AMPEG

Norddeutscher Rundfunk

IT-Sicherheit für „Das Beste am Norden“: Zentrales Monitoring - Übersicht ist der Schlüssel

A Security Lighthouse Case Study

Zentrales Monitoring - Übersicht ist der Schlüssel

Mit Fernsehproduktionen wie der „Tagesschau" oder Radioübertragungen wie dem legendären „Hamburger Hafenkonzert" gehört der NDR zu den bedeutendsten Sendeanstalten Deutschlands. IT-Sicherheit ist hier auch mit Blick auf den öffentlich-rechtlichen Programmauftrag von höchster Bedeutung. Während der Erstkontakt bereits längere Zeit zurücklag, war 2020 für den NDR endgültig der Augenblick gekommen, AMPEG ins Boot zu holen. Heute ist das AMPEG Security Lighthouse zentrales Tool der IT-Sicherheit.

Der Norddeutsche Rundfunk (NDR) ist die gemeinsame Landesrundfunkanstalt der Freien und Hansestadt Hamburg, Niedersachsens, Schleswig-Holsteins und Mecklenburg-Vorpommerns. Nachdem der Sender 1954 aus der Spaltung des NWDR in NDR und WDR entstanden war, ging man am 1. April 1956 zum ersten Mal „on Air". Der NDR ist Mitglied der ARD. Als gemeinnützige Anstalt des öffentlichen Rechts hat der NDR den Auftrag, zu informieren, zu bilden, zu beraten und zu unterhalten. Der NDR unterhält in jedem seiner vier Staatsvertragsländer ein eigenes Landesfunkhaus: in Hannover, Kiel, Schwerin und Hamburg. 13 Studios und sechs Korrespondentenbüros tragen ganz wesentlich zur regionalen Verankerung des NDR im Norden bei. Am weltweiten ARD-Korrespondentennetz ist der NDR mit Büros in Brüssel, London, Neu Delhi, New York, Peking, Singapur, Stockholm, Tokio und Washington beteiligt. Insgesamt beschäftigt der NDR knapp 3400 feste und über 1100 freie Mitarbeiterinnen und Mitarbeiter.

„Das Beste am Norden" - unter diesem Slogan bietet der NDR eine große Programmvielfalt. Neben den Beiträgen für das hauseigene NDR Fernsehen steuert der Sender Produktionen zum ARD-Gemeinschaftsprogramm „Das Erste" sowie zur ARD Mediathek bei. Dazu kommen Inhalte für die Gemeinschaftsprogramme von ARD und ZDF: ARTE, 3sat und Phoenix sowie die ARD-Digitalprogramme ONE und tagesschau24.

Fotos Studio Lüneburg aus 2010 ©NDR/Marcus Krüger

Zum Audioangebot für den ganzen Norden gehören die vier regionalen Hörfunkprogramme aus den Landesfunkhäusern Niedersachsen, Schleswig-Holstein, Mecklenburg-Vorpommern und Hamburg, die Pop-Welle NDR 2, das junge Programm „N-JOY", „NDR Kultur" und das Informationsprogramm „NDR Info" sowie ein vielfältiges Angebot an Podcasts, Features und Hörspielen in der ARD Audiothek.

Zentrales Monitoring - Übersicht ist der Schlüssel

Viele Sendungen, die untrennbar mit der deutschen TV-Landschaft verbunden sind, gehen auf den NDR zurück. So entsteht zum Beispiel die tagesschau, Deutschlands erfolgreichste Nachrichtenmarke, beim NDR in Hamburg, wo ARD-aktuell angesiedelt ist. Als digitale Marke ist die tagesschau auf dem Nachrichtenkanal tagesschau24, auf tagesschau.de, der tagesschau-App und im Social Web präsent. Auch bei der Talkshow „Anne Will" oder dem „Eurovision Song Contest" ist der NDR federführend. Mit dem 1929 zum ersten Mal ausgestrahlten „Hamburger Hafenkonzert" hat der NDR die älteste bestehende Rundfunksendung der Welt im Programm.

Journalistisch relevante Daten schützen

Was bedeutet IT-Sicherheit in einer Rundfunkanstalt wie dem NDR? Zunächst einmal geht es darum, die Standard-Systeme zu schützen. Beim NDR zählen dazu neben Informationen betriebswirtschaftlicher Art im SAP-System auch die Finanzbuchhaltung und Personaldatenverwaltung, sowie die Kommunikations- und Kollaborationssysteme. So gesehen lässt sich der Sender mit jedem anderen Unternehmen oder Institution

Fotos Lüneburg 2021 ©NDR/Christian Spielmann

vergleichen, in denen es z.B. darum geht, das Eindringen von Verschlüsselungstrojanern zu verhindern. Darüber hinaus rückt aber auch die gesamte medienspezifische IT in den Fokus, mit der beim NDR die Medien produziert werden. Darunter sind gelegentlich extrem schützenswerte Daten, die direkt mit der journalistischen Arbeit zusammenhängen. Man denke etwa an die Panama Papers von 2016, einem investigativen Projekt zur Aufdeckung

internationaler Geldwäsche, an dem auch NDR-Journalisten beteiligt waren. Sensible und journalistisch relevante Daten dieser Art gilt es, zuverlässig zu schützen. Last but not least muss sich ein Sender auch vor Extremfällen wie dem Unterschieben falscher Nachrichten oder gar dem Kapern einer Sendung schützen. Vor dem Hintergrund solcher Worst-Case-Szenarien kommt dem IT-Sicherheitssystem eine besonders hohe Bedeutung zu.

Das Problem mit der Übersicht

NDR und AMPEG waren bereits langjährig in Kontakt, wie Agnes Graf, Mitgründerin und Geschäftsführerin des Unternehmens erzählt: „Der Wille, mit uns zusammenzuarbeiten, war von Anfang an da. Anforderungen und Produkt passten im Laufe der Zeit immer besser zusammen, sodass im Jahr 2020 dann die endgültige Entscheidung für die Implementierung des Security Lighthouse getroffen wurde."

Aufschlussreich ist ein Blick auf die Ausgangsposition: Der NDR betreibt sehr viele Systeme, die man sich datenmäßig als Inseln vorstellen kann. Das beginnt beim Domain-Server, der die Authentifizierungsinformationen annimmt und beantwortet. Die Antiviruslösung ist ganz woanders verortet, ebenso die Systeme zum Patchen. Um den Stand eines Patches zu erfahren, mussten immer unterschiedliche Personen kontaktiert werden, wie der NDR sagt. Man bekam dadurch eine Sicht, die aber auch wieder interpretiert werden musste. Sind innerhalb einer solchen Insel beispielsweise hundert Rechner angeschlossen, brauchte es vormals Wochen, um ihren Sicherheitsstand exakt zu benennen. Für den NDR lag die Lösung auch nicht darin, einem Verantwortlichen den Durchgriff auf den Verwaltungsserver zu gestatten, da mit dieser Erlaubnis etwas zu tun ein neues Sicherheitsrisiko verbunden ist. Hinzu kommt, dass die Anforderungen an die IT-Sicherheit kontinuierlich steigen. Und je mehr Systeme im Spiel sind, desto höher ist das Informationsbedürfnis. Vor diesem Hintergrund hat sich der NDR auf die Suche nach einem zentralen System gemacht, das lediglich Daten abgreift und korreliert. Mit dem AMPEG Security Lighthouse wurde diese Lösung gefunden.

Rund 9000 Systeme angebunden

Das Projekt startete 2020 mit der Einführung der Basics des Security Lighthouse. „Zu diesem Grundpaket gehören das Active Directory, der Virenschutz und das Patch-Management", erklärt Michael Hänsel, Projektleiter bei AMPEG. „Das sind beim NDR aktuell die drei Hauptquellen, aus denen wir unser Security Lighthouse mit Daten befüllen. Ziel ist es, die Installation weiter auszubauen, mit weiteren Anbindungen z.B. für die Netzwerkgeräte und das Software Inventory." Das Proof of Concept (PoC) fand von April bis Juni 2020 statt und bestätigte die Funktionalität des Systems. Über das Security Lighthouse kann der NDR heute für mehr als 9000 Systeme - Server, Rechner und andere Sondergeräte, die dem Personal in den in- und ausländischen Büros zugeordnet sind, den aktuellen Sicherheitsstatus kontinuierlich beobachten.

Zentrales Monitoring - Übersicht ist der Schlüssel

Auch Nichtereignisse werden angezeigt

Dabei schälen sich drei Kernvorteile heraus. Da ist erstens das Korrelieren der Daten aus verschiedenen Quellen. Man kann alles filtern und die sicherheitsrelevanten Informationen in der übersichtlichen und einfach zu bedienenden Oberfläche zusammentragen. Zweitens kann man in dieser Oberfläche und mit diesem Zugriff nichts „kaputt" machen. Man kann das Security Lighthouse den Mitarbeitenden überlassen, ohne erhöhte Rechte vergeben zu müssen. Jeder kann in der Oberfläche sehen, was auf seinen Rechnern passiert und was er tun muss, z.B. patchen oder rebooten. Drittens unterstützt Security Lighthouse das Anzeigen von Nichtereignissen. Es werden auch Systeme gefunden, die sich aus bestimmten Gründen nicht mehr melden, z.B. ein defekter Rechner, der sich keine Pattern mehr zieht oder bei Updates Probleme hat. Da der Sender insgesamt rund 9000 Systeme betreut, würde man singuläre Ausfälle und Sicherheitslücken dieser Art nicht bemerken, wie der NDR sagt. Das Produkt hingegen ist dafür ausgelegt und bietet komplette Transparenz. Ein Beispiel: Ein Rechner meldet sich zwar an der Domain an, zieht sich aber weder Pattern noch Updates. Der gilt dann im AMPEG System als not covered und erscheint auf dem Dashboard rot. Das fällt jetzt sofort auf, während es vorher für den NDR ein erhebliches Problem darstellte, solche Lücken in den Listen zu finden.

Fotos Sendestudio Ausbildung ©NDR/Cordula Kropke

Problemlose Implementierung

Die Einführung von Security Lighthouse gestaltete sich auch mit Blick auf den Aufwand problemlos. Security Lighthouse ist ein unkompliziertes System, das nicht viel Ressourcen und Aufwand kostet und sich beim NDR leicht bereitstellen ließ. Der Wartungsaufwand ist gering. Für das Personal des NDR ist es außerdem von Vorteil, dass innerhalb von Security Lighthouse keine eigene Benutzerverwaltung notwendig ist. Man berechtigt einfach User oder Gruppen aus der Domäne. Ein Kennwort muss dafür auch nicht vergeben werden. Als zentraler Verwalter dieser Systeme kann man sehr freigiebig mit diesem Lese-Recht sein, weil die Mitarbeitenden eben keine Macht auf die Systeme ausüben. Nicht mehr Zugriffsrechte als unbedingt nötig. Security Lighthouse entspricht diesem Grundsatz.

Zentrales Monitoring - Übersicht ist der Schlüssel

Teamwork im Remote-Modus

Der Projektstart fiel mit dem Beginn der Corona-Pandemie zusammen. Persönliche Begegnungen zwischen den IT-Spezialisten des NDR und von AMPEG konnten aufgrund der Auflagen zum Infektionsschutz nicht stattfinden. Trotz anfänglicher Skepsis entschied man sich deshalb, das Projekt im Remote-Modus aufzusetzen. Dass dieses ungewohnte Vorgehen von Anfang an gut funktioniert hat, unterstreicht für Michael Hänsel die Unkompliziertheit des Produkts.

Was ist für die Zukunft geplant? „Aktuell arbeitet der NDR mit den drei Basis Kollektoren des Security Lighthouse, wie schon erwähnt. Um die Auswertungsmöglichkeiten im Lighthouse bedarfsgerecht zu erhöhen, stehen sogenannte Company Categories zur Verfügung. Eine davon haben wir inzwischen aufgelegt. Hierdurch wurde für senderelevante Systeme eine eigene 'Sicht' geschaffen.“ Unter senderelevanten Systemen versteht man beim NDR Systeme, die bestimmte Elemente zu einer Sendung beitragen, z.B. das Einblenden von Spruchbändern unter den Moderatoren oder von Grafiken. Damit diese senderelevanten Systeme reibungslos funktionieren, darf es keine Reboots während der Sendungen geben. Durch die flexible Einrichtung eines zusätzlichen Dashboards nur für eine dedizierte Nutzergruppe konnte eine „Spezialsicht“ realisiert werden, die den individuellen Anforderungen dieser Systeme gerecht wird.

Neben zusätzlichen Company Categories und einem Software Inventory sind für den NDR auch weitere Anbindungen aus dem Security Lighthouse „Werkzeugkasten“ denkbar, z.B. Network Devices oder das Mobile-Device-Management. Damit ließen sich weitere Bereiche zentral im Security Lighthouse darstellen. Darüber hinaus würden mehr Personenkreise einbezogen werden, und das Security Lighthouse würde eine noch größere Verbreitung beim NDR bekommen.

Die Lösung wurde realisiert bei:

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

Mit Unterstützung von:

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

und cirosec GmbH
Ferdinand-Braun-Straße 4
74074 Heilbronn
www.cirosec.de