GOVERNMENT EXECUTIVE

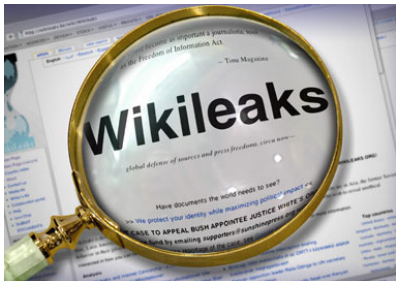
Underwritten by

ArcSight An HP Company

Ten Big Federal Security Breaches

By now, it's no longer news that federal systems, like those of the private sector, other levels of government and foreign countries, are under constant threat. It seems that every day another agency falls victim to a cyberattack.

Here's a look at 10 of the biggest breaches of federal systems ever—several of which, frighteningly, have occurred within the past year.



WikiLeaks

In 2009 and 2010, an Army soldier stationed in Iraq allegedly used his access to SIPRNet and the Joint Worldwide Intelligence Communications System to download military airstrike videos, war documents and more than 250,000 State Department diplomatic cables. The government has charged Pfc. Bradley Manning with passing sensitive data to WikiLeaks, which has made some of the information public. Tim Brown, chief security architect at CA Technologies, says the leak "showed us that the insider is a direct line to sensitive data."

Veterans Affairs

A government laptop stolen from the home of a VA data analyst in 2006 contained Social Security numbers and other personal information for 26.5 million veterans and active-duty troops. A class action suit brought by veterans groups was settled by the agency for $20 million. "Several VA data breaches occurred before and after this big and expensive incident," says Katie Johnson, a spokesperson for Awareity, a risk management company. "Most breaches could have been prevented."

RSA-Lockheed

In May 2011, hackers breached the computer systems of major defense contractors, among them Lockheed Martin, lead contractor of the F-35 fighter jet program, the most expensive weapons program in history. Hackers gained access to the contractors' computer systems after compromising the SecurID system of RSA. Two years earlier, in an unrelated incident, hackers stole terabytes of data on the F-35, reported the *Wall Street Journal*.

Operation Buckshot Yankee

In 2008, a flash drive infected with malicious code was plugged into a military laptop at a base in the Middle East, resulting in "the most significant breach of U.S. military computers ever," said William J. Lynn III, deputy secretary of Defense, in *Foreign Affairs* magazine. The code invaded a network run by U.S. Central Command and established "a digital beachhead from which data could be transferred to servers under foreign control." The incident, says Stewart A. Baker, former assistant secretary for policy at DHS, "is a wake-up call."

Stuxnet

In a cyber reversal, security experts have speculated that the U.S. or Israel was behind a 2010 attack by the computer worm Stuxnet, the first malware created to subvert industrial systems. The attack was on the Natanz uranium enrichment facility in Iran. The worm, which affects the Siemens Supervisory Control And Data Acquisition (SCADA) systems, is believed to have disabled as many as 1,000 gas centrifuges. Some analysts consider the incident to be the first true example of cyber warfare.

Attacks on National Laboratories

During the July 4, 2011, weekend, hackers unleashed sophisticated attacks against the Energy Department's Thomas Jefferson National Accelerator Facility, its Pacific Northwest National Laboratory and Battelle, the contractor that manages PNNL. The attacks disrupted web sites, internal communications and email. "These facilities are responsible for homeland security, nuclear non-proliferation, energy and the smart grid," says A.N. Ananth, CEO of Prism, an IT company. In April, a cyberattack targeted the Oak Ridge National Laboratory, downloading data and disrupting Internet access and email systems.

Senate Hacked

In June 2011, the Lulz Security (or LulzSec) hacker consortium broke into the computer network of the U.S. Senate. The seemingly politically motivated attack followed an assertion by the Pentagon that cyberattacks originating from foreign countries could be treated as acts of war. Then-CIA director Leon Panetta observed that such attacks could disable systems of finance, defense, government and the power grid. The LulzSec attack, however, did not compromise sensitive data, reported the deputy Senate sergeant at arms.

Drone Intercepts

Since at least 2009, militants in Iraq and Afghanistan have used $26 commercial software to intercept live video feeds transmitted by U.S. predator drones operating in those countries, the *Wall Street Journal* reported. The breach is significant because of the ease with which adversaries compromised sophisticated technology to access real-time battlefield information. The intercepts also "mark the emergence of a shadow cyber war within the U.S.-led conflicts overseas," according to the newspaper.

FAA Intrusion

In February 2009, hackers broke into the computer network of the Federal Aviation Administration and gained access to sensitive records, including personnel files of 45,000 FAA employees. President Obama responded by ordering a 60-day cybersecurity policy review. The incident "highlighted the necessity to defend computer networks from cyber intrusions," noted the Center for Strategic and International Studies.

Pentagon Files

In March 2011, a foreign intelligence service stole 24,000 files, which likely were related to the development of new weapons, by hacking into the computer system of an unnamed Defense contractor. "This incident is significant because of the volume of files compromised, the target, and the context in which it was revealed," observes the Center for Strategic and International Studies. The Pentagon disclosed the breach while introducing Defense's new cyber strategy, which seeks to more aggressively identify and disrupt hackers before they strike.