NEWS 16 MAY 2013

DHS: Critical infrastructure threats up 68% in 2012

National Cybersecurity and Communications Integration Center (NCCIC) Director Larry Zelvin and NPPD Office of Cybersecurity & Communications acting Assistant Secretary Roberta Stempfley, in written testimony, told the US House Committee on Homeland Security that in 2012, US-CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure and the Department of Homeland Security's industry partners – a staggering 68% increase from 2011.

"The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities," Zelvin and Stempfly said in their testimony.

"Cyber crime also has increased significantly over the last decade," the two noted. "Sensitive information is routinely stolen from private sector and government networks, undermining the integrity of the data contained within these systems."

The US Department of Homeland Security (DHS) currently sees malicious cyber activity from foreign nations and non-state actors engaged in intellectual property theft and information operations, terrorists, organized crime and insiders. Their methods range from distributed denial-of-service (DDoS) attacks and social engineering, to viruses and other malware introduced through remote access, thumb drives, supply chain exploitation and leveraging the access of trusted insiders.

For instance, in March 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December 2011.

"The attacks were highly targeted, tightly focused and well crafted. Stolen information could provide an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems," the two testified. "While there is no evidence that anyone has tried to subvert the operation of these industrial control systems, the intent of the attacker remains unknown. DHS immediately began an action campaign to alert the oil and natural gas pipeline sector community of the threat and offered to provide assistance."

US-CERT also issued more than 7,455 actionable cyber-alerts in 2012 that were used by private sector and government agencies to protect their systems, and had more than 6,400 partners subscribe to the US-CERT portal to engage in information sharing and receive cyber-threat warning information. The NICCIC responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US-CERT to respond to significant private sector

cyber incidents, which includes analyzing data and sharing results, developing mitigation recommendations, and providing alerts and warning to potential future victims.

Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to the DHS's public and private sector partners.

Most recently, DHS has been engaged with private sector and international partners during the series of DDoS incidents on the banking industry over the last few months. DHS provided information to over 120 international partners, many of whom have contributed to mitigation efforts. DHS, along with the FBI and other interagency partners, has also deployed on-site technical assistance to provide in-person support, and has conducted numerous classified briefings on the nature of the threat and mitigation strategies to hundreds of financial sector IT security specialists.

https://www.infosecurity-magazine.com/news/dhs-critical-infrastructure-threats-up-68-in-2012/