NY village makes ransom payments to keep computers running

July 31 2015, byMichael Virtanen

A village in central New York made ransom payments of $300 and $500 last year to keep its computers running after two official-looking emails released malware throughout its system, state auditors said.

The comptroller's office, which has audited 100 municipal computer systems the past three years, said Ilion's experience should warn others of the growing threat, which can infiltrate computers and make them inaccessible. The big problem for the village of 8,000 was its financial software.

"The payroll, village accounting systems, they were all locked up," Mayor Terry Leonard said.

Other agencies across the country have also dealt with the malicious software known as ransomware.

In Maine this year, Lincoln County sheriff's office computers were infected and held hostage. Sheriff Todd Brackett said after several attempts to retrieve the records, his agency paid a ransom of about $300 and the FBI helped track the payment to a Swiss bank account but failed to identify the hackers.

In suburban Chicago, the Midlothian village police paid a $500 ransom in bitcoin, a digital currency that's virtually untraceable, to get its files unencrypted.

Ilion officials have endorsed new security steps and trained staff last year specifically on looking out for suspicious emails. They have been working with the auditors who identified various security gaps. They haven't had another attack since, Leonard said.

According to state auditors who investigated last summer, the first email attachment converted all data stored in the system into an unreadable encrypted format. A $300 ransom payment in January 2014 was made as directed, electronically transmitting the number of a prepaid credit card to a designated portal. Ilion's technology consultant entered the card number to get the decryption keys.

The second email, which also appeared to be for village business, led to more encryption and a $500 ransom payment in May 2014.

"These incidents should be a wake-up call to local government officials around the state," Comptroller Thomas DiNapoli said. "While the dollar amounts were small and no vital information was disclosed, this attack shows how the lack of basic IT safeguards can potentially cost taxpayers and cripple the day-to-day operations of municipalities or school districts."

The auditors cited user accounts for ex-employees that hadn't been closed, generic accounts used by more than one individual, lack of a recovery plan for security incidents with backup data, and staying current about ongoing threats.

Village police were contacted, but the hackers weren't identified, Leonard said.

Citation: NY village makes ransom payments to keep computers running (2015, July 31)