View on Web

Global IT Outage - How do We Pivot from Chaos to Control

26th Jul,2024

In an increasingly interconnected digital world, a single point of failure can trigger a cascade of disruptions across the globe. We realized this recently when an innocuous software update by **cybersecurity** giant CrowdStrike inadvertently brought 8.5 million Windows devices to their knees, causing widespread chaos across various sectors. Airlines grounded flights, broadcasters went off air, and critical services like healthcare and banking faced severe disruptions. The infamous ‘Blue Screen of Death (BSOD)’ became a shared experience for millions, highlighting our deep dependence on digital infrastructure.

How can we prevent future IT outages?

In the wake of the CrowdStrike incident that brought millions of systems to a standstill, the cybersecurity landscape finds itself at a crossroads. How do we balance robust protection with system stability?

1. **Embrace the Power of AI and Machine Learning (ML):** Leveraging **AI** and ML can predict and identify potential vulnerabilities before they're exploited, detect anomalies in real-time, allowing for swift responses to emerging threat and automate incident response, thereby reducing human error and response time.
2. **Decentralize with Blockchain Technology:** **Blockchain** technology can help distribute data across multiple nodes, making it harder for attackers to compromise entire systems. What's more, implementing immutable audit trails, makes it easier to track and respond to security incidents. By moving away from centralized systems, we can create a more resilient digital ecosystem that's harder to take down with a single strike.
3. **Zero Trust Architecture:** Trust No One, Verify Everything: The traditional perimeter-based security model is no longer sufficient. Zero Trust Architecture (ZTA) offers a more robust approach. Under this approach, enterprises can verify every user, device, and application attempting to access resources, implement micro-segmentation to limit the impact of potential breaches and continuously monitor and adapt access privileges based on behavior and context.
4. **Collaborative Threat Intelligence Networks:** Cybersecurity shouldn't be a solitary effort. A synergy among organizations, industries, and even nations is needed for sharing real-time threat intelligence to improve collective defense, pooling resources for more effective R&D and creating standardized response protocols for global incidents.

How CSM Tech wards off IT outages with a smart pivot

At CSM Tech, we take to out-of-the-box thinking when it comes to troubleshooting. Our ingenuity in choosing products different from others has fortified our cyber defenses. We chose not to incorporate products that claim to work on the kernel level to secure the environment. Rather, we go with those who work on the user space. By operating in the user space, solutions like CYQER (Cyber Yield Quantification for Enterprises and Reporting) dramatically reduces the risk of critical system failures like BSOD. This clever positioning allows for robust security monitoring without the potential for system-wide destabilization. By leveraging standard kernel APIs, it maintains a harmonious relationship with the operating system.

The other key takeaway is that we shun the practice of allowing automatic updates. Instead, we allow updates only after approving them. Moreover, as an organization, we subscribe to the view that any third party security system should not be permitted to interact with kernel. Also, our patch update must be well tested in simulation environment as well as real systems.

The recent global IT outage serves as a wake-up call, reminding us of the brittleness and fragility of our digital ecosystem. In a world where the next global IT outage seems to be lurking around the corner, we must level up our incident response to future-proof our digital economy. It’s stability over agility.

AUTHOR:

Jayajit Dash

Senior Manager- Corporate Communications (Marketing)