AUTO TIMES

- Phishing stoppt Fertigung
- Backup? Fehlanzeige!
- MES im Lockdown

OEM VERSCHÄRFT SECURITY-ANFORDERUNGEN

Stuttgart - Ein führender deutscher Automobilhersteller kündigte an, alle Tier-1- und Tier-2-Zulieferer ab Q2/2026 einem IT-Security-Audit zu unterziehen.

Erwartet und verlangt nachweisbare Basiskontrollen wie Zugriffsschutz, Wiederanlauf, Patch-Management, Sicherheitsmonitoring sowie eine klare Netztrennung in der Produktion.

"Supply Chain Security ist geschäftskritisch", so ein Sprecher. Bei gravierenden Lücken behalte man sich vor, Aufträge zurückzustellen.

Ransomware legt Zulieferer tagelang lahm

Kassel, 10.01.2026

Ein mittelständischer Automotive Zulieferer aus Nordhessen wurde Opfer eines schweren Ransomware Angriffs. Die Produktion stand für 72 Stunden still, der Schaden wird auf über 500.000 Euro geschätzt.

DER ANGRIFF

Laut Informationen des Unternehmens erfolgte der Einbruch einer Phishing-Mail, die ein Mitarbeiter in der Buchhaltung öffnete. Die Erpresser Software verschlüsselte innerhalb von 2 Stunden nicht nur Office-Daten, sondern auch das produktionssteuernde MES-System.

"Wir hatten kein funktionierendes Backup Konzept", so der Geschäftsführer unter der Bedingung der Anonymität. Die Angreifer forderten ein Lösegeld von 250.000 Euro in Bitcoin.

FOLGEN

Das Unternehmen entschied sich gegen die Zahlung und setzte die Systeme neu auf – mit Unterstützung externer Forensiker. Drei Fertigungslinien standen still, Liefertermine konnten nicht eingehalten werden. Ein OEM-Kunde verhängte Vertragsstrafen wegen Lieferverzugs.

"Auch kleine Zulieferer sind Ziele", warnt Dr. Sabine Müller vom BSI. "Angreifer wissen: Produktionsausfälle erzeugen Zahlungsbereitschaft."