• ABU

ASIA-PACIFIC BROADCASTING UNION
- Kuala Lumpur, Malaysia

• ASBU

ARAB STATES BROADCASTING UNION
- Tunis, Tunisia

• AUB

AFRICAN UNION OF BROADCASTING
- Dakar, Senegal

• CBU

CARIBBEAN BROADCASTING UNION
- St. Michael, Barbados

• EBU

EUROPEAN BROADCASTING UNION
- Geneva, Switzerland

• IAB

INTERNATIONAL ASSOCIATION OF BROADCASTING
- Montevideo, Uruguay

• NABA

NORTH AMERICAN BROADCASTERS ASSOCIATION
- Toronto, Canada

WBU Cyber Security Recommendations for Media Vendors' Systems, Software and Services

The World Broadcasting Unions (WBU) developed the following cyber security 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 Broadcasting 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 cyber security best practices.

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

1. Apply these cyber security recommendations when planning and designing their systems, software and services;
2. Require media vendors to state their degree of compliance with these cyber security 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 Cyber Security Recommendations

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

- "P1" designation represents critical provisions for the overall cyber security.
- "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.

Specific Recommendations

1. Communications

1.1. The media vendor shall release information automatically and immediately in the event a 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). (P2)

[1] https://tech.ebu.ch/docs/r/r143.pdf
[2] http://nabanet.com/project/naba-cyber-security/

1.3. There must be designated media vendor point(s) of contact, or other contact options, available on a 24/7 basis to address cyber security questions, incidents, incident reports and even zero-day critical attacks on the media vendors' products and services. (P3)

2. Authentication

2.1. The media vendor's systems, software and services must integrate with centralized authentication services, provided via Active Directory and/or LDAP certification and validation. (P2) In addition, multi-factor authentication shall 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 (ex. ability to segregate role-based account management capabilities) must be supported. (P3)

3. Controls

3.1. The media vendor shall support the security updates for all third-party components used, including the operating system platform and runtime environments used. (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. (P1)

3.3. 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. The media vendor's software shall meet currently supported OS/application systems and patch sources as soon as possible but within a maximum of thirty (30) days after release. (P1)

3.5. In case of a high risk (e.g. zero-day) vulnerability (own or third party), the vendor must inform the user and provide a workaround to mitigate the issue in case the device is connected to the internet. (P1)

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

3.7. The media vendor's software development must follow industry-standard development policies (e.g. OWASP Top 10). There shall be controls preventing cross-site scripting and SQL injection for Web front-ends. (P1)

3.8. 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)

3.9. The media vendor shall ensure that all of its products are sufficiently "cleaned" before release to ensure that no test code remains from the software development process. (P2)

3.10. The media vendor shall perform regular internal technical security analyses (i.e. penetration and vulnerability tests). (P2)

3.11. The media vendor must provide and support its approved security control guidelines when providing any third-party service, including cloud services. (P2)

3.12. All media vendor's systems, software and services must support risk management assessment and monitoring tools. The Internet browser used for system management shall be kept up-to-date with the latest security patches. (P3)

3.13. All media vendor applications must use modern protocols and services which have the ability to be heavily secured, monitored and analyzed by security tools, such as using HTTP/REST (tcp/443) instead of CIFS (tcp/445), MSSQL (tcp/1433) protocols. (P3)

3.14. The media vendor shall track and address all vulnerabilities and maintain an up-to-date and available register of this process. (P3)

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. (P2)

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.) (P3)

4.4. The media vendor should have a secure coding practice in place, complete with penetration testing with SOC I Type II (i.e. SSAE 16) certification, etc. This includes the certification of end-point tools (i.e. execution protection, advanced malware protection, etc.) with secure configuration guidelines. (P3)

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. (P3)

5. Encryption

5.1. Encrypted (e.g. TLS-based) network protocols (https, ftps, sftp) as well as certificates and PKI usage must be supported. All media vendors' systems, software and services must avoid the use of clear text protocols (i.e. http, telnet, ftp, etc.). (P1)

5.2. The media vendor’s systems, software and services must support the encryption of sensitive data, key ownership and management. Industry-accepted encryption algorithms from machine-to-machine at the application level shall be used (i.e. AES256). In addition, the client shall have the option to control a Master Key for encryption. (P2)

6. Network Configuration

6.1. There shall be no direct connection of control components with the Internet. (P1)

6.2. Transport Layer Security must be provided (Ex. SSL, TLS, IPsec) with all accounts complying with best-practice password complexity requirements. (P1)

6.3. The media vendor’s system, software and service must support a sufficiently granular segmentation of internal and external networks (i.e. multi-VLAN support, routing, etc.) (P2)

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

World Broadcasting Unions
January 2018