MONTRA SOLUTIONS

Protecting America's NextGen 911 Networks

How Securing MSRP Traffic Can Make a Difference for Public Safety Answering Points

Hackers and cybercriminals are increasingly targeting emergency response networks throughout the country.

Henry County, Tenn., faced a ransomware attack where hackers shut down the dispatch system for the county's 911 call center and demanded $2,000 in bitcoin to turn it back on, resulting in the call center manually taking information from callers. The city of Baltimore's 911 system was hacked, which caused a temporary disruption that also forced call center support staff to manually manage calls.[1]

According to reports, more than 40 attacks in the last three years have targeted 911 dispatch centers. However, these attacks could increase as traditional 911 networks transition to NextGen 911, which enables receipt of video, text and other data from the public over a variety of computer networks.

The risks associated with NextGen 911, including data breaches, malware, denial of service attacks and more, highlight just how critical it is for local governments to secure their emergency response networks. Advanced security solutions that protect Message Session Relay Protocol (MSRP) communications, a protocol that enables the exchange of instant messages, large files, images and other data over an internet network, can help local governments modernize without increasing risk.

The Emergence of 911: Understanding Public Safety Answering Point (PSAP) Architecture

Though residents in any U.S. location can dial the same three-digit number when they need help, the underlying infrastructure of the country's 911 network is a patchwork of disparate systems.

The U.S. has 5,700 separate state and local public safety answering points (PSAP), each of which operates differently and typically provides service at the county level. When someone dials 911, emergency calls are routed by telecom providers over a dedicated line to the appropriate PSAP, which uses computer software to manage caller information and dispatch these calls to the relevant public safety agency.

Traditional PSAPs rely on legacy technologies, which function as closed internal networks that have minimal interconnections with other systems. This reduces the attack surface, but it also makes technology modernization more challenging.

However, traditional 911 networks have slowly evolved. Over the last decade, e911 services, which can identify mobile calls, have become more prevalent. This has paved the way for the emergence of NextGen 911 systems, which don't rely on the standard voice-based telephone networks that traditional 911 networks do.[2] NextGen 911 uses IP-based networks that enhance the response capabilities of 911 call centers and public safety agencies. They enable PSAPs to perform call transfer and data sharing and allow them to accept calls from mobile, text and voice applications. Today, there are more than 2,200 partially implemented NextGen 911 systems that accept texts.

Though NextGen 911 systems allow PSAPs and public safety agencies to deliver more responsive service that saves lives, they also come with increased security risks, says Kenny Holmes, Head of Public Sector at Fortinet, which provides security-driven networking solutions for government.

"The biggest risks are outages, which can come in the form of denial of service attacks that overrun the service provider or infrastructure in some way," Holmes says.

Other security risks include malware, ransomware and spoofing, a security event that involves an unauthorized device disguising itself as an authorized device. Malicious applications created by hackers that steal, corrupt and modify data, eavesdrop on conversations, and obtain data on the location of victims and first responders are another security threat. So is swatting, which involves the manipulation of IP-based calls to make authorities think these calls are coming from locations where serious crimes have occurred. When this happens, public safety agencies dispatch teams to the location, which wastes public resources.

Holmes says public safety agencies can reduce these security issues by mitigating risks in the MSRP protocol, which is responsible for transmitting instant messages over IP networks. By focusing on securing MSRP messages, agencies can make their systems more secure and reduce the likelihood that a denial of service, malware or other cyberattack occurs.

Securing PSAPs: The Advantage of an MSRP-Focused Security Solution

An MSRP protocol is used to facilitate large-scale instant messaging — including transferring large files such as video and images — within NextGen 911 systems.

Text-to-911 and NextGen 911 systems are typically self-contained, proprietary solutions that communicate with Text Control Centers (TCCs) via the MSRP protocol and integrate directly with these systems' emergency dispatch software. However, TCCs don't perform security inspections on MSRP messages, which can contain malicious URLs, malware attachments and other security threats. The best approach is to perform security inspections on MSRP messages before they enter these systems. However, most point solutions on the market don't have this capability.

Doug Boreham, Principal Systems Engineer for the State and Local Government, and Education Team at Fortinet, says public safety agencies need an MSRP protocol decoder, an advanced security solution that "analyzes those text messages and attachments as they're flowing from the Text Control Center into the PSAP."

He says agencies can deploy an appliance or network device in-line within their existing call workflow and PSAP architecture to properly inspect MSRP traffic and provide security reinforcement.

Automated solutions can generate MSRP messages much faster than a human can type, which can overwhelm NextGen 911 systems and block emergency calls. However, with an MSRP protocol decoder, PSAPs can limit the rate of MSRP messages coming into NextGen 911 systems.

"If the messages are coming in at a rate that's much faster than a human can process, an MSRP protocol decoder can alert your administrators that this is a problem. If a certain threshold is reached, it can potentially trigger automated actions such as dropping those messages," Boreham says.

The solution also can inspect text messages or images for security threats like malware, as well as inspect embedded malicious URLs. PSAPs need advanced threat detection capabilities and an MSRP protocol decoder can provide this by applying existing intrusion prevention systems (IPS) signature sets to MSRP traffic to surface known threats and block this malicious traffic. It also can detect and flag MSRP messages that are frequently repeated, monitoring certain predetermined thresholds and alerting IT administrators when these thresholds are exceeded.

This solution bolsters security by creating redundancy and ensuring PSAPs have no single point of failure. An MSRP protocol decoder also makes PSAPs more resilient because it can be scaled to support increases in traffic growth associated with multimedia messages, while giving them access to threat intelligence and insights they can use to combat future security threats.

Boreham says an MSRP-focused security solution "raises the awareness of your organization so you can know what's going on and then act as needed. That's very important in an environment where seconds literally mean the difference between life or death," he says.

Conclusion

As more local governments transition to NextGen 911 systems, security is paramount.

Holmes says rather than adopting point solutions with narrow capabilities, local goverments need a platform to provide a security strategy with products that work together and offer automation via artificial intelligence and machine learning. Fortinet calls this "The Fabric" since it further allows for adopting solutions that are already integrated to strengthen the overall security posture.

To accomplish this, Holmes says local governments should seek the help of a security-focused technology provider that understands their organization's IT infrastructure. They also should consider an enterprise security platform that provides end-to-end visibility and has features like MSRP protection and proactive detection and prevention response capabilities mapped to standards like the NIST Framework. With this approach, PSAPs can scale their IT infrastructure as new data sources emerge that need to be routed through NextGen 911 systems.

All the services local governments deliver to constituents are important, but arguably none are more critical, timely and urgent than 911 services. With advanced MSRP-focused security solutions, local governments can make their 911 networks more resilient even as they modernize these systems to deliver more responsive service. Saving lives is the core mission of PSAPs and public safety agencies, but today that means more than just dispatching emergency responders to the scene. Cybersecurity has become just as essential to public safety and adopting the right solutions can empower local governments with the capabilities they need to render potentially lifesaving aid to constituents when they need it most.

This piece was written and produced by the Government Technology Content Studio, with information and input from Fortinet.

1. https://www.nist.gov/industry-impacts/cybersecurity-framework 2. https://www.911.gov/issue_nextgeneration911.html & Fortinet NextGen911 Webinar

PRODUCED BY: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

FOR: FORTINET®

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.
www.fortinet.com