PROTECTOR

3|2021
März
49. Jahrgang

ASW Bundesverband –
Allianz für Sicherheit in der Wirtschaft e.V.

schlütersche
www.sicherheit.info

Kompliziert

Wie Notversorgung und Klimatechnik in Rechenzentren funktionieren | **24**

Effizient

Alles im Blick: Wie Besucher und Lieferanten gemanagt werden | **34**

Riskant

Szenario Erdbeben: Wie kann die Bevölkerung geschützt werden? | **54**

Sicherheit von Rechenzentren

Maximale Geschäftskontinuität durch physische Sicherheit von Siemens | **14**

Foto: Siemens

Foto: Getty Images/iStockphoto

Wer trägt bei einem Fernzugriff auf Alarmsysteme die Verantwortung für jederzeit verfügbare Verbindungen?

Alarmsteuerung aus der Ferne– ein Sicherheitsrisiko?

Eine kontinuierliche Überwachung und Fernwartung von Sicherheitsanlagen hat viele Vorteile. Doch wer trägt dabei die Verantwortung?

STEPHAN HOLZEM

Die Vorteile des Fernzugriffs auf Alarmsysteme liegen auf der Hand. Das Ausfallrisiko einer Anlage wird minimiert, Serviceeinsätze können effizienter gestaltet werden. Aber wer trägt bei einem Fernzugriff die Verantwortung für jederzeit verfügbare Verbindungen und einen hohen Sicherheitslevel, der vor Cyberangriffen schützt?

Plattform- oder cloudbasierte Dienste, die Kunden gegen monatliches Entgelt zur Verfügung stehen, finden sich zunehmend im Bereich der Sicherheitstechnik. Einsätze von Servicetechnikern vor Ort sollen auf das Notwendigste beschränkt bleiben – aus Gründen des Gesundheitsschutzes genauso wie auf Basis der Zielvorstellungen von Kunden: mehr Effizienz in den Prozessen, mehr Transparenz über die Leistungen.

„Der Fernzugriff auf sicherheitstechnische Anlagen ist bereits gängige Praxis."

Klar ist: Bereits heute bieten viele Unternehmen die Möglichkeit der Aufschaltung auf ihre Gewerke. Ob Einbruchmeldeanlagen, Video-

überwachung oder Zutrittskontrollsysteme, der Fernzugriff auf sicherheitstechnische Anlagen für Monitoring und Fernwartung ist gängige Praxis. Die Anforderungen, die sich hieraus ergeben, sind allerdings hoch.

Voraussetzungen für Fernzugriffe

- Die Vernetzung der Sicherheitsgewerke sollte abgebildet werden. Insellösungen – jeder bietet ein eigenes Portal für den Fernzugriff an – bergen die Gefahr der Intransparenz über Zugriffe und Zuständigkeiten sowohl für Errichter als auch Unternehmen.
- Die Sicherheit muss gewährleistet sein. Dabei geht es um mehr als sichere Verschlüsselungstechnologien und weitere Mechanismen zur Datensicherheit. Wichtig ist ein sicheres Gesamtkonzept, bei dem klar geregelt ist, wer die Verantwortung für welche Teile der Infrastruktur hat. Das ist alles andere als trivial.

Problem der Haftungsrisiken

Ein Beispiel: Bei einer Brandmeldeanlage in einer Schule oder einem öffentlichen Gebäude gibt es zurzeit allein drei Verantwortungsbereiche für den Fernzugriff:

1. Verantwortlich für eine sichere Alarmverbindung ist der „Anbieter für den Alarmübertragungsdienst“ – der „ATSP“.
2. Der Betrieb der Brandmeldeanlage liegt in der Verantwortung des zuständigen Errichters. Dieser muss bei einem Ausfall jederzeit auf die Anlage zugreifen können, um Fehlerzustände zu bewerten und einen Störeinsatz vor Ort durch den Fernzugriff effektiv vorzubereiten.
3. Und schließlich hat auch der Hersteller der Brandmeldeanlage immer öfter einen direkten Zugriff auf die Brandmeldeanlage, um den Errichtern der Anlagen verschiedene Dienstleistungen anzubieten. Dazu gehören sowohl Remote-Unterstützung, aber auch die Übermittlung von Echtzeit-Alarminformationen oder die zentrale Speicherung von Ereignissen.

„Mit den kommenden Normen 50136-10 für Remote Access und 50710 für Remote Services wird die Verantwortung für einen sicheren Fernzugriff auf sicherheitstechnische Anlagen zukünftig klar geregelt.“

Stephan Holzem, Geschäftsführer TAS Sicherheits- und Kommunikationstechnik

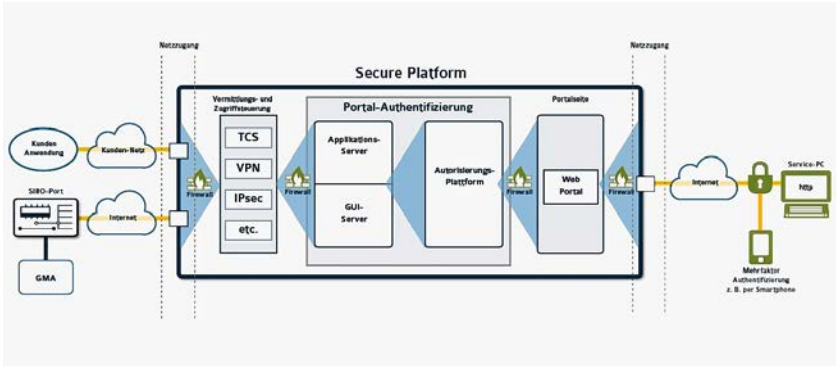
Installiert jeder der drei seinen eigenen Fernzugriff mit eigenen Routern, wird im Störfall oder bei einem Cyberangriff jeder die Verantwortung auf den Anderen abschieben. Denn bis dato ist der Fernzugriff ein relativ unklar geregelter Bereich – mit Haftungsrisiken für den Betreiber von sicherheitstechnischen Anlagen.

Wer verantwortet den Fernzugriff auf Alarmsysteme?

Das soll sich in Kürze ändern. Mit den zurzeit entstehenden Normen für Remote Access und Remote Services ist der Provider für die Fernzugriffs-Infrastruktur verantwortlich. Dieser sogenannte Remote Access Infrastructure Service Provider (RAISP) muss sich um sichere Verbindungen und Schutz gegen Cyberangriffe kümmern.

Das bundesweit tätige Unternehmen TAS Sicherheits- und Kommunikationstechnik stellt daher seinen Kunden, unter anderem Leitstellenbetreibern und Errichterfirmen, nicht nur die Infrastruktur für den Fernzugang zur Verfügung. Die TAS übernimmt die Verantwortung für den sicheren Fernzugriff über ihre „Secure Platform“. Im Gesamtkonzept enthalten ist auch eine Risikobewertung, die Berücksichtigung der geltenden Richtlinien für die sicherheitstechnischen Anlagen sowie die strikte Einhaltung der Datenschutz-Regeln. „Sicherheit als Service“ – oft zitiert, aber relativ unkonkret – wird hier greifbar. ■

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



Verschiedene Alarmsysteme können auf die TAS Secure Platform aufgeschaltet werden. Neben dieser Flexibilität bietet die Plattform ein Höchstmaß an Sicherheit für das Monitoring und die Fernwartung von Gefahrenmeldeanlagen.

Foto: Getty Images/Stockphoto