

Fremdhardwareerkennung bei der Mercedes-AMG GmbH



Mercedes-Benz

Im Zuge des kontinuierlichen Ausbaus der IT-Security-Infrastruktur der Mercedes-AMG GmbH und der wachsenden Zahl von eingesetzten externen Partnern und Dienstleistern, die eigene IT-Ausrüstung zum Einsatz bringen, bestand die Aufgabe bei der Mercedes-AMG GmbH darin, diese Fremdgeräte im Netzwerk erkennen, lokalisieren und abwehren zu können.

Diese Erkennung sollte vom angeschlossenen Netzwerkgerät sowie vom Betriebssystem unabhängig, campusweit und ohne Erneuerung der schon bestehenden LAN-Infrastruktur (Local Area Network) gewährleistet werden.

Als Basis wurde die Appliance **ARP-GUARD** der Firma ISL GmbH in einem redundanten und für Lastverteilung genutzten Aufbau eingesetzt. Durch die auf einer Linux-Architektur basierenden Appliance, konnten weitere gewünschte Funktionen problemlos implementiert werden. Die Funktionsweise lässt sich zusammengefasst wie folgt darstellen: Sobald eine Hardware mit dem Netzwerk verbunden wird, überprüft das System in seiner Datenbank, ob das Gerät als vertrauenswürdige Netzwerkkomponente bekannt ist. Ist das Gerät bekannt und legitim wird entsprechend Netzwerkzugriff gewährt. Ist das Gerät unbekannt, ausgemustert oder auf sonstige Art und Weise als nicht vertrauenswürdig eingestuft, wird es automatisch in ein, in der Funktion über eine Firewall sehr eingeschränktes, Quarantäne-VLAN (Virtual Local Area Network) verschoben. Durch dieses Isolieren der Hardware vom restlichen Netzwerk wird in einem hohen Maße zum Schutz der Netzwerkinfrastruktur und den angeschlossenen Systemen beigetragen. Auch weitere Sicherheitsinteressen, wie das Abwandern von Know-How oder der Schutz vor unbekanntem und evtl. mit Viren und Malware verseuchten Rechnern, werden bedient.

DaimlerChrysler <COMMUNICATIONS2>, Stuttgart

Presse-Information



Mercedes-Benz