An accessible best practices guide to implementing effective cybersecurity policies and procedures within the PSAP.

Cybersecurity Attacks: Detection and Mitigation

A Guide for PSAPs

July 2018

APCO International
Leaders in Public Safety Communications®

APCO Cybersecurity Committee

Contents

Introduction 2

Phone Systems 3

Radio Systems 4

US Homeland Security Warns on Critical Vertical Attacks 4

Network-based Information Technology Systems 4

What to do After an Attack 5

Policy and Procedure 7

Conclusion 8

References 10

Introduction

This document is a continuation of An Introduction to Cybersecurity: A Guide for PSAPs[1] prepared by APCO International's Cybersecurity Committee. The primary goal of this document is to specifically address the types of attacks a PSAP is likely to encounter, the systems that are likely to be attacked and how to mitigate the immediate impacts of an attack.

According to the U.S. Department of Homeland Security's (DHS') Cybersecurity Strategy, "During the last several decades, advances in technology have fundamentally changed the world. Substantial growth in Internet access, use of Internet-enabled devices, and the availability of high speed information technology systems and large datasets have facilitated productivity, efficiencies, and capabilities across all major industries. This proliferation of technology also presents new cybersecurity challenges and leads to significant national risks. More than 20 billion devices are expected to be connected to the Internet by 2020. The risks introduced by the growing number and variety of such devices are substantial."[2]

It is critical that agencies understand what systems are likely to be affected and what an attack to those systems might look like. An attack against a smartphone operating system, such as autodialing multiple times during a Distributed Denial of Service (DDoS) attack, might be obvious. Other attacks, such as with code inserted by way of shortened links, malicious scripts or multiple variants of malware or spyware that the user will never see, are more insidious. To identify attacks, obvious or insidious, it is important to be aware of the dangers of threats embedded in a system that could be collecting data over time or be part of an attack.

If an agency does not already have a plan in place to deal with a cybersecurity attack, it is imperative to take immediate action, formulate a plan and make it readily available to Emergency Communications Center (ECC) staff. Ensure that a point-of-contact is identified who is ready to activate the appropriate cyber response resources while Public Safety Telecommunicators (PST) and first line supervisors strive to keep services operating. Ensure that direct contact information is identified for telephone and 9-1-1 systems service providers, as well as the account representatives for Computer Aided Dispatch (CAD), Records Management Systems (RMS) and logging and recording software. Many

Impact on Law Enforcement

"We all operate daily in the cyber realm – we check email, we search the Web and we stream videos. The same holds true for the daily life of a police chief, a sergeant or a patrol officer. The difference between police and the rest of us lies in the risk that comes with all of those virtual activities. An unprotected database with confidential informant information can lead to lives lost. An unsecured network that is hacked can paralyze an entire department."

Cybersecurity Guide for State and Local Law Enforcement - NCAP

[1] www.apcointl.org/download/introduction-to-cyber-security-a-guide-for-psaps/?wpdmdl=6250
[2] www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

of these systems have mobile components, all of which can be vulnerable to a cyberattack. Keeping a current, verified, direct contact list for all service providers and vendors must be a priority for an ECC.

Phone Systems

The type of attack that a ECC's phones system is most likely to experience is a Telephony Denial of Service (TDoS) attack. According to APCO's P43 report, a TDoS attack is, "flood of unwanted, malicious inbound calls. The calls are usually into a contact center or other part of an enterprise, which depends heavily on voice service."[3] The goal of this type of attack is to overwhelm the phone system with calls.

TDoS attacks vary in complexity. In the simplest form, TDoS attacks come from one single contact point that may or may not utilize a spoofed number. This type of attack is most effective against smaller agencies since it does not take a substantial number of phone calls to tie up all of the phone lines. However, recent events have demonstrated that with relatively little sophistication, and only moderate resources, a TDoS attack can impact large ECCs as well. Regardless of the complexity of the attack, if the volume of phone calls is significant enough, any TDoS event can tie up resources making it difficult not only to locate the source but to also identify and process legitimate requests for service. More complex attacks, "employ sophisticated spoofing technology with calls appearing to originate from all over the country."[4]

Prevention and mitigation of a TDoS attack is not an easy task. Each ECC should consult with respective IT departments to identify options available for preventing an attack and how to respond to an attack so as to mitigate impact. The plan should include a training component to educate employees on what an attack would look like and what steps the agency will take to mitigate the impact. At a minimum, each ECC should have readily available emergency contact lists for all potentially impacted systems. At the onset of the attack, the best defense is to immediately contact the experts in those systems and engage their assistance. As another example of response, the ECC may distribute alternate phone numbers to the community.

[3] www.apcointl.org/ext/pages/p43/p43book.html

[4] securelogix.com/threats/telephony-denial-of-service-tdos-attacks/

Radio Systems

Interference to radio channels can reduce the capacity of a trunking system or render a conventional system unusable. Interference could be the result of intentional jamming, saturation or an actual "hack" of control elements or base stations. Additionally, connectivity between various components of the radio system and the radio consoles may be subject to Denial of Service (DoS) and other types of network attacks causing the loss of some or all system elements.

A plan in place to mitigate the loss and/or reduction of service should be available at all ECCs. To supplement this plan, ECCs should ensure that personnel are trained to recognize anomalies and that supervisors are trained to recognize when the system is experiencing issues and are prepared to notify the proper personnel for corrective action. Supervisors should be trained in basic radio troubleshooting, so that they are able to distinguish a relatively routine problem from one that has larger implications.

Agencies should consider the design and features of the radio system. For example, agencies should consider whether it is practical to use an isolated network for the radio system. If this option is chosen, what will the interoperability challenges be? Additionally, the radio system features should include a network management system that can notify the personnel when a system element becomes non-responsive or the network is compromised. If the radio system does not have such notification features, agencies should research what would be required to implement this type of control element.

Network-based Information Technology Systems

Network based systems (i.e., CAD, e-mail, etc.) which communicate with other systems or devices are typically connected to the public network which makes them especially vulnerable targets. ECC staff should be trained and able to recognize service interruptions or abnormal system behavior and whether or not the interruption or behavior is believed to be the result of a cyber-attack.

Phishing attacks are one of the most commonly used tactics to deliver malware, or other undesired code, which enables hackers to access a networked IT system. One of the most common ways of gaining access is

US Homeland Security Warns on Critical Vertical Attacks

The National Cybersecurity and Communications Integration Center (NCCIC) at the US Department of Homeland Security has issued a warning on an emerging sophisticated campaign targeting critical verticals, including public health, critical manufacturing and IT.

The campaign has been active since at least May 2016, NCCIC said, using multiple malware implants. The threat actors appear to be leveraging stolen administrative credentials (local and domain) and certificates—and could instigate a medium-priority incident affecting public health or safety, national security, economic security, foreign relations, civil liberties or public confidence.[5]

[5] www.us-cert.gov/ncas/alerts/TA17-117A

by sending out legitimate looking emails which will deliver malware when opened or when an attached file/link is opened.

Agencies must develop an action plan for how to deal with possible attacks. Agencies should train employees to identify phishing emails and to prevent other cyber-attacks. Prompt notification to an agency's IT Department is the best defense once a possible attack is identified.

If a system starts to function abnormally, employees should know who to advise, what information is required to report the issue and what immediate actions are needed. Agencies should develop policies and procedures for mitigating or minimizing the effects of a cyberattack. As an example, an agency in conjunction with their IT staff may develop a procedure for disconnecting potentially infected or compromised systems from the network as shutting down the system may not be an alternative. Some malicious code activates when a system shutdown is initiated, with the initial attack only being a precursor to the actual attack. Having the ability to disconnect or firewall the running system immediately isolates it from other systems on the network and is often a very effective step.

What to do After an Attack

Agencies need to have a plan for maintaining the ability to function while the issues are addressed. If an agency has been the victim of a cybercrime, the IT department should be the first contact after an attack is identified. IT staff most likely will have the agency follow steps to isolate the computer from the rest of the network and then will run diagnostics on that particular piece of equipment before taking further action. A large number of cybercrimes are not locally perpetrated and the hacking of computers for fraudulent or disruptive reasons is a crime. Often, the attackers live outside the state, and even the country from their victims. If the IT Department determines that the computer has been compromised, local law enforcement agencies should be contacted. They will be able to determine the criminal nature of the event, and jurisdiction. If the local agency determines the crime is interstate in nature, they will contact the appropriate federal authorities. There are several federal agencies that reports can be filed with for help in tracking down cyber criminals and helping to stop the spread of cybercrimes. Local law enforcement agency should have the information needed to make such a report.

According to DHS, a cyber incident is a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. State, Local, Tribal and Territorial (SLTT) partners are encouraged to voluntarily report suspected or confirmed cyber incidents to a federal entity. In particular, a cyber incident should be reported if it:[6]

- May impact national security, economic security, or public health and safety.
- Affects core government or critical infrastructure functions.
- Results in a significant loss of data, system availability, or control of systems.
- Involves a large number of victims.
- Indicates unauthorized access to, or malicious software present on critical information technology systems.
- Violates federal or SLTT law."[7]

Once an attack or hack has been identified, or even suspected, it is never too soon to report it. When reporting cyber incidents, there is some basic information that should be provided that will help expedite aid to the agency. Even if some of the information is incomplete, or unavailable, it will still be helpful to report as much as possible.

SLTT law enforcement can report to the federal government in person, by e-mail, by phone or via online tools. Who and where to report the incident to depends on the type of incident that is being reporting.

[6] www.dhs.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting_3.pdf
[7] Law Enforcement Cyber Incident Reporting, FBI File repository

Incident Type:	**Organization and Points of Contact**
Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance	National Cybersecurity and Communications Integration Center (NCCIC) (http://www.dhs.gov/about-national-cybersecuritycommunications-integration-center) NCCIC@hq.dhs.gov or (888) 282-0870
Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information	Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml) Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)
Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights	ICE HSI Field Offices (http://www.ice.gov/contact/inv/) ICE HSI Cyber Crimes Center (http://www.ice.gov/cyber-crimes/)
Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity	FBI Field Offices (http://www.fbi.gov/contact-us/field) Cyber Task Forces (http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-thenations-cybersecurity-1) Internet Crime Complaint Center (IC3) (https://www.ic3.gov) Law Enforcement Online Portal (https://www.cjis.gov/CJISEAI/EAIController) or (888) 334-4536

Policy and Procedure

A critical part of any agency's cybersecurity plan are the policies and procedures in place to direct ECC personnel in the event of an attack. When an attack occurs time is critical and ECC employees must have easily accessible guidance steps to take and must be able to access the relevant information quickly. Having written policies and guidelines on what steps to take when made aware of an attack will help ensure that when the attack is ended, the damage is assessed and mitigated as quickly as possible.

When developing these procedures, consider the following elements:

- Create a cyber-attack response team that includes the following departments:
  - IT Department Staff
  - System Vendor
  - Executive Staff
  - Other agencies with neighboring or concurrent jurisdiction
  - State and Federal partners
- How will the response differ if an ongoing attack operating behind the scenes is discovered?
- Who is the point of contact to activate the response team? First-line supervisors and PSTs will be too busy trying to keep operations running smoothly.
- In addition to notifying the response team, what actions should first-line supervisors take at the onset/discovery of an attack?
- What are the procedures for activating additional personnel to respond to the center?
- Is an alternate / backup ECC available? If so, is it likely to be affected by the same attack or will it likely be available for use?
- Who is responsible for documenting the incident?
- Preparation of an after-action report (AAR).
- What type of cyber security training is being provided to ECC personnel and how often is the training?

Protecting 9-1-1 call centers from cyber threats: Federal action needed

"NG9-1-1 will allow our growingly wireless society to access 9-1-1 through texting and mobile apps, as well as send images, videos, emails, and other documents…any of which could contain embedded viruses that rapidly infect the network. First responders are also making greater use of data and cloud computing. Sensitive public safety information stored on the cloud such as emergency medical patient care reports and police body camera video could become targets for cyber hacking."[8]

Conclusion

Mitigating the impact of a cybersecurity attack is heavily dependent upon the steps taken prior to the attack itself. Policies and procedures must be in place guiding employees on how to avoid exposure to cybersecurity threats. These policies and procedures must also advise personnel what to do when an attack occurs or when the evidence points to a possible attack.

Educating all of ECCs employees about cybersecurity prevention and identification is also key. PSTs are likely to be the first to experience any adverse effects. Therefore, they must be informed and ready to take action immediately. If an attack occurs, the ECC should have a designated response team with each member's roles clearly defined. It is important to know what additional resources are available and how to reach out to those entities.

[8] www.securityinsights.org/2015/05/protecting-911-call-centers-from-cyber-threats-federal-action-needed/

Cybersecurity is now a way of life for ECC professionals. While it has not historically been a concern, today's technology environment makes cybersecurity a necessity for every ECC. Being educated, prepared and aware of the ever present threat is the only way to mitigate it. By being proactive today, ECCs can better deal with the attacks that are sure to come tomorrow. As with anything in public safety, we must plan for the "when", not just the "if".

References

APCO Introduction to Cybersecurity. (2016, August). Retrieved from www.apcointl.org/resources/cybersecurity/cyber-security-guide-for-psaps/file.html

APCO Project 43 – Broadband Implications in the PSAP. (2017, August). Retrieved April, 2018, from https://www.apcointl.org/doc/911-resources/apco-projects/716-apco-p43-report/file.html

Brown, R., Cabrera, E., Carabin, D., Furay, J., Garcia, C., McNeal, C., Wright, W. (2016, June). Cybersecurity Guide for State and Local Law Enforcement. Retrieved June, 2018, from https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/NCAPCybersecurityGuide-2016.pdf

Cyber Incident Response. (2017, February 17). Retrieved April, 2018, from https://www.dhs.gov/cyber-incident-response

FCC TFOPA Report (FINAL). (2016, December). Retrieved April, 2018, from transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

Framework for Improving Critical Infrastructure Cybersecurity. (2018, April 16). Retrieved April 18, 2018, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Law Enforcement Cyber Incident Reporting. (n.d.). Retrieved June, 2018, from https://www.dhs.gov/sites/default/files/publications/Law Enforcement Cyber Incident Reporting.pdf

NIST Special Publication 800-63B, Digital Identity Guidelines. (2017, June). Retrieved April, 2018, from pages.nist.gov/800-63-3/sp800-63b.html

SANS Institute, Acceptable Use Policy Document. (2003). Retrieved April, 2018, from www.sans.org/reading-room/whitepapers/policyissues/acceptable-policy-document-369

Seals, T. (2017, May). US Homeland Security Warns on Critical Vertical Attacks. Retrieved June, 2018, from https://www.infosecurity-magazine.com/news/us-homeland-security-vertical

Sommers, S. (2015, May). Protecting 911 call centers from cyber threats: Federal action needed. Retrieved June, 2018, from https://www.securityinsights.org/2015/05/protecting-911-call-centers-from-cyber-threats-federal-action-needed/

The Telephony Denial of Service (TDoS) Threat. (n.d.). Retrieved June, 2018, from https://securelogix.com/threats/telephony-denial-of-service-tdos-attacks/