EBU

OPERATING EUROVISION AND EURORADIO

R 143

CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES

RECOMMENDATION

Geneva
April 2016

Cybersecurity Recommendation for media vendors' systems, software & services

EBU Committee	*First Issued*	*Revised*	*Re-issued*
TC	2016		

Keywords: Security, Services, Infrastructure, Broadcasting, IP.

Recommendation

The EBU, considering that,

1. Media companies increasingly employ third parties to provision their systems, software and services.

2. Production workflows and infrastructures are rapidly migrating to generic IT technologies.

3. Cyberthreats (e.g. malware and ransomware) are increasingly easier to perform and are continuously evolving.

4. Connected media devices still tend to have a low security threshold inherited from the era of non-connected broadcast media.

Recommends that media companies:

1. Apply the annexed security safeguards when planning and designing their systems, software and services.

2. Require potential vendors of systems, software and services to declare their ability to comply with the annexed security safeguards (by completing columns A, B & C) when responding to tenders or requests for technology.

3. Define their minimal vendor system acceptance level on the basis of this recommendation with full awareness of the potential risks.

Note

The annexed security safeguards have been drawn up using inputs from recognised European safety institutes including ANSSI[1], BSI[2], together with inputs from a group of European broadcasters with recent, hard-won experiences of dealing with security issues.

[1] Agence Nationale de la Sécurité des Systèmes d'Information (France) : http://www.ssi.gouv.fr

[2] German alliance for cybersecurity : https://www.allianz-fuer-cybersicherheit.de/

Page is intentionally blank. This document is formatted for two-sided printing.

Annex: Recommended Security Requirements

Vendor Security Requirement	A Do you provide this requirement? (Yes or No)	B If you answered "No" in column A, when will this requirement be met / provided?	C Your Questions/Remarks
1. Organisational Safeguards			
1.1 Product lifecycle & internal processes			
Follow well known best practices or information security standards when developing and implementing security measures			
Strive for a broadly accepted certification regarding the implemented security measures			
"Implemented, written development policies (e.g. following OWASP Top 10…)"			
Mandatory test stages (security gates) required within the development cycle			
Implemented code analyses during development cycle			
Cleaning of products to ensure that no test code remains from the development process			
Regular technical security analyses (penetration and vulnerability tests)			
Tracking and handling of vulnerabilities			
Clearly define the product lifecycle and ensure that patches and updates are available over that lifecycle.			
Support for security updates for all third-party components, including the operating system platform and Runtime Environments used.			
1.2 Communication			
Appointed points of contact or other contact options for security questions and incidents			
Information process for customers in case a weakness in a product becomes known			

Vendor Security Requirement	A Do you provide this requirement? (Yes or No)	B If you answered "No" in column A, when will this requirement be met / provided?	C Your Questions/Remarks
"Vendor shall support customer maintenance access procedures (RAS, VPN, Accounts, Password) "			
2. Product Safeguards			
2.1 Documentation			
Explicit instruction to change passwords from their defaults is necessary			
Proper description of security functionalities			
"Documentation of interfaces, access points, network communication and features"			
"Inclusion of information on how to integrate the product in a security concept (e.g. different network zones, central authentication service, workflows, interfaces, only the necessary TCP/UDP ports are open …)"			
Recommendation on hardening or best practice configuration			
Description of the patch management process regarding security updates			
2.2 Authentication and Authorization			
"Must support central authentication services (e.g. LDAP, active directory, Radius)"			
Session timeout support			
Support for role based access control			
Support of personalized accounts			
Enforce change of default passwords			
Support for implementation of a password policy			
Two-factor authentication support for internet facing products			
Strong authentication such as two-factor authentication			
Support for AAA logging on centralized logging server			

Vendor Security Requirement	A Do you provide this requirement? (Yes or No)	B If you answered "No" in column A, when will this requirement be met / provided?	C Your Questions/Remarks
2.3 Encryption			
Encrypted password storage and transfer			
Support of state-of-the-art encryption technologies, following the best practice recommendations			
"Support for encrypted (e.g. TLS based) network protocols (https, ftps, sftp)"			
"Avoid clear text protocols (http, telnet, ftp) "			
Support of certificates and PKI usage			
2.4 Base configuration			
Support for logging (at minimum, failed and successful login events AAA)			
"Support for centralized logging of log files (Syslog, Events Logs)"			
Option to control connection of USB and portable media			
Deactivation of unneeded network protocols and services			
"Must support effective protection against Virus/Malware and Exploits (e.g. Antivirus, EMET) on server and client side."			
Hardened base operating system if provided by the vendor			
Must support vulnerability scanners			
Support for monitoring (min. SNMPv2)			
Backup / Restore support (configuration settings)			
Possibility for decoupling the operating system from the software itself (allowing OS and Runtime Environments patching)			
2.5 Network configuration			
"Support for sufficiently granular segmentation of networks (MPLS, Multi VLAN support, Routing)"			
No direct connection of control components with the Internet (licensing issues)			

Vendor Security Requirement	A Do you provide this requirement? (Yes or No)	B If you answered "No" in column A, when will this requirement be met / provided?	C Your Questions/Remarks
"If Internet connection is needed, support for content inspection (e.g. forward and reverse proxy, including authentication mechanisms)"			
Support for maintenance access points in a demilitarised zone (DMZ) so that vendors or administrators first connect to a DMZ instead to the application itself. (e.g. Jumphosts)			
2.6 Application security			
Implemented proper input validation inside the application			
Controls against Cross Site Scripting and SQL Injection for web frontends (e.g OWASP Top 10)			
"Support add-on plug-in release management (e.g. Flash, Java, PHP, ...)"			
Regular patch management for provided applications			
Application runs in non-admin context (fewest privileges possible)			
Zero day vulnerability management and communication			
3. Vendor ISMS			
There is a documented Cyber Security Policy in place			
An effective Cyber Security Organisation is established			
A CISO is named who is granted the needed competencies to fulfil the role			
An Audit plan exists that includes regular audits and penetration tests of the internal infrastructure			
"Cyber Security is included in employee trainings, regular awareness campaigns are conducted"			