Automobilwoche

October 19, 2022 03:46 PM

Größere Angriffsfläche

KLAUS-DIETER FLÖRECKE

Foto: Continental

Cybersecurity: Im August hatten Hacker die IT-Systeme von Zulieferer Continental im Visier.

Neue Fahrzeugarchitekturen und zunehmende Vernetzung erhöhen die Gefahr von Cyberattacken. Die Hacker gehen dabei immer professioneller vor.

Cyberangriffe auf Unternehmen der Automobilbranche nehmen zu. Erst im August hatten Hacker die IT-Systeme des Zulieferers Continental infiltriert. Während die Attacke auf den Konzern nach eigenen Angaben abgewehrt werden konnte, hatte es zuvor Eberspächer schlimm erwischt. Firmenchef Martin Peters sprach davon, dass der

Angriff dem schwäbischen Unternehmen einen "mittleren zweistelligen Millionenbetrag gekostet" habe. Mithilfe einer sogenannten Ransomware hatten die Täter Zugriff auf die Systeme erhalten.

Angriffe mit Erpressungssoftware sind aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) aktuell die größte Bedrohung. Als Einfallstor nutzen die Angreifer in der Regel die Office- IT-Netzwerke. Die Hacker stellen hohe Lösegeldforderungen und drohen, sensible Daten bei Nichtzahlung zu veröffentlichen. Gleichzeitig wird die Vernetzung der IT-Infrastruktur von Autoherstellern und Zulieferern immer umfangreicher. Dadurch erhöht sich laut BSI die Angriffsfläche – und das Schadenspotenzial steigt.

Zwei Hauptprobleme

Der Umgang mit Schwachstellen, insbesondere der Soft- und Hardware von Produktionsanlagen, ist eine besondere Herausforderung. Es gibt zwei Hauptprobleme, die nicht nur für die Automobilbranche gelten: Einerseits etabliert sich die Versorgung mit Sicherheits-Updates bei vielen Unternehmen erst langsam. Andererseits werden für ältere Komponenten zum Teil gar keine Aktualisierungen bereitgestellt, so dass sich identifizierte Schwachstellen nicht schließen lassen.

Eine weitere gefährliche Entwicklung ist laut Branchenexperten, dass Kriminelle in einem Ökosystem zusammenarbeiten und Ransomware-as-a-Service anbieten. In diesem System komme jedem Akteur eine spezifische Rolle zu. Dabei stellen einige Akteure etwa die Verschlüsselungssoftware sowie eine Plattform für Verhandlungen bereit. Andere führen die Attacken aus.

Flotten und Unternehmen im Fokus

Doch nicht nur Unternehmen können von Angriffen getroffen werden. Auch die neuen Funkschnittstellen im Fahrzeug, insbesondere in Verbindung mit dem Infotainmentsystem, stellen sich immer wieder als verletzlich heraus. "Die gesamte Automobilindustrie befindet sich in einem massiven Wandel. Die Palette an Bedrohungen im Bereich Cyberkriminalität ist massiv explodiert", sagt Cristian Ion, Leiter der Abteilung Risikoanalyse und Sicherheitstechnik bei Cymotive Technologies, einem Spezialisten für Cybersicherheit. Die Zunahme von vernetzten Fahrzeugflotten habe im Störungsfall weitreichende Konsequenzen. "Bei einer Smart City, die auf autonom fahrenden Systemen inklusive der Logistikketten mit selbstfahrenden Fahrzeugen aufbaut, kann es dazu kommen, dass bei Störungen eine ganze Stadt oder Region zum Erliegen kommt."

Für Cymotive-Geschäftsführer Dirk Reimer besteht die große Gefahr nicht in Form von Angriffen auf Einzelpersonen. Die Angriffsziele seien dafür zu komplex und die Kosten zu hoch. Die eigentliche Bedrohung seien Hacker, die sich professionalisieren, um damit Geld zu verdienen. Im Fokus der Kriminellen stünden Flotten und Unternehmen.

Autos mit häufig entkoppelten Systemen

Vor der Einführung des Notrufs eCall in Europa im Jahr 2018 war die Konnektivität in Fahrzeugen kein großes Thema. "Es konnte immer nur ein einzelnes Fahrzeug angegriffen werden, aber nicht ganze Flotten", sagt Reimer. Doch mit der kontinuierlichen Einführung von Konnektivität in den Fahrzeugen habe sich das geändert. Zwar gibt es heute in den Autos noch weitestgehend entkoppelte Systeme. Lenkung, Gas und Bremse funktionieren vielfach mechanisch. Aber in Zukunft werden diese Dinge im Fahrzeug zunehmend vernetzt. "Das heißt, wir haben mehr By-Wire-Lösungen. Mit der wachsenden Komplexität der Systeme wird es dann auch neue Angriffsvektoren geben", befürchtet Reimer.

Er ist davon überzeugt, dass sich durch die sich wandelnden Fahrzeugarchitekturen auch die Angriffsszenarien ändern. Zwar sind die spektakulären Fälle von Angriffen auf die IT von Unternehmen mit Erpressungssoftware im Fahrzeug derzeit noch nicht möglich, "da dort die Vernetzung mit den neuen Softwarearchitekturen erst noch kommt. Aber wir müssen heute schon sicherstellen, dass solche Angriffe rechtzeitig detektiert und entsprechend abgewehrt werden können."

Lesen Sie auch:

Onlinedienst T-Connect: Hacker klauen Daten Hunderttausender Toyota-Kunden

Zweistelliger Millionenbetrag: So lief die Cyberattacke bei Eberspächer

Dazu aus dem Datencenter:

Top-5-Risiken in der Automobilindustrie - 2022