WHITEPAPER

Digitalisierung und Cybersicherheit bei der Zutrittskontrolle

Eine Untersuchung der Systeme und Protokolle, mit denen Unternehmen das volle Potential der Zutrittskontrolle nutzen und eine intelligentere, sichere Welt schaffen können.

Juli 2021

AXIS COMMUNICATIONS

Inhalt

1 Zusammenfassung

Die Entwicklung der Cloud-Konnektivität verändert das Gesicht der physischen Sicherheitsbranche und zwingt die Installateure, sich anzupassen, um im Geschäft zu bleiben. Die Kontrolle der Zutrittssysteme scheint sich gerade in den Bereich der globalen Technologiefirmen zu verschieben. Das weckt Erwartungen eines höheren Mehrwerts der Systeme selbst, die immer intelligenter, besser skalierbar und Edge-basierter werden.

Diese Entwicklung bedeutet angesichts ihrer Möglichkeiten zur Integration in andere Unternehmenssysteme auch, dass die Cybersicherheit bei Entwicklung und Deployment eine noch wichtigere Rolle spielen muss, insbesondere, wenn man dabei auf einer bestehenden Infrastruktur aufbaut. Die Überwindung technischer Hindernisse wie einer seriellen Architektur, fehlenden MAC-Adressen usw. ist ein entscheidender Schritt beim Übergang zu digitalen Zutrittssystemen, die den Anforderungen von heute und morgen gewachsen sind.

Die Implementierung und Sicherung eines digitalen Systems für die Zutrittskontrolle bedeutet auch die Befolgung bewährter Verfahren, um die größtmögliche Sicherheit zu erzielen. Alle beteiligten Systemkomponenten müssen analysiert und getestet werden, egal ob Geräte, Lieferanten oder Protokolle. Sie alle müssen vertrauenswürdig und zuverlässig sein. Außerdem muss man immer die Bedrohungslandschaft im Blick behalten und wie man die Gefahren neu entdeckter Schwachstellen und Fehler eingrenzen kann.

Ganz besonderes Augenmerk sollten Sie den Lieferanten widmen, deren Geräte Sie in Ihr Netzwerk lassen. Ein seriöser Anbieter sollte seine eigenen Verfahren zur Sicherung seines Angebots bereitwillig offenlegen, beispielsweise durch Veröffentlichung eines Hardening Guides, durch Bereitstellung spezieller Verwaltungstools zur leichteren Verwaltung und Sicherung der Netzwerkgeräte usw. Außerdem sollte der Lieferant offen und ehrlich über seine Strategie zum Umgang mit erkannten Schwachstellen und Fehlern sprechen.

2 Einführung: Die Zukunft der Zutrittskontrolle

Die Cloud-Konnektivität hat der physischen Sicherheitsbranche spannende neue Einsatzzwecke und Installationsmöglichkeiten eröffnet. Endbenutzer und Käufer verlangen immer intelligentere, integrierte und besser auf ihr Unternehmen abgestimmte Lösungen mit Überwachungs- und Zutrittskontrollfunktionen, die weit über die Möglichkeiten herkömmlicher Technologien hinausgehen.

Viele Lieferanten haben ein starkes Geschäftsmodell rund um ihre Expertise, ihren Service und ihr Wissen über die physische Sicherheit aufgebaut. Die Netzwerk-Konnektivität und das IoT stellen sie jedoch vor ständig neue Herausforderungen, weshalb auch Anbieter und Installateure herkömmlicher physischer Sicherheitssysteme die Sprache der IT, offener Plattformen, IP-Konnektivität und Softwareintegration lernen müssen, um sich an veränderliche Marktbedingungen anpassen und dauerhaft im Markt bestehen zu können.

Es hat den Anschein, dass sich die Kontrolle schnell von den Anbietern elektronischer Zugangssysteme auf globale Technologieunternehmen verlagert, die nun die Macht haben, die Sicherheit in eine Richtung zu lenken, die ihre traditionelle Funktionsweise in Frage stellt. Intelligente Gebäude und Städte stellen große Chancen dar und viele sagen dem modernen Markt für Zutrittskontrolle ein schnelles Wachstum voraus, da die leichte Einrichtung und der Funktionsumfang der heutigen Technologien in der intelligenten Umgebung viele Vorteile bringen.

Wenig überraschend setzen viele auf gehostete Zutrittskontrolle, nachdem die Tech-Giganten die Vorteile von Cloud-Technologien aufgezeigt haben. Dies wurde während der COVID-19-Pandemie offensichtlich. Diese Unternehmen verfügen über die Größe, Reichweite und Ideen, um radikale Veränderungen

voranzutreiben. Und auch die physische Sicherheit wird sich verändern, wenn Unternehmen den Wert der Cloud zu schätzen lernen und nach gehosteten Lösungen für alle ihre sicherheitstechnischen und betrieblichen Anforderungen fragen.

Im Moment sind viele Hersteller aber noch nicht bereit für diesen schwierigen Markt. Ihre Geschäftsmodelle basieren weiterhin auf starren, proprietären Designs. Der Übergang zu intelligenten Lösungen für physische Sicherheit steht im direkten Gegensatz zu dieser herkömmlichen Herangehensweise, die wohl nicht mehr lange zeitgemäß sein wird. Der Wandel wird nicht über Nacht stattfinden und die neuen Cloud-Hosting-Lösungen müssen sich erst noch allgemein durchsetzen, aber diese Welt ist die Domäne der neuen Akteure, die gerade die Branche erobern.

In der Zukunft wird man deshalb von der Zutrittskontrolle und der physischen Sicherheit insgesamt mehr erwarten. Zutrittssysteme werden zu Datenerfassungsstellen, Tür-Steuerungen werden zu intelligenten Ein- und Ausgängen für Alarme. QR-Codes für die Besucherverwaltung und biometrische Gesichtserkennung für berührungslose Zutrittskontrolle werden immer häufiger in Form von Analysefunktionen direkt vor Ort in einer Kamera oder einem Sensor abgewickelt werden. Der Zutrittskontrolle steht eine spannende und herausfordernde Zukunft bevor, für alle, die sich darauf einlassen und sie mitgestalten möchten. Eine echte Innovationschance für eine intelligentere, sicherere Welt.

Dieser Artikel untersucht verschiedene Aspekte, die für die Zutrittskontrolle besonders wichtig sind, einschließlich vieler der grundlegenden Funktionen dieser Systeme. Außerdem werden Überlegungen über Best Practices für Lieferanten vorgestellt, mit Informationen und Vorschlägen für Endbenutzer, damit sie auf Augenhöhe mit ihrem Anbieter verhandeln und souveräne Kaufentscheidungen treffen können.

3 Herausforderungen und neue Entwicklungen im Markt der Zutrittskontrolle

Bei physischen Zutrittssystemen (PACS) geht es hauptsächlich um die Eingrenzung von Risikofaktoren durch das Gewähren bzw. Blockieren des physischen Zutritts. Somit ist beim Design eines Zutrittssystems ein ausgewogenes Konzept erforderlich, bei dem die möglichen Bedrohungen berücksichtigt werden müssen.

Da heute immer mehr Gebäude durch immer ausgefeiltere elektronische Lösungen für die Zutrittskontrolle geschützt werden, stellen diese Systeme eine schnelle und effiziente Lösung für die Verwaltung der Zutritte im gesamten Unternehmen dar. Sie hinterlassen eine digitale Spur, die überprüft und bei Bedarf überwacht werden kann. Außerdem sind sie vollständig in andere Systeme wie HR- und Besucherverwaltung integriert.

Diese Vereinheitlichung der Systeme liefert wertvolle Einblicke, die die betriebliche und sicherheitstechnische Entscheidungsfindung erleichtert und gleichzeitig den Zutritt steuert. Damit wird eine sorgfältige Auswertung des Systems auf seine Cyber-Reife unverzichtbar. Kriminelle werden immer raffinierter und die Bedrohungslandschaft entwickelt sich ständig weiter, so dass es nicht leicht ist, alle Gefahren durch geklonte Zugangsdaten, Bedrohungen von innen oder Cyberangriffe von außen zuverlässig abzuwehren.

Doch auch die Architektur selbst stellt ein Problem dar. Viele traditionelle Zutrittssysteme basieren auf einer veralteten Infrastruktur. Da konvergierende Sicherheitstechnologien häufig diese Infrastruktur nutzen, müssen die Anbieter erstens ihre Hardware so anpassen, dass sie mit diesen Unternehmensnetzwerken verbunden werden kann. Zweitens müssen sie wissen, wie wichtig die IT-Sicherheit ist und dass sich die Sicherheitslandschaft in ständigem Wandel befindet, was eine permanente Analyse erforderlich macht, um die vielen Gefahren für Unternehmen zuverlässig abzuwehren.

Überlegungen zur Cybersicherheit sollten bei der Entwicklung neuer Sicherheitssysteme im Mittelpunkt stehen. Technologien für die Zutrittskontrolle sind ein wesentlicher Bestandteil jeder physischen Sicherheitslösung und sollten daher nach anerkannten Grundsätzen der Cybersicherheit, der Meldung

von Vorfällen und bewährten Praktiken hergestellt werden. Man darf nie vergessen, dass die Integrität eins Systems nur so gut wie sein schwächstes Glied ist. **Ein System, dass dies nicht berücksichtigt,** ist potentiell gefährdet. Wenn es nicht in der Lage ist, anerkannte Wiederherstellungsmaßnahmen anzunehmen, zu melden und umzusetzen, kann es am Ende nicht für die notwendige physische Sicherheit sorgen, die seine eigentliche Aufgabe ist.

3.1 Zugangsdaten und Cybersicherheit (Cyber Maturity)

Die immer stärkere Beteiligung der IT-Branche beginnt die Art zu verändern, wie Technologien bewertet, installiert und gewartet werden. Eine wichtige Überlegung für IT-Stakeholder ist die Auswertung derZugangsdaten eines Unternehmens im Hinblick auf die Cybersicherheit, mit besonderer Beachtung der entsprechenden Kenntnisse der Anbieter. Dieses Wissen wird auch als Cyber Maturity bezeichnet. Dies bezeichnet ein gutes Verständnis der Bedrohungslandschaft und wie die Risiken eingegrenzt werden können. Die umfangreiche Dokumentation und Anleitungen zur Cybersicherheit, die bereits für IP-Kameras erstellt wurden, können auch auf die physische Zutrittskontrolle angewendet werden, denn die Herausforderungen, Beurteilungen und Erklärungen von Cyber-Risiken und möglichen Angriffen gelten in gleichem Maße auch für diese Produkte.

3.2 Die Zukunft der Sicherheitssystemarchitektur

Moderne Geräte für die Zutrittskontrolle werden über Netzwerkkabel und RJ45-Stecker angeschlossen. Netzwerke versorgen die Zutrittskontrolle mit Strom und ermöglichen die Kommunikation zwischen den Geräten und den zentralen Verwaltungssystemen. Der Übergang zu TCP/IP-basierten Systemen ist die treibende Kraft für die Weiterentwicklung der Zutrittskontrolle. Seit der Einführung der ersten wirklich IP-fähigen Tür-Steuerungen (AXIS A1001) 2013 hat sich PACS stetig weiterentwickelt. Heute bietet es eine Vielzahl fortschrittlicher Funktionen, die allein mit der herkömmlichen Technologie niemals möglich gewesen wären.

Beispiele für diese Innovationen sind QR-Code-Leser für die berührungslose Zutrittskontrolle, Gesichtserkennung durch die Integration von IP-Kameras oder Autokennzeichen-Lesegeräte. Sie alle interagieren mit PACS-Datenbanken und treffen selbst die Entscheidung über die Gewährung oder Verweigerung des Zutritts. Wichtige Vorteile von IP-Systemen sind ihre geringen Installationskosten bei einfacher Konfiguration und Geräteverwaltung. Ihre problemlose Integration mit anderen Geräten schafft eine zukunftsfähige Lösung, die eine einfache Plug-and-Play-Konnektivität neuer Sicherheitstechnologien und -verbesserungen sofort bei Verfügbarkeit ermöglicht.

3.3 IP im Vergleich zur herkömmlichen Zutrittskontrolle

Neue, moderne Lösungen für die Zutrittskontrolle nutzen die Vorteile von IP, insbesondere bei kontaktlosen Systemen, die der Endbenutzer heute als selbstverständlich voraussetzt. Die Benutzer dürften außerdem erwarten, dass die Zutrittskontrolle mit Smartphones und Tablets kompatibel ist, nicht nur im Hinblick auf mobile Zugangsdaten. Wie wird die Branche bessere, nützlichere sowie zeit- und kostensparendere Zutrittssysteme entwickeln? Und wird sie mit den von den großen Technologieunternehmen vorangetriebenen Innovationszyklen mithalten können? Dies sind die Herausforderungen für die Lieferanten.

Bis jetzt wurden die neuen Chancen noch nicht genutzt, möglicherweise weil die bisherigen Zutrittssysteme auf Tür-Steuerungen basieren, die in einer seriellen Architektur installiert und über RS-485-Kabel mit einer zentralen Einheit oder einem Server verbunden sind. Die meisten Systeme sind außerdem proprietär. Die Tür-Steuerung ist also „gesperrt" und kann nur von einer vom Lieferanten bestimmten Software verwaltet werden. Das schränkt den Endbenutzer auf einen einzelnen Hardware- und Software-Lieferanten ein.

Aufgrund ihrer Komplexität müssen diese Systeme zudem oft von Experten installiert und konfiguriert werden.

Die Erweiterung traditioneller Zugangssysteme wird dadurch erschwert, dass man dabei üblicherweise eine zentrale Steuerung für eine bestimmte Anzahl von Türen anlegt. Nicht dem Standard entsprechende Konfigurationen sind wegen der eingeschränkten Systemflexibilität oft mit hohen Kosten verbunden. Eine einzige zusätzliche Tür kann eine Systemerweiterung so sehr verteuern, dass sie wirtschaftlich nicht mehr vertretbar ist.

IP-Netzwerke ermöglichen die Einführung einer viel einfacheren, installationsfreundlicheren PACS-Architektur, die deutlich flexibler und viel leichter anpassbar ist. IT-Profis bevorzugen echte IP-Geräte in netzwerkbasierten Zutrittssystemen. Diese Profis müssen unbedingt in den Designprozess für die Zukunft einbezogen werden, denn sie sind es, die dafür sorgen werden, dass diese IP-Geräte tatsächlich eingesetzt werden. Diese wiederum sind der Schlüssel für Kostensenkungen bei Erweiterungen, was eine Voraussetzung für zukünftige Designs für die Zutrittskontrolle sein wird.

3.4 Offene Protokolle

Für die Zukunft der Zutrittskontrolle müssen die Hersteller bereit sein, ihre Fertigkeiten und Möglichkeiten in einem offenen Protokollforum zu teilen. Viele Entwickler von Zutrittssystemen sind, wie es scheint, zu dieser Offenheit nicht bereit. Sie möchten die Endbenutzer lieber auf ihre eigenen Lösungen festlegen, um sich zukünftige Einnahmen zu sichern. Diese Strategie bietet allerdings keinen langfristigen Nutzen. Die Benutzer verlangen mehr von ihren Lösungen, und dafür sind sie gerne bereit, ihre Daten zu teilen.

Systemdesigner und Anbieter von Zugangshardware verfügen nur selten über die Ressourcen oder das IT-Fachwissen, um alle von den Benutzern im Rahmen einer umfassenden physischen Sicherheitslösung geforderten Lösungen anbieten zu können. Viele scheinen nicht zu erkennen, dass ihre Angebote schnell von innovativen neuen Lösungen verdrängt werden, die sowohl ihr Geschäftsmodell als auch ihr Ansehen im Markt für Zutrittskontrolle gefährden. Die neuesten Systeme bieten so hochentwickelte Funktionen und die Entwicklung ist so rasant, dass eine Zutrittskontrolle bald völlig unnötig sein könnte, verdrängt von intelligenten E/A-Einheiten.

Wenn sie dem gegenüber offen sind, können die Hersteller passende Geräte sogar für kleine Zugangssysteme entwickeln, die möglichst einfach sein und zu wettbewerbsfähigen Kauf- und Installationskosten angeboten werden müssen. Dieselben Geräte können dann bei Bedarf an größere, technisch komplexere Anlagen angepasst werden. Diese Flexibilität zeichnet moderne Sicherheit aus. Sie sorgt dafür, dass ein heute gekauftes System in Zukunft relevant bleibt, auch wenn das Unternehmen des Kunden wächst und sich seine Anforderungen ändern.

Weitere Informationen zur Offenheit und offenen Technologien finden Sie auf der Website von ONFIV unter *www.onvif.org*. Diese Branchenvereinigung versucht, die Entwicklung hin zu offenen Standards zu lenken.

4 Technische Hindernisse für die Annahme

Bei den technischen Verbindungen, Schnittstellen und Geräten, die eine digitale Zutrittskontrolle ermöglichen, ist viel zu beachten. Der Wechsel von traditionellen zu Cloud-basierten Systemen bleibt mitunter nicht ohne Folgen. In den folgenden Abschnitten werden die Punkte behandelt, die bei der Unterstützung bestehender Technologien zu beachten sind, sowie die zugehörigen Prozesse, damit diese nicht zu einem Hindernis für Upgrades oder Wechsel zu neuen Lösungen werden.

4.1 RS-485-Steuerung

Eine Überlegung ist die Nutzung der RS-485-Steuerung und die mögliche Gefahr der Installation halbintelligenter Geräte, die meist keine MAC-Adresse (MAC=Media Access Control) haben, wodurch sie nur schwer zu identifizieren sind. RS-485, auch als TIA-485(-A) oder EIA-485 bekannt, ist ein Standard zur Festlegung der elektrischen Merkmale von Treibern und Empfängern in seriellen Kommunikationssystemen. Die elektrischen Signale sind gleichmäßig und Multipoint-Systeme werden unterstützt. Doch RS-485 bestimmt nur die physische Schicht: den Generator und den Empfänger. Es regelt nicht die entscheidende Kommunikationsschicht.

Das Fehlen einer MAC-Adresse oder eine serielle Architektur an sich bedeutet nicht grundsätzlich Probleme mit der Zuverlässigkeit oder dem Betrieb eines Zutrittssystems, denn diese Designs bilden schließlich seit über 30 Jahren die Grundpfeiler der Zutrittskontrolle. Höhere Sicherheitsfunktionen lassen sich aber nur schwer visualisieren, wenn nicht jedes einzelne Steuergerät in einem Zutrittssystem intelligent ist und einzeln angesteuert werden kann. Wir sind überzeugt, dass nur vollständig intelligente Systeme und vollständig zugängliche Geräte in Zukunft den erwarteten Mehrwert bieten können. „Vollständig zugänglich" bedeutet dabei aber nicht, dass die Cybersicherheit der Geräte eingeschränkt wäre – ganz im Gegenteil.

4.1.1 Open Supervised Device Protocol (OSDP)

Ein neues Kommunikationsverfahren, akzeptiert von der IEC und mit dem Potential zur Verbesserung der Kommunikation bei der Zutrittskontrolle, ist das Open Supervised Device Protocol (OSDP). Dieser Kommunikationsstandard für die Zutrittskontrolle wurde von der Security Industry Association (SIA) weiter verbessert, um die Interoperabilität zwischen den Produkten für Zutrittskontrolle und Sicherheit zu verbessern. OSDP nutzt eine 128-Bit-Verschlüsselung, unterstützt Multidrop-Installationen und überwacht Verbindungen, um Probleme bei den Lesegeräten zu melden. Ein weiterer wichtiger Punkt ist, dass OSDP für die Funktionen Kartenleser, Türöffner und Alarmkontakte lediglich 2 Kabel benötigt, während früher mehrere Anschlüsse pro Tür erforderlich waren. Laut SIA-Website wurde OSDP von der International Electrotechnical Commission (IEC) im Mai 2020 als internationaler Standard anerkannt und im Juli 2020 als IEC 60839-11-5 veröffentlicht. SIA OSDP wird ständig verbessert, um seine branchenführende Position zu erhalten.

4.2 Der Wert von Geräten mit MAC-Adresse

Die MAC-Adresse ist die weltweit eindeutige Hardware-Adresse eines Netzwerkadapters oder -Geräts. Im Hinblick auf IT-Netzwerke ist die MAC-Adresse genauso wichtig wie eine IP-Adresse. MAC-Adressen identifizieren eindeutig einen Computer im LAN, und sind für Netzwerkprotokolle wie TCP/IP unbedingt erforderlich. Die MAC-Adresse ist fest in das Gerät integriert. Zwar kann über das Betriebssystem die Adresse scheinbar verändert werden (Spoofing), aber dies ist natürlich nicht ratsam. Die Adresse sollte von Ihrer Sicherheitslösung geschützt werden.

TCP/IP und andere Mainstream-Netzwerkarchitekturen arbeiten normalerweise mit einem OSI-Modell (Open Systems Interconnection), bei dem die Netzwerkfunktion in mehrere Ebenen eingeteilt ist. MAC-Adressen funktionieren auf der Data-Link-Schicht (Schicht 2 im OSI-Modell) und erlauben Computern, sich eindeutig in einem Netzwerk zu identifizieren. Das Filtern nach MAC-Adressen bringt eine zusätzliche Ebene der Sicherheit. Bevor ein Gerät einem Netzwerk beitreten darf, vergleicht der Router die MAC-Adresse des Gerätes mit einer Liste genehmigter Adressen. Steht die Adresse des Clients auf der Liste des Routers, wird ihr der Zugang gewährt, andernfalls verweigert.

4.2.1 Power over Ethernet (PoE)

PoE bietet anwendungsübergreifend zwei große Vorteile: Kosteneinsparungen und Flexibilität bei der Aufstellung der Geräte. PoE nutzt dasselbe Kabel für Stromversorgung und Datenübertragung. Dadurch kann die Gerätearchitektur im Vergleich zu herkömmlichen Designs vereinfacht werden. Viele Zutrittssysteme werben mit einer IP-Anbindung.

5 Wodurch kennzeichnen sich Best Practices?

Die Verwaltung der Zutrittskontrolle ist eine wichtige Komponente bei der effektiven Abwicklung von Personenströmen und Zugangsbeschränkungen. Es ist zu wenig, wenn Unternehmen einfach nur Türen verriegeln oder Absperrungen aufstellen. Sie benötigen mehr Steuerungsoptionen, um ihren Kunden einen besseren Service bieten und jederzeit einen hohen Grad an Sicherheit gewährleisten zu können. Best Practices für eine umfassende Zutrittskontrolle umfassen viel mehr als nur die Auswahl der passenden Werkzeuge. Vielmehr muss die entsprechende Architektur vorhanden sein, es müssen hochwertige Technologien eingesetzt, die richtigen Verfahren und Protokolle beachtet und die Mitarbeiter und alle Beteiligten zur richtigen Einstellung und den richtigen Verhaltensweisen ermutigt werden.

5.1 Die Verantwortlichen und das konvergente Sicherheitskonzept

So wie wir eine in derselben Infrastruktur konvergierende Technologielandschaft erleben, die eine reibungslose Funktion der für diese Standorte erforderlichen Betriebstechnologien sicherstellen soll, benötigen wir auch einen konvergenten Entscheidungsfindungsprozess. Wir haben bereits erfolgreiche Beispiele dafür gesehen, wie ein konvergentes Sicherheitskonzept Strukturen aufgebrochen und verschiedenen Geschäftsteams zur besseren Zusammenarbeit verholfen hat. Diese Konvergenz ist heute, da klassische elektronische und physische Sicherheitsangebote in Unternehmensnetzwerken nebeneinander existieren, wichtiger denn je.

Sicherheitsteams müssen sich auf Technologien verlassen können, die ihre operativen Anforderungen unterstützen. So können sie den damit verbundenen Risiken begegnen und gleichzeitig IT-Sicherheitsrichtlinien unterstützen und sicherstellen, dass physische Geräte keine Hintertür in das Unternehmensnetzwerk öffnen. Wenn alle Beteiligten zusammenarbeiten, ist es möglich, eine sichere Cyber- und physische Umgebung zu schaffen.

5.2 Was von Partnern, Anbietern und Lieferanten zu erwarten ist

Drittparteien müssen unbedingt wissen, wie wichtig es ist, dass sie bei all ihren Handlungen Best Practices in Bezug auf Sicherheit befolgen und dass sie gezielt an der Erfüllung spezifischer Bedürfnisse arbeiten. Beziehungen zu Dritten sind der Schlüssel dafür, eine gesunde Lieferkette aufzubauen und eine starke und vertrauensvolle Bindung herzustellen.

Wichtige Überlegungen bei der Bewertung Dritter und ihres Einflusses auf die Lieferkette: Verständnis und Berücksichtigung der Risiken im Hinblick auf Cybersicherheit > Ausgereifte Strategie für Cybersicherheit mit entsprechenden Prozessen und Tools > Kenntnis der Auswirkungen von Richtlinien und Gesetzen auf das Angebot eines Herstellers > Nachweis, wie das Unternehmen die Compliance-Anforderungen des Benutzers erfüllen kann > Cybersicherheit ist ein Prozess, nicht nur eine Technologie. Die Unternehmen müssen ein Lebenszyklus-Management für Cybersicherheit nachweisen können, das den Schutz des Kundenunternehmens sicherstellt.

5.3 Sicherheitsmanagement: Steuerung und Lieferantenprozesse

Wie bei allen wirkungsvollen Sicherheitsmaßnahmen geht es auch bei der Cybersicherheit darum, dass nicht nur oberflächliche Schutzmechanismen zum Einsatz kommen. Es geht darum, das IP-Kameranetzwerk auf jeder Ebene angemessen zu schützen: von den ausgewählten Produkten und Partnern bis hin zu den festgesetzten Anforderungen.

5.3.1 Standards und Richtlinien

ISO 27001 – Das Sicherheitsverwaltungssystem Information Security Management ISO/IEC 27001 verlangt Folgendes:

- die systematische Untersuchung der Informationssicherheitsrisiken einer Organisation unter Berücksichtigung von Bedrohungen, Schwachstellen und Auswirkungen
- die Planung und Implementierung einer kohärenten und umfassenden Reihe von Informationssicherheitskontrollen bzw. sonstiger Formen des Risikomanagements (wie Risikovermeidung oder -transfer), um für inakzeptabel gehaltene Risiken auszuräumen
- die Einführung eines allgemeinen Managementprozesses, damit Informationssicherheitskontrollen weiterhin durchgängig den Informationssicherheitsbedürfnissen der Organisation entsprechen.

5.3.2 Cyber Essentials Plus

Cyber Essentials ist ein staatlich gefördertes und von der Industrie unterstütztes Programm, das Organisationen hilft, sich vor gängigen Online-Bedrohungen zu schützen. Das Programm wertet die Richtlinien und Verfahren von Unternehmen aus und ist ein wirksamer Indikator dafür, ob Unternehmen die Herausforderungen der Cybersicherheit verstanden haben. Dabei geht es insbesondere um:

- Sichere Konfigurationen
- Zugriffskontrolle und -verwaltung
- Schutz vor Malware
- Management von Sicherheitspatches
- Firewall und Internet Gateways

Für Technologiehersteller sollte die erste Verteidigungslinie in der Minderung der Risiken in Verbindung mit ihren eigenen Systemen bestehen. Seit dem 1. Oktober 2014 verlangt die britische Regierung von allen Bietern bei Ausschreibungen, die bestimmte sensible und personenbezogene Daten betreffen, die Zertifizierung nach dem Programm Cyber Essentials.

5.3.3 Secure by Design, Secure by Default

Das 2019 vom Surveillance Camera Commissioner des britischen Innenministeriums eingeführte Programm **Secure by Design, Secure by Default** legt Mindestanforderungen für die Hersteller von Sicherheitskamerasystemen und -komponenten fest. Das Programm fordert von den Herstellern einen ganzheitlichen Ansatz zur Lösung zugrundeliegender Sicherheitsprobleme, anstatt nur Symptome zu beheben. Handeln in großem Maßstab soll den Gesamtschaden an einem System oder Komponententyp möglichst minimieren.

„Secure by Design, Secure by Default" bezieht sich auf die langfristigen technischen Bemühungen, die richtigen Sicherheitsprimitive in Software und Hardware einzubauen. Es bezieht sich auch auf die ebenso

anspruchsvolle Aufgabe, dafür zu sorgen, dass diese Primitive so verfügbar und nutzbar sind, dass sie der Markt ohne Weiteres einführen kann.

Zur Unterstützung unserer Technologien hat Axis „Secure by Design, Secure by Default" an den Verhaltenskodex der National Cybersecurity Strategy angeglichen:

- Kennwortabfrage
- Anzeige der Kennwortstärke
- HTTPS-Verschlüsselung
- 802.1x
- Fernzugriff DEAKTIVIERT (NAT-Überschreitung)

6 Leitlinien und Tools (Lieferantenprozesse)

Um ihr Netzwerk zu sichern, werden oft mehrere technische Kontrollen angewendet, um eine „mehrstufige Verteidigungslinie" zu schaffen und einzelne Ausfallpunkte und Anfälligkeiten möglichst auszuräumen. Ein wichtiger Prozess, der dabei allerdings oft übersehen wird, ist die Systemhärtung (engl. „System Hardening"). Dies bezeichnet Konfigurationsänderungen an Standardeinstellungen des Systems, um es besser vor Bedrohungen der Informationssicherheit zu schützen. Gleichzeitig hilft dieser Prozess, die Menge an inhärenten Schwachstellen zu minimieren.

6.1 Manufacturing Hardening Guide

Ein Systemhärtungsverfahren sollte für alle mit einem Netzwerk verbundenen Geräte eingeführt sein. Dazu gehören Workstations, Server und andere Netzwerkgeräte. Da jeder Hersteller Setup und Konfiguration seines eigenen Systems am besten kennt, sollte er Partnern und Benutzern die nötigen Daten liefern, um die Integrität ihrer Geräte und der Anlage des Endanwenders zu schützen. Ein Härtungsleitfaden sollte technischen Rat für jeden enthalten, der an der Einführung von Videoüberwachungslösungen beteiligt ist. Es sollte eine Baseline-Konfiguration festsetzen und umfassende Informationen zum Umgang mit der veränderlichen Bedrohungslandschaft enthalten.

Alle Lieferanten sollten bei Design, Entwicklung und Test von Geräten Best Practices im Bereich der Cybersecurity beachten, um das Risiko von Schwachstellen zu minimieren, die bei einem Angriff ausgenutzt werden könnten. Allerdings setzt die Absicherung eines Netzwerks, seiner Geräte und der unterstützten Dienste die aktive Beteiligung der gesamten Lieferkette sowie der Endanwenderorganisation voraus. Eine sichere Umgebung hängt von ihren Nutzern, den Prozessen und der Technologie ab. Ein guter Härtungsleitfaden sollte Baseline-Anwendungsfälle wie CIS Controls Version 6.1 berücksichtigen. Diese Kontrollen waren früher als SANS Top 20 Critical Security Controls bekannt.

6.2 Geräteverwaltung

Ein Gerätemanager ist ein Werkzeug, das verknüpfte Geräte vor Ort auf einfache, kostengünstige und sichere Weise verwaltet. Dieses stellt für Installateure und Systemadministratoren ein hoch effizientes Tool zur Wahrnehmung aller wichtigen Aufgaben in den Bereichen Installation, Sicherheit und Wartung dar.

Gerätebestands-/Asset-Management-System:

- Konto- und Kennwortrichtlinie

- Effiziente Installation von Firmware-Upgrades und Anwendungen
- Cyber-Sicherheitskontrollen anwenden – HTTPS verwalten und IEEE 802.1x-Zertifikate hochladen, Konten und Passwörter verwalten
- Zertifikat Lebenszyklusverwaltung – Alle wichtigen Installations-, Sicherheits- und operativen Aufgaben verwalten
- Schnelle und einfache Konfiguration neuer Geräte – Einstellungen für Sichern und Wiederherstellen
- Für Standorte jeder Größe geeignet – Installationen an einem oder mehreren Standorten

6.3 Herausforderungen in Verbindung mit OEM / ODM

Erstausrüster (OEM, Original Equipment Manufacturers) sind Hersteller, die das Produkt eines anderen Unternehmens unter eigenem Namen und eigener Marke weiterverkaufen. Ein Original Design Manufacturer (ODM) ist ein Unternehmen, das von anderen Unternehmen in Auftrag gegebene, jedoch zum Teil selbst entwickelte Produkte herstellt, die letztlich unter dem Markennamen des Auftraggebers verkauft werden. Diese Unternehmen erlauben es dem Markenunternehmen, in die Produktion einzusteigen, ohne eigene Fabriken bauen oder betreiben zu müssen.

Vieles spricht dafür, dass sich ein Hersteller bemüht, ein Produkt über OEM oder ODM von einem anderen Anbieter zu beziehen. Zunächst entfallen auf diese Weise alle Fertigungsrisiken und -kosten, und das Unternehmen kann sich auf Verkauf und Marketing konzentrieren. Das ist einer der Hauptgründe dafür, dass viele Kamerahersteller in der Sicherheitsbranche OEM oder ODM mit ihren Markenprodukten beauftragen. Berichten zufolge verkaufen tatsächlich 96 Lieferanten OEM- oder ODM-Kameras, die von einem anderen Anbieter hergestellt wurden.

Das bringt verschiedene Schwierigkeiten mit sich, nicht zuletzt im Hinblick auf die Cybersicherheit. Schwachstellen in den Produkten eines Herstellers werden dadurch an alle Wiederverkäufer und Partner in der gesamten Lieferkette weitergereicht. Es kann außerdem die umfassende Sichtbarkeit der Lieferkette stark erschweren. Angesichts der großen Zahl zwischengeschalteter OEMs und ODMs könnte auch ein Endanwender, der die Angebote sorgfältig geprüft hat und die Technik eines bestimmten Herstellers ablehnt, diese am Ende unwissentlich unter anderem Namen trotzdem nutzen.

6.4 CPU Mikroprozessor-Chip

In Geräten eingebaute, generische CPU-Verarbeitungschips wurden bereits Ziel von Hackerangriffen, da sie viele Schwachstellen aufweisen. Einer der Hauptgründe dafür ist die Skalierbarkeit, die aus einer einzigen identifizierten Schwachstelle generiert wird. Jüngere Beispiele sind die Sicherheitslücken „Meltdown" und „Spectre", zwei zusammenhängende Side Channel Attacks gegen moderne CPU-Mikroprozessoren, bei denen über unzulässige Codes unberechtigterweise auf Daten zugegriffen werden konnte.

Die meisten Geräte - von Smartphones bis zur Hardware in Rechenzentren - können in gewissem Umfang anfällig sein. Die großen Betriebssystemanbieter haben Patches entwickelt, die die Probleme abschwächen, auch wenn einige Teile der Patches über den Ausrüstungshersteller (OEM) installiert werden müssen, da sie plattformspezifische Elemente umfassen. Das National Cybersecurity Centre (NCSC) rät, diese Patches schnellstmöglich in den Geräten zu installieren.

6.5 Firmware-Strategie

Signierte Firmware ist wichtig für Endanwender und mindert einige der potenziellen Risiken für Geräte, die im Logistik- und/oder Vertriebsprozess manipuliert wurden. Die Signatur, manchmal „Hash" genannt, wird bei der Verteilung auf der Firmware angebracht. Ein Prozessor berechnet seinen eigenen Hashwert und lädt nur Firmware-Images mit dem Hash-Wert eines signierten Zertifikats, dem es vertraut.

6.6 Schwachstellen-Management

Die ständige Zunahme der Internetkriminalität und der damit verbundenen Risiken zwingt viele Organisationen, der Informationssicherheit mehr Aufmerksamkeit zu widmen. Schwachstellen-Management sollte Teil der Anstrengungen jeder Organisation um die Beherrschung von Informationssicherheitsrisiken sein. Dieses gibt einer Organisation einen ständigen Überblick über Schwachstellen in ihrer IT-Umgebung und die damit verbundenen Risiken. Nur die Identifizierung und Behebung von Schwachstellen in der IT-Umgebung kann Angreifer daran hindern, in die Netzwerke einer Organisation einzudringen und Daten zu stehlen.

Die Lieferanten müssen unbedingt Schwachstellen in ihren Betrieben ausräumen und beispielsweise Verfahren anwenden, die Schwachstellen in allen Systemen erfassen und beheben sowie verhindern, dass bei Änderungen und der Einführung neuer Systeme neue Schwachstellen eingeführt werden. Alle Probleme in Verbindung mit Risiken, die ein Lieferant eingeht, müssen dem Endbenutzer mitgeteilt und mit ihm abgestimmt werden. Andernfalls könnten Angreifer Schwachstellen in den Systemen für Cyberangriffe gegen ein Unternehmen und seine Lieferanten ausnutzen.

IT-Sicherheitspatches und Updates für Sicherheitslücken müssen rechtzeitig in einem genehmigten Prozess installiert werden, um Sicherheitsverstöße zu vermeiden. Bei Lieferantensystemen, die aus irgendeinem Grund nicht aktualisiert werden können, müssen Maßnahmen zum Schutz des anfälligen Systems ergriffen werden. Alle Änderungen müssen im Einklang mit dem Änderungsmanagementprozess des Lieferanten durchgeführt werden.

6.7 Sicherheitsbenachrichtigungen

Sicherheitsberater helfen, die Risiken durch bekannte Schwachstellen einzugrenzen. Der Sicherheitsberater kann auf offizielle Schwachstellenberichte wie CVE (Common Vulnerability and Exposure) verweisen, die eine Beschreibung der Schwachstellen, eine Risikoeinschätzung, Empfehlungen und Informationen über den Verfügbarkeitszeitpunkt eines Service-Release enthalten. Die meisten Lieferanten arbeiten nach einem indirekten Vertriebsmodell und haben ein Partnerprogramm eingeführt.

Mit Benachrichtigungen über Sicherheitshinweise können Kunden, die nicht in einem Partnerprogramm eines Herstellers registriert sind frühestmöglich und bei Kommunikation an den Kanal relevante Cybersicherheitsinformationen erhalten. Das ist ein wesentliches Tool für Endanwender, bei denen Ausrüstung installiert ist, die jedoch keinen Ansprechpartner im Unternehmen haben, der die Installation ursprünglich durchgeführt hat.

6.8 Building Security in Maturity Model (BSIMM)

Das BSIMM ist ein Bewertungsrahmen für Softwaresicherheit, mit dem Organisationen ihre Softwaresicherheit mit anderen Initiativen vergleichen und herausfinden können, wo sie stehen. BSIMM hilft wie folgt, Prozesse, Aktivitäten, Rollen und Verantwortlichkeiten zu beurteilen:

- Design- und Architekturprüfungen

- Codeprüfungen
- Tests auf bekannte Sicherheitslücken
- Ausführung eines Tools zum Scannen auf Standard-Sicherheitslücken, das CVE-Schwachstellen in Open-Source-Programmen finden kann

6.9 Long Term Support (LTS)

Long Term Support (LTS) ist eine Produktlebenszyklus-Verwaltungsrichtlinie, bei der eine stabile Softwareversion über einen längeren Zeitraum als in der Standardversion verwaltet wird. Long Term Support Firmware sollte nur Patches für Stabilität, Performance und Sicherheit umfassen. Die Anbieter stellen bis zu 10 Jahre nach Markteinführung eines Geräts LTS Firmware bereit.

Es wird erwartet, dass LTS parallel, aber unabhängig von bestehender aktiver Softwareunterstützung laufen wird. Einer der Hauptvorteile von LTS-Unterstützung liegt darin, dass sie die Integration mit Dritten in Verbindung mit der ursprünglichen Firmware-Version beibehält.

6.10 Wissensvermittlung und Kooperation

Einer der Schlüsselbereiche, der bei der Auswahl eines Technologieanbieters berücksichtigt werden sollte, sind die Fortbildung und der Support, den er anbietet. Da sich die Herausforderungen, mit denen sich Channel und Industrie insbesondere im Hinblick auf die Cybersicherheit konfrontiert sehen, ständig wandeln, sollten die Hersteller das Thema nach Möglichkeit proaktiv angehen und dem Markt Sicherheiten und Inhalte bieten. Mögliche Beispiele sind:

- Kostenlose Präsenzkurse zur Cybersicherheit
- Online-Schulungen zur Cybersicherheit
- Online-Schnelltest zur Cybersicherheit
- Hardening Guide
- Schwachstellenstrategien
- Best Practices für Cybersicherheit
- Konzepte und Terminologie der Cybersicherheit

7 Erstellen eines Cyber-Hygieneprofils: nächste Schritte und Überlegungen

Gute Cyberhygiene umfasst die Identifizierung, Priorisierung und Reaktion auf Risiken für die entscheidenden Services und Produkte einer Organisation. Best Practices für Cyber-Hygiene helfen, Datensicherheitsverletzungen und falsche Systemkonfigurationen zu verhindern und die zugehörigen Risiken für das Unternehmen zu minimieren. Außerdem müssen sich die Beteiligten auf die wichtigsten Bedrohungen einigen und das Risikomanagement auf die hauptsächlichen Ziele ausrichten.

Die folgenden Überlegungen sind keine umfassende Aufstellung, aber sie können die effiziente Abwehr von Cyber-Bedrohungen unterstützen.

7.1 Lieferanten

Überprüfung der Registrierungen und Zertifizierungen

Überprüfen Sie entsprechende Registrierungen und Zertifizierungen. Lassen Sie sich z. B. Bescheinigungen über eine ISO9000-Registrierung und andere Qualitätszertifizierungen vorlegen. Überprüfen Sie, ob die Produkte des Lieferanten für den Einsatz in einem Unternehmensnetzwerk konzipiert sind.

Achten Sie auf Nachweise für Best Practices

Achten Sie darauf, dass der ausgewählte Anbieter Best Practices bei der Cybersicherheit nachweisen kann. Er sollte einen Cyber-Härtungsleitfaden vorlegen können, der Cyber- und physische Sicherheitsmaßnahmen und Best Practices zum Schutz des Netzwerks beschreibt.

Prüfen Sie Ihren Anbieter

Prüfen Sie sorgfältig, bevor Sie eine Kaufzusage machen. Überprüfen Sie, ob die Geschäftsbedingungen klar und transparent sind. Aus finanzieller Sicht sollte gefragt werden, was mit dem Produkt und Support passieren würde, wenn das Unternehmen in Schwierigkeit geraten sollte.

Sichern Sie Ressourcen für laufenden Support

Überprüfen Sie, ob Ihr Anbieter über die nötigen Ressourcen verfügt, um auch in Zukunft die Lösungen zu entwickeln, die Sie Ihrer Einschätzung nach benötigen werden. Überprüfen Sie, ob Ihr Anbieter die nötige Größe, Reichweite und Fähigkeiten hat, um Ihre betrieblichen Anforderungen auch in Zukunft zu unterstützen.

Definieren Sie Ihre zukünftigen betrieblichen Anforderungen

Konzentrieren Sie sich auf Ihre zukünftigen Anforderungen. Intelligente Geräte und Lösungen können die Erweiterung eines Unternehmens unterstützen und es zukunftssicher machen. Sie sollten also das Gefühl haben, dass Ihr Lieferant Ihre Erwartungen erfüllen oder übertreffen wird, und er sollte Wartungsverträge und laufenden Support anbieten.

Lassen Sie sich Nachweise für ethische Geschäftspraktiken zeigen

Überprüfen Sie auf Nachweise für ethische und nachhaltige Praktiken. Eine Partnerschaft, die auf Vertrauen und gemeinsamen Zielen aufbaut, ist eine solide Grundlage für langfristigen Erfolg. Kann der Anbieter Umweltmanagement-Systeme, ein CSR-Programm (soziale Unternehmensverantwortung) oder eine ethische Beschaffungsrichtlinie vorweisen?

7.2 Produkte und Systeme

Sorgfältige Prüfung

Führen Sie eine technische Due-Diligence-Prüfung des Systems und seiner Kernelemente durch, um sicherzugehen, dass keine grundlegenden Faktoren vorliegen, die den laufenden Betrieb beeinträchtigen könnten. Achten Sie darauf, dass klare Informationen zur Risikoeinschätzung und -minderung vorliegen.

Überprüfen Sie den Wartungsvertrag

Überprüfen Sie den Inhalt des Vertrags, beispielsweise ob der Service- und Wartungsvertrag Software-Updates und Firmware-Upgrades des Herstellers umfasst.

Sichern Sie die angeschlossenen Geräte

Vertrauen Sie auf Ihr per Netzwerk angeschlossenes physisches Sicherheitssystem. Sicherheitssysteme sollten mit dem Ziel der Cybersicherheit eingerichtet werden: Ändern Sie Standard-Benutzernamen und -Passwörter, installieren Sie die neueste Firmware, nutzen Sie Verschlüsselung (idealerweise HTTPS) und deaktivieren Sie den Remote-Zugriff.

Fordern Sie eine Erklärung über Design-Sicherheit an

Ihr Lieferant sollte in der Lage sein, eine Erklärung zur Konstruktionssicherheit als Nachweis für den Cybersicherheitsstatus aller mit dem Netz verbundenen Geräte vorzulegen.

Beurteilen Sie die Intelligenz des Systems

Die angeschlossenen Geräte sind vollständig intelligent, wenn sie mit einer MAC-Adresse vernetzt sind und einen festen Bestandteil der Systemarchitektur bilden. Geräte ohne MAC-Adresse sind nicht intelligent und können nicht einzeln identifiziert, verwaltet oder geschützt werden.

Überprüfen Sie die Einhaltung der DSGVO / des Bundesdatenschutzgesetzes

Die DSGVO trat 2018 zusammen mit der aktuellen Fassung des Bundesdatenschutzgesetzes in Kraft. Achten Sie darauf, dass die Produkte und Systeme entsprechend des Bundesdatenschutzgesetzes und der DSGVO ausgelegt sind.

T10168631/DE/M1.7/2107

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Sprechanlagen und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen zu Axis bietet Ihnen unsere Webseite *axis.com*.