Doc T-22/10-3

RECOMMENDATION 1/2022

Supporting the WBU-TC Recommendations related to Cybersecurity issued in 2022

Considering

1. that broadcasters are now heavily reliant on integrated IT infrastructure for its efficiency and ease of use;

2. that broadcasters and the media industry are increasingly using the internet as a delivery platform for live streaming and OTT and IBB services;

3. that the connected environment, with its ease of use also brings its own safety and security risks;

4. that there is a continuous increase in threats like malware, ransomware and others;

5. that there has been reports of increasing number of cyberattacks targeted at media organisations in the region;

6. that broadcasters need be aware of these threats and take the necessary precautions to safeguard their networks and valuable content,

Noting

7. that the World Broadcasting Union's Technical Committee with support from the various broadcasting unions, has developed a set of recommendations related to Cybersecurity applicable in different levels of the broadcast chain.

The ABU Technical Committee Recommends

1. The ABU members take note of the WBU proposed Recommendations as in the three documents below:

    a. WBU Cybersecurity Recommendations for Media Vendors' Systems, Software and Services. (an updated to the 2018 version) (see Annex 1)
    b. WBU Recommendations on Best Practices to Mitigate Social Engineering (see Annex 2)
    c. WBU Recommendations on Cybersecurity Training and Awareness (see Annex 3)

2. The ABU members should move ahead to implement these recommendations within their workflows and their organisations wherever applicable.

3. The ABU members take Cybersecurity as a serious threat and regularly review and evaluate the security systems and protocols in place to be better prepared for potential attacks and threats.

WBU Cybersecurity Recommendations for Media Vendors' Systems, Software and Services

The World Broadcasting Unions (WBU) developed the following cybersecurity recommendations which reflect the performance aspirations of both organizations in media vendors' systems, software and services.

Based on the original work by the European Broadcasting Union (EBU) and North American Broadcasters Association (NABA), these recommendations are intended to create a dialogue with media vendors with the goal of their achieving more consistent and effective compliance with cybersecurity best practices.

The WBU recommends that its union members, and media companies in general:

1. Apply these cybersecurity recommendations when planning and designing their systems, software and services;
2. Require media vendors to state their degree of compliance with these cybersecurity recommendations when responding to requests for information (RFIs), requests for proposals (RFPs) and requests for quotations (RFQs);
3. Define their own minimum risk acceptance level on the basis of these recommendations.

High-Priority Cybersecurity Recommendations

The WBU has identified cybersecurity recommendations considered as high-priority with the following categorisation:

- "P1" designation represents critical provisions for the overall cybersecurity.
- "P2" designation recognizes important recommendations.
- "P3" designation represents best-practice arrangements.

This recommendation provides the minimal set of security requirements for broadcast equipment vendors. More specific requirements available in other regional specifications such as the EBU R143[1] or NABA[2]'s Cybersecurity requirements may augment the following recommendation for regional compliance.

This document uses the term high risk, which can be determined in advance by an agreement (SLA) between the media vendor and broadcaster on the level of security threat (i.e., by using CVSS scores). It is proposed that high risk starts at 7 on the CVSS scale. This is a suggestion and has to be adapted to the risk and criticality of the system and environment that it's deployed in. A critical patch is a patch that fixes a high-risk vulnerability.

Specific Recommendations

1. Communications

1.1. The media vendor shall routinely and timely release information in the event any security weakness in its product(s) becomes known. (P1)

1.2. The media vendor shall support maintenance access and procedures (i.e., RAS, VPN, secure accounts, secure passwords). (P1)

1.3. There must be designated media vendor point(s) of contact, or other contact options, available on a 24/7 basis to address cybersecurity questions, incidents, incident reports and even zero-day critical attacks on the media vendors' products and services. (P1)

2. Authentication

2.1. The media vendor's systems, software and services should integrate with centralized authentication services, provided via Active Directory and/or LDAP certification and validation. (P2) In addition, multi-factor authentication must be supported for all Internet-facing devices. (P1)

2.2. A password policy for all systems, software and services must be supported, including the forced change of default passwords, complex passwords and automatic expiration. (P1)

2.3. The media vendor's systems, software and services must support AAA (Authentication, Authorization and Accounting) logging on a centralized logging server. (P1)

2.4. With respect to Layer 3 network capabilities, communications between trusted and un-trusted sources must be restricted to source & destination IP addresses only, as well as the lowest possible number of TCP/IP ports, to minimize the application attack surface. Session timeout support must be included as well. (P2)

2.5. Network login protocols (e.g., ability to segregate role-based account management capabilities) must be supported. (P3)

3. Controls

3.1. The media vendor shall provide security updates, including for all third-party components used such as the operating system platform and runtime environments used. To limit the damage that could be caused by attackers, critical patches should be implemented as soon as possible but as a target, not later than 30 days after release of the underlying patch. Non-critical patches should be implemented within a month but no later than 90 days of release. In case of a high-risk (e.g., zero-day) vulnerability (own or third party), the vendor must provide a workaround to mitigate the issue. (P1)

3.2. The media vendor's software, system and services must be able to be protected effectively against virus, malware and exploits on both the server and client side. For Systems that cannot meet this requirement, Mandatory Access Control mechanisms like application allow-listing must be put in place. (P1)

3.3. For media systems running on a general-purpose computer, the media vendor's software, system and services will provide the capability to decouple the operating system from the software itself, thus allowing for the separation of patching of both OS and runtime environments. (P1)

3.4. System Updates:

- The Product or service lifecycle should be clearly defined so that the Customer is aware of key dates. Patches and updates should be made available to ensure that security can be maintained throughout the lifecycle of the Product or service, from implementation to decommission. (P1)
- The Vendor should also support the upgrade of the software components of the system (OS, DBMS, Application Server, etc.) if any of these components becomes unsupported. (P1)

3.5. The media vendor's software must support a proxy (and reverse proxy) option when initiating Internet access, for both inbound and outbound traffic. (P1)

3.6. The media vendor's software development must follow industry-standard secure development policies (e.g., OWASP Secure Coding Practices in its latest version).

3.7. For web front-ends, controls should be in place to counter the current OWASP Top 10 vulnerabilities. (P1) 3.8. Software installers should be cryptographically signed by the vendor. (P1)

3.9. The media vendor must provide the option to remove or disable USB ports as well as the ability to disable the auto-start sequence of USB/CD/DVD media, as a pre-setting. (P2)

3.10. The media vendor shall ensure that all of its products are sufficiently "cleaned" before release to ensure that no test code or default accounts ("vendor backdoors" via hardcoded passwords, ssh keys, etc.) remains from the software development process. (P2)

3.11. The media vendor shall perform regular internal technical security analyses (i.e., penetration and vulnerability tests). (P1)

3.12. The media vendor must provide and support its approved security control guidelines when providing any third-party service, including cloud services. (P1)

3.13. All media vendor's systems, software and services must support risk management assessment and monitoring tools. (P2)

3.14. The vendor product needs to be compatible with current patched mainstream browsers. (P3)

3.15. The media vendor shall have a process to track and address well known vulnerabilities (i.e., as logged in the NIST National Vulnerabilities Database) and maintain an up-to-date and available register of this process. (P1)

4. Documentation

4.1. All media vendors' systems, software and services shall be provided with documented interfaces, access points, ports, network communication and features. (P1)

4.2. The media vendor shall describe its patch management programme, specifically with respect to security updates. (P1)

4.3. The media vendor shall include recommendations on how to integrate the system, software or service in a secure architecture (e.g., different network zones, central authentication service, workflows, interfaces, etc.) (P2)

4.4. The media vendor should have a secure coding practice in place, complete with penetration testing against current standards. This includes end-point tools (e.g., execution protection, advanced malware protection, etc.) with secure configuration guidelines. (P1)

4.5. The media vendor shall provide automatic alerting and notification of software patch updates. (P3)

4.6. The media vendor shall put both physical and digital security controls in place throughout the delivery of its system, software or service. (P2)

5. Encryption

5.1. Encrypted (e.g., TLS-based) network protocols (https, ftps, sftp) and certificates and PKI following the latest recommendations issued by cybersecurity standards organizations such as NIST or other authoritative standards organizations must be supported. All media vendors' systems, software and services must avoid the use of clear text protocols (e.g., http, telnet, ftp, etc.). Self-signed certificates should not be used. Integration with Automated Certificate Management Environment (ACME) certificate providers as a minimum should be supported. (P1)

5.2. The media vendor's systems, software and services must support the encryption of sensitive data, key ownership and management. Encryption algorithms following the latest recommendations issued by cybersecurity standards organizations such as NIST or other authoritative standards organizations, should be used from machine-to-machine at the application level. In addition, the client shall have the option to control a Primary Key for encryption. Systems must be designed in order to accept changes in cryptographic protocols whenever old protocols become obsolete. (P1)

6. Network Configuration

6.1. If the OS has a built in firewall then the application/vendor should use/support it (e.g., Windows/Linux), when it doesn't compromise timely availability of data. (P2)

6.2. The media vendor's system, software and service must support a sufficiently granular segmentation of internal and external networks (e.g., multi-VLAN support, routing, etc.) (P1)

6.3. The media vendor's system, software and service must support maintenance access points in a demilitarized zone (DMZ) so that vendors or system administrators first connect to a DMZ instead of to the application itself. (P3)

7. The Vendor should apply the same level of security control assessment procedure to its own suppliers.

The Vendor should require its own potential Suppliers and Vendors of main subsystems, software and services that are embedded in their Products to declare their ability to comply with security controls assertation and guidance with the same level of details provided in this Recommendation. Vendors should communicate the results to their customers. (P1)

_____

World Broadcasting Unions, March 2022

WBU Recommendations on Best Practices to Mitigate Social Engineering

Social engineering has become more commonplace in the enterprise and increasingly complex to address. Cyber criminals have become very adept at manipulating employees into handing over sensitive or valuable enterprise information.

Social engineering is predicated on psychological manipulation of the employee. Typically, it involves email (i.e., “phishing”) or some other form of communication that invokes a sense of fear, pressing need, response to authority, elation, etc., in the employee, motivating him/her to take action by clicking on a phishing e-mail, a malicious link or by revealing sensitive information.

Social engineering operates on the psychological level of the employee. As every employee is different, social engineering has become a pernicious threat to the enterprise to mitigate. Cyber criminals need only to deceive one employee in order to be successful in launching malware, receiving sensitive information, gaining access to the enterprise building or network, etc. Cyber criminals have been known to research the social media presence of individual employees in advance in order to make their phishing emails more personal and relevant.

Some of the steps that have proven to help the enterprise mitigate the risk are as follows.

In all cases, when in doubt, employees should contact their internal IT resources or internal security team before taking any action.

1. Train

Employee training on ways to detect and mitigate social engineering is critical. Comprehensive Security Awareness should be undertaken in the enterprise on a reoccurring basis and should include social engineering testing and simulated phishing attacks. Training should focus on implementing enterprise- wide behavioural change on the part of the employee and should be performed on an on-going, proactive basis. Often, social engineering may include impersonation of a senior company official, such as the CEO, requesting the employee to take an unusual action such as sending sensitive files or issuing last-minute payments.

Further, employees should be trained to adopt a “zero-trust” attitude toward external requests. In fact, employees can be encouraged to “think like a cyber criminal” to reinforce their preparedness.

2. Delete requests for personal information or passwords

Although this would appear to be obvious, cyber criminals sometimes offer bogus rewards or other false incentives in return for personal information, or even passwords. In addition, they might send emails impersonating a government department, law office, bank or insurance company, as examples. Since the payload of some of these email requests may contain malware, they should either be deleted or routed to the enterprise cybersecurity team for analysis, as mentioned.

3. Limit information released to third parties

Some cyber criminals will contact the enterprise IT team posing as software or hardware salespeople. In order to better tailor their bogus unsolicited offer, they will ask for information on the hardware or software an enterprise is using, e.g., firewalls, routers, security software, etc. The more information they receive, the better position they are in to exploit latent vulnerabilities.

When faced with such requests, it is recommended to route these questions to a designated central point of contact in the enterprise, someone who is responsible for vetting the requestor and the need for the requested information. Employees should be trained that the default response to such requests is never to release any information.

4. Secure your devices, network and software

As a general IT best practice, ensure all required software patches are installed promptly and security software updates are set to be installed automatically. Employ a rigorous password policy, whereby passwords must be changed regularly and comply with complexity requirements.

5. Use multi-factor authentication (MFA)
One of the main targets of cyber criminals are credentials, as they facilitate their access to internal enterprise networks and assets. Using multi-factor authentication can help to mitigate this risk.

6. Reject requests for help or offers for help
Legitimate external companies and organizations do not contact an employee for help. If an employee did not specifically request assistance from the sender, an email offer of such assistance is most likely a scam. Delete email requests from charities or other organizations with which your organization does not have a relationship.

7. Always escort guests when physically visiting an enterprise
Physically accessing enterprise facilities through “tail-gaiting” or “piggy-backing” provides the cyber criminal with direct access to internal networks and devices. Guests should always be escorted from the point of legal entry into the building to the visited employee and then escorted out. All visits should be logged in advance with security and credentials should be validated by enterprise security before access is granted.

8. Question people in the enterprise you don’t know
It is not improper to politely challenge the credentials of unescorted people in the enterprise that are not recognized. If their status is circumspect, enterprise security should be immediately involved.

9. Learn to react slowly
As the majority of social engineering attacks are attempted by phishing, cyber criminals try to motivate the employee to react emotionally and quickly to offers for help, gifts, false demands by senior management, etc. Employees must learn to react slowly and review the request thoroughly, when confronted by a reported sense of urgency. When such requests are received, they should either be deleted or routed to the enterprise cybersecurity team for analysis.
In general, there are four steps that can be used to help mitigate social engineering:

- Verify the requester is who they say they are;
- Verify that the requestor is an employee of the stated company;
- Verify that the requester is authorized to make the request;
- Whenever in doubt, employees should route such requests to the enterprise cybersecurity team for analysis and further action.

_____
World Broadcasting Unions, October 11, 2022

WBU Recommendations on Cybersecurity Training and Awareness

Introduction

Employee training on how to detect and mitigate cybersecurity threats is critical to the on-going health of the enterprise.

Comprehensive security training and awareness should be undertaken in the enterprise on a reoccurring basis and should include items such as social engineering testing, simulated phishing attacks, etc. Training should focus on implementing enterprise-wide behavioural change on the part of the employee and should be performed on an on-going, proactive basis.

Further, employees should be trained to adopt a “zero-trust” attitude toward external requests. In fact, employees can be encouraged to “think like a cyber criminal” to reinforce their preparedness.

Best Practices

Make the Enterprise Cybersecurity Policy Clear to All Employees

- Ensure the organization has a Board of Directors and senior management approved policy on cybersecurity, clearly outlining the strategy and tactics to achieve this policy and its implications for all employees.
- The Board and senior management should include cybersecurity threats to the corporate risk register. This will ensure the full implications of these threats are identified and mitigation plans are documented and tracked as they are put in place.
- Ensure employees understand that all corporate devices issued for their use remain the property of the company and as such, are governed by corporate policies and procedures. Such devices are not the property of the employee.

Adopt a “Zero Trust” Approach to Cybersecurity

- A “Zero Trust” approach to cybersecurity is predicated on the concept of “never trust, always verify”.
- In this approach, all devices, email requests, etc. are to be considered suspect, irrespective of ownership, authorship, location or the fact they could have been verified previously.

Encourage Employees to Take Responsible Care of their Devices

- Ensure that the organization has and maintains a 100% accurate inventory of all devices that are allowed to access any internal network. If there are devices accessing internal networks that are not identified as corporate devices, immediately confiscate them and/or deny them continued access to any network resources.
- Ensure that all security patches are applied as soon as required and are not delayed by employee tardiness.
- Ensure that any employee device that has either been retired or replaced by a newer model is returned to the enterprise IT or cybersecurity department.
- Ensure that all devices of any employee who has left the enterprise be returned to the enterprise IT or cybersecurity department.

- Ensure that all mobile devices have appropriate segmentation between corporate and private applications, if the latter is permitted.
- Ensure employees understand how to create complex passwords and change them at regular intervals.
- Ensure multi-factor authorization is enabled on as many applications as possible.

Teach Employees How to Spot Suspicious Activity

- Employees should be trained to identify some of the tell-tale signs of suspicious activity on their devices, such as: new text messages with imbedded hyperlinks; device sluggishness; additional start-up or boot steps; slow keyboard reaction times; etc.

Collectively Examine Individual Cases of Cybersecurity Breaches

- On an ongoing basis, review prior cases of cybersecurity threat or breaches with employees to educate them on how such threats can be successful in their own enterprise.

Run Simulated Cyber Attacks, Gather Metrics and Retrain

- On a regular basis several times a year, run simulated phishing and social engineering attacks across the entirety of the enterprise, including the C-suite.
- Gather metrics on those employees who fail these trials and offer specific training.

Make Cybersecurity an Ongoing Conversation

- Ensure employees understand that their role is fundamental to the success of any cybersecurity programme.
- Engage employees through regular workshops, seminars, etc. on their perceptions of the enterprise cybersecurity programme, including areas for improvement.

_____
World Broadcasting Unions, October 11, 2022