Airline industry swooping in to prevent cyberattacks

November 8 2013, by Paresh Dave

Worried that computer hackers attacking banks and media companies could easily shift targets, the airline industry is taking preemptive steps to ensure it doesn't become the next victim.

Although the "hacking" of planes midair to bring them down is unlikely, many networks, including airline reservation systems and airport parking meters, could be vulnerable to cyberattacks, which could disrupt air travel, weaken travelers' confidence and deal a major blow to a fragile economy.

"The aviator guys are getting together because they see what's going on in every other sector," said Paul Kurtz, chief strategy officer for computer security firm CyberPoint International. "It's just a matter of time before the bad guys start wondering, 'How do we start making money off attacking the aviation industry?' "

New technologies and tighter budgets have added to the complexity of safely transporting 2.6 billion air passengers a year worldwide. But officials at airlines, airports and aircraft makers believe they can develop enough safeguards to limit the effects of hackers.

Boeing Co., which by the nature of its business has always focused on aircraft safety and reliability, is now also stressing network and computer systems security. Worries about defects such as hydraulic leaks have been brought up alongside concerns that a miscreant could surreptitiously inject malicious commands somewhere in the 18 million lines of computer programming that help power its latest jet, the 787 Dreamliner.

"I know the media worries about the kid in seat 14B on his laptop hacking the flight controls," Michael Sinnett, Boeing's vice president of product development, said at an industry conference this summer. "I'm here to tell you that's not going to happen. But the question is, 'Do I have to worry about a guy inside my system for four years before the code even hits the streets?' "

Most of the code is written by Boeing contractors, and Boeing and aviation regulators test for errors. Even afterward, Boeing assumes programs will do something unexpected and prepares backup plans.

For pilots, large suitcases filled with instruction manuals have been reduced to laptops and, more recently, tablet computers. Weather updates and other flight-related information - once relayed via air traffic controllers or paper printouts - are increasingly beamed by Wi-Fi and the new NextGen air traffic control system directly into the cockpit.

Kurtz said protecting those links is relatively easy in the U.S.

"But somewhere in Asia or Africa, the updates and maintenance might not be as (buttoned-down)," he said.

Yet not all airports in the U.S. are ready to guarantee secure connections for airlines. LAX has been among the large airports at the forefront of strengthening defenses through education and monitoring.

But Dom Nessi, LAX's chief information officer, said that the airport doesn't offer airlines a dedicated connection because "we don't think we can give them a secure service."

Like other airports, LAX remains a juicy target for hackers. A phishing attack in late June and early July tried to deceive airport employees into opening fraudulent emails, Nessi said.

The airport's cybersecurity investigators said the "highly targeted" emails encouraged users to download files that when opened could have given the remote attacker "complete control over the victim machine," including the ability to monitor their Internet browsing and email.

The experts traced the attack to a foreign government, Nessi said. Phishing emails have led to several major cyberattacks, including one that led to a New York Times website outage for two days in August.

"Every day a new threat emerges, so you have to build an organization that evolves and evolves rapidly," Nessi said.

The two Washington, D.C., area airports recently began rigorous testing of computer networks and teaching employees about protecting their computers from hackers, said Martha Woolson, information technology security manager for the Metropolitan Washington Airports Authority.

Woolson said a year and a half ago several employees fell for a phishing email designed to look like one sent by US Airways. During a recent wave of phishing, more than 30 airport workers came to her for advice when they received the email.

Woolson has gone as far as distributing magnets with a simple warning, "When at work, don't go to any site that would embarrass your granny."

Cybersecurity experts suggested that airlines and airports must expect that hackers eventually will shut down crucial systems. Having a strategy in place to quickly recover is essential, they said.

"Many airlines are worried about hackers but have no idea where to start," said Joe Ayson, senior director for aviation cybersecurity firm AvIntel. "Our goal as a practice is to ensure there's a constantly revised mitigation process in place that's an actual living, breathing part of operations."

He recounted the recent experience of an airline in Africa whose reservation system had been sputtering for six weeks. The airline didn't realize it had been plagued by a computer virus. Ayson's team found ways to keep the airline running despite the issues.

Peter Andres, vice president of corporate security for Deutsche Lufthansa AG, said being a "sexy" industry heightens the challenges.

"There are so many people who love to play with simulators, who listen to controls, who really study this stuff," Andres said. "But that of course gives more transparency and tools to people who have malicious intent."

Airlines, airports and aircraft makers see themselves at a crossroads. The sooner they can show that computer-related threats have been minimized, the more likely the industry won't face additional government regulation.

"It's the kind of homework that's been long overdue," Andres said.

About the only regulation desired by the industry is legislation protecting airlines from liability and lawsuits if they share information about "hacks" with one another and the government.

To be sure, airlines run the risk of overreacting about the risks of technology. Boeing's Sinnett compared cybersecurity with lightning. Every plane is struck by lightning once a year, he said to conference attendees. But Boeing doesn't expect a plane to get hit by a dozen shocks at once.

"You account for it as much as you can and reduce its impact," Sinnett said. "It's not perfect physics, but it's a black art."

Citation: Airline industry swooping in to prevent cyberattacks (2013, November 8) retrieved 21 May 2024 from https://phys.org/news/2013-11-airline-industry-swooping-cyberattacks.html