One small update brought down millions of IT systems around the world—it's a timely warning

July 22 2024, by David Tuffley

Credit: Gerd Altmann/Pixabay

This weekend's global IT outage caused by a software update gone wrong highlights the interconnected and often fragile nature of modern IT infrastructure. It demonstrates how a single point of failure can have far-reaching consequences.

The outage was linked to a single update automatically rolled out to

[Crowdstrike Falcon](#), a ubiquitous cyber security tool used primarily by large organizations. This caused Microsoft Windows computers around the world to crash.

CrowdStrike has since fixed the problem on their end. While many organizations have been able to resume work now, it will take some time for IT teams to fully repair all the affected systems—some of that work has to be done manually.

How could this happen?

Many organizations rely on the same cloud providers and cyber security solutions. The result is a form of digital monoculture.

While this standardization means computer systems can run efficiently and are widely compatible, it also means [a problem can cascade](#) across many industries and geographies. As we've now seen in the case of CrowdStrike, it can even cascade around the entire globe.

Modern IT infrastructure is highly interconnected and interdependent. If one component fails, it can lead to a situation where the failed component triggers a [chain reaction](#) that impacts other parts of the system.

As software and the networks they operate in becomes more complex, the potential for unforeseen interactions and bugs increases. A minor update can have unintended consequences and spread rapidly throughout the network.

As we have now seen, entire systems can be brought to a grinding halt before the overseers can react to prevent it.

How was Microsoft involved?

When Windows computers everywhere started to crash with a "blue screen of death" message, early reports stated the IT [outage](#) was caused by Microsoft.

In fact, [Microsoft confirmed](#) it experienced a cloud services outage in the Central United States region, which began around 6pm Eastern Time on Thursday, July 18 2024.

This outage affected a subset of customers using various Azure services. [Azure](#) is Microsoft's proprietary cloud services platform.

The Azure outage had far-reaching consequences, disrupting services across multiple sectors, including [airlines](#), [retail](#), banking and media. Not only in the United States but also internationally in countries like Australia and New Zealand. It also impacted various Microsoft 365 services, including PowerBI, Microsoft Fabric and Teams.

As it has now turned out, the entire Azure outage could also be [traced back to the CrowdStrike update](#). In this case it was affecting Microsoft's virtual machines running Windows with Falcon installed.

What can we learn from this episode?

Don't put all your IT eggs in one basket.

Companies should use a multi-cloud strategy: distributing their IT infrastructure across multiple cloud service providers. This way, if one provider goes down, [the others can continue](#) to support critical operations.

Companies can also ensure their business continues to operate by building in redundancies into IT systems. If one component goes down, others can step up. This includes having backup servers, alternative data centers, and "failover" mechanisms that can quickly switch to backup systems in the event of an outage.

Automating routine IT processes can reduce the risk of human error, which is a common cause of outages. Automated systems can also monitor for potential issues and address them before they lead to significant problems.

Training staff on how to respond when outages occur can manage a difficult situation back to normal. This includes knowing who to contact, what steps to take, and how to use alternative workflows.

How bad could an IT outage get?

It's highly unlikely the world's entire internet could ever go down due to the distributed and decentralized nature of the internet's infrastructure. It has multiple redundant paths and systems. If one part fails, traffic can be rerouted through other networks.

However, the potential for even larger and more widespread disruptions than the CrowdStrike outage does exist.

The catalog of possible causes reads like the script of a disaster movie. Intense solar flares, similar to the Carrington Event of 1859 could cause widespread damage to satellites, power grids, and undersea cables that are the backbone of the internet. Such an event could lead to internet outages spanning continents and lasting for months.

The global internet relies heavily on a network of undersea fiber optic cables. Simultaneous damage to multiple key cables—whether through

natural disasters, seismic events, accidents, or deliberate sabotage—could cause major disruptions to international internet traffic.

Sophisticated, coordinated cyber attacks targeting critical internet infrastructure, such as root DNS servers or major internet exchange points, could also cause large-scale outages.

While a complete internet apocalypse is highly unlikely, the interconnected nature of our digital world means any large outage will have far-reaching impacts, because it disrupts the online services we've grown to depend upon.

Continual adaptation and preparedness are vitally important to ensure the resilience of our global communications infrastructure.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: One small update brought down millions of IT systems around the world—it's a timely warning (2024, July 22) retrieved 22 July 2024 from https://techxplore.com/news/2024-07-small-brought-millions-world.html