CrowdStrike Incident

August 7, 2024

On Friday, July 19, 2024, the world experienced the largest global IT outage in history – 8.5 million Windows devices encountered an error screen known as the “blue screen of death”. This affected companies ranging from banks to airlines to hospitals. What happened? Let’s examine to see what we can learn.

Who is CrowdStrike

At the heart of the outage is a cybersecurity vendor called CrowdStrike. They develop software to help companies detect and block hacks. CrowdStrike is known as an “endpoint” security firm – they remotely connect to their client’s laptops or mobile devices (endpoint) to apply cyber protections. Many companies use and install their software on their machines, across their organization.

What happened?

Before updates are applied, best practice is to perform a patch “sandbox test”. This is where an update is applied in a safe, environment to observe, analyze and ensure everything still functions as expected. If all goes well, then proceed with applying the update to production. CrowdStrike skipped the patch testing step and applied the full update in production.

Their software requires deep access to a computer operating systems (OS) to scan for threats. In this case, machine’s running Microsoft’s Windows OS crashed due to an issue in the way a software update issued by CrowdStrike, interacted with Windows. Because of their cybersecurity footprint, once the update was applied, this caused a global outage.

What can we learn?

This event is an opportunity to reflect on what organizations should be doing to improve resilience. McLennan Community College (MCC) has plans to review these areas, as part of our Cybersecurity Roadmap.

Response

This event demonstrates the need for every organization to have a robust incident response plan in place – a set of instructions on how to respond and recover systems in this type of incident. Organizations should evaluate the effectiveness of their response plans to determine any gaps.

Plans should be reviewed regularly and tested to minimize the impact to recover quickly.

Business Contingency Plan (BCP)

After an incident such as this, many organizations engage in implementing business continuity plans (BCPs) – help organizations recover and restore mission-critical functions in events. Organizations frequently experience challenges in this area during a ransomware event, with no plan to rebuild the resources to support mission-critical functions. To prepare, organizations should conduct a business impact analysis (BIA) and integrate the information into BCPs, reducing the risk of prolonged business disruption.

Single Point of Failure (SPOF)

CrowdStrike was the single point of failure (SPOF) in this incident – a design flaw in the system, that poses potential risk. SPOF could lead to a situation where just one error or malfunction causes the whole system to stop working. To avoid this, ideally, if a system fails, another should be in place to immediately take its place – adding redundancy (duplicate system). A redundancy should exist anywhere a SPOF currently exists.

Software Supply Chain

The scale of this event has highlighted the risks of cyber events affecting supply chains more than any event in recent history. With financial transactions stalled and hospitals unable to provide care, we cannot blindly accept updates from software impacting key systems. Organizations should consider and plan for incidents like this and have negative consequences on their supply chains as part of their BCP.

For organizations lucky enough to avoid any adverse impact from this event, it's crucial to recognize this could have happened to any organization just as easily. It is better to be prepared than to be lucky.

Revision #1
Created 12 December 2024 18:55:50 by Laura J. Crapps
Updated 12 December 2024 18:56:57 by Laura J. Crapps