NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | September 2, 2015

Recent Threat Analysis

September 2, 2015

Oil and Gas: Industry Among Sectors with Highest Cyber Risk

The NJCCIC assesses with high confidence the cyber risk to the oil and gas industry is high and the energy sector at large is a priority target of foreign intelligence services. While state-sponsored groups have demonstrated the capability to launch cyberattacks that cause physical damage to energy infrastructure, New Jersey's energy sector is most likely to face reconnaissance and intelligence collection activities aimed at exfiltrating data and establishing persistence on high-value networks, for potential use in future sabotage operations. New Jersey's high risk level is largely due to its significance as a major distribution center for petroleum products throughout the Northeast; the Nation's largest production pipeline terminates in Linden and the State is home to three operating oil refineries, over 75 oil and gas companies, and five key interstate natural gas carrier pipelines.

Latest Cyber Alerts

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

NJ CyberLog

September 2, 2015

Insider Threat Demands a Proactive Approach

These days, so much attention is given to external cybersecurity threats that it is often easy to forget insider threats can be just as damaging, especially when it comes to theft of intellectual property, trade secrets, personally identifiable information (PII), and other sensitive data. Insider threats can include current or departing employees, contractors, third party vendors, technicians, business partners, and anyone granted administrator privileges. If organizations do not have the right preventative measures in place and management is not cognizant of the indicators of an inside threat, they are putting themselves at great risk for devastating and potentially irreparable damage.

Tip of the Week

"Don't Fall for Ransomware"

Scammers keep developing new tricks to try to snag money from users; the newer forms of tricks involve the use of ransomware. The scammers will infect vulnerable machines through the use of a computer virus, which will lock your computer and files and demand a payment for its release. These forms of viruses will also try to coerce users into paying a false fine by mimicking local police or security services.

NJCCIC Announcements

On September 16 and 17, the New Jersey Office of Homeland Security and Preparedness (OHSP) and the U.S. Department of Homeland Security (DHS) are collaborating to present a cybersecurity workshop for local businesses and government. Seats are limited to 200 and are filling up quickly. Make your reservation to attend this event through the link provided below.

Managing Cyber Risk for Local Gov't and Small Businesses

Connect with us!

---

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

communications@njohsp.gov
Trenton, NJ | 08625 US