Ohne Normen keine Cybersicherheit

Wie Normen das Schutzniveau vor Cyberattacken stärken

Bei vielen Unternehmen hält das Risikomanagement mit der digitalen Transformation nicht mehr Schritt. Die beschleunigte Digitalisierung von Kernprozessen hat im Zuge der Pandemie die Lücken vergrößert: Kriterienkataloge für neue Schadensereignisse werden unregelmäßig aktualisiert. Selten findet eine ganzheitliche Folgenabschätzung potenzieller Cyberattacken auf den eigenen Betrieb und dessen Lieferkette statt.

Andreas Resmann

Analysten schätzen, dass sich die durchschnittlichen Gesamtkosten für die Wiederherstellung und Ausfallzeit eines blockierten IT-Systems innerhalb eines Jahres von etwa 760.000 auf 1,8 Millionen US-Dollar mehr als verdoppelt haben. Hinzu kommen Cybergefahren durch die weltweiten Sanktionen gegen russische Unternehmen sowie Folgen und Kollateralschäden des Russland-Ukraine-Kriegs auf Dateninfrastrukturen.Aktuelle Top Cyberrisiken für Unternehmen und Infrastrukturen sind:

- Zero-Day-Angriffe über bislang unbekannte Schwachstellen in der Software,
- Ransomware-Angriffe und Erpressung mit Schadsoftware über Internet und Intranet,
- Identitätsdiebstahl, Social Engineering, Phishing,
- Einschleusen von Schadsoftware in die

Netzwerke (OT, IT) mittels externer Geräte und
- Einbruch in Fernzugängen von Zulieferern, Dienstleistern oder Wartungsservices (MSP).

Einen Eindruck über die Hebelwirkung moderner, professionellen Cyberkriminalität bot der Angriff auf den US-IT-Dienstleister Kaseya. Eine sogenannte Zero-Day-Attacke ging voraus, die Schwachstellen einer Software ausnutzt, bevor der Hersteller die Lücke erkennen und schließen kann. Bei dem auf Wartungssoftware spezialisierten IT-Dienstleister schleusten Angreifer ein schadhaftes Update in die Virtual System Administrator-Software (VSA) ein und erpressten nach erfolgreicher Verschlüsselung 70 Millionen US-Dollar Lösegeld. Die Attacke löste einen Domino-Effekt aus. Die verschlüsselte Abrechnungssofortware blockierte die Clients von Firmen und Händlern weltweit. Zur Schadensbegrenzung mussten sie ihre Server abschalten – so auch eine Supermarktkette in Schweden, die vorübergehend ihre Filialen schloss. Laut US-Behörden waren von der Attacke zwölf Länder betroffen, allein in den USA über 200 Unternehmen.

Fundamente für die Cybersicherheit und IT-Compliance

Entschlossene Angreifer sind jederzeit in der Lage, neue Schwachstellen in weitverbreiteten Serverprogrammen zu nutzen und ihre Cyber-Attacken auf Lieferketten auszudehnen. Die zentralen Fragen lauten daher, inwiefern die bisherigen Prozesse auf Cybersicherheit ausgelegt sind und Schutz bieten vor:
- dem Ausfall von Geräten,
- der Manipulation von Daten und Software und
- vor unautorisierten Zugriffen auf sensible, personalisierte Informationen.

Wie die Praxis zeigt, setzen Unternehmen mit einem hohen Reifegrad bei der IT-Sicherheit vor allem organisatorische Maßnahmen um und sie sensibilisieren sämtliche Anwender kritischer IT-Prozesse für die vielschichtigen Bedrohungspotenziale. Mittlerweile tarnen Cyberkriminelle ihre Angriffe, indem sie den Betriebszustand imitieren, während das bereits infiltrierte Unternehmen keine Störungen feststellt. Folglich sollten Unternehmen selbst dem Normalzustand misstrauen, vorausschauend mit einem Frühwarnsystem nach Bedrohungen suchen, um einschleichende Angriffe aufzudecken und Schutzmaßnahmen einleiten zu können. Voraussetzung ist die Definition von Indikatoren (z. B. Datenverkehr, Scan-Aktivitäten), die den Normalzustand als Grundzüge eines sicheren Systembetriebs beschreiben und bei Abweichungen bzw. untypischen Interaktionen Abwehrmaßnahmen auslösen können.

Konzepte zur Cybersicherheit müssen über die reine Prävention vor IT-Ausfällen hinausgehen. Eine robuste Resilienz, die vielfältige digitale Transformationsrisiken berücksichtigt, baut auf der Bestandsaufnahme sensibler Systemkomponenten auf. Gerade mit der klassischen Dokumentation aus dem Qualitätsmanagement kön- »»

INFORMATION & SERVICE

LITERATUR

VDA-Band ACSMS 2020: Automotive Cybersecurity Managementsystem Audit

AUTOR

Andreas Resmann ist Vice President Service Division Audit bei DEKRA SE.

KONTAKT

Andreas Resmann
andreas.resmann@dekra.com

nen sich Betriebe ein Fundament legen, um die veränderten IT- und Sicherheitsanforderungen der Lieferkette, der Kunden und der Stakeholder zu verstehen und auf Attacken vorbereitet zu sein.

Mit dieser inhaltlichen Grundlagenarbeit können Risiken teils schneller erkannt werden als mit einem einseitigen Fokus auf die technische Ausrüstung. Auch wenn kein Standard die Dynamik der Digitalisierung in Gänze erfassen kann, sind Unternehmen dennoch gut beraten, mit einem Framework aus zentralen Richtlinien und Normen die Cybersicherheit auf ein belastbares Fundament zu stellen, um so die technischen Maßnahmen steuern und anpassen zu können.

Vorteil mit Europäischer Datenschutzgrundverordnung

Mit den Anforderungen der DSGVO entwickeln Unternehmen wichtige Maßnahmen gegen Datenschutzrisiken, die implizit auch mit einer verbesserten Cybersicherheit zusammenhängen. Zentral ist die *Datenschutz-Folgenabschätzung*, wenn eine Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko für Rechte und Freiheiten betroffener Personen zur Folge hat. Die Betroffenenrechte müssen in den Geschäftsabläufen des Unternehmens abgebildet und gegenüber den Betroffenen umgesetzt werden, etwa:

- das Recht auf Löschung,
- das Recht auf Datenübertragbarkeit sowie
- die Informationspflichten des Verantwortlichen gegenüber dem Betroffenen.

Informationssicherheits-Managementsystem nach ISO 27001

Aus der internationalen Norm ISO 27001 leiten sich mittlerweile die meisten IT-Sicherheitsstandards ab. Dort wo Betriebe bereits über ein zertifiziertes QM-System nach ISO 9001:2018 verfügen sowie die kritischen IT-Prozesse und -Komponenten erfasst sind, existieren bereits wichtige Grundlagen für ein integriertes Sicherheitsmanagementsystem nach ISO 27001.

Als grundlegende Prämisse fordert die Norm, die relevanten externen und internen Geschäftsvorgänge zu verstehen und zu beschreiben. Dazu gehört u.a. eine Inventarisierung aller Betriebsmittel und Systemkomponenten, die mit Daten oder Datenverarbeitenden Einrichtungen im Zusammenhang stehen. Die regulatorischen Vorgaben sowie die Schnittstellen und Abhängigkeiten mit anderen Unternehmen sind ebenso zu dokumentieren. Das Unternehmen muss einen Plan zur Risikobehandlung formulieren, Sicherheitsziele für relevante Funktionen und Ebenen festlegen und sie stets auf dem aktuellen Stand halten. Bei Vorfällen und Ereignissen in der IT-Sicherheit (Incident Management-Verfahren) muss es Verhaltens- und Reporting-Regeln geben. Die Norm enthält im Anhang einen breiten Katalog an Zielen und Maßnahmen, um das eigene Sicherheitsniveau zu bewerten.

Cyber Security Management System im Automobilsektor

In der Automobilbranche wird deutlich, wie Cybersicherheit nur noch mit einem breiten strategischen Managementansatz zu erreichen ist. Die Mobilität vernetzt sich auf allen Ebenen: über Internet, Wi-Fi, Bluetooth und Sensoren (Infotainment, Verkehrsdaten, Assistenzsysteme, OTA (Over-The-Air) Updates, Mobilitätsdienstleistungen etc.). Damit sind nicht nur Hersteller und ihre Lieferkette, sondern auch die Fahrzeuge Zielscheibe von IT-Manipulationen und Remote-Angriffen. Ein hohes Sicherheitsniveau muss daher die elektrisch-elektronische Architektur in allen Produktionsstufen und über den gesamten Lebenszyklus eines Fahrzeugs vor Cyberattacken schützen – von der Entwicklung bis zur Außerbetriebsetzung.

Mit Blick auf die Zukunftsfelder der Automobilindustrie (Connected Car, energieeffiziente Antriebskonzepte, automatisiertes Fahren) werden Sicherheitsstrategien deutlich, wie künftig ein *Cyber-Security-Management-Systems (CSMS)* sämtliche Strukturen der Produktions- und Lieferkette einbezieht. Ab Juli 2022 verlangt die EU deshalb die Implementierung eines CSMS für jeden neuen Fahrzeugtyp. Ab Juli 2024 ist ein CSMS für alle Neufahrzeuge verpflichtend.

Die Anforderungen stellen für die Pro-

duktsicherheit in der Automobilbranche einen Paradigmenwechsel dar. Hersteller müssen den Zulassungsbehörden künftig darlegen, dass sie ein CSMS für das Gesamtfahrzeug und nicht nur für einzelne Systeme und Komponenten eingeführt haben. Die Regularien bestimmen, dass Hersteller über die gesamte Lebensdauer eines Fahrzeugs ein Managementsystem sowohl für Cyber Security (UN-R 155) als auch für Software Updates (UN-R 156) betreiben müssen. Die Genehmigungsbehörden prüfen für jede technische oder Software gestützte Komponente, ob das Risiko für einen Cyberangriff auf angemessen Weise bewertet wurde und Minderungsmaßnahmen zur laufenden Überwachung bestehen. Die Managementsysteme müssen im dreijährigen Turnus durch Audits überprüft werden.

Weltweite geltende neue Regelwerke

Die Cybersicherheits-Anforderungen für Fahrzeuge basieren auf den weltweit geltenden neuen Regelwerken *WP.29 UN ECE* und *ISO/SAE 21434*. Allerdings ist die ISO 21434 derzeit von keiner Akkreditierungsstelle als 3rd-Party-Zertifizierungsstandard anerkannt. Die Norm beschreibt die Umsetzung der R155. Die zur Auditierung dazugehörige Beschreibung des Auditverfahrens (ISO/PAS 5112) ist im März 2022 veröffentlicht worden.

Die Regelungen nach UN ECE gehen momentan über den Geltungsbereich des ISO/SAE-Standards hinaus, weil WP.29 auch die Kommunikation zu Clouds, zu anderen Fahrzeugen oder zu digitalen Verkehrsleitsystemen umfasst. Zwar ist noch nicht endgültig geklärt, inwiefern auch Backendsysteme für die Typenzulassung relevant sind, doch die Praxis des Connected Car wird darauf hinauslaufen, dass ein Cyber-Security-Management-Systems nach ISO/SAE 21434 sämtliche Strukturen der digitalen Mobilität einbeziehen wird.

Fahrzeughersteller (OEM) müssen entsprechend der UNECE die Risiken in der Supply Chain überblicken und steuern, wobei ein international anerkannter Standard zur *3rd-Party-Auditierung* der gesamten Supply Chain derzeit nicht verfügbar ist. Um die geltenden Fristen halten zu können, konzentrieren sich Homologationsbehörden (z.B. Kraftfahrtbundesamt) bei ihren Überprüfungen derzeit darauf, ob die OEM die Anforderungen der *UN-R 155* erfüllen.

Software Update Management System (SUMS)

Gemäß *UN ECE R-156 / ISO 24089* (aktuell im Entwurfsstadium) müssen Updates von Software-Funktionen, die für die Typgenehmigung relevant sind (z. B. Abgas-, Brems-, Motorsteuerung) so entwickelt und validiert werden, dass sie auch nach dem Update noch gesetzeskonform arbeiten.

Weil bereits ab 2024 alle neu produzierten Fahrzeuge die Verordnung erfüllen müssen, kann es für Hersteller möglicherweise vorteilhaft sein, auf Update-Fähigkeiten einzelner Komponenten zu verzichten. Dadurch entfällt die Pflicht, ein *SUMS* auf solche Komponenten auszuweiten. Werden solche Komponenten von Zulieferern bereitgestellt, so kann ein Fehler nur noch durch Austausch einer ganzen Komponente behoben werden. Die hätte wiederum ein erhöhtes Gewährleistungsrisiko des Zulieferers zufolge.

Gap-Analyse anhand bestehender Managementsysteme

Im Kontext *Connected Car* hat in der Automobilbranche nahezu jeder Unternehmensbereich Auswirkungen auf die Cybersicherheit der Organisation und der Produkte. Unternehmen sollten daher die Grundlagen für die Sicherheitsanforderungen künftiger Typenzulassungen anhand bestehender Frameworks entwickeln. Dabei unterstützt eine Gap-Analyse anhand bestehender Managementsysteme.

Zur Vorbereitung eignet sich beispielsweise die weltweit harmonisierte, technische Spezifikation *IATF16949*. Mit ihrer prozessorientierten Ausrichtung auf Key Performance Indicators (KPI) konnten bereits viele Zulieferbetriebe ihre Prozessqualität im Automotive-Sektor verbessern. Weil dieser Standard auf der Struktur der IS 9001 basiert und insbesondere die Bereiche Entwicklung, Fertigung und Wartung im Fokus hat, bietet er auch Grundlagen für Cyber-Security.

Gleiches gilt für das *TISAX-Assessment VDA-ISA*, um in der Automobilindustrie den Nachweis der Informationssicherheit in der Lieferkette zwischen Herstellern, Zulieferern und Dienstleistern zu erleichtern. Zudem bietet der VDA-Band ACSMS 2020 (Automotive Cybersecurity Managementsystem Audit) für die 2nd Party- Auditierung des CSMS einen hilfreichen Fragenkatalog mit einem Bewertungsschema.

Fazit: Die skizzierten Wege zeigen, dass die Normen keine Technologien zur Stärkung der Cybersicherheit präferieren. Eine Norm allein wird Fahrzeuge nicht sicherer machen, jedoch eine weit gefasste Sicherheitskultur im Unternehmen und in der Lieferkette.

Um die Cybergefahren möglichst gering zu halten, müssen strenggenommen alle Komponenten und Systeme als unsicher eingestuft werden. Hier bietet das Qualitätsmanagement wichtige Grundlagen, um darauf aufbauend mit allen verfügbaren Informationen effektive Sicherheitsmaßnahmen einführen und steuern zu können. Erst wenn das Bewusstsein für Cybersicherheit in der Unternehmensstrategie, der gesamten Prozesslandschaft und über alle Wertschöpfungsstufen verankert ist, kann in den datengetriebenen Märkten und Geschäftsmodellen ein hohes Schutzniveau entstehen. ■