Broadcast Cybersecurity Precautions & Verification

Wayne M. Pecena CPBE, CBNE
Texas A&M University
Educational Broadcast Services - KAMU TV & FM
College Station, TX USA
w-pecena@tamu.edu

Abstract – Cybersecurity continues to be a challenge and a priority for the broadcast IT engineer. Cyber threats and tactics continue to evolve and the proper cybersecurity precautions must be implemented to protect the IP dependent broadcast plant and insure reliable operation. Proactive precautions must be in place and must be verified before any unknown gaps are exploited by the cybercriminal. This paper and accompanying presentation will provide practical to-do cybersecurity precaution steps and techniques to verify precautions thought to be in place are effectively implemented.

Cybersecurity Resources & Principals

Due diligence is necessary regarding cybersecurity in the broadcast station. One must accept that addressing cybersecurity is a reality whether in a small radio station or a state-of-the-art major market station. The migration to an Information Technology (IT) based Internet Protocol (IP) network infrastructure has brought advantages to stations in system capability, flexibility, scalability, ease of installation and cost effectiveness. However, the advantages create exposure to potential cyberattacks and protecting the broadcast IT based infrastructure grows more challenging each year. Cybersecurity is an essential responsibility of the broadcast engineer that cannot be ignored.

The broadcast IT engineer must invest time to study and understand that cybersecurity can be a complex undertaking, as well as confusing and challenging. Self-study resources include those from the National Institute of Standards and Technology (NIST), the Cybersecurity Infrastructure Security Agency (CISA) and the Information Technology (IT) cybersecurity industry at large.

The NIST Cybersecurity Framework [1] provides a structured set of guidelines and best practices for protecting IT assets and mitigating cybersecurity risks. Originally developed for government agencies, industry has adopted the framework that is often considered the “bible” of cybersecurity. The framework is organized into five (5) core areas of Identify, Protect, Detect, Respond and Recover as illustrated in Figure 1.

The core areas or pillars are further divided into several categories and sub-categories before reaching a specific guideline or best practice to implement. As an example, the “Protect” core area contains six (6) categories, the “Data Security” category is further divided into five (5) sub-categories. Each of the sub-categories such as “data-in-transmit is protected” then offers “Control & Control Enhancement (supplemental guidance)” steps. In this example the control states that “confidentially and integrity of transmitted information” must be protected. The corresponding control enhancement yields the control

This paper is excerpted from the Proceedings of the 2024 NAB Broadcast Engineering and Information Technology (BEIT) Conference, © 2024, National Association of Broadcasters, 1 M Street SE, Washington, DC 20003 USA.

achieved by “the system implementing cryptographic mechanism” (encryption). The NIST framework can become complex due to > 1,000 paths to follow in order to reach a specific action. Because of this complexity, numerous summarized best practices lists are developed by the cyber industry, government agencies and trade groups. Best practice checklists should be used that originate from trusted sources to insure actions are in line with the NIST framework and industry principals.

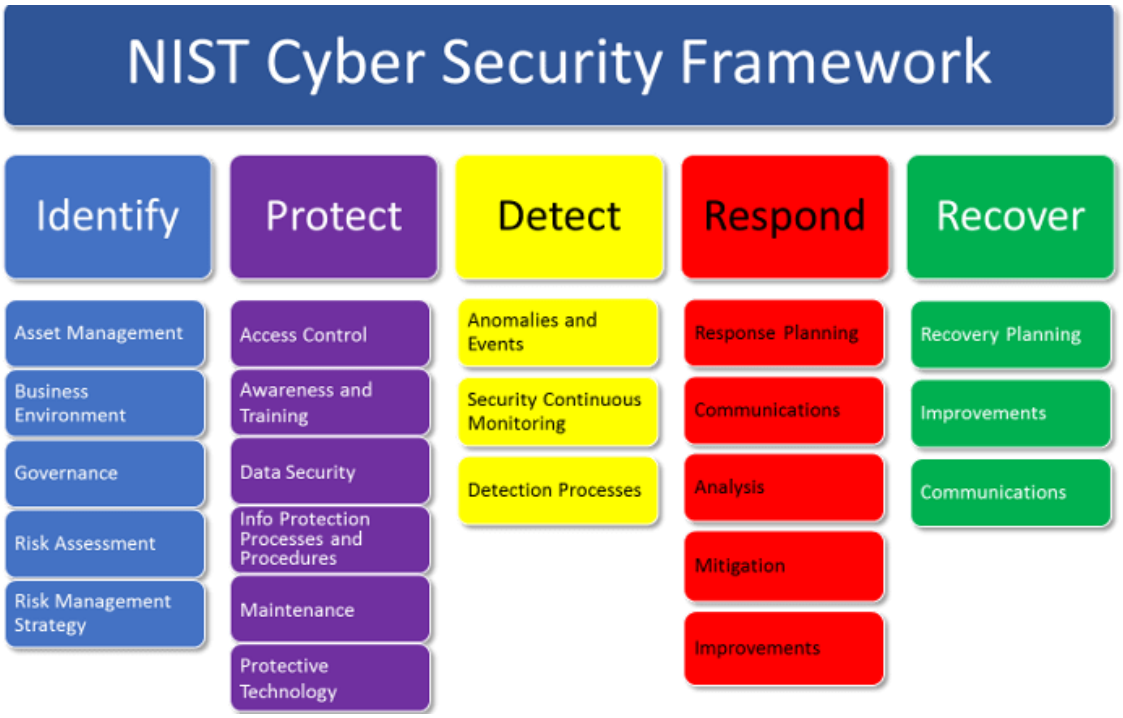


FIGURE 1

CISA offers a wide range of resources and services ranging from tutorials, to cybersecurity tools, best practice checklists, vulnerability scans and cybersecurity training exercises. The resources are organized to reflect different audiences. Specific groups include educational institutions, small businesses and local or state governments.

CISA cybersecurity recommendations begin with “adopting a heightened security posture”. [2]
The posture is based upon achieving four (4) key goals:

- Minimize the attack surface
- Monitor & protect network
- Develop & test an incident response plan
- Insure operational resilience

Minimization of the attack surface seeks to limit visibility of IT resources to a threat actor. If a cyber event should occur, the reach of that attack is limited to a contained area rather than spreading throughout the organization’s IT infrastructure and network. A common characteristic of malware is to spread throughout the network. Figure 5 illustrates the “east-west” movement throughout a network.

Monitoring of the network and IT infrastructure is important to know when abnormal conditions occur. Each organization has a baseline of normal operations. Changes in operational patterns without a corresponding business process change indicate possible cyber activity occurring.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Function	Category	Subcategory
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

FIGURE 2

A proactive incident response plan is critical to restoring operational status, should a cyber event occur. An incident is not the time to determine restoration options. The focus should be execution of a pre-determined plan of action. NIST recommended incident response plans focus upon [3]:

- Plan preparation
- Incident detection
- Incident containment & recovery
- Post-event analysis

Minimization of the attack surface is the first goal of the adoption of a heightened security policy. Further guidance is provided by CISA in the ways in which to achieve a minimized attack surface by hardening the infrastructure [4]:

- Maintain infrastructure software & patch updates
- Perform regular vulnerability scans
- Use antivirus software of hosts
- Use email spam filtering
- Remove unnecessary host accounts, services and software
- Implement Multi-factor Authentication (MFA)
- Insure host default logins are changed & a strong password policy enforced

Operational resilience is achieved through the use of fault-tolerant hardware in the infrastructure and effective use of data backup systems. Fault-tolerant systems are characterized by the use of diversity, redundancy and replication in system design. [5] Host operating systems with fault-tolerant capabilities must be utilized to provide effective reliability. Industry practices state that at least “5 nines” (99.999%) of reliability is required to be classified as a fault-tolerant system.

Due to the diversity of cybersecurity precautions and the diversity of infrastructure environments deployed, adopting a risk-based approach is recommend in order to prioritize implementation resources. Priority is given to high-risk high-impact highly likely to occur threats often followed by high-risk impact with to low likelihood of occurring. Less priority is given to low-risk impact threats. Figure 3 illustrates the risk-based assessment approach.

The CISA Known Exploitable Vulnerabilities (KEV) catalog [6] of cyberthreats can be used as a resource to create your risk-based implementation plan prioritizing time and resource deployment in cyber prevention efforts. Appendix B contains a sampling of the KEV catalog information available.

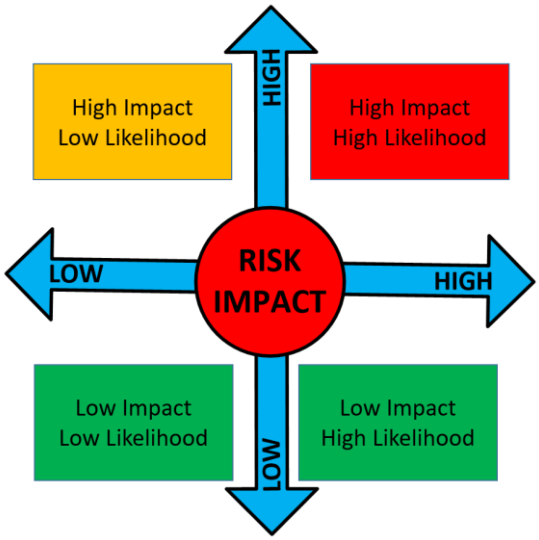


FIGURE 3

The cybersecurity industry at large provides several core principles that form the guidelines and best practices used to reduce cyber risks and protect broadcast IT assets.

The principal of Defense in Depth (DiD) is one of those core principles that establishes redundant levels or layers of security controls within the IT infrastructure, such that there is no single reliance upon a single cyber precaution [7]. If a security precaution should be breached or fail, another precaution will be in place to prevent further impact. A critical aspect of DiD implementation is to have the proper network architecture.

A layered or segmented network is essential. The segmented network is the traditional “flat” network compartmentalized by dividing into smaller sub-networks or subnets as illustrated in Figure 4. Each subnet can have the appropriate security controls applied that fit the workflows occurring within that subnet. Security is enhanced by minimizing the attack plane, providing containment if a cyber breech should occur by minimizing movement throughout the overall network. Movement throughout the network or “east-west” movement as shown in Figure 5 is a common goal of virus and ransomware malware. Network performance enhancement often results as network service broadcasts are contained within individual networks segments rather than propagated throughout the entire network.

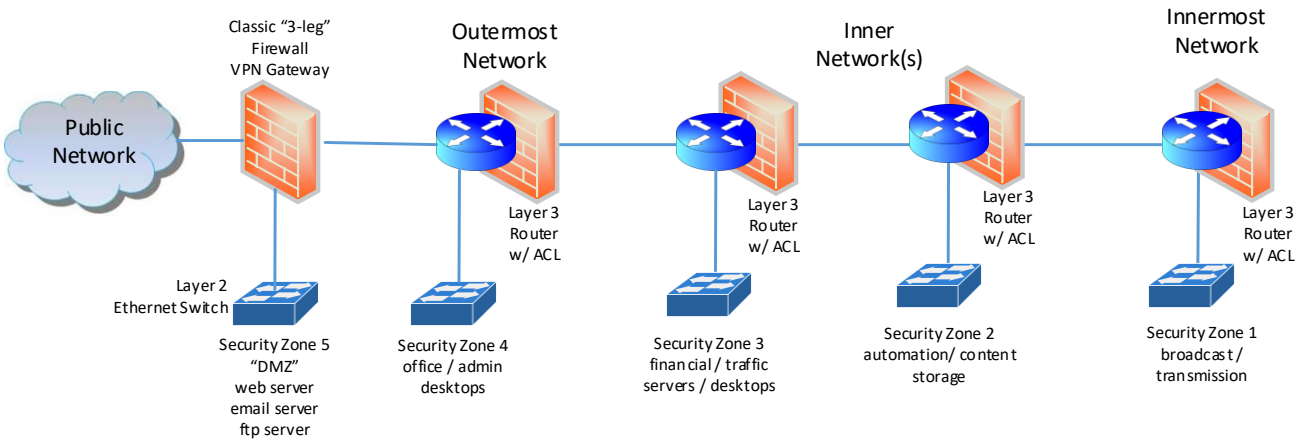


FIGURE 4

With a segmented network infrastructure in place, further DiD steps are implemented. These steps include physical infrastructure security and managed Ethernet switch security features, such as port security and packet filtering to control access. Packet filtering is accomplished by basic Access Control List (ACL) stateless filtering or stateful filtering through a firewall. In many situations, both types of packet filtering are utilized. Further security controls can be implemented for encryption provided by IP Security (IPsec), Transport Layer Security (TLS), or Secure Shell (SSH). Encryption and Multi-Factor Authentication (MFA) should be used for any remote access via a public network or the Internet. I use a Virtual Private Network (VPN) to remotely access my broadcast network via the Internet.

The principal of Least Privilege (PoLP) often referred to as “deny by default” is based upon limiting access rights to users and applications to the minimum level required to perform the defined business function. Limiting access to IT assets reduces the risk of abuse and propagation of a cybersecurity threat via “east-west” movement throughout an IT system.

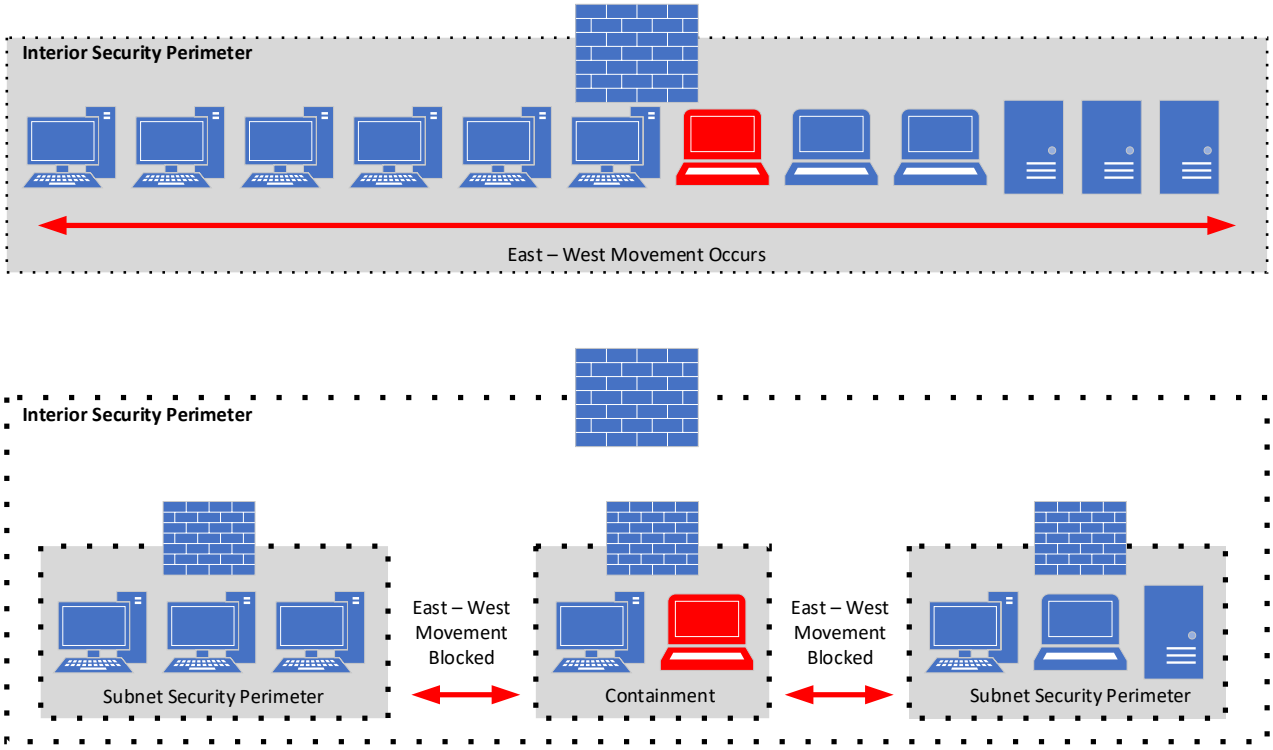


FIGURE 5

The CIA Triad (Figure 6) is the core objective of IT security [8]. It establishes the goals of insuring Confidentiality, Integrity, and Availability of IT systems. Confidentiality refers to the data within the IT infrastructure that is only available to authorized users and systems, whether flowing through networks, stored at rest or within a workflow process. Integrity refers to insuring that data has not been modified, tampered with or altered. Availability ensures IT resources are available to authorized users and applications and not available to those not authorized such as the threat actor.

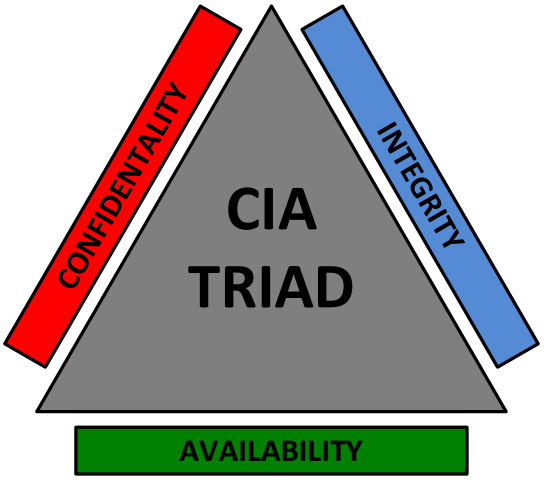


FIGURE 6

CYBERSECURITY MITIGATION ACTIONS

From the viewpoint of the threat actor or hacker, the CIA Triad becomes a target. The objectives of the triad become specific target areas for the threat actor. Confidentiality is lost as an organizations data is breeched and exposure of sensitive or private information occurs. Integrity is lost as malware may be embedded, man-in-the-middle (MiTM) implemented also exposing sensitive information through data record alteration. Availability is impacted through Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, physical infrastructure outages from sabotage or malware insertion.

Cyber-attacks share a common sequence of events or steps as illustrated by Figure 7. The sequence of steps begins with the identification of a potential target host device or devices. Discovery of potential target(s) often occurs through network reconnaissance tactics with the goal of gathering information about host devices. Information gleamed may include the host operating system including version, active services along with the version executed on the host and insight to potential device default login information. Vulnerabilities of specific operating system versions or services can then be evaluated for potential attack targets.

Reconnaissance tactics may employ various discovery tools and tactics. Tools including the popular "ping" command within all IP enabled operating systems, open-source port scanners such as nmap [9] or more sophisticated discovery and payload delivery tools such as Metasploit [10]. Online search engines such as Shodan [11] may also be utilized that allows IP host search via metadata keywords. Tactics for information discovery through social media channels can be used to gather information and insight about an organization and potentially its internal network. "Dumpster diving" can also be used to recover configuration information from discarded infrastructure equipment, as well as printed technical documentation.

Stopping or minimizing network reconnaissance becomes a critical first step in cybersecurity mitigation.

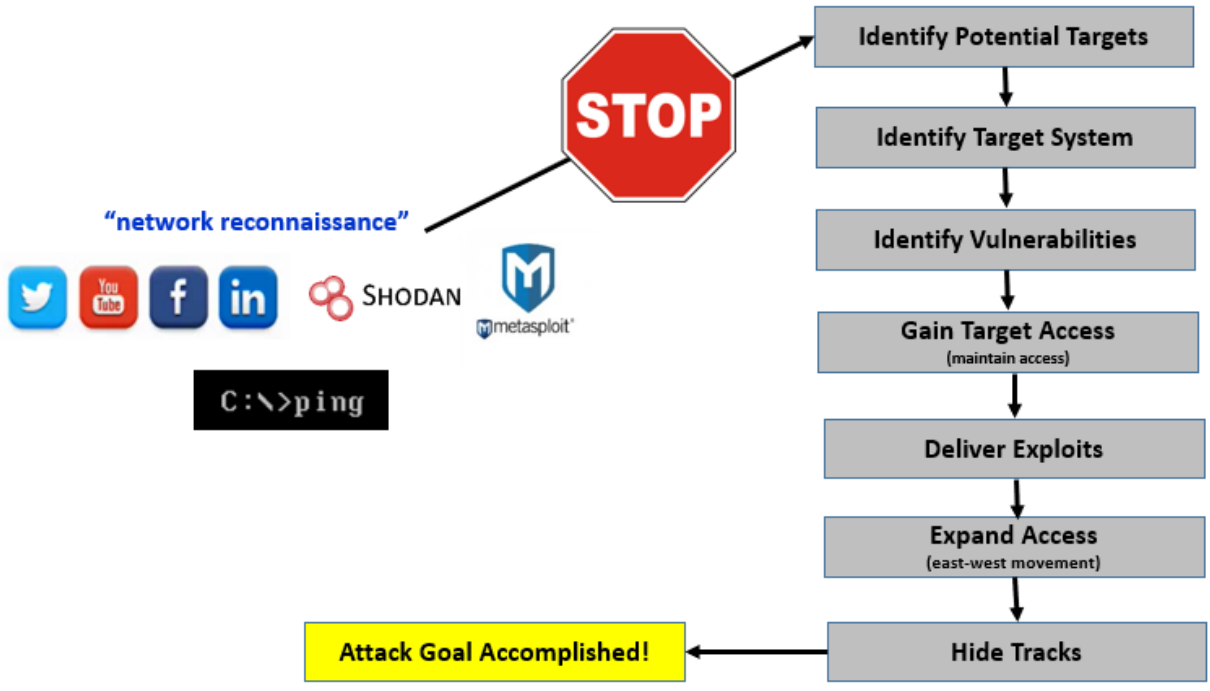


FIGURE 7

Cybersecurity mitigation efforts should begin with an accurate inventory of all IT assets in the organization. Complete and accurate system documentation is hopefully available, but often it is not or not up to date. Tools such as nmap can be used to assist in the gathering of host information. Appendix A is an example of possible nmap host discovery executed by the command line “nmap -sn 192.168.1.0/24”. Note that nmap requires the subnet mask to be expressed in the Classless Inter-domain Routing (CIDR) “/ shorthand” notation. In this example the entire class C IP block of 192.168.1.0 network addresses are scanned.

If desired, further insight can be found by identification of the physical Ethernet switch port that the host device is connected to via the Media Access Control (MAC) address discovered by nmap. Physical wire tracing is then deployed from the Ethernet switch port the mystery host device.

With an accurate inventory in hand, a risk-based approach should be used to establish priority of resources and time to deploy your specific cybersecurity plan. High-risk impact actions are given priority implementation with less attention given to low-impact low-risk threats. Resources such as the CISA KEV catalog, software and equipment manufacturers as well as any regulatory influence can be used to assist in determining potential vulnerabilities and their potential risk impact.

The physical network infrastructure should be protected from possible tampering. Protections can range from a single locked network equipment cabinet for a small facility, to a caged island in a shared equipment environment. A dedicated IT network and server room is likely to be found in larger facilities. Access monitoring and access control capability should be provided. Security camera monitoring and access cyber-locks or access badges are common physical security practices.

A segmented network architecture is essential to integration of the DiD principal of multiple barriers. Figure 4 offered a conceptual diagram of a possible segmented network architecture in a broadcast environment. In this example, the broadcast transmission sub-network is the innermost network and is considered the most secure as the core network. To reach the core network, the threat actor must breech all previous layers or segments as illustrated in Figure 8.

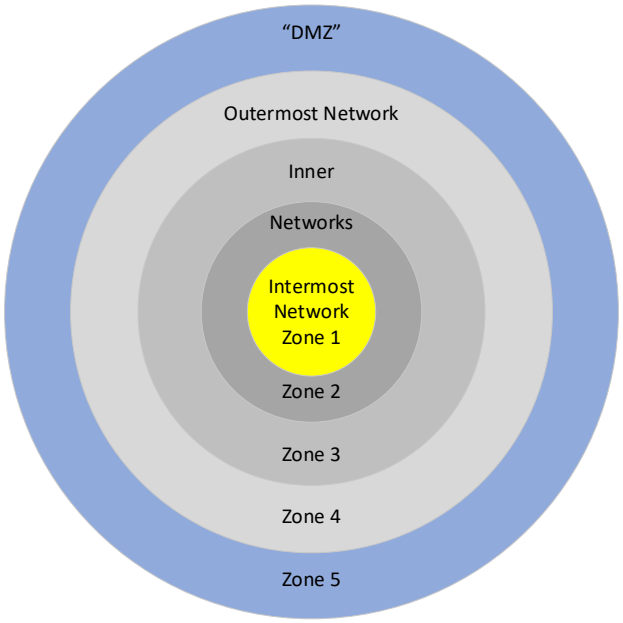


FIGURE 8

It is common practices to construct a segmented network using the Virtual Local Area Networks (VLAN) features of a managed Ethernet switch. This approach allows a common physical network infrastructure to support the individual VLANS. Ethernet switch port security features can be enabled to limit what specific host device is connected to an Ethernet switch port. The host device MAC address is used to identify the host device. It is recommended that only one host device be connected to a switch port and the port configuration set to permit only a single host MAC address. Default Ethernet switch configurations commonly allow multiple host devices to be connected to a single switch port. If a foreign device should be connected, the port security feature configuration programming will drop the incoming Ethernet frame, disable the switch port and generate a port security violation system message alerting the broadcast IT engineer.

Each VLAN or network segment is an isolated network although a common physical network medium is used. Each VLAN has its own IP address space with no inter-VLAN communications. Where interoperability between a host on one network segment to a host on another segment, IP routing must be implemented. Packet filtering is used to limit the interoperability available by allowing or permitting communications between specific host devices. Packet filtering can be implemented in a stateless manner by an Access Control List (ACL) and/or in a stateful manner through the use of a firewall. Permit or deny decisions can be based upon IP header information including:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Protocol
- Logical operator combinations of the above

Additional equipment security features include encryption, Multi-factor Authentication (MFA) and the use of Virtual Private Networks (VPN) when remote access is required. VPN access with MFA is a common practice to permit secure remote access when the public Internet is involved.

With a segmented network in place, attention is addressed to the host devices connected to the network. The goal is to harden these devices by reducing their attack surface. The broadcast network often contains many different types of hosts ranging from desktop computers, servers, security system components, building control and access devices, wireless access points and broadcast specific equipment. These devices share common characteristics of being IP enabled via a wired Ethernet interface or a wireless interface, contain memory and a processor and an operating system. Operating systems are likely one of three industry offerings:

- Microsoft Windows (limited feature embedded & full capability)
- Linux (limited feature embedded & full capability)
- Proprietary (IE Cisco IOS, NX-OS or HP ProCurve, Comware)

Whereas the specific hardening actions of the typical operating systems are beyond the scope of this paper, general host hardening steps include the following actions:

- Removing any un-used applications and/or disabling services not required
- Blocking service port access with packet filtering if a service cannot be disabled
- Deleting un-used accounts or stale accounts
- Changing default configurations including default access passwords
- Maintaining software patches/updates
- Closing any “backdoor” access
- Utilize “strong” password policies

A structured cybersecurity plan should include the following as minimum mitigation actions:

- DiD used to provide redundant precautions implemented in a structured and coordinated manner
- Implement a segmented network for cybersecurity protection and performance enhancement
- Inventory IT assets and utilize a risk-based approach to establish priorities
- Establish physical infrastructure security measures
- Utilize Ethernet switch port security
- Use stateful and stateless packet filtering to control and limit resource access
- Apply PoLP to users and applications
- Use encryption & Multifactor Authentication (MFA) for any remote access
- Keep network hardware and operating systems updated and current
- Ensure default login credentials are changed, strong & unique passwords
- Delete any stale or unnecessary accounts
- Disable all host services not required or used
- Use packet filtering to block any service port if not able to be disabled
- Perform routine vulnerability and malware scans with current signature files
- Maintain critical system backups that followed the 3-2-1
- Routinely test backup systems for operability and reliability
- Establish infrastructure monitoring and alerting to identify when abnormalities occur

Cybersecurity Verification

With cybersecurity precautions in place, the same tools that a malicious hacker or threat actor might use to verify the cybersecurity precautions thought to be in place, are indeed in place and function as intended. Penetration testing tools can be used to confirm visibility from the public Internet or if hosts are visible, that the visibility is known and external protection implemented. Spot checks should be used when firmware and software updates are performed, as device configurations can be changed to defaults. The basic tool used for penetration testing is a port scanner, such as “nmap”. A port scanner identifies host devices visible on a network and determine services enabled by active port identification. Online search engine port scanning tools, such as Shodan can be useful for quick routine checks of public network visibility.

More in-depth penetration testing, or pen testing, can performed by outside cybersecurity consultants or by use of more sophisticated tools such as “Metasploit”. The scope of a penetration test [12] can focus upon a specific functional area such as:

- Network infrastructure
- Software applications
- Physical security
- Mobile device
- WiFi & VPN access
- Social engineering

A comprehensive penetration test will incorporate all function areas. Pen testing, regardless of scope is the last step in a cybersecurity prevention plan. For the broadcast IT engineer, it is the “proof of performance” of their broadcast IT system.

With a solid cybersecurity prevention plan in place, one should be able to have a sense of confidence in their cybersecurity mitigation. Whereas, adequate technology-based precautions may be in place, social engineering poses yet another often more challenging threat. NIST defines social engineering as tricking someone to reveal information or grant access by manipulation of human emotion [13].

Social engineering is often based on persuasion of emotions with a sense of urgency to exploit a victim's lack of knowledge, fear or curiosity [14]. Personal information is often used by the attacker to establish a relationship of trust with the targeted victim. In accomplishing this, information may be divulged or the victim tricked to unintentionally download malware through voice phone calls, SMS messaging, email and even postal service mail.

Phishing is the most common tactic ranging from mass user audience attempts to focused or targeted users. Mass phishing attempts are not oriented at a specific individual or group. Mass phishing does not utilize personal information in an attempt to establish a sense of trust. "Spear" phishing is focused at a specific individual or group utilizing personal information to establish authority and trust. "Baiting" tactics attempt to lure the victim into divulging sensitive information or inflict a system with malware.

Prevention of successful social engineering attempts is best accomplished through ongoing education of all users in recognizing social engineering tactics and their response to attack attempts. Users should be cautioned in opening attachments only from trusted sources, avoid attaching unknown USB memory devices to hosts and questioning information requests from unknown sources.

Do not overlook CISA resources to aid in ongoing staff education efforts regarding social engineering [15].

Concluding Thoughts

Cybersecurity has been at the forefront for several years now as virtually all broadcast stations are reliant on an IT based IP network infrastructure. The reality is that cybersecurity is an ongoing process and can never be ignored. With a solid cybersecurity mitigation plan in place, ongoing routine system monitoring, updates of signature files, updates to firmware and software updates is necessary. Continuous user education is also required as use of social engineering is growing and the tactics utilized becoming more creative. Cybersecurity threats constantly evolves and protections must also evolve.

References

[1] https://www.nist.gov/cyberframework

[2] www.cisa.gov/shields-up

[3] "Computer Security Incident Handling Guide", Special Publication 800-61 Revision 2, August 2012, National Institute Standards and Technology, U.S. Department of Commerce

[4] www.cisa.gov/shields-technical-guidance

[5] Brumfield, C., "Cybersecurity Risk Management", 2022, p. #48

[6] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[7] https://csrc.nist.gov/glossary/term/defense_in_depth

[8] Cisco Networking Academy, "CCNA Cybersecurity Operations", 2018, p. #384

[9] https://nmap.org/book/man.html#man-description

[10] https://www.metasploit.com/

[11] https://www.shodan.io/

[12] Nutting, R., "CompTIA PenTest+ Certification ", 2019, p. #45, #105, #147, #345

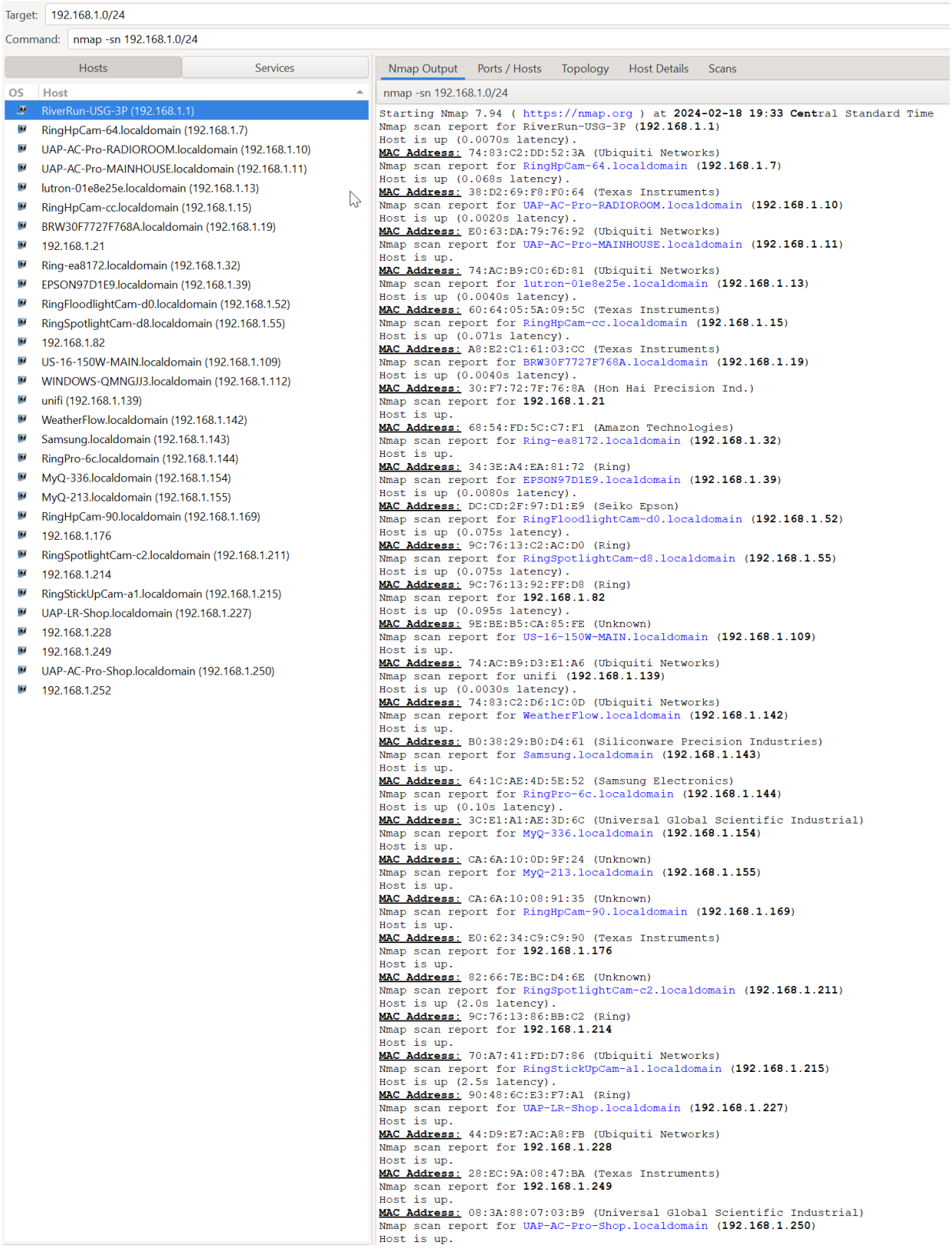
[13] https://csrc.nist.gov/glossary/term/social_engineering

[14] https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

[15] https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Appendix A

Example network host inventory determined through the nmap utility:



Appendix B

Excerpt of CISA KEV catalog information: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

cveID	vendorProject	product	vulnerabilityName	dateAdded
CVE-2023-6448	Unitronics	Vision PLC and HMI	Unitronics Vision PLC and HMI Insecure Default Password Vulnerability	12/11/2023
CVE-2023-49897	FXC	AE1021, AE1021PE	FXC AE1021, AE1021PE OS Command Injection Vulnerability	12/21/2023
CVE-2023-47565	QNAP	VioStor NVR	QNAP VioStor NVR OS Command Injection Vulnerability	12/21/2023
CVE-2023-7101	Spreadsheet::ParseExcel	Spreadsheet::ParseExcel	Spreadsheet::ParseExcel Remote Code Execution Vulnerability	1/2/2024
CVE-2023-7024	Google	Chromium WebRTC	Google Chromium WebRTC Heap Buffer Overflow Vulnerability	1/2/2024
CVE-2023-23752	Joomla!	Joomla!	Joomla! Improper Access Control Vulnerability	1/8/2024
CVE-2016-20017	D-Link	DSL-2750B Devices	D-Link DSL-2750B Devices Command Injection Vulnerability	1/8/2024
CVE-2023-41990	Apple	Multiple Products	Apple Multiple Products Code Execution Vulnerability	1/8/2024
CVE-2023-27524	Apache	Superset	Apache Superset Insecure Default Initialization of Resource Vulnerability	1/8/2024
CVE-2023-29300	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	1/8/2024
CVE-2023-38203	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	1/8/2024
CVE-2023-29357	Microsoft	SharePoint Server	Microsoft SharePoint Server Privilege Escalation Vulnerability	1/10/2024
CVE-2023-46805	Ivanti	Connect Secure and Policy Se	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	1/10/2024
CVE-2024-21887	Ivanti	Connect Secure and Policy Se	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	1/10/2024
CVE-2018-15133	Laravel	Laravel Framework	Laravel Deserialization of Untrusted Data Vulnerability	1/16/2024
CVE-2024-0519	Google	Chromium V8	Google Chromium V8 Out-of-Bounds Memory Access Vulnerability	1/17/2024
CVE-2023-6549	Citrix	NetScaler ADC and NetScaler	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	1/17/2024
CVE-2023-6548	Citrix	NetScaler ADC and NetScaler	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	1/17/2024
CVE-2023-35082	Ivanti	Endpoint Manager Mobile (EI	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vu	1/18/2024
CVE-2023-34048	VMware	vCenter Server	VMware vCenter Server Out-of-Bounds Write Vulnerability	1/22/2024
CVE-2024-23222	Apple	Multiple Products	Apple Multiple Products Type Confusion Vulnerability	1/23/2024
CVE-2023-22527	Atlassian	Confluence Data Center and S	Atlassian Confluence Data Center and Server Template Injection Vulnerability	1/24/2024
CVE-2022-48618	Apple	Multiple Products	Apple Multiple Products Improper Authentication Vulnerability	1/31/2024
CVE-2024-21893	Ivanti	Connect Secure, Policy Secur	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) V	1/31/2024
CVE-2023-4762	Google	Chromium V8	Google Chromium V8 Type Confusion Vulnerability	2/6/2024
CVE-2024-21762	Fortinet	FortiOS	Fortinet FortiOS Out-of-Bound Write Vulnerability	2/9/2024
CVE-2023-43770	Roundcube	Webmail	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	2/12/2024
CVE-2024-21412	Microsoft	Windows	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	2/13/2024
CVE-2024-21351	Microsoft	Windows	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	2/13/2024
CVE-2020-3259	Cisco	Adaptive Security Appliance	Cisco ASA and FTD Information Disclosure Vulnerability	2/15/2024
CVE-2024-21410	Microsoft	Exchange Server	Microsoft Exchange Server Privilege Escalation Vulnerability	2/15/2024