National Cyber Security Awareness Month 2014: Guidance for Public Safety Communications Professionals

Introduction

Public safety communications systems are becoming more integrated with advanced technologies than ever before. These developments bring both the promise of new capabilities, and the inherent issues of cyber security. The phased implementation of Next Generation 9-1-1 (NG9-1-1) and the ongoing work of the First Responder Network Authority (FirstNet) have created new imperatives and challenges for agencies to protect themselves from cyber risks and attacks. Reports of cyber breaches at major retailers and financial institutions are becoming all too common. Now imagine the same type of breach occurring in a public safety environment. As agencies start utilizing Internet Protocol (IP)-based networks and more mobile platforms, it becomes increasingly important to take steps to protect sensitive operations and confidential data. Additionally, as agencies move toward IP-based communications systems, the need to protect a network from external and internal intruders needs to become a priority.

October is National Cyber Security Awareness Month and is intended to remind everyone to be vigilant and safeguard their networks and the information passed over their networks. This paper provides information for public safety communications professionals on the ongoing threats to their networks and recommends ways to prevent, mitigate, and report cyber threats and attacks.

APCO continues to work with its partners in the federal government and industry to remain focused on keeping IP-based public safety networks and communications as secure as possible. Remember that prevention of cyber attacks starts with the end user and each person in an organization should be trained on how to identify, prevent, mitigate, and report any attack.

Identifying threats

The symptoms of an attack can vary depending on what the attacker is trying to accomplish. Damage can range from a minor slowdown of systems to a massive breach of data, or even worse, a complete shutdown of the network being attacked. It is important to identify a threat and respond to it in a timely manner in order to minimize the damage.

Traditional security measures will not always be sufficient to detect cyber attacks. Personnel responsible for public safety networks need to be able to identify the possible warning signs of an attack such as:

- An increase in the data being accessed/viewed by a particular user account;
- Unauthorized changes to an operating system;
- Unusual spikes in demand for network access or resources; or
- Unusual activity occurring outside of normal business hours (for example, activity in a secure database that would normally only occur at certain times of the day).

There are several types of attacks that public safety agencies and employees, such as those working in a Public Safety Answering Point, Emergency Operations Center, or police, fire or EMS department, need to be particularly aware of. They include, but are not necessarily limited to:

- **TDoS (Telephony Denial of Service)** – A TDoS attack is an attempt to overload a phone system by making a large amount of calls (often using automated dialing methods). This often involves an attempt to extort money from an individual or organization. In recent cases, a call is placed to an organization demanding payment as ransom to prevent a threatened TDoS assault. It is important to train personnel to immediately report this type of call to a supervisor. Initial indication of a TDoS attack may be a large number of "silent" calls that quickly fill up phone lines, which can impact 9-1-1 call-taking equipment at a PSAP that shares the same equipment. The system becomes overloaded, and normal business calls may be missed. In the public safety environment, this means that calls received on the administrative lines may not get through. In a worst case scenario, the phone system could be completely overwhelmed due to the large call volume, making it unusable.
- **DoS/DDoS (Denial of Service/Distributed Denial of Service)** – A Denial of Service (DoS) attack is an attempt to exhaust resources available to a network or server and interrupt access to genuine users. It is typically caused by infecting a user with a Trojan (i.e hidden or concealed) virus that then attacks the server through the infected machine. A Distributed Denial of Service attack (DDoS) is perpetrated by more than one host. In these attacks, a group of infected user computers attack a server/network simultaneously in an attempt to disrupt daily operation. Similar to TDoS attacks, DoS/DDoS attacks may include an attempt to extort money from an organization.
- **Swatting/Spoofing** – Swatting is when a person "tricks" emergency services into dispatching personnel to a fake incident. The incident is usually one that would send a

large amount of responders or even a "SWAT" team to a scene. The caller "spoofs" his or her number, making it very difficult to know who the real caller is. Spoofing is using the telephone system to indicate that the caller is calling from somewhere other than its real location. Often, during these types of attacks, a caller will utilize local information to make the incident seem more realistic. Swatting attacks continue to become more prevalent and can cause agencies to utilize a large amount of resources that would otherwise be available for other responses.

Swatting should be considered a serious threat to the operations of a public safety agency. In many of the cases, the suspects have been successful in having a large response to a fake incident. For example, see this FBI press release regarding an incident at the University of Connecticut that resulted in a multiple hour lockdown and required the response of the university police, Connecticut State Police Bomb Squad, and a SWAT team: http://www.fbi.gov/newhaven/press-releases/2014/wethersfield-man-charged-federally-for-role-in-swatting-incidents-at-uconn-elsewhere.

- **Network Intrusion –** Intrusion attacks should be considered a serious threat to the confidential data housed inside a public safety network. An intrusion attack is any use of a network that compromises the stability or the security of information stored on computers connected to it (see http://ids.cs.columbia.edu).
- **Phishing** – In an NG9-1-1 environment, information (data) contained in an email, text message, or other form of communication can make its way into a PSAP. Bad actors, posing as a victim or witness, could attempt a "phishing" attack in an effort to invade or take down the network. In a phishing attack, the bad actor includes a clickable piece of information (data) in an email or text message that if opened introduces malware into the public safety network. Consider the example of a purported "witness" directing a telecommunicator to examine a photo of a suspected perpetrator of a crime uploaded on social media. The link to the site sent by the bad actor could actually be a link to malware infecting the telecommunicator's computer.
- **Phishing phone calls** – Cybercriminals may call a PSAP's administrative or non-emergency lines and offer to help solve computer problems or sell a software license. If trust is gained, cybercriminals might then ask for user names and passwords or recommend a visit to a website to install software that will let them access a computer to "fix" it. This could lead to sensitive or confidential information being exposed, manipulated, or stolen.
- **Installation of hardware or software that contains malicious logic or unintentional vulnerability** – A considerable threat to agencies is installing hardware or software that may contain harmful or malicious code. In some cases, this occurs internally from users that bring outside hardware, such as a thumb drive, which are capable of housing any number of malicious software to infect a network. Agencies need to ensure they have a sufficient level of trust with suppliers of hardware and software – often referred to as supply chain security.

Prevention

A key element in the prevention of cyber attacks is the need to train employees on the proper use of their workstations. Administrators should outline a training program that includes, but are not limited to:

- Safe web browsing – Limit what web pages an employee can access and explain the consequences if this limit is violated. Closely monitor employee activity when browsing the web.
- Smart passwords – Utilize a password system that requires the use of multiple types of characters, does not allow the use of common words, and has to be changed on a regular basis. Ensure that employees understand that a password should not be shared, even amongst peers, as this could lead to a serious breach in security.
- Do not allow employees to utilize foreign devices (thumb drive, etc.) in any workstation.
- Require that all employees log out of their workstations at the end of their shift. If an employee is going to step away from their workstation, it should be locked to keep anyone else from accessing their accounts.
- Encourage employees to report any unusual activity to a supervisor immediately. Diligence in reporting has proven to be a successful way to minimize the effects of an attack.

Also important in preventing a cyber attack is having a plan in place designed to handle such an attack. Even agencies that currently use legacy systems should start looking at how they will protect their information as they transition from legacy systems into an IP environment. It is no longer sufficient to just have a firewall and good anti-virus protection in place. Public safety networks and systems require advanced methods to protect data and connections. Education is one of the best weapons against these attacks. It is important that agencies become generally knowledgeable of NG9-1-1 and IP-based communications platforms in order to best understand how attacks can be perpetrated. Additional information about NG9-1-1 networks can be found at www.apcointl.org/resources/next-generation-communications-systems.html which has several sections on topics such as text to 9-1-1, FirstNet, and emerging technologies.

In addition to educating staff on the technology involved in next generation systems, and the vulnerabilities inherent with these new technologies, PSAP managers, supervisors and network administrators need to look for ways that intruders may enter their "closed" networks through third party vendors. Ask service providers and vendors how they protect their connections and hardware from attack and use that information to put together a solid plan. PSAP directors/managers should work closely with their vendors and ask question on how they account and detect cyber breaches. Employees should have access to an updated list of vendor contact information and should be trained to contact them if unusual situations arise.

Agencies should reach out to local and state agency staff that are responsible for IT network security. As technology continues to grow, and the demand to have quicker and more seamless access to 9-1-1 increases, the need to have a well thought out plan of action becomes more important.

There are a number of federal resources available as well. For tips to secure web browsers, for example, see https://www.us-cert.gov/publications/securing-your-web-browser. In addition, the Department of Homeland Security's "Stop.Think.Connect" campaign has tips and a simple action plan for responding to an incident: http://www.dhs.gov/stopthinkconnect-cyber-tips. The FBI has information on how to protect your computer here: http://www.fbi.gov/scams-safety/computer_protect. The Federal Communications Commission offers a few helpful links, including a "Small Biz Cyber Planner 2.0" and a one page Cybersecurity Tip Sheet.

Mitigation

Deploying a policy that regularly checks the status of a network can help mitigate the effectiveness of an attack. The opportunity to stop an attack quickly becomes more possible if someone or some mechanism is frequently monitoring network activity. Systems administrators should avoid falling into a false sense of security just by employing firewalls, virus software, etc. A combination of automated technology and vigilant staff are important to limiting your exposure.

Mitigating the potential damage from a cyber attack can be as simple as checking the status of the network on a frequent basis. In addition, make sure personnel are trained on recognizing these attacks. Quick reporting of issues can reduce, and in some cases stop, an attack before it has time to damage or compromise a network.

The following are specific measures that can be taken for various types of attacks:

TDoS Attack

- Get in touch with your appropriate telephony service provider to learn how to address a TDoS attack should it occur. The discussion may involve both a 9-1-1 system service provider and an administrative line provider. Keep the contact information for these providers current and make sure that all employees know how to contact them if they have an issue.
- Look for ways to isolate critical phone lines (such as incoming 9-1-1) from administrative lines. Do not allow the administrative lines to roll over to incoming emergency lines.
- Organizations should not pay any extortion/blackmail attempts.
- Notify the telephony service provider, as it may be able to block part of the attack.

Additional information from APCO about TDoS attacks and best practices on handling this type of attack can be found at http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/

DoS/DDoS Attack

- Speak with the appropriate network service provider and inquire about the protections they have built into their networks so that agencies can build upon these protections to assist in keeping their networks safe and running.

- Be prepared to have a backup (redundant) system. If an attack should occur, train all users how to switch to this system. Redundant servers should be incorporated into the design of the system and should facilitate allowing administrators to switch (or in some cases automatically switch) to the redundant node in case of a failure or overload situation.
- Take down the name and call back number of the caller that is using extortion to threaten an attack. The supervisor should report the incident to local investigators as soon as possible.

Swatting/Spoofing

Telecommunicators should be aware of this type of threat. However, calls should be handled according to standing policies. If, after the initial response, it is determined that a swatting event has occurred, the agency should investigate it as they would any other case. All pertinent information about the caller (name, location, call back number) should be recorded and any voice recordings should be saved for the investigation. The agency may contact state resources or the FBI for additional assistance in handling this type of case. Specific recommendations as to mitigation of Swatting and Spoofing attacks are currently under development.

Network Intrusion

Automatic detection systems can be used as one method to detect this type of attack. However, it is a combination of methods that will best secure a network. It is important for system administrators to keep their anti-spyware, anti-virus, and anti-phishing software updated and active. Equally important is to have a good network security policy in place for users to follow. Intrusion attacks are often perpetrated through a user's action without that individual knowing that he or she is the vehicle being used for the attack. Limiting internet access, restricting what devices can be plugged into a work station, and requiring password changes on a regular basis will assist in avoiding this type of attack. Agencies should make a priority out of instituting a continuing education program for employees at all levels on the importance of network security. Training on network intrusion detection is available from a number of private and academic sources.

Information about planning and mitigation can be found via the following links:

http://transition.fcc.gov/cyber/cyberplanner.pdf

http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

http://transition.fcc.gov/cyber/cyberplanner.pdf)

http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

Reporting

Depending on the type of attack, steps can be taken to assist in the investigation. A list of these steps is included below; please also refer to the links at the bottom of this paper for additional resources.

TDoS attacks should be reported to the Internet Crime Complaint Center at www.IC3.gov. Ensure that in the title of a report the keyword TDoS is used. Identify your organization as a PSAP or public safety organization. Provide as much detail as possible including;

- Call logs from the "collection call" and TDoS.
- Time, date, originating phone number, and identifying characteristics about the caller.
- Call back number for the "collections" company or requesting party.
- Method of payment and account number where the requester wants the ransom to be paid.

A DDoS attack should also be reported to the FBI's Internet Crime Complaint Center at www.IC3.gov and should include as much information about the attack as possible. Agencies can also contact the local FBI office to receive additional information about reporting this type of incident.

Swatting attacks are generally handled at the agency level. An agency should contact its state resources for additional guidance on this type of attack. It is important to keep all of the information pertaining to the call including, recordings, ANI/ALI information, and any other information that may assist in identifying the suspect.

Intrusion attacks are also generally handled at the local level. Diligence in finding the source of the attack and taking corrective measures to reduce an agency's data loss or corruption is very important. An agency may also seek assistance from its state government on dealing with this type of breach.

Conclusion

As technology continues to play a larger role in public safety communications, the need for better security procedures becomes a more important aspect of conducting business. Personnel need to become better educated on the risks associated with these threats and how to react if they are the victim of an attack. Cyber-based attacks can have serious ramifications. Additional information about cyber security can be found at https://www.apcointl.org/advocacy/topics/cybersecurity.html. The security of public safety networks relies on the diligent efforts of the people tasked with maintaining these systems. Awareness is the first step towards a comprehensive Cyber Security policy, and towards protecting our networks and agencies from these attacks both now, and in the future.

References

APCO – Best Practices for TDoS attacks
http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/

APCO Government Relations Cybersecurity Resources and Information
https://www.apcointl.org/advocacy/topics/cybersecurity.html

FBI – Internet Crime Complaint Center
www.IC3.gov

Next Generation 9-1-1 Information
www.apcointl.org/resources/next-generation-communications-systems.html

www.ng911institute.org