USING AI AS A CYBERSECURITY FORCE MULTIPLIER

Joseph Mara, vice president Americas, state and local government and education for Symantec, discusses technologies that not only improve cybersecurity but also help address cybersecurity staffing shortages.

The recent ransomware attack against multiple cities in Texas reportedly was a targeted attack. Does this indicate that the nature of these attacks is changing? If so, what are the implications for government agencies?

We recently published a special Internet Security Threat Report on targeted ransomware (https://www.symantec.com/security-center). These targeted attacks are very destructive and inclusive. Protecting the significant amount of personally identifiable information (PII) that organizations have in their systems is very important, and some municipalities — especially the smaller ones — don't have the appropriate resources in place to protect everything. That can make them easy targets for a ransomware attack. I don't want to say that smaller cities can't protect themselves, but they could be a potential target.

How are technologies like artificial intelligence (AI) and machine learning being used to improve security?

The strength of AI lies in the ability to analyze a huge volume of data across large networks. It allows state and local agencies to detect patterns and abnormalities; it signals potential threats; and it does so faster than any human could do alone. AI enables organizations to determine quickly and efficiently how to respond, so it's very important. Machine learning takes it a step further by enabling the solution to learn as it goes.

Where will AI and machine learning have the biggest impact?

The biggest impact will be in the security operations center, where these technologies act as a force multiplier. A lot of agencies face a shortage of cybersecurity professionals, so AI and machine learning can help augment their resources. The good news is that AI is rapidly becoming commercialized, meaning it's being embedded into existing products so state and local agencies don't have to worry about hiring experts in that area.

What emerging technologies should our readers be aware of?

Behavioral analytics is an interesting area. Leveraging AI, you can learn what constitutes normal behavior on the network, both in terms of the system and humans. Then, by monitoring for what is abnormal, you can take actions to help protect yourself. If something happens you can quickly remediate the threats targeting your system. In the past, organizations recognized cyber threats only after the damage was done, which is way too late. Today's technologies accelerate every aspect of the cybersecurity life cycle, from detection to response and mitigation.

What else can agencies do to strengthen their security stance?

Agencies can no longer approach cybersecurity in a fragmented way — meaning buying products to solve for a specific vulnerability without thinking about how they should be integrated together. They need to adopt an integrated cyber defense approach that unifies products, services and partners to drive down the cost and complexity of cybersecurity. This approach combines information protection; threat protection; identity management; compliance; and intelligence and automation across endpoints, networks, applications and clouds.

Learn more at **Carah.io/GT-Cyber-Symantec**

Integrated Cyber Defense for State & Local Government

Enhancing cyber capabilities to identify, protect, and respond to advanced threats.

Learn more at: www.symantec.com/state-local-gov

Symantec™