

Federal Computer Week

Number of reported cyber incidents jumps

- By [Ben Bain](#)
- Feb 17, 2009

Federal civilian agencies reported three times as many cyber-related incidents in fiscal 2008 as they did in fiscal 2006 to the Homeland Security Department's office that coordinates defenses and responses to cyberattacks. Meanwhile, an official says the office suspects the actual number of cyber incidents is higher.

The agencies reported to DHS' United States Computer Emergency Readiness Team (US-CERT) a total of 18,050 incidents in fiscal 2008, compared with 12,986 in fiscal 2007 and 5,144 in fiscal 2006, according to DHS officials. Overall, the total number of incidents reported to US-CERT from commercial, foreign, private, and federal, state and local government sectors rose from 24,097 in fiscal 2006 to 72,065 in fiscal 2008.

The Federal Information Security Management Act requires agencies to report cyber incidents, which are defined as acts that violate computer security or acceptable-use policies. The types of incidents include unauthorized access, denial of service, malicious code, improper usage, and scans, probes and attempted access.

Mischel Kwon, US-CERT's director, said that the numbers represent both an increase in malware and improvements in the capabilities of US-CERT and agencies to detect and report cyber incidents.

"As we mature and become more robust, and we deploy more tools, incident numbers will go up," she said. "Both parts of the story are true: There is an increase in mal events, and there is an increase in capabilities in order to detect those mal events."

Kwon added that the numbers were a bit deceiving because the reports are based on manual reporting by agencies and that there are few security operations centers that monitor federal agency networks. She said agencies don't have the tools or analysts to review data to determine if incidents have occurred.

"We feel those numbers are actually very low because it is manual reporting" from the agencies, she said.

US-CERT, the operational arm of DHS' National Cyber Security Division, works to analyze and reduce threat capabilities throughout government and industry, disseminate warning information and coordinate incident response activities. US-CERT also runs Einstein, a federal network-monitoring system. It is in the process of deploying a second version of the system with enhanced capabilities.

Kwon said Einstein is currently deployed at 26 locations across 13 agencies and although many of the incidents are detected through it, the system only allows DHS to see one percent of network traffic amounting to "a very, very small view of the federal civil space."

Kwon added that visibility across the federal network and incident reporting will improve as the second version of Einstein is deployed and agencies continue to reduce the number of connections they have to Internet under the Trusted Internet Connection project.



She said that the trend in incident reporting shows the government is doing the right thing by pursuing the TIC initiative, building security operation centers and by putting an emphasis on understanding incidents more clearly.

According to DHS, reports of unauthorized access to federal government systems jumped from 704 in fiscal 2006 to 2,321 in fiscal 2007 to 3,214 in fiscal 2008. However, incidents categorized as scans, probes and attempted access remained relatively constant with 1,388 reports in fiscal 2006, 1,661 in fiscal 2007 and 1,272 in fiscal 2008. Reports of denial of service incidents fell from 37 in fiscal 2006 to 26 in fiscal 2008.

The data also showed increases for reported federal government incidents that involved malicious code from 1,468 in fiscal 2006 to 2,274 in fiscal 2008 and improper usage up from 637 in fiscal 2006 to 3,762 in fiscal 2008.

Kwon said she thinks that incidents will get easier to discuss in the future as incident-response centers rework the categorization under which incidents are classified.

“We feel the need to upgrade the taxonomy categories because they are really from 2002. We feel like events have changed since then so that’s something to be looked at in the future,” she said.

“The past form of incident response used to be based upon a ticket and it was very stove-piped. Each agency thought their incident had just effected them, and we realized over the past few years that the incidents are actually connected and that it is rare to find an incident that doesn’t affect three or more agencies. We’re all using the same space,” Kwon said.

About the Author

Ben Bain is a reporter for Federal Computer Week.



© 1996-2009 1105 Media, Inc. All Rights Reserved.