Sichere Kommunikation

Individuelle Sicherheitsstrategien und 5G-Netze für mittelständische Unternehmen

Bei allen Vorteilen, die digitale Transformation birgt auch Risiken. Hackerangriffe treffen nicht mehr nur die großen Player, sondern auch kleine und mittelständische Unternehmen (KMU). Bereits kleine Sicherheitslücken oder menschliches Versagen reichen aus, um Hackern Tür und Tor zu öffnen. Mit ihrem Spezialwissen sind sie für Hacker ebenso interessant, wie große Unternehmen. Produktionsausfälle, Beschädigungen von Maschinenparks, Patentdiebstahl oder Cyber-erpressung zeigen die Dringlichkeit von passenden IT-Sicherheits-vorkehrungen auf. Für eine effiziente und kostenorientierte Sicherheits-strategie bieten sich Managed-Security-Lösungen an. Als System-integrator hat die telent GmbH mit ihrer Tochterfirma KORAMIS GmbH umfangreiche Erfahrungen mit regulatorischen Verfahren.

Die telent GmbH unterstützt Kunden von der Schwachstellenanalyse über die Netzplanung bis zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung mit einem ganzheitlichen Sicherheitskonzept. Die individuellen Lösungen umfassen SIEM-Tools, Support-Leistungen für den Schutz von IT-/OT-Umgebungen und gesonderte Anwendungen für Multi-Vendor-Umgebungen. Hierfür fügen die telent-Spezialisten einen Mix aus unterschiedlichen Technologien aus Hard- und Software, maschinellem Lernen und künstlicher Intelligenz zusammen. Der Datenfluss wird lückenlos überwacht, und durch Korrelationsinformationen und Algorithmen werden Gefahren schnell erkannt und durch Alarme sichtbar gemacht. Im Security Operation Center (SOC) hat das Experten-Team von telent das Netz kontinuierlich im Blick, sucht nach Bedrohungen und entfernt sie. Das Managed Security Portfolio beinhaltet üblicherweise die 24/7-Netzüberwachung mit Echtzeitalarmierung und Notfallkonzepten. Der integrierte Incident-Management-Workflow sorgt für die umgehende Behebung von Angriffen und Ausfällen.
Neben den zahlreichen technischen Anpassungen gilt es, die sicherheitsrelevante Aufmerksamkeit bei den Mitarbeitern zu schulen. In Trainings und Kampagnen werden die Mitarbeiter angeleitet, das System durch ihr sicheres Verhalten gegen Angriffe zu härten.

Netzsegmentierung, Systemhärtung und Sandboxing

Weitere Maßnahmen zum Schutz vor Angriffen von kriminellen Hackerorganisationen sind Isolierung, Systemhärtung und Sandboxing. Mit diesen drei Verfahren wird das System vor tiefgreifenden Risiken sowohl von innen als auch von außen geschützt. Mit dem Prinzip der Netzsegmentierung wird das Unternehmensnetz in unterschiedliche Segmente unterteilt. Fällt ein gehacktes Segment aus, bleibt das restliche Unternehmensnetz weiterhin funktionsfähig.
Der Einfluss des sicherheitsrelevanten Faktors Mensch soll durch Systemhärtung kleingehalten werden. Daher werden Regeln festgelegt, wer auf welche Systeme und deren Unterbereiche Zugriff hat und wer nicht.
Sandboxing (Sandkasten) steht für eine Technik, mit der eine Software oder ein Prozess innerhalb einer isolierten, von den restlichen System- oder Netzressourcen abgeschotteten Laufzeitumgebung ausgeführt wird. Das gesamte System ist in mehrere Sandboxes unterteilt, so dass das Betriebssystem und kritische Anwendungen isoliert betrieben werden können. Eindringlinge und Malware können so nicht auf diese Bereiche zugreifen. Der große Vorteil dieser Methode: Sie schützt auch vor Zero-Day-Exploit-Attacken, bei denen Sicherheitslücken ausgenutzt werden, bevor sie geschlossen werden können. telent integriert diese Maßnahmen in das individuell angepasste und umfassende Managed-Security-System.

Schutzmauer gegen kriminelle Hacker

Besonders gefährdet sind Betreiber von kritischen Infrastrukturen (KRITIS), z.B. Verkehr, Gesundheitsversorgung, Energie und ITK-Technik. Störungen und Ausfälle können eine signifikante Gefahr für Gesellschaft, Wirtschaft und Staat darstellen.
Kritische Infrastrukturen benötigen ein hohes Schutzniveau, um zielgerichteten Angriffen von kriminellen Organisationen und Hackern standhalten zu können. Maßnahmen zur Systemhärtung helfen, solche Gefah-

telent GmbH, www.telent.de

ren abzuwehren, und schützen gleichzeitig vor Risiken, die Mitarbeiter oder Fremdfirmen durch Bedienfehler verursachen. Härten bedeutet, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software eingesetzt wird, die für den Betrieb des Systems notwendig ist und deren unter Sicherheitsaspekten korrekter Ablauf garantiert werden kann. Gemeinsam mit dem auf Cybersicherheit spezialisierten Tochterunternehmen KORAMIS und mit weiteren Partnern stellt telent ein komplettes Portfolio von Produkten und Dienstleistungen bereit, mithilfe dessen Betreiber von KRITIS diesen besonderen Sicherheitsanforderungen gerecht werden können.
KORAMIS erarbeitet kundenspezifische Lösungen für Automatisierungs-, Prozess- und Netzleittechnik und ist der führende Anbieter von ganzheitlichen Lösungsangeboten im Bereich Industrial Continuity Management – kurz ICM – mit den Kernkompetenzfeldern Industrial Security, Industrial Software und Industrial Automation. Durch das Bündeln ihrer Kernkompetenzen bieten die beiden Unternehmen schon heute umfangreiche Sicherheitslösungen für die Zukunftsmärkte Industrie 4.0, Internet der Dinge (IoT) und Smart Energy. Dies beginnt mit einer ganzheitlichen Schwachstellenanalyse der gesamten IT-Infrastruktur und reicht bis zur kontinuierlichen Sicherheitsüberwachung in Echtzeit. Neben der Analyse gehört zu unserem Ansatz auch die Überprüfung der individuellen Security-Strategie. Diese verringert das Risiko externer und interner Systemmanipulationen erheblich und erhöht den Schutz Ihrer IT-Infrastruktur maßgeblich.

Private LTE-/5G-Campusnetze – Schlüsseltechniken der digitalen Transformation

Neue digitale Anwendungen im Industrie- und KRITIS-Umfeld erfordern eine zuverlässige, schnelle und sichere Datenkommunikation. Durch die Bereitstellung des Frequenzbereichs von 3,7 bis 3,8 GHz für private Mobilfunknetze hat die Bundesregierung den Weg für Campusnetze, z.B. für die chemische Industrie, Logistikdienstleister, größere Mittelständler, lokale Industrieanlagen und Forschungseinrichtungen bereitet.
Eigene pLTE-/5G-Campusnetze bieten schon mal eine hohe Datensicherheit, weil die Daten das eigene Netz nicht verlassen und so weniger Angriffsfläche geboten wird. Zudem kann das Netz durch ein eigenes, optimal angepasstes Sicherheitssystem vor Hackerangriffen geschützt werden.
Extrem hohe Bandbreiten, kurze Signallaufzeiten und die Möglichkeit, eine große Anzahl an Endgeräten einzubinden, sind weitere Vorteile eines privaten Netzes. Der neue Standard für 5G ermöglicht mit seinen erweiterten Leistungsmerkmalen völlig neue Einsatzmöglichkeiten für den Mobilfunk in der Industrie (Industrielles Internet der Dinge – IIoT). Private pLTE-/5G-Campusnetze ermöglichen somit neue Anwendungsszenarien wie die Effizienzsteigerung in der Produktion durch Augmented Reality (AR). Unternehmen haben zudem die volle Kontrolle über ihre Funkinfrastruktur und schaffen somit eine zukunftssichere, flexible und ausbaufähige Kommunikationslösung.

Die telent-Spezialisten fügen für ihre individuellen Managed-Security-Lösungen einen Mix aus unterschiedlichen Technologien aus Hard- und Software, maschinellem Lernen und künstlicher Intelligenz zusammen

Technik und Services für Breitbandnetze

Eine schnelle Internetanbindung ist heute ein bedeutender Standortvorteil für Städte und Kommunen. Bei der Nutzung zeichnet sich ein klarer Trend in Richtung TriplePlay (schnelles Internet, TV und Telefonie) ab.
Fundamentale Planung, solide Durchführung, konsequente Betreuung und Nachbetreuung sind entscheidende Erfolgsfaktoren beim Breitbandausbau. Der Aufbau von Netzinfrastrukturen für FTTx-Breitbandzugänge braucht ein abgestimmtes Vorgehen – von der Bedarfsermittlung über die Planung und Bauausführung bis hin zu Betrieb und Wartung. Als herstellerunabhängiger Systemintegrator arbeitet telent mit ausgewählten Herstellern zusammen und unterstützt Unternehmen, Energieversorger und Kommunen mit langjähriger Erfahrung in der kompletten Wertschöpfung für FTTx-Projekte.
telent deckt die komplette Wertschöpfungskette bei FTTx-Projekten ab. Als herstellerunabhängiger Systemintegrator arbeitet telent zudem mit ausgewählten Herstellern zusammen und liefert aktive und passive Komponenten, um hochwertige Breitbandnetze zu bauen. Maßgeschneiderte Netzkonzepte umfassen moderne Hybridtechnologien sowohl für den kombinierten kupferbasierten Ausbau als auch den Glasfaserausbau. telent plant gemeinsam mit dem Kunden und liefert zudem vorkonfektionierte und vormontierte Multifunktionsgehäuse (MFG) mit aktiver Technik für den KVz-Ausbau. Diese sind als Outdoor-Standorte sowie Gesamtlösungen für den kombinierten FTTx-Ausbau mit allen Technologien und passenden Endgeräten geeignet.
Wir entwickeln individuelle Ende-zu-Ende-Lösungen für die aktive Technik unter Berücksichtigung der aktuellen Anforderungen für OPEN ACCESS mit Diensteanbietern und Netzbetreibern.