CDE #65181

CYBER HIDE AND SEEK

Finding and removing cyber attackers hiding in your system.

By Stephen Martini

ANDREY_POPOV/SHUTTERSTOCK.COM

In early 2021, the Washington County Consolidated Communications Agency (WCCCA) northwest of Portland, Oregon, faced two significant projects — finalizing a new 52-site, multi-simulcast trunked radio system and hiring a new director. Mark Buccholz accepted the role on March 11, 2021, a few weeks after the radio system experienced the first of two ransomware attacks.

On February 17, the radio system was still in a non-production environment as final testing and system acceptance continued when cybersecurity hackers initiated a ransomware attack on a server used for radio ID management.

"The remote management server allows us to define templates and do all the prep work for programming radios in the field," Buccholz said. "So, to access that, you create users and passwords who can connect remotely and program radios in the field."

He said the system was 90% complete and in the process of upgrading sites and installing the new remote management servers when the agency was struck by cyberattack. Since the system was not yet accepted from the vendor, ownership of the system had not passed to the county so the responsibility to address and resolve the attack was still on the provider.

"It's like being on a job site when you're constructing a home," Buccholz said. "You're out there doing some work on the house and the contractor is also doing work on the house, but the house really isn't yours until that substantial completion date or occupancy is approved and it becomes yours. Things that fail before that date are the responsibility of the contractor."

A field technician identified the attack after arriving at work and seeing the ransom message on the computer screen announcing the hack. The technician chose to disconnect the system from the network and, since it was still early in the project, the vendor decided not to pay the ransom. Instead, they reconstructed all the data, including templates, that was put on the remote management servers, wiping the servers related to the situation.

They pulled information from backups on file prior to the ransomware attack to restore the data where possible.

When Buccholz came on board in March 2021, he received no briefing about the ransomware attack and heard no mention of one occurring.

"I'm not sure who among WCCCA management even knew," he recalled. "The technicians treated it with such low concern that I don't believe that even the depths of our vendor partner knew. The field technician and the local shops knew and some of the local WCCCA technicians knew. But after they restored the servers, they thought that was that and moved on. They were confident the system was disconnected from any other networks. It didn't have any exposure to the rest of the environment so that was the end of the story. Nothing else to talk about, nothing else happened."

Fast forward to early June 2021.

Buccholz was now the director, and over Memorial Day weekend WCCCA was hit again with a ransomware attack on the same server. As a side note, technicians should be wary of holidays as a time when cyber attackers seek to invade systems when they assume no one is actively monitoring, allowing several days to steal and encrypt data without being noticed.

"This time, I got notified about it and I wanted to know what was going on and what the plan was," he said. "The vendor was involved, and we had some discussions about what they were going to do. There were several servers involved this time: a primary and a few ancillary servers. None of these were on the primary network. It was still pre-cut over so we were fortunate. We have multiple networks so had it got onto the radio network, our radio system would have been exposed but the rest of our systems (CAD, administration and others) are on separate systems to prevent this situation. But it could have been on all the radio equipment had the remote management server been connected to more parts of the network."

Buccholz pumped the brakes.

"This time, I said hold on, what's going on here? The plan was to disconnect, wipe the machine and rebuild, as they did before."

Technicians set up an air-gapped computer to check the external SSD backup drive which, unfortunately, was still attached to the remote management server. All files on the backup drive had been encrypted with multiple files infected by various viruses. They confirmed the backup drive was encrypted with the same ransomware pattern as the primary servers and had become infected because technicians did not detach it physically from the primary server.

Buccholz applied the brakes, telling technicians to disconnect the server, then not touch it. He sought answers regarding how this happened, how they were impacted, what specifically was happening now and which members of the vendor partner were involved in resolving it.

By the time you are aware of a ransomware attack, the attackers likely have all the information they could possibly use and are simply seeking a payout.

"I think this is how the issue never got run up the chain the first time," Buccholz said. "Since the issue happened again, that means whoever got in the first time knew how to get in again because we didn't take the proper steps to prevent it."

The vendor partner hired cyber forensic specialists to look at the machine and determine what was going on. Initial investigations appeared to point to a single device programmer's machine deployed at a neighboring public safety department that accessed the network through the department's Wi-Fi network. However, that proved to be false. On June 9, further forensic work revealed activity coming from IP addresses common to European ISPs not identified on the deny list (a list of known ISPs not allowed access to a network).

Investigators determined this activity had been going on for many days before the ransomware attack occurred. By the time the entire system was encrypted, forensic experts could tell the hackers had been on the machine for more than a week.

"During that time, they were probably extracting data and doing whatever they wanted to do," Buccholz said. "Viewing as much as they could and, I think, when they determined there was no more information worth gathering, they decided to execute the ransomware."

Simply put, by the time you are aware of a ransomware attack, the attackers likely have all the information they could possibly use and are simply seeking a payout.

Now the question is, how did they gain access?

The hackers used known usernames to log into the system. Once they had usernames, they also had the password because the vendor used common passwords shared across multiple technicians working multiple projects across multiple locations. Because usernames and passwords were not changed following the first hack, the hackers used those to access the system at WCCCA. This could apply anywhere the vendor did business. Once the hackers determined the sequence (in Los Angeles, for example) they could use the same credentials to access a system being managed by the same vendor somewhere else (like Boston, for example).

"This answered several questions because the field tech did not notify his chain of command, didn't think about how they got connected, repeated the rebuild and assigned the exact same usernames and passwords," Buccholz said. "Imagine: 'Username1, Username2, Username3,' and so on, and the passwords were all assigned the same. WCCCA team members signed in remotely using that username schema and the same password, too."

With these passwords, the attackers had the same access as field techs to create, modify and view data on the system.

"Once we discovered what happened, I was worried that this could be easily repeated at other sites across the nation because of the likelihood the password or usernames could be used," he said. "A threat actor would still need to figure out what your domain name is, but the risk is still there."

WCCCA and the vendor partner again determined *not* to pay the ransom and to invest the resources to rebuild and the work done in the previous four months since the last attack.

After the forensic investigation was complete, they started recovery. Since the backup device connected to the network was also encrypted by the ransomware, their only opportunity to restore was investing a lot of work and time to rebuild all the system setups and design templates — hours and hours of labor. This still made more sense than paying the ransom, since the security and value of the data lost wasn't worth the ransom costs.

They focused on rebuilding, changing usernames and passwords, and making firewalls much more secure. They moved firewalls from restricting ISPs from a deny list to requiring ISPs to comply with an allow list. While the deny list says this list of IPs cannot access our system, an allow list says only these approved IPs can access, restricting all others.

"It's highly restrictive and from the basics, it's a pain, but we moved to that to have the security we need," Buccholz said. "Every time you want someone to do something from a different location you need to manage the allow list, which is more annoying but more secure."

The rebuild took another month to complete and put WCCCA back in business.

The system wasn't down, as it was still in the final acceptance phase prior to being moved into production, but the ability to move to the new system was delayed. Also, resources weren't assigned around the clock as they would have been if the system were online. Instead, a few agency technicians and some from the vendor worked side-by-side during regular business hours to restore the lost data.

According to APCO cybersecurity resource "Three High-Value, Low-Cost Strategies to Strengthen ECC Cyber Defense" (apcointl.org/cybersecurity-resources) prepared by the Cybersecurity Committee, "a strong cyber defense strategy is owned, managed and monitored by ECC management. That takes into account that virtually every area for which ECC management is responsible has a cybersecurity element. For every SOP, every application, every system and every time any of those items is upgraded or changed, the questions must be asked: 'What is the impact on our cybersecurity management plan?' and 'What is the risk to our continued operations?'"

One of those three strategies includes password management. Buccholz' experience isn't unique, according to the committee, which states, "Balancing the need for quick access to applications at the beginning of each shift and following breaks with the need for longer, more complex passwords can create an operational nightmare. Add into this mix the needs and 'requirements' of vendors, who often want to keep usernames and passwords the same across all their customers to make remote support easier, and it creates a situation in which cyber thugs rejoice."

Because usernames and passwords were not changed following the first hack, the hackers used those to access the system at WCCCA.

With 30 years in high technology in both the private and public sectors, Buccholz isn't surprised about the vulnerabilities in sharing common usernames and passwords among private-sector partners.

"I've known over my 30-year career that I could get into other agency's systems because I know the username and password my vendor uses to access my system," he said. "If I know what their domain is, I could go to their IP address, get a username prompt and have the same situation. If you're a vendor and have people who are assigned to remotely connect and solve problems, those people can't remember all these usernames and passwords so, what they tend to do, is use the same one on multiple sites. That's a plan for disaster."

The APCO Cybersecurity Committee recommends patch management and hardening of the Windows operating system. Buccholz also moved to instill a culture of cybersecurity awareness.

The team took the following steps in response to the cyberattack:

- All distribution point and remote management servers were wiped and rebuilt from scratch. Data was restored from an older offsite backup.
- They no longer attached user device programmers to user networks. They re-engineered device programmer connectivity to match the existing "grab and go" radio programmer kit that WCCCA radio technicians developed.
- They created unique usernames and passwords.
- They went through firewall configurations and confirmed the appropriate required access was in place in both WCCCA and vendor firewalls.
- They implemented two factor authentication wherever possible.

"One part of a cyberattack is recovering from it," Buccholz said, "but another is conducting the analysis of it and determining how did they get in and what have we done to prevent that. In our case, we didn't tell enough people. We kept it quiet enough that there wasn't sufficient thought given to how they got in, how this happened and how to avoid it."

Password Best Practices

In addition to patch management and windows hardening, APCO offers tips to strengthen password security, including:

- **Complexity** — This means a mix of upper- and lower-case letters, numbers and special characters. Turn on password complexity in active directory (AD) if AD is in use.
- **Force logoff** — This means logging off end users after a specific time has elapsed, typically recommended to be a couple hours longer than the duration of a normal shift.
- **Maximum password age** — This is the timeframe for requiring users to change their password. The Criminal Justice Information System requirement is 90 days (note that there is some flexibility here when passphrases are implemented).
- **Minimum password length** — Should be a minimum of 12 characters; 15 for administrative accounts.
- **Password history length** — This defines the number of times a new password must be created before re-using a previous password. This should, ideally, be at least 11 times.
- **Lockout attempts** — The number of times an incorrect password can be entered before the system locks out that user. This should be 5 or less attempts.
- **Lockout duration** — This defines how long the user is locked out following too many attempts entering the incorrect password. This should be 30 minutes.

He recognizes solutions must come in partnership with internal team members and external partners. Of the incident, he said, "As much as I was upset with our vendor because their environment and their response was insufficient after the first attack, which could have prevented the second attack, I still have a significant relationship with our vendor and continue to work with them to make our system stronger."

Buccholz also recognizes this isn't an isolated incident. After all, this wasn't the first time he dealt with a cyberattack on the job. A few years before while working with a different agency, a telecommunicator clicked on a link allowing malware access to the network, which lead to a similar situation.

APCO's Cybersecurity Committee stressed the ECC director must "work with vendors to ensure and enforce that the ECC password policy is being used on new and legacy systems."

And it's a responsibility Buccholz takes seriously.

"After the second occurrence, those usernames and passwords were never used at our site again," he said. "Since the incident, passwords have been security-based with recommended lengths and usernames that are not common — unique to our site and not easily recognized by a remote cyberhacker just trying to connect to systems by guessing things." ●

Stephen Martini, RPL, CPE, *is APCO First Vice President and Director, Metro Nashville (Tennessee) Department of Emergency Communications. He can be reached at Stephen.Martini@nashville.gov.*

CDE EXAM #65181

1. APCO's Cybersecurity Committee recommends three strategies to strengthen cyber defense: planning, patch management/windows hardening and _____.
   a. Password management
   b. Firewalls
   c. Fences
   d. Soldiers

2. WCCCA was hit twice by the same cyber attackers.
   a. True
   b. False

3. What mitigation effort did technicians take to recover from the first cyberattack?
   a. Replace all existing equipment.
   b. Wipe all previous backup servers and start from scratch.
   c. Restore lost data from previous backup servers.
   d. Reset all usernames and passwords, and initiate two-factor authentication.

4. When did the second attack occur?
   a. During a busy week.
   b. During a holiday weekend.
   c. During an emergency.
   d. During a shift change.

5. Cyberattacks impacting non-production equipment aren't a concern because the software is not used in a "live" operational setting.
   a. True
   b. False

6. Technicians initially planned to recover from the second attack the same way they did after the first.
   a. True
   b. False

7. Forensic investigators were used to help understand the why, how and who behind the attacks, providing a road map to how to avoid future attacks.
   a. True
   b. False

8. What did cyber attackers use to gain access to the WCCCA system?
   a. Known usernames and common passwords used by technicians.
   b. Complex passwords and hard-to-guess usernames.
   c. Multi-factor authentication.
   d. A gate key.

9. From where did the attacks originate?
   a. A neighboring public safety department
   b. New York City
   c. Canada
   d. Europe

10. There are a variety of steps you can take, identified by APCO's Cybersecurity Committee or the WCCCA, to mitigate against a similar attack on your network.
    a. True
    b. False

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "Hide and Seek," then click on "enroll me" and choose **"Hide and Seek (65181)"** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.