https://www.sdxcentral.com/articles/news/top-cyber-cops-give-security-tips-preventing-attacks/2017/09/?c_action=home_slider
Top Cyber Cops Give Security Tips for Preventing Attacks
29/09/17

Jessica Lyons HardcastleSeptember 28, 2017
1:30 pm PT

SAN JOSE, CALIFORNIA — Deterring a hacker from attacking your network can be as simple as changing a password from 1-2-3-4, according to top U.S. intelligence officials.

MK Palmore, an information security risk management executive at the FBI's San Francisco Cyber Branch, said protecting an enterprise can be boiled down to three key elements. "Commitment from management, practicing information security fundamentals, and information sharing," he said, during the opening keynote today at a NetEvents conference in San Jose, California. "This message, while simplistic, is not being followed. Businesses don't spend enough time about those issues."

Related Articles

Gap, FedEx, Caesars Entertainment Rain Love on Oracle Cloud

Level 3 Warns Investors about Canadian Firm’s Mini-Tender Offering

Hardware Maker Lancom Gets Into SDN

He also recommended two-factor authentication, which implements an extra layer of security on top of a password and username.

“It’s an obstacle to threat actors,” Palmore said. “It’s not insurmountable,” he added, but for many hackers “it is a waste of their time. They will move on to a target that is easier to breach.”

While newer technologies like artificial intelligence (AI), machine learning, and deep analytics have made security software more sophisticated, hackers also use these same tools.

For example, machine learning can very quickly crunch massive data sets and develop models to detect irregularities in device behavior or network traffic, said Anup Ghosh, chief strategist of next-gen endpoint at security software company Sophos. “We are very good at being able to use deep learning in security products by performance measure of high detection of unknown threats,” he said.

But, he added, machine learning can also be used for evil: “Machine learning is good at crafting Twitter and Facebook campaigns that are very good at getting humans to click on those links.”

To this end, it’s important to train employees not to open attachments from unknown senders and not to click on unknown URLs, said Dr. Ronald Layton, deputy assistant director of the U.S. Secret Service.

“Awareness does not equal behavioral change,” Layton said. “So we need to find new and innovative ways of training and getting our message out.”

This also involves training employees to treat things like account information and social security numbers as “classified information,” said Michael Levin, former deputy director of the U.S.

Department of Homeland Security and the founder and CEO of the Center for Information Security Awareness, which provides security training courses for businesses.

“Part of the problem is changing the culture,” Levin said. “Treating it as top-secret data, and having a process in the organization for doing that. Security has to be just as important as being polite to customers and something that employees are thinking about when they turn on their computer every day.”

Finally, information sharing — with other companies and with law enforcement — is key. The FBI and U.S. Secret Service work with enterprises to prevent security breaches. Additionally, collaborative efforts like the Cyber Threat Alliance connect companies and provide a way to share threat information and collectively improve threat defense.

Levin compared these information-sharing efforts to a Neighborhood Watch program. “Create public-private relationships to help you before there’s an incident. Having law enforcement contacts and private sector contact is best practice now.”

“Prevention is the best strategy,” added Layton, who said prevention comes down to basic security hygiene. “Most successful hacks and breaches are because low-level controls were not in place. Patch management. Change passwords from 1-2-3-4. It’s the low-level stuff that will get you to the extent where the bad guys will say, ‘I’m going to go somewhere else.’”

Photo: (left to right) MK Palmore, Ronald Layton, and Michael Levin discuss hackers and security tips at a NetEvents conference.