Das Internet der Dinge für Unternehmen

Geschäftschancen im Bereich IoT nutzen – aber sicher!

Lösung im Überblick

Alcatel·Lucent Enterprise

IoT mischt die Karten neu

Das Internet der Dinge (Internet of Things, IoT) hat das Potenzial, Unternehmen und Wirtschaft zu revolutionieren: Es tun sich ganz neue Wege auf, um Daten und Informationen zu sammeln. Dabei werden große Trends u. a. Mobilität, Automatisierung und Datenanalyse in Technologie und Wirtschaft zusammengeführt. IoT bedeutet die Verbindung physischer Objekte über ein Netzwerk, durch integrierte Sensoren, Aktoren und andere Geräte, die in der Lage sind, Informationen in Echtzeit innerhalb eines Netzwerks zu erfassen und zu übertragen. Die gesammelten Daten können dann für folgende Zwecke analysiert werden:

- **Optimierung von Produkten und Prozessen**, durch Senkung der Betriebskosten, gesteigerte Produktivität und die Entwicklung neuer Produkte und Dienstleistungen
- **Erkenntnisse über die Bedürfnisse und Vorlieben der Kunden**, um individuellere Produkte und Dienstleistungen anbieten zu können
- **Konzeption intelligenterer und effizienterer Unternehmen**, durch proaktive Überwachung kritischer Infrastrukturen und Gestaltung effizienterer Prozesse
- **Verbesserung der Nutzererfahrung** durch das Angebot neuer oder verbesserter Produkte und Dienstleistungen, um sich als datengesteuertes Unternehmen von der Konkurrenz abzuheben

Das IoT wächst und wächst

In zahlreichen Branchen ist bereits für die nahe Zukunft ein verstärkter Einsatz von IoT-Lösungen geplant. Im Jahr 2022 wird der Markt für das Internet der Dinge um voraussichtlich 18 % auf 14,4 Milliarden aktive Verbindungen anwachsen. Es wird erwartet, dass es bis 2025, wenn die Lieferkettenprobleme nachlassen und sich das Wachstum weiter beschleunigt, etwa 27 Milliarden vernetzte IoT-Geräte geben wird.

Quelle https://iot-analytics.com/number-connected-iot-devices

IoT und seine Herausforderungen

Das IoT führt zu beispiellosen Datenströmen, die die Netzinfrastruktur in Bezug auf Leistung und Management herausfordern. Gleichzeitig steigen die Sicherheitsrisiken an allen Endpunkten. Mit Blick auf diese Probleme müssen Netzwerke neu ausgelegt werden, damit mehr Netzwerkintelligenz, ein höherer Automatisierungsgrad und Sicherheit möglich sind.

Was es braucht, ist eine kosteneffiziente Netzwerkinfrastruktur, die große Datenströme sicher verarbeiten kann, aber auch einfach zu managen und zu betreiben ist. Was muss die Infrastruktur leisten?

- **Einen einfachen, automatisierten Prozess für das Onboarding von IoT-Geräten bieten.** Große IoT-Systeme können Tausende von Geräten oder Sensoren umfassen, und die manuelle Bereitstellung und Verwaltung all dieser Endpunkte ist komplex und fehleranfällig. Beim automatischen Onboarding erkennt die Netzwerkinfrastruktur Geräte dynamisch und ordnet sie dem entsprechenden, gesicherten Netzwerk zu.
- **Die richtigen Netzressourcen bereitstellen, damit das IoT-System ordnungsgemäß und effizient funktioniert.** Viele Geräte im IoT-System liefern unternehmenskritische Informationen, die ein bestimmtes Maß an QoS erfordern. Einige Anwendungsfälle erfordern beispielsweise, dass eine angemessene Bandbreite in einer Hochleistungsnetzinfrastruktur reserviert wird, damit die Bereitstellung der Dienste zuverlässig funktioniert.
- **Eine sichere Umgebung zum Schutz vor Cyberangriffen und Datenverlust bereitstellen.** Da die vielen vernetzten Geräte und Sensoren im IoT eine Fülle potenzieller Angriffsvektoren darstellen, ist die Sicherheit ein ausschlaggebender Faktor, um die Cyberkriminalität in Schach zu halten. Diese Sicherheit muss auf mehreren Ebenen ansetzen, unter anderem bei der Segmentierung der IoT-Netze selbst.

Anfällig für Cyberkriminalität

Mit dem Internet der Dinge wächst auch die Bedrohungslage: Je mehr Sensoren und verbundene Geräte, desto größer die Angriffsfläche im Netzwerk. Das Internet der Dinge ist besonders anfällig, da bei der Herstellung vieler IoT-Geräte die Sicherheit nicht mitgedacht wird oder die Hersteller beim Thema Sicherheit nicht auf dem neuesten Stand sind. Folglich sind IoT-Systeme zunehmend das schwächste Glied in der Unternehmenssicherheit.

Steve Turner, Analyst bei Forrester, erklärt, dass sich seines Wissens Angriffe mit Ransomware relativ gleichmäßig auf alle Branchen verteilen. Allerdings finden derartige Vorfälle in bestimmten Branchen wie etwa kritischen Infrastrukturen und im Gesundheitswesen medial die größte Beachtung.[1]

IoT-Endgeräte stellen Risiken für Assets im gesamten Netzwerk dar. Durch eine Aufteilung in Segmente über eine virtuelle Netzwerksegmentierung werden IoT-Geräte und die Anwendungen, mit denen sie gesteuert werden, isoliert und Bedrohungen auf diese Weise eingedämmt – ohne die Kosten oder Komplexität, die separate Netzwerke verursachen würden.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Aufbau einer sicheren IoT-Infrastruktur

Der Schutz des Datenverkehrs und der IoT-Geräte ist eine Herausforderung, die sich nicht durch eine einzige Sicherheitstechnologie lösen lässt. Benötigt wird ein strategischer Ansatz, in dessen Rahmen die Vorteile mehrerer Sicherheitsvorkehrungen kombiniert werden.

Damit Unternehmen die Vorteile von IoT bei minimierten Risiken nutzen können, bietet Alcatel-Lucent Enterprise (ALE) eine Zero-Trust-Netzwerkstrategie mit mehrstufiger Sicherheit an.

Die Strategie von ALE bietet Schutz auf jeder Ebene der Infrastruktur, vom einzelnen Benutzer und Gerät bis hin zur Netzwerkebene. Die Makro- und Mikrosegmentierung des Netzwerks ist ein einfacher und sicherer Weg für eine garantiert sichere Einbindung von Geräten und die Bereitstellung der richtigen Netzwerkressourcen für einen ordnungsgemäßen und effizienten Betrieb des Systems. Es entsteht dabei eine sichere Umgebung, die vor Cyberangriffen schützt.

IoT-Segmentierung

Eine IoT-Segmentierung bedeutet, dass allen Benutzern, Geräten und Anwendungen innerhalb des ALE-Netzwerks Profile zugewiesen werden. Diese Profile, über die Rollen, Zugriffsberechtigungen, QoS-Level und weitere richtlinienrelevante Informationen definiert sind, werden an alle Switches und Access Points im Netzwerk übermittelt.

- Bei der Makrosegmentierung werden IoT-Geräte in „virtuellen Segmenten“ platziert. Mittels Netzwerkvirtualisierung ist es möglich, dass mehrere Geräte und Netzwerke dieselbe physische Infrastruktur nutzen, während sie vom Rest des Netzwerks isoliert bleiben.
- Mikrosegmentierung bedeutet, dass die Geräte innerhalb eines virtuellen Segments unterschiedlichen QoS- und Sicherheitsregeln unterliegen können. Dadurch wird eine höhere Granularität erreicht und die Netzwerksicherheit steigt, da verhindert wird, dass verschiedene Gerätetypen im selben Segment miteinander interagieren, wenn dies nicht vorgesehen ist.
- Wenn in einem durch Makro- und Mikrosegmentierung aufgeteilten Netzwerk ein Gerät in einem Teil des Netzwerks kompromittiert ist, hat dies nicht nur keine Auswirkung auf Geräte oder Anwendungen in anderen virtuellen Segmenten, sondern das Problem kann auch nicht innerhalb des betroffenen Segments auf andere Gerätetypen übergreifen.
- Beim Herstellen der Verbindung mit einem neuen IoT-Gerät erkennt das Netzwerk automatisch das Geräteprofil und das Gerät wird der entsprechenden virtuellen Umgebung zugeordnet.
- Die Kommunikation bleibt auf die Geräte innerhalb dieser virtuellen Umgebung und auf die Anwendung im Rechenzentrum beschränkt, mit der diese Geräte gesteuert werden.
- Da alle Benutzer ebenfalls Profile innerhalb des ALE-Netzwerks besitzen, kann der Zugang zu den virtuellen IoT-Segmenten auf autorisierte Personen und Gruppen beschränkt werden.

Tiefgreifende Sicherheit

- Zusätzlich zur IoT-Segmentierung bieten ALE-Netzwerktechnologien eine mehrschichtige Sicherheit über mehrere Netzwerkebenen hinweg.
- Profile auf Benutzerebene gewährleisten, dass Benutzer mit den entsprechenden Zugriffsrechten authentifiziert und autorisiert werden.
- Auf Geräteebene wird vom Netzwerk sichergestellt, dass die Geräte authentifiziert werden und den festgelegten Sicherheitsregeln entsprechen.
- Auf Anwendungsebene können vom Netzwerk Regeln für die einzelnen Anwendungen oder Anwendungsgruppen festgelegt werden, u. a. für eine Sperrung oder Bandbreitenbegrenzung oder um zu steuern, welche Benutzer auf welche Anwendungen zugreifen dürfen.
- Auf der Netzwerkebene profitieren ALE-Switches von einem sicheren, diversifizierten Code. Dieser schützt die Netzwerke vor inhärenten Schwachstellen, Code Exploits, eingebetteter Malware und potenziellen Backdoors, durch die Switches, Router und andere geschäftskritische Hardware kompromittiert werden könnten.
- Mit den Smart Analytics-Funktionen von ALE, z. B. Deep Packet Inspection und anderen Technologien, werden die Daten- und Anwendungstypen erkannt, die über das Netzwerk übertragen werden. So lassen sich ungewöhnliche Datenverkehrsmuster und unbefugte Aktivitäten im Netzwerk identifizieren.

Operatives und Netzwerkmanagement von Anfang bis Ende

Netzwerklösungen von ALE bieten auch erhebliche Vorteile im operativen Bereich und beim Management.

- ALE ermöglicht den Betrieb mehrerer separater virtueller Netzwerke auf einer einzigen, gemeinsamen Infrastruktur. CAPEX-Investitionen in mehrere physische Infrastrukturen sind damit überflüssig
- Mit der Unified Access-Lösung von ALE können kabelgebundene und drahtlose Technologien als ein einziges, stabiles Netzwerk zusammenarbeiten mit einem gemeinsamen Angebot von Netzwerkdiensten, einem Richtlinienrahmen, einem gemeinsamen Authentifizierungsschema und einer zentralen Authentifizierungsdatenbank
- Die Netzwerklösungen von ALE verfügen außerdem über nur ein Managementsystem für alle Elemente der Infrastruktur; u. a. werden kabelgebundene LAN- und drahtlose WLAN-Netzwerke einheitlich verwaltet Das Alcatel-Lucent OmniVista® 2500 Network Management System und Alcatel-Lucent OmniVista® Cirrus Network Management as a Service für cloudbasiertes Management bieten eine zentrale Bedienoberfläche zur Verwaltung virtueller Umgebungen, Switches, Access Points und aller anderen Netzwerkkomponenten.

Ein leistungsstarkes Netzwerk-Portfolio

Switches, Access Points und Controller von ALE unterstützen die neueste Generation der Funktionen mit hoher Bandbreite und niedriger Latenz und sind in der Lage, eine große Anzahl von Geräten in Umgebungen mit hoher Dichte zu verwalten. Die Netzwerkprodukte und -lösungen von ALE erfüllen die Netzwerkanforderungen von Unternehmen jeder Größe. ALE bietet auch eine Auswahl an robusten Switches, Access Points und Routern für die Netzwerkbereitstellung im Außenbereich oder in rauer Umgebung an.

IoT-Szenarien in Schlüsselindustrien

IoT-Lösungen versprechen Unternehmen mehr Intelligenz und Erfolg. In bestimmten Branchen sind diese Vorteile besonders ausgeprägt.

Gesundheitswesen

Das Internet der Dinge (IoT) hat das Potenzial, das Gesundheitswesen zu revolutionieren: Es verändert, wie Krankenhäuser, Praxen und andere Pflegeeinrichtungen Daten sammeln und nutzen. Im IoT werden die wichtigsten Trends in Technologie und Wirtschaft Mobilität, Automatisierung und Datenanalyse zusammengeführt, um die Patientenversorgung zu verbessern. Die Daten, die diese Geräte sammeln, können anschließend zu folgenden Zwecken analysiert werden:

- Verbesserung der Patientenversorgung durch neue oder verbesserte Pflegeleistungen und Dienste, die zur Differenzierung in einer datengesteuerten Gesundheitseinrichtung beitragen
- Optimierung der Prozesse durch die Entwicklung neuer Dienstleistungen, Arbeitsabläufe und Lösungen, die die Effizienz steigern und die Betriebskosten senken
- Mehr Wissen über die Bedürfnisse und Präferenzen der Patienten und die Möglichkeit für Gesundheitseinrichtungen, eine individuellere Pflege und ein besseres Erlebnis zu bieten
- Smartere Krankenhausnetzwerke durch proaktive Überwachung kritischer Infrastrukturen und automatisierte Bereitstellung und Verwaltung der IT-Infrastruktur

Mit dem Einsatz des IoT im Gesundheitswesen wächst auch die Bedrohungslage: Je mehr Sensoren und verbundene Geräte, desto größer die Angriffsfläche im Netzwerk. Das IoT im Gesundheitswesen ist besonders anfällig, da bei der Herstellung vieler IoT-Geräte die Sicherheit nicht mitgedacht wird oder die Hersteller beim Thema Sicherheit nicht auf dem neuesten Stand sind. Folglich können IoT-Systeme potenziell das schwächste Glied in der Cybersicherheit von Krankenhäusern, Praxen und Pflegeeinrichtungen sein.

Bildungswesen

Bildungseinrichtungen sind in der Welt des IoT keine Ausnahme. Eine Welt, in der in jedes erdenkliche Produkt Technologie eingebaut wird. Das IoT bringt Universitäten und Schulen zahlreiche Vorteile: Es liefert eine neue Generation intelligenter Objekte, die das Lernerlebnis enorm verbessern und die Sicherheit auf dem Campus potenziell deutlich erhöhen. IoT-Geräte, ob klein wie ein Lichtsensor oder groß wie Smartboards, revolutionieren die Verwaltung ebenso wie die Art und Weise der Wissensvermittlung. IoT-Geräte:

- schaffen neue Wege des Lernens

  für Schüler und Studierende, da individuellere und dynamischere Lernerfahrungen unterstützt werden, z. B. durch immersive digitale Lehrbücher und spielbasiertes Lernen
- verändern, wie Lehrkräfte ihren Unterricht gestalten und Leistungen abprüfen mit smarten audiovisuellen Geräten, digitalen Videorekordern zur Aufzeichnung des Unterrichts und Online-Prüfungen
- vereinfachen den Betrieb für die Schulverwaltung durch proaktive Überwachung kritischer Infrastrukturen und effizientere, kostengünstigere Prozesse für das Management der HLK-Anlagen, Beleuchtung oder Grünanlagen
- schaffen ein sichereres Umfeld für Schüler, Studierende und Lehrkräfte durch digitale Überwachungskameras, intelligente Türschlösser und vernetzte Schulbusse

In diesen umgestalteten Schulen

und Universitäten lassen sich riesige Datenmengen über das Umfeld und die Leistungen der Schüler und Studierenden sammeln, speichern und analysieren. Dadurch erhalten die Einrichtungen eine Datenlage, die sie in die Lage versetzt, ihre Prozesse für den Erfolg der Schüler- und Studierendenschaft zu verbessern und zu ermitteln, welche Lücken noch zu schließen sind.

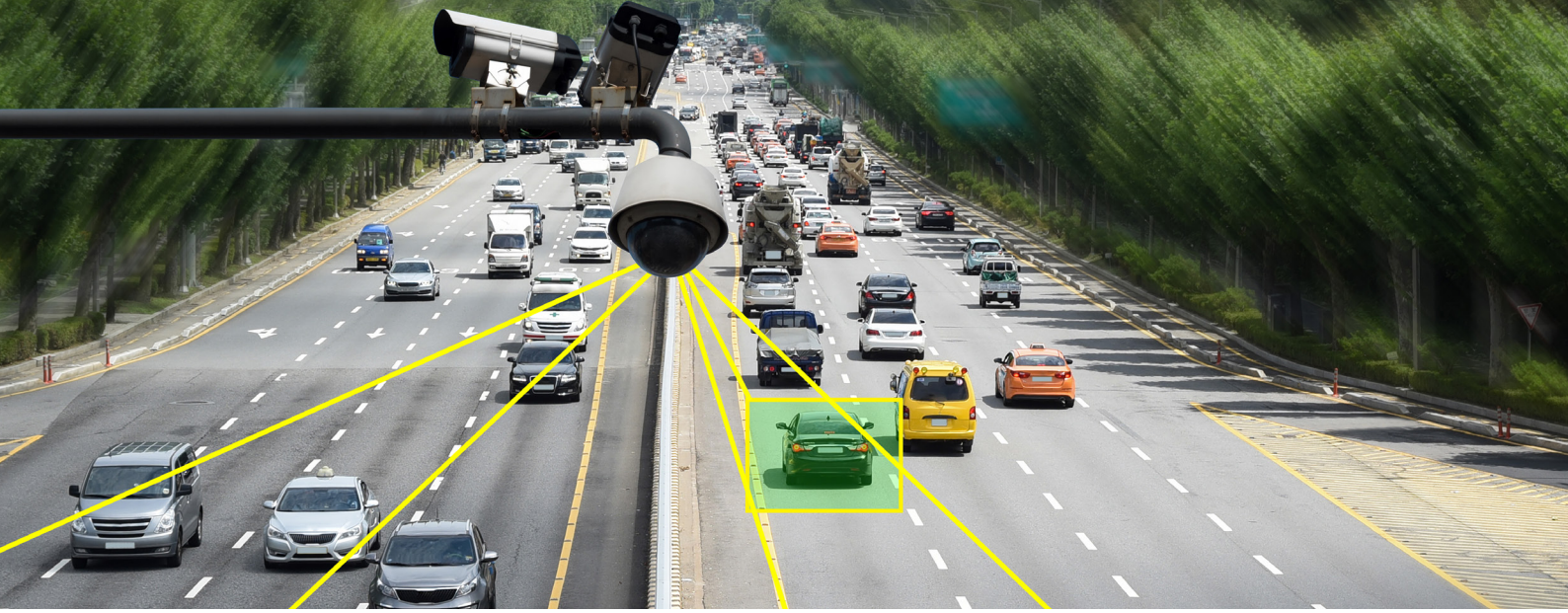
Diese Transformation bringt sowohl Chancen als auch Gefahren mit sich. Eine umfassende Verteidigungsstrategie, die in die Tiefe geht, ist zwingend erforderlich. Sie sorgt für eine sichere Verbindung zu den IoT-Geräten und verhindert Verletzungen des Datenschutzes und der Sicherheit der Forschung oder eine Gefährdung der Authentizität und Integrität der Daten.

Öffentlicher Sektor

Staatliche Stellen und Kommunen springen auf den IoT-Zug auf. Intelligente Städte bieten große Geschäftschancen und neue Möglichkeiten, sich in den Dienst der Bürger zu stellen und sie zu schützen. In diesen vernetzten Städten setzen die Versorger verstärkt intelligente Zähler ein, um anpassungsfähige Preissysteme zu schaffen, und Immobilienentwickler statten Neubauten mit Sensoren und Automatisierungskomponenten aus. Intelligente Parkplätze sparen den Bewohnern der Städte Zeit und sind effizienter, und intelligente Abfalleimer melden, wenn sie fast voll sind. Das Internet der Dinge hilft Kommunen und Behörden bei der Erfassung von Mobilitätsdaten und Datentrends, die die Grundlage kritisch wichtiger Analysen bilden, die wiederum für die Formulierung von Strategien für Städte und für eine langfristige Planung unverzichtbar sind. IoT sorgt für:

- Bessere Vernetzung der Bürger und Einrichtungen der öffentlichen Hand, um reaktionsschnell qualitativ hochwertige und sichere Dienstleistungen und Ressourcen bereitzustellen, die das Engagement und das Vertrauen zwischen Behörden und den Bürgern, für die sie da sind, dadurch verbessern, dass sich durch sie Lebensqualität, Arbeitsfähigkeit und Nachhaltigkeit erhöhen
- Erhöhte Sicherheit im Nahverkehr durch weitreichende Kenntnisse über den Betrieb der Verkehrssysteme mit Hilfe von Sensordaten, die alles von einer auffälligen Geschwindigkeit der Stadtbahnen über Straßentemperaturen bis hin zum Echtzeit-Standort der Nahverkehrsbusse erfassen
- Weniger Staus und Energieverbrauch durch Smart City-Technologien, die Echtzeitdaten nutzen, um die Skalierbarkeit der Ressourcen zu verbessern, damit gestiegene Anforderungen erfüllbar sind. Sie bieten die notwendige Flexibilität, um rasch auf schnell wechselnde Verkehrsmuster, Schwankungen beim Wasser- oder Energieverbrauch oder Veränderungen der Luftqualität zu reagieren
- Verbesserte Betriebsleistung und Wartung durch proaktive Überwachung kritischer öffentlicher Infrastrukturen und effizientere Prozesse zur Senkung der Betriebskosten und Verbesserung der Systemkapazitäten
- Verbesserung der öffentlichen Sicherheit durch schnellere und effektivere Reaktion auf Notfälle

Die Messlatte für die Cybersicherheit muss jedoch hoch – sehr hoch – gelegt werden. In IoT-vernetzten Städten, in denen nicht alle Anwendungen, Sensoren und Geräte mit Blick auf eine hohe Sicherheit entwickelt wurden, ist eine intelligente und automatisierte Infrastruktur erforderlich, die diese Geräte in Kategorien einteilt und verhindert, dass sie mit Geräten kommunizieren, mit denen eine Kommunikation nicht beabsichtigt ist. Diese Containerisierung trägt erheblich zu mehr Sicherheit bei und überführt die öffentliche Einrichtung in eine Zero-Trust-Umgebung, bei der auf mehreren Ebenen, in Form einer Cyberstrategie nach dem Ansatz „Defense-in-Depth“, für Schutz gesorgt ist.



Transportwesen

Das Internet der Dinge (IoT) verändert die Verkehrsbranche: Wie Systeme Daten und Informationen sammeln, wird durch die Verknüpfung von Automatisierung und Datenanalyse grundlegend verändert. Sensoren, Aktoren und andere Geräte sind in der Lage, Daten über die Aktivitäten im Netz in Echtzeit zu sammeln und zu übermitteln. Diese Daten können dann von den Verkehrsbehörden analysiert werden, um das Reiseerlebnis und die Sicherheit der Reisenden zu verbessern, Staus zu reduzieren und den Energieverbrauch zu senken und gleichzeitig die betriebliche Leistung zu optimieren.

Das IoT steht im Mittelpunkt der Transformation des Verkehrs und sorgt für mehr Sicherheit, effizienteres Reisen, verbesserte Fahrzeug- und Flugzeugwartung und ein strategischeres Verkehrsmanagement. Beispiele für IoT-Anwendungen im Verkehrssektor:

- Effizienzsteigerungen, um die Systemkapazität zu erhöhen und die Sicherheit und den Komfort der Fahrgäste zu verbessern und gleichzeitig Kosten und Risiken zu senken
- Dynamische straßenseitige Anzeigetafeln für intelligente Verkehrssysteme, die in Echtzeit den Straßenzustand, Mautgebühren, Fahrbahnsperrungen und Fahrzeiten anzeigen
- Autonome Fahrzeuge, die in der Lage sind, ihre Umgebung zu erkennen, Verhalten vorherzusagen, mit anderen Fahrzeugen und ihrer Umgebung zu kommunizieren und sofort auf reale Verkehrssituationen zu reagieren
- Videoüberwachung, um die Bewegung von Menschen und Menschenmengen zu beobachten und verdächtiges Verhalten und unbeaufsichtigtes Gepäck frühzeitig und automatisch zu erkennen

Cyberangriffe können das Tagesgeschäft für längere Zeit beeinträchtigen. Nicht nur, dass die Dienste unterbrochen sind, auch die Preisgabe hochsensibler Daten stellt in diesem Sektor ein großes Risiko dar. Während einige Angriffe auf die Cybersicherheit darauf abzielen, Geld zu erpressen, sollen andere Versuche Chaos und Verwirrung stiften, indem sie ganze Systeme lahmlegen. Störung von Verkehrsampeln, Blockieren des Zugriffs auf wichtige Dateien und Daten, Unterbrechung von Lohnabrechnungsvorgängen und Beeinträchtigung von Fahrkartenautomaten und Fahrkartenschaltern sind nur einige Beispiele.

- 2018 wurde Bay & Bay Transportation Opfer eines massiven Ransomware-Angriffs auf die Systeme, mit denen das Unternehmen seine Flotte von 300 Lkw managt.
- Im Jahr 2018 legten Hacker 2.000 Computer des Verkehrsministeriums von Colorado lahm und blockierten damit wochenlang den Betrieb. Kürzlich sind Cyberkriminelle in drei von 18 Computersystemen der New Yorker Metropolitan Transit Authority eingedrungen.
- In der ersten Jahreshälfte 2020 wurde ein atemberaubender Anstieg von Ransomware-Vorfällen verzeichnet: insgesamt +715 % im Vergleich zum Vorjahr
- Im Jahr 2020 wurden die E-Mail-Adressen und Reisedaten von 9 Millionen EasyJet-Kunden gestohlen. Bei 2.208 dieser Kunden waren anschließend die Daten ihrer Kreditkarten kompromittiert. Dieser Cyberangriff und die Auswirkungen der weltweiten Pandemie führten dazu, dass die Fluggesellschaft 45 % ihres Aktienwerts verlor und den ersten Jahresverlust in ihrer 25-jährigen Geschichte verzeichnete.

Sichere IoT-Netzwerke und IoT-Strategien sind möglich

Die Produkte und Lösungen von ALE schaffen ein sicheres Netzwerk als Fundament. Dieses unterstützt Unternehmen bei der Implementierung von IoT-Systemen, welche Erkenntnisse zur Optimierung von Produkten und Prozessen liefern, Organisationen intelligenter und effizienter machen und ein besseres Kundenerlebnis liefern. Die Strategien für IoT-Containment und mehrstufige Sicherheit von Alcatel-Lucent Enterprise reduzieren die Risiken und vereinfachen die Einrichtung von IoT-Netzwerken, indem sie die Einbindung von Geräten erleichtern, einen effizienteren Betrieb ermöglichen und die Sicherheit deutlich erhöhen. ALE hilft Unternehmen, das volle Potenzial des IoT auszuschöpfen, indem es ein höheres Maß an Netzwerkintelligenz, Automatisierung und Sicherheit bietet.

Sie möchten noch mehr über dieses Thema wissen?

Weitere Informationen zu den IoT-Lösungen von ALE finden Sie unter ALE IoT-Sicherheit.

Alcatel·Lucent Enterprise