Brought to you by: CIO FROM IDG

CYBERSECURITY: BEYOND THE SCOPE OF MORTALS

Cybersecurity has long been described as an arms war. When the good guys learn how to counter an attack, the bad guys up the ante with new techniques. But as both sides take advantage of advanced technology, it's increasingly clear that enterprises need a combination of smart people and scalable security solutions that leverage automation and artificial intelligence (AI).

When one country is accused of using cybercrime to interfere in another's election, causing that nation to stage cyber "bombs" for a potential retaliatory strike against its attacker, there's no denying that we've reached new heights of awareness and concern regarding cybersecurity.

Earlier this year, the reported leak of CIA and NSA hacking tools was a wakeup call telling us the lines separating state-sponsored cyber espionage and criminal elements is exceedingly thin, at best.

"Cybersecurity is a fast-morphing technology, meaning that making any assumptions about what will be needed six months from now is difficult at best," *TechRepublic* notes in a recent article on scenario planning for potential future cyber threats.

CYBER ARMS RACE

The technology behind cybercrime is evolving rapidly, putting new tools in the hands of both perpetrators and defenders. "The rise of AI-enabled cyberattacks is expected to cause an explosion of network penetrations, personal data thefts, and an epidemic-level spread of intelligent computer viruses," University of Louisville Cybersecurity Lab Director Roman V. Yampolskiy writes in a recent article for the *Harvard Business Review*.

"Ironically, our best hope to defend against AI-enabled hacking is by using AI," he adds. "But this is very likely to lead to an AI arms race, the consequences of which may be very troubling in the long term, especially as big government actors join the cyber wars."

Big data technology provides cybersecurity strategists with tools to anticipate developing threats. "[W]hen we notice an uprising popularity in certain pieces of technology, we can use this information as a forecast in terms of where to focus our cybersecurity applications," Jenn Livingston writes in *CIO*. "Security breaches have a notorious reputation for being relatively random, spontaneous and out of the ordinary. However, when we properly analyze the data being produced by these platforms, we can be a step ahead of the curve in terms of preparation and security software implementation that protects the user's personal data."

WAR GAMING

When the recent WannaCry malware assault essentially brought the UK's National Health System to a halt, it was clear that such attacks have the potential to put lives at risk. In such a perilous and constantly changing environment, it is essential that the top minds in cybersecurity take their cue from military strategists who are constantly war-gaming scenarios in efforts to envision potential attacks and plot out defenses.

"The first thing we have to understand is the only constant in cybersecurity is change," says Rackspace Chief Security Officer Brian Kelly. Rackspace and technology consulting firm Ernst & Young (E&Y) have been working together for several years on the implementation of cybersecurity capabilities. Now they've allied in war-gaming activities aimed at anticipating and thwarting assaults.

"We constantly have to be thinking about what's new, what's different, what we can anticipate in the future," says Kelly. "The only way we can then translate that to the day-to-day operations is to practice and that's really what's behind these war games. It's to take a practical look at evolving threats, evolving tactics, evolving approaches, expose our operators to those, and allow them not only to become familiar but also to learn how to adapt and to evolve our techniques and our tool sets."

Kelly says it is critical to move beyond table-top scenario planning and ensure that cybersecurity teams experience what in the military is termed "the fog of war" and feel the heat of the battle they are likely to encounter during a cyber assault.

"Many of our analysts come from a military or operational background," says David Neuman, chief information security officer with Rackspace, who spent 28 years in the military, with three combat tours. "They are very familiar with a continuous cycle of readiness and exercises are [a] key component to that."

TRAINING FOR CATASTROPHIC EVENTS

As the WannaCry assaults demonstrated, cyberattacks can be catastrophic-level events. That means your security teams should have practice in addressing a simulated event, so they learn how to respond quickly, adjust to the unanticipated, and implement resolutions to mitigate any damage.

Part of the preparation is making sure you have the right people, processes, procedures, and tools in place to deal with cyberattacks. "We test what it is we've built and through that testing not only do we learn but we get validation of what we are," says Brannon Lacey, Rackspace vice president and general manager for the company's managed security service. "The end result is better preparedness, which ultimately means a reduction of business impact on our customers when bad things happen."

With cybersecurity unemployment expected to remain at a 0% rate through 2021, finding the right people to staff security teams will be a challenge. As CSO recently pointed out, there are currently approximately 350,000 cybersecurity openings in the U.S., compared to 780,000 people employed in cybersecurity positions. According to Cyber Seek, there are currently 88,000 information security analysts employed in the United States, representing a shortfall of 40,000 for available positions.

That imbalance between supply and demand means that no matter how much enterprises invest in technology solutions, many are going to be short-staffed when it comes to putting the right people in place to leverage those tools. Many will need to turn to managed security partners to fill the gaps in their defenses.

To learn more about how managed security services can bring value to your organization, check out https://www.rackspace.com/en-us/managed-security-services.