



kapsch >>>
challenging limits

Kapsch BusinessCom

Sicherheit 4.0 für Industrie 4.0.

Security Audits für Produktionsumgebungen als integrierter Bestandteil einer umfassenden Sicht auf IT- und OT-Security.

Angriffe abwehren, Produktionsumgebungen schützen: Die immer weiter zunehmende Digitalisierung von Fertigungsprozessen verlockt Cyberkriminelle dazu, auch Steuerungsanlagen, Roboter und ähnliche Systeme ins Visier zu nehmen. Daher ist Cyber Security nur in einer Gesamtbetrachtung von IT und OT wirkungsvoll. Nutzen Sie jetzt das erweiterte Security-Portfolio von Kapsch zur Beseitigung von Schwachstellen und zum Schutz vor neuen Bedrohungen.

Hochintelligent, aber extrem anfällig: *Produktionsumgebungen wirksam gegen Angriffe schützen.*

Das Arbeitsplatzrechner und Server Opfer von Cyberangriffen werden können, ist bekannt. Aber wie sieht die Bedrohungslage für Produktionsumgebungen aus? Fertigungsanlagen sind heutzutage vernetzt und automatisiert. Die Kommunikation läuft über LAN/WLAN und Mobilfunk. Die Prozesse arbeiten mit digitalen Sensoren, die Instruktionen kommen von computergestützten Steuerungssystemen. Rohmaterialien werden von intelligenten Transportlösungen befördert und von Robotern bearbeitet. Die fertigen Produkte werden automatisch qualitätsgeprüft. Und die gesamte Produktionsumgebung ist meistens komplett oder zumindest teilweise in das ERP-System integriert.

Ganzheitliche Securitylösungen für Bedrohungen aller Art.

Das alles macht Fertigungsanlagen anfällig gegenüber internen und externen Bedrohungen. Neben den bisher bekannten Angriffszielen eines Unternehmens, etwa Nutzer-Endgeräte als Einfallstor und Mail- und File-Server als Endziel, geraten damit auch Produktionssysteme in den Blick von Angreifern. Die kostspieligen Auswirkungen reichen von Industriespionage bis zu Sabotage. Schwachstellen werden oft erst bemerkt, wenn der Schaden schon eingetreten ist. Um diese Angriffe zu verhindern, ist es besonders wichtig, effektive Vorsorgemaßnahmen zu setzen. Die Security-Spezialisten von Kapsch unterstützen Sie dabei, Ihre Produktionsumgebungen nachhaltig abzusichern.



Security Audits für Ihre Produktionsumgebung. *Unsere Dienstleistungen.*

- > Durchführung von Port- und Schwachstellenscans zur Identifizierung von erreichbaren Diensten in der Produktionsumgebung
- > Überprüfung der Netzwerksegmentierung, unternehmensweit mit Fokus auf den Zugriff in die Produktionsumgebung
- > Identifizierung von vorhandenen technischen Schwachstellen oder Konfigurationsschwächen von Systemen und Diensten in der Produktionsumgebung, die zur unberechtigten Übernahme, missbräuchlichen Verwendung oder zu Systemausfällen führen können
- > Sicherheit von Netzwerk/Funkverbindungen
- > Computersysteme der Steuerungsanlage
- > Zugriffskontrolle/Fernwartung
- > Bewertung der Sicherheit der Produktionsumgebung auf Basis von einschlägigen Standards und Normen
- > Welche Zugänge müssen von welchen Netz-Segmenten aus erreichbar sein bzw. welche können in Absprache mit betroffenen Abteilungen gesperrt werden?
- > Erarbeitung und Dokumentation von alternativen Maßnahmen
- > Dokumentation der Ergebnisse

Kapsch Security Audit Services:

Ihr Partner für alle Fälle.

Kapsch ist der einzige TÜV Trusted IT-Security Auditor in ganz Österreich. Unsere Sicherheitsüberprüfungen von Produktionsumgebungen sind reversionssicher (z. B. für Wirtschaftsprüfer, Risikoversicherer) und werden auf Basis folgender Normen und Standards durchgeführt:

- > IEC 62443 (Industrial communication networks – Network and system security)
- > VDMA – Leitfaden Industrie 4.0
- > NIST 800-82 (Guide to ICS Security)
- > OWASP IoT Security Guidance (Manufacturer IoT Security Guidance)
- > ISO 27001

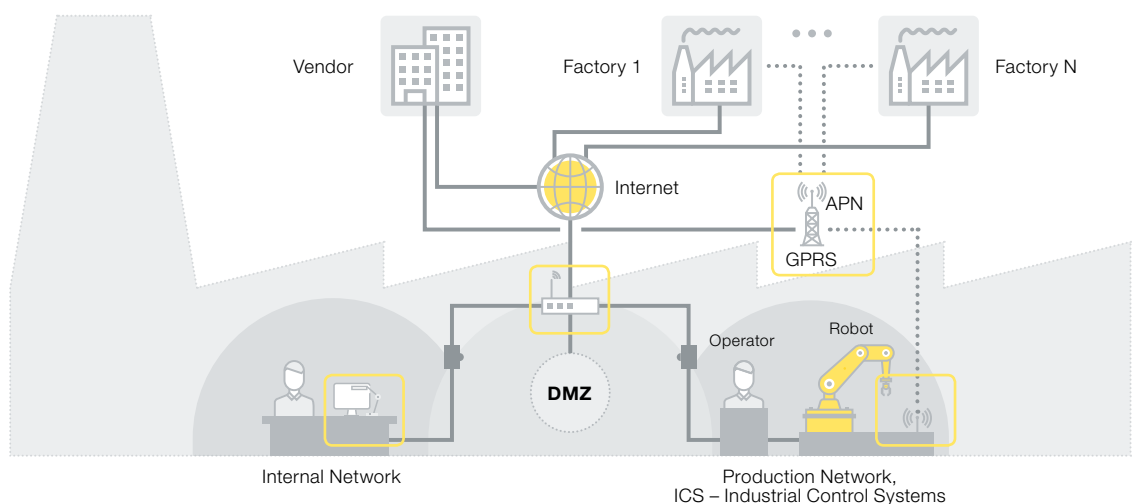
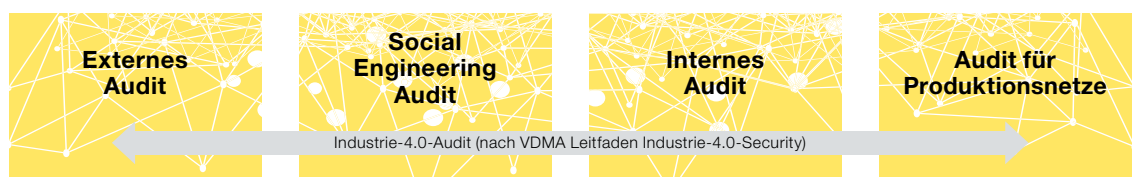
Die Spezialisten von Kapsch verfügen u. a. über die folgenden Zertifizierungen:



- > TÜV Trusted IT-Security Auditor
- > Akkreditierung zur Auditudurchführung nach ÖNORM A 7700
- > CIS Information Security Auditor nach ISO 27001
- > CIS Information Security Manager
- > Zertifizierter Datenschutzbeauftragter (nach dem Austrian Standards Zertifizierungsschema P43)
- > GPEN (SANS GIAC Penetration Tester)
- > CISSP (Certified Information Systems Security Professional)
- > GCFA (SANS GIAC Certified Forensic Analyst)
- > OSCP (Offensive Security Certified Professional)
- > CCE (Certified Computer Examiner)
- > CHFI (Computer Hacking Forensic Investigator)
- > CompTIA Security+

Unser Portfolio im Überblick.

Sicherheit für alle Unternehmensbereiche.



Kapsch BusinessCom

Kapsch BusinessCom ist ein Unternehmen der Kapsch Group und unterstützt als führender Digitalisierungspartner Unternehmen bei der Steigerung der Business Performance und Entwicklung neuer Geschäftsmodelle. Kapsch agiert dabei als Berater, Systemlieferant und Dienstleistungsanbieter. Mit seinem umfassenden Know-how im Umgang mit großen Datenmengen und Security sowie einer Vielzahl erfolgreicher Use Cases in zahlreichen Branchen ist Kapsch BusinessCom der ideale Begleiter bei der digitalen Transformation. Das umfangreiche Portfolio in Österreich, Rumänien und der DACH-Region umfasst Technologielösungen für intelligente und vor allem sichere ICT-Infrastrukturen, smarte Gebäude-, Medien- und Sicherheitstechnik sowie Outsourcing-Services. Kapsch setzt dabei auf Herstellerunabhängigkeit und Partnerschaften mit weltweit führenden Anbietern wie HPE, Cisco oder Microsoft sowie auf ein breites Netzwerk aus Partnern aus der Forschung und branchenspezifischen Lösungsanbietern – vom Start-up bis zum Großkonzern. Im Bereich Security arbeiten wir unter anderem mit Barracuda, Check Point, McAfee und Palo Alto Networks zusammen.

Kapsch BusinessCom hat über 17.000 Kunden – z. B. Allianz, Erste Bank, ÖBB, OMV, ORF und Vodafone – und betreut diese lokal und global. Rund 1.200 Mitarbeiterinnen und Mitarbeiter der Kapsch BusinessCom erzielten im Geschäftsjahr 2016/17 einen Umsatz von rund 320 Mio. Euro.

>>> www.kapsch.net