Securing The Next Generation Of 911

Published on 8 Jun 2021

While conducting research for my 2021 Wisconsin Public Safety Commission (WIPSCOM) conference presentation, it became immediately clear that securing the nation's public safety answering points (PSAPs) is no longer just an IT challenge.

Shifting from an analog to digital operating environment — the next generation of 911 — will require strategic investments into three key areas: people, processes and technology. As call center technology evolves nationwide, the need for greater cybersecurity in the public safety space has never been more important.

Internet connected systems

Traditionally, PSAPs received calls over analog telephone networks consisting of copper wire transmission lines and dated cellular networks spanning a smaller area in close proximity to call centers. With the introduction of next generation 911 and the accompanying digital telephone

networking services, the exposure of call center networks to would-be attackers has exponentially increased, allowing potential access from anywhere due to internet connected systems.

A good analogy is thinking of the points of entry into your home. The legacy method allowed two entries into the house — the front and back door. With the introduction of digital networks, there are now more doorways into the home or call center, signifying a greater need for security and employee awareness of threats.

First responder organizations

Since 2019, there have been approximately 300 cyberattacks impacting local government agencies, including police stations, emergency dispatch call centers and first responder organizations. 125 of these attacks specifically focused on public safety agencies such as firefighting or EMT stations, with attacks reported in all 50 states. More recent examples show that cyberattacks focusing on our first responders are increasing at an alarming rate.

Many of these recent attacks target people using a technique called social engineering. This is when attackers attempt to trick victims through telephone calls and/or emails to assist the attacker in introducing viruses to the network, provide sensitive data or share usernames and passwords to achieve their criminal motives. Cyber criminals' primary objective is to use social engineering techniques to achieve a much more serious attack: ransomware.

Critical computer systems

> Ransomware is a type of malicious software (malware) that prevents access to sensitive files

Ransomware is a type of malicious software (malware) that prevents access to sensitive files, data and critical computer systems using encryption that only the attacker can unlock. Victims must pay a random sum of money, usually in an untraceable cryptocurrency, to the attacker who promises to decrypt data once they receive the funds.

A look at attacker motivations can help us all understand — and mitigate — the threat to our first responders. Here are three primary reasons why cybercriminals target public safety answering points:

- **Monetary gain**: Infecting a PSAP with ransomware can lead to significant payouts in order to restore first response services.
- **Disruption of services**: Shutting down critical services can put threat actors in the public eye while also playing a major role in multi-stage attacks.
- **Cheap thrills**: Attackers and, at times, even misguided amateurs can target critical services for notoriety or social standing.

Mitigating cyber risk

> The human element, actions or inactions played a direct role in 85% of data breaches

Regardless of the motivation, the outcome is generally the same: a disruption of first response services that are critical to protecting our communities and families. According to Verizon's 2021 Data Breach Investigations Report, the human element -- or people’s decisions, actions or inactions -- played a direct role in 85% of data breaches.

As cyber threats targeting PSAPs and first responder teams continue to grow in number and severity, addressing the threat through employee awareness and education is a good first step in mitigating cyber risk. Here are four steps any PSAP can take now to assess and mitigate cyber threats targeting their organization.

Security awareness training

Educate employees with security awareness training - Ongoing security training efforts should occur at a general level for all PSAP employees, followed by more targeted, role-based

security training for key roles and departments such as call center managers, dispatchers or those with access to sensitive data. General security awareness training efforts should focus on broad but relevant security topics employees are likely to encounter, such as how to identify a phishing email.

> Security training programs should occur at least annually, and training content reviewed semi-annually

Role-based security training efforts should go one step further and include topics like how management should respond to ransomware payment demands or how to verify the identity of external callers asking for sensitive information or urgent payments. Security training programs should occur at least annually, and training content reviewed semi-annually to ensure completeness, accuracy and relevance of training content related to your operating environment.

Physical building access

Verify and strengthen employee access controls - This includes physical building access and logical access to any information or computer systems your organization operates. Most organizations have several internal or external users such as vendors, cleaning companies and other organizations who come into contact with the offices or other physical locations, increasing the risk of theft or unauthorized access via impersonation or tailgating attacks.

Ensure exterior locations are sufficiently secured via electronic badge access or a minimum of key access with code entry. First responders and public service agencies should train employees to visibly display employee badges and report infringements to management in the event an attacker infiltrates the building.

Multi-Factor authentication

> External visitors should be required to announce their arrival in advance to the organization

External visitors should be required to announce their arrival in advance to the organization, enter through designated areas, check-in with a receptionist or direct contact, log their entry, show identification and wear a clearly identifiable visitor badge.

Access to computer systems that contain sensitive data such as employee records or connections to other state and federal agencies should be secured via multi-factor authentication. Multifactor authentication is a security term referring to authenticating a computer system using several factors, including something you know (e.g., username or password) , something you have (e.g., smartphone) or something you are (e.g., fingerprints or voice pattern). Using two or more factors when accessing a computer system is crucial to keeping the cybercriminals out!

Federal threat intelligence

Leverage free resources to mature your cybersecurity posture - First responders and public service organizations have many free cybersecurity resources at their disposal. This includes federal threat intelligence via security advisories, which outline vulnerable software or hardware products they use, and direct consultation services from cyber response teams local to the area, which are taxpayer funded.

> The US-CISA also provides regional consultation services to assist all local government agencies

Every first responder and public service organization should consider becoming a member of a relevant Information Sharing and Analysis Center (ISAC) such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), as they provide free threat intelligence services and consultation resources to help boost cybersecurity. The US-Cybersecurity and Infrastructure Security Agency (US-CISA) also provides regional consultation services to assist all local government agencies in maturing their cybersecurity posture.

Public service organizations

Hire external security firms to identify and correct weaknesses - To the extent allowed by budgets and personnel, first responders and public service organizations should hire external security or audit firms to assess the state of their cybersecurity practices and posture.

These firms specialize in security best practices and assess security controls' adequacy across a wide array of organizations. It is often useful to bring these firms in for a fresh perspective on how the organization operates and its vulnerabilities. These engagements are typically performed annually and focus on core computer systems and business processes that involve sensitive data.

View this article on TheBigRedGuide.com.

Author Profile

Adam Kohnke

You may also be interested in...

Need For Wearable Technology In Mission-Critical Environments

The front line fire and rescue teams have had their hands full during the pandemic, more so than one might think. In the UK, for instance, f...

Fires At Rental Storage Units Highlight Need For Sprinklers

Rental storage units represent a serious and unpredictable risk for firefighters. For example, hundreds of rented units at a three-story, se...

Thinning Forests To Prevent Wildfires Can Yield A Useful Byproduct: Bi...

Thinning forests to prevent wildfires include the removal of diseased trees and other debris by private, state, and federal land managers. T...

What Are Emerging Technologies In Wildfire Prevention And Protection?

Wildfire season presents special challenges to firefighters, and environmental trends point to even more frequent wildfires in the future, d...