knox news.

OPINION *This piece expresses the views of its author(s), separate from those of this publication.*

CrowdStrike outage illustrates that effective cybersecurity is the sum of its parts

Bill Carroll Guest columnist

Published 6:08 a.m. ET Aug. 7, 2024 | **Updated 6:08 a.m. ET Aug. 7, 2024**

To most people, the word “cybersecurity” is an enigma, which can make understanding the recent CrowdStrike outage challenging. The takeaway is that a resilient cybersecurity posture cannot be had with a single tool or any silver bullet.

Here’s why: Imagine a house occupied by a family. It is ringed by a fence and guarded by a dog. The doors are solid wood, and the windows are made of double-paned glass. They have locks, and the doors have deadbolts. The automatic garage door requires a remote opener. There are also sensors on the doors and windows that will sound the alarm and alert you to an intruder. The alarm system will automatically alert the police department if triggered. Lastly, members of the family have been instructed not to open doors for strangers or open unexpected packages.

In corporate scenarios, cybersecurity is a combination of the fence (firewall) and dog (deterrent), unbroken windows (penetration tests), the locks (hardening permissions), the keys (strong passwords) and the garage door opener (access badge). The informed family is equivalent to employees who have gone through security awareness training. The alarm system component is what CrowdStrike and similar companies provide.

That alarm system is called managed detection and response, or MDR for short. The outage, according to CrowdStrike, was due to a defect in a software update rather than a security breach. The effect was immediate and led to widespread shutdowns for airlines, banks, health care organizations and more.

Time, money, productivity and stress

Outages, whether created from software issues or a malicious attack, can have the same negative outcome. Any loss of critical systems costs users and customers time, money and productivity and causes a great deal of stress.

This incident highlights the critical importance of having a well-run software development lifecycle, where new code is properly tested before it is pushed out on a global scale.

But effective cybersecurity is far more than good quality assurance. It's a mosaic of best practices, policies and procedures — and leading technologies and tools — all working together. It requires a holistic and programmatic approach: assessing the current environment, designing a customized program and protecting the organization.

What cybersecurity providers should do

In our view, the best defense against a disruption is to engage a trusted security partner who will create a layered strategy to provide multiple levels of protection by assessing the proper security needs for each "house," then designing the appropriate protection strategy. This could include installing a fence if you don't already have one, testing window locks and doors to validate their ability to deter intruders, verifying there are no broken windows, and making sure the alarm system is operational and monitored at all times.

More technically, cybersecurity providers should ensure that any updates or new implementations undergo rigorous testing before being deployed. This reduces the risk of defects that could lead to outages or security breaches. Furthermore, they should continuously monitor your systems; stay current on the latest trends and threats; and update policies and protocols as needed. It is your provider's job to manage change, mitigate risk and adapt with the terrain.

No single software or service offering alone is complete. Dropping an MDR solution into an environment without managing the entire plan and security strategy for the environment leads to mistakes and failures. Oversight by experts, in coordination with technology, remains critical. Invest in partners who go beyond point solutions: ones who can assess current state, gaps and objectives; design and implement critical components of that strategy; and provide continuous oversight and expertise to ensure security outcomes are achieved.

This is an incredibly fast-paced industry, where change and adaptation are constant. The best security partnerships drive improved security outcomes over time, regardless of what tools are

hot at any given moment. As the cybersecurity landscape continues to evolve, so too must our strategies.

Find the right security partner — because tools break.

Bill Carroll is CEO of Avertium, a Knoxville-based cybersecurity and compliance solutions company.