North American Broadcasters Association

Your voice in the international broadcasting community

Risk Awareness & Continuity Committee (RACC)

November 1, 2015

The objective of this document is to help establish the base expectations of NABA members concerning cyber security for vendor products, hardware, software and services. This will hopefully open a dialogue to drive the media industry toward more consistent compliance with cyber-security best practices. Below are the top cyber controls that are recommended media vendors develop, possess, and provide:

1. Documentation & Testing
   - 1.1. A written physical & cyber security policy that meets existing best practice (*ex. NIST, DHS*).
   - 1.2. Secure coding practice & Pen Testing with SOC I Type II (*aka SSAE 16*) certification, etc. This includes certification for end point tools *(ex. Execution protection, advanced malware protection*) with secure configuration guidelines.
   - 1.3. Options for automatic alerting and notification of patch updates.
   - 1.4. Physical and digital security controls by vendor through delivery of product, software or service.
   - 1.5. Vendor direct line contact available 24/7 for zero day critical attacks on their product/service.
2. Authentication
   - 2.1. Active Directory and/or LDAP certification & validation.
   - 2.2. Network login protocols (*ex. SSO with ability to segregate role based account management capabilities*). If externally facing additional network controls should be supported (*Two-Factor Authentication*).
   - 2.3. Ability to monitor and extract open format log data and key performance indicators.
   - 2.4. Support for Layer 3 network capabilities. Communications between trusted and un-trusted sources may be restricted to source & destination IP(s) as well as lowest possible number of TCP/IP ports to minimize application attack surface.
3. Controls
   - 3.1. Active AV support with validation/certification as well as best practice configurations (*directories, etc.*) for 'top 3 AV products'.
   - 3.2. Support risk management assessment and monitoring tools.
     - 3.2.1. Applications should also use modern protocols and services which have the ability to be heavily secured, monitored, & analyzed by security tools – ex. using HTTP/REST (*tcp/443*) instead of CIFS (*tcp/445*), MSSQL (*tcp/1433*) protocols.
   - 3.3. Vendor approved security control guidelines when leveraging cloud services.
   - 3.4. Option to remove USB ports and ability to disable auto start of USB/CD/DVD media as a presetting.
   - 3.5. Options for encrypting sensitive data and key ownership/management.
     - 3.5.1. Industry accepted encryption algorithms from machine to machine in application level (*ex. AES256*).
     - 3.5.2. Allow user/purchaser to control Master Key for encryption.
   - 3.6. Applications should;
     - 3.6.1. Meet currently supported OS/application systems and patch sources within 90 days of release.
     - 3.6.2. Support a proxy *(& reverse proxy*) option when initiating internet access. Where possible applications should support proxy services for both inbound and outbound traffic.
     - 3.6.3. Assure solution infrastructure components do not run in "User mode" but instead run as a service.
       - 3.6.3.1. Have an option to run in non-admin context.
     - 3.6.4. Transport Layer Security (*Ex. SSL, TLS, IPsec*) with all accounts used complying with industry standard best practice password complexity requirements.
     - 3.6.5. Only minimum required services should be active by using industry accepted best practice for system hardening (*ex. CIS benchmarks*).