AUSTRALIAN AIRPORTS VULNERABLE TO HACKERS

News / Airports / Routes

Australian airports may have a strong safety culture, but they are vulnerable to hackers with malicious intent because they have been focusing more on their physical assets than on their IT systems, says former hacker turned IT consultant Phil Kernick.

Mr Kernick, now the general manager of CQR Consulting, said cyberspace should now be considered the fifth domain of warfare after land, sea, air and space and the image of a hacker as a slightly overweight video game enthusiast sitting in a basement had been replaced by a sophisticated army of attackers.

"When the bad guys are nation-states you can't stop them getting in," he said during a presentation to the Australian Airports Association annual conference in Hobart. He said no precaution would ultimately be good enough to protect against every threat but steps could be taken to lower the risk.

Hacked by ISIS

There has been increased scrutiny on the security of airline systems following an apparent cyber-attack on LOT Polish Airlines computers issuing flight plans in Warsaw in June. In April, Hobart Airport's website was hacked by supporters of radical group Islamic State, although no threat was made against flights in that case.

International Air Transport Association chief executive Tony Tyler in July said airlines were facing "close to an asymmetric warfare" from cyber attackers given the difficulty of defending systems when the threat continually evolved.

"Attacks are happening every day," Mr Kernick said. "Shout out to Hobart Airport. Good work having your website hacked by ISIS. You didn't own it or manage it but it was built by someone else and hosted elsewhere and it wasn't looked after."

Lax Atmosphere

Mr Kernick said it was very easy for someone to place a 4G hacking device aimed at network access into a power point at an airport by perhaps marking it with a label saying "security system" or "environmental system" and adding "do not touch" on it. He said it could also be placed inside an airport carpark, and neither method was likely to attract any attention or security checks.

In the airport industry, workers need to carry access cards once past the security screened area and for access to the tarmac and strict security checks are in place. But Mr Kernick said the heightened security could also lead to a lax atmosphere because everyone assumed someone could not reach a restricted area without the proper access.

"The more you think you do physical security well, the easier the job is [for intruders], because you believe your security works," Mr Kernick said. "This is how they get into bank data centres. It is surprisingly easy."

He said another easy route for hackers would be to send a fake job application with an attachment to the human resources team of an airport and then gain access to the rest of the system.

He said a hacker with malicious intent could cause great damage and disruption by gaining access to the airport's physical systems by locking doors or turning off the air conditioning at a facility in a tropical location. "You are going to have a bad day [if that happens]," he said to the airport operators in the room.

Fifth Domain of Warfare

Mr Kernick said those airports looking to the Australian Security Intelligence Organisation for assistance in the event of a hacking might end up disappointed. In one case he worked on, ASIO knew hackers from a foreign government had access to a business for eight months before it informed the chief executive. ASIO waited in order to monitor the hackers's technique, but t didn't tell the business about it until all of the data was stolen.

"If you think the Australian security services will protect you because you are an airport I wouldn't be that confident," he said.

Mr Kernick said airlines needed to put in place an IT safety officer just as they had safety officers covering physical assets.

"If you want to survive the next decade where cybersecurity is the fifth domain of warfare you need to treat security as safety," he said. "Stop thinking about it as if it is an IT issue because it isn't. If you deal with it like safety you will go a long way to staying safe."

15 OCTOBER 2015

SOURCE: THE SYDNEY MORNING HERALD
ARTICLE LINK:
https://50skyshades.com/index.php/news/airports-routes/australian-airports-vulnerable-to-hackers