ALLIANCE™
(https://www.globalseafood.org)

Responsible Seafood ADVOCATE

Intelligence

How vulnerable are seafood companies to cybercrime? More than they might think

15 November 2021

By Hank Hogan

Cybercrime, in particular ransomware, is a potential problem for aquaculture firms, but protective steps can be taken

In January, aquaculture equipment supplier Akva Group became a cybercrime victim, with a ransomware attack reportedly costing the company $6 million in the first quarter. Beyond acknowledging the attack and its impact, Akva declined to further comment. However, the incident could be a sign of things to come as others in the aquaculture industry could soon be targeted.

In September, the United States Federal Bureau of Investigation (FBI) warned of cybercriminals targeting the food and agriculture sector, listing a string of incidents in a Private Industry Notification. It's part of a growing threat: According to the cybersecurity company PurpleSec, the worldwide damage from ransomware jumped from $11.5 billion in 2019 to $20 billion in 2020.

In ransomware attacks and other cybercrime, an attacker first gains access, perhaps by tricking victims into downloading malicious software. Using this so-called malware, criminals can then scout out the

Software updates, multi-factor authentication and limiting unnecessary connections to the Internet can minimize the impact of cybercrime.

network to find and manipulate sensitive data. Attackers could, for instance, export the data but otherwise keep quiet about the breach. In ransomware, on the other hand, the criminal locks down the data and sends a threatening note demanding payment to unlock it.

A confluence of factors contributed to recent the growth of these attacks, said Matthew Radolec, senior director of incident response and cloud operations at the data security company Varonis. Pandemic misinformation resulted in the circulation of a multitude of emails inviting users to click on a link, which would unleash malware. More employees worked remotely since the Covid-19 pandemic began, and often on a wider array of devices, which opened up new attack avenues.

“There are a lot more ways to get in than there were before,” Radolec noted.

And it became easier and easier to exchange large amounts of hard-to-track cryptocurrency, the cybercriminal's preferred way to get paid. The result, according to Radolec, is a perfect cybercrime storm.

In fact, current conditions are so favorable that there's a whole industry dedicated to these criminal activities. Criminal groups, according to cybersecurity firms, are offering ransomware as a service, a business model that leases malware to anyone who signs up. The cost can range up to several thousand dollars. That's a small sum compared to the **almost quarter-million dollars average ransom demand** (https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020) in Q3 2020 and more than $150,000 average demand in Q4 2020, according to ransomware analysis firm Coveware.

Those ransoms are set so that the cost seems worth it, especially as compared to the hit that can come from something like a fish packaging operation shut down for days or weeks, Radolec pointed out. After collecting a payoff, though, criminals can threaten to leak sensitive information or contact customers to create brand damage. These extra extortion attempts are possible because the criminals are likely still in the network and will almost certainly have made a copy of any acquired data, Radolec said.

"It is, frankly, a very gloomy ecosystem right now for a lot of companies," he admitted.

Some things will help, he quickly added, like new technologies and procedures. These will require investments of time, money and energy, along with in-house or outsourced technical expertise.

Blockchain expands its aquaculture presence with shrimp and salmon

By tracking products from farm to plate, blockchain helps reduce fraud and improve standing with consumers. But it's only part of the solution.

Global Seafood Alliance 0

On the technology side, many cyberattacks use exploits that have been around for years and for which there are patches, some more than five years old, that fix the software holes that let attackers in. So, the technology basics, which include regular patching of software, are critical.

Just as important is beefing up security through procedural changes like multi-factor authentication. In this approach, a password by itself is not enough to gain access to a system. Instead, users must also enter a code texted to a phone or otherwise authenticate themselves. Such extra verification can stop attackers even after they steal a password or trick someone into revealing it.

A third part of the solution is design and philosophy, which means fresh thinking about cybersecurity like physical security. In the physical world, there will be a fence, and often cameras and people looking at it. Employees wear badges and lock important items away. Keeping an eye on things, cybersecurity-wise, can be part of a similar defense-in-depth solution.

When implementing these countermeasures, Radolec challenged firms, particularly smaller ones, to think about the value versus the cost of connectivity. In cybersecurity circles and in the FBI industry alert, the recommendation is for air gaps, or physical barriers, that separate sections of a network or portions of data from everything else.

An example might be a computer that monitors a pump that circulates water in a tank. If the computer connects to nothing else, then it has an air gap between it and the rest of the world. Another instance might be a disk that stores backup data, with the disk only connected during a backup. The rest of the time there is an air gap between the disk and everything else.

As can be seen, an air gap may be permanent, or it could be one where something or someone makes and breaks a connection. An air gap, especially one involving a manual connection and disconnection, can be cumbersome. But the cost may be acceptable if it keeps a company's crown jewels safe.

For the aquaculture industry, Radolec put it this way: "The things you use to catch the fish or farm the fish, do they really need to be connected to the Internet?"

Follow the *Advocate* on Twitter @GSA_Advocate (https://twitter.com/GSA_Advocate)

Author

HANK HOGAN

Hank Hogan is a freelance writer based in Reno, Nevada, who covers science and technology. His work has appeared in publications ranging from Boy's Life to New Scientist.