GALEANU MIHAI/ISTOCK/GETTYIMAGESPLUS/GETTY IMAGES

TECHNOLOGY

Preventing Cyberattacks

Local governments can access multiple sources of help

by Mike Taylor
Florida League of Cities

Almost daily, we hear about the aftereffects of cyberattacks and the financial and human resources needed to recover from even the smallest compromise. The discussion generally focuses on the need for data backups because it is essential to have strong backup technology and procedures, such as backing up all critical data and storing that data in multiple locations to minimize downtime following an attack.

However, the tools that can help prevent an attack are often not discussed. With cyberattacks, the popular saying "it's not if but when" may be true for many organizations. All cities should dedicate time and resources to prevent cyberattacks.

It can be daunting to keep up with new (and old) terms, technologies and concepts. Articles and experts refer to tools with little explanation of what they mean or can do for a municipality's security program. Unfortunately, long gone are the days of simply running antivirus software on all computers and servers that are the endpoints in your organization. Today, a strong cybersecurity program resembles an onion and includes many layers of protection.

TOOLS AND TECHNOLOGY

A robust cybersecurity program consists of many tools and technologies that create a trustworthy computing environment. Fortunately, there are resources to help select the right tools for our organizations. Some resources are even free to local governments. (See cybersecurity resources on p. 26.)

Simply installing traditional antivirus and antimalware software that rely on signatures, which are like fingerprints that can help identify viruses, no longer protects computers and networks. While using signatures is still a viable method for detecting malware, it should be only one layer in the endpoint security strategy. Some technologies that add layers of protection on top of traditional antivirus programs include:

- **Endpoint detection and response** (EDR) – This proactive technology identifies threats that antivirus companies haven't identified or patched. EDR continuously monitors network endpoints looking for anomalies in expected patterns to identify threats. EDR can respond to help mitigate an attack, including quarantine of the suspected malware to remove the threats and provide a root cause analysis. Extended detection and response (XDR) is an extension of EDR that improves capabilities and insight into the network and can cover more than just endpoints to include cloud services and other platforms that are a part of an organization's network.
- **Ransomware rollback** – This tool can revert an affected system to a known healthy state while identifying the process that caused the ransomware attack and remediating the problem. Ransomware rollback is sometimes included in EDR/XDR offerings.
- **Application whitelisting** – This process approves files running in a network environment and prevents files not on the approved list from running without intervention. With the proper administration, it is a powerful tool to keep cyber issues from cropping up. The drawback is that it requires careful setup and ongoing maintenance.
- **Next-generation firewalls** – These firewalls differ from traditional ones that provide simple data packet and traffic

filtering by taking a deeper dive into the packets to identify malicious content before allowing traffic inside the network. These firewalls also provide application controls that can help filter malicious applications, user controls for more granular control of user security and sandboxing that sends files to be reviewed for malware before being let through.

- **Intrusion prevention systems** (IPS) **and intrusion detection systems** (IDS) – These systems are often included in next-generation firewalls but can be standalone products. An IDS continually monitors for malicious traffic via rules, behavior analysis or both. IDS is more passive and acts as an alert system to let you know when potentially malicious traffic is detected. IPS does what IDS does but will attempt to stop the malicious traffic from gaining entry into the network.

TRAINING OPPORTUNITIES

Having all of these security precautions is an excellent start, but there are times when it is not possible to have these systems in place. Even if you do, it could still not be enough. It is often said that the weakest link in an organization's security posture is the human element. Our users are inherently good and want to do the right thing, but the bad guys are good at identifying and manipulating weaknesses to get us to click on links or open malicious files. That's where user security awareness training comes into play.

A security awareness training program is extremely important and should have buy-in from the highest levels of the organization. All employees who work with a computer should be required, at a minimum, to have annual meaningful training that discusses current and emerging cyberattack trends. The Florida Legislature passed a bill this year (CS/HB 7055) that requires local governments to adopt cybersecurity standards and participate in annual trainings. (See more information, p. 33.) However, security awareness should be something users are mindful of year-round.

In addition to regular training, organizations should evaluate programs that incorporate phishing tests and reminders throughout the year. Simple activities to implement are providing tips on having a safe computing environment and recognizing October as Cybersecurity Awareness Month. (For more information, visit *bit.ly/3IPxzQ3*.)

It can be difficult to ascertain what security precautions are in place, where weaknesses may be present and what can be done to strengthen an organization's security posture. Understanding some of the newer concepts and technologies and the available resources to help in the cybersecurity battle means you don't have to go it alone!

Mike Taylor is the Associate Director of Technology Services for the Florida League of Cities. QC

Attendees at the 2022 Florida Local Government Information Systems Association (FLGISA) conference participate in "war games."

Cybersecurity Resources for Local Government

- The **Florida Local Government Information Systems Association** (FLGISA) is a member organization for local government IT professionals and focuses solely on local government information technology issues. The FLGISA offers resources to help IT professionals stay up to date, including two hosted conferences each year, cybersecurity and disaster recovery committees and message boards for members to share information. Go to *flgisa.org* for more information. There is a nominal membership fee, but it provides all IT staff access to FLGISA resources.
- The **Cybersecurity and Infrastructure Security Agency** (CISA) is a federal initiative designed to provide tools and resources to government entities to strengthen cybersecurity. Security insights and news, penetration testing and scanning, training, protection and detection, governance and cyber response are available. Many resources are free and can be viewed at *cisa.gov/cybersecurity*.
- The **Multi-State Information Sharing and Analysis Center** (MS-ISAC), operated by the **Center for Internet Security**, works with the **Department of Homeland Security** and CISA and is free to local government agencies. Free resources include a cybersecurity awareness toolkit, cyber alerts, malicious code analysis, computer emergency response, threat assessments and webinars. Paid services such as intrusion detection systems, penetration testing, phishing engagements and vulnerability assessments are available. For more information, go to *cisecurity.org/ms-isac*.

PHOTO COURTESY OF MICHAEL VAN ZWIETEN