Hackers breach US air traffic control computers

8 May 2009

The seal of the Federal Aviation Adminstration (FAA). Hackers broke into US air traffic control computers on several occasions over the past few years and increased reliance on Web applications and commercial software has made networks more vulnerable, according to a government audit.

Hackers broke into US air traffic control computers on several occasions over the past few years and increased reliance on Web applications and commercial software has made networks more vulnerable, according to a government audit.

Among the breaches was an attack on a Federal Aviation Administration (FAA) computer in February 2009 in which hackers gained access to personal information on 48,000 current and former FAA employees, the report said.

In 2006, it said, a viral attack on the Internet spread and forced the FAA to shut down some of its air traffic control (ATC) systems in Alaska.

The audit was conducted by an assistant inspector general in the US Transportation Department and released this week. A copy of the report was obtained by Internet news agency CNET and posted online.

"The need to protect ATC systems from cyber attacks requires enhanced attention because the (FAA) has increasingly turned toward the use of commercial software and Internet Protocol-based technologies to modernize ATC systems," the report said.

It said the use of commercial software and Web applications may increase efficiency but "inevitably poses a higher security risk to ATC systems than when they were developed primarily with proprietary software."

Software vulnerabilities were "especially worrisome at a time when the nation is facing increased threats from sophisticated nation-state sponsored cyber attacks," the report said.

"By exploiting these vulnerabilities, the public could gain unauthorized access to information stored on Web application computers," it said.

"In addition, these vulnerabilities could allow attackers to compromise FAA user computers by injecting malicious code onto the computers," it said.

The report said a security test identified 763 "high-risk" vulnerabilities which could provide an attacker with immediate access into a computer system and allow them, for example, to execute remote commands.

The Wall Street Journal said an FAA spokeswoman, Laura Brown, had rejected some of the report's conclusions, including the extent of the 2006 breach that led to the partial ATC shutdown in Alaska.