Bilder: Gückel

Die Teilnehmer am ersten Tag des PROTECTOR & WIK Forums Zutrittskontrolle 2016: Stehend von links: Albrecht Kimmich, Thomas Maier, Axel Schmidt, Andreas Albrecht, Kester Peter Brands, Volker Kraiss, Frederik A. Hamburg, Robert Karolus, Jürgen Schneider, Thomas Christian. Sitzend von links: Dirk Nehr, Hartmut Beckmann, Armin Weinmann, Jochen Becker.

PROTECTOR & WIK Forum Zutrittskontrolle 2016

Einfachheit im Komplexen

Der Technologiewandel in der Zutrittskontrolle schreitet weiter voran. Die Technik setzt immer häufiger auf IT-Architektur auf und nutzt die Vorteile vernetzter Systeme. Damit einher gehen eine erhöhte Komplexität, veränderte Nutzeranforderungen und neue Bedrohungen. Wie man künftig funktionale und sichere System realisiert, diskutierten die Experten beim Forum Zutrittskontrolle 2016 von PROTECTOR & WIK.

Prozesse lautet das einleitende Stichwort von Moderator Volker Kraiss, der die anwesenden Experten auf ein neues Bild der Zutrittskontrolle einstimmte. „Zwar gilt nach wie vor: Die Zutrittskontrolle spielt sich in erster Linie an Türen ab. Die Türsteuerung mit all ihren funktionalen Abhängigkeiten muss verlässlich funktionieren. Aber Zutrittskontrolle ist längst nicht nur Türsteuerung. Zutrittskontrolle wird wesentlich von Prozessen des Kunden bestimmt. Wir sprechen schon längst nicht mehr nur über einzelne Komponenten oder isolierte Systeme. Bei der Konzeption und Planung von Zutrittskontrollsystemen ist der ganzheitliche Ansatz gefragt. Man muss das Große und Ganze in einem hochkomplexen IT-Umfeld im Blick haben“, fordert Kraiss und stößt damit durchaus auf Zustimmung bei den Teilnehmern.

Frederik Hamburg von der OSS Association vergleicht Systeme von damals und heute: „Früher konnte ein Tür-Controller wahrlich nicht viel, quasi nur Türen öffnen. Das konnte er aber dafür sehr schnell. Wenn man nun gewollt hätte, damit das Licht im dritten Stock anzuschalten, wäre das sehr schwierig geworden. Heute sieht es ganz anders aus, der Controller ist ein Windows- oder Linux-Rechner, der an die Wand geschraubt wird. Dafür kann man einfach andere Programme schreiben und dann funktioniert auch eine Lichtsteuerung problemlos. Für den Benutzer wird es dabei sogar einfacher in der Bedienung, wenn man es richtig anstellt.“

Integrative Wirkung

Hartmut Beckmann von Uhlmann & Zacher spürt die Wirkung einer zunehmenden Integration: „Der Wandel, den jeder in der Branche wahrnehmen kann, geht aus meiner Sicht in Richtung Integration von Zutrittskontrolle in Gesamtsysteme. Für uns bedeutet das auf Seiten der Produkte, dass wir vielleicht gar keine eigene Software mehr programmieren, sondern nur Schnittstellen und Integrationsmöglichkeiten bereitstellen.“

Jochen Becker von der Xccelo GmbH ergänzt: „Auch die IT-Infrastrukturen verändern sich grundlegend – Systeme werden verstärkt virtualisiert und in Cloud-basierten Konzepten betrieben. Wenngleich Systeme der Zutrittskontrolle erst Zug um Zug betroffen sein werden, so ist der Wandel doch zwangsläufig, und er wird auch Auswirkungen auf bestehende Systeme haben. Die Infrastrukturen, wie wir sie heute kennen, werden längerfristig nicht mehr in dieser Form existieren."

Robert Karolus von Interflex verweist ebenfalls auf einen Wandel in der Technik: „RFID galt lange Zeit als Standard. Heute wird gefordert, mit dem Smartphone eine Türe öffnen zu können. Gängige Leseverfahren funktionieren über Bluetooth und NFC. Wir haben dadurch ganz neue Möglichkeiten, die über die Basis-Funktion Tür auf/Tür zu hinausgehen. Hinter jeder Lösung stecken verschiedene Prozesse, die immer komplexer werden. Bei der Konzeption von Zutrittslösungen ist es daher unumgänglich prozessorientiert vorzugehen."

Frage der Perspektive

Damit wären einige Punkte des technischen Wandels bereits skizziert, jedoch gibt es verschiedene Perspektiven der Zutrittskontrolle. Ein wesentlicher Aspekt der Zutrittskontrolle ist die ganz praktische Funktionsweise am Zutrittspunkt, die sich eher wenig ändern dürfte. So glaubt auch Albrecht Kimmich von Kaba nicht, dass sich die grundsätzlichen Anforderungen an die Zutrittskontrolle wandeln: „Es wird sich am Durchtrittspunkt selbst nicht viel ändern, die Personen müssen dort hindurch, und das möchten sie möglichst schnell und unkompliziert. Aber der Prozess selbst, wie die Berechtigungen vergeben werden, oder wie man das Besuchermanagement regelt, dies alles ist mittlerweile komplex. Auch die Herausforderungen, was die Smartphones angeht, steigen – allein schon durch die Gewährleistung von Datensicherheit."

Ähnlich sieht es Axel Schmidt von Salto Systems: „Zutrittskontrolle wird Zutrittskontrolle bleiben, es geht immer darum, dass Personen durch bestimmte Türen möchten, und man prüft, ob sie dazu berechtigt sind. Diesen Prozess muss man immer abbilden, auch wenn er möglicherweise in Zukunft anders aussehen wird. Früher hatte auch niemand darüber nachgedacht, Offline-Komponenten einzusetzen oder Mobiltelefone einzubinden, mit denen man sich an der Tür ausweist. Mittlerweile arbeiten wir zudem mit Web-basierten Systemen, die deutliche Vorteile mit sich bringen."

Dass sich künftig Grundlegendes ändern wird, glaubt Armin Weinmann von Intrakey nicht: „Die Systemarchitektur in der Zutrittskontrolle, wenn wir von der physikalischen Architektur ausgehen, wird sich nicht groß ändern. Es wird immer ein Medium geben, es wird immer ein Endgerät an der Tür geben, ob es nun batteriebetrieben oder verdrahtet ist, und es wird immer eine übergeordnete Instanz geben, die verwaltet oder Berechtigungen prüft. Das hat sich bewährt, und hier sehe ich keine Trends in eine andere Richtung."

Intelligente Steuerzentralen

Das Konzept der Zutrittskontrolle scheint also gleich zu bleiben, die verwendete technische Grundlage wandelt sich aber, und auch die eingesetzten Komponenten verändern sich. Ein

„Es macht keinen Sinn, die Zeit bis zu den proprietären Systemen zurückzudrehen. Und es bringt auch nichts, sich der Realität zu verweigern. Unternehmen die kritische Infrastrukturen bereitstellen, müssen sich zunehmend gegen digitale Angriffe aus dem Cyber-Umfeld schützen. Durchgehende End-to-End – Verschlüsselung, starke Authentifizierung und zentrale Aktualisierung der Codierungsschlüssel sind wesentliche Sicherheitselemente, die man bei zukünftigen Dispositionen von Zutrittskontrolle beachten sollte“
Jürgen Schneider,
Nedap Technology Partner NTP for Security Management GmbH

„RFID galt lange Zeit als Standard. Heute wird gefordert, mit dem Smartphone eine Türe öffnen zu können. Gängige Leseverfahren funktionieren über Bluetooth und NFC. Wir haben dadurch ganz neue Möglichkeiten, die über die Basis-Funktion Tür auf/Tür zu hinausgehen. Hinter jeder Lösung stecken verschiedene Prozesse, die immer komplexer werden. Bei der Konzeption von Zutrittslösungen ist es daher unumgänglich prozessorientiert vorzugehen.“
Robert Karolus,
Produkt Manager, Interflex Datensysteme GmbH & Co.KG

„Die Sicherheit ist ein sehr wichtiges Thema, insbesondere wenn es um vernetzte IT-Systeme geht. Es betrifft jedoch nicht nur die Zutrittskontrolle. Man muss das gesamte IT-Netzwerk, sowie den Mobile-Bereich und das Internet of Things in die Betrachtung mit einbeziehen. Hier müssen wir alles tun, um Schwachstellen zu vermeiden. Das fängt bei den Leserprotokollen an, geht über die Applikationssoftware im Kundennetzwerk bis hin zu externen Cloud-Servern.“
Thomas Christian, Produktmanager Zutrittskontrollsysteme, Bosch Sicherheitssysteme GmbH

ganz wesentlicher Faktor ist heute jedoch auch die Software, die die Intelligenz von Systemen ausmachen kann. Frederik Hamburg findet, hier ist der Wandel am deutlichsten zu sehen: „Gerade die Software wird sich in Zukunft sicherlich stark wandeln. Sie wird immer komfortabler werden und noch mehr Integrationsmöglichkeiten bieten. Dabei muss man sich nicht mehr nur auf Zutrittskontrolle beschränken, sondern kann viele artverwandte Problematiken abdecken.“

Für Jürgen Schneider von Nedap NTP ist dabei die Handhabung ein entscheidender Faktor: „Der Anwender möchte immer einfacher mit Zutrittssystemen arbeiten können – das Thema Usability steht hier im Vordergrund. Anderseits nimmt auch die Komplexität der Anlagen zu, was für die Branche eine große Herausforderung bedeutet.“

Axel Schmidt fordert, die Komplexität nicht auf den Anwender abzuwälzen: „Für den Anwender darf es nicht schwieriger werden in der Bedienung. Vielmehr muss die Handhabung noch einfacher gemacht werden, gerade, wenn man mehrere Systeme zusammenbringt. Für den Hersteller hingegen wird es tatsächlich immer schwerer, weil die Systeme in sich aufwendiger werden. Alles von den Karten über die mobile Technik, bis hin zur Sicherheit in der Infrastruktur abzudecken, ist schon eine Herausforderung.“

Für Thomas Christian von Bosch Sicherheitssysteme ist die steigende Komplexität unausweichlich: „Zutrittskontrolle wird komplexer, weil diverse Integrationsmöglichkeiten in die Gesamtlösung des Kunden gefordert sind. Man muss Synergien nutzen und beispielsweise mit dem Zutrittsleser auch eine Einbruchmeldeanlage scharf und unscharf schalten oder man integriert ein Besuchermanagement oder Möglichkeiten zur Energiesteuerung. Zu den Anforderungen gehört auch, nur einen Ausweis für alle Applikationen im Gebäude zu verwenden.“

Gleiches gilt für die Software, meint Thomas Maier von SOAA: „Der Kunde möchte letzten Endes eine gemeinsame Oberfläche haben, in der er alle Systeme – mechanische und elektronische Schließanlagen – bedienen kann. Er möchte keinen doppelten Aufwand, sondern dass Daten optimal abgeglichen werden. Die Software muss seine Prozesse effektiv abbilden und dabei alle relevanten Teilgewerke umfassen.“

Offen für Angreifer

Die Verlagerung in Richtung IT sowie die große Bedeutung von Software und Schnittstellen bringt auch Gefahren mit sich, die man von einer isoliert arbeitenden Zutrittskontrolle auf proprietärer Basis so nicht kannte. Und so fragt auch Moderator Volker Kraiss in die Runde: „Das Angriffsverhalten der Cyber-Kriminellen wird immer ausgefeilter und komplexer. Wie geht man mit diesen vielfältigen Bedrohungen um? Welchen Stellenwert nehmen – bezogen auf die Zutrittskontrolle – Cybercrime und IT-Security ein?“

Jochen Becker sieht definitiv Bedrohungspotenzial: „Cyber-Crime ist ein Geschäftsmodell, bei dem man bedenken muss, was sich das organisierte Verbrechen davon verspricht, ein System zu hacken. Was ist also die Zielsetzung der Angriffe? Das Ziel muss nicht unbedingt sein, dass sich ein Angreifer beispielsweise Zutritt in sensible Bereiche einer Bank verschafft, sondern es kann auch darin liegen, dass Prozesse und Betriebsabläufe gestört und beeinträchtigt oder sogar eine Institution destabilisiert wird, was Aus-

wirkungen auf die wirtschaftliche Leistungsfähigkeit des betroffenen Unternehmens haben kann."

Axel Schmidt ergänzt: „Natürlich existiert heute viel Cyber-Crime. Und berechtigt ist auch die Frage, ob der Zutritt selbst das Ziel ist, oder ob das Stören der normalen Geschäftsprozesse beabsichtigt ist. Wenn man bei einem großen Industriebetrieb morgens die Anlage lahmlegt und plötzlich 20.000 Leute vor dem Werksgelände stehen, kann man sich vorstellen, welche Auswirkungen das hat."

Auch für Kester Brands von Tyco sind die Bedrohungen zu spüren: „Wir sind beispielsweise in den USA von unseren großen Kunden aufgefordert worden, an einem Cyber-Protection-Programm teilzunehmen, was dann auch weltweit ausgedehnt wird. Und das ist auch richtig so, denn: Wir werden mehr und mehr softwarelastiger und müssen hier entsprechend für Sicherheit sorgen. Es gilt, die Schotten in den Systemen dicht zu machen, so dass Angriffe schon an der Basis abgewehrt werden können."

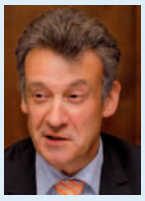
Jürgen Schneider stimmt zu: „Es zeigt sich, dass die Gefahr durch Cyber-Attacken heute schon real sein kann. Sofern die Zutrittskontrolle Bestandteil des Unternehmensnetzwerks ist, wird sie davon nicht ausgenommen. Wir müssen Zugangskontrolle und Zutrittskontrolle im Gesamtkontext der Unternehmenssicherheit betrachten."

Maßnahmen ergreifen

Die erste Herausforderung bei der Abwehr von Hackern, Spionen und anderen Angreifern ist es, potenzielle Schwächen zu erkennen. Dirk Nehr vom Fraunhofer Institut IPT hat sich als Anwender selbst schlau gemacht: „Wir haben uns in der Planungsphase lange mit dem Thema beschäftigt, welche Systeme bereits gehackt worden sind und welche nicht. Wir haben uns damals natürlich für ein sicheres System entschieden. Aber dieser Zustand wird nicht ewig anhalten, denn ich glaube, dass es möglich sein wird, auch dieses System irgendwann zu knacken. Man muss also Sicherheit als fortlaufenden Prozess begreifen, sein System regelmäßig überprüfen und auf die neuen Sicherheitsanforderungen hin anpassen und erweitern."

Ein wirksames Mittel ist es, das eigene System selbst anzugreifen oder testweise angreifen zu lassen, wie Frederik Hamburg weiß: „Wir führen tatsächlich Penetrationstests durch. Das traurige Ergebnis der Analyse ist, dass wir in allen Fällen, in denen wir beauftragt worden sind, hineingekommen

„Auch die IT-Infrastrukturen verändern sich grundlegend – Systeme werden verstärkt virtualisiert und in Cloud-basierten Konzepten betrieben. Wenngleich Systeme der Zutrittskontrolle erst Zug um Zug betroffen sein werden, so ist der Wandel doch zwangsläufig, und er wird auch Auswirkungen auf bestehende Systeme haben. Die Infrastrukturen, wie wir sie heute kennen, werden längerfristig nicht mehr in dieser Form existieren."
Jochen Becker,
Geschäftsführer, Xccelo GmbH



„Gerade die Software wird sich in Zukunft sicherlich stark wandeln. Sie wird immer komfortabler werden und noch mehr Integrationsmöglichkeiten bieten. Dabei muss man sich nicht mehr nur auf Zutrittskontrolle beschränken, sondern kann viele artverwandte Problematiken abdecken."
Frederik A. Hamburg,
OSS Association,
Geschäftsführer, Zugang GmbH

„Die Anforderungsprofile der Kunden werden heute natürlich durch die Consumer-Industrie und Cloud-Anwendungen beeinflusst. Man muss sich hier fragen, wie geht man damit um? Es wird immer wieder den Wunsch geben, gewisse Dinge mit einer App zu regeln."
Thomas Maier, Vorstand,
SOAA Standard für
Industrieapplikationen eG

„Zutrittskontrolle wird Zutrittskontrolle bleiben, es geht immer darum, dass Personen durch bestimmte Türen möchten, und man prüft, ob sie dazu berechtigt sind. Diesen Prozess muss man immer abbilden, auch wenn er möglicherweise in Zukunft anders aussehen wird."
Axel Schmidt, Geschäftsführer,
Salto Systems GmbH

sind. Jedoch immer durch das Ausnutzen organisatorischer Schwächen, denn es ist um ein Vielfaches aufwendiger, sich in ein System hineinzuhacken."

Robert Karolus ergänzt: „Gerade in Konzernen ist es zwischenzeitlich üblich, sogenannte Penetrationstests durchzuführen, das gilt auch für die Sicherheit der Software. Darauf legen Konzerne besonders viel Wert, da immer wieder Sicherheitslücken in Web-Applikationen gefunden werden. Wenn die Schwachstellen behoben werden, macht es den Angreifern das Leben schwer. Eine End-to-End-Verschlüsselung per AES oder SSL ist dabei absolut sinnvoll."

Dafür plädiert auch Thomas Christian: „Wir müssen unsere Zutrittskontrollsysteme durch Verschlüsselung der Daten von der Ausweiskarte bis in die übergeordnete Software sichern. Da wir uns jedoch vermehrt in Kunden-Netzwerken bewegen, wo nicht nur die Zutrittskontrolle einen Angriffspunkt darstellt, liegt es letztendlich in der Verantwortung des Kunden, sein gesamtes Netzwerk entsprechend abzusichern, da die potentiellen Angriffspunkte überall im IT-Netzwerk liegen können."

Cloud-basierte Zukunft

Dass alle an einem Strang ziehen müssen, wenn es um rundum sichere Lösungen geht, ist einleuchtend. Was den Umfang der Maßnahmen angeht, muss man heute allerdings berücksichtigen, dass das Netz des Kunden nicht unbedingt beim hauseigenen Server aufhört. Die Einbindung von Smartphones, Apps und Cloud-Diensten stellt Anwender vor weitere Herausforderungen.

Thomas Maier gibt zu bedenken: „Die Anforderungsprofile der Kunden werden heute natürlich durch die Consumer-Industrie und Cloud-Anwendungen beeinflusst. Man muss sich hier fragen, wie geht man damit um? Es wird immer wieder den Wunsch geben, gewisse Dinge mit einer App zu regeln. Und davon abgesehen, muss man sich nur die Entwicklung im SAP-Umfeld anschauen. Hier gibt es jedes Jahr bis

zu 100 Prozent Zuwachs bei den Cloud-Lösungen. Von daher wird es nicht mehr allzu lange dauern, bis die Kunden Cloud-basierten Zutritt fordern – und darauf sollten wir in der Anbieterstruktur vorbereitet sein. Cloud-basierende Lösungen haben den großen Vorteil, dass man bei auftretenden Sicherheitsrisiken – Cyberangriffen – sehr schnell reagieren kann."

Dirk Nehr ist offen für neue Lösungen: „Wenn man in Zukunft das Handy mit einbinden kann, um die Bürotür zu öffnen, dann ist das doch ein Fortschritt in Sachen Komfort. Wichtig ist aber, dass die Sicherheit nicht auf der Strecke bleibt."

Dass neue Lösungen in der Zutrittskontrolle Einzug halten werden, glaubt auch Jochen Becker: „Infrastructure as a Service und Software as a Service werden die Business-Modelle der nächsten zehn oder 20 Jahre sein. Damit einhergehen wird auch das Ende der proprietären Protokolle. Man wird universell innerhalb einer Cloud-Infrastruktur arbeiten, dort kann man keinen proprietären Ansatz mehr fahren, sondern nur funktional die Aufgaben voneinander abgrenzen."

Kester Brands ist verhalten optimistisch: „Software as a Service gab es als Ansatz vor mehr als zehn Jahren schon, und er hat sich damals in Deutschland und in Europa nicht so richtig durchgesetzt. Wir stehen aber durch die Cloud-Dienste jetzt vor einem Wandel auch in diese Richtung, und wir als Unternehmen müssen und werden ihn mitgehen. Wir docken sehr stark an die IT-Welt an und sollten auch was diese Business-Modelle angeht, vorbereitet sein. Letztendlich bestimmt der Endanwender, wie schnell es in diese Richtung geht." Der Wandel ist also vielfältig und betrifft nicht nur Technologie und Systemarchitektur, sondern auch die Nutzeranforderungen, die zunehmend von Einflüssen aus IT und Consumer-Sparte geprägt werden. Nun gilt es, sich zukunftsfähig aufzustellen, damit weder Sicherheit, noch Komfort, noch Geschäftsmodelle darunter leiden. MG

Artikel als PDF
www.sicherheit.info
Webcode: 1140496