NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Bi-Weekly Cyber Rollup

July 30, 2021

Included In This Summary

Click on the *section header* to go directly to that location in the summary.

NORTH DAKOTA AND REGIONAL

(U) Ransomware Advisory

(U) Attorney General Wayne Stenehjem joins fellow Attorneys General in alerting businesses to take prompt action to protect operations and personal information. “The current proliferation of ransomware attacks throughout the country have thrust to the forefront this critical issue and looming threat and could have unparalleled consequences to consumers, businesses and critical infrastructure,” said Stenehjem. Stenehjem co-chairs the National Association of Attorneys’ General’s Internet Safety/ Cyber Privacy & Security Committee, which serves as a resource for the attorney general community to discuss privacy issues.
Source: (U) https://attorneygeneral.nd.gov/consumer-resources/scam-prevention/ransomware-advisory

(U) Telehealth Usage Rises During Pandemic In North Dakota

(U) Telehealth visits — long-distance meetings of patients and doctors via technology — have increased during the pandemic, according to the federal Centers for Disease Control and Prevention. From late June to early November of last year, an average of about 30% of health care visits took place using telehealth. The agency also found that weekly telehealth visits dropped as COVID-19 cases declined and rose when cases increased.
Source: (U) https://www.govtech.com/news/telehealth-usage-rises-during-pandemic-in-north-dakota

(U) BEK Communications Cooperative Acquires Cybernet Security

(U) John Nagel, CyberNet Security founder and CEO, is an entrepreneur and native North Dakotan who formed the company in 2017. In addition to becoming BEK’s chief security officer and vice president of market development, Nagel will continue to lead the cybersecurity business. “We are thrilled to join forces with BEK in bringing cyber security services to their customers and expanding cyber security offerings to North Dakota businesses and the nine other states BEK serves today," he said.
Source: (U) https://www.jamestownsun.com/business/announcements/7120435-BEK-Communications-Cooperative-acquires-CyberNet-Security

(U) FMWF Chamber to Host Cybersecurity Session Aug. 19

(U) The Fargo Moorhead West Fargo Chamber of Commerce will host "The Urgency for Cybersecurity," a session on protecting your organization from cyber threats, from 8 a.m. to noon Aug. 19 at the Holiday Inn, 3803 13th Ave. S. John Bonhage, a special agent with the FBI in Minneapolis, will deliver the keynote presentation, "How the FBI is tackling the cyber threat - What we are seeing and what is of concern," at 11 a.m. at the Holiday Inn in Fargo.
Source: (U) https://www.inforum.com/business/7127806-FMWF-Chamber-to-host-cybersecurity-session-Aug.-19

NATIONAL

(U) United States Senate and Transportation Security Administration Take Steps Toward Expanding Cybersecurity Requirements

(U) Last week, the United States Senate and the Transportation Security Administration (TSA) each took steps toward expanding cybersecurity requirements for private sector entities. Meanwhile, TSA issued its second Security Directive since the Colonial Pipeline ransomware attack, setting forth cybersecurity requirements for critical pipelines.
Source: (U) https://www.mondaq.com/unitedstates/security/1097488/united-states-senate-and-transportation-security-administration-take-steps-toward-expanding-cybersecurity-requirements

(U) Pipeline Operators Raise Concerns Over Aggressive TSA Cybersecurity Directives

(U) Since the Transportation Security Administration (TSA) announced two pipeline-specific cybersecurity directives in May, pipeline operators have voiced concerns about aggressive timelines and impacts on safety if major equipment changes become necessary, according to TSA Administrator David Pekoske, during a Senate hearing Tuesday. Companies running pipelines are, for the first time, working under required cybersecurity measures. "They say that the directive could require them to replace thousands of pieces of equipment all over the country. Not only would it be expensive, take a long time, [but] supply chain shortages are an issue," Sen. Marsha Blackburn, R-Tenn., said during the hearing.
Source: (U) https://www.utilitydive.com/news/pipeline-cyber-security-tsa-requirements/604216/

(U) Biden Pushes Cybersecurity Upgrades for Critical Infrastructure After Recent Hacks

(U) President Biden just signed a national security directive aimed at boosting defenses against ransomware attacks and the hacking of critical infrastructure like energy, food, water, and power systems. The directive sets performance standards for technology and systems used by private companies in those sectors — though it can't force those companies to comply. For reference, almost 90% of the country's critical infrastructure is owned and run by the private sector, and the government has limited authority over their cybersecurity requirements. But the official says the Biden administration may pursue legislative options, with help from Congress, to require the kind of technological improvements that would defend against such cyberattacks.
Source: (U) https://www.npr.org/2021/07/28/1021742325/biden-pushes-cybersecurity-upgrades-for-critical-infrastructure-after-recent-hac

(U) Senate Reviews Cybersecurity Threats to US Water Systems

(U) Officials and water sector professionals warned of ongoing cybersecurity vulnerabilities in the nation’s water and wastewater utility infrastructure at a Senate hearing on escalating cyber-attacks against U.S. utilities and water-management organizations. “I believe that the next Pearl Harbor, the next 9/11 will be cyber, and we are facing a vulnerability in all of our systems, but water is one of the most critical and I think one of the most vulnerable,” said Sen. Angus King (I-Maine), co-chairman of the Cyberspace Solarium Commission to the Senate Environment and Public Works Committee, on July 21.
Source: (U) https://www.enr.com/articles/52173-senate-reviews-cybersecurity-threats-to-us-water-systems

INTERNATIONAL

(U) China Finalizes Data Security Law

(U) On June 10, 2021, the final version of Data Security Law (DSL) of the People's Republic of China was published, and the DSL will take effect Sept. 1, 2021. While the DSL provides for a three-level data classification system, the obligations for each classification level are described in vague and broad terms.
Source: (U) https://www.natlawreview.com/article/china-finalizes-data-security-law

(U) Iran's Secret Cyber Files

(U) Classified documents, allegedly from Iran, reveal secret research into how a cyber attack could be used to sink a cargo ship or blow up a fuel pump at a petrol station. The internal files also include information on satellite communication devices used by the global shipping industry as well as a computer-based system that controls things like lights, heating and ventilation in smart buildings across the world. The papers appear to reveal a particular interest in researching companies and activities in western countries, including the UK, France and the United States.
Source: (U) https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871

(U) Russia, US Launch Cybersecurity Dialogue, Three Rounds Already Held, Says Diplomat

(U) Russia and the US have launched bilateral cybersecurity dialogue Russian Deputy Foreign Minister Sergey Ryabkov told reporters on Wednesday. "We are beginning to have a better understanding of security issues in the cyber sphere […] starting with the use of the corresponding malware with criminal intent and ending with targeting critical infrastructure objects online. They need an in-depth professional discussion on a bilateral basis, and this dialogue has been launched," he said.
Source: (U) https://tass.com/politics/1320507

(U) Hackers Used Never-Before-Seen Wiper in Recent Attack on Iranian Train System

(U) Researchers with cybersecurity company SentinelOne reconstructed the recent cyberattack on Iran's train system in a new report, uncovering a new threat actor and a never-before-seen wiper. On July 9, local news outlets began reporting on a cyberattack targeting the Iranian train system, with hackers defacing display screens in train stations by asking passengers to call '64411', the phone number of Iranian Supreme Leader Khamenei's office.
Source: (U) https://www.zdnet.com/article/hackers-used-never-before-seen-wiper-in-recent-attack-on-iranian-train-system-report/

Email: ndslic@nd.gov NDSLIC: 701-328-8172