CrowdStrike Outage: A Wake-Up Call for the IT Industry

I've seen my fair share of challenges and innovations in my three decades in the IT sector. However, the recent global IT outage caused by a software update from the New York Stock Exchange listed, CrowdStrike, was unprecedented. This incident, which disrupted national infrastructure, healthcare services, and parts of the travel infrastructure, is typically associated with cybersecurity attacks or hacks, not routine software updates.

Tim Walker, MD, Aura Technology

The Unfolding of an Unusual Event

It's rare for such a large, well-established company to release a software update that caused such widespread disruption. Most organisations of CrowdStrike's size have stringent processes to test updates before deployment, ensuring they don't cause significant issues. The CEO quickly clarified that it was not a security hack but an internal error. Unfortunately, this explanation might further damage the firm's credibility, highlighting a significant lapse in its internal processes.

The Magnitude of the Impact

The scale of the incident was enormous. Updates are a necessary evil, primarily aimed at plugging security holes, or enhancing features, but careful deployment is essential. While individual customers may not have been directly affected, businesses and government infrastructures bore the brunt of the outage. It included travellers, stock market users, and healthcare services like the NHS app.

For many, updates are a source of frustration. They can disrupt workflows and cause temporary inconveniences. However, in this case, the consequences were far more severe. The outage affected critical services, highlighting the interconnected nature of modern infrastructure and the potential ripple effects of IT failures. Microsoft confirmed that over 8.5 million devices were impacted globally.

The Response and Recovery

CrowdStrike acted swiftly to release an update to fix the bug they created. Most infrastructures applied the update, and systems gradually returned online. However, some systems may have taken longer to recover due to internal configuration issues. By the first Monday after the event, most organisations using CrowdStrike were operational again. However, this incident has likely prompted many businesses to reconsider their IT service providers and the products they use for security.

Lessons Learned and Moving Forward

This incident is a stark reminder of the importance of robust testing and quality assurance processes. Consulting with a reputable IT service provider is crucial for businesses that still may be experiencing issues as a knock-on effect of the disruption. Managing IT internally can be limiting; external experts can provide the necessary support to navigate such crises.

Moreover, the event underscores the need for continuous improvement in IT practices. Companies such as CrowdStrike must invest in better testing protocols and ensure that updates are thoroughly vetted for use on operating systems such as Microsoft's before deployment. The goal should be to minimise the risk of such widespread disruptions in the future, and to quickly remediate/roll back in the event of an issue.

Conclusion

The CrowdStrike outage was a wake-up call for the IT industry. It highlights the vulnerabilities in our interconnected world and the critical role that IT plays in maintaining the smooth functioning of essential services. As we move forward, companies must learn from this incident and take proactive steps to prevent similar occurrences. The stakes are high, and the cost of failure is too great to ignore.

Contact Aura Technology
auratechnology.com
03333 208 601
tim.walker@auratechnology.com