Auto Casualty

What Does Network Security Look Like When There Is No Perimeter?

October 8, 2017
4 MIN READ

Erez Nir

Recently, it's been said by many in the IT Industry that 'the perimeter is dead'. But what, exactly, does that mean? Think of it this way: it hasn't been that long since all users, devices and applications were corralled into a closed network with defined entry and exit points. Essentially, the 'wagons were circled' and a firewall could be built to protect the perimeter. Today, however, boundaries are blurred between work and home network, business-issued and personal devices, physical and virtual architectures, and of course, on premises and cloud infrastructure. There are so many different ways to operate a modern business nowadays, and so much information going into and out of a business network through many entry and exit points, that there simply is no well-defined perimeter that is easily secured.

Bolstering the weakest link—human behavior

So what are CTOs and CIOs to do? Sticking with past solutions and incrementally improving upon them is no more an option than finding a shiny, new, silver bullet. And unlike Bank of America, most enterprises do not have unlimited security budgets. Here's a statistic to get you thinking about what to do: in 2015, the responsibility for more than 40 percent of all data breaches that contained personally identifiable, personal health, bank, insurance and social information, was traced to employees, either due to intentional or accidental action. The lesson here is that the human factor is a key threat to be addressed, and that's a good place to start. At the most basic level, both training and personal responsibility are key. Beginning with onboarding and throughout each employee's tenure, they must receive ongoing training on the important role they play in protecting company and client data. When addressing this, everything matters—passwords, email, unauthorized software, personal and company-issued mobile devices—and training programs must cover all these areas.

> In 2015, the responsibility for more than 40 percent of all data breaches that contained personally identifiable, personal health, bank, insurance and social information, was traced to employees, either due to intentional or accidental action. The lesson here is that the human factor is a key threat to be addressed, and that's a good place to start.

Long term, I believe layering in identity-defined security, in which access is not only tied to an individual user, but also to the context in which he or she is accessing certain information, is the next logical step in the process. I'm over-simplifying here, but the idea is one of a central identity management platform that grants employees, customers and partners access to all applications, databases and back-end services based on who they are, where they are, what device they are using and what they want or need to access. Through automation, a network with identity-defined security could efficiently manage an unlimited number of identities. Further, it could be deployed on premises, in a cloud solution or in some combination of the two. It could even identify, flag or stop unusual, though permitted, access, much the way next-generation, behavior-based antivirus software does.

Addressing the here and now

While identity-defined security may be in Mitchell's future, we are taking an aggressive approach to the here and now. We have a focused, five-year information security and risk management plan in place—we're currently on year four—to secure the Mitchell network, customer data and employee information. Each year, we re-evaluate the plan, make changes as new technology (and threats) dictate, commit resources and look ahead to another year. The resources we commit are both financial and human. We dedicate a substantial part of our IT budget to security each year, and we also understand the value of having the right people with the right skillsets in place now in the future. Our security efforts are led by cross-functional team members focused on application security, network vulnerability, security information and event management (SIEM) implementation, and more. And one final thought on the topic: at Mitchell, we're in the fortunate position of having strong partnerships with our clients, and we're always looking for opportunities to work closely with them by sharing best practices and key learnings. In fact, we are currently looking to do this is through our newly formed Technology Advisory Council, a roundtable where CTOs and CIOs from our client and partner community come together to exchange information and ideas. If you are a Mitchell client and would like to know more about Mitchell's Technology Advisory Council, please contact PCTechCouncil@Mitchell.com.