Basic cybersecurity precautions against ransomware are key to minimizing the damage

October 30 2020, by Richard Forno

A typical ransomware attack seizes control of a victim's computer files and holds them for ransom. Credit: [So5146/Wikimedia](), [CC BY-SA]()

Government computer systems in Hall County, Georgia, including a voter signature database, were hit by a ransomware attack earlier this fall in the first known ransomware attack on election infrastructure during the 2020 presidential election. Thankfully, county officials reported that the voting process for its citizens was not disrupted.

The attack follows on the heels of a ransomware attack last month on eResearchTechnology, a company that provides software used in clinical trials, including trials for COVID-19 tests, treatments and vaccines. Less than a week after the attack in Georgia was revealed, the FBI warned that cyber criminals have unleashed a wave of ransomware attacks targeting hospital information systems.

Attacks like these underscore the challenges that cybersecurity experts face daily—and which loom over the upcoming election. As a cybersecurity professional and researcher, I can attest that there is no silver bullet for defeating cyber threats like ransomware. Rather, defending against them comes down to the actions of thousands of IT staff and millions of computer users in organizations large and small across the country by embracing and applying the basic good computing practices and IT procedures that have been promoted for years.

What is ransomware?

Ransomware is a form of malicious software, or malware, that typically encrypts a victim's computer files, holds the files hostage and then demands a payment to send the decryption key that unlocks the files. Individual ransomware payments usually range from a few hundred to a few thousand dollars, with the expectation that a relatively low dollar amount will motivate the victim to quickly pay the attacker to end the incident.

Ransomware attacks frequently begin through email as a typical phishing

message purporting to be from someone the potential victim trusts, such as a co-worker or friend. However, emerging types of ransomware exploit existing or recently discovered security vulnerabilities—in other words, they hack in – to gain system access without requiring any user interaction at all.

Once a computer system is compromised, there are many things a ransomware attack can do. But the most common outcome is encrypting a user's data to hold it for a ransom payment. In other cases, ransomware encrypts a victim's data and the ransomware's creator threatens to release personal or sensitive information onto the internet unless the ransom is paid.

While ransomware attacks can affect any internet user or organization, attackers tend to target entities known for having less-robust cybersecurity defenses, including hospitals, health systems and state or local government computers. But health care remains an enticing ransomware target: In 2019, 759 health care providers in the U.S. were hit. Overall, ransomware attacks cost users and companies over US$7 billion in 2019 as a result of either ransoms paid or through costs incurred in recovering from attacks.

Ransomware's toll

The first high-profile ransomware incident was launched by North Korea in 2017. Using malware called "Wannacry," the attackers brought the British National Health Service to a paralyzing halt. Hospitals lost access to their computer systems and routine and emergency care was disrupted. But that was a preview of things to come: In 2020, a patient in Germany died after being diverted to another hospital due to a ransomware incident.

In 2020, during the COVID-19 pandemic, a ransomware attack crippled

over 250 medical facilities run by American-based Universal Health Services. At eResearchTechnology, staff conducting COVID-19 clinical trials were locked out of their data and unable to conduct business for nearly two weeks.

And it's not just health care organizations. The city of Atlanta was crippled by ransomware in 2018. Baltimore was similarly paralyzed in 2019. In both cases, city services—from tax collection and business licensing to real estate transactions—were unavailable to citizens. Numerous smaller cities around the world also have been affected by ransomware attacks.

However, even organizations with good IT policies and procedures find it extremely costly to investigate and recover from ransomware attacks, whether or not they pay the ransom. For example, an organization's routine data backup can also inadvertently include ransomware code. This means victims need to ensure they are not restoring the ransomware infection when they reconstruct their systems after an attack. Depending on the victim's backup procedures, locating a ransomware-free backup can be a very time-consuming process.

Ransomware and election 2020

The 2016 elections underscored the importance of ensuring the security and integrity of information related to government operations, including elections. Unfortunately, for many state and local governments, ransomware concerns are just another in a long line of issues that cybersecurity teams must contend with during periods of limited budgets and staffing.

Much has already been written about the vulnerable and fragile state of America's election systems, ranging from obsolete operating systems installed on voting machines to insecure networks and systems that

exchange and store vote tabulations, to ensuring the protection of voter registration databases.

Making this situation more challenging is that many local governments don't know what's happening on their networks. A nationwide survey conducted by University of Maryland, Baltimore County researchers in 2016 reported that nearly 30% of local government officials would not know if a cyberattack was affecting them. This lack of awareness means an attack could be well underway and causing havoc before security teams realize it—let alone respond.

Despite a growing awareness of the threat, ransomware has the potential to adversely affect the 2020 election. Unfortunately, if state and local election offices haven't implemented strong cybersecurity protections by now, it's probably too late to do anything meaningful given that voting is well underway. So it's no surprise that election offices across America are considering potential nightmare scenarios that include cyberattacks that might disrupt election activities.

Fuel for disinformation

Elections are based on trust—trust in the voting mechanisms and procedures, trust in the voting data and trust in the overall electoral process. But trust in all these items is under active attack by adversaries both at home and from abroad using a variety of influence and disinformation techniques that have become more refined since 2016.

Thankfully, ransomware attacks are unlikely to cripple the entire U.S. election given the decentralized nature of voting jurisdictions and systems. However, even a few successful attacks could contribute to disinformation campaigns that erode confidence in the outcome of the election.

How to lower the risk

At this point, since the election is already happening, state and local governments should increase the monitoring of their computer systems and implement even more stringent security controls on any devices or computers that might touch election-related networks in any way. Sharing real-time information about threats and working with the DHS, FBI and Office of the Director of National Intelligence election security teams, along with other states' election offices, also will help keep election officials informed. Additionally, major technology vendors and the U.S. military are taking active steps to disrupt cybersecurity threats, including ransomware, that may target the electoral process.

As with most cybersecurity problems, the ransomware threat can be minimized by implementing common-sense best practices—many of which have been recommended for decades but often are not followed. These include keeping systems up to date, ensuring security software is installed and current, monitoring network activities and implementing appropriate IT policies and procedures to include resilient backup practices. For individual users, thinking before clicking an email link—even from people you know—is excellent self-defense to make many ransomware or phishing attacks less likely to succeed.

None of these practices is specific to the ransomware threat or election security. But for this and other cyber threats, the best thing to do is continuing to implement and enforce those common-sense, decades-old best practices of information protection that can help guard against the ever-widening range of cyberthreats—including ransomware.

Provided by The Conversation