Put Strong Processes in Place to Reduce Risks

Connection™
PUBLIC SECTOR SOLUTIONS
we solve IT™

1.800.800.0019
www.connection.com/ps

Face to Face on Cyber Security

Agency networks are becoming more complex, increasing the security risk and underscoring the need for a comprehensive security strategy that looks beyond technology. Digital transformation, mobility in the workforce, the Internet of Things, and hyper connectivity are all examples of disruptive technologies that have increased agencies' security risk.

However, the biggest disruption for an agency is the security threat, according to Stephen Nardone, Director of Security and Mobility Practices, Connection® Public Sector Solutions. Cyber attacks and breaches are growing and cyber criminals are the best-funded, best-trained cyber experts in the industry. "There's no way you can keep pace with that," says Nardone. "Frequently the attacker is already on the inside of your environment, and you just don't know it."

They are not really trying to wreak havoc, but rather to learn, he says. "Even though you may consider yourself not being an interesting target, you could be a good learning target for any cyber criminal that may be out there."

Network breaches are on the rise, says Nardone. There were more than 34 million identity-related breaches on government systems in 2015, representing 19 percent of the total breaches that happened. In 2016, that dropped to 13 million, but increased in percentage to 37 percent. So the attacks decreased in the amount of information compromised, but the number of attacks has increased and that trend continues.

Gone Phishing

Phishing is a big problem in the government space, especially in the unclassified realm. "You put a lot of energy in building a tremendous infrastructure, you have great firewalls and intrusion prevention and detection, but the attacker can still get on the inside based on phishing," he says.

In a survey conducted last year, Connection found that about 42 percent of IT leaders see a breach due to employee error or negligence as a top issue. About 35 percent of them worry about malware tailored to specific audiences. Simple phishing works, and someone doesn't need to be a very good hacker to do it. For example, someone could send an email to all employees complementing them on their great work and providing a link to a gift card. Once the link is opened, it will pull down malware onto the network.

Once in the system, the hacker can introduce new malware into other systems and introduce other tools such as a key-stroke logger that could capture identities and passwords. Ultimately the result can be an entirely compromised environment.

How can an agency take control of the situation? By building a comprehensive security program that addresses not only the technology, but also people and process, says Nardone. "The technology does exist, but it's how the users are using the technology and are they actually behaving in safe and secure ways, [that] is really the key," he says.

An agency has to address organizational security issues including roles and responsibilities, all the way up to audit and compliance management. Sticking to the three pillars of security management—protect, detect, and react—as well as following FISMA, and the NIST Cyber Security Framework can help. As threats become more sophisticated, Connection also recommends agencies follow a six-step process to understand what needs to be done from a programmatic perspective, says Nardone.

Those steps are:

1. Carry out comprehensive outside and inside testing
2. Develop a sound back up plan for ransomware and advanced threats that compromise data
3. Utilize a unified security stack to reduce the amount of vendors
4. Deploy endpoint security that includes behavioral level tools that respond to events
5. Utilize sandboxing that is tied back to the end point
6. Create virtualization that helps containerize how users gain access to information

From a practice perspective, comprehensive security testing and assessment is essential. "Make sure you are testing your environment the same way the bad guy is going to be attacking your environment," says Nardone.

Created in partnership with PUBLIC SECTOR MEDIA GROUP