Included In This Summary
Click on the section header to go directly to that location in the summary.

NORTH DAKOTA AND REGIONAL
(U) BSC Hosted Third Annual CyberCon October 6th-7th
(U) North Dakota Launches Statewide Cybersecurity Campaign
(U) NDIT is Working with Colleges to Make Education More Cyber-safe
(U) Kratos Participates in North Dakota’s Innovation Day

NATIONAL
(U) Illinois Community College Addressing Cybersecurity Breach
(U) ACLU Raises Questions About Massachusetts Data Privacy
(U) Russian Who Hacked LinkedIn, Dropbox Sentenced to 7 Years in Prison
(U) 55 New Security Flaws Reported in Apple Software and Services

INTERNATIONAL
(U) Chinese APT Group Targets Media, Finance, and Electronics Sectors
(U) Researchers Uncover Cyber Espionage Operation Aimed at Indian Army
(U) Critical Flaws Discovered in Popular Industrial Remote Access Systems
(U) Researchers Find Vulnerabilities in Microsoft Azure Cloud Service
NORTH DAKOTA AND REGIONAL

(U) BSC Hosted Third Annual CyberCon October 6th-7th
(U) Bismarck State College’s third Annual CyberCon was hosted this past week on October 6th and 7th. North Dakota’s Chief Information Officer Shawn Riley and Chief Information Security Officer Kevin Ford delivered presentations, as well as several other members of North Dakota’s cyber security community of professionals. Source: (U) https://bismarcktribune.com/news/state-and-regional/third-annual-cybercon

(U) North Dakota Launches Statewide Cybersecurity Campaign
(U) North Dakota Information Technology (NDIT) has launched “DefeND,” a new statewide awareness campaign designed to educate North Dakotans about the dangers that lurk in cyberspace. The campaign will run on TV and digital channels over the next several months and is designed to alert citizens to common threats and security mistakes, such as phishing, weak passwords, sharing personal information online and other vulnerabilities. Source: (U) https://www.govtech.com/security/North-Dakota-Launches-Statewide-Cybersecurity-Campaign.html

(U) NDIT is Working with Colleges to Make Education More Cyber-safe
(U) North Dakota IT and the state’s university system are partnering to make colleges more cyber-safe. This isn’t a new partnership. They’ve worked together for several years in securing these large educational facilities that are naturally prone to cyber-attacks. North Dakota University Systems is still in charge of cybersecurity for the schools, but now, NDIT is providing a cyber tool kit to enhance that effort. Source: (U) https://www.kxnet.com/ndit-is-working-with-colleges-to-make-education-more-cyber-safe/

(U) Kratos Participates in North Dakota’s Innovation Day
(U) Kratos Defense & Security Solutions, a leading National Security Solutions provider and industry-leading provider of high-performance unmanned systems, participated in North Dakota’s Innovation Day on Autonomous Systems Policy. At the event at Grand Farm in Horace, ND, Kratos showcased its Autonomous Truck-Mounted Attenuator (ATMA), a driverless version of the mobile crash barriers utilized for road construction and highway maintenance vehicles, shielding workers and equipment ahead from errant drivers entering the work zone. Source: (U) https://news.yahoo.com/kratos-participates-north-dakota-innovation-120000739.html
NATIONAL

(U) Illinois Community College Addressing Cybersecurity Breach
(U) Heartland Community College in Normal, Ill., is working with outside consultants to address a security breach in its computer system. The college’s online operations, including classes, remained shut down on Tuesday morning as a safety measure after the college detected an outside source had compromised some of its systems on Monday, college officials said. The college said the shutdown was part of an effort to investigate and contain the security breach. "The college is not aware of any student or personnel data compromised by this action," the college said in a statement.

(U) ACLU Raises Questions About Massachusetts Data Privacy
(U) The American Civil Liberties Union of Massachusetts (ACLU) is seeking information from state education agencies about how they are working to protect the privacy of both K-12 and college students amid the coronavirus pandemic. Despite the fact that remote education is now the norm in Massachusetts and “not the exception,” the state still lacks sufficient privacy protections to ensure students are not being improperly monitored or tracked by corporations and the government, Kade Crockford, director of the ACLU’s Technology for Liberty program, wrote in a statement.

(U) Russian Who Hacked LinkedIn, Dropbox Sentenced to 7 Years in Prison
(U) A Russian hacker who was found guilty of hacking LinkedIn, Dropbox, and Formspring over eight years ago has finally been sentenced to 88 months in United States by a federal court in San Francisco. Yevgeniy Aleksandrovich Nikulin, 32, of Moscow hacked into servers belonging to three American social media firms, including LinkedIn, Dropbox, and now-defunct social-networking firm Formspring, and stole data on over 200 million users.

(U) 55 New Security Flaws Reported in Apple Software and Services
(U) A team of five security researchers analyzed several Apple online services for three months and found as many as 55 vulnerabilities, 11 of which are critical in severity. The flaws — including 29 high severity, 13 medium severity, and 2 low severity vulnerabilities — could have allowed an attacker to "fully compromise both customer and employee applications, launch a worm capable of automatically taking over a victim’s iCloud account, retrieve source code for internal Apple projects, fully compromise an industrial control warehouse software used by Apple, and take over the sessions of Apple employees with the capability of accessing management tools and sensitive resources."
Source: (U) https://thehackernews.com/2020/10/apple-security.html
INTERNATIONAL

(U) Chinese APT Group Targets Media, Finance, and Electronics Sectors
(U) Cybersecurity researchers uncovered a new espionage campaign targeting media, construction, engineering, electronics, and finance sectors in Japan, Taiwan, the U.S., and China. Linking the attacks to Palmerworm (aka BlackTech) — likely a China-based advanced persistent threat (APT) — Symantec's Threat Hunter Team said the first wave of activity associated with this campaign began last year in August 2019, although their ultimate motivations remain unclear. "While we cannot see what Palmerworm is exfiltrating from these victims, the group is considered an espionage group and its likely motivation is considered to be stealing information from targeted companies," the cybersecurity firm said.

(U) Researchers Uncover Cyber Espionage Operation Aimed at Indian Army
(U) Cybersecurity researchers uncovered fresh evidence of an ongoing cyberespionage campaign against Indian defense units and armed forces personnel at least since 2019 with an aim to steal sensitive information. Dubbed "Operation SideCopy" by Indian cybersecurity firm Quick Heal, the attacks have been attributed to an advanced persistent threat (APT) group that has successfully managed to stay under the radar by "copying" the tactics of other threat actors such as the SideWinder.

(U) Critical Flaws Discovered in Popular Industrial Remote Access Systems
(U) Cybersecurity researchers have found critical security flaws in two popular industrial remote access systems that can be exploited to ban access to industrial production floors, hack into company networks, tamper with data, and even steal sensitive business secrets. The flaws, discovered by Tel Aviv-based OTORIO, were identified in B&R Automation's SiteManager and GateManager, and MB Connect Line's mbCONNECT24, two of the popular remote maintenance tools used in automotive, energy, oil & gas, metal, and packaging sectors to connect to industrial assets from anywhere across the world.
Source: (U) https://thehackernews.com/2020/10/industrial-remote-access.html

(U) Researchers Find Vulnerabilities in Microsoft Azure Cloud Service
(U) According to the latest research, two security flaws in Microsoft’s Azure App Services could have enabled a bad actor to carry out server-side request forgery (SSRF) attacks or execute arbitrary code and take over the administration server. "This enables an attacker to quietly take over the App Service's git server, or implant malicious phishing pages accessible through Azure Portal to target system administrators," cybersecurity firm Intezer said in a report published and shared with The Hacker News. Discovered by Paul Litvak of Intezer Labs, the flaws were reported to Microsoft in June, after which the company subsequently addressed them.
Source: (U) https://thehackernews.com/2020/10/microsoft-azure-vulnerability.html