Risk-averse organizations chose CrowdStrike for cybersecurity. Now its software is causing chaos

July 19 2024, by Matt O'brien

A Crowdstrike office is shown in Sunnyvale, Calif., on Friday, July 19, 2024. An overnight outage was blamed on a software update that cybersecurity firm CrowdStrike sent to Microsoft computers of its corporate customers including many airlines. Credit: AP Photo/Haven Daley

Airlines, banks, hospitals and other risk-averse organizations around the world chose cybersecurity company CrowdStrike to protect their computer systems from hackers and data breaches.

But all it took was one faulty CrowdStrike software update to cause global disruptions Friday that grounded flights, knocked banks and media outlets offline, and disrupted hospitals, retailers and other services.

"This is a function of the very homogenous technology that goes into the backbone of all of our IT infrastructure," said Gregory Falco, an assistant professor of engineering at Cornell University. "What really causes this mess is that we rely on very few companies, and everybody uses the same folks, so everyone goes down at the same time."

The trouble with the update issued by CrowdStrike and affecting computers running Microsoft's Windows operating system was not a hacking incident or cyberattack, according to CrowdStrike, which apologized and said a fix was on the way.

But it wasn't an easy fix. It required "boots on the ground" to remediate, said Gartner analyst Eric Grenier.

"The fix is working, it's just a very manual process and there's no magic key to unlock it," Grenier said. "I think that is probably what companies are struggling with the most here."

While not everyone is a client of CrowdStrike and its platform known as Falcon, it is one of the leading cybersecurity providers, particularly in the transportation and banking sectors that have a lot at stake in keeping their computer systems working.

Delayed flight schedules are displayed on a screen at LaGuardia Airport in New York on Friday, July 19, 2024, after a faulty CrowdStrike update caused a major internet outage for computers running Microsoft Windows. Credit: AP Photo/Yuki Iwamura

"They're usually risk-averse organizations that don't want something that's crazy innovative, but that can work and also cover their butts when something goes wrong. That's what CrowdStrike is," Falco said. "And they're looking around at their colleagues in other sectors and saying, 'Oh, you know, this company also uses that, so I'm gonna need them, too.'"

Worrying about the fragility of a globally connected technology ecosystem is nothing new. It's what drove fears in the 1990s of a

technical glitch that could cause chaos at the turn of the millennium.

"This is basically what we were all worried about with Y2K, except it's actually happened this time," wrote Australian cybersecurity consultant Troy Hunt on the social platform X.

Across the world Friday, affected computers were showing the "blue screen of death"—a sign that something went wrong with Microsoft's Windows operating system.

But what's different now is "that these companies are even more entrenched," Falco said. "We like to think that we have a lot of players available. But at the end of the day, the biggest companies use all the same stuff."

Founded in 2011, CrowdStrike describes itself in its annual report to financial regulators as having "reinvented cybersecurity for the cloud era and transformed the way cybersecurity is delivered and experienced by customers." It emphasizes its use of artificial intelligence in helping to keep pace with adversaries.

The Austin, Texas-based firm is one of the more visible cybersecurity companies in the world and spends heavily on marketing, including Super Bowl ads. At cybersecurity conferences, it's known for large booths displaying massive action-figure statues representing different state-sponsored hacking groups that CrowdStrike technology promises to defend against.

Porter Passengers wait at Toronto Pearson Airport on Friday, July 19, 2024, after a faulty CrowdStrike update affected computers running Microsoft Windows, causing a major internet outage. Credit: Chris Young/The Canadian Press via AP

CrowdStrike CEO George Kurtz is among the most highly compensated in the world, recording more than $230 million in total compensation in the last three years. Kurtz is also a driver for a CrowdStrike-sponsored car racing team.

After his initial statement about the problem was criticized for lack of contrition, Kurtz apologized in a later social media post Friday and on NBC's "Today Show."

"We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption," he said on X.

Richard Stiennon, a cybersecurity industry analyst, said this was a historic mistake by CrowdStrike.

"This is easily the worst faux pas, technical faux pas or glitch of any security software provider ever," said Stiennon, who has tracked the cybersecurity industry for 24 years.

While the problem is an easy technical fix, he said, it's impact could be long lasting for some organizations. "It's really, really difficult to touch millions of machines. And people are on vacation right now, so, you know, the CEO will be coming back from his trip to the Bahamas in a couple of weeks and he won't be able to use his computers."

Stiennon said he did not think the outage revealed a bigger problem with the cybersecurity industry or Crowdstrike as a company.

"The markets are going to forgive them, the customers are going to forgive them, and this will blow over," he said.

Citation: Risk-averse organizations chose CrowdStrike for cybersecurity. Now its software is causing chaos (2024, July 19) retrieved 19 July 2024 from https://techxplore.com/news/2024-07-averse-chose-crowdstrike-cybersecurity-software.html