c/o NABA
205 Wellington St. W., Toronto, ON M5V 3G7
Canada

Tel: +1-416-205-3363
Email: wbu@worldbroadcastingunions.org
Web: www.worldbroadcastingunions.org

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.

[1] https://tech.ebu.ch/docs/r/r143.pdf [2] https://nabanet.com/cybersecuritysubcommittee/

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