Whitepaper

Cybersicherheit: die größte Herausforderung für den Einzelhandel

Das Organisieren der Cybersecurity und des Life Cycle Managements für IoT Geräte sind entscheidend für das operative Geschäft des Einzelhändlers und den Aufbau einer langfristigen Vertrauensbasis zum Kunden.

Co-Autoren:
Graham Swallow, Leiter Einzelhandelssegment, Nordeuropa, Axis Communications
Steven Kenny, Industry Liaison Architecture and Engineering, Axis Communications

AXIS COMMUNICATIONS

Table of contents

1. Einführung

Es liegt in der Natur der Sache, dass Einzelhändler, bei denen regelmäßig Waren und Geld den Besitzer wechseln, zum Ziel krimineller Handlungen werden. Lokalzeitungen berichten von Läden, die von Gelegenheitstätern bestohlen werden. Perfekt eingespielte, bestens organisierte Banden, die es auf bestimmte Einzelhändler und hochwertige Waren abgesehen haben, stellen eine zusätzliche Herausforderung für Sicherheitsdienstleister dar. Allerdings endet heute die Bedrohung für Einzelhändler nicht bei physischen Straftaten, sie setzt sich in der digital vernetzten Welt fort. Die Kriminalität im Online-Einzelhandel stellt eine wachsende Herausforderung dar. Es ist keine Überraschung, dass der Einzelhandel als die Branche gilt, die am stärksten durch Cyberbedrohungen gefährdet ist[1].

Kundendaten sind für Cyberkriminelle eine attraktive Handelsware. In den letzten 12 Monaten wurden 19 schwerwiegende Datenschutzverletzungen gemeldet[2]. Aus einem von der Cybersicherheitsfirma Sharp Security[3] veröffentlichten Bericht geht hervor, dass durchschnittlich 80-90 % des Login-Datenverkehrs eines Online-Händlers auf „Credential Stuffing"-Attacken entfallen, denn Angreifer nutzen die Bemühungen der Einzelhändler um eine reibungslose Kauferfahrung aus. Das ist der höchste Prozentsatz in allen Sektoren, die für den Bericht untersucht wurden.

Datenschutzverletzungen sind eine echte Gefahr sowohl für Unternehmen als auch Kunden, denn sie können das Vertrauen schädigen, das Verbraucher in Marken haben. Außerdem können bei Nichteinhaltung der DSGVO potenzielle Strafen von 20 Mio. EUR oder 4 % des globalen Umsatzes gegen den Einzelhändler verhängt werden, je nach dem, welcher Wert höher ist. Nach einer Studie der KPMG haben 19 % der Verbraucher erklärt, sie würden im Falle eines Verstoßes nicht mehr bei einem Einzelhändler einkaufen, und 33 % sagten, sie würden für einen längeren Zeitraum nicht mehr dort kaufen[4].

Dieses Whitepaper soll ein Bewusstsein für die Herausforderungen schaffen, die zu bewältigen sind, und dafür, wie die Verhaltensweisen und der Aufbau der Lieferkette eines Einzelhändlers das Risiko oder die Gefährdung reduzieren können. Hacker werden den Weg des geringsten Widerstands gehen und sich auf Bereiche fokussieren, die die wertvollsten Daten enthalten; daher sollte man sich vor Augen halten, dass der IT-Lieferant jedes Einzelhändlers Ziel des Cyberkriminellen sein könnte, in der alleinigen Absicht, seine Technologien zu nutzen, um über eine Hintertür auf das Vermögen des Einzelhändlers zugreifen zu können.

[1] *The 2018 SecurityScorecard Retail Cybersecurity Report (www.verdict.co.uk/retail-cyber-attacks)*

[2] *https://store.businessinsider.com/products/the-data-breaches-report*

[3] *http://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Credential_Spill_Report_2018.pdf*

[4] *www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1*

2. Herausforderungen bei der Cybersicherheit für Einzelhändler

Der IT-Chef eines Unternehmens mit Verantwortung für die gesamte IT-Sicherheit erklärte auf der Retail Business Technology Expo, dass Manager für den Schutz vor Warenschutz bzw. für die Gewinnsicherung verantwortlich sind und jeder seinen Teil zum Unternehmensergebnis und damit zum Aktiengewinn beitragen kann, indem die Cybersicherheit mit hoher Priorität behandelt wird. Um die Bedeutung von Cybersicherheit zu unterstreichen, hat das Weltwirtschaftsforum einen Bericht[5] veröffentlicht, der aussagt, dass Investoren der Cybersicherheit Priorität zuordnen müssen oder Gefahr laufen, Geld zu verlieren. Zu den Überlegungen im Gesamtbericht gehören Folgende:

> Cyberattacken führen zu steigender Nachfrage nach sicheren digitalen Produkten
> Investoren haben eine Verantwortung und die Chance, Unternehmen zur Priorisierung von Cybersicherheit zu motivieren
> Cyber Due Diligence stärkt das Vertrauen der Kunden, schützt die Erträge der Investoren und schafft einen sicheren digitalen Markt für alle

Betriebsausfälle
Ein Ausfall der Infrastruktur, ausgelöst durch einen DDoS-Angriff (Distributed Denial of Service) kann zu Betriebsausfällen führen. Da die meisten Einzelhändler eine Omni-Channel-Strategie verfolgen, nehmen Gefährdung und die Interaktion zwischen Kunde und Einzelhändler auf digitaler Ebene zu. Die Funktionsfähigkeit eines Unternehmens hängt stark von der Konnektivität der entwickelten Technologien ab, und so können Betriebsausfälle durch Hackerangriffe das Unternehmen erhebliche Summen kosten.

Nach einer Studie des Ponemon Institute[6] liegen die geschätzten Durchschnittskosten einer Minute Betriebsausfall aufgrund eines DDoS-Angriffs bei ca. 20.000 Euro; die durchschnittliche Ausfallzeit pro DDoS-Angriff beträgt 54 Minuten. Zwar wirken sich viele verschiedene Faktoren auf diese Zahlen aus; der potenzielle Einfluss weiterer Aspekte wie beispielsweise Reputationsverlust, Kundenabgang und Rechtskosten muss jedoch auch berücksichtigt werden und ist unter Umständen noch schwerer zu messen.

Folgende Aspekte wirken sich auf Betriebsausfälle aus und sollten berücksichtigt werden:

> Funktionsfähige Websites als Schnittstelle zum Kunden
> Funktionsfähige Backend-Systeme
> Gewährleistung der Verfügbarkeit von POS-Systemen
> Schutz von IoT-Vermögenswerten
> Die interne Bedrohung

Die Sicherheit von Kundendaten kann auch durch Mitarbeiter des eigenen Unternehmens bedroht sein, wenn diese versuchen, Daten zu stehlen. Unternehmen sollten eine klare Risikostrategie formulieren sowie für einen angemessenen und methodischen Umgang mit diesen Risiken sorgen, beispielsweise durch das Erstellen von Referenzen der eigenen Beschäftigten.

Darüber hinaus wurde im Zusammenhang mit zunehmender Cyberkriminalität gegenüber Einzelhändlern von Bitsight.com[7] berichtet, dass vier neue Cybersicherheitsbedrohungen für den Einzelhandel zunehmen, nämlich Erstattungsbetrug, Geschenkkartenbetrug, Angriffe auf Lieferketten und IoT-Schwachstellen. Dieser Bericht nimmt nachstehend Bezug auf die beiden letzteren.

Angriffe auf Lieferketten
Vom Werk bis zur Tür des Kunden haben technologische Verbesserungen der Einzelhandelslieferkette den Einkaufsprozess schneller und komfortabler werden lassen. Allerdings lässt die wachsende Verknüpfung zwischen einem Einzelhändler und seinen vielen Lieferanten und Kunden auch das Risiko einer Datenschutzverletzung wachsen.

---

[5] *www3.weforum.org/docs/WEF_Incentivizing_responsible_and_secure_innovation.pdf*

[6] *www.corero.com/resources/files/analyst-reports/CNS_Report_Ponemon_Jan13.pdf*

[7] *www.bitsight.com/blog/4-emerging-retail-cybersecurity-threats*

Angriffe auf die Daten eines Unternehmens, über den Umweg von Geschäftspartnern, gibt es schon lange. Zwei der größten Datenschutzverletzungen in der Geschichte des Einzelhandels, Target und Home Depot, waren das Ergebnis von Angriffen über Dritte[8]. Neben der drohenden Datenschutzverletzung müssen sich Einzelhändler auch um größere Geschäftsausfälle durch Lieferausfälle sorgen. Wenn ein einzelnes Versand- oder Transportunternehmen gehackt wird, kann dies der Logistik insbesondere in der Haupteinkaufssaison starke Kopfschmerzen verursachen.

EY veröffentlichte kürzlich den Cybersicherheitsbericht "Is cybersecurity about more than protection? (EY Global Information Security Survey 2018–19), in dem immer häufiger die Schwachstellen in Verbindung mit Partnerunternehmen zu suchen sind. Nur 15 % aller Unternehmen haben Schritte zum Schutz gegen Bedrohungen unternommen, die über Dritte entstehen, 36 % sind sich durch Selbstbewertungen (22 %) oder unabhängige Bewertungen (14 %) der Risiken bewusst. Das bedeutet, dass für 64 % das Thema nicht präsent ist, obwohl sie den Schaden zu verantworten haben.

Um sich vor Angriffen auf ihre Lieferkette zu schützen, müssen sich Einzelhändler ein präzises, kontinuierliches Bild von der Leistungsfähigkeit ihrer Geschäftspartner im Bereich Cybersicherheit verschaffen.

IoT-Schwachstellen

Das Internet der Dinge (IoT) ist im Begriff, eine nächsten großen Innovationen für Einzelhändler zu werden. Viele Unternehmen beginnen bereits damit, IoT-Geräte für die Warenverfolgung, zur prädiktiven Ausrüstungswartung, Kundenstromanalyse und für viele weitere Aufgaben einzusetzen, die sich nun ohne weiteres automatisieren und mit dieser Technologie effizient wahrnehmen lassen.

Allerdings stellen alle diese neu vernetzten Geräte mögliche Einstiegspunkte für Cyberkriminelle dar. Während die Cybersicherheitsbranche und Aufsichtsbehörden sich bemühen, mit der starken Zunahme von IoT-Geräten Schritt zu halten, müssen Einzelhändler die Kosten und Vorteile, die mit einer Führungsrolle beim Einsatz vernetzter Geräte verbunden sind, gegeneinander abwägen.

Neuerdings gibt es Beispiele dafür, das IoT-Geräte zum Ziel hochkarätiger Attacken werden. Das Mirai Botnet[9] nutzte unsicher konfigurierte IoT-Geräte, um nach geöffneten Telnet-Ports zu suchen und sich nach Möglichkeit mit Standard-Passwörtern einzuloggen. Es konnte rasch eine ‚Botnet-Armee' zusammenstellen, eine Reihe von DDoS-Angriffen entwickeln und bei zahlreichen Einzelhändlern und Online-Seiten Betriebsausfälle herbeiführen.

Die BBC berichtete über ein ähnliches Ereignis, das 2016 stattfand. Mirai #14[10] kaperte insgeheim eine riesige Zahl handelsüblicher Videoüberwachungskameras. Die Hacker fanden heraus, dass die Kameras und weitere, ähnliche Geräte eine Sicherheitslücke aufwiesen, die ausgenutzt wurde, um die Kontrolle verschiedener Systeme zu übernehmen und so eine vernetzte ‚Cyber-Armee' für den Angriff auf ein identifiziertes Ziel aufzustellen. Dieser Zwischenfall wurde für vermeidbar erachtet, war jedoch aufgrund unzureichender Sicherheitsmaßnahmen innerhalb der Kameras aufgetreten. Das zeigt die Bedeutung von Akkreditierungen wie beispielsweise der Selbstzertifizierung „Secure by Default", die der UK Surveillance Camera Commissioner 2019 freigegeben hat.

Während sich diese IoT-Beispiele auf Schwachstellen beziehen, die überall im Internet exponiert sind und zur Waffe umfunktioniert werden, um einen DDoS zu entwickeln, gibt es Beispiele dafür, wie andere IoT-Geräte mit direkter Auswirkung auf den Benutzer gehackt werden und zum Verlust von Kundendaten führen. Auf die High-Roller-Datenbank eines Kasinos wurde angeblich über die Sicherheitslücke eines Aquarium-Thermostats zugegriffen. Es wird berichtet, dass die Angreifer diese Schwachstelle ausnutzten, um sich Zugriff auf das Netzwerk zu verschaffen.

---

[8] *www.bitsight.com/blog/4-emerging-retail-cybersecurity-threats*

[9] *www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html*

[10] *www.bbc.co.uk/news/uk-46840461*

Bei Informationssicherheitsspezialisten ist es durchaus bekannt, dass sich Hersteller vorwiegend auf Leistung und Nutzbarkeit von IoT-Geräten konzentrieren, jedoch Sicherheitsmaßnahmen und Verschlüsselungsmechanismen außer Acht lassen, was zur routinemäßigen Hackerangriffen führt. Genau deshalb ist Supply Chain Diligence so wichtig.

Lücken in der Sicherheitstechnologie

Ein Benutzer ist potenziell gefährdet durch die Unternehmen, mit denen er zusammenarbeitet, und die Technologien, die diese in ihrem Wirkungskreis einsetzen. Ein hohes Sicherheitsniveau aller installierten Technologien ist zwingend erforderlich, um Personen, Vermögenswerte und die Marke zu schützen. Es wäre katastrophal, wenn die Sicherheitssysteme und -unternehmen, in die investiert wurde, um das Geschäft zu schützen, Ursache eines Cybersicherheitsverstoßes mit anschließendem Datenverlust, Geldstrafe und Schädigung der Marke würden.

Umso wichtiger ist es, dass Einzelhändler sichere Technologien einsetzen, um ihre Vermögenswerte zu schützen. Darüber hinaus sollten sie eine gründliche Beurteilung der Lieferketten von Unternehmen durchführen, die den Auftrag haben, einen sicheren Standort für Mitarbeiter und Kunden zu gewährleisten und dabei das Ansehen der Marke und das Geschäftsvermögen zu schützen.

3. DSGVO / DPA 2018: Datenschutz und Privatsphäre

Der Schlüssel liegt darin, die Balance zwischen einer Verbesserung der Kundenerfahrung und einer angemessenen Sicherheit vor Ort zu finden, ohne die Privatsphäre des Kunden zu verletzen. Die Risiken, hinsichtlich der Einhaltung der Datenschutz-Grundverordnung (DSGVO) sowie unzureichender Cybersicherheit zu leichtfertig zu agieren, werden aktuell vielfach in der Presse erörtert. Sowohl British Airways[11] als auch die Marriott Hotels[12] machten Schlagzeilen, nachdem Bußgelder wegen des Verlusts von Kundendaten gegen sie verhängt worden waren. Das ICO kam zu dem Schluss, dass Marriott bei der Übernahme von Starwood keine ausreichende Due-Diligence-Prüfung vorgenommen hatte und mehr hätte tun müssen, um die Sicherheit seiner IT-Systeme zu gewährleisten.

Eine Unternehmensstrategie zur Umsetzung von Cybersicherheitsmaßnahmen wird also immer wichtiger - denn damit lassen sich Geldbußen in Folge von Cyberattacken minimieren. Nach EU-Recht können Regulierungsbehörden jetzt Strafen in Höhe von 20 Mio. EUR oder 4 % des globalen Konzernumsatzes einer Firma verhängen, je nach dem, welcher Wert höher ist.

Die Durchsetzung der DSGVO und des Data Protection Act 2018 bedeutet, dass alle EU-Unternehmen, die personenbezogene Daten von Einwohnern der EU - auch wenn sie keine EU-Staatsbürger sind - erheben, speichern oder anderweitig verarbeiten, dies unter Einhaltung der gesetzlichen Vorgaben tun müssen. Einzelhändler müssen nun immer genauer auf die Erhebung und Speicherung von Kundendaten achten. Während Videoüberwachungssysteme in der Einzelhandelsumgebung eine Notwendigkeit sind, haben möglicherweise viele ihre gesamte Strategie neu bewertet, um für die umfassende Einhaltung von DSGVO und DPA 2018 zu sorgen.

Aspekte der DSGVO: Welche Arten von Daten werden erhoben?

Die Analyseanwendungen von Axis für den Einzelhandel erheben Daten in numerischer Form und speichern beispielsweise die Anzahl der Personen, die in einem definierten Zeitraum einen Laden/Standort betreten/verlassen. Keine der Anwendungen speichert Videodaten, die sich im Standardbetriebsmodus zur Identifizierung von Menschen verwenden lassen. Deshalb stellen die gespeicherten Daten keine personenbezogenen Daten dar. Nach der Erhebung werden die Daten dem Benutzer in Form eines bedienerfreundlichen Dashboards präsentiert, in dem relevante Kennzahlen, Diagramme und Statistiken angezeigt werden.

[11] *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/*

[12] *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/*

Aspekte, die bei der Untersuchung einer Videoüberwachungsstrategie für Sicherheit und Schadensverhütung zu berücksichtigen sind:

- **Artikel 13 & 14** – Die Informationspflicht. Videoüberwachungskameras erfassen Bilder, mit denen sich Personen identifizieren lassen, was bedeutet, dass diese Bilder unter die Definition personenbezogener Daten (PII) gemäß der DSGVO fallen. Ein geeignetes Leitsystem muss vorgesehen sein, um über den Betrieb der Videoüberwachung, den Grund dafür und den Ansprechpartner zu informieren, falls ein Auskunftsbegehren eingeht.
- **Artikel 15** – Auskunftsrecht der betroffenen Person. Es gab zwar immer die Möglichkeit, Videomaterial über die eigene Person anzufordern (Auskunftsbegehren der betroffenen Person), aber sie war kostenpflichtig. Da dies nun kostenlos ist, ist die Anzahl der Begehren, die umgesetzt werden müssen, gestiegen. Auch wenn bei einem Begehren eine angemessene Datenmenge benötigt wird, ist der Verantwortliche verpflichtet, dem Begehren nachzukommen und dabei mit einer exportierbaren Schwärzungslösung die Identitäten anderer betroffener Personen in der Szene zu schützen. Eine Frage, die gestellt werden muss, ist die, ob dieses Begehren ein einfacher Prozess ist, der sich zeitnah und ohne übermäßige Kosten durchführen lässt. Oder ob die aktuelle Lösung bedeutet, dass diesem Begehren nicht ohne die Notwendigkeit nachgekommen werden kann, einen Dritten zu beauftragen. Gleichzeitig ist es außerdem wesentlich, die Integrität und Sicherheit des exportierten Videomaterials zu schützen; exportiertes Material muss als passwortgeschützte Datei bereitgestellt werden, um die Empfehlung des ICO einzuhalten.
- **Artikel 25** - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen - Verantwortliche und Datenverarbeiter müssen technische und organisatorische Maßnahmen ergreifen, um die Datenschutzgrundsätze wirksam umzusetzen. Das ist auch im Verhaltenskodex des Surveillance Camera Commissioner's (SCC), ‚Secure by Design, Secure by Default', aufgegriffen, in dem die wichtigsten Kriterien aufgelistet sind, die Kamerahersteller erfüllen müssen.
- **Artikel 30** – Verzeichnis von Verarbeitungstätigkeiten. Um die gesetzliche Vorgabe in Artikel 30, EU-DSGVO „Verzeichnis von Verarbeitungstätigkeiten" zu erfüllen, muss das Videoverwaltungssystem/DVR/NVR usw. ein Aufzeichnungsprotokoll liefern, das transparent macht, wie das System eingesetzt wurde. Es wird empfohlen, das Videoverwaltungssystem privilegbasiert zu konfigurieren, so dass spezielle Funktionen basierend auf Genehmigungsebenen aktiviert und deaktiviert werden. Beim Live-Video-Streaming werden Start und Stopp aufgezeichnet, so dass sich der Live-Betrieb identifizieren lässt. Sollte ein ‚Auskunftsbegehren einer betroffenen Person' auftreten, werden die entsprechenden Videoexportdaten umfassend aufgezeichnet. Exportiertes Videomaterial wird mit Zeit- und Datumsstempel versehen. Die Möglichkeit zum Export basiert auf Privilegien und kann nur von einem autorisierten Operator wahrgenommen werden. Informationen in Verbindung mit dem Urheber des Videoexports werden aufgezeichnet und dokumentiert, damit der Operator die nötigen Berichtsinformationen wie beispielsweise ‚Rechtfertigung für den Videoexport', ‚Wer der vorgesehene Empfänger ist und warum' liefert, und schließlich wird exportiertes Videomaterial als einmalige, passwortgeschützte Datei geliefert, um die Integrität des exportierten Videos zu schützen.
- **Artikel 32** – Sicherheit der Verarbeitung. Unter Berücksichtigung der Implementierungskosten und der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein. Der Hauptschwerpunkt in diesem Bereich liegt auf der Pseudonymisierung und Verschlüsselung personenbezogener Daten. Gemäß dem SCC-Verhaltenskodex muss HTTPS-Verschlüsselung angewandt und vorkonfiguriert aktiviert sein.
- **Artikel 35** – Datenschutz-Folgenabschätzung. Vor einer Systeminstallation muss eine Datenschutz-Folgenabschätzung durchgeführt werden, denn dies ist eine gesetzliche Vorschrift in Abschnitt 64 DPA 2018 / DSGVO und Artikel 35 der DSGVO.

Diese Aufzählung ist zwar nicht vollständig, hebt jedoch einige der Schlüsselaspekte hervor, die Verantwortliche und Datenverarbeiter bei der Einführung von Videoüberwachungssystemen zu berücksichtigen haben. Nachdem es einige Widerstände dagegen gab, dass Videoüberwachungs-/ CCTV-Systeme der DSGVO entsprechen müssen, wurden bereits Strafen gegen CCTV-Betreiber/ Benutzer von Sicherheitssystemen in UK und Frankreich verhängt; Österreichs erste DSGVO-Geldbuße wurde wegen Nichteinhaltung beim Einsatz eines CCTV-Systems auferlegt.

4. Videoüberwachungssysteme

Neben klassischen Sicherheitsanwendungen auf Basis von IP-Überwachungskameras lassen sich diese Systeme zur Erhebung unternehmenskritischer Daten für die Geschäftsoptimierung nutzen. Neben den offensichtlichen Sicherheitsanwendungen mit der kontinuierlich zunehmenden Ausgereiftheit von IP-Überwachungskameras lassen sich diese Systeme zur Erhebung unternehmenskritischer Daten für die Geschäftsoptimierung nutzen.

Die Daten können zur Steigerung der Betriebseffizienz, Verbesserung der Systemgesundheit und Einhaltung der Sicherheitsvorgaben sowie zur Reduzierung der Betriebskosten herangezogen werden. Die Einführung und Durchsetzung der DSGVO hat Einzelhändler veranlasst, die Daten zu bewerten, die potenziell erhoben werden, ebenso wie die Verfahren ihrer Speicherung und Nutzung. Andere Abteilungen, die von diesen Daten profitieren sind Marketing, Finanzen, Logistik, Personalplanung und Visual Merchandising.

4.1 Geschäftsoptimierung: Schlüsselfunktionen

Wenn Videoüberwachungskameras zur Geschäftsoptimierung eingesetzt werden, ist es wichtig zu verstehen, dass die Technologie zur Erhebung statistischer Daten angewandt wird, die sich zu Berichten zusammenfassen lassen, um Businesstrends und -intelligence zu liefern. Damit können Einzelhändler geschäftliche Entscheidungen treffen.

Anders als bei einem Videoüberwachungssystem, das zur Schadensverhütung eingeführt wird und Mitarbeitern und Kunden Sicherheit durch das Sammeln von Videomaterial bietet, wird hier zur Datenerhebung für statistische Zwecke nur Sensortechnologie genutzt, so dass die erhobenen Daten nicht als personenbezogene Daten (PII) klassifiziert werden können. Alle diese Daten können bei der Entscheidungsfindung eine Rolle spielen, um die Kundenerfahrung zu fördern. Durch die Überwachung von Warteschlangen, das Verständnis der Besucherfrequenz und die Analyse der Ladengestaltung können Mitarbeiter dorthin abgestellt werden, wo ihre Anwesenheit am sinnvollsten ist, um den Bedarf zu decken.

Beispiele für Anwendungen, die Business Intelligence liefern können, sind folgende:

- Personenzählung
- Analyse von Warteschlangen
- Analyse von Belegungsdaten und Auslastung
- Intelligenter Verfolgungsalgorithmus zum Erfassen von längerem Verweilen

Zu den Vorteilen solcher Anwendungen gehören:

Optimierung von Ladengestaltung und Personalzuweisung
Verständnis dessen, was die Kunden wollen: wie sie sich an einem Standort bewegen, wie viel Zeit sie in verschiedenen Bereichen verbringen und wie sie sich im Laden verhalten. Kenntnis der geschäftigsten und ruhigsten Tageszeiten im Laden, so dass eine geeignete Personalzuweisung erfolgen kann und die Service Level entsprechend optimiert werden können. Die Statistiken der einzelnen Läden können verglichen werden, um die Effektivität für eine Reihe von Standorten zu messen.

Effiziente Marketingkampagnen
Mit programmierten und Live-Werbedurchsagen entsprechend den Kundendemografien können Unternehmen optimale Wirkungsgrade bei Marketingkampagnen erreichen. Entsprechend lassen sich Displays in beliebten oder häufiger besuchten Bereichen aufstellen, und Musik kann auf Alter oder Geschlecht abgestimmt werden, um die Wahrnehmung einer besseren Kundenerfahrung herbeizuführen.

Übertragung in eine oder mehrere Zonen
Live-Alarme können an Mitarbeiter gesendet und vorprogrammierte Durchsagen für Kunden durchgeführt werden, um den Wirkungsgrad zu optimieren. Außerdem sind spezifische Bereiche eines Ladens ohne Weiteres erreichbar, in denen eine geeignete Mitteilung verbreitet werden soll.

Warteschlangenlänge und -zeit effizient überwachen und messen
Das Messen von Warteschlangen und der Dauer des Zahlvorgangs sowie die Identifizierung von Bereichen, in denen es Serviceengpässe geben könnte, ermöglicht eine problemlose Zuweisung und Verteilung der Mitarbeiter, um so zeitnah und reibungslos Wartezeiten zu reduzieren.

4.2 Die Verantwortlichen und das konvergente Sicherheitskonzept

So wie wir eine in derselben Infrastruktur konvergierende Technologielandschaft erleben, um die für die reibungslose Funktion dieser Standorte erforderlichen Betriebstechnologien bereitzustellen, sollten wir auch einen konvergenten Entscheidungsfindungsprozess haben. Wir haben erfolgreiche Beispiele dafür gesehen, dass ein konvergentes Sicherheitskonzept Strukturen aufbrechen und verschiedene Geschäftsteams zur Zusammenarbeit ermächtigen kann. Diese Konvergenz war nie wichtiger als heute, wo klassische elektronische und physische Sicherheitsangebote Seite an Seite in Unternehmensnetzwerken zu finden sind.

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

4.3 Was von Partnern, Anbietern und Lieferanten zu erwarten ist

Es ist wichtig, Due Diligence anzuwenden und dafür zu sorgen, dass Dritte verstehen, wie wichtig es ist, dass ihre Priorität bei allem, was sie tun, auf der Beibehaltung bewährter Sicherheitsverfahren und einer Arbeitsweise liegt, die bestimmte Erfordernisse erfüllt. Beziehungen zu Dritten sind der Schlüssel dafür, eine gesunde Lieferkette aufzubauen und eine starke und vertrauensvolle Bindung herzustellen.

Wichtigste Aspekte, die bei der Bewertung Dritter und ihres Einflusses auf die Lieferkette zu berücksichtigen sind:

- Sie verstehen und erkennen Risiken rund um das Thema Cybersicherheit
- Sie können einen ausgereiften Cybersicherheits-Ansatz mit entsprechenden Prozessen und Werkzeugen vorweisen
- Sie verstehen die Auswirkungen behördlicher und gesetzlicher Vorgaben auf ihr Angebot
- Sie können demonstrieren, wie sie die Compliance-Anforderungen eines Benutzers unterstützen werden
- Cybersicherheit ist ein Prozess und nicht nur eine Technologie - sie können ein Lebenszyklusmanagement im Bereich Cybersicherheit nachweisen, um damit das Unternehmen Dritter zu schützen.

Aspekte der Lieferkettenbewertung
Die Bewertung der Lieferantentechnologien sollte weit über die operativen und technischen Merkmale des Geräts hinausgehen. Der Due-Diligence-Prozess sollte mit der Betrachtung des Unternehmens als Ganzes beginnen, einschließlich seiner Strategien und Verfahren. Die Bewertung des Cyber-Reifegrads eines Unternehmens ist wichtiger denn je.

5. Sicherheitsmanagement: Externe Steuerung und Lieferantenprozesse

Wie bei allen wirkungsvollen Sicherheitsmaßnahmen geht es auch bei der Cybersicherheit um die Stärke der eingesetzten Mittel. Es geht um den angemessenen Schutz des IP-Kameranetzwerks auf jeder Ebene: von den gewählten Produkten und eingesetzten Partnern bis zu den festgesetzten Anforderungen.

5.1 Standards and Richtlinien (externe Steuerung)

ISO 27001 – Informationssicherheitsmanagement
ISO/IEC 27001 ist ein Sicherheitsmanagementsystem, das Folgendes voraussetzt:

> die systematische Untersuchung der Informationssicherheitsrisiken einer Organisation unter Berücksichtigung von Bedrohungen, Schwachstellen und Einflüssen
> die Planung und Implementierung einer kohärenten und umfassenden Reihe von Informationssicherheitskontrollen bzw. sonstiger Formen der Risikobehandlung (wie beispielsweise Risikovermeidung oder Risikotransfer), um die Risiken anzugehen, die für inakzeptabel gehalten werden
> die Einführung eines übergeordneten Managementprozesses, damit Informationssicherheitskontrollen weiterhin auf fortlaufender Basis den Informationssicherheitsbedürfnissen der Organisation entsprechen.

Cyber Essentials Plus
Cyber Essentials ist ein staatlich gefördertes und von der Industrie unterstütztes Programm, das Organisationen hilft, sich vor üblichen Online-Bedrohungen zu schützen. Cyber Essentials ist ein wirksamer Indikator für Unternehmen, die die mit der Cybersicherheit verbundenen Herausforderungen verstehen. Cyber Essentials ist eine Bewertung der Strategien und Prozesse eines Unternehmens. 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 Regierung von allen Bietern bei Ausschreibungen, bei denen mit bestimmten sensiblen und personenbezogenen Daten umgegangen wird, die Zertifizierung nach dem Programm Cyber Essentials.

Secure by Design & Secure by Default
Bei ‚Secure by Default' geht es um die Anwendung eines ganzheitlichen Ansatzes bei der Lösung zugrundeliegender Sicherheitsprobleme im Gegensatz zur Behandlung von Symptomen, um das Handeln in großem Maßstab, um den Gesamtschaden an einem System oder Komponententyp zu reduzieren. ‚Secure by Default' bezieht sich auf die langfristigen technischen Bemühungen mit dem Ziel, die richtigen Sicherheitsprimitiven in Software und Hardware einzubauen. Es bezieht sich auch auf die ebenso anspruchsvolle Aufgabe, dafür zu sorgen, dass diese Primitiven so verfügbar und nutzbar sind, dass sie der Markt ohne Weiteres einführen kann.

Zur Unterstützung unserer Technologien hat Axis ‚Secure by Default' an den Verhaltenskodex National Cybersecurity Strategy angeglichen:

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

5.2 Leitlinien und Tools (Lieferantenprozesse)

Manufacturing Hardening Guide
Wenn es um die Absicherung eines Netzwerks geht, setzen Organisationen oft verschiedene technische Kontrollen ein, um ein Konzept der ‚mehrschichtigen Verteidigung' zu realisieren. Dieses Konzept hilft, die einzelnen Problem- und Expositionsstellen einzuschränken. Ein wichtiger Prozess, der allerdings oft übersehen wird, ist ‚System Hardening'. Dazu gehört die Durchführung von Konfigurationsänderungen an Standardeinstellungen des Systems, so dass das System vor Bedrohungen der Informationssicherheit besser geschützt ist. Darüber hinaus trägt dieser Prozess dazu bei, die Menge an inhärenten Schwachstellen zu minimieren.

Ein ‚System Hardening'-Prozess sollte für alle Geräte eingeführt sein, die mit einem Netzwerk verbunden sind. Dazu gehören Workstations, Server und Netzwerkgeräte. Da Hersteller den Setup und die Konfiguration ihres Systems besser als die meisten anderen kennen, sollte es in ihrer Verantwortung liegen, Partnern und Benutzern die nötigen Daten zu liefern, um die Integrität ihrer Geräte und des Eigentums des Endanwenders zu schützen. Ein ‚Hardening Guide' sollte technischen Rat für jeden enthalten, der an der Einführung von Videoüberwachungslösungen beteiligt ist. Er sollte eine Baseline-Konfiguration festsetzen und umfassende Informationen zum Umgang mit der veränderlichen Bedrohungslandschaft enthalten.

Alle Lieferanten sollten sich bemühen, bei Design, Entwicklung und Test von Geräten bewährte Verfahren der Cybersecurity anzuwenden, um das Risiko von Schwachstellen zu minimieren, die bei einem Angriff ausgenutzt werden könnten. Allerdings setzt die Absicherung eines Netzwerks, seiner Geräte und der von ihm 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.

Beispiele für gute Hardening Guides sollten Baseline-Anwendungen wie beispielsweise CIS Controls - Version 6.1 entsprechen[13]. Diese Controls waren bisher unter dem Namen SANS Top 20 Critical Security Controls bekannt. Dieses Dokument bezieht sich auf diese CSC (Critical Security Control) durch die Kennzeichnung CSC#.

Geräteverwaltung
Device Manager ist ein am Standort eingesetztes Tool, mit dem sich vernetzte Geräte schnell, kostengünstig und sicher verwalten lassen. Es bietet Installateuren und Systemadministratoren ein hoch effizientes Tool zur Wahrnehmung aller wichtigen Aufgaben in den Bereichen Installation, Sicherheit und Wartung.

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 - Wahrnehmung aller wichtigen Installations-, Sicherheits- und operativen Aufgaben
- Schnelle und einfache Konfiguration neuer Geräte – Einstellungen für Sichern und Wiederherstellen
- Für Standorte jeder Größe geeignet – Installationen an einem oder mehreren Standorten

OEM / ODM
Erstausrüster (OEM) 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. Dank solcher Firmen kann das Markenunternehmen produzieren, ohne an der Organisation mitwirken oder eine eigene Fabrik 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 den Verkaufs- und Marketingprozess fokussieren. Das ist einer der Hauptgründe dafür, dass viele Kamerahersteller in der Sicherheitsbranche OEM oder ODM mit ihren Markenprodukten beauftragen. Berichten zufolge beziehen immerhin 96 Lieferanten Kameras über OEM oder ODM von einem anderen Anbieter.

[13] *www.cisecurity.org/critical-controls.cfm*

Das bringt verschiedene Herausforderungen mit sich - eine der offensichtlichsten ist die Cybersicherheit. Wenn einer der Hersteller eine Schwachstelle hat, kann sich das auf alle anderen Wiederverkäufer und Partner in der gesamten Lieferkette auswirken. Es kann außerdem die umfassende Sichtbarkeit der Lieferkette stark erschweren. Angesichts der bloßen Anzahl zwischengeschalteter OEMs und ODMs könnte ein Endanwender, der den Due-Diligence-Prozess durchgeführt und Technologien eines bestimmten Herstellers abgelehnt hat, diese Technologien unter anderem Namen schließlich unbeabsichtigter Weise doch nutzen, ohne irgendetwas davon zu wissen.

CPU Mikroprozessor-Chip
Es hat sich gezeigt, dass in Geräten eingebaute, serienmäßige CPU-Verarbeitungschips Ziel von Hackerangriffen sind, da sie viele Schwachstellen aufweisen. Einer der Hauptgründe dafür ist die Skalierbarkeit, die aus einer einzigen identifizierten Schwachstelle generiert wird. Zu neuerlichen Beispielen gehören die Sicherheitslücken ‚Meltdown' und ‚Spectre'[14], zwei zusammenhängende Side Channel Attacks gegen moderne CPU-Mikroprozessoren, die mit unzulässigen Codes unberechtigt auf Daten zugreifen können.

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 Cyber Security Centre (NCSC) rät, diese Patches schnellstmöglich in den Geräten zu installieren.

Firmware-Strategie
Signierte Firmware ist wichtig für Endanwender und mindert einige der potenziellen Risiken für Geräte, die im Logistik- / Vertriebsprozess manipuliert wurden. Die unterschriebene Signatur, manchmal ‚Hash' genannt, wird im Vertrieb auf der Firmware angebracht. Ein Prozessor berechnet seinen eigenen Hash-Wert und lädt nur ein Bild mit einem Hash, der mit dem von einem Zertifikat, dem er vertraut, signierten übereinstimmt.

Schwachstellen-Management
Die ständige Zunahme der Internetkriminalität und der damit verbundenen Risiken zwingt die meisten Organisationen, der Informationssicherheit mehr Aufmerksamkeit zu widmen. Ein Schwachstellen-Managementprozess sollte Teil der Bemühungen jeder Organisation um die Beherrschung von Informationssicherheitsrisiken sein. Mit diesem Prozess kann sich eine Organisation einen ständigen Überblick über Schwachstellen in ihrer IT-Umgebung und die damit verbundenen Risiken verschaffen. Nur durch die Identifizierung und Minderung von Schwachstellen in der IT-Umgebung kann eine Organisation Angreifer daran hindern, in ihre Netzwerke einzudringen und Daten zu stehlen[15].

Es ist wesentlich, dass Lieferanten das Schwachstellen-Management in ihren Betrieben sicherstellen, einschließlich Prozessen, die Schwachstellen in allen Systemen erfassen und beheben sowie verhindern, dass bei Änderungsprozessen und der Einführung neuer Systeme neue Schwachstellen eingeführt werden. Alle Fragen in Verbindung mit Risiken, die der Lieferant akzeptiert, müssen dem Endanwender mitgeteilt und mit ihm geklärt werden. Wird dieses Prinzip nicht umgesetzt, könnten Angreifer Schwachstellen in Systemen dazu ausnutzen, Cyberattacken gegen ein Unternehmen und seine Lieferanten durchzuführen.

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

[14] *https://meltdownattack.com/*

[15] *www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180*

Benachrichtigungen über Sicherheitshinweise
Sicherheitshinweise tragen zur Reduzierung der Risiken bekannter Schwachstellen bei. Der Sicherheitshinweis kann sich auf offizielle CVE (Common Vulnerability and Exposure) oder sonstige Schwachstellenberichte beziehen. Sicherheitshinweise umfassen eine Schwachstellenbeschreibung, Risikobewertung, Empfehlungen und Informationen dazu, wann eine Dienstfreigabe verfügbar sein wird. Die meisten Lieferanten arbeiten nach einem indirekten Vertriebsmodell und haben ein Partnerprogramm eingeführt.

Mit Benachrichtigungen über Sicherheitshinweise können Kunden, die in keinem 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 vielleicht keinen Ansprechpartner im Unternehmen haben, der die Installation ursprünglich durchgeführt hat.

Building Security in Maturity Model (BSIMM)
BSIMM ist ein Rahmen zur Messung der Software-Sicherheit, mit dem Organisationen ihre Software-Sicherheit mit Initiativen anderer Organisationen vergleichen und herausfinden können, wo sie stehen. BSIMM hilft bei der Bewertung von Prozessen, Aktivitäten, Rollen und Verantwortlichkeiten. Dazu gehört Folgendes:

> Design- und Architekturprüfungen
> Codeprüfung
> Tests auf bekannte Sicherheitslücken
> Einsatz eines Tools zum Scannen auf Standard-Sicherheitslücken, das verwendet wird, um CVE-Schwachstellen in Open-Source-Programmen zu finden.

Long Term Support (LTS)
Long Term Support ist eine Produktlebenszyklus-Verwaltungsrichtlinie, bei der eine stabile Version von Computersoftware über einen längeren Zeitraum als in der Standardversion verwaltet wird. Long Term Support Firmware sollte nur Patches für Stabilität, Performance und Sicherheit umfassen. Lieferanten bemühen sich, bis zu 10 Jahre lang nach Markteinführung eines Geräts LTS Firmware bereitzustellen.

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

Wissensvermittlung und Kooperation
Einer der Schlüsselbereiche, der bei der Auswahl eines Technologieanbieters berücksichtigt werden sollte, sind die Fortbildung und der Support, den er zu bieten hat. Mit der Weiterentwicklung der Herausforderungen, mit der Channel und Industrie insbesondere im Hinblick auf Cybersicherheit konfrontiert sind, sollten Hersteller das Thema nach Möglichkeit proaktiv angehen und dem Markt Sicherheiten und Inhalte bieten. Potenzielle Beispiele sind:

> Kostenlose Teilnahme an Präsenzkursen der Akademie zur Cybersicherheit
> Online-Trainingsakademie zur Cybersicherheit
> Online-Schnelltest zur Cybersicherheit
> Hardening Guide
> Schwachstellenstrategien
> Bewährte Verfahren der Cybersicherheit
> Konzepte und Terminologie der Cybersicherheit

6. Nächste Schritte und Zukunftsaspekte

Wir alle müssen unseren Teil dazu beitragen, dass ein starker Fokus auf Cybersicherheit gerichtet wird. Es ist wichtig, die Fragen zu überdenken, die gestellt werden sollten, um das entsprechende Risiko für Unternehmen zu minimieren:

1. Können wir Unterstützung vom Netzwerkarchitekten oder Sicherheitschef der Organisation erhalten?
2. Können wir den Cyber-Reifegrad von Technologiepartnern und Systemintegratoren beurteilen?
3. Überdenken, ob Sicherheitssysteme auch im Hinblick auf Cybersicherheit eingeführt sind:
   a. Wurden Standard-Benutzername und Kennwort geändert?
   b. Ist die neueste Firmware-Version eingeführt?
   c. Wird Verschlüsselung (idealerweise HTTPS) angewandt?
   d. Wurde Fernzugriff deaktiviert?
4. Schließt der Service- und Wartungsvertrag auch Updates der Hersteller-Firmware ein?
5. Unterstützen die eingesetzten Technologien die Fähigkeit, die DPA 2018 / DSGVO einzuhalten?

DE/R1/2004

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerklösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für Videoüberwachung und -analyse sowie Zutrittskontrolle und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.500 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen über Axis finden Sie unter www.axis.com

AXIS COMMUNICATIONS