Sicherheits-Berater
Informationsdienst zur Sicherheit in Wirtschaft und Verwaltung

Security over IP – der Feind in meinem (Sicherheits-)Netz

01.12.2018

Die klassische Sicherheitstechnik verändert sich durch die Digitalisierung schon seit einiger Zeit fundamental – darüber waren sich alle Teilnehmer des 1. SIMEDIA Fachforums "Security over IP" (als Fortführung einer Seminarreihe zum selben Thema) am 24. und 25. Oktober 2018 in Frankfurt einig. In den Fachvorträgen zu Themen wie u. a. Digitalisierung der Sicherheitstechnik, Informationssicherheit nach dem Stand der Technik, Datenschutz im digitalen Zeitalter oder auch in Praxisberichten machten die Referenten u. a. der Siemens AG, der Berliner Verkehrsbetriebe, der Europäischen Zentralbank, der Jans Group oder auch der von zur Mühlen'sche GmbH die Entwicklungen wie auch die Herausforderungen der digitalen Technologie deutlich.

Im Rahmen eines IP-gestützten Sicherheitsmanagements werden (bzw. sind bereits) zunehmend Gewerke wie die Zutrittskontrolle, die Videoüberwachung oder die Einbruchmeldetechnik in Unternehmen in digitale und netzwerkgestützte Lösungen umgesetzt. Auf der einen Seite ergeben sich dadurch neue Möglichkeiten, wie in den Vorträgen eindrücklich gezeigt wurde: Die einzelnen Systeme lassen sich gut miteinander verknüpfen, es stehen dem Sicherheitsverantwortlichen viel mehr Funktionen zur Überwachung und Einsatzsteuerung zur Verfügung und sämtliche Gewerke sind, im besten Fall auch mit einer leicht bedienbaren Oberfläche, bequem in einer Sicherheitszentrale steuerbar. Jedoch wurde auch deutlich, dass es viele Stolpersteine auf dem Wege zu einem ganzheitlichen IP-basierten Sicherheitsmanagementsystem gibt, die oftmals unterschätzt werden.

So erscheint es z. B. immer wieder als eine Herausforderung, die IP-Fähigkeit der einzelnen Systeme herzustellen, da die Konverter nicht immer fähig sind, auf der Netzwerkstruktur zusammenzuarbeiten oder eine Harmonisierung von Port-Security und Meldern ist erst durch individuelle Einstellungen an der jeweiligen Firmware möglich. Zudem spielt auf einmal das Thema IT-Sicherheit eine Rolle: Der traditionelle Sicherheitstechniker, der sich früher mit Verkabelungen und Kreuzschienen herumgeschlagen hat, muss sich durch die Anbindung sämtlicher Gewerke an IP-Netze nun auch mit Fragen des erweiterten Datenschutzes, ausreichenden Redundanzen wie auch der IT-Sicherheit an sich beschäftigen – Begriffe wie Switch, Storage oder Client gehören damit zum sicherheitstechnischen Fachvokabular.

Durch die Netzwerkanbindung der Sicherheitstechnik lässt sich im Gegensatz zur analogen Welt erheblich schwerer bestimmen, wer die Kontrolle über ein beliebiges Gerät hat. Ein Einfalltor besteht potenziell damit überall dort, wo Systeme einen Netzzugang besitzen, wie sich in der Vergangenheit mehrfach gezeigt hat: So waren von der Schadsoftware Mirai 2016 mehr als eine Million IoT-Anwendungen, u. a. auch Überwachungskameras, als Teil eines Botnetzes mit einem Angriffsdurchsatz von 1,2 Terabit pro Sekunde betroffen und durch die Persirai-Schadsoftware konnten 2017 theoretisch über 120.000 Kameras weltweit für digitale Angriffe genutzt werden. Und damit sind auch die Kollegen der IT-Abteilung direkte Prozesspartner, wenn es um die physische Sicherheit des Unternehmens geht, was zu erheblichen Herausforderungen in der Praxis führen kann.

Die unterschiedlichen Erwartungen der einzelnen Stakeholder spielen u. a. in der Planung und Projektierung eine Rolle, wenn es z. B. um die Verfügbarkeit der Systeme geht: Während die IT teilweise nur zu den klassischen Arbeitszeiten greifbar ist, benötigt die Unternehmenssicherheit

Zugriff auf alle Systeme 24/7 – also auch bei Ausfall von Teilsystemen und einzelnen Geräten. Zudem verbirgt sich durch die enorme Vielzahl an unterschiedlichen Schnittstellen zwischen den einzelnen Systemen ein enormes Fehlerpotenzial. Und auch die notwendigen und teilweise zeitaufwendigen Updates der benutzten Software stellen den Sicherheitsverantwortlichen und das Sicherheitsmanagement immer wieder vor eine Herausforderung, denn neben dem zeitlichen Faktor kann es bei fehlender Inkompatibilität der einzelnen Systeme nach der Aktualisierung zu Problemen kommen.

Um ein IP-basiertes Sicherheitsmanagement zuverlässig betreiben zu können, helfen Normen, Zertifizierungen oder Standards wie die weltweit anerkannte ISO 27000-Reihe. Selbst wenn in vielen Unternehmen Spezialisten für diese Fragen verantwortlich sind, ist sicherlich eine Sensibilität wie auch ein Grundwissen zu Themen der IT-Sicherheit für den traditionellen Sicherheitstechniker relevant, um mit den zuständigen IT-Experten – ob intern oder auch mit externen Dienstleistern – auf Augenhöhe kommunizieren zu können.

Die Überführung der Sicherheitstechnik in ein ganzheitliches und ausreichend IT-gesichertes Sicherheitsmanagement wie auch der weitere Betrieb wird sicherlich eine der maßgeblichen Herausforderungen für die Unternehmenssicherheit in Zukunft sein – es gibt also genug Diskussionsbedarf für das nächste SIMEDIA Fachforum "Security over IP", welches nächstes Jahr wieder im Herbst stattfinden wird.

: : : Katja Rothe : : :

Ein Beitrag des Informationsdienstes

Sicherheits-Berater
TeMedia VerlagsGmbH

Kontakt:
Alte Heerstr. 1
53121 Bonn

Tel. +49 228 96293-80
Fax +49 228 96293-90
E-Mail: info@sicherheits-berater.de
Internet: www.sicherheits-berater.de
