This headline appeared in June after a cooperative effort between the federal government and the Center for Internet Security (CIS) thwarted a prolonged operation to spy on aviation systems at 75 U.S. airports, but not before hackers breached the networks of two of them.

Authorities actually discovered this threat in 2013, when the federal government notified CIS about an advanced persistent threat (APT) targeting airports. Typically APTs involve Nation State attackers employing sophisticated methods to creep around a network for as long as necessary to obtain the information they seek. In this case the attackers sent spear phishing emails to aviation personnel containing vulnerabilities that the CIS reports were difficult to detect and execute.

This is not a rare event; in fact it’s one that is happening far more frequently than ever before. According to the annual CIS report, there were 48 significant computer security incidents in 2013, more than double the number recorded in 2012.

It’s also something that’s striking globally. In late September, news media reported hackers broke into the server of India’s largest airport operator, the Airports Authority of India, and stole crucial data including financial information, payroll data, and more.

“Here’s the scary part about these incidents: They are attacking and targeting airports—and nobody really knows why,” says Andre Allen, information and cyber security manager at GCR Inc., an international software and technology firm in the airport space.

Not only that but, according to Mark Gazit, CEO of Theta Ray, a national firm offering cyber security solutions, the average time to discover a threat is approximately 240 days. But, he adds, it can take a month or more for an organization to recover.

Even more concerning are the words of Dom Nessi, deputy director/chief information officer at Los Angeles World Airports (LAWA): “I think around a network for as long as necessary to obtain the information they seek. In this case the attackers sent spear phishing emails to aviation personnel containing vulnerabilities that the CIS reports were difficult to detect and execute.

This is not a rare event; in fact it’s one that is happening far more frequently than ever before. According to the annual CIS report, there were 48 significant computer security incidents in 2013, more than double the number recorded in 2012.

It’s also something that’s striking globally. In late September, news media reported hackers broke into the server of India’s largest airport operator, the Airports Authority of India, and stole crucial data including financial information, payroll data, and more.

“Here’s the scary part about these incidents: They are attacking and targeting airports—and nobody really knows why,” says Andre Allen, information and cyber security manager at GCR Inc., an international software and technology firm in the airport space.

Not only that but, according to Mark Gazit, CEO of Theta Ray, a national firm offering cyber security solutions, the average time to discover a threat is approximately 240 days. But, he adds, it can take a month or more for an organization to recover.

Even more concerning are the words of Dom Nessi, deputy director/chief information officer at Los Angeles World Airports (LAWA): “I think the headline read: “Nation State-sponsored Attackers Hacked Two Airports, Report Says.”

KEYWORDS IN CYBER SECURITY

- Advanced persistent threat. An advanced persistent threat finds a hole in a network that allows hackers in so they can sit back and monitor what an airport is doing.
- Cyber hygiene. Steps computer users can take to improve their cyber security and better protect themselves and their organizations online.
- Malware, short for malicious software. Software that compromises the operation of a system by performing an unauthorized function or process.
- Phishing (spear phishing). An attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Virus. Computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.
airports have a long way to go, both in the United States and internationally, to meet the challenges of today’s cyber threat. That’s not to say that individual airports haven’t succeeded in terms of cyber security, but many airports still have work to do.

CAUSES OF CYBER INSECURITY
Dr. John McCarthy, cyber security fellow at Cranfield University and head of research with the International Centre for Airport Cyber Research, is concerned about airports being vulnerable to attacks for three key reasons:

• Airports are very inflexible environments with many different stakeholders. Just getting all the stakeholders in the same room to discuss issues such as cyber security is a challenge.

• Airports are cost driven. Without adequate funding, airports might not invest in the technology they need to secure their networks.

• Airports are cost driven. Without adequate funding, airports might not invest in the technology they need to secure their networks.

WHERE VULNERABILITIES LIE

According to Nessi, safety and security systems, bagage and handling technology, and the building’s facility control systems are attractive targets for cyber crooks. But in stark contrast, says McCarthy, most airport cyber security efforts focus on the traditional IT network, not on these systems.

“Recent technological developments and the need to increase efficiency have resulted in the merging of traditional IT networks with SCADA (Supervisory Control and Data Acquisition) Systems. Now airports often have homogeneous networks that are bolted together with cyber security as an after thought,” explains McCarthy in “Cybersecurity: Keeping Cyber Secure.”

“This phenomenon means that some of the more interesting appearing systems pose the most risk. For instance, many people would not lump industrial control systems into their cyber vulnerabilities. But HVAC, airfield lighting, automated parking systems, automated people movers, and bagage systems all provide entry points into an airport’s network.

“Those systems are at risk because most people don’t think they could be compromised,” McCarthy says. “They don’t even think of them as being connected to the Internet. If you don’t at least start looking at your risk associated with your critical systems and putting some controls around them, you’re very vulnerable.”

Another area to consider, says McCarthy, is the airport Website. McCarthy recently performed a hacking demo at an airport in Rome where he breached their Website and placed a malware on it. “A hacker could cause collateral damage to an airport through a system most people don’t even think to protect,” he says.

“They hack into the Website, change your parking URL to a nearly identical one that they own, send out a phishing email to your customers telling them they’ll get full off their parking if they book online, and all of this money goes to the hackers. And they haven’t even touched the IT system in the airport!”

DIGITAL DEFENDERS

Nessi recommends taking the Defense in Depth strategy in a comprehensive way. Defense in Depth is defined as the coor of multiple security countermeasures to protect the integrity of an organization’s information assets. The idea is that it’s more difficult to defeat a complete and multi-layered defense system than to penetrate a single barrier.

Defense in Depth minimizes the proba- bility that malicious hackers will succeed by employing a well-designed strategy that aids system administrators and security personal in identifying attempts to compromise a computer, server, proprietary network or IP/ISP (internet service provider). Should a hacker gain access to an airport’s network, Defense in Depth minimizes adverse impacts and gives administrators time to roll through the network looking for suspicious activity. Human eyes still need to review those logs every single day. “A hacker will find a vulnerability, exploit it, and use vulnerable code to automate attacks. Defense in Depth strategy aids in early detection by making it more difficult to compromise a system. Without Defense in Depth, cyber crooks can continue their attacks and continue to gain access with greater ease,” says Nessi.

This strategy utilizes antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection and biometric verification. “On your perimeter, you have firewalls and intrusion detection systems, and a variety of systems that monitor and protect your network.” Nessi says. “You have technology to protect your data and technology to protect your applications, and hand in hand they protect that your interaction on the Web. You have technology that protects your desktop environment. And now we have technology that protects our mobile devices.”

Allen also recommends adding application software into your overall Defense in Depth strategy, noting that this technology can prevent up to 80 percent of the threats trying to sneak in. This technology can limit how that it will only operate those applications a user needs to perform his or her job. If a user clicks on an email containing malware, the malware won’t execute and the technology quarantines it. This gives network administrators time to respond and deploy their defenses,” he says.

Though technology used in the Defense in Depth strategy aids in early detection by looking for suspicious network activity, it may not be enough and threats may still slip through. Gaizt stresses, “Early detection is one of the biggest holes in cyber security today. It’s unacceptable to think about an airport or an airline that doesn’t have smoke detectors. But we don’t always have cyber attack detection systems.”

The challenge is not just in understanding the connection between cyber security and their business, they’ll get serious about the funding,” he says.

“The utilization of your organization’s systems is not a personal right of an employee,” he explains. “Nobody has enough funding to do everything.”

ANDRE ALLEN: HOW TO BUILD YOUR DIGITAL DEFENSE

Figure out where you are. “What is the current state of your cyber security? he asks. “What are you protecting currently? What vulnerabilities exist? List the systems that you have. Allen recommends classifying the systems by asking the following questions:

• What kind of systems are they?

• Are they critical?

“These would be systems that if down could cause major disruptions or a loss of life.

Prioritize protection. After identifying the systems, determine which are most critical to protect. “You can’t do everything—that’s a given,” he explains. “Nobody has enough funding to do everything.”

The Multi-State Information Sharing and Analysis Center is considered by many as the focal point for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal and territorial governments. This CERST organization offers Web-based training that Allen says can greatly enhance employees’ understanding of cyber security.

Training should cover good cyber hygiene, which McCarthy describes as everything from not downloading or opening unknown emails, password protection, how to look at those logs to see if there is anything there, he says. “If they think there is something going on, they need to report it.”

HOW TO BUILD YOUR DIGITAL DEFENSE

• Hire good cyber security people to monitor your systems. Those certified by ISOC have the training needed to adequately protect IT and your network.

• Place cyber security professionals in the right areas. They need to be in a position to oversee IT operations and the IT environment in an unfeathered manner.

• Give cyber security experts the authority to do what they need to do for an airport to be cyber secure.

• Remember cyber security is a 24/7 business. You have to commit to dealing with it 24 hours a day seven days a week. “Cyber security needs to be part of your board, your C-level suites, your technology, etc. It’s not just your IT people,” he says.

DOM NESSI’S TIPS FOR BETTER CYBER SECURITY

• Protect your systems. “If your network was built with very few safeguards internally, it was built for failure,” says Nessi. “It’s not built to facilitate communication. The human element of it has made it a dangerous place to be.”

For this reason, Defense in Depth also includes employee training and education of employees. LAWA provides annual cyber security training for its workers. Says McCarthy, “We need to educate all levels of the organization in sound practical senses. Airports could stop 90 percent of all cyber security issues by properly training all members of the organization.”

ANDRE ALLEN: HOW TO BUILD YOUR DIGITAL DEFENSE

• Figure out where you are. “What is the current state of your cyber security?” he asks.

• List the systems that you have. Allen recommends classifying the systems by asking the following questions:

• What kind of systems are they?

• Are they critical?

“These would be systems that if down could cause major disruptions or a loss of life.

• Prioritize protection. After identifying the systems, determine which are most critical to protect.

• "You can’t do everything—that’s a given," he explains. "Nobody has enough funding to do everything."