CDE #54568

MUDDY FOOTPRINTS ALL OVER YOUR NETWORK

How intrusion detection and prevention systems can help guard against cyber sabotage

ISTOCK.COM/D-KEINE

By Megan Bixler

Imagine that you and your significant other went out to dinner. When you get home, your front door is open. As you go inside, you notice that your living room looks different. Your television is missing, and there are muddy footprints all over. You conclude that somebody broke into your house and stole your television. An alarm system would have helped to alert you that this was happening.

We've all heard countless times how anything that touches the internet is susceptible to a cyberattack. With the internet of things (IoT), Next Generation 9-1-1 (NG9-1-1), and countless other things that are connected to the internet, the risk for cyberattacks is at an all-time high. The television thief story is a real-world example of what an intrusion detection system (IDS) can do. According to the National Institute of Standards and Technology's (NIST) "Guide to Intrusion Detection and Prevention Systems (IDPS),"[1] "Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices." An IDS is analogous to what an alarm would provide in a break-in. It warns when an attacker (e.g., thief or cybercriminal) gains unauthorized access to possessions or systems.

"An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents."[2] IPS provides policies and rules for network traffic to alert the necessary people (often network administrators) of suspicious traffic. Simply put – IDS identifies the problem, and IPS stops the problem. The rest of this article will use the term IDPS. An IDPS is primarily focused on identifying possible incidents, logging information about them, attempting to stop them and reporting them to security administrators.[3]

In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS typically perform the following functions:

- Recording information related to observed events. Information is usually recorded locally and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

- Notifying security administrators of important observed events. This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.
- Producing reports. Reports summarize the monitored events or provide details on particular events of interest.[4]

PROS OF IDPS

An IDPS is seemingly the right choice for any jurisdiction – especially one moving to NG9-1-1. IDPS increase network control while leaving minimal effort on the IT department. As described above, it is designed to catch malicious cyber activity and prevent damage by automatically reacting to those threats. Other key benefits of using an IDPS system are that it:

- Automatically notifies administrators of suspicious activity and stops a cyberattack.
- Blocks detected malicious activity from accessing your networks.
- Resets connections if network errors are detected by changing the security environment.
- Uncovers the presence of unfamiliar networks and hosts.
- Reduces the maintenance burden on IT staff.
- Sets rules to allow or deny specific traffic from entering your network.
- Provides insight into real-time data streams.[5]

LIMITATIONS FOR IDPS

As with any cybersecurity solution, there are considerations to ensure that this is the right solution for your jurisdiction. Some of these include:

- IDPS does not block or prevent incidents from happening. This needs to be a part of an overall comprehensive cybersecurity plan.
- IDPS can still be susceptible to cyberattacks. Cybersecurity cannot be a single pronged approach.
- IDPS can use a lot of bandwidth. If you are using an IDPS system, be sure to have adequate bandwidth to support your operations and the system.
- IDPS, like physical security systems, can report false positives. It is important to investigate any positive reports of network intrusion.

EMERGENCY COMMUNICATIONS CYBERSECURITY CENTER (EC3)

In 2016 the FCC established the Task Force on Optimal Public Safety Answering Point (PSAP) Architecture (TFOPA). This task force was charged with reporting findings and recommendations for five topics:

- Optimal PSAP system and network configuration in terms of emergency communications efficiency, performance and operations functionality.
- Cost projections for conversion to an annual operation of PSAPs that incorporate such optimal system design.
- Comparative cost projections for maintenance of all existing PSAPs annually and upgrading them to NG9-1-1.
- Recommendations on ways to ensure states use E9-1-1 funding for their intended purpose.
- Whether states that divert E9-1-1 funds should be ineligible to participate on various FCC councils, committees and working groups.

A final 2016 report and a 2017 supplemental report outlined cybersecurity considerations for NG9-1-1. One of those recommendations was the incorporation of the EC3.

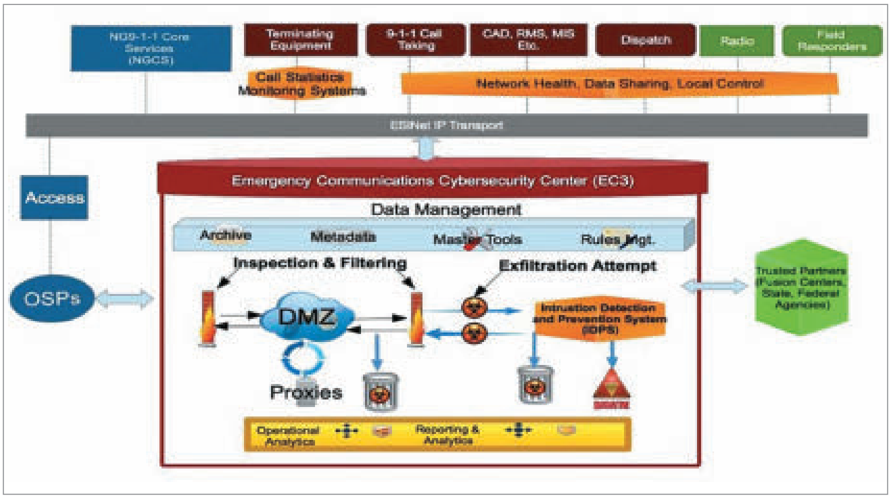
The EC3 concept (see Figure 1) allows for PSAPs from within and across jurisdictions, to connect to the core cybersecurity system and benefit from its capabilities, whether state, local, tribal or territorial. According to the FCC TFOPA final report:

> *The TFOPA has determined that an additional layer should be introduced into the recommended future architecture. The intent of the logical architecture proposed in the form of the EC3 is to create a centralized function for securing NG networks and systems. By centralizing certain features, including cybersecurity in general, and Intrusion Detection and Prevention Services (IDPS) specifically, public safety can take advantage of economies of scale, multiple resources, and systems and best practices which may already be in place or at a minimum readily available for deployment and use.*[6]

As noted, IDPS are made to identify cyber threats and mitigate those threats. The EC3 concept encourages a holistic approach to emergency communication cybersecurity, which will allow local authorities to share costs, benefiting from comprehensive services and capabilities that might otherwise be cost prohibitive.

CONCLUSION

Today's 9-1-1 systems are vulnerable to a plethora of cyberattacks. As our industry moves to NG9-1-1, we need to be vigilant and protect valuable 9-1-1 networks. As APCO's *Broadband Implications for the PSAP* report states, "cybersecurity should be 'baked in,' not bolted on."[6] When implementing new systems and networks, emergency communications centers should consider all cybersecurity measures in the initial plans to secure sensitive data. In 2016 and 2017, the FCC recommended the use of IDPS systems for emergency communications due to the identification and mitigation capabilities


NG9-1-1 Core Services (NGCS)
Terminating Equipment
9-1-1 Call Taking
CAD, RMS, MIS Etc.
Dispatch
Radio
Field Responders
Call Statistics Monitoring Systems
Network Health, Data Sharing, Local Control
ESINet IP Transport
Access
OSPs
Emergency Communications Cybersecurity Center (EC3)
Data Management
Archive
Metadata
Master Tools
Rules Mgt.
Inspection & Filtering
Exfiltration Attempt
DMZ
Proxies
Intrusion Detection and Prevention System (IDPS)
Trusted Partners (Fusion Centers, State, Federal Agencies)
Operational Analytics
Reporting & Analytics

of this technology. Overall, any jurisdiction should frequently review their cybersecurity program with guidance from the NIST'S "Framework for Improving Critical Infrastructure Cybersecurity."[8] ●

Megan Bixler, *is the Standards Program & Consulting Services Manager for APCO International. She works in the Comm Center and 9-1-1 Services department as the staff liaison for standards development initiatives and oversees consulting services. Her email is Bixlerm@apcointl.org.*

REFERENCES

1 National Institute of Standards and Technology, "Guide to Intrusion Detection and Prevention Systems (IDPS)(Draft)." csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

2 Ibid.

3 ibid.

4 Federal Communications Commission, "Task Force on Optimal PSAP Architecture (TFOPA)." transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf.

5 Ibid.

6 Vector Security, "Prevention and Detection: Does Your Business Need IPs, IDS or Both?" vectorsecurity.com/blog/prevention-and-detection-does-your-business-need-ips-ids-or-both

7 Federal Communications Commission, "Task Force on Optimal PSAP Architecture (TFOPA)." transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

8 APCO International, Broadband Implications for the PSAP: Analyzing the Future of Emergency Communications. apcointl.org/ext/pages/p43/p43book.html

9 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

CDE EXAM #54568

1) IDPS stands for:
   a. Industry detection for public safety
   b. Intrusion detection and prevention systems
   c. Intrusion detection for public safety
   d. Intrusion documentation for public services

2) EC3 stands for:
   a. Emergency communications cybersecurity center
   b. Emergency communications center cybersecurity
   c. Emergency communications center CPE protection
   d. Emergency communications cyberattack counterattack

3) The FCC TFOPA report outlined an EC3 concept that includes IDPS components.
   a. True
   b. False

4) Cybersecurity should never be thought of when implementing new systems
   a. True
   b. False

5) The EC3 concept has the following considerations:
   a. IDPS system
   b. Inspection and filtering of data
   c. Scalability
   d. All of the above
   e. None of the above

6) The EC3 will monitor network health.
   a. True
   b. False

7) IDPS is primarily focused on:
   a. Identifying phishing or ransomware attempts, logging information about them, and sending an e-mail to security administrators
   b. Identifying physical intruders, attempting to stop them by notifying an alarm company, and automatically reporting them to local police
   c. Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators
   d. Identifying social media trends and characterizing the language for natural disasters.

8) IDPS cannot be a single pronged approach to a jurisdiction's cybersecurity plan.
   a. True
   b. False

9) The EC3 allows jurisdictions to take advantage of:
   a. Economies of scale
   b. Multiple resources
   c. Systems and best practices that may already be in place or at a minimum readily available for deployment and use.
   d. All of the Above

10) IDPS systems do not help the IT department.
   a. True
   b. False

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 "2020 Public Safety Communications Magazine Article Exams," then click on "enroll me" and choose "Muddy Footprints All Over Your Network **(54568)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.