INFOKOM.
digital.
sicher.
vernetzt.

IABG Whitepaper **5G Security**

Mit der Einführung von 5G wird ein breites Spektrum an Anwendungen für die Industrie und öffentliche Hand möglich werden. Industrie 4.0 wird richtig in Fahrt kommen. Vernetzt arbeitende Roboter können sich mit kurzer Latenz zuverlässig austauschen und ihre Arbeiten effektiv koordinieren. Der Einsatz einer hohen Anzahl von energiesparenden und batteriebetriebenen Sensoren ermöglicht einen vollautomatisierten Produktionsbetrieb und, durch die Verfügbarkeit ihrer Daten, eine Effizienzsteigerung.

Ein echtzeitfähiger Datenaustausch und breitbandige Kommunikationsmöglichkeiten sind besonders für die Fahrzeuge in der automatisierten Logistik notwendig. Auch dies wird erst mit der 5G Funktechnik realisierbar. Diese technischen Möglichkeiten und die damit verbundenen ökonomischen Interessen in der „Fabrik der Zukunft" lassen Sicherheitsbetrachtungen oftmals in den Hintergrund rücken, was in der Regel zu hohen Folgekosten führen kann, wenn Sicherheitslücken ausgenutzt werden und zu Stillständen im Produktionsbetrieb führen.

Beispielsweise können IoT Endgeräte wie einfache Sensoren zu Gunsten der Energieeffizienz bereits über Signalisierungsmechanismen Statusinformationen austauschen, wodurch Angriffsmöglichkeiten zur Manipulation der Daten geöffnet werden. Um dem entgegenzuwirken sollten Authentifizierungsabfragen, insbesondere bei günstigen Sensoren, speziell überprüft werden und die Integrität einfacher Sensorsysteme durch ein erweitertes Sicherheitskonzept gewährleistet werden.

Auch die künftige Integration vieler Sensoren in komplexe IT-Systeme durch massenhafte Vorkonfiguration mittels eSIM ermöglicht Cyberangriffe durch Vortäuschen einer anderen Identität und die Möglichkeit falsche Statusinformationen von manipulierten Endgeräten an Steuergeräte zu verbreiten. Mit inversen SIM-Locks, die eine SIM Konfiguration an ein bestimmtes vordefiniertes und katalogisiertes Gerät knüpfen, kann unbemerkten Manipulationen an Endgeräten vorgebeugt oder diese sogar ausgeschlossen werden.

Die IT-Architektur eines 5G Netzes unterscheidet sich wesentlich von der IT in bisherigen Mobilfunknetzen. Cloud-basierte Netze schaffen mit ihren modernen und effizienten Technologien eine erhöhte Flexibilität im Netz welche auch als Edge Clouds an der Basisstation die Leistungsfähigkeit erhöhen.

Im Bereich der Sicherheit entstehen hier neue Risiken, sowohl beim Betrieb von Applikationen als auch beim Betrieb der Rechencluster selbst. Beispielsweise besteht hier die Möglichkeit über Schwachstellen in der Virtualisierung das gesamte Rechencluster zu kompromittieren. Aber auch der nicht autorisierte Zugriff auf Daten und der dementsprechende Datenabfluss wären vorstellbar. Diese Risiken lassen sich nur mit entsprechenden technischen Maßnahmen, wie z.B. der Überwachung des Netzwerkverkehrs auf der Virtualisierungsebene, verhindern.

Mit service-orientierten Architekturkonzepten werden die Verarbeitungseinheiten in sogenannte Containern gekapselt, welche bestimmte Features nach Bedarf bereitstellen. Besonders vorteilhaft für die Entwickler und Betreiber der IT-Plattform ist hier ein kontinuierlicher Entwicklungs- und Integrationsprozess (engl. CI/CD Process), um sich möglichst schnell an neue Anforderungen anzupassen. Hierbei entsteht durch jeden Build-Prozess ein Einfallstor für manipulierte oder korrumpierte Codesnippets, die unbemerkt in den operativen Einsatz gelangen können. Die Anforderungen der Informationssicherheit müssen von Beginn an auf Compliance geprüft werden. Ein effizientes Schwachstellenmanagement (CVE-Scoring) der eingebundenen Software-Bibliotheken sollte fester Bestandteil eines jeden Entwicklungsprozesses sein. Auch im Betrieb muss für die Umsetzung eines effizienten CI/CD Prozesses eine agile Methode für die Bewertung der IT-Sicherheit der aktiven Software geschaffen werden. Die dafür erforderliche enge Verzahnung des IT-Security Managements mit der SW-Entwicklung sollte schon im Entwicklungsprozess fest etabliert werden.

Für weitere Informationen wenden Sie sich bitte an:
Maik Holzhey • Tel. + 49 89 6088-2294 • Holzhey@iabg.de