EVENT SUMMARY

tech.ebu.ch/mcs2019

Disclaimer: This report is intended as a quick overview of the event. Before quoting any of the speakers we recommend that you refer to the original presentation and check with the speakers themselves. Videos will be available in due course.

KEYNOTE

MEDIA CYBERSECURITY SEMINAR
AN EBU EVENT

Managing cybersecurity at a large multimedia group

Andreas Schneider (CISO, Tamedia)

At Switzerland's largest private media company the aim for cybersecurity is to be "**device and location agnostic**".

The **CISO reports directly to a board member**, alongside the CTO and CIO.

Rather than trying to control everything, with approved apps and tools, a Google-inspired **Zero Trust approach** assumes *the device will be hacked*. So the boundary is moved to the application. Two-factor authentication is used, and any device that has the Endpoint Detection Response tool installed is trusted. Bring Your Own Device is then possible, which helps with talent retention.

Taking an **agile CISO approach** means using a lot of automation and doing user-focused security. Users are given a data-driven personal security rating and encouraged to take steps to improve it, for example by using encryption, patching, etc.

"*We work together to shape the technology for the whole group. You're not an advisor anymore – you are responsible. But you can have an impact on the whole company.*"

1. CYBERSECURITY LANDSCAPE

Smart holes in your perception

Alex “Jay” Balan (Bitdefender)

The security-related stories that are reported in the mass media can cast an unhelpful spotlight on certain issues, while **blinding you to issues that are more critical**.

Placing a sticker over the webcam on your laptop may give you a false sense of security. In real life scenarios, the only actual situations when the camera was taken advantage of was in cases of blackmail where the user knowingly used the camera, but never with malware.

The greatest risks come with machine learning processes that capture what you type, backdoor APKs on Android devices giving access to the microphone, the hacking of app suppliers allowing access to permissions that have been granted to that app, etc.

“*Passwords must die! If you have any way to disable the usage of passwords in your organizations, do it.*”

Deep learning based deepfake detection

Anthony Sahakian (Quantum Integrity)

Deepfakes are created by a Generative Adversarial Network (GAN) where one AI system creates the fake images or videos while the AI other system tries to correctly identify the fakes. The result is **ever-more accurate imitations**.

Today a GAN network cannot recreate a whole person from scratch, but that capability will come within 5-10 years.

Quantum Integrity is building one of the first deepfake detectors, but it’s a challenge. There is limited data to work with (and they’d like to talk to anyone who can provide more source material) and it’s hard to keep up with the fast pace of deepfake development.

The next project for Quantum Integrity will be a blockchain-based project to track and trace images from the moment of creation.

2. VULNERABILITY MANAGEMENT

Crowdsourced Security: get hacked before you get hacked

Inti de Ceukelaire (intigriti)

If a hacker finds a vulnerability in your system will they know how to contact you? Can they be sure you won't sue? Will you care and will you fix the vulnerability? These, and other questions, are why you should have a Responsible Disclosure policy. **It's a great way to do passive security research**.

EBU R 161 is a comprehensive guide on how to establish a policy. And it should be complemented by a Safe Harbour policy (like that of Dropbox) that undertakes to help defend anyone who is acting in line with your disclosure policy.

You may have a "Hall of Fame" to highlight those who identify significant bugs. T-shirts or other gifts are also offered as rewards. But while Responsible Disclosure policies are a good start, **offering a real Bug Bounty – usually through an external broker – is even more effective**. The money paid is proportional to the significance of the bug identified.

There are some important **things to do before implementing a Responsible Disclosure programme**: check your assets and your DNS; check your cloud configuration; and review your business flows.

Implementing Responsible Disclosure at VRT

Wim Wauterickx & Gerben Dierick (VRT)

The aim of VRT's RD policy is to make their systems safer. It represents an agreement with ethical hackers to allow them to **help VRT without the risk of being prosecuted**.

1. Make sure the policy is available (including via /security.txt) and has approval of your legal department
2. Make sure you have a communication channel, with a secure key
3. Don't underestimate the process you need to implement (monitoring the mailbox, respond in time, obtain developer time to fix bugs)
4. Recognize the ethical hackers with a hall of fame or rewards

Wim: "*As a CISO you have your blind spots. Pen testers have checklists: they know the weak spots but they have no creativity. Ethical hackers don't have checklists.* ***They have a goal and a motivation to succeed and they're very creative***."

The RD policy was quietly put online in January 2019. **Without any publicity it generated ten useful reports** (e.g. sub-domain takeover risk, an unpatched VPN endpoint).

A Bug Bounty programme has now been launched, initially privately. It has already been the source of some high quality bug reports. Rewards range from €250 to €2,500.

3. CONTENT PIRACY

Price of piracy: the hidden threats within illicit streaming services

Norbert van der Laan (Irdeto)

Illicit streaming is used as **a means of delivering malicious software** – malware. ISDs are highly vulnerable. They are made cheaply and sold at a low price (around €25) but are not supported on an ongoing basis. Most run old versions of Android that have many vulnerabilities. The largest botnet yet discovered was shown to have started by taking advantage of ISDs.

Pirate websites are also a source of malware. An Irdeto analysis of the Cricfree site found many concerns: lots of pop-ups, browser extensions added, malware pretending to be an Adobe Flash update, new search managers, fake antivirus programmes.

Consumers are targeted by pirates who seek a return on their investment. **Streaming piracy is a security blind spot** – there's nowhere to complain and users already sense they are doing something wrong. There is a willingness to click as they seek to watch a live game.

There is a need to **create awareness among end users of the risks of using illicit streaming services**, whether web-based or on illicit streaming devices (ISDs).

Broadcast signal piracy and the challenges for broadcasters

Diane Hamer (BBC)

While BBC makes its licence-funded services freely available in the UK, audiences outside of the UK can access content legitimately via several distribution channels handled through BBC Studios. There is a subset of pirate IPTV operators that specialize in offering – and monetizing – UK broadcasters' free-to-air content.

One example is MyTVAbroad, a site that at first glance seems to be professional and legitimate. With customers around the world paying GPB 389 per year, the annual revenue generated by the service is estimated at GBP 4 million. That example is the tip of the iceberg: at least 90 different such services carry BBC channels illegally.

The pirates are well-resourced, highly mobile, can hide and move their location, and are very profitable. In one case, an operation where the UK police seized GBP 250k worth of equipment was up and running again within two weeks.

"*We need to get better at prevention, detection, investigation and enforcement. We need to explore technical solutions and legal remedies.*"

4. CONTENT PROTECTION

Content security in federated cloud media workflows

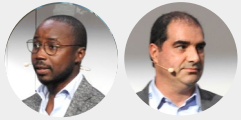
Ben Schofield (Consultant)

Media workflows, although still primarily on premise, are moving inexorably to the cloud. This is driven by several factors, among them the need for scale and resilience, cost pressures, changing audience behavior and the need to react quickly.

There has been a rise of domain specialists that can be put together in an end-to-end workflow. They're all **cloud-native and can connect together with API-based integration** and increasingly with standards-based messaging.

Today's content security audits, for example from the MPA, cover three domains: organization and management; physical (facility, asset management, transport); and digital (infrastructure, content management, content transfer).

Moving to app & cloud involves a different approach. There is an **evolution of the content security chain**. Standards and patterns play an important role. The UK-based dpp has a Committed To Security checklist for self-certification. The US Studios are working on a Trusted Partner Network. This will bring in a single common set of audits.



Protecting live content over satellite and beyond

Adi Kouadio (EBU) & Julien Mandel (ATEME)

BISS-CA is a standard that can be used to protect live sport content in both free-to-air and payTV scenarios. **Piracy is a major threat for live sport**, where companies pay billions for exclusive rights. There is an awareness of the need to enable the creation of more forensic data to pursue the pirates.

The original standard, BISS, was created in 2002 to secure satellite transmission feeds across different providers. However, the 64 bit keys used are no longer secure and there was a need to enable content tracking.

BISS-CA, developed by the EBU with ATEME and Nevion, allows the management of a diverse set of IRDs in real time, entitling and revoking them in-stream. It uses 128 bit public key encryption **and allows for watermark insertion at the receiver side**.

It already has **wide industry support**, including most of the Tier 1 vendors. BT Sport is using it for all HD feeds from the English Premier League, and it was used during the African Cup of Nations. Most of the major sports federations are investigating the protocol for future deployment at their major events.

5. CYBERSECURITY IN AGILE ENVIRONMENTS

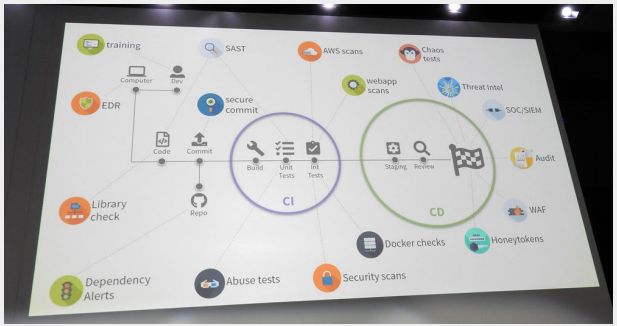
Shift Left security

Andreas Schneider (Tamedia)

The idea of Shift Left security is to move security considerations to the far left of the development timeline, rather than only thinking about them at the end. It's all about **bringing security to the developers**.

Shift Left means you start with the developer's computer. They want to use their own devices and you have to embrace that. Tamedia also trained some developers on how to hack: if you know how to break things you also know how to build them properly.

The main principles are **a secure computer and secure code**. All along the CI/CD pipeline there are steps that can be taken, such as chaos tests, code analysis, security scans, dependency alerts. And most of these can and should be automated.



Secure development life cycle

Dennis 't Jong (NPO)

There are many scary figures related to security: 24,000 malicious mobile apps blocked every day; 65% of companies have over 500 users who are never prompted to change their passwords; 74% of companies have over 1,000 stale sensitive files.

The business must require reliable applications. If the functionality is ready but the security is not there, do you bring it to production? And who will accept the risks. **Regardless of which development models you use, there are security questions to be asked**.

For Scrum and Agile, are security requirements on the backlog? What does a sprint provide? For Lean Startup, you have a problem to solve – is security part of it? Is your MVP safe? In DevOps, is security part of both development and operations?

Incorporate security into your teams – it's not standard knowledge for developers. Treat it as a functional requirement, an enabler rather than a disabler.

The EBU group is working on a **new recommendation (R 168) on best practices for a secure development life cycle**. Watch this space!

6. CYBERSECURITY INFRASTRUCTURE

Two years' experience with a media company SOC

David Garcia (France Télévisions)

A SOC is a Security Operations Centre. It's not about managing firewalls – it's about incident response, and the kill chain, which describes the steps of the response.

FTV implemented its first SOC, with an external provider, in November 2017.

While there are fixed costs, **the variable costs are more significant** as they are related to the amount of data you send to the SOC. At FTV, not all logs are sent to the SOC – some basic alerts are generated internally from the general data lake.

Collecting logs isn't easy – you will need to work with your company to identify them and configure your equipment so that the correct logs are sent to the data collector. And the SOC must be able to parse the logs you're sending them.

FTV's first pentest will take place soon.

Active Directory Security

Sylvain Cortes (ALSID)

Active Directory has been the root cause of all widespread cybersecurity compromises, including the famous cases such as Target, Sony, etc. **AD security is difficult to manage** as there can be thousands of changes everyday and you need to differentiate between regular changes and strange behaviour.

Although AD is 20 years old, it's only in recent years that we've learned how to fix AD design to prevent problems with advanced malware. Even updating to the latest version of Windows is not sufficient – if the AD design is not safe, you will have problems.

Attackers aim to gain access to a single workstation, and then laterally to other workstations, before trying to use **privilege escalation** to gain access to servers and eventually the AD domain manager.

A framework, e.g. attack.mitre.org, can help to identify the necessary changes. Among the key issues to address, two key ones:

- Use different Admin accounts at different levels – don't use an AD domain admin account when using workstations.
- Use hardening techniques for your AD, including the free LAPS software from Microsoft that allows workstation password management using the local admin account.

6. CYBERSECURITY INFRASTRUCTURE (II)

A novel approach to outsourced SOC

Christian Raemy (Hacknowledge)

SOC implementation is complex because it needs to encompass every component of your IT systems. **It requires a lot of expertise, it's expensive and it's challenging**.

The goal is to get from the billions of events – logins, group changes, etc. – down to just a few alerts that relate to real compromises that you can address.

The solution offered combines the logs received from the customer with sensors on the network. These are combined to detect hostile activities, anomalies, data breaches, etc.

The SIEM (Security Incident & Event Management) system can be built on a virtual platform, but for real operation its **better to use hardware** or it can be overwhelmed quickly with the volume of data to be processed.

A one-year journey into SOC: the EBU adventure

Stéphane Perroud (EBU)

The EBU started its SOC implementation process in March 2018 with a Request for Information, followed by an RfP. A proof-of-concept in summer 2018 was followed by the **SOC going into operation in December 2018**.

An SIEM was setup in-house with physical devices, with selected logs sent to the external SOC provider. The provider is only used to raise alerts – **mitigation and resolution is handled internally**.

In the first year of operation several problems were encountered, including with the Windows and Linux Event Forwarders or with sensors overloading.

Critical success factors for an efficient SOC are:

- Monitor all SOC components – receiving no alerts doesn't mean you're safe
- **Test, test, test** all your use cases – what works today may not work tomorrow
- Plan your incident responses – for each use case defined you should have a response plan in place.

7. IP INFRASTRUCTURE SECURITY

Is your supply chain as solid as a rock?

Eric Barenzung (0x70)

Zero risk does not exist. Having many suppliers is risky, because it increases your attack surface. Security is a continuous process – you have to **manage your suppliers** on an annual basis. And your suppliers' suppliers.

You should start by raising awareness within your company, convincing your colleagues that security should be a part of the procurement process. Then you must evaluate the risks and perform a Business Impact Analysis.

EBU R 143 is one example of a set of criteria that can be used to evaluate suppliers. A radar can then be developed to highlight critical areas. It is recommended to map your suppliers and the risk associated with each.

Since it's impossible to have zero risk, **it is worth taking out cyber insurance**, which is now available from all insurance companies. It forms part of your risk management, transferring the risk to the third party. Typically companies use it to insure cases where the probability is low but the impact is high.

Security by Design: Building BBC Cardiff

Mike Ellis (BBC)

The decision to adopt IP-based production in the new BBC Cardiff building raised many cybersecurity challenges. A lot of risk is added with the move from point-to-point, specialized equipment to globally connected commodity equipment.

Security should not be seen as an option when building, buying and installing equipment. Broadcasters need to work with suppliers and help them understand. But. And air-gapping isn't security! **broadcasters must also build a layer of security into the systems**

Start by **reading just 22 pages**: EBU recommendations R 143 (cybersecurity for vendors), R 148 (security tests for networked equipment) and R 160 (equipment vulnerability management), plus the OWASP Top 10 Most Critical Web Application Security Risks.

BBC is working on a model that involves protecting sensitive content and systems within site-specific secure zones that can keep running without outside connectivity. Access, even remote access, can be managed in a secure way using a combination of Identity and Access Management and **Privileged Access Management**.

Deploy the patches! Count on paying for software support and licensing!

7. IP INFRASTRUCTURE SECURITY

Connected Media Risk Assessment Methodology

Alvaro Martin Santos (RTVE)

As part of his doctoral research, he is investigating the security of IP-based infrastructure for media production.

At the recent JT-NM Tested interoperability tests at Wuppertal, a team from the EBU Media Cybersecurity group ran a parallel cybersecurity scan. 65,000 TCP ports and the 100 most used UDP ports were scanned. 68 devices were tested.

A total of **387 vulnerabilities were found across the 68 devices**, with 18% of them rated from critical to highly critical. Even those that were not critical were exploitable.

There is a significant gap between the ideal state for cybersecurity and the current state. A risk assessment methodology has been designed, based on several well-known methodologies from non-media industry sources.

Future steps will include the creation of a general framework for the media industry and, hopefully, ISMS ISO 27001 certification.

SEE YOU NEXT TIME!

tech.ebu.ch/mcs2019
tech.ebu.ch/groups/mcs