SMART AGRICULTURE IS A GROWING FIELD FOR CYBER THREATS

Introduction

Expanding technologies and supply chain

The COVID-19 pandemic has introduced dynamic changes for global agriculture. As the sector recovers from disrupted patterns of food consumption, impacted labor supply, and disrupted transportation across national borders; heat, droughts, and floods continue to add to producers' concerns. Moreover, price fluctuations due to international market conditions are creating uncertainty in futures markets that are of great concern to farmers hedging prices.

To cope with uncertainties, the agriculture industry is looking to precision farming technology. It promises to improve efficiency operations in the field as well as integration with agribusinesses concerned with purchasing, storage, transportation, and processing. One study reported that those adopting precision farming increased crop production by 11 percent while lowering input expenses by 9 percent on average.[1]

However, as is so often the case across most industries, efficiency gains from new technology comes at a price with increased vulnerability to cybercrime topping the list.

Why insecurities in supply chain matter

In the past, cyberattacks on farmers and agribusinesses typically used phishing, social engineering, and other malware such as banking Trojans to steal money from farmers' online banking and trading accounts. However, the recent sophisticated attack on meatpacking giant JBS USA proved cybercriminals will spare no industry, including those feeding the world. Attacks have graduated from one-off "retail" level attacks to "wholesale" attacks that simultaneously impact a broad segment of agriculture through sophisticated ransomware.

One Sunday morning, the IT staff at JBS discovered that ransomware had encrypted JBS' mission-

[1] Mario Paez, Dealing with Increasing Cyber Risks in Agriculture, Marsh and Mclennan Agency, March 10, 2021. https://www.marshmma.com/blog/client-advisory-or-dealing-with-increasing-cyber-risks-in-agriculture

critical files. To resume operation, JBS paid the attackers $11 million in Bitcoin.[2] Meat producers scrambled to find new buyers as well as grocery chains and restaurants who suddenly had to deal with higher costs from supply shortages.[3]

Agriculture has become a growth market for cybercrime. In 2020, agriculture companies in the U.S. suffered a 600 percent increase in data breaches compared to 2019.[4] As the digital transformation takes hold in agriculture, the types and numbers of cyber attacks will only increase.

> The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as a pill and large as an airplane, into a part of the IoT. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us more smarter and more responsive, merging the digital and physical universes.[5]

[2] Dustin Volz, JBS Paid $11 Million to Resolve Ransomware Attack, WSJ, June 10, 2021. https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

[3] Jacob Bunge and Jessica Newman, Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants, Wall Street Journal, June 11, 2021. https://www.wsj.com/articles/ransomware-attack-roiled-meat-giant-jbs-then-spilled-over-to-farmers-and-restaurants-11623403800

[4] Jacob Bunge, Food Giant ADM Bolsters Its Defense Against Hacks, CEO Says, Wall Street Journal, June 24, 2021 https://www.wsj.com/articles/agriculture-giant-adm-is-shoring-up-cyber-defenses-ceo-says-11624555232

[5] "What is the IoT? Everything you need to know about the Internet of Things right now," by Steve Ranger, ZDNet, February 3, 2020

Emerging Ag Technology Increases Threat Surfaces

Precision technologies are creating an agriculture internet of things. These include sensors, autonomous farm equipment, and various robots reducing or eliminating human labor with a variety of tasks. Furthermore, today's cutting-edge farmers are using artificial intelligence and data analytics to improve production. Data-driven planting uses sensors to assess crop and soil conditions, pests, and more. In addition, sensors monitor temperatures during food processing and transportation to prevent spoilage.

Increasingly, farms are also using driver-assisted and fully autonomous farm equipment as well as and robotic devices to remediate issues found by sensors in every phase of crop cycles from plowing, to planting to harvesting and delivery. Likewise, sensors and robots are in evidence in livestock operations for monitoring and emending feed consumption, recording animal weight and in other parts of the cycle. This is just the beginning. Charles Sturt University (CSU) in Australia is creating a "hands-free" smart farm in which robots do all the work without any human workers.[6]

Each of these devices and the software that runs them and the networks that connect them are entryways for cyber attacks on farms and their agribusiness partners. This is because sensors and robotic devices constantly exchange data via APIs across the Internet.[7] Attackers can insert malware such as ransomware into these data streams or disrupt data with denial of service attacks. One could imagine some smart college students inserting a Remote Access Trojan (RAT) to create crop circles using a farmer's own cultivator or harvester. In addition, as large buyers like Cargill send price information to farmers via their smartphones, even phones can become an attack vector for stealing farmers' account credentials and for other attacks.

Adding to the complexity of securing Ag IT environments is the use of cellular, Bluetooth, and Wi-Fi networks as well as USB drives to transfer data. Each method of data transfer presents its own threats on top of threats to hardware and software. Because of the complexity of Ag IT environments, information firms that specialize in agriculture – if compromised by attackers – are potential sources of supply-chain attacks that introduce malware to large numbers of farm IT environments through normal software updates and patches.[8]

---

[6] Mike Levin, The Rising IoT Threat to the Agriculture Industry and the Global Food Supply, F5 .com, September 15, 2020. https://www.f5.com/labs/articles/threat-intelligence/the-rising-iot-threat-to-the-agriculture-industry-and-the-global-food-supply

[7] Ibid.

[8] Payal Dhar, Cybersecurity Report: "Smart Farms" Are Hackable Farms, IEEE Spectrum, IEEE Spectrum, May 2021. https://spectrum.ieee.org/riskfactor/telecom/security/cybersecurity-report-how-smart-farming-can-be-hacked

> The reality of security today is that security leaders have too many tools. Gartner found, in the 2020 CISO Effectiveness Survey, that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more. Too many security vendors results in complex security operations and increased security headcount.[9]

Consolidated Security Architecture for Agriculture

As farms and Ag businesses begin to rival manufacturing and retail sectors in the complexity of their networking environments, experts acknowledge that it can take up to 60 different cybersecurity engines to provide effective protection against today's sophisticated multi-vector threats. As agriculture increases cyber security measures, it is tempting to add point solutions to secure new assets as you bring them online.

However creating a patchwork of standalone security solutions has severe drawbacks.

First, using a mass of point solutions is unwieldy and costly end-to-end from sourcing, to installation, to daily administration and management. A farm's limited IT staff must monitor and manage each security control separately, which creates an enormous workload. This large workload leads to mistakes such as missing attacks in progress and causing security misconfigurations that let attacks through defenses. In addition, point solutions can leave gaps in security coverage. One answer for agriculture organizations is to consider the merits of a consolidated security architecture.

Consolidated security architecture provides all of the security engines needed to protect against attacks on: Ag IoT devices; accounting, management and other software as a service applications; email, Internet, networks, smartphones, endpoints, cloud deployments, encrypted traffic, networks and other infrastructure elements. Importantly, consolidated security architecture ensures compatibility of all security controls as well as lets administrators monitor and manage all security through a single user interface. This lowers the burden on IT and security staffs which promotes greater accuracy during event response and administering security configurations.

[9] "Gartner Top Security and Risk Trends for 2021," by Gartner, April 5, 2021

Now, consolidated security architecture is being enhanced with artificial intelligence (AI) to make security operate more autonomously from human control. This takes tasks like classifying threats and making policy updates out of the hands of staff members to reduce labor costs and improve threat prevention. AI support makes changes to security policies almost instantaneous across hundreds of gateways. At the same time an AI-guided security architecture can optimize the performance of network resources to minimize latency, improving service levels.

Digital information technology is driving the largest change in agriculture since the introduction of steam engines. For commercial farmers and Ag businesses, there is no going back. Embracing consolidated security architecture enhanced by artificial intelligence to streamline cybersecurity is the next transitional step for Agriculture.

To understand more about supply chain attacks, visit this page.

To learn what IoT security solutions you should invest in, download the The Ultimate Guide for Delivering IoT Security, an IDC Technology Spotlight.

To learn how to benefit from reduced TCO and increased protection with a consolidated security architecture, check out Check Point Infinity.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com