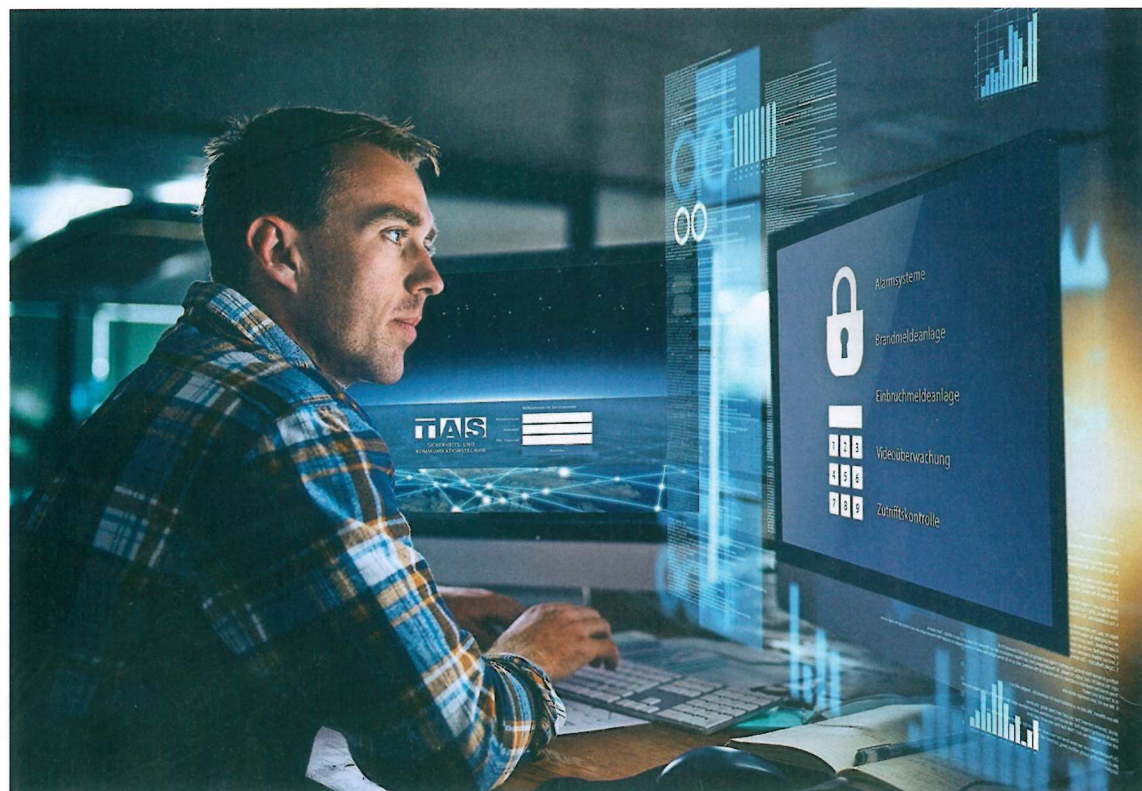




Für einen sicheren Fernzugriff auf Gefahrenmeldeanlagen müssen mehrere Aspekte beachtet werden.

Foto: TAS

Wer übernimmt die Verantwortung?

Remote Services sind inzwischen für Gefahrenmeldeanlagen gängige Praxis. Neben Cybersecurity geht es hierbei auch um die Verantwortung für den sicheren Fernzugriff.

DANIEL KAUMANN

Der Fernzugriff auf technische Anlagen hat viele Vorteile. Auch bei Alarmsystemen setzen viele Unternehmen auf Remote Services, um zum Beispiel teure Vor-Ort-Einsätze zu reduzieren und durch kontinuierliches Monitoring eine bessere Verfügbarkeit der Systeme zu gewährleisten. Dabei gibt es allerdings zwei kritische Aspekte, die berücksichtigt werden müssen: Der Schutz vor unerlaubtem Zugriff auf die Plattform, über die der Fernzugriff erfolgt. Und zweitens muss der Service Provider, der die Infrastruktur für Remote Services zur Verfügung stellt, die stän-

„Wir bieten mit der TAS Secure Plattform sicheren Fernzugriff auf Alarmsysteme.“

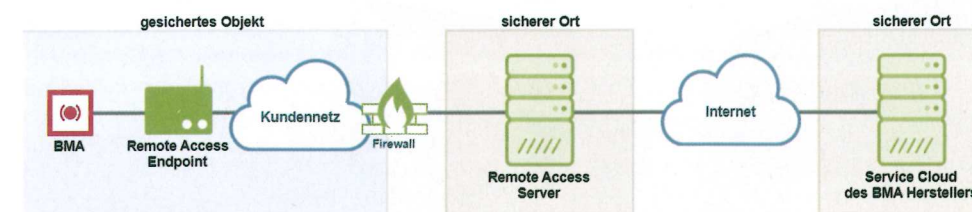
Daniel Kaumanns,
Produktmanager TAS

dige Verfügbarkeit und IT-Sicherheit des Remote Access sicherstellen. Eine Verantwortungsübernahme, die künftig klar geregelt ist.

Hoher Schutz gegen Cyberangriffe

TAS Sicherheits- und Kommunikationstechnik, ein Spezialist für Alarmübertragungsgeräte und Anbieter von Sicherheitslösungen für Konzerne, Logistiker und Filialketten, erfüllt mit der TAS Secure Plattform beide Anforderungen.

Wie ist die Sicherheit der Verbindung zwischen dem Service-PC beim Errichterunternehmen auf der einen Seite und den sicherheitstech-



Für eine normkonforme Konnektivität koppelt die TAS die Plattformen des Herstellers und des Errichters, indem sie die Verbindung über ihren Sicherheitsrouter bis hin zur TAS Secure Platform zur Verfügung stellt.

Infografik: TAS

nischen Gewerken auf der anderen Seite gewährleistet? Über das Web-Portal wird für jeden Nutzer ein eigenes Konto eingerichtet, das durch Zweifaktor-Authentifizierung gesichert ist. Übertragungseinrichtungen oder auch Gefahrenmeldeanlagen wie zum Beispiel Videokameras, Einbruch- und Brandmeldeanlagen erhalten einen separaten und sicheren 1:1 Zugang zur Secure Platform. Alle Systemzugriffe werden dokumentiert. Zudem ist die Betriebssicherheit durch mehrere Firewalls, Monitoring der Plattform und Penetrationstests gewährleistet.

Alle Daten und Zugangsberechtigungen werden unter Berücksichtigung von Datenschutzvorgaben zentral administriert. Zugriffsberechtigungen können im Bedarfsfall unmittelbar geändert oder entzogen werden.

Verantwortung für sicheren Fernzugriff

Datensicherheit ist ein Punkt, doch wer trägt die Verantwortung für einen sicheren Fernzugriff – ganz zu schweigen von Haftungsrisiken im Falle eines Cyberangriffs? Denn gerade zu Remote Services gibt es im Normenumfeld von Einbruch- und Überfallmeldeanlagen, Zutrittskontrolle, Videoüberwachungssystemen und Brandmeldeanlagen nur wenig rechtssichere Aussagen. Das soll sich ändern. In den neu entstehenden Normierungen – Fpr EN 50710 für Remote Services und prTS 50136-10 für Remote Access – wird dies klar geregelt. Normativ wird ein direkter Fernzugriff auf eine sicherheitstechnische Anlage über einen Standardrouter nicht mehr zulässig sein.

Neu definiert wurde die Rolle des „Remote Access Infrastructure Providers (RAISP)“. Dieser verantwortet künftig die IT-Sicherheit der Plattform und aller Komponenten sowie die ständige Verfügbarkeit der Verbindungen. Die TAS ist das erste Unternehmen in Deutschland, das auf Basis dieser entstehenden Normen nach VdS zertifiziert wurde.

Die im Hause entwickelte TAS Secure Platform wird nicht nur im eigenen Servicecenter genutzt, sondern auch Errichtern gegen monatliches Entgelt angeboten. Das ist wirtschaftlich interessant, denn Errichter müssen ihre IT-Infrastruktur nicht anpassen, keine Service-Arbeitsplätze für das Monitoring der Anlagen zur Verfügung stellen oder die Software auf dem neuesten Stand halten.

Einsatzbeispiel Plattformkopplung Brandmeldeanlagen

Ein Hersteller von Brandmeldeanlagen ermöglicht Errichtern den Fernzugriff auf seine Melder über die eigene Cloud. Für eine normkonforme Konnektivität koppelt die TAS beide Plattformen, indem sie die Verbindung über ihren Sicherheitsrouter

bis hin zur TAS Secure Platform zur Verfügung stellt.

Somit wird nicht nur ein sicherer Fernzugriff auf die Übertragungstechnik und die Brandmeldeanlagen für den zuständigen Errichter gewährleistet, auch die Monitoring Daten der Anlagen werden direkt an die Herstellerplattform weitergeleitet. Als Remote Access Infrastructure Provider verantwortet die TAS die Sicherheit und Verfügbarkeit der Verbindungen. ■

» Telefonbau Arthur Schwabe GmbH & Co. KG:
www.tas.de/home

SICHERHEITSEXPO in München

DIE STÄRKSTE ABWEHR
DEUTSCHLANDS
ON TOUR



**Echtzeit-Intervention
hautnah erleben!**

24.-25. November
an Stand E08



JETZT ANMELDEN!

Protection One
Alles sicher!