Massive IT outage spotlights major vulnerabilities in the global information ecosystem

July 22 2024, by Richard Forno

Credit: Pixabay/CC0 Public Domain

The global information technology outage on July 19, 2024, that paralyzed organizations ranging from airlines to hospitals and even the

delivery of uniforms for the Olympic Games represents a growing concern for cybersecurity professionals, businesses and governments.

The outage is emblematic of the way organizational networks, cloud computing services and the internet are interdependent, and the vulnerabilities this creates. In this case, a faulty automatic update to the widely used Falcon cybersecurity software from CrowdStrike caused PCs running Microsoft's Windows operating system to crash. Unfortunately, many servers and PCs need to be fixed manually, and many of the affected organizations have thousands of them spread around the world.

For Microsoft, the problem was made worse because the company released an update to its Azure cloud computing platform at roughly the same time as the CrowdStrike update. Microsoft, CrowdStrike and other companies like Amazon have issued technical work-arounds for customers willing to take matters into their own hands. But for the vast majority of global users, especially companies, this isn't going to be a quick fix.

Modern technology incidents, whether cyberattacks or technical problems, continue to paralyze the world in new and interesting ways. Massive incidents like the CrowdStrike update fault not only create chaos in the business world but disrupt global society itself. The economic losses resulting from such incidents—lost productivity, recovery, disruption to business and individual activities—are likely to be extremely high.

As a former cybersecurity professional and current security researcher, I believe that the world may finally be realizing that modern information-based society is based on a very fragile foundation.

The bigger picture

Interestingly, on June 11, 2024, a post on CrowdStrike's own blog seemed to predict this very situation—the global computing ecosystem compromised by one vendor's faulty technology—though they probably didn't expect that their product would be the cause.

Software supply chains have long been a serious cybersecurity concern and potential single point of failure. Companies like CrowdStrike, Microsoft, Apple and others have direct, trusted access into organizations' and individuals' computers. As a result, people have to trust that the companies are not only secure themselves, but that the products and updates they push out are well-tested and robust before they're applied to customers' systems. The SolarWinds incident of 2019, which involved hacking the software supply chain, may well be considered a preview of today's CrowdStrike incident.

CrowdStrike CEO George Kurtz said "this is not a security incident or cyberattack" and that "the issue has been identified, isolated and a fix has been deployed." While perhaps true from CrowdStrike's perspective—they were not hacked—it doesn't mean the effects of this incident won't create security problems for customers. It's quite possible that in the short term, organizations may disable some of their internet security devices to try and get ahead of the problem, but in doing so they may have opened themselves up to criminals penetrating their networks.

It's also likely that people will be targeted by various scams preying on user panic or ignorance regarding the issue. Overwhelmed users might either take offers of faux assistance that lead to identity theft, or throw away money on bogus solutions to this problem.

What to do

Organizations and users will need to wait until a fix is available or try to

recover on their own if they have the technical ability. After that, I believe there are several things to do and consider as the world recovers from this incident.

Companies will need to ensure that the products and services they use are trustworthy. This means doing due diligence on the vendors of such products for security and resilience. Large organizations typically test any product upgrades and updates before allowing them to be released to their internal users, but for some routine products like security tools, that may not happen.

Governments and companies alike will need to emphasize resilience in designing networks and systems. This means taking steps to avoid creating single points of failure in infrastructure, software and workflows that an adversary could target or a disaster could make worse. It also means knowing whether any of the products organizations depend on are themselves dependent on certain other products or infrastructures to function.

Organizations will need to renew their commitment to best practices in cybersecurity and general IT management. For example, having a robust backup system in place can make recovery from such incidents easier and minimize data loss. Ensuring appropriate policies, procedures, staffing and technical resources is essential.

Problems in the software supply chain like this make it difficult to follow the standard IT recommendation to always keep your systems patched and current. Unfortunately, the costs of not keeping systems regularly updated now have to be weighed against the risks of a situation like this happening again.

Provided by The Conversation