AMPEG

AMPEG
Security Level Management

Keep the attack surface small

Norddeutscher Rundfunk

IT security for "The Best of the North‟: Central monitoring - overview is the key

A Security Lighthouse Case Study

Central monitoring - overview is the key

With television productions such as the "Tagesschau" or radio broadcasts such as the legendary "Hamburg Harbour Concert", NDR is one of the most important broadcasters in Germany. IT security is of utmost importance here, also in view of the public service programming mandate. While the initial contact had already been made some time ago, in 2020 the moment had finally come for NDR to bring AMPEG on board. Today, the AMPEG Security Lighthouse is the central tool for IT security.

Norddeutscher Rundfunk (NDR) is the joint regional broadcasting corporation of the Free and Hanseatic City of Hamburg, Lower Saxony, Schleswig-Holstein and Mecklenburg-Vorpommern. After the station was created in 1954 from the splitting of the NWDR into NDR and WDR, it went "on air" for the first time on 1 April 1956. NDR is a member of the ARD. As a non-profit institution under public law, NDR's mission is to inform, educate, advise and entertain. The NDR maintains its own state broadcasting centre in each of its four states: in Hanover, Kiel, Schwerin and Hamburg. Thirteen studios and six correspondents' offices contribute significantly to the regional anchoring of the NDR in the North. The NDR participates in the worldwide ARD correspondent network with offices in Brussels, London, New Delhi, New York, Beijing, Singapore, Stockholm, Tokyo and Washington. In total, NDR employs almost 3,400 permanent and over 1,100 freelance staff.

Fotos Studio Lüneburg aus 2010 ©NDR/Marcus Krüger

"The Best of the North" - under this slogan, NDR offers a wide variety of programmes. In addition to the contributions for the in-house NDR Fernsehen, the broadcaster contributes productions to the ARD joint programme "Das Erste" as well as to the ARD Mediathek. In addition, there is content for the ARD and ZDF joint programmes: ARTE, 3sat and Phoenix as well as the ARD digital programmes ONE and tagesschau24. The audio offering for the whole of the north includes the four regional radio programmes from the state broadcasting houses of Lower Saxony, Schleswig-Holstein, Mecklenburg-Vorpommern and Hamburg, the pop wave NDR 2, the young programme "N-JOY", "NDR Kultur" and the information programme "NDR Info" as well as a diverse range of podcasts, features and radio plays in the ARD Audiothek.

Central monitoring - overview is the key

Many programmes that are inseparable from the German TV landscape can be traced back to NDR. For example, tagesschau, Germany's most successful news brand, is created at NDR in Hamburg, where ARD-aktuell is based. As a digital brand, tagesschau is present on the news channel tagesschau24, on tagesschau.de, the tagesschau app and on the social web. NDR also plays a leading role in the talk show "Anne Will" or the "Eurovision Song Contest". With the "Hamburg Harbour Concert", broadcast for the first time in 1929, NDR has the oldest existing radio programme in the world in its programme.

Protect journalistically relevant data

What does IT security mean in a broadcasting company like NDR? First of all, it is about protecting the standard systems. At NDR, this includes not only information of a business nature in the SAP system, but also financial accounting and personnel data management, as well as the communication and collaboration systems. Seen in this light, the broadcaster can be compared to any other company or institution where, for example, it is a matter of preventing the intrusion of encryption Trojans. Beyond that, however, the entire media-specific IT that is used to produce the media at NDR also comes into focus. This occasionally includes extremely sensitive data that is directly related to journalistic work. Consider, for example, the Panama Papers of 2016, an investigative project to uncover international money laundering in which NDR journalists were also involved. Sensitive and journalistically relevant data of this kind must be reliably protected. Last but not least, a

Fotos Lüneburg 2021 ©NDR/Christian Spielmann broadcaster must also protect itself from extreme cases such as the foisting of false news or even the hijacking of a programme. Against the background of such worst-case scenarios, the IT security system is particularly important.

The problem with the overview

NDR and AMPEG had already been in contact for many years, as Agnes Graf, co-founder and managing director of the company, explains: "The will to work with us was there from the beginning. Over time, the requirements and the product became more and more compatible, so that in 2020 the final decision was made to implement the Security Lighthouse."

A look at the starting position is revealing: the NDR operates very many systems that can be thought of as islands in terms of data. This starts with the domain server, which accepts and answers the authentication information. The antivirus solution is located somewhere else, as are the systems for patching. To find out the status of a patch, different people always had to be contacted, as the NDR says. This gave them a view, but it also had to be interpreted. If, for example, a hundred computers are connected within such an island, it used to take weeks to name their security status exactly. For the NDR, the solution was also not to allow a person in charge to have access to the administration server, because this permission to do something entails a new security risk. In addition, the demands on IT security are continuously increasing. And the more systems are involved, the greater the need for information. Against this background, the NDR went in search of a central system that simply collects and correlates data. This solution was found in the AMPEG Security Lighthouse.

Around 9000 systems connected

The project started in 2020 with the introduction of the Security Lighthouse basics. "This basic package includes the Active Directory, virus protection and patch management," explains Michael Hänsel, project manager at AMPEG. "At NDR, these are currently the three main sources from which we fill our Security Lighthouse with data. The goal is to expand the installation further, with additional connections for network devices and the software inventory, for example." The proof of concept (PoC) took place from April to June 2020 and confirmed the functionality of the system. Via the Security Lighthouse, the NDR can now continuously monitor the current security status for more than 9,000 systems - servers, computers and other special devices assigned to staff in the domestic and foreign offices.

Central monitoring - overview is the key

Non-events are also displayed

Three core advantages emerge. First, there is the correlation of data from different sources. Everything can be filtered and the security-relevant information gathered in the clear and easy-to-use interface. Secondly, you cannot "break" anything in this interface and with this access. You can leave the Security Lighthouse to the employees without having to grant increased rights. Everyone can see in the interface what is happening on their computers and what they have to do, e.g. patch or reboot. Thirdly, Security Lighthouse supports the display of non-events. It also finds systems that no longer report for certain reasons, e.g. a defective computer that no longer pulls patterns or has problems with updates. Since the broadcaster looks after a total of around 9000 systems, singular failures and security gaps of this kind would not be noticed, as NDR says. The product, on the other hand, is designed for this and offers complete transparency. An example: a computer logs on to the domain, but does not download any patterns or updates. It is then considered not covered in the AMPEG system and appears red on the dashboard. This is now immediately noticeable, whereas previously it was a considerable problem for the NDR to find such gaps in the lists.

Fotos Sendestudio Ausbildung ©NDR/Cordula Kropke

Problem-free implementation

The implementation of Security Lighthouse was also straightforward in terms of effort. Security Lighthouse is an uncomplicated system that does not cost a lot of resources and effort and was easy to deploy at NDR. The maintenance effort is low. For the NDR staff, it is also an advantage that no separate user administration is necessary within Security Lighthouse. You simply authorise users or groups from the domain. A password does not have to be assigned for this either. As the central administrator of these systems, you can be very generous with this read permission because the employees do not exercise any control over the systems. No more access rights than absolutely necessary. Security Lighthouse complies with this principle.

Central monitoring - overview is the key

Teamwork in remote mode

The start of the project overlapped with the beginning of the Corona pandemic. Personal meetings between the IT specialists of NDR and AMPEG could not take place due to the infection control requirements. Despite initial scepticism, it was therefore decided to set up the project in remote mode. For Michael Hänsel, the fact that this unusual procedure worked well from the start underlines the uncomplicated nature of the product.

What is planned for the future? "Currently, the NDR is working with the three basic collectors of the Security Lighthouse, as already mentioned. In order to increase the evaluation possibilities in the Lighthouse according to demand, so-called Company Categories are available. We have now set up one of these. This has created a separate 'view' for broadcast-relevant systems." At NDR, broadcast-relevant systems are systems that contribute certain elements to a broadcast, e.g. the insertion of banners under the presenters or of graphics. In order for these broadcast-relevant systems to function smoothly, there must be no reboots during the programmes. By flexibly setting up an additional dashboard only for a dedicated user group, it was possible to realise a "special view" that meets the individual requirements of these systems.

Besides additional company categories and a software inventory, other connections from the Security Lighthouse "toolbox" are also conceivable for the NDR, e.g. network devices or mobile device management. This would allow further areas to be represented centrally in Security Lighthouse. In addition, more groups of people would be involved and the Security Lighthouse would become even more widespread at the NDR.

The solution was realised at:

Norddeutscher Rundfunk (NDR)
Rothenbaumchaussee 132
20149 Hamburg, Germany
www.ndr.de

With support from:

AMPEG GmbH
Stavendamm 22
28195 Bremen, Germany
www.ampeg.de

and cirosec GmbH
Ferdinand-Braun-Straße 4
74074 Heilbronn, Germany
www.cirosec.de

AMPEG