Rethinking security in the age of COVID-19

Agencies should begin preparing now for the next crisis and for looming budget constraints

Jim Richberg
Public-Sector Field CISO, Fortinet

ALTHOUGH AGENCIES ARE FOCUSED on telework security, they also need to think about what's over the next hill. They should be aware that sequestration is likely just around the corner. Given the mounting deficit due to the pandemic-related stimulus package, I believe flat will be the new up for agency budgets, and when IT allocations shrink, security is often deprioritized.

Now is the time to find smart ways to spend money. Agencies should look for multifunctional solutions, such as software-defined networking, and choose options that are intrinsically secure.

The AI revolution

Fortunately, we are on the cusp of a revolution driven by the intersection between the platform-based approach to cybersecurity and increasingly mature artificial intelligence. That convergence will tip the balance from attacker to defender.

Data-driven analytics (specifically machine learning) enable agencies to characterize normal activity, focus on abnormal activity in real time and parse whether it is innocuous, potentially harmful or malicious.

Attackers try and fail repeatedly before they succeed in penetrating a target, and they leave detectable traces. If intruders make it inside, they typically have to figure out where they are and fumble their way through mapping the network in search of crown jewels.

If an agency's IT platform takes full advantage of security policy-driven automation, everyone else can be inoculated while Patient 0 (to use a pandemic metaphor) is still being exposed. In addition, real-time visibility and granular control of a platform's components can enable zero trust and dynamic segmentation, allowing agencies to minimize the consequences of a successful penetration.

Assessing what worked — and what didn't

I was struck by the ease with which some federal agencies and their supporting contractors were able to deal with the challenge of migrating to telework at the onset of COVID-19 compared to others.

In the best cases, agencies that had capabilities such as next-generation firewalls and TIC-compliant policies could allow employees to download client software onto their remote devices, establish secure connections and resume work. In other cases, a lack of firewalls, bandwidth, or relevant IT or security policies made it labor-intensive to establish remote connectivity, and the resulting connections were unstable and slow.

Now is the time for those agencies to examine how many of the challenges were caused by the inherent limitations of legacy architectures and products that weren't designed to meet new use cases.

There are viable commercial solutions that address all these challenges. Agencies don't have to — and frankly shouldn't — reinvent the wheel in terms of technologies or best practices, especially when budgets shrink. ■

Jim Richberg is public-sector field chief information security officer at Fortinet.