SECURITY ADVISORY

CYBER STASH

July, 2024

CrowdStrike Fallout

Mitigating Social Media Risks

Context

In recent days, an incident involving CrowdStrike's Falcon platform has ignited a flurry of posts across social media platforms. Reports of Windows hosts encountering blue screen errors following a flawed content update have highlighted a critical cybersecurity concern often underestimated: the inadvertent exposure of organizational vulnerabilities through social media.

The outcry on platforms like LinkedIn and Facebook inadvertently disclosed users' reliance on CrowdStrike for endpoint security. Beyond immediate operational disruptions, this exposure introduces a subtler yet significant risk: targeted attacks. Adversaries proficient in reconnaissance capitalize on such disclosures to gather intelligence on potential targets. This intelligence can inform the development of customized endpoint exploits meticulously crafted to evade or compromise CrowdStrike's defenses.

Compounding this emerging incident is attacks from malicious actors who are mimicking CrowdStrike's official site, disseminating counterfeit code and instructions under the guise of assisting entities affected by the outage. In responding to this incident, it's crucial for organizations to mitigate risks stemming from social media exposure, while also remaining vigilant against fraudulent attempts to exploit the situation for malicious purposes.

Mitigation

Organizations must proactively manage the aftermath of such incidents by Managing Social Media Exposure:

Delete Social Media Posts: Employees who have disclosed sensitive information inadvertently should be urged to promptly delete their posts.

Educate Employees: Raise awareness among employees about the inadvertent disclosure of cybersecurity measures on social media platforms. Establish clear guidelines on what can and cannot be shared regarding organizational IT infrastructure and security solutions.

Monitor and Mitigate: Regularly monitor social media channels for mentions of company-specific IT systems and take appropriate action to mitigate exposure.

Enhancing Disaster Recovery and Business Continuity

In light of incidents that cause widespread impact:

Independence and Redundancy: Ensure independence between primary and secondary systems. This includes hosting critical applications on diverse infrastructure and employing different operating systems, security tooling, and update schedules.

Backup Strategy: Develop a comprehensive backup strategy that accounts for diverse scenarios, including cyber incidents, ensuring quick restoration of operations without compromising security.

Diverse Communication Channels: Ensure redundancy in communication channels used to provide recovery guidelines. This includes utilizing multiple platforms such as email, SMS, and dedicated internal communication tools to reach employees and stakeholders.

Preparedness and Testing: Regularly test the effectiveness of alternative communication methods in simulated scenarios to ensure they can be activated swiftly during an actual incident.

Documentation and Accessibility: Maintain comprehensive documentation of recovery procedures and ensure they are accessible offline or through alternative means if primary access is disrupted.

Employee Training and Awareness: Educate employees on how to access recovery guidelines through different channels and emphasize the importance of following established protocols even in challenging communication scenarios.

Exercise Caution: Avoid accessing unofficial or suspicious websites claiming to offer fixes or solutions related to the CrowdStrike incident.

Official Sources Only: Obtain technical information, updates, and remediation guidance exclusively from CrowdStrike's verified communication channels, such as their official website and Customer Portal.

Enhance Cybersecurity Awareness: Educate employees and stakeholders about the risks of engaging with unauthorized sources during technical incidents, emphasizing the importance of verifying information before taking action.

References

- https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/
- https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/widespread-outages-relating-crowdstrike-software-update
- https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.