https://buffalonews.com/news/local/experts-say-ransomware-attack-on-buffalo-public-schools-should-have-been-anticipated/article_60a77598-8446-11eb-8b6b-d3137700ab43.html

Experts say ransomware attack on Buffalo Public Schools should have been anticipated

Sandra Tan
Mar 13, 2021

New and repaired Buffalo Public Schools laptop computers.

Harry Scull Jr./News file photo

Sandra Tan

Buffalo Public Schools leaders were taken by surprise by the ransomware attack on the district's network Friday. But they shouldn't have been.

Cybercriminals are particularly fond of targeting government agencies and school districts, which are generally less likely to devote the financial resources necessary to guard against attacks, according to cybersecurity experts.

"It’s very common for schools to be targeted," said Holly Hubert, founder of Amherst-based GlobalSecurityIQ.

According to the K-12 Cybersecurity Resource Center, nearly 350 cyberattacks on school districts or educational agencies were publicly reported in 2019, three times more incidents than the year before. But that figure has been rising over the past year.

Close to home, the Victor Central School District near Rochester was down for a week early last month due to a ransomware attack.

Not only are school districts less likely to hire cybersecurity experts or invest in the outside services needed to prevent ransomware and other cybersecurity attacks, experts said, but school districts have become even more vulnerable because they've had to fast-track new remote learning models due to the coronavirus pandemic.

"They were trying to do the best they could to keep things moving, but obviously if you move too quick, you’re going to leave vulnerabilities that people can take advantage of," said Kyle Cavalieri, president of the Buffalo-based Avalon Cyber, which has offices in multiple states.

He referenced information from the FBI and Department of Homeland Security stating that more than half of reported ransomware attacks on state and local governments and schools in August and September involved schools, which keep valuable, confidential information and are less likely to have top-level cybersecurity.

"They’re kind of low-hanging fruit," he said.

And ransomware is only one type of cybersecurity threat.

Cavalieri, whose company has worked with roughly half a dozen schools and districts to address cybersecurity incidents over the past year, said he worked with a Long Island school that had its website defaced. Not only was the main website altered, but the criminal hackers also managed to access Zoom meetings for classes, change school grades, and send emails to parents and students.

That school, North Shore Hebrew Academy, had anti-Semitic slurs and Nazi images posted on its website, followed later by Zoom class break-ins. It subsequently made national news in December.

"It was terrible," said Cavalieri, whose company has been cooperating with the FBI to investigate the attack.

For schools and districts he's dealt with, he said, getting schools back online has ranged from days to weeks.

Experts say that the length of time it will take for the Buffalo Public Schools to get back online depends on the district's backup measures and advance planning.

"It depends on their level of preparedness," Hubert said.

Cavalieri said the Buffalo Public Schools are likely in the process of working with GreyCastle Security to figure out not only how the attacker got into the network to take it over, but also whether there are any other back-door mechanisms left by the bad actor that are sitting dormant, waiting to be opened if the main hole in the system gets plugged.

"These types of things just take time," he said.

The pressure to get the school district network up and running is immense since many students are still working remotely, and the district has been preparing to bring more grades back into the classroom starting Monday.

"The District is working with technology industry experts and law enforcement authorities to resolve the ransomware attack we experienced on Friday morning. We are continuing to work throughout the weekend to protect and recover our information systems. We will let you know by Sunday afternoon whether we will be returning to school on Monday," said district spokeswoman Elena Cala in an email Saturday.

The district is also likely to be faced with the decision of whether to pay any ransom demand. Law enforcement representatives discourage payment to criminals, even though payment is sometimes the fastest and cheapest way to quickly bring back a down system and even though it rewards the criminal.

"I really don’t ever advocate paying unless they really, really have to," said Hubert, a former FBI agent who specialized in cybercrime. "Trying to roll back and leverage your backups is really your best course of action."

Some organizations and businesses, however, feel that because of their circumstances, they need to pay to keep operating and may negotiate with the hackers to lower the ransom demand, Cavalieri said. The criminals then provide the unlock codes to encourage future victims to pay up.

Ultimately, however, cyberattack prevention needs to be a priority, particularly for school districts and other public agencies that tend to shortchange this type of work. It's not enough to have a good information technology staff, Hubert said. Cybersecurity is its own specialty, similar to physicians in the medical field, who are not equipped to deal with every type of illness or surgery.

"When law enforcement leaves and computer systems go back online, what back doors could have been left behind?" Hubert said. "Really, your job is just beginning."

Sandra Tan

Reporter

I use the Erie County government beat to find issues and stories that tell us something important about how we live. An alumna of the Columbia Journalism School and Buffalo News staff reporter since 2000, I can be reached at stan@buffnews.com