Fight Against Ransomware Starts with People, Not Technology

Strategy and culture are key to the Education Department's holistic approach to cybersecurity.

Ben Haseltine

Wed, 06/13/2018 - 15:32

Illustration: Hipspeeds/iStock

With new security system and firewall developments, hackers are more determined than ever to breach these systems under the guise of malware and ransomware. Ransomware attacks have increased by more than 90 percent from 2016 to 2017, according to the Malwarebytes Cybercrime Tactics and Techniques: 2017 State of Malware Report.

Dell EMC and RSA's June 7 government briefing in Washington, D.C., highlighted the effects of ransomware and other challenges within the cybersecurity enterprise.

Speakers from the Education Department and the National Institute of Standards and Technology joined industry speakers to discuss how to make government systems more secure. There was a common theme around increasing protection from malware and ransomware software used to gain access to personal data.

Ransomware is software that infiltrates a user’s data, consequently holding the data in question for ransom. Typically, it’s prohibiting the users' access to their files or threatening to publish private information online in exchange for bitcoin or some other form of payment.

This type of cryptoviral extortion has affected millions around the world, whether in the form of a Trojan horse that was on a single desktop or a massive virus like WannaCry — the worldwide cyberattack that targeted computers running the Microsoft Windows operating system. The WannaCry attack in 2017 held people's personal files ransom in exchange for a series of bitcoin payments and sparked a sense of urgency and awareness for the need to strengthen cybersecurity. .

Now, ransomware and malware security are at the forefront of the issues facing the cybersecurity industry. For Tina Rodriguez, senior adviser of cybersecurity at the Education Department, the issues surrounding these obstacles are much simpler than the technology involved.

“Many problems with cybersecurity are human," she said. "The solution can be the application of a new tool at times . . . but you need to make sure that the tools you have are well provisioned and work well, and that people know how to use them."

The responsibility falls on the executives working with the data and personal information to have a clear understanding of all the procedures and systems involved, while managing the security with vigilance. This means making sure all data is backed up to the point of redundancy, and usingfirewalls, anti-malware and layered protection to reduce the threat of ransomware.

But most importantly, Rodriguez stressed the need to ensure basic administrative and technical work is running smoothly, so the cybersecurity tools running can be as automated as possible. The responsibility of maintaining security has to be the cornerstone of culture.

“You just need to make sure you're building a strategy, when you are creating your culture, that you are moving forward, and taking a more holistic approach, and that you’re not just placing technology on top of a person problem,” Rodriguez said.

View printer friendly version
ransomware
malware
cyberattacks
Federal Cybersecurity
RSA
Department of Education