SPOTLIGHT

How to Prepare for the Next Generation of Cyberattacks

An interview with Tony Lauro, Senior Enterprise Security Architect, Akamai Technologies

Today, cyberattacks around the world are becoming more prevalent and more complex. 2016 saw seven of the largest Distributed Denial of Service (DDoS) attacks in history, and three of those attacks occurred in Q4. Hackers use DDoS attacks to render IT systems inoperable, and they are extremely difficult to defend against. The introduction of a massive amount of Internet of Things (IoT) connected devices into IT environments further complicates cybersecurity protocols.

But there are ways to stay vigilant. For state and local agencies, identifying web traffic within an IT environment, staying aware of common attackers and methods, and focusing on protecting the enterprise as a whole can help prevent DDoS attacks. GovLoop recently sat down with Tony Lauro, Senior Enterprise Security Architect at Akamai Technologies, to discuss the changing cybersecurity landscape and how to prevent harmful DDoS attacks and more. Akamai Technologies is a content delivery and cloud services provider.

First, Lauro discussed how state and local agencies must be able to distinguish what web traffic within a system is good, bad, or just ugly. If a user within an environment, like a tax information database, is searching for a singular data point and is using the system normally, then this is probably safe traffic. If, however, a user is attempting to access large swaths of data or personnel records, then the user account may be compromised or malicious.

Properly monitoring user traffic is only going to get harder for state and local government because of the increasing amount of IoT devices connected to the web, according to Lauro. He noted, "Unless you have a method for identifying what baseline user activity looks like and creating security controls around good traffic, you won't be able to weed out bad traffic or misconfigured traffic."

Next, Lauro stressed that for state and local agencies to properly prevent cyberattacks, they need to gather intelligence on common threats and hackers targeting public sector agencies. There are currently search engines and botnets helping hackers infiltrate critical infrastructure, and agencies are constantly being threatened by phishing scams that use innocuous emails to breach firewalls.

Although it's difficult to keep up with the latest cyberthreats, Akamai's software can help government stay on top of trends by monitoring malicious IP addresses and cyberattacks around the world. "We already have a criminal track record for users, so when they attempt to attack your systems, we're going to apply your security model, based on that previous activity. That way you are not waiting for them to attack you with full force."

Lauro added that updating software and preventing it from being breached is crucial for agencies because it's where important data is stored. But software is also the most difficult component of an IT system to defend because legitimate system users are also interacting with platform interfaces.

Lastly, an agency cannot be fully protected if it doesn't take into account threats that can emerge from within the enterprise system. Lauro compared this to a house's front door being locked and guarded, but a contractor, who legitimately enters, may still make the entire house more vulnerable to attack. For agencies, this is comparable to when an employee opens up an innocuous email that turns out to be malware or a phishing campaign. Once a hacker uses this method to breach a system, they can move laterally within an environment and access sensitive data.

Akamai created their enterprise solutions to defend against these types of attacks by scanning outbound requests for any malicious software. The system then flags the activity before a browser can download the malware, notifies the administrator of a potential cyberattack in progress, and automatically blocks the attack. This is then coupled with the intelligence that Akamai gathers about common web threats to efficiently root out cyberattacks before they even occur.

State and local agencies must properly identify their incoming and outgoing web traffic, anticipate common threats, and defend the entire enterprise system in order to prevent future cyber breaches. Agencies can leverage new technologies, industry intelligence, and automated processes to conserve spending and manpower, and by saving resources on IT functions and maintenance, state and local government will have a larger bandwidth to devote to serving their constituents.