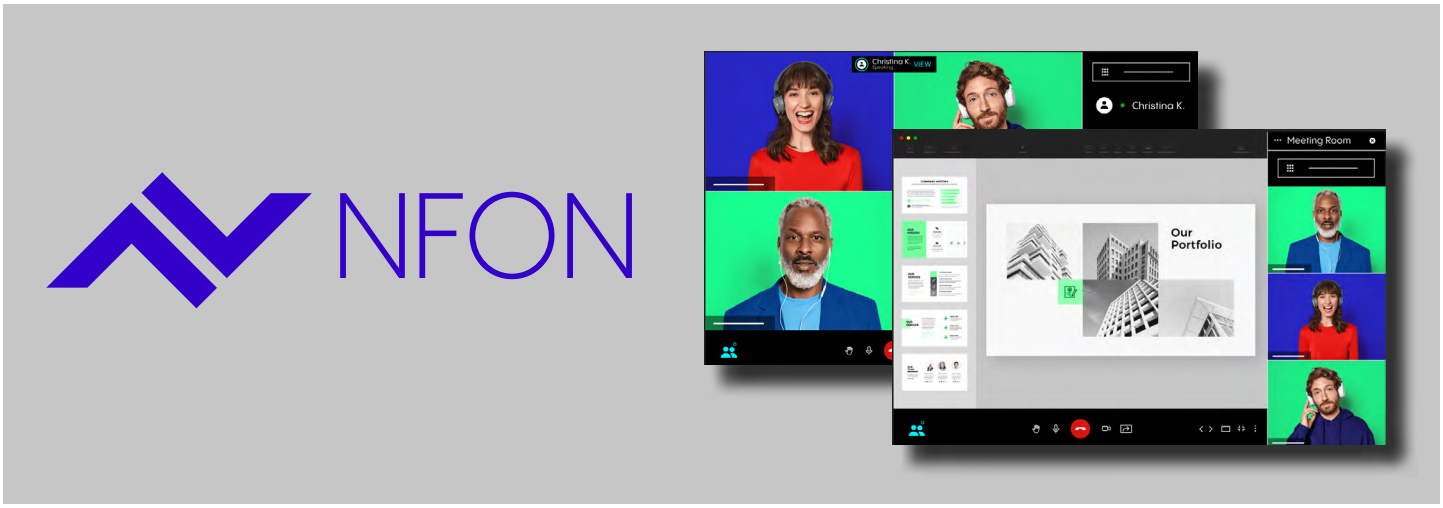

MYRA

CASE STUDY

# Absicherung von Cloud Communication Services erfordert Maßarbeit

**Case Study**
NFON

**Lösungen**
DDoS Protection
Hyperscale WAF
Secure DNS




# Elementar & hochkomplex: Wie NFON die IP-Telefonie vor Cyberkriminellen schützt

## Executive Summary

Die NFON AG ist mit mehr als 50.000 Kunden führender europäischer Anbieter von Cloud-basierten Telefonanlagen. Das Unternehmen ist in 15 europäischen Ländern aktiv und zählt mehr als 500 Mitarbeiter:innen. Digitale Kommunikationslösungen sind aus dem Alltag der meisten Firmen nicht mehr wegzudenken. Insbesondere seit Beginn der Corona-Pandemie sind Unified-Communication-Lösungen aus der Cloud in vielen Betrieben das Tool der Wahl, um Kunden, Partner und Beschäftigte miteinander zu verbinden – ganz unabhängig vom Standort. Der Schutz solcher elementaren Digitaldienste ist entscheidend, um das operative Geschäft dieser Firmen vor Ausfällen abzusichern. Bereits seit 2014 schützt NFON deshalb seine VoIP-Dienste mit den Security-as-a-Service-Lösungen von Myra Security.

## Zielsetzung

Die Absicherung von VoIP-Technologien gegen DDoS-Angriffe ist äußerst komplex, da bei der IP-Telefonie große Mengen von verbindungslosem UDP-Traffic anfallen. Dieser Datenverkehr lässt sich durch herkömmliche Schutzmethoden nur schwer bis unmöglich qualifizieren. Im Angriffsfall kann deshalb schadhafter Traffic nicht von regulären Anfragen unterschieden werden, was eine erfolgreiche Mitigation des Angriffs verhindert. Für diese technologische Hürde galt es, die passende Lösung zu finden.

## Dynamisches Whitelisting

Um die Herausforderung der Traffic-Qualifikation zu bewältigen, entwickelte Myra zusammen mit NFON eigens eine dynamische Whitelisting-Lösung. Dabei werden seitens NFON periodisch die IPs von registrierten und authentifizierten Endgeräten und anderen authentifizierten Verbindungen erfasst und in einem IP-Set zum Whitelisting bei Myra hinterlegt. Im konkreten Angriffsfall werden zunächst nur noch die Signalisierungsprotokolle und die Audio/Video-Pakete der bereits registrierten Clients durchgelassen. Die Herausforderung dieser Lösung liegt darin, dass zehntausende IP-Adressen pro Stunde zuverlässig erfasst und verwaltet werden müssen.

Technisch erfolgt die VoIP-Absicherung über den DDoS-Schutz für Infrastrukturen und Rechenzentren (Layer 3/4). Zusätzlich zum implementierten DDoS-Schutz setzt NFON auf die Myra Hyperscale WAF (Web Application Firewall) auf Layer 7, um damit etwa auch Legacy-Anwendungen vor Cyberattacken zu schützen. Zum Schutz der Namensauflösung der NFON-Domains kommt außerdem der Myra Secure DNS zum Einsatz.

## Umsetzung mittels Infrastrukturschutz

Die Schutztechnologien von Myra sind unabhängig von der bestehenden Infrastruktur und kurzfristig implementierbar, weil sie keine zusätzliche Hard- oder Software erfordern. Myra übernimmt nahezu die komplette Einrichtung und Konfiguration der Dienste. Der Aufwand auf Kundenseite fällt minimal aus.

Für die Aufschaltung des Infrastrukturschutzes erstellt zunächst der Kunde die RIPE-Route-Objekte für seine Netze gemäß der Vorgaben durch Myra. Um die Konfiguration

für die Netze kümmert sich das Expertenteam des Myra Network Operations Center (NOC). Mittels „More Specific"-Annoncierungen zieht Myra im Angriffsfall den kompletten eingehenden Traffic auf die eigenen Scrubbing Center. Dort wird der Angriffs-Traffic verworfen und der verbleibende saubere Traffic über eine vorher vereinbarte Verbindung dem Kunden wieder zugeleitet. Um diese Umschaltung zu automatisieren, kann Myra die Flow-Daten des Kunden auswerten. Dafür stellt der Kunde eine virtuelle Maschine zur Verfügung, die Myra-Fachleute übernehmen die Definition der Schwellenwerte und gleichen diese regelmäßig mit dem Kunden ab. Für die Traffic-Weiterleitung stehen direkte Verbindungen, virtuelle LAN-Verbindungen sowie GRE-Tunnel und IPSec zur Verfügung. Im Fall von NFON erfolgt die Übergabe des Clean-Traffics zwischen Myra und der Kundeninfrastruktur über zwei GRE-Tunnel.

## Secure DNS und Hyperscale WAF

Der Umzug der Namensauflösung samt zugehöriger Konfiguration von NFON auf Myra Secure DNS kann dank Hidden Primary ohne großen Aufwand delegiert werden. Die DNS-Server von Myra nutzen für das Routing Anycast, wodurch eine optimale Performance bei hoher Redundanz sichergestellt ist.

Die technische Aufschaltung auf Layer 7 für das WAF-Schutzsystem ist prinzipiell über zweierlei Wege möglich: Entweder erfolgt eine Anpassung des DNS-Eintrags über den CNAME-Eintrag oder der autoritative DNS-Server wird mithilfe eines Imports bestehender Zonen an Myra übertragen. Sobald nun die entsprechenden TLS-Zertifikate des Kunden per API oder Upload im Myra Dashboard zur Verfügung gestellt wurden, kann die TLS-Verbindung terminiert und eine Deep Packet Inspection durchgeführt werden. In enger Abstimmung mit dem Kunden übernimmt das Myra NOC abschließend die Konfiguration der Filterregeln. Maßgeschneiderte Filter erlauben eine granulare Traffic-Steuerung, um schadhafte oder verdächtige Anfragen mit der Myra Hyperscale WAF abzufangen, noch bevor sie die Systeme von NFON und deren Kunden erreichen.

## Datenschutz & Compliance „Made in Germany"

Vertraulichkeit und Integrität sind bei der elektronischen Kommunikation via VoIP mindestens ebenso wichtig wie die technische Sicherheit. Angesichts dessen war es für NFON entscheidend, bei der Providerwahl auf ein deutsches Unternehmen zu setzen, das dieselben strengen Datenschutz- und Sicherheitsvorgaben erfüllt wie NFON. Mit einem hochzertifizierten Anbieter wie Myra (ISO 27001 auf Basis von IT-Grundschutz, PCI-DSS-zertifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, KRITIS-qualifiziert, BSI-C5-Testat Typ 2, Trusted Cloud) erreicht NFON rechtssichere Compliance und DSGVO-Konformität. Diese Eigenschaften tragen auch dazu bei, strategische Geschäftspartner wie die Deutsche Telekom zu gewinnen, die ihre IT-Projekte mittels anspruchsvoller PSA-Verfahren (Privacy and Security Assessment) absichert. Für eine erfolgreiche Zusammenarbeit werden dabei Sicherheit und Datenschutz auf höchstem Niveau vorausgesetzt – sowohl bei NFON selbst, als auch bei angeschlossenen Dienstleistern.

## Resümee

Seit Aufschaltung der Myra-Schutzdienste profitiert NFON von passgenauen Sicherheitslösungen, die den besonderen Anforderungen moderner Cloud-Kommunikation im Unternehmensumfeld entsprechen. Die IP-Telefonie-Lösungen des Unternehmens sind damit zuverlässig vor Cyberattacken geschützt – und das unter strikter Einhaltung strengster Datenschutzvorgaben.

Jan-Peter Koopmann, Vorstandsmitglied und CTO bei NFON, resümiert die erfolgreiche Zusammenarbeit mit Myra wie folgt: „Myra hat für uns ein Produkt entwickelt, das essenziellen Schutz für die IP-Telefonie-Dienste von NFON bietet. Eine vergleichbare Lösung konnte uns in dieser maßgeschneiderten Form kein anderer Anbieter liefern. Bei Myra erhalten wir individuelle Services, die auch unseren hohen Ansprüchen an Datenschutz und Compliance gerecht werden."

### Die Zusammenarbeit mit Myra bietet NFON folgende Vorteile:

- DDoS-Schutz mit dynamischem Whitelisting für die Absicherung von VoIP-Diensten
- Absicherung von Legacy-Anwendungen mittels Hyperscale WAF
- Absicherung der Namensauflösung durch Myra Secure DNS
- regulatorisch rechtssichere Partnerschaft mit einem hochzertifizierten Provider aus Deutschland
- Made in Germany, rechtssichere DSGVO-Konformität
- lokaler 24/7-Support aus Deutschland über das Myra NOC am Hauptsitz in München

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021

PCI DSS Certified

BSIG KRITIS-qualifiziert

EU-DSGVO konform

BSI C5 TESTAT TYP 2

Trusted Cloud SERVICE 10043

CERTIFIED IDW PS 951 ISAE 3402

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister