Doc T-20/10-2

DRAFT

RECOMMENDATION 1/2020

Supporting the WBU Cybersecurity Recommendations on Broadcasters' Use of Cloud-based Services

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, particularly given the current increased migration to IP-based production and distribution technologies;

3. that broadcasters are extensively using cloud-based services for different applications of content processing, sharing and delivery;

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

5. that there is a continuous increase in threats like malware and ransomware, and there has been recent cyberattacks targeted at media organisations;

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 already published two such recommendations to educate and guide broadcasters on the importance of taking necessary measures,

8. that the World Broadcasting Union with support from its broadcasting unions have now developed a third set of recommendations as a guide for broadcasters' use of cloud-based services,

The ABU Technical Committee Recommends

1. The WBU proposed Recommendations on Broadcasters' Use of Cloud-based Services (see Annex), provides a comprehensive set of guidelines that can be considered by broadcasters and media organisations to enhance their security profile specifically when working with Cloud-based services.

2. The ABU members should move ahead to implement the proposed recommendations which will further strengthen and safeguard their networks from potential cyberattacks.

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

World Broadcasting Unions Cybersecurity Recommendations on Broadcasters' Use of Cloud-based Services

Introduction

The World Broadcasting Unions (WBU) has already produced two recommendations associated with cybersecurity, namely:

- WBU Core Cyber Security Controls, 2018 (https://nabanet.com/wp-content/uploads/2019/08/WBU-TC-Core-Cyber-Security-Controls-2018-10-03.pdf)
- WBU Cybersecurity Recommendations for Media Vendors' System, Software and Services, 2018 (https://nabanet.com/wp-content/uploads/2018/02/WBU-Cyber-Security-Recommendations-for-Media-Vendors-2018-01-29.pdf)

The WBU is now issuing cybersecurity recommendations associated with broadcasters' use of cloud-based services.

Cloud-based Services

The use of cloud-based services by broadcasters is now ubiquitous across the industry. Use cases can range from traditional internal virtual facilities to the use of third-party public services, for the delivery of all broadcast applications, such as content hosting, virtualized production, delivery over IP, etc.

Cloud capacity can be commissioned within minutes, making broadcasters more agile and more able to deploy additional functionality in response to market needs. Like any other third-party service employed, broadcasters need to be fully cognizant of the cybersecurity implications of employing this capacity.

Existing Union Cybersecurity Recommendations

Many of the WBU's Broadcast Unions and their members have been actively engaged in cybersecurity, in terms of producing recommendations, holding colloquia, sharing best practices and mitigation strategies and providing training. The Asia-Pacific Broadcasting Union, the European Broadcasting Union and the North American Broadcasters Association, as examples, have all made efforts in this regard.

Some of the same Unions have already made specific cybersecurity recommendations with respect to the use of cloud-based services. They are:

- EBU R146 – Cloud Security for Media Companies, 2017 (https://tech.ebu.ch/publications/r146)
- NABA's Initial Recommendations for Public Cloud Services, 2019 (https://nabanet.com/wp-content/uploads/2019/09/Initial-Recommendations-for-Public-Cloud-Services-02072019-FINAL.pdf)
- NABA's Initial Cybersecurity Recommendations for Software as a Service (SaaS), 2019 (https://nabanet.com/wp-content/uploads/2019/09/Initial-Recommendations-for-SaaS-02072019-FINAL.pdf)

WBU Recommendations

The WBU recommends that all Unions pay specific attention to all aspects of cybersecurity when considering the use of cloud-based services, particularly given the current migration to IP-based production and distribution technologies.

The WBU recommends that all Unions refer to and employ the existing Unions' recommendations, as previously noted.

In addition, the WBU makes the following general recommendations with respect to the use of cloud-based services by broadcasters:

1. Cloud security is a shared responsibility between the cloud service provider and the broadcaster. The demarcation of responsibilities between the parties should be clearly defined and documented before any data is migrated;
2. Broadcasters should undertake a priority classification of potential data to be transferred. This will ensure overly sensitive or mission critical material is retained in the enterprise and not transferred to the public cloud;
3. Comprehensive cloud access controls and associated authentication rights should be implemented for broadcasters' use. In addition, internal enterprise access controls should be replicated in the cloud, multiple processes regarding access and identity management should be avoided;

4. The use of virtual private cloud is preferred to multi-tenant public cloud from a cybersecurity perspective as it provides integrated control and threat assessment for the broadcaster;
5. Continuous and stringent vulnerability assessments must be undertaken by the cloud service provider to minimize both service provider and broadcasters' vulnerabilities;
6. Data encryption in the cloud is crucial for robust cybersecurity, including when such data is in motion or at rest. This is particularly important when importing or exporting data;
7. Broadcasters should implement comprehensive Intrusion Detection Systems (IDS) when implementing any cloud solution, to identify unauthorized data ingress or egress;
8. A data deletion policy and associated processes should be documented between the parties before migrating to the cloud;
9. As part of the broadcaster's overall enterprise security program, continually train broadcasters' employees on cloud security, including the detection and mitigation of malicious or suspicious activity in the cloud environment;
10. Regularly conduct security audits, including third-party audits, of all broadcasters' systems, including all cloud infrastructure, in order to identify and mitigate vulnerabilities and security gaps.

October 13, 2020