigorous testing and quality assurance
2. Incremental Updates and Redundancy Measures
3. Disaster Recovery Planning and Communications
4. Collaboration and information sharing
5. Continuous monitoring and improvement

By adopting the best practices, organizations can reduce the risk of similar incidents and protect their customers, reputation, and profits. The CrowdStrike outage serves as a wake-up call for theindustry to prioritize cybersecurity resiliency and preparedness.