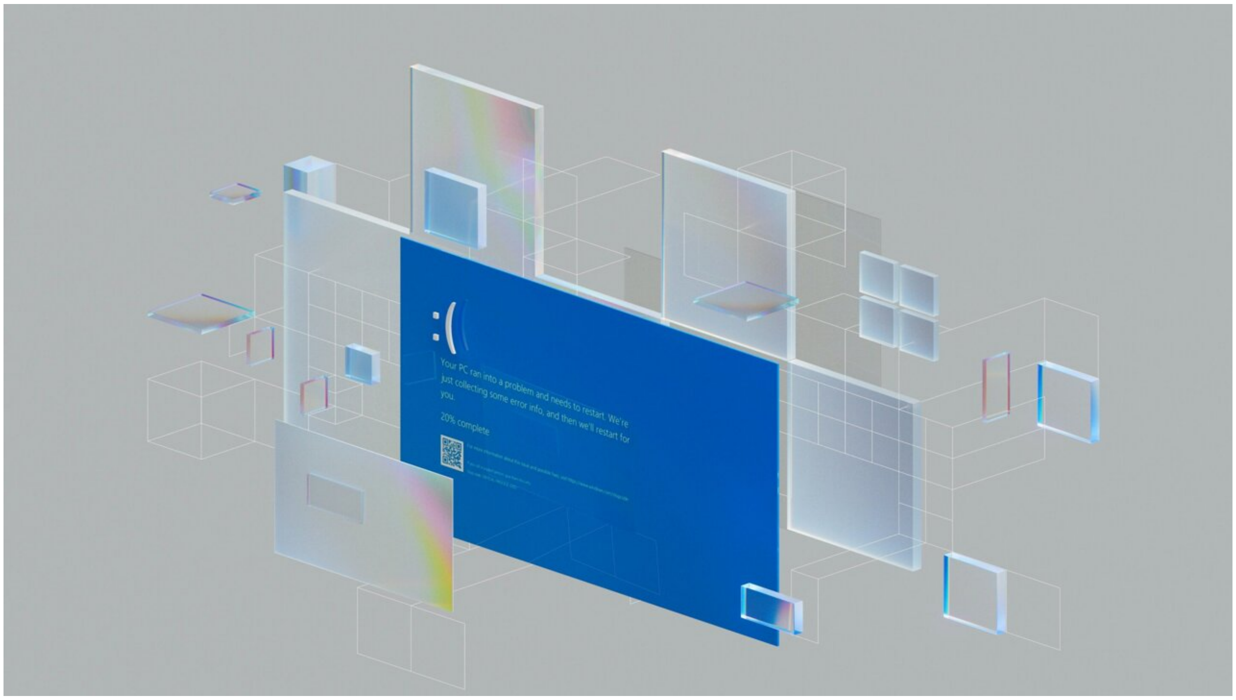
TechXplore

CrowdStrike's cyber blunder could be warning of worse to come, say experts

July 29 2024, by Michael E. Kanell and Drew Kann, The Atlanta Journal-Constitution


:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
20% complete

Credit: Unsplash/CC0 Public Domain

Our laptops, desktops and phones, our businesses, data, emails, our access to internet information and services—really, anything digital that traverses cyberspace and passes through a computer server—are all dependent on support and protection from security companies whose staffing and software are sometimes imperfect.

Not much you can do to change that.

Bad actors are out there—smart, devious and often hidden far from the reach of your local law enforcement, said Jon Powell, cybersecurity expert and partner at Atlanta-based accounting firm Moore Colson.

"It is unfortunately just the world we live in," he said. "I don't need to be next door to you to rob you."

That means all companies need digital gatekeepers, the way a modern power plant needs guards. So, companies—and their employees—depend on software supplied by specialists like CrowdStrike, an Austin-based firm that has become a world leader in protecting company servers from hacking, theft, manipulation and other cyber disruption.

But the gatekeeper can goof, too.

The guard at the plant gate can fall asleep, get fooled or overpowered by an intruder. Or—as seems to have happened with CrowdStrike earlier this month—stumble unintentionally while making his rounds, perhaps cutting off electricity and sending much of the city into darkness.

With a company like CrowdStrike, a misstep can make for a global problem, which is what happened in the early hours of July 19 at servers around the world when CrowdStrike apparently sent out a faulty software update to many users of Microsoft systems.

It was a very big deal, causing inconvenience and costing billions, but it could have been so much worse.

Airline scheduling was disrupted, particularly for Delta Air Lines, and many thousands of passengers stranded, but no in-air passengers were imperiled. Some hospitals lost access to computer systems and canceled non-urgent surgeries.

Many supermarkets and other businesses lost their transaction systems, so customers couldn't pay for items. Some logistics companies had to delay delivery of some packages, but none of the impact was lethal.

In many ways, our tech systems are chains and we depend on all the links, said Zarik Megerdichian, CEO of Loop8, a California-based company that sells personal privacy controls for software.

"This event serves as a warning for the problems a single point of failure can cause," he said. "We learned that businesses are only as secure as their weakest link and even the big players we all know and trust are vulnerable. In many ways, companies got off easy."

At Georgia Power, for example, the CrowdStrike outage didn't disrupt electricity service for its 2.7 million customers, even though the company's online support and account access functions were impaired. Those services were restored by Monday, though the aftereffects of the technology meltdown bled into the early part of this week.

Mondays are always busy for the utility, but a Georgia Power spokesman said it was experiencing higher than normal call volumes to start the week. The crush of calls was likely because customers were temporarily unable to address issues or schedule service through the company's online portals on July 19, the spokesman said.

Due to the issues and backlog, Georgia Power paused electricity service disconnections for several days. As of Wednesday, the company had resumed disconnecting customers for nonpayment of bills.

However, those kinds of tech troubles might just be foreshadowing.

There's reason to fear that next time, the shutdown systems, inaccessible records and off-line computers could be mortal threats and not just inconveniences, said Aleksandar Tomic, associate dean, strategy, innovation, and technology at Boston College.

"It gives you an idea of what warfare of the future would be like," he said. "If we went into a conflict with Russia, this is a picture of what it might be like. We were lucky this time that no vital systems were affected, like water."

Citation: CrowdStrike's cyber blunder could be warning of worse to come, say experts (2024, July 29) retrieved 29 July 2024 from https://techxplore.com/news/2024-07-crowdstrike-cyber-blunder-worse-experts.html