Future cybersecurity incidents are almost a certainty, asserts US policy arm of global computing society

August 26 2024

Credit: Pixabay/CC0 Public Domain

The Association for Computing Machinery's US Technology Policy Committee (USTPC) has released a "Statement on Mass Cybersecurity

Incidents Likely to Recur." On July 18, 2024, CrowdStrike, a US-based cybersecurity technology company, released a sensor configuration update which caused a global outage affecting an estimated 8.5 million computers. Several critical infrastructure sectors including airlines, 911 emergency systems, banks, government agencies, health care, and hospitals around the world were impacted.

While CrowdStrike has provided some information as to how the accident happened, ACM USTPC urges that all the details be thoroughly and publicly investigated so that system operators, technologists, and policymakers can take steps to guard against such accidents in the future.

"The CrowdStrike incident underscored weaknesses in two kinds of infrastructures," explains Jody Westby, CEO, Global Cyber Risk LLC and a principal author of the new USTPC Statement.

"On one level, we realized that the global technical infrastructure is fragile. Despite the fact that the latest technologies had been deployed to protect these systems, a major outage still occurred. At the same time, we also realized that our existing legal and policy infrastructure is insufficient to respond to these kinds of attacks. A great deal of work needs to be done to shore up both of these kinds of infrastructures, and we hope this USTPC Statement will bring attention to these critical needs."

The USTPC Statement also notes that "…the global nature of the outage highlights the need for improved international cooperation and coordination. The ability of companies globally to obtain information about the outage, government efforts, and technical guidance was largely deficient, and each country and company was on its own—particularly if their systems were down."

"The scale of the CrowdStrike accident was certainly unprecedented,

and its reach into critical infrastructures was alarming on many levels," added Carl Landwehr, visiting professor at the University of Michigan, and a principal author of the ACM Statement.

"But to computer scientists familiar with the underlying technology, this accident is not especially surprising, and future incidents are, unfortunately, almost a certainty. We need to learn more about how this happened to mitigate any potential repeat of this disaster. As a non-partisan organization of computer scientists who advise government leaders on technology policy, we have outlined eight key questions that should form the basis of a public investigation."

In surveying what they know about the CrowdStrike incident, the ACM experts noted that while the update caused thousands of Microsoft Windows-based systems to crash, systems based on Linux, Mac OS, and other operating systems were unaffected.

The core questions posed in the USTPC Statement include:

- How did some systems avoid the consequences of this error, while others did not?
- Why was the errant software released without thorough testing?
- What lessons can we draw concerning the architecture and implementation of systems?
- What best practices should be followed for automatic system updates?
- Why were some systems able to come back up faster than others?
- What were the most efficient ways to restart systems that required manual intervention?
- What notification should be required?

In suggesting next steps, the USTPC members urged that the public investigation of the CrowdStrike incident should be undertaken by the

US government's Cyber Safety Review Board (CSRB).

In addition to principal authors Carl Landwehr and Jody Westby, USTPC members Andrew Grosso, Jim Hendler, Jeanna Matthews, Stuart Shapiro, Gene Spafford, and Alec Yasinsac provided comments during the development of the Statement.

More information: The full USTPC Statement may be accessed here.

Provided by Association for Computing Machinery

Citation: Future cybersecurity incidents are almost a certainty, asserts US policy arm of global computing society (2024, August 26) retrieved 28 August 2024 from https://techxplore.com/news/2024-08-future-cybersecurity-incidents-certainty-asserts.html