KI basierte/unterstützte Smartretail-Konzepte, Anwendungen & Trends, und deren Supply Chain Security Requirements

Dominic Lachat, 03.10.23, IKT Sicherheits-Konferenz, Linz

NEXGEN

NEXGEN

“KI basierte/unterstützte Smart Retail-Konzepte, Anwendungen & Trends, und deren Supply Chain Security Requirements.“

- Vorstellung diverser Smart Retail Konzepte
- Supply Chain Security Requirements: Die NIS 2 Direktive und ihre Auswirkungen auf Smartretail-Konzepte
- Neu Anforderungen und Pflichten wegen NIS 2

KI unterstützte Smartretail-Konzepte

Smart Retail-Konzepte beziehen sich auf innovative Ansätze und Technologien, die im Einzelhandel eingesetzt werden, um das Einkaufserlebnis zu verbessern, die Effizienz zu steigern und personalisierte Dienstleistungen anzubieten. Hier sind einige Beispiele für Smart Retail-Konzepte:

1. Künstliche Intelligenz (KI): KI-Technologien wie maschinelles Lernen und Bilderkennung ermöglichen personalisierte Empfehlungen, automatisierte Kundenservice-Chats oder die Analyse von Verkaufsdaten, um Trends und Vorhersagen zu generieren.
2. Internet of Things (IoT): Durch die Vernetzung von Geräten und Sensoren können Einzelhändler Daten in Echtzeit sammeln und analysieren, um beispielsweise den Lagerbestand zu optimieren oder Kundenverhaltensmuster zu erkennen.
3. Augmented Reality (AR) und Virtual Reality (VR): AR- und VR-Technologien ermöglichen es Kunden, Produkte virtuell anzuprobieren oder in einer virtuellen Umgebung zu erleben, was das Einkaufserlebnis interaktiver und ansprechender macht.

Diese Smart Retail-Konzepte sollen den Einzelhandel modernisieren, die Kundenzufriedenheit verbessern und den Einzelhändlern helfen, wettbewerbsfähig zu bleiben.

NEXGEN

KI unterstützte Smartretail-Konzepte - Trends

Trends im Bereich KI-unterstützte Smartretail-Konzepte

- KI lokal auf Workstations ➔ KI in der Cloud
- Der Kunde macht die Erfassung der Daten selber oder die KI unterstützt den Retailer bei der Erfassung der Einkaufs-Daten
- Die KI ermöglicht einen Einkauf automatisiert auf Korrektheit zu überprüfen.
- Eine KI überprüft das Einkaufsverhalten eines Kunden

KI unterstützte Smartretail Konzepte - Lösungsbeispiele

Diverse Ansätze

- Self-Scanning mit KI unterstützter Transaktionsüberprüfung
- Verkauf mittels KI – unterstützter Artikelerkennung (ohne Selfscanning)
- Grab – and – Go Stores
- KI unterstützes Loss Prevention

SUPERSMART

NEXGEN

Self-Scanning mit KI unterstützter Transaktionsüberprüfung

Lösungsbeispiel «Supersmart» von Supersmart:

Das Supersmart Scan & Go Loss Prevention System besteht aus intelligenten Hardwarekomponenten und einer auf künstlicher Intelligenz (KI) basierenden Software, die die Checkout-Zeiten und -Prozesse am Point of Sale optimiert und Umsatzverluste durch Schwund drastisch reduziert.

Supersmart eliminiert Warteschlangen, macht den Einkaufsprozess einfacher und sicherer, erhöht die Zufriedenheit und damit die Loyalität Ihrer Kunden.

SUPERSMART

NEXGEN

Self-Scanning mit KI unterstützter Transaktionsüberprüfung

Lösungsbeispiel «Supersmart» von Supersmart

- Self-Scanning mit speziellen MDEs oder Smartphone’s
- Checkout über Waage (2 Varianten)
- Berechnung der Korrektheits-Wahrscheinlichkeit der Transaktion
- Normaler Bezahlvorgang an Kasse oder über Smartphone

SUPERSMART

NEXGEN

Self-Scanning mit KI unterstützter Transaktionsüberprüfung

SUPERSMART

NEXGEN

Verkauf mittels KI – unterstützter Artikelerkennung

Lösungsbeispiel «Tablesmart»

- Kein Self-Scanning notwendig
- Checkout über Kassen-Waageneinheit
- Berechnung der Korrektheits-Wahrscheinlichkeit der Transaktion
- Normaler Bezahlvorgang an der Tablesmart

SUPERSMART

NEXGEN

AI Retailer Systems

NEXGEN

Grab & Go – Stores

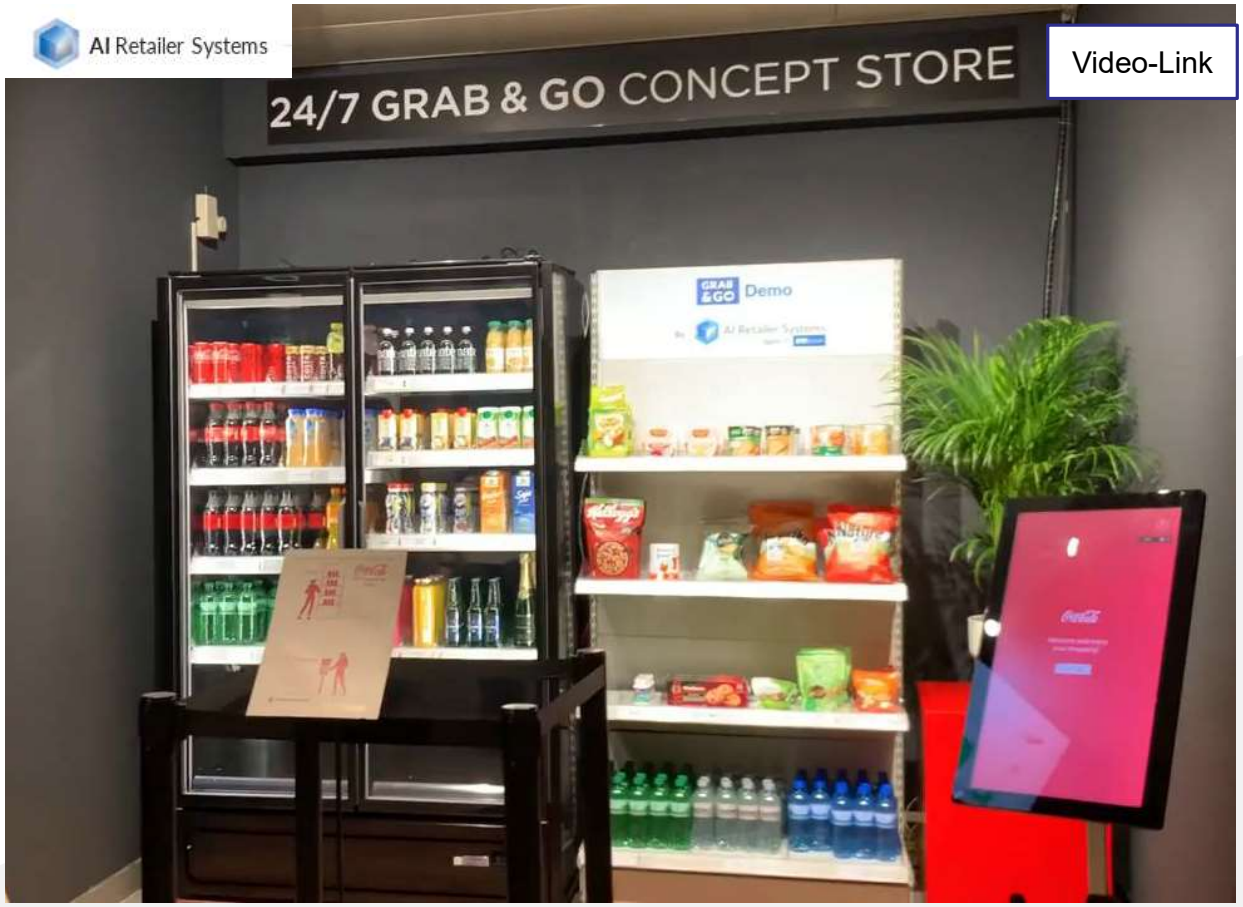
Lösungsbeispiel «Grab & Go Store» von AI Retailers

- Kameras für die Regalüberwachung
- Kameras für die Personen-Identifikation (Anonymisiert)
- Wiegezellen in den Regalen (optional)
- Hybrid-Version (KI-Verarbeitung lokal und in der Cloud)
- USP: Beim Verlassen des Ladens ist die Transaktion korrekt erfasst & bezahlt. Im Gegensatz zu anderen Lösungen, bei welchen die Bilddaten im Nachgang noch von Menschen kontrolliert werden

Grab – and – Go Stores – Beispiel AI-Retailer

AI Retailer Systems

Video-Link



AI Retailer Systems

NEXGEN

KI unterstütztes Loss Prevention

AIRS nutzt handelsübliche Kameras an der Ladendecke, um in Echtzeit festzustellen, wer was gestohlen hat, und gibt bei Diebstahlsfällen mit hoher Wahrscheinlichkeit eine Warnung aus, die an den Filialleiter weitergeleitet wird oder automatisch einen Alarm oder eine Warnung an den Self-Scanning-Kassenterminals auslöst.

- Analysephase: um festzustellen, wie und wo (in der Filiale oder an Self-Scanning-Terminals) Diebstahl stattfindet, einschließlich der Art der Täter (neue oder wiederkehrende Kunden
- Präventionsphase 1: Echtzeitwarnungen von höchstwahrscheinlichen Diebstählen im Einkaufsbereich
- Präventionsphase 2: Echtzeit-Diebstahlswarnungen an Self-Scanning-Terminals (stationär oder mobil)

NEXGEN

Supply Chain Security Requirements

- Smart-Retail-Konzepte nutzen Cloud-Services für die KI, für die Verarbeitung und die Speicherung von Daten
- Die Abverkäufe/Transkationen werden in der Cloud gespeichert. Die Daten für die Warenwirtschaft sind somit auch in der Cloud. Die Warenwirtschaft ist die Basis für die Belieferung der Läden und die Bestellung bei den Lieferanten

Die zunehmende Abhängigkeit der Supply Chain des Lebensmittel-sektors von der Digitalisierung und vernetzten Systemen setzt ihn einem steigenden Risiko von Cyber-Bedrohungen aus. Um diesen Risiken zu begegnen, wird die NIS2-Richtlinie erhebliche Auswirkungen auf den Lebensmittelsektor in der gesamten EU haben.

NEXGEN

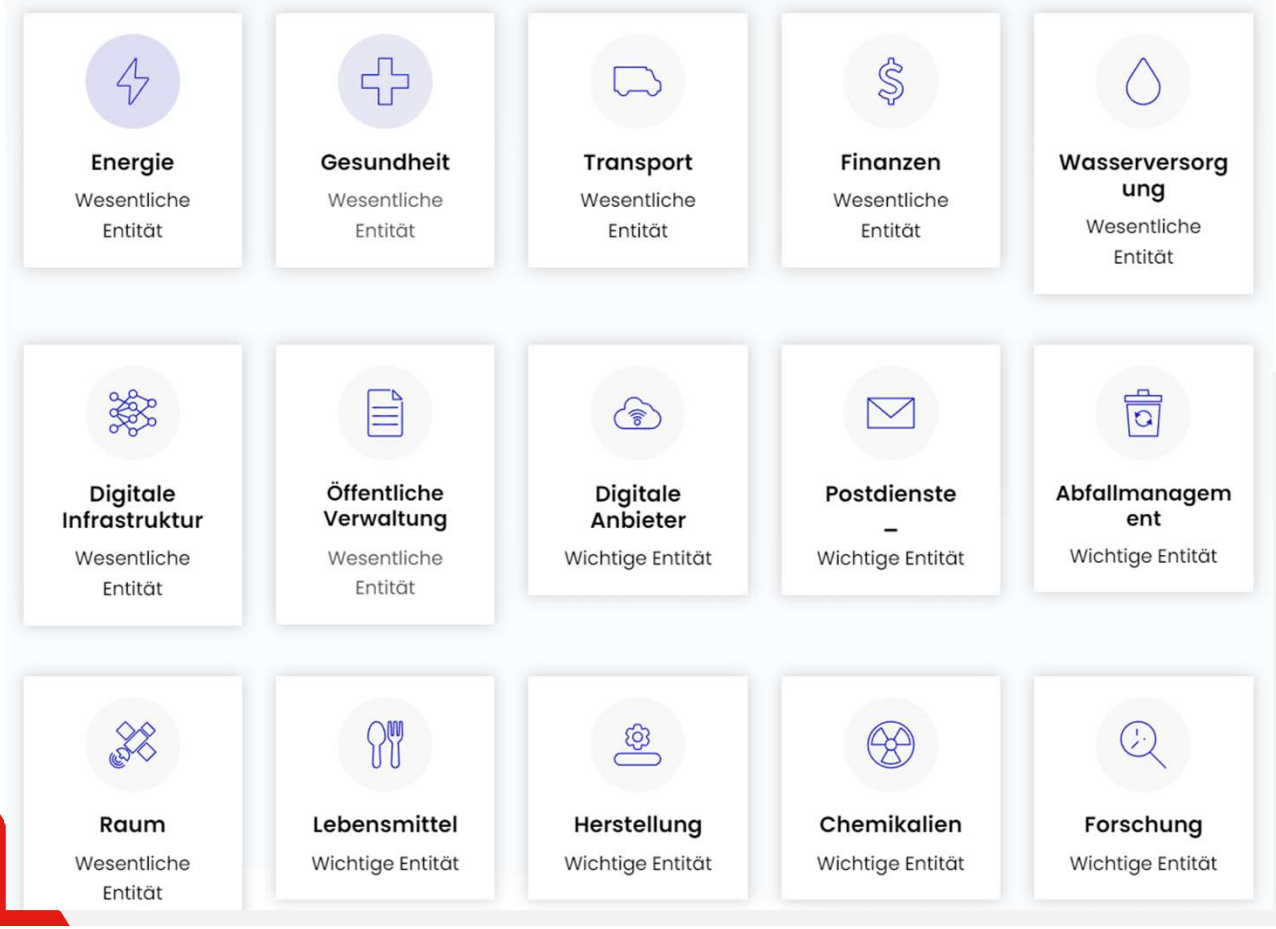
NIS 2 - Richtlinie

Die NIS 2-Richtlinie, auch bekannt als Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, hat zum Ziel, die Cybersicherheit in der Europäischen Union zu stärken.

Sie legt Anforderungen für Betreiber wesentlicher Dienste und digitale Dienstleister fest, um deren Widerstandsfähigkeit gegen Cyberangriffe zu verbessern.

Der Sinn dieser Richtlinie besteht darin, die Sicherheit kritischer Infrastrukturen und digitaler Dienste zu gewährleisten und somit das Vertrauen in die digitale Wirtschaft und Gesellschaft zu stärken.

NIS 2 – Richtlinie: Wer ist betroffen?



Wesentliche Entitäten (EE)
Größenschwelle: je nach Branche unterschiedlich, in der Regel jedoch 250 Mitarbeiter, 50 Mio. € Jahresumsatz oder 43 Mio. € Bilanzsumme

Wichtige Entitäten (IE)
Größenschwelle: je nach Branche unterschiedlich, in der Regel jedoch 50 Mitarbeiter, 10 Mio. € Jahresumsatz oder 10 Mio. € Bilanzsumme

Quelle: https://nis2directive.eu/

NEXGEN

NIS 2 – Richtlinie: Neu Food Sektor (auch Einzelhandel)

Komplexität der Lieferkette
Der Lebensmittelsektor besteht aus einer komplexen Lieferkette, an der Millionen kleiner Organisationen beteiligt sind, die mit geringen Gewinnspannen arbeiten. Diese Komplexität macht es schwierig, angemessene Sicherheit zu implementieren.

IoT-Geräte
Der Lebensmittelsektor verlässt sich zunehmend auf IoT-Geräte, um Prozesse in Bereichen wie Lebensmittellagerung und -transport zu überwachen und zu steuern. Diese Geräte können anfällig für Cyberangriffe sein.

Legacy-Systeme
Viele Lebensmittelunternehmen verlassen sich auf veraltete Systeme, die möglicherweise nicht mit modernen Cybersicherheitsmaßnahmen kompatibel sind, wodurch sie potenziellen Angriffen ausgesetzt sind.

Ransomware-Angriffe
Die Agrar- und Lebensmittelindustrie ist häufig Ziel von Ransomware-Angriffen, die zu erheblichen finanziellen Verlusten und Störungen der Lieferkette führen können.

Begrenztes Budget
Vielen Organisationen im Lebensmittelsektor fehlen die finanziellen Mittel, um in angemessene Cybersicherheitsmaßnahmen zu investieren. Dadurch sind sie nicht in der Lage, modernen Bedrohungen zu begegnen.

Zugriff Dritter
Lebensmittelunternehmen verlassen sich bei wichtigen Dienstleistungen, einschließlich Logistik und Transport, häufig auf Drittanbieter, und diese Anbieter können Schwachstellen aufweisen, die ausgenutzt werden könnten.

NEXGEN

NIS 2 : Neue organisatorische Herausforderungen

Risikomanagement
Um der neuen Richtlinie zu entsprechen, müssen Organisationen Maßnahmen ergreifen, um Cyber-Risiken zu minimieren. Zu diesen Maßnahmen gehören das Vorfallmanagement, eine stärkere Sicherheit der Lieferkette, eine verbesserte Netzwerksicherheit, eine bessere Zugangskontrolle und Verschlüsselung.

Meldepflichten
Wesentliche und wichtige Einrichtungen müssen über Prozesse zur zeitnahen Meldung von Sicherheitsvorfällen mit erheblichen Auswirkungen auf ihre Leistungserbringung oder Empfänger verfügen. NIS2 legt spezifische Benachrichtigungsfristen fest, beispielsweise eine 24-Stunden-„Frühwarnung“.
.

Unternehmensverantwortung
NIS2 verlangt von der Unternehmensleitung, die Cybersicherheitsmaßnahmen des Unternehmens zu überwachen, zu genehmigen und darin geschult zu werden sowie Cyberrisiken anzugehen. Verstöße können zu Strafen für das Management führen, einschließlich Haftung und einem möglichen vorübergehenden Ausschluss von Führungspositionen.

Geschäftskontinuität
Unternehmen müssen planen, wie sie die Geschäftskontinuität im Falle schwerwiegender Cybervorfälle sicherstellen wollen. Dieser Plan sollte Überlegungen zur Systemwiederherstellung, zu Notfallmaßnahmen und zur Einrichtung eines Krisenreaktionsteams umfassen.

Quelle: https://nis2directive.eu/

Für die Verringerung der Risiken, respektive die Einhaltung der NIS 2 Directive hats an dieser Konferenz die richtigen Ansprechpartner

Herzlichen Dank für Ihre Aufmerksamkeit

Fragen?