CDE #47929

CYBERSECURIT

VS148/SHUTTERSTOCK.COM

Y FOR NG9-1-1

By Megan Bixler

Since the first 9-1-1 call was made in 1968, PSAPs have had to manage security threats that are introduced by technology. Traditionally, emergency communications have mostly been based upon "copper wire" technology. Even in this environment, PSAPs are faced with substantial cybersecurity risks through various cyberattack vectors. There have been numerous news articles, web publications and reports on the various attack vectors currently being used against 9-1-1 today. These attack vectors include phishing, spoofing/swatting, Telephonic Denial of Service (TDoS), Distributed Denial of Service (DDoS) and ransomware. Understanding these threats is an important step in preparing for the increasingly complicated cybersecurity landscape for Next Generation 9-1-1 (NG9-1-1).

PHISHING

Phishing is the fraudulent practice of sending emails purporting to be from a reputable company, or even the recipient's own organization or agency, in order to induce individuals to reveal personal information, such as passwords or credit card numbers. According to research[2], phishing emails are the start of 91 percent of successful cyberattacks.

Phishing emails started off simple. Remember the overseas prince that surprised you with an unknown bloodline to royalty and inheritance of a million dollars? Surprisingly, that prince couldn't afford the thousand-dollar transfer fee so he needed your credit card information. Now, phishing emails are much more sophisticated. These emails can be seemingly from your employer directing you to download a document – which happens to be a virus that allows remote access to your computer. They can be from what appears to be a government agency, or even your own bank.

The best way to combat phishing emails is to look at incoming email with a cautious eye. Two of the best (and easiest) methods to combat phishing emails are to stay informed about current phishing techniques and taking a critical look at each email. A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with "Dear Customer" so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link. By this, I mean go to a trusted and verified link for that provider or entity, not the link provided in the email. Don't call any number listed in the phishing email, look up the actual number for that provider or agency. While the websites may "look" right, there is always something amiss in the background. Don't take a chance, do the research yourself and when you discover phishing, report it to that entity's actual fraud department.

SPEAR PHISHING

In spear phishing campaigns, nefarious sources will customize their attacks to target an organization. For example, hackers will start to research their intended target before the phishing campaign begins. Spear phishing is especially commonplace on social media sites like LinkedIn, Facebook, Twitter and Instagram, where attackers can use multiple sources of information to craft a targeted attack email. This research is primarily done through social media and starts with cat phishing (targeting an individual). The goal is the same as deceptive phishing: lure the victim into clicking on a malicious hyperlink or email attachment, so that they will hand over their personal data.

To protect against this type of scam, organizations should conduct ongoing employee security awareness training that, among other things, discourages users from publishing sensitive personal or corporate information on social media. Agencies should also invest in solutions that are capable of analyzing inbound emails for known malicious links and email attachments.

DENIAL OF SERVICE

According to the United States Computer Emergency Readiness Team (US-CERT), Denial of Service events are when, "… an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.) or other services that rely on the affected computer."[3] Essentially, in a denial of service attack, services become unavailable when an attacker "floods" networks (e.g., through telephonic, data or other means) with information.

For public safety, denial of service attacks primarily come in two different forms: TDoS and DDoS. TDoS events involve a "flood" of impostor phone calls that prohibit legitimate phone calls from being answered. DDoS events are a "flooding" of data to a system or website that overwhelm the system and renders it unavailable.

If you are a victim of a denial of service attack, there is little you can do personally to stop it. However, as discussed below, there are several federal resources for assistance. Look for the signs that an attack is occurring, such as slow network performance, unavailable websites, and an increased amount of spam emails, and don't hesitate to contact the appropriate authorities.

RANSOMWARE

Ransomware is a type of malicious software that infects and restricts access to a computer or certain data until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.[4]

Cyber hygiene best practices are the best methods to thwart these attacks. These best practices can be found in APCO's Cybersecurity Guide for PSAPs[5] To minimize disruption from a ransomware attack, be sure to keep current backups of your system.

SPOOFING/SWATTING

According to the Federal Communications Commission (FCC)[6], spoofing 9-1-1 occurs when a caller deliberately falsifies the information transmitted to your ANI/ALI display to disguise their identity or location. Using this technique to deceive an emergency service agency to send a police response team (i.e., SWAT team) to another person's address is known as "swatting."

Spoofing or swatting can have serious repercussions for public safety – from creating a public relations issue to diverting the attentions of emergency resources. There are several characteristics of a spoofing/swatting campaign to watch for:[7]

- Suspicious story or scenario given by the caller
- Tone of caller and background noise does not match the situation
- Claims of hostages, rifles, explosives or automatic weapons present at the location
- Calls originating from an unknown source or "relay service" or other Internet Service Provider (ISP) application enabling proxy calls
- No signs of forced entry at location
- No unusual activities or out of place vehicles in the area
- Individual claims to be armed and suicidal or intends to shoot law enforcement upon arrival
- Story changes or escalates during the call
- Only a single caller is reporting a high-profile incident

"With the transition to IP-based technology and NG9-1-1, understanding and dealing with these threats becomes increasingly complicated. To truly combat cybersecurity attacks in a NG9-1-1 environment, a thoughtful and critical look must be taken at current and potential threats.

Spoofing is illegal and should be reported via the proper government channels that are mentioned below.

INCREASED SECURITY RISKS IN NG9-1-1

NG9-1-1 comes with a plethora of new technologies that will benefit public safety telecommunicators and the public alike. As outlined in the P43 Report[1], these technological features will change the emergency communications landscape. These new technologies will enable PSAPs to share data, improve location data and accuracy, improve emergency services for the deaf and hard of hearing community, and gain multimedia data to assist in triaging calls for service. All of these new technological advances will enable the public safety telecommunicator to glean more information with each call and send assistance more effectively.

With the transition to IP-based technology and NG9-1-1, understanding and dealing with these threats becomes increasingly complicated. To truly combat cybersecurity attacks in a NG9-1-1 environment, a thoughtful and critical look must be taken at current and potential threats. A common industry tool to assess information security within an organization is called the "CIA Triad." In this instance, "CIA" stands for the three information security goals: confidentiality, integrity and availability. Confidentiality means keeping the data secure from anyone who should not have it and ensuring that data is accessible by those who are authorized to view it. Integrity is keeping information safe from unauthorized changes. Finally, availability is the ability to reliability access that information.[8] Understanding these concepts helps information security planners to think about the type of security they need and what should be implemented.

RESOURCES THAT ARE AVAILABLE FOR ASSISTANCE

If your PSAP experiences a cyberattack, there are a number of resources available for assistance.

- File a complaint with the Internet Crime Complaint Center (www.ic3.gov)- co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). In the report, include keywords such as PSAP and public safety.
- File a report with your local police department or sheriff's office. If the investigator is unsure of how to proceed, there are resources available to assist. The FBI, FCC and Federal Trade Commission (FTC) are all available resources.
- The Department of Homeland Security (DHS), National Coordinating Center for Communications (NCC) and National Cybersecurity and Communications Integration Center (NCCIC) are all engaged in this process, and can help coordinate and distribute information (Phone: (703) 235-5080, email: ncc@hq.dhs.gov).

In order to assist in investigations, consolidate call logs, call and CAD recordings, and IP logs, and be sure to mark for long-term retention. The more data you can gather, and save, the more likely authorities can properly investigate the incident. Cybersecurity is a multi-faceted threat. As a result, we need to take a multi-faceted approach to how we react to, and defend against, the ever evolving cyber threat landscape. ●

Megan Bixler *is APCO International's Technical Program Manager for the Communications Center and 9-1-1 Services Department.*

References

1. "Project 43: Broadband Implications for the PSAP" www.APCOp43.org
2. "91% of Cyber Attacks Start with A Phishing Email: Here's How to Protect Against Phishing" https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing
3. Security Tip (ST04-015: Understanding Denial-of-Service Attacks https://www.us-cert.gov/ncas/tips/ST04-015.
4. Ransomware https://www.us-cert.gov/security-publications/Ransomware.
5. https://www.apcointl.org/resources/cybersecurity/cyber-security-guide-for-psaps/file.html.
6. Spoofing and Caller ID https://www.fcc.gov/consumers/guides/spoofing-and-caller-id
7. Spoofing and Swatting: The Threat to Public Safety and the American Public. https://medium.com/homeland-security/spoofing-and-swatting-the-threat-to-public-safety-and-the-american-public-947c5316f65.
8. "Cyber Risks to Next Generation 911" https://www.dhs.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer%20FINAL%20508C%20(003).pdf

CDE EXAM #47929

1. 9-1-1 should not worry about cyberattacks because 9-1-1 systems are completely hardened and protected.
   a. True
   b. False

2. Which type of cyberattack does the following apply to? "Fraudulent practice of sending emails purporting to be from a reputable company in order to induce individuals to reveal personal information, such as passwords or credit card numbers."
   a. Ransomware
   b. Denial of service
   c. Phishing
   d. Spoofing/swatting

3. Which type of cyberattack does the following apply to? "_____ is a type of malicious software that infects and restricts access to a computer until a ransom is paid."
   a. Ransomware
   b. Denial of service
   c. Phishing
   d. Spoofing/swatting

4. Which type of cyberattack does the following apply to? "An attacker attempts to prevent legitimate users from accessing information or services."
   a. Ransomware
   b. Denial of service
   c. Phishing
   d. Spoofing/swatting

5. Which type of cyberattack does the following apply to? "Occurs when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity."
   a. Ransomware
   b. Denial of service
   c. Phishing
   d. Spoofing/swatting

6. The CIA Triad is a tool to access information security within an organization.
   a. True
   b. False

7. Spoofing isn't illegal and there is no need to report to government agencies.
   a. True
   b. False

8. Once a cyberattack has ended, which of the following should you mark for long-term retention to assist in investigations?
   a. Consolidated call logs
   b. Call and CAD recordings
   c. IP logs
   d. All of the Above

9. Cybersecurity attacks do not commonly start with a phishing attack.
   a. True
   b. False

10. If your PSAP is impacted by a cyberattack, which agencies should you contact?
    a. FBI (via the IC3 portal)
    b. Local authorities
    c. DHS-NCC- NCCIC
    d. All of the Above

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 the "CDE article" in the search box, and click on the "2018 Public Safety Communications Magazine Article Exams," then click on "enroll me" and choose "Cybersecurity for NG9-1-1 **(47929)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.