David M. Nicol

In the Petri Dish: Cybersecurity Pushed to the Edge

As I write this column in the third week of March 2020, my university, in response to the COVID-19 pandemic, has spent the last week preparing to hold all of its classes online for the rest of the Spring 2020 semester. In the space of two weeks, it has become common practice for colleges and universities across the United States to move their classes from in person to online. I brought my son (and his friend whose parents live overseas) home from their college, and they will complete their semester online from our dining room table.

In the last week, the university put protocols and directives in place for employees to work from home whenever possible. I head an institute with 40 employees; our offices are now empty of people. Last week, I was on a video conference with U.S. government sponsors of one of my projects, and I saw a prompt pop up on my program manager's computer screen; working from home, he has to click on the prompt to prove that he is indeed working at his computer. He said he gets several of these every day. This is annoying, I'm sure, and a little demeaning.

At this particular instant, several countries are locked down, and many U.S. states, including my own, have declared shelter-in-place orders. For the foreseeable future, my university's business will be done almost exclusively over the Internet, as will the business of most organizations who can shift to that mode of operation.

When I am in the office on the university network, there are internal mechanisms in place that protect access to university servers and databases. The load on this infrastructure is well understood, and the security controls have been tuned to work under that load. Many of the functions I routinely use at the office can be accessed from outside of the university network, but I first need to establish a virtual private network (VPN) tunnel through a particular service managed by the university. Now, each of the 10,000 or so academic and administrative staff in the university will be depending on that service every day to continue "business as usual as we can make it." If it fails to scale with the load, many essential business functions will not be possible to do remotely, period, without changing the security controls.

The Internet, in general, and security services, in particular, are now being hit with demands that will test their limits of scalability. I believe that my home Internet service provider is being affected. I have to reboot the cable modem two to three times a day to restore lost service, and the available bandwidth wildly varies between 10% and 150% of the capacity I'm paying for. My own experience is just a microcosm of what's going on everywhere. The cybersecurity infrastructure will hold up to this new load, or it won't. First indicators on this are not promising; a colleague has heard from friends in Europe that many commercial VPNs there are failing. By the time this editorial appears in print, we'll have a much better idea of how well cybersecurity at the edge is able to hold up.

The Internet, in general, and security services, in particular, are now being hit with demands that will test their limits of scalability.

As the future unfolds, there will undoubtably be breaches and attacks that are enabled by the confusion. Controls might be loosened

Digital Object Identifier 10.1109/MSEC.2020.2983357
Date of current version: 14 May 2020

 Copublished by the IEEE Computer and Reliability Societies

With greater dependency on the public communication infrastructure, organizations become more vulnerable to distributed denial-of-service attacks.

to work around VPN scaling issues; people will find ways to circumvent failing security controls when those controls impede their ability to work. All of this will create entry points and expose access and information that otherwise would have been protected. This is a prime opportunity for phishing attacks because more people are online and anxious for news and are working within new, unfamiliar workflows. This makes it harder to recognize abnormal requests or emails. Also, with greater dependency on the public communication infrastructure, organizations become more vulnerable to distributed denial-of-service attacks.

We are in a Petri dish, involuntarily testing (among other things) the scalability of cybersecurity at the edge. We will learn lessons from this experience and how to better secure this way of working. We'll have to; working remotely will be normal for many of us for quite a while. ■

Digital Object Identifier 10.1109/MSEC.2020.2981215