TechXplore

Ransomware attack on sheep farmers shows there's no room for woolly thinking in cyber security

6 March 2020, by Roberto Musotto and Mostafa Naser

Credit: Shire of Katanning

While many Australians were preoccupied with panic-buying toilet paper, sales of another commodity encountered a very different sort of crisis.

Wool sales were severely disrupted last week by a ransomware attack on IT company Talman Software, which processes more than 75% of sales in Australia and New Zealand.

A ransomware attack is a form of cyber-extortion, involving software that encrypts all of the files on a system. In this case, cyber-criminals then demanded A$8 million to unlock the files. Talman has refused to pay and has instead built a replacement version of the software.

Wool sales were halted for several days and hastily rescheduled, with an estimated 70,000 bales held in limbo. The industry's turnover in a typical week is up to A$80 million, but prices may now drop as the postponed sales cause a glut in the market.

A ransomware attack on such an important sector of Australia's economy shows how vital it is for authorities to defend markets against cyber threats. It is a matter of when, not if, these attacks will happen. There is a ransomware attack on a business every 14 seconds and by 2021 it will be every 11 seconds.

Diverse defences

How do we improve our resilience? One way is to avoid being too dependent on particular technologies. The wool industry already knew Talman Software's dominant role represented a significant vulnerability.

Having a wider choice of software providers, not to mention an offline alternative, would have reduced or avoided the disruption.

Previous ransomware attacks on vital infrastructure, including last month's attack against Toll Group, have shown the need for companies to keep their operations and IT systems separate.

We can define "operations" as the software and hardware that allow a company to keep its assets and processes working. IT systems, meanwhile, are the software and hardware that handles the company's information and data.

Separating the two would make it harder for hackers to disrupt a company's operations by invading its IT system. However, this would make it impossible to use IT systems to control operations remotely, which would bring its own pros and cons. Imagine a nuclear power plant—do you fit it with a remote shutdown option that could be crucial in an emergency but might also become a tempting target for hackers?

Governments need to help

This issue is bigger than simply a threat to companies' profits. Although the latest attack targeted a commercial company, it damaged the economic welfare of farmers in two countries.

Fending off future attacks shouldn't be a job just for companies seeking to safeguard their own profits—governments need to help too.

Governments should have a cyber-resilience unit that supports businesses in such emergencies. They should also provide support funds for victims, and national compulsory cyber insurance to guarantee the least disruption possible.

Governments need to defend public and economic infrastructure such as transport networks, power grids and important commercial markets.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

APA citation: Ransomware attack on sheep farmers shows there's no room for woolly thinking in cyber security (2020, March 6) retrieved 29 September 2022 from https://techxplore.com/news/2020-03-ransomware-sheep-farmers-room-woolly.html