Ag, food industries should prepare for cyberattacks

By Jennifer Whitlock
Texas Farm Bureau
Field Editor

In an increasingly digital world, federal agencies say critical infrastructure industries of the United States - including agriculture - are being targeted for cyberattacks.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and National Security Agency (NSA) released an alert in mid-October warning the food and agriculture sector to beware of BlackMatter ransomware attacks, in which an organization's electronic data are encrypted and held hostage by hackers until a ransom is paid to restore access.

Since July, BlackMatter, a Russian cybercrime cell, has targeted many critical infrastructure entities, including two in the food and agriculture sector.

BlackMatter is a ransomware-as-a-service tool, meaning the developers profit from cybercriminal affiliates who deploy it.

A separate private industry notification from the FBI's Cyber Division in September noted one U.S. bakery company lost access to its computer systems in July through a ransomware attack, halting production, shipping and receiving for one week.

"Ransomware may impact businesses across the sector, from small farms to large producers, processors and manufacturers, markets and restaurants," the FBI stated.

Financial loss, loss of productivity, remediation costs, loss of proprietary information or personally identifiable information and reputational damage are just some of the losses businesses may incur from a ransomware or cyberattack, according to the FBI.

An Iowa grain cooperative, NEW Cooperative, was also recently targeted, with BlackMatter attackers demanding $5.9 million to restore access to its data. The systems attacked controlled crop irrigation, livestock feed schedules and inventory distribution, a letter from Iowa Sens. Chuck Grassley and Joni Ernst to the Department of Homeland Security (DHS) said.

"NEW Cooperative controls 40% of the grain distribution in the country," the senators wrote. "The company's rapid return to alternative operations averted a crash in grain prices, but the threat of continued attacks has dire consequences."

The legislators asked DHS to further investigate recent BlackMatter attacks and to explain how the agency is preparing the agricultural sector against future incidents.

BlackByte, another ransomware group, claims it attacked Farmers Cooperative Elevator Co. in Iowa. They threatened to release sensitive data - such as sales, financial and accounting information - if the ransom wasn't paid.

"The extent of the damage from the NEW Cooperative and Farmers Cooperative Elevator Co. attacks is not isolated to the grain market. Feed from the cooperatives' grain supply sustains millions of livestock," the senators said. "These attacks will affect the supply chain that puts food on the shelves in grocery stores across the country."

Ongoing ransomware attacks affecting the food and agriculture sector demonstrates the importance of cybersecurty as an element of supply chain security, the agencies said.

To prevent ransomware or cyberattacks, individuals and businesses should take proactive measures, including the use of strong passwords, routine update and backup procedures and implementing multi-factor authentication, according to the CISA, FBI and NSA alert.

Strong passwords should not contain personal information like a birth date, address or phone number, because that information is readily available online and easy to guess. CISA advises using both upper and lowercase letters, numbers and special characters in creating strong passwords.

Multi-factor authentication often requires a code sent directly to the user's associated phone number or email to complete logging into a device, making it less likely a random hacker can gain access.

Security basics like keeping operating systems and web browsers up to date, using antivirus software and backing up data in case it is lost or damaged can help keep systems protected, as well.

"The threat of ransomware goes beyond specific impacts to a victim company. It has risen to a national security issue," Rob Joyce, NSA director of Cybersecurity, said in a statement. "Employing the mitigations in the joint advisory with CISA and FBI will protect networks and mitigate the risk against BlackMatter and other ransomware attacks."

JBS, one of the world's largest meatpackers, was hit by a cyberattack in June, which forced the shutdown of several slaughterhouses.

Other cyberattacks in the food and agriculture sector have happened throughout the year, and the U.S. Senate Judiciary Committee held a hearing about the threat of ransomware attacks in late July.

For more information and best practices on securing computer systems, visit stopransomware.gov.

These photos conclude the submissions of your Halloween cuties! Thank you for your participation!