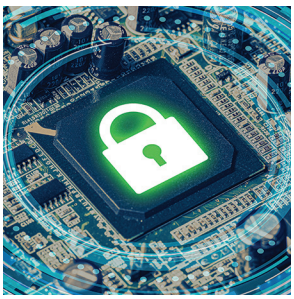
TECHNOLOGY

Defeating RANSOMWARE

There's no magic bullet, but try these less-magical best practices

by Michael J. van Zwieten
Florida League of Cities
Florida Local Government Information Systems Association



It's scary to think that one click on a link in a phishing email could take down your entire city.

Ransomware has become a dangerous enough threat for local governments to start paying serious attention to how they handle their internal defenses to mitigate against these intruders. Malicious software (malware) used to be considered more of an annoyance and typically not too destructive, but now criminal groups have figured out how to profit by holding your files ransom, taking down your entire network and preventing you from performing business operations.

Phishing is a form of social engineering to tempt people to click on a link in an email or a fake website that they believe is legitimate. According to the FBI, 90 to 95 percent of successful phishing attacks are received through email. Clicking that link carries with it the potential for the hacker to run additional malware attacks that set off a ransomware event.

Ransomware is a malicious form of software that encrypts most files on a network's local computers and servers, demanding a ransom if you want the files back. This malware may retreat into the bowels of your network and just sit there, learning and watching. This gives the attackers months or more to examine what is on your network so they can compromise administrative accounts and have unfettered access to any available content. Yes, even your backups can be compromised. At a time of their choosing, hackers will set off the ransomware attack to cause maximum damage in the hopes of cashing in on a hefty ransom. City staff will be unable to work, while residents continue to expect the same level of service.

However, ransomware can be overcome. It all comes down to best practices. IT professionals are constantly fine-tuning or learning about new practices for the ever-changing threat landscape. The key is to have robust security layers.

The following best practices will minimize the chances of malware, intrusions or disaster-level events on your network, including ransomware.

WEAPONS-GRADE BACKUPS

One of the most important components in the fight against ransomware is to ensure that your backups work. These need to be weapons-grade level backups that are kept offline. Ransomware may attack and encrypt your backup sets, making any kind of restoration impossible, so ensure you have some redundancy built in.

IT professionals typically abide by the 3-2-1 rule: a minimum of three backup copies of the data, using two different devices or storage media, and one backup set offsite. If something happens to one backup set, you would have two others to rely on.

Storage media and hard drives will ultimately fail, so it's important to spread the risk by using different devices or storage media to place these backups on. Keeping a backup set offsite or in the cloud ensures that your data will be safe even if your entire network is encrypted by ransomware.

Today's backup solutions can take periodic images of all of your servers or important data, replicate this data and send it to various locations. Regularly test backups. Periodically restore files and folders, and test the restoration of an entire server.

PHISHING TRAINING

Properly train your employees. Security training should be held on a regular basis to teach your employees about general computer security and the various types of dangers found on the internet.

Employees must be able to identify phishing emails to determine what's real versus what's fake, know what attachments to look for and heavily scrutinize a file or message they weren't expecting from that sender.

In addition, regularly test your employees by sending them bogus phishing emails to keep their skills sharp. Services that provide this type of testing can give detailed results of your phishing campaign, allowing you to provide further training for those who clicked on a bogus link or opened the attachment.

Drive home a "Stop. Think. Act." slogan in your organization. Stop – when presented with a possible suspicious email or link. Think – Analyze the content of the email, look at where the link is pointing, determine who the real sender is, etc. Act – If it fails the smell test, delete or report it. If employees are concerned that a file or link may be malicious, they should be encouraged to ask questions.

Employees are one click way from being the last bastion between a failed ransomware attack and a successful one. Keep them engaged!

NETWORK SECURITY MONITORING

Appliances or software applications that provide network security monitoring will listen to all traffic traveling across your network and spot anomalies. Using their built-in database of known signatures to look out for, they generate instantaneous alerts for IT staff to investigate suspicious items further.

These are referred to as "intrusion detection systems." IDS appliances detect only anomalies and create alerts, while "intrusion prevention systems" appliances also prevent potentially malicious network traffic from traveling inside or outside your network, cutting off any communications with the intruder.

These appliances can quickly detect and block traffic before it has a chance to do damage to the network. Monitoring, maintaining and understanding these types of appliances is complex and typically requires an employee with a network security role at the organization. If a jurisdiction does not have staff with this expertise, these services can be implemented by contracting with a managed security service provider.

FILTERING

To prevent malware, it is vital to run software that filters out the bad from the good. No single filter is going to prevent all malware from getting through, which is why you want a diverse set of security filters protecting your network.

The most well-known and oldest is anti-virus (AV) software, which is a necessity on workstations and servers. Unfortunately, AV software is becoming less effective due to the increased sophistication of today's malware.

Anti-spyware (AS) software, which also includes anti-malware software, is recommended to be running alongside your AV software for increased security and detection of these types of intruders.

Email filtering, also a necessity, scans and strips malicious attachments from the email and filters a good amount of spam and phishing emails before they even arrive in the employee's inbox.

Domain name server (DNS) filtering denies access to known-malicious IP addresses if an employee clicks on a bad link.

Web filtering analyzes each link requested by a web browser to access the internet and denies access to those it deems to be harmful.

When combined and kept up to date, these security layers drastically lower the risk of malware from entering the network.

APPLICATION WHITELISTING (AWL)

AWL software is a powerful defense against ransomware, malware or unwanted software. It determines if a certain program file is on an "allowed" whitelist for permission to run on the computer. If it is not found on the whitelist, the program is denied from running.

This type of software is very complex and labor-intensive for IT staff to maintain, but it does leave you with an extremely secure and controlled network environment.

PRINCIPLE OF LEAST PRIVILEGE

The "principle of least privilege" is an important concept of granting each person restrictive access to applications, files and folders on the network that are necessary for that person to do his or her job; no more, no less. If ransomware takes a foothold on an employee's computer, damage would be limited to the permissions and privileges of his or her account, helping contain the spread of destruction.

MULTI-FACTOR AUTHENTICATION (MFA)

Passwords alone are no longer considered a secure method to lock down an account. Malicious actors have been successful with using phishing emails to trick people into giving up their username and password through an online login page that mimics a legitimate website, also called an account compromise.

The hacker will log into this person's online email account and send similar phishing emails to his or her contacts, or others with whom that person has communicated, causing more people to be compromised. Using compromised account information, hackers may be able to remotely gain access to the city's network to unleash malware or ransomware.

One way to stop these types of compromises is to use MFA, also known as two-factor authentication (2FA), which requires two pieces of information to gain access to a system. One is the person's password. The other is a random code that can be received as an SMS text on the person's mobile device or displayed on a mobile "authenticator" app.

It is recommended to use MFA for any account accessible from the internet.

REMOTE DESKTOP PROTOCOL (RDP)

Another path that could allow a hacker onto your network is though RDP. Microsoft Windows desktops and servers have a useful utility built into them called "remote desktop." It allows someone with valid credentials to remotely access the PC or server and view what is displayed on the screen.

In some cases, computers or servers may be directly accessible using RDP off the open internet, allowing anyone to attempt to access them.

While remote access to your desktop and server is convenient, they are vulnerable to attacks. These types of attacks allow the hacker to try every known word in the dictionary, use lists of common password phrases and every combination of characters to land on your password. Millions of attempts can be made, and they won't give up until successful.

Once they are logged into a PC or server on your network, it's simple to launch an attack.

Block all remote access through RDP off the open internet. Provide for more secure remote access methods using VPN or Remote Desktop Services Gateway in combination with multi-factor authentication.

PATCHING

Downloading and installing updates across your network is time-consuming and can be daunting. Without a consistent patching schedule, it can fall by the wayside.

To stay ahead of malware infections, your desktops, servers, appliances, third-party applications and hardware must be running the latest iterations of their software. Vendors that produce these products continually fix bugs or known exploits that hackers or malware use to evade your defenses.

A system that has not been patched for years or even months is a hacker's dream. While there are products to help automate many of these tedious patch installations, these patching products are not perfect, nor will they get everything on your network.

It takes dedicated staff time to find patch installations that failed or tackle the patches for third-party products, applications and hardware. However, even if you've patched to the latest versions, hackers are notorious for their ability to break through defenses. Hackers will use a "Zero Day" exploit, which is taking advantage of a weakness that isn't yet publicly known, where no patch has been developed yet to prevent it.

Staff must keep a watchful eye on what workarounds are available to repel these threats until a patch does get released. Once this emergency patch becomes available, it should be tested and deployed across the organization.

By subscribing to Microsoft, SANS, MS-ISAC or other vendors' security bulletins, you will be regularly notified about what items require critical attention.

DISABLE MACROS

It is highly recommended to disable all macros from running in Microsoft Office products because of security issues. Malware authors use this functionality to deliver malicious Word or Excel documents that contain dangerous code that could trigger a malware event.

If you receive a Microsoft Office attachment from outside your organization that prompts you to "enable macros," it is recommended that you do not. Likewise, PDF documents have the ability to execute malicious Java code, which could be embedded within the document. It is very difficult to tell what these incoming documents may have waiting within them.

Likewise, it is also considered best practice to disable Javascript actions within Adobe Acrobat or other PDF viewers. If possible, force these settings across your organization with "group policies" using Microsoft's Active Directory so that employees are not able to change these settings.

DISASTER RECOVERY PLAN

In addition to having a disaster recovery plan that covers how your organization will recover from an unplanned incident or natural disaster so business operations are quickly up and running, it is important to include a scenario of recovering from a malware outbreak in that plan. Continually refine and update this document as computer equipment, personnel, backup methods or procedures change or evolve within the organization.

For most of us, it's not a matter of "if" an event like this will happen; it's a matter of "when." No network is unhackable. While we continue to strengthen our defenses with best practices and next-gen tools, hackers will continue to find new exploits and avenues into our networks. If we focus on being ready to react using the best tools and best practices available, we can minimize damage and downtime.

Michael J. van Zwieten, CGCIO, MCSE, is director of technology services for the Florida League of Cities and serves as the executive director of the Florida Local Government Information Systems Association. FLGISA is an association for chief information officers, IT managers and technology decision-makers from local governments in Florida. The FLGISA sponsors an annual conference and winter symposium that tackle current IT topics such as cybersecurity, cover the latest technology trends presented by subject-matter experts and provide time for peer-sharing. For more information or membership, contact the FLGISA administrator at *admin@flgisa.org* or visit *flgisa.org*. QC

CYBERSECURITY TRAINING AVAILABLE

A series of four regional "Cybersecurity for Local Governments" workshops are being offered for city and county managers and their department heads, elected officials and others interested in local government's unique cybersecurity challenges. (Note: These workshops are non-technical and not intended for IT directors or staff.)

The workshops are being offered through a partnership between **Cyber Florida at the University of South Florida**, the **USF School of Public Affairs**, the **Florida League of Cities**, the **Florida City and County Management Association** and the **Florida Local Government Information Systems Association**. Attendees will hear from leaders of public sector organizations that have been hacked, learn best practices to establish a cyber-secure culture, participate in an intense simulated cyberattack and more.

The workshops will be held:

- **October 24 in Tampa** as part of Florida Cyber Conference 2019 at the Tampa Convention Center.
- **November 19 in Fort Lauderdale** before the Florida Association of Counties Legislative Conference.
- **January 24 in Jacksonville** hosted by the University of North Florida.
- **February 13 in Tallahassee** following the Florida League of Cities Legislative Action Days.

There is no charge to attend, but space is limited. Registrations will be accepted on a first-come, first-served basis.

For more information or to register, visit *cyberflorida.org/gov*.