Blindes Vertrauen war gestern: Das neue Sicherheitsparadigma für die digitale Logistik

Rentabilität mit mobilen industriellen Robotern steigern

Autor:
Denis Niezgoda
Chief Commercial Officer International
Locus Robotics
www.locusrobotics.com

Moderne Lagerumgebungen arbeiten heute, dank mobiler Automatisierungslösungen, mit beeindruckender Präzision. Durch ein harmonisches Zusammenspiel von Mensch und Technologie werden Abläufe beschleunigt, Durchlaufzeiten verkürzt und dadurch die gesamte Prozesseffizienz enorm gesteigert. Um diese technologische Leistungsfähigkeit zu erreichen, bedarf es jedoch einer hochkomplexen digitalen Infrastruktur. In dieser sind Steuerung und Planung der Warenflüsse, automatisierte Kommissionierung, Bestandsverwaltung, Transportlogistik, Sicherheits- und Zugriffssysteme sowie die Vernetzung mit Lieferkettenmanagement und Echtzeitüberwachung eng miteinander verzahnt.

Autonome mobile Roboter

Insbesondere autonome mobile Roboter (AMR) werden dabei zunehmend zu erfolgsentscheidenden Werkzeugen innerhalb dieser vernetzten Logistik. Eingebunden in ein Ökosystem aus Sensoren und dirigiert von KI-gestützten, cloudbasierten Steuerungsplattformen, sorgen sie dafür, dass Betreiber von Lagerumgebungen auch in Spitzenzeiten und angesichts eines anhaltenden Arbeitskräftemangels hochflexibel und maximal erfolgreich arbeiten können. Diese umfassende digitale Vernetzung hat sich damit längst zum Motor moderner Lagerlogistik entwickelt. Doch mit jedem digitalen Knotenpunkt, jeder Datenverbindung und jeder Schnittstelle wächst auch die Angriffsfläche für Cyberkriminelle.

Wenn Lieferketten zum Einfallstor werden

Forscher des Massachusetts Institute of Technology kamen im Rahmen einer aktuellen Studie [1] zu dem Ergebnis, dass die Migration in Cloud-Umgebungen, vernetzte Lieferkettenstrukturen und die maschinenübergreifende Kommunikation Schwachstellen schaffen, die mit herkömmlichen Schutzkonzepten nicht mehr beherrschbar sind. Öffentlich zugängliche Netzwerkzugänge, heterogene Sicherheitsstandards und fragmentierte IT-Landschaften bieten Angreifern zahlreiche Ansatzpunkte. Hinzu kommen Risiken in der Automatisierungstechnik selbst sowie an den Schnittstellen zwischen menschlichen Bedienern und Maschinen. Traditionelle Sicherheitsmaßnahmen – meist eine Firewall als Schutzwall um das Unternehmensnetzwerk – haben als alleinige Sicherheitsinstanzen ausgedient.

Existenzielle Bedrohung

Die Zahlen sprechen eine klare Sprache: Die Dimension der dadurch herrschenden Gefahr lässt sich nicht länger ignorieren. Der Digitalverband Bitkom zeichnete bereits 2024 ein dramatisches Bild [2]: 81 Prozent aller deutschen Unternehmen wurden innerhalb von zwölf Monaten Opfer von Datendiebstahl, Spionage oder Sabotage – ein Anstieg von neun Prozentpunkten gegenüber dem Vorjahr. Der volkswirtschaftliche Schaden erreichte infolgedessen die Rekordmarke von 266,6 Milliarden Euro, eine Steigerung um 29 Prozent. Allein durch Cyberkriminalität hatte die deutsche Wirtschaft Verluste von 178,6 Milliarden Euro zu beklagen, wobei Ransomware und Phishing die bevorzugten Angriffsmethoden darstellen.

Noch alarmierender ist die Tatsache, dass 65 Prozent der betroffenen Firmen ihre Existenz durch Cyberattacken aktuell real bedroht sehen. Im Jahr 2021 lag der Wert noch bei lediglich 9 Prozent. Diese Entwicklung macht deutlich, dass digitale Sicherheit längst kein optionales Zusatzfeature mehr darstellt, sondern sicherheits- und erfolgsentscheidend ist. Betriebsunterbrechungen, Lieferausfälle und Datenverluste gefährden nicht nur Wertschöpfungsketten, sondern auch das mühsam aufgebaute Vertrauen von Kunden und Geschäftspartnern.

Never Trust, Always Verify

Das neue Sicherheitsparadigma: Die erfolgversprechendste Antwort auf diese Bedrohungslage heißt Zero Trust. Dieses Sicher-

heitskonzept bricht radikal mit bisherigen Logiken, denn es geht nicht mehr davon aus, dass Nutzer und Geräte innerhalb des Firmennetzwerks automatisch vertrauenswürdig sind. Stattdessen gilt, dass jeder Zugriff – von innen wie von außen – kontinuierlich überprüft, authentifiziert und autorisiert werden muss. Zero Trust funktioniert dabei wie eine digitale Grenzkontrolle, die bei jeder Transaktion Identität, Berechtigung und Herkunft akribisch prüft.

Strategiewechsel

Dieser Strategiewechsel ist schon lange überfällig, denn manipulierte Software, kompromittierte Nutzerkonten und gezielte Phishing-Attacken überwinden traditionelle Perimeterschutzmaßnahmen längst mühelos. Laut dem Analystenhaus Gartner [3] werden bis Ende 2025 mindestens 60 Prozent aller Unternehmen weltweit eine Zero-Trust-Strategie implementiert haben. Insbesondere die Logistikbranche ist hier besonders gefragt, da ihre komplexen, weitverzweigten Strukturen sie zu einem besonders lohnenden Ziel machen.

Sichere Automatisierung

Zero Trust in der Praxis: Führende Anbieter autonomer mobiler Roboter, wie etwa Locus Robotics, haben Zero Trust bereits von Beginn an in ihre Systemarchitektur integriert. Die Roboterflotten kommunizieren ausschließlich über verschlüsselte, private Netzwerke. Jede Datenübertragung durchläuft mehrfache Authentifizierungsstufen, wobei Kontroll- und Datensysteme strikt getrennt voneinander arbeiten. Diese Architektur isoliert potenzielle Schwachstellen und ermöglicht es, Bedrohungen frühzeitig zu identifizieren und zu neutralisieren.

Spezifische Risiken

Gerade bei autonomen Systemen zeigen sich spezifische Risiken: GPS-Spoofing kann Roboter fehlleiten, Funkstörungen die Kommunikation unterbrechen oder unsichere Betriebssysteme Einfallstore öffnen. Das Zero Trust Maturity Model [4] der US-amerikanischen Cybersecurity and Infrastructure Security Agency definiert fünf zentrale Schutzebenen: Identität, Gerät, Netzwerk, Applikation und Daten. Moderne Sicherheitskonzepte kombinieren daher verschlüsselte Netzwerke, mehrstufige Authentifizierung, dynamische Zugriffsrechte und verhaltensbasierte Zugriffskontrolle.

Identity & Access Management

Besonders das Identity & Access Management hat sich hierbei besonders bewährt. Dieses Framework verwaltet digitale Identitäten in Echtzeit und passt Berechtigungen dynamisch an aktuelle Verhaltensmuster an. So lässt sich präzise steuern, wer auf welche Ressourcen zugreifen darf – wodurch Sicherheitsrisiken unmittelbar minimiert werden.

Der unterschätzte Faktor Mensch

Doch selbst die ausgefeilteste Technologie bleibt wirkungslos, wenn der Mensch zur eigentlichen Schwachstelle wird. Social Engineering – die gezielte Manipulation von Menschen mit der klaren Absicht, sie zur Preisgabe vertraulicher Informationen zu bewegen oder sicherheitsgefährdende Handlungen auszuführen – zählt nach wie vor zu den erfolgreichsten Angriffsmethoden. Nur durch kontinuierliche Schulungen, gezielte Awareness-Programme und eine gelebte Sicherheitskultur lässt sich dieses Risiko in Unternehmen effektiv und nachhaltig eindämmen. Zero Trust darf deshalb nicht allein als reine IT-Initiative verstanden werden, sondern muss fest im Unternehmensbewusstsein verankert sein.

Strategischer Vorteil durch umfassenden Schutz

Die Einführung von Zero Trust ist mehr als eine Schutzmaßnahme – sie ist ein strategischer Wettbewerbsvorteil. Unternehmen, die diesen Ansatz konsequent umsetzen, erfüllen nicht nur regulatorische Anforderungen wie ISO 27001, NIST oder den BSI IT-Grundschutz. Vielmehr stärken sie ihre Resilienz, schützen sich effektiver vor Bedrohungen und bauen Vertrauen bei Kunden und Partnern auf. KI-gestützte Threat-Intelligence-Systeme ermöglichen es zudem, Angriffe schneller zu erkennen und gezielter abzuwehren.

Digitale Sicherheit

Eine fortwährende Reise: Die Weiterentwicklung von Logistiksystemen schreitet kontinuierlich voran und parallel dazu wandelt sich auch das Spektrum und die Intensität von Cyberbedrohungen. Technologische Innovationen wie etwa die Blockchain für mehr Lieferkettentransparenz, digitale Zwillinge oder der 5G-Mobilfunkstandard stellen fortlaufend neue Anforderungen an die IT-Sicherheit. Unternehmen, die ihre Wettbewerbsfähigkeit und das Vertrauen ihrer Kunden und Partner bewahren möchten, müssen Sicherheit als dauerhaften Transformationsprozess verstehen. Das Zero-Trust-Prinzip stellt kein zeitlich begrenztes Projekt dar, sondern beschreibt einen fortwährenden Entwicklungspfad zu einer resilienten und zukunftsfähigen Logistik. ◄

Referenzen

[1] https://omnichannel.mit.edu/wp-content/uploads/2025/02/MIT_OmnichannelSupplyChain_WarehouseFutureVulnerabilities_2025_FullReport.pdf
[2] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024
[3] https://www.gartner.com/en/newsroom/press-releases/2023-05-10-gartner-predicts-zero-trust ps://www.cisa.gov/zero-trust-maturity-model