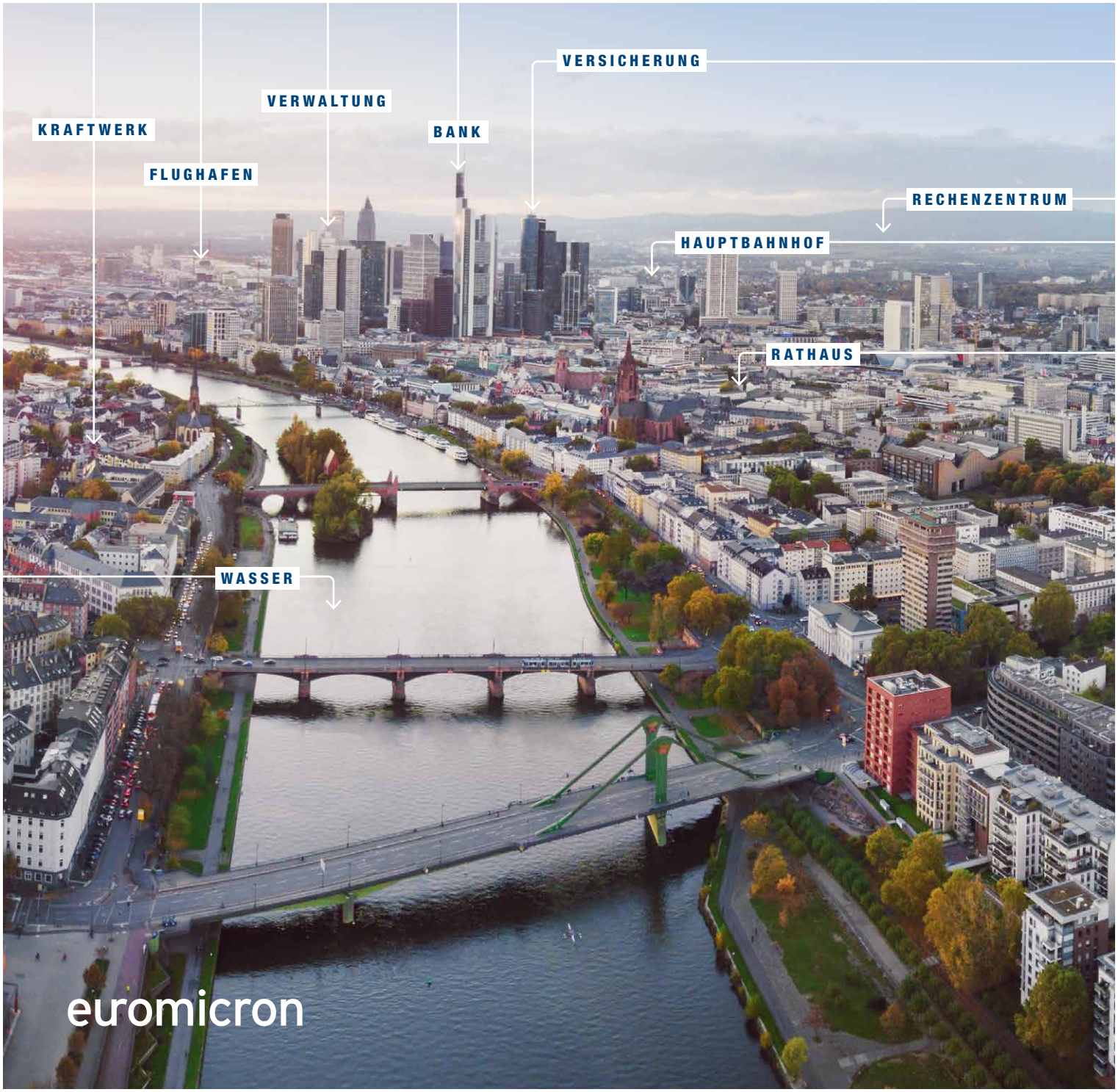
Kritische Infrastrukturen

euromicron
trendpaper

Verfügbarkeit
Sicherheit
Performance



Sichere Infrastrukturen

Wir leben in einer vernetzten Welt. Netzwerkinfrastrukturen sind die Lebensadern moderner Gesellschaften. Besondere Wichtigkeit hat ihre Funktionsfähigkeit für den Betrieb Kritischer Infrastrukturen (KRITIS). Die Bundesregierung stuft „Organisationen und Einrichtungen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“, als Kritische Infrastrukturen ein.

KRITIS gliedern sich in die neun Sektoren:

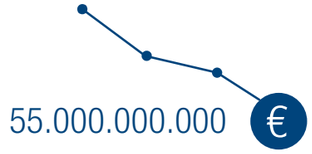
Energie ‹
Transport und Verkehr ‹
IT- und Telekommunikation ‹
Gesundheit ‹
Wasser ‹
Ernährung ‹
Finanz- und Versicherungswesen ‹
Staat und Verwaltung ‹
Medien und Kultur ‹

Digitalisierung erfordert Sicherheit

Auch KRITIS-Betreiber nutzen die heutigen technischen Möglichkeiten der Automatisierung, der Vernetzung sowie die Chancen, die das „Internet der Dinge“ bietet, um ihre Prozesse zu optimieren, die Produktivität zu steigern und Kunden zu binden. An die Netze der KRITIS-Betreiber werden spezielle Anforderungen hinsichtlich der Verfügbarkeit, Integrität und Vertraulichkeit gestellt. Einerseits geht es um Sicherheitsstandards und Abwehr von Angriffen, andererseits um ausreichend ausfallsichere Systemlösungen.

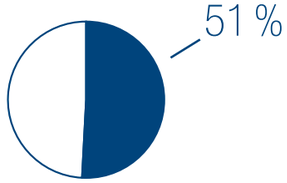
Für KRITIS-Betreiber gelten höchste Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit und Nachvollziehbarkeit ihrer IT-Infrastruktur. Nur so wird Stabilität gewährleistet.

Im IT-Sicherheitsgesetz, das Mitte 2015 in Kraft trat, hat der Gesetzgeber die KRITIS-Betreiber dazu verpflichtet, bis zum Jahr 2020 wirkungsvolle technische und organisatorische Vorkehrungen zur Vermeidung und zur Nachvollziehbarkeit von Störungen zu treffen. Die euromicron Gruppe ist mit den Anforderungen, Richtlinien und Normen zur Umsetzung vertraut und schnürt für KRITIS-Unternehmen ein rechtssicheres Gesamtpaket.



Laut Bitkom entsteht der deutschen Wirtschaft durch Spionage, Sabotage und Datendiebstahl jährlich ein Schaden von 55 Milliarden Euro.

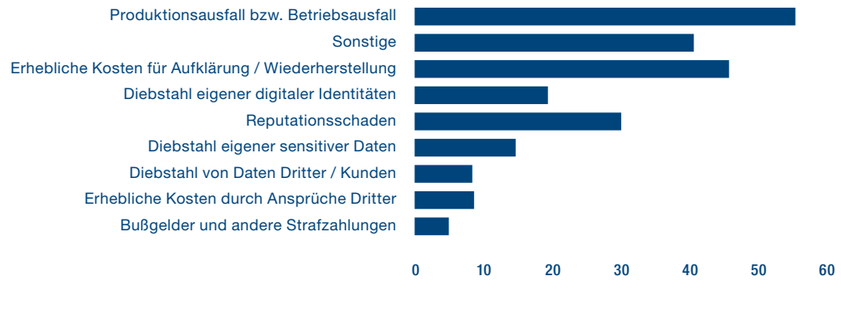
Der Branchenverband Bitkom schätzt, dass bereits mehr als 51% aller Firmen Opfer von **Industriespionage** wurden.



85 %

der befragten Betreiber Kritischer Infrastrukturen waren im Jahr 2016 Ziel einer Cyberattacke.

Von 169 Befragten gaben ... folgende Schäden an:



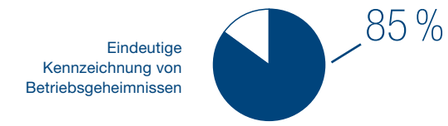
Angriffe von Hackern auf IT-Netze können verheerende Folgen haben.

Das zeigte im Mai 2017 der Hackerangriff mit der Schadsoftware WannaCry auf Firmen und Behörden: Krankenhäuser in Großbritannien mussten ihre Patienten nach Hause schicken,

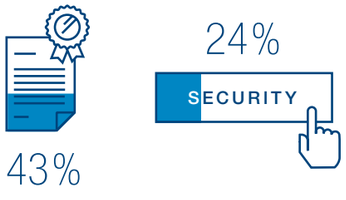
450 Computer der Deutschen Bahn waren lahmgelegt.

Vor ein paar Jahren machte der Computerwurm Stuxnet von sich reden, weil er wichtige Komponenten von Anlagen zur Uranaufbereitung auszuschalten drohte.

Organisatorische Sicherheit



Nur wenige Unternehmen führen Sicherheits-Zertifizierungen oder regelmäßige Sicherheits-Audits mit externen Spezialisten durch.



Laut Bitkom: Nur jedes dritte Unternehmen meldet Attacken. Die Sorge in Bezug auf Imageschäden schreckt davon ab, über Cyberkriminalität zu reden.

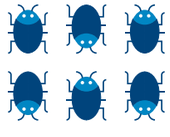
In den vergangenen zwölf Monaten wurden zwei Drittel der Unternehmen (67 Prozent) Opfer von mindestens einem IT-Angriff. Weitere 14 Prozent vermuten einen solchen, sind sich aber nicht sicher.

Die in Komponenten für industrielle Kontrollanlagen gefundenen Schwachstellen haben sich in fünf Jahren verzehnfacht. Im Jahr 2015 bekannten Lücken gelten 49 Prozent als kritisch, 42 Prozent als mittelschwer.

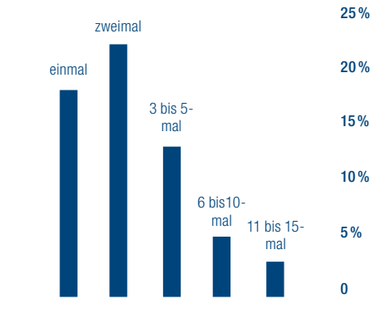
Die Lage der IT-Sicherheit in Deutschland 2016

560 MIO.

Gesamtzahl der bisher bekannten Schadprogramm-varianten für Computersysteme



Zahl der Zwischenfälle, die die Kontrollsysteme von Anlagen betrafen



Wir verbinden Kompetenz mit Effizienz

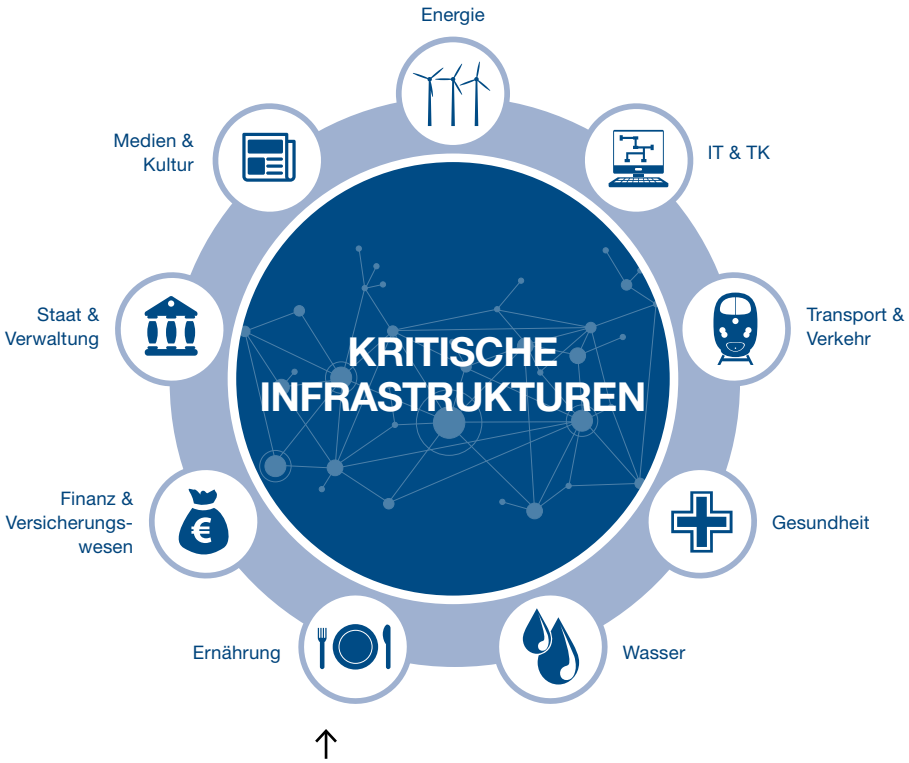
euromicron ist der deutsche Spezialist für das „Internet der Dinge“. Wir versetzen unsere Kunden in die Lage, Prozesse und Infrastrukturen effizient und sicher zu vernetzen und den Weg in die digitale Zukunft erfolgreich zu gestalten. Betreiber Kritischer Infrastrukturen und Industrieunternehmen vertrauen auf unsere Expertise. Insbesondere **telent verfügt über umfassende Praxiserfahrung als Systemintegrator und Spezialist für Planung, Aufbau und Betrieb sicherer Netze und Systeme im Bereich KRITIS. **KORAMIS** bringt darüber hinaus spezialisierte Expertise für ganzheitliche Lösungen rund um Cybersecurity, Automatisierungs-, Prozess- und Netzleittechnik mit.**

GANZHEITLICHE LÖSUNGEN FÜR JEDE UNTERNEHMENSGRÖSSE

Gerade für kleine und mittelständische KRITIS-Betreiber stellt es eine Herausforderung dar, die Anforderungen des Gesetzgebers mit eigenen Ressourcen umzusetzen. Wir bieten deshalb maßgeschneiderte Lösungen für Unternehmen jeder Größenordnung an. Auf Kundenwunsch integrieren wir die Technik in die bestehenden Systeme. Wir verbinden Informationssicherheit und Verfügbarkeit mit Investitionssicherheit und erzeugen Mehrwert: Wir legen unseren Fokus in vernetzten Umgebungen einerseits auf die Minimierung von Risiken und andererseits auf die Steigerung von Effizienz und Produktivität.

Unser Schwerpunkt liegt auf:

- IP- und Betriebsnetzen
- IoT-Funklösungen
- Smart Services
- Cybersecurity
- Managementsystemen für Informationssicherheit (ISMS)
- PMR-(Professional-Mobile-Radio-) Lösungen
- Netz- und Assetmanagement-Systemen
- Rund-um-die-Uhr-Service und -Support (24/7)



Das öffentliche Leben ist abhängig von funktionierenden Unternehmen und Institutionen. Unsere Aufgabe ist es, sie mit leistungsstarken und zuverlässigen Lösungen auszustatten.

euromicron hält für KRITIS-Betreiber ein komplettes Portfolio aus Sicherheitsprodukten und -dienstleistungen bereit. Damit werden Betreiber von KRITIS den Anforderungen auf Grundlage der Normen und Richtlinien an IT-Sicherheit gerecht.

Wir entwickeln für unsere Kunden individuelle Security-Strategien mit Blick für das Ganze: So schärfen wir auch das Bewusstsein der beteiligten Menschen für sicherheitsrelevante Themen und kümmern uns um die Abwehr von Cyberangriffen, wie sie beispielsweise von kriminellen Organisationen ausgehen.

KRITISCHE INFRASTRUKTUREN

Prozess zur hochverfügbaren IoT-Infrastruktur

Wir unterstützen KRITIS-Betreiber bei der Erarbeitung maßgeschneiderter vertikaler Lösungskonzepte, IoT-Migrationsstrategien sowie Cybersecurity-Maßnahmen. Dazu stellen wir die jeweils technisch und wirtschaftlich sinnvollsten Lösungen aus den Bereichen Infrastruktur, Plattform, Applikation und Service bereit.

SCHRITT 1

Analyse der Ist-Situation

- Beratung
- Bestandsaufnahme
- Systemplanung im geforderten Rahmen, zum Beispiel gemäß IT-SiG, ISO 27001
- Ermittlung von Optimierungspotenzialen

SCHRITT 2

Definition der Ziele

- Abgleich: Kundenanforderung, Sicherheit und Wirtschaftlichkeit
- Optimierungsziele und Steigerung der Effizienz definieren
- Überführung von bestehenden Technologien festlegen
- Beim Einsatz neuer Technologien: Best-of-Breed-Ansatz
- Systemintegration in Multivendor-Umgebungen
- Service-Konzepte definieren

SCHRITT 3

Konzept und Planung

- Technisches Konzept
- Art der eingesetzten Technologien bestimmen
- Netzplanung und NMS-Konzepte
- Sicherheitskonzept inklusive Rollen- und Rechtekonzept
- Notfallkonzept
- Business-Continuity-Konzept
- Zulassung

SCHRITT 4

Umsetzung

Implementierung und Montage

- Standort- und Infrastrukturmanagement
- Infrastrukturbaumaßnahmen
- Installation und Inbetriebnahme

Projektmanagement

- Projektplanung und -kontrolle
- Bauüberwachung
- Transport- und Logistiksteuerung
- Berücksichtigung von Informationen aus Planung und Workflowmanagement für Inbetriebnahme, Aufbau und Wartung
- Dokumentation

Normenkonforme Umsetzung von Cybersecurity gemäß folgenden Richtlinien und Regelwerken:

- Security gemäß IEC 62443
- ISO/IEC 27001 ff.
- BSI-Grundschutz und -Branchenstandards

SCHRITT 5

Service-Support und Betrieb

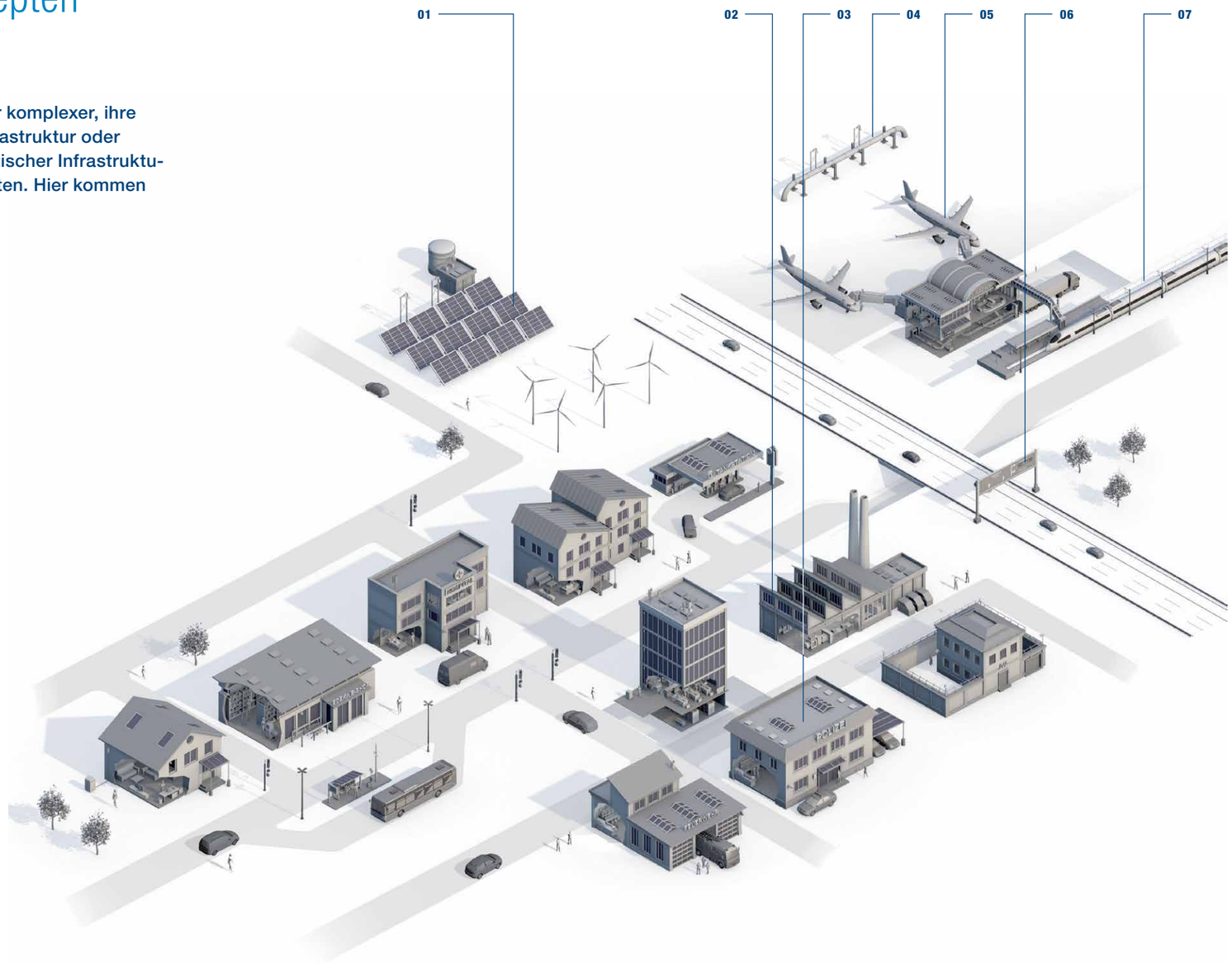
- Vor-Ort-Kundeneinsatz und Instandhaltung
- Logistik-, Ersatzteile- und Reparaturmanagement
- Service Competence Center (SCC)
- Betriebsführung (NOC)
- Qualifizierung und Training
- **Managed Security Services**
  Betrieb, Überwachung und Support Ihrer (Industrial)-Security-Umgebung
- **Schwachstellenanalyse**
  Aufzeigen von Schwachstellen und Ausarbeitung von Lösungsvorschlägen
- **Systemhärtung**
  Absicherung kritischer Systeme mittels Whitelisting bzw. Sandboxing
- **Schulung und Bewusstseinsbildung von Mitarbeitern aller Ebenen**

Die Vorteile der KRITIS-Expertise von euromicron:

- Tiefe Kenntnis des Kundennetzes ermöglicht optimierte Lösungen
- Alles aus einer Hand – schlüsselfertig
- Flächendeckender Service
- Rund-um-die-Uhr-Support

IoT-Lösungen in Stadtkonzepten von heute und morgen

Das Zusammenspiel einzelner Systeme wird immer komplexer, ihre Verfügbarkeit immer wichtiger. Ausfälle bei der Infrastruktur oder betriebskritischen Anwendungen der Betreiber Kritischer Infrastrukturen kann sich eine moderne Gesellschaft nicht leisten. Hier kommen wir ins Spiel.



AUSWAHL AN REFERENZPROJEKTEN:

01 – Energieversorger
Zuverlässige Energieinformationsnetze für einen stabilen Betrieb im Bereich Kraftwerke, Smart Grid und dezentrale Energieversorgung

02 – Versorgung und Entsorgung
Überwachungssysteme zur Wasserver- und -entsorgung, Smart Services zur Optimierung der Abfallwirtschaft

03 – Behörden und Sicherheitskräfte
Ausfallsichere und resiliente Kommunikationsnetze, Notfall- und Überwachungssysteme

04 – Tunnel
Hochverfügbare IP- und Sicherheitsinfrastruktur, Netzwerktechnik, Industrie-Switche, Videoüberwachung

05 – Flughäfen
Ganzheitliche Sicherheitstechnik: Flugleitsysteme, Betriebsfunk, Fluchttürsteuerung, Brandmeldetechnik, Videoüberwachung

06 – Individualverkehr
Dynamische Verkehrs- und Parkleitsysteme

07 – Bahn / Schienenverkehr
Leitstandtechnik und Videosysteme, Kommunikationssysteme für die Vernetzung elektronischer Stellwerke

DIE WEICHEN STEHEN AUF „FAHREN“

Im Schienenverkehr geht es immer ums Timing. Ausfälle an der Infrastruktur zu kompensieren ist aufwendig, kostet Zeit und verringert die Pünktlichkeit. Weichen sind dabei ein entscheidender Infrastrukturbaustein – für reibungslose Abläufe müssen sie unter höchsten Belastungen zuverlässig funktionieren. Mit vorbeugender Wartung (Predictive Maintenance) sorgt euromicron im Schienenverkehr eines großen Schienennetzbetreibers für reibungslosen Betrieb. Störungen werden frühzeitig erkannt, Teile können schon vor einem Ausfall ausgetauscht werden. Der Vorteil: Die vorbeugenden Wartungsarbeiten werden so geplant, dass sie den laufenden Schienenverkehr nicht beeinträchtigen.

https://www.euromicron.de/referenzen/gefahrenmanagement-sicherheitstechnik

KRITISCHE INFRASTRUKTUREN

Ihre nächsten Schritte zur Sicherung Ihrer Kritischen Infrastruktur

01 Ist Ihre Organisation vom IT-Sicherheitsgesetz betroffen?

02 Haben Sie eine verabschiedete (IT-)Sicherheitsrichtlinie sowie ein Sicherheitskonzept?

03 Gibt es in Ihrem Unternehmen einen entsprechend qualifizierten Sicherheitsbeauftragten?

04 Ist das Personal in (IT-)Sicherheitsfragen und dem Umgang mit (IT-)Sicherheitsvorfällen geschult?

05 Unterhalten Sie ein Informationssicherheitsmanagementsystem (ISMS)?

06 Liegen Notfallkonzepte für kritische IT-Anwendungen Ihrer ITK-Infrastruktur vor?

07 Gibt es ein Business-Continuity-Management, das die Wiederaufnahme des Betriebes nach Schadensfällen gewährleistet?

Fragen Sie uns!

Wir beraten Sie gerne und ebnen den Weg zur Sicherheitsorganisation mit optimalem Nutzen für Ihr Unternehmen.

IMPRESSUM

Herausgeber und Copyright

euromicron AG

Zum Laurenburger Hof 76
60594 Frankfurt am Main

Tel.: +49 69 631583 - 0
Fax: +49 69 631583 - 17

info@euromicron.de
www.euromicron.de

Konzept, Gestaltung und Realisation

MPM Corporate Communication Solutions, Mainz
www.mpm.de

euromicron