Cybersecurity-Herausforderungen angehen

Priorisierung verschafft Ruhe im Auge des Change-Orkans

Die Automobilindustrie befindet sich in einem beispiellosen Transformationsprozess. Hinzu kommen enorme Herausforderungen bei der Absicherung digitaler Lieferketten gegen Cyberangriffe. Cybersecurity-Anbieter Asvin sorgt mit kontextbezogener Risikoanalyse für Übersicht beim Stressabbau.

Von Jürgen Frisch, freier Journalist aus Leinfelden-Echterdingen

Wenn der Körper geschwächt ist, haben Viren und gutgemeinte Ratgeber ein leichtes Spiel. Software-Defined Vehicles verdrängen Verbrenner, Mobilität verschiebt sich von PS zu Convenience. Als böte das allein nicht genug Anlass zu Sorge, setzen Hacker und Regulierer noch eins drauf. Immer perfidere Angriffe auf der einen, immer umfangreichere Regulierungsvorgaben auf der anderen Seite setzen die Autobauer zusätzlich unter Druck.

Allein in Deutschland wurden 2023 laut Bitkom durch Cyberangriffe Schäden in Höhe von 148 Mrd. Euro verursacht. Gleichzeitig wollen die EU und internationale Verbände ihre Industrien auf aktuelle Cybersicherheits-Level heben und ihnen dadurch neue Wettbewerbsvorteile verschaffen. Letzteres ist gut gemeint, aber schlecht gemacht, denn auf dem Weg von der EU-Vorgabe NIS 2 bis zur Umsetzung in nationales Recht vergehen Jahre der Unsicherheit. Darum ächzen die Unternehmen derzeit darunter, dass sie sich zusätzlich zum Transformationsdruck um Compliance kümmern müssen. Weltweit liegen enorm viele nationale sowie internationale Rechtsvorschriften auf diesem Gebiet vor, von denen etwa die Hälfte noch einige Jahre benötigen, bis sie zur Geltung gelangen. Auch das erzeugt Unsicherheit.

Big Tech und Regulierung nehmen OEMs in den Zangengriff

Die NIS-2-Verordnung (Network and Information Security Directive) der EU befindet sich bereits kurz vor der Umsetzung, der Cyber Resilience Act (CRA) wird noch rund zwei Jahre brauchen. Bereits wirksam und auch umgesetzt für vernetzte Fahrzeuge sind UNECE R 155 und R 156. Derweil stehen entwicklungs- und produktionsfokussierte OEMs finanzstarken oder staatlich gelenkten Wettbewerbern gegenüber, die in branchenfremden Marktsegmenten wie Big Tech Monopole bilden oder die unter Niedriglohn- und regulierungsarmen Bedingungen operieren, beispielsweise in China. Kein leichtes Umfeld für Produkt- und Security-Verantwortliche, die ihre neue Position im Mega-Wachstumsmarkt New Mobility finden und besetzen müssen.

Gerhard Steininger ist VP Sales und Business Development bei Asvin in Stuttgart. Er war zuvor Projektleiter bei einer international tätigen

Die UNECE-Cybersecurity-Richtlinie

Die UNECE R 155 regelt das Thema Cybersecurity für die Automobilbranche beispielsweise mit Maßnahmen für ein Cybersecurity-Management-System (CSMS) und spezielle Cybersecurity-Typgenehmigungen für Fahrzeuge. Die UNECE R.156 betrifft das Software-Update-Management-System (SUMS); alle zertifizierungsrelevanten Software-Updates müssen entsprechend dokumentiert werden. Zulassungen nach diesen Standards laufen aktuell in den weltweit 54 UNECE-Ländern mit mehr als 32 Mio. Fahrzeugen pro Jahr. (ih)

Bild: by-studio/stock.adobe.com

Beratungsfirma und hat dort große Security-Projekte im Automotive-Umfeld geleitet. Ihm zufolge sind die Herausforderungen in der Automobilbranche bezüglich Cybersecurity vielfältig, aber beherrschbar. Wichtig sei jedoch eine klare Segmentierung und die Möglichkeit zur Priorisierung: »Bei Cybersecurity in der Autoindustrie unterscheiden wir in on-board (das Fahrzeug), das produktnahe IT-Back-End und die traditionelle IT. Innerhalb oder neben der traditionellen IT betrachten wir insbesondere noch die Operational Technology (OT), also die IT der Produktion.«

Mit Spezialsoftware die kritischsten Threats priorisieren

In der OT, so Steininger, gebe es in der Automotive-Industrie, aber auch insgesamt im Manufacturing noch viel Handlungsbedarf. »Hier steht die Verfügbarkeit im Vordergrund. Ausfälle, vor allem aber ein Produktionsstillstand, müssen auf jeden Fall vermieden werden. Darum lässt sich OT nicht mal eben patchen so wie in der IT. Die Anlagen müssen durchlaufen.« Unternehmen sind daher gezwungen, immer die neuesten Geräte mit den aktuellen Updates im Einsatz zu haben. Aber das ist laut Steininger häufig nicht der Fall. Bei Angriffen wie Industriespionage, Sabotage oder IP-Diebstahl sei es also wichtig, die kritischsten Schwachstellen und Bedrohungen zu identifizieren sowie deren Mitigierung priorisieren zu können. Dann sei ein effektives Risikomanagement für die OT mit entsprechenden Resilienzmaßnahmen praktikabel. Cybersecurity im Fahrzeug wird durch UN ECE R155 geregelt. Die Autobauer benötigen hierfür ein CSMS (Cybersecurity-Management-System). Dies regelt die Prozesse und Verantwortung in der Organisation, damit ein Fahrzeug in Bezug auf Cybersecurity sicher auf den Straßen bewegt werden kann. Geprüft wird dies durch eine spezielle Typgenehmigung, die vom Kraftfahrtbundesamt und den technischen Diensten abgenommen wird.

Priorisierung macht Cyber-Readiness und Compliance parallel beherrschbar

»Wir können im Prinzip die gesamte digitale Lieferkette des OEM und seinen Tier-One- bis

Software-Bill of Materials – die IT-Stückliste

Automobilhersteller sind verpflichtet, eine Software-Bill of Materials (SBOM) zu erstellen. Es handelt sich dabei um eine Liste aller Software-Komponenten, die in einem System eingesetzt sind. Zum Einsatz kommen solche Listen sowohl bei den Softwareherstellern als auch bei den Anwendern und bei den Aufsichtsbehörden. Damit Hersteller Schwachstellen in ihren Komponenten schnell schließen können, müssen sie wissen, welche Komponenten wo verbaut sind. Betreiber können anhand dieser Listen feststellen, ob ihre Komponenten oder ihre IT-Umgebung von einer gemeldeten Lücke betroffen ist. Behörden wiederum stellen sicher, dass Software-Hersteller die regulatorischen Anforderungen erfüllen.

Die SBOM ist eine von mehreren Quellen, die das Asvin-Produkt Risk by Context als Input für die Risikoanalyse nutzt. Damit diese Analyse auch alle Lücken findet, müssen Automobilhersteller und Anwender aus anderen Branchen diese Dokumente stets aktualisieren, wenn sie ihre Software-Landschaft ändern. (ih)

Tier-Three-Zulieferern abbilden, und zwar bis in ihre letzten Verästelungen in einem Kontexte darstellenden Graphenmodell«, sagt Steininger. »Daraus erstellen wir einen Risiko-Score für die betrachtete Umgebung. Aus diesem Score heben wir dann die für das ganze Unternehmen oder eine seiner Produktionseinheiten oder eines seiner Lieferanten-Netzsegmente wichtigsten Vulnerabilitäten hervor, um die sich zuallererst gekümmert werden sollte.«

Die so durchgeführte Risikoanalyse sorgt dafür, dass beispielsweise ein gefährdetes Asset, also ein zu schützendes Gut wie ein Datensatz oder ein Gerät, rechtzeitig untersucht wird. Damit kann der OT-Sicherheitsverantwortliche identifizieren, welches das kritischste Netzwerksegment, im Netzwerksegment die kritischste Komponente oder in der Komponente die kritischste externe Schnittstelle ist, die primär und dringend beobachtet und gefixt werden sollte.

Für jedes Niederlassungs-Land die Compliance-Regeln im Griff

In Summe gibt es weltweit Hunderte verschiedener Regularien bezüglich Cybersecurity – über unterschiedliche Branchen, über unterschiedliche Länder, also mit sehr speziellen lokalen Ausprägungen. In den USA hat jeder Bundestaat eine eigene Gesetzgebung diesbezüglich für die unterschiedlichen Industrien. Auch hierbei legt Asvin-Software über die Risikobewertung den Fokus auf die jeweils erforderliche Compliance. OEMs und Zulieferer können damit ihre Cybersicherheitsmaßnahmen um den Regulierungs-Aspekt ergänzen, dieser läuft in der Risikoanalyse dynamisch mit. »Große Tier-One-Supplier haben meist Hunderte weltweit verteilter Standorte. In diese können wir hineinzoomen: in die dortigen Netzwerke, in das Produktions-Equipment, in galvanische oder andere Anlagen«, erläutert Steininger, und ergänzt: »So können Anwender immer tiefer in ihre OT gehen und zum Beispiel feststellen, wie Geräte gepatcht werden und wo dabei irreguläres Verhalten sichtbar ist. Wenn jedoch ein altes Gerät in der Produktion hängt, lässt es sich natürlich nicht so einfach patchen, denn Patchmanagement geht bis auf die Speichereinträge hinunter. Wenn so ein altes Gerät nun ausfällt, stellt das ein Problem dar, denn das ist im Produktionsbereich tabu, Stichwort ‚Availability'.«

Mit dem Produkt Risk by Context (RBC) können Produktionsverantwortliche oder CISOs abschätzen, welche der OT-Geräte, die sie für die und die Funktion brauchen, problemlos patchen können und welche nicht. Mit RBC macht Asvin sichtbar, welche Schwachstellen die Software eines IoT-Geräts aufweist und ob dieses Gerät Einfluss auf eine unternehmenskritische Funktion hat, diese also direkt beschädigen kann. Daraus lässt sich also ableiten, ob die Schwachstellen sofort behoben werden müssen.

Log4J – die Ursache für die Durchsetzung der SBOM

Konkretes Beispiel für die Wichtigkeit präziser und vor allem schneller Lokalisierung von Schwachstellen ist der Log4J-Vorfall im Dezember 2021. Damals hatten staatliche Behörden und auch Security-Anbieter mehrere Monate gebraucht, um zu identifizieren, wo Log4J in ihren IT-Systemen genau verbaut war.

Durch den Log4J-Vorfall wurde die Software-Bill of Materials (SBOM) verpflichtend – in den USA zuerst; in Europa ist man grade dabei, dies umzusetzen. Treiber sind in diesem Fall die Unternehmen, die die Cybersicherheit ihrer Prozesse dadurch in den Griff bekommen wollen. Denn mit der SBOM ist genau ersichtlich, welche Software verwendet wird. Darüber hinaus ist ein Abgleich mit CVE-Listen möglich. Aber dann steht bereits das nächste Problem an: Tausende von Vulnerabilitäten. Wo fängt man da an? An dieser Stelle greift das dynamische Risk-Management und die Priorisierung von Asvin-Software: Die kontextbezogene Risikoanalyse kann die kritischsten Fälle hervorheben, deren Bearbeitung also planbar machen. Damit unterstützt Asvin OEMs und Tier-x dabei, Security-by-Design-Konzepte umzusetzen. Cybersecurity wird so vom Problem zum verkaufsfördernden Feature.

Priorisierung sorgt für Planbarkeit im Cyberspace

Auch die Cybersicherheitsmaßnahmen lassen sich durch Priorisierung wirkungsvoll planen. Wie weit kommt man mit 50.000 oder 100.000 Euro? Wie lässt sich eine Million Euro am zielführendsten einsetzen, sodass die meisten kritischen Risiken abgedeckt werden? RBC versetzt Unternehmen in die Lage, genau solche Überlegungen überhaupt anstellen zu können. Diesen Ansatz verfolgen einige der Asvin-Kunden und Kooperationspartner gemeinsam mit der Cybersicherheitsforschung von Asvin am MIT. Dort wird beispielsweise erprobt, wie sich Risiken rollenbasiert über die Supply-Chain darstellen lassen.

Der Cybersecurity-Markt hierfür ist vielversprechend und bietet vielfältige Wachstums- und Wertschöpfungschancen. Auf Produktebene wird Security by Design das nächste große Thema, gerade in Bezug auf die neuen anstehenden Regularien wie NIS 2 und Cyber Resilience Act (CRA). Derzeit beträgt das Marktvolumen für cybersichere Produkte und Services rund 100 Mrd. Dollar pro Jahr. Kein Wunder, denn derzeit werden weltweit erst unter ein Prozent der Cybersecurity-Incidents überhaupt gemeldet. »Das ist frappierend. Der Markt für Cyberresilienz wächst, weil sich etwas ändern muss. Jeder versucht derzeit noch, Risiken einfach zu übertünchen oder Vorfälle nicht zu melden. Aber die Unfälle, die Angriffe, die sind da«, sagt Steininger abschließend. (ih)

Cybersecurity-Vorfälle in Deutschland

Insgesamt 136.865 Fälle von Cybercrime hat die Polizei 2023 in Deutschland registriert. Enthalten darin sind bekannte Angriffsvektoren, Ransomware-Angriffe, DDOS-Angriffe (Distributed Denial of Service) und andere bösartige Aktivitäten von Hackern. Bei den Akteuren unterscheiden Studien des Massachusetts Institute of Technology und von Asvin drei Ebenen: 70 Prozent ungezielte Massenattacken von Hackern, 29 Prozent gezielte Angriffe von Cyberkriminellen und 1 Prozent sogenannte Advanced Persistent Threats von staatlich unterstützten Akteuren. »Die Advanced Persistent Threats können Unternehmen praktisch vernachlässigen, denn das sind gerade einmal 1 Prozent«, berichtet Gerhard Steininger, Vice President Sales beim Security-Spezialisten Asvin. »Dagegen kann man sich auch nur mit einem enorm hohen Aufwand absichern. Abwehren kann und muss die Autoindustrie dagegen die ungezielten Hackerangriffe und die gezielten Angriffe von Cyberkriminellen. Eine Risk-by-Context-Analyse gibt ihnen das Werkzeug, um ihre Abwehrmaßnahmen und Investments zu priorisieren.« (ih)