Consulting
DETECON

Pressemitteilung

Vernetzte Zulieferer brauchen ganzheitliche Sicherheitskonzepte

- Umfrage auf 2. Automotive Suppliers‘ Day von T-Systems
- Zulieferer befürchten Zunahme an Cyber-Bedrohungen
- Interne Netze und Daten in der Regel gut geschützt
- IT als Teil des Autos erzeugt hohen Bedarf an unternehmensübergreifenden und produktbezogenen Sicherheitskonzepten

Köln/Eschborn, 5. März 2014. Noch haben nicht alle Automobilzulieferer mit ihren Kunden und Lieferanten ein gemeinsames Konzept für IT-Sicherheitsanforderungen definiert. Während die interne IT-Security mehrheitlich umfassend geregelt ist, fehlt es im externen Ökosystem eines Zulieferers an durchgängigen Maßnahmen für die IT-Sicherheit. Das sind die Ergebnisse einer Befragung, die die Managementberatung Detecon unter den Besuchern des speziell für die Zuliefer-branche ausgerichteten 2. Automotive Suppliers‘ Day von T-Systems in Stuttgart durchgeführt hat.

Die Befragten waren sich einig, dass die Bedrohung durch Cyberangriffe und Industriespionage mit der zunehmenden Verschmelzung von IT und Fertigungs-technik wachsen wird. Hinsichtlich der eigenen Organisation sehen sich die Zulieferer relativ gut aufgestellt: Befragt auf einer fünfstufigen Zustimmungsskala, ob ein ganzheitlicher Security-Ansatz für IT-Sicherheit, IT Risk Management, Compliance und Datenschutz vorhanden ist, deutet der Mittelwert von 3,5 darauf hin, dass interne Sicherheitsvereinbarungen mehrheitlich vorhanden sind. Noch höhere Zustimmung (4,4) erfährt die Frage, ob eine zentrale Anlaufstelle für akute Sicherheitsvorfälle (Security Incidents & Response) etabliert wurde. Im Gegensatz dazu konnten die Zulieferer mit einem Mittelwert von 2,5 nicht umfassend bestätigen, mit ihren Lieferanten oder Kunden, den Automobilherstellern, ein gemeinsames Konzept für IT-Sicherheitsanforderungen definiert zu haben.

„Zwar ist dieses Manko den Akteuren in der Regel bekannt, aber die gemeinsame Umsetzung gestaltet sich schwierig“, so Mark Großer, Security-Experte bei Detecon. „Viele partnerübergreifende Sicherheitsvereinbarungen betreffen in der Regel nur einzelne Baugruppen. Immer wichtiger ist aber die Sicht auf das Auto als ganzheit-liches Produkt, für das die IT zentrale Komponenten wie Geschwindigkeit, Bremsen und Licht entscheidend vernetzt und regelt. Und damit ja auch die Sicherheit des Fahrers garantieren muss.“

Nur einen Zustimmungsmittelwert von 2,2 erlangte die Aussage, dass für eigene elektronische Komponenten ein Sicherheitskonzept existiert, das auch böswillige IT-Angriffe auf die Sicherheit des Fahrers abwehrt. „Auch wenn dieses Bedrohungsszenario nicht für alle Zulieferer und ihre Komponenten gleichermaßen gilt, macht es doch deutlich, dass Safety und Security gemeinsam zu betrachten sind“, so Großer. „Auf dem PC gibt es jeden Tag Sicherheitsupdates – warum sollte das beim Connected Car anders sein, wenn es letztlich ein fahrender Rechner ist?“

„Die OEMs und Zulieferer sind heute natürlich auch über die IT global eng vernetzt, die Zulieferer müssen der Emerging-Market-Strategie der Hersteller folgen“, betont Dr. Thomas Siems, Leiter des Geschäftsbereichs Automotive bei Detecon. „Neben den klassischen Feldern wie Auftragsverarbeitung, Supply Chain Management und der lokalen IT in den Produktionshallen gibt es auch zunehmend gemeinsame Entwicklungsplattformen, da bei der geringen Fertigungstiefe der OEMs der Innovationsdruck auf die Zulieferer wächst.“ Die Sorge, dass Angriffe über das Zulieferer-Netzwerk auf den OEM erfolgen könnten, sei dabei durchaus berechtigt, da an dieser Stelle alle Informationen zentral zusammenlaufen. „Hier sind die OEMs stark gefordert, ein übergreifendes Security-Konzept und Policies für alle Zulieferer abzustimmen, damit die Bedrohung beherrschbar und nicht zu komplex wird.“

Heinz Egeler, der bei T-Systems für das globale Automobil-Zulieferergeschäft verantwortlich ist, unterstreicht: „Um in der neuen Welt erfolgreich sein zu können, müssen Zulieferer künftig weit mehr mit anderen Partnern zusammenarbeiten. Das kann nur funktionieren, wenn wir uns auch beim Thema Security mehr miteinander vernetzen.“

Die vollständige Auswertung der Umfrage steht unter www.detecon.com/suppliersday zum kostenlosen Download zur Verfügung.

Detecon International GmbH
Detecon ist eine führende, weltweit agierende Unternehmensberatung, die seit über 30 Jahren klassisches Management Consulting mit hoher Technologiekompetenz vereint. Ihr Leistungsschwerpunkt liegt im Bereich der digitalen Transformation: Detecon hilft Unternehmen aus allen Wirtschaftsbereichen, ihre Geschäftsmodelle und operativen Prozesse mit modernster Kommunikations- und Informationstechnologie an die Wettbewerbsbedingungen und Kundenanforderungen der digitalisierten, globalisierten Ökonomie anzupassen. Das Know-how der Detecon bündelt das Wissen aus erfolgreich abgeschlossenen Management- und ICT-Beratungsprojekten in über 160 Ländern. Sie ist ein Tochterunternehmen der T-Systems International, der Großkundenmarke der Deutschen Telekom.

Weitere Informationen unter:
www.detecon.com

Pressekontakt
Detecon International GmbH
Gerhard Auer
Sternengasse 14 – 16
D-50676 Köln
Phone: (+49 221) 9161-1013
Fax: (+49 221) 9161-1017
e-Mail: gerhard.auer@detecon.com