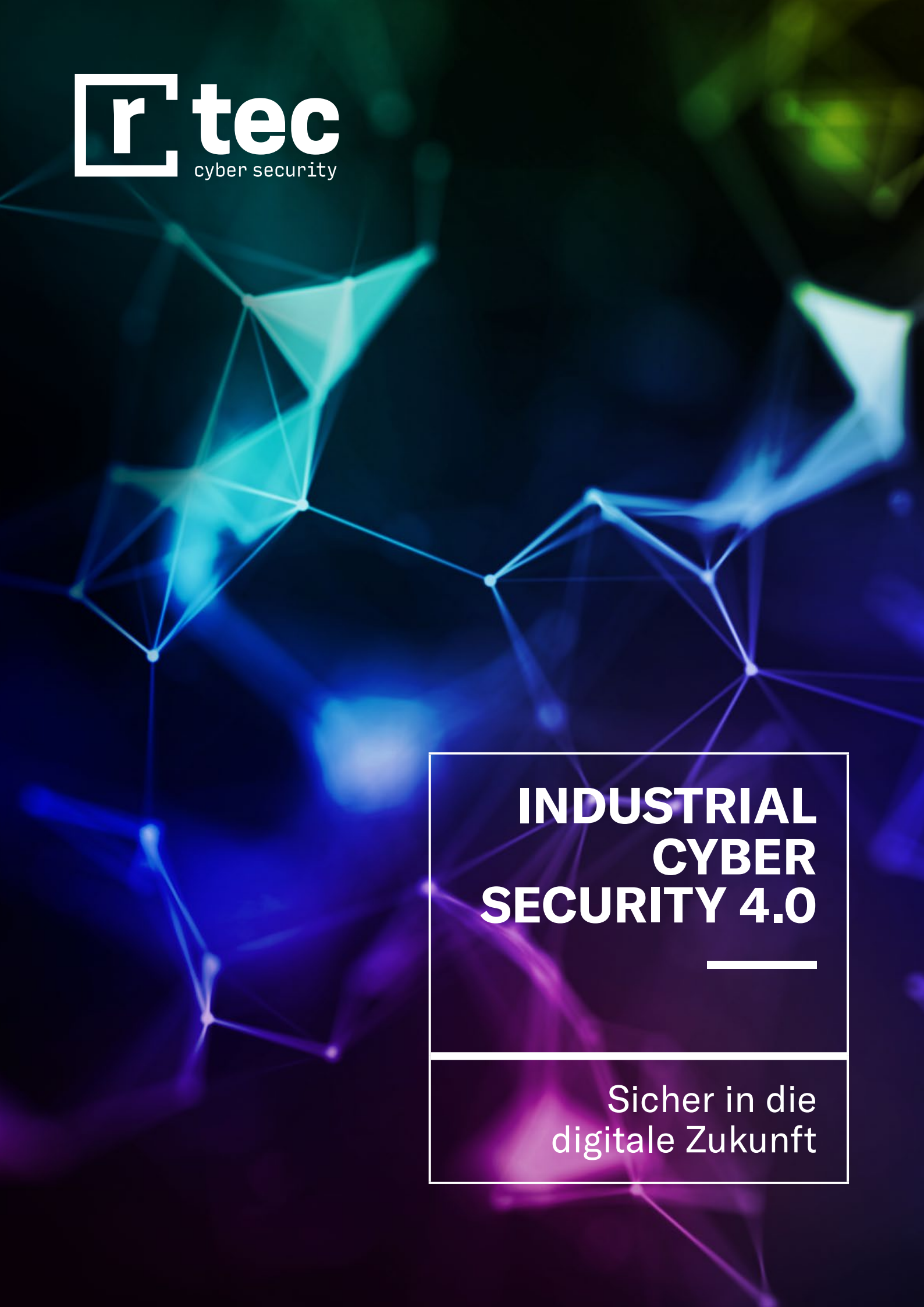

r tec
cyber security
INDUSTRIAL CYBER SECURITY 4.0
Sicher in die digitale Zukunft

Industrial Cyber Security 4.0

Industrie 4.0

Die Vernetzung von Maschinen und Anlagen und der schnelle Datenaustausch zwischen Office-Welt, Engineering, Produktion und Logistik, kunden- und lieferantenübergreifend, sind das Rückgrat der Industrie 4.0 und bieten eine Optimierung und Erweiterung der Wertschöpfungskette. Unternehmen sind aus digitaler Sicht grenzenlos geworden.

Mit der Öffnung der bisher hermetisch abgesicherten Produktionsbereiche und der fortschreitenden Vernetzung der Produktionssysteme mit Informations- und Kommunikationssystemen steigt das Risiko, Opfer von Cyber Angriffen zu werden.

Während Angriffe auf Basis von Verschlüsselungstrojanern oder Social-Engineering-Attacken im Office-Netzwerk auf die Erpressung von Geld abzielten, sind erfolgreiche Attacken im Produktionsumfeld ungleich gefährlicher. Massive Störungen, Produktionsausfälle bis hin zum Stillstand der kompletten Produktion und Schäden in Millionenhöhe können die Folgen sein.

IT Security ist Teil der Wertschöpfung und kein Kostenthema. Kritische Einheiten müssen über die gesamte Wertschöpfungskette geschützt werden.

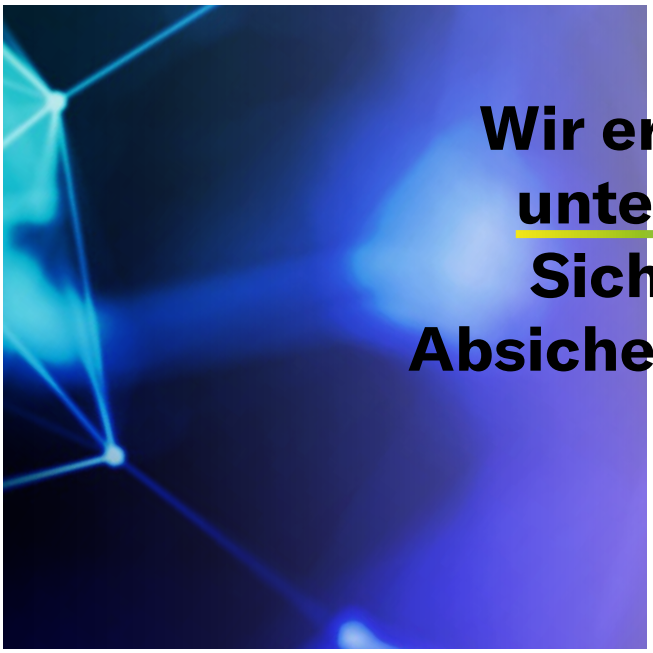
Nur mit Security 4.0

Cyber Security ist daher ein kritischer Erfolgsfaktor für eine erfolgreiche Digitalisierungsstrategie in der Industrie. Etablierte IT-Security-Maßnahmen aus der Office-Welt sind aufgrund der Besonderheiten der Maschinen und Anlagen – extreme Verfügbarkeitsanforderungen, langen Lebenszykle und Zugriffseinschränkungen – nicht oder nur bedingt übertragbar.

Produktionsnetzwerke erfordern individuelle und häufig mehrstufige, kombinierte Lösungen, um vor Viren- oder Malware-Befall, Datendiebstahl und Industriespionage sowie vor menschlichem Fehlverhalten und Sabotage geschützt zu sein.

Bedrohungen im Umfeld Produktion/Industrie 4.0

- Malware jeder Art, da Virenschutzprogramme und regelmäßige Updates in Steuerungen und deren Betriebssystemen oft nicht realisiert werden können
- Verschlüsselungstrojaner als Spezialform der Malware, die inzwischen auch gezielt für Industrieumgebungen entwickelt werden
- Industriespionage, häufig auch durch Fremdstaaten gelenkt
- Manipulation und gezielte Sabotage von Systemen
- Menschliches Versagen/Bedienungsfehler, die gravierende Auswirkung auf das Gesamtsystem aufgrund der hohen Vernetzung haben können



Wir erarbeiten mit Ihnen ein unternehmensspezifisches Sicherheitskonzept für die Absicherung Ihrer Produktion.

Dr. Stefan Rummenhöller, Geschäftsführer und Firmengründer

Unsere Vorgehensweise

- Analyse des Ist-Zustandes und Erstellung eines Cyber Security Konzeptes passend zum jeweiligen Industrieumfeld und der bereits vorhandenen AnlagenSicherheitsarchitektur
- Aufbau der für das Industrieumfeld, Anlagen, Steuerungen und Leitsysteme passenden Schutzmaßnahmen
- Überwachung der Anlagennetze und aller verbundenen Systeme auf sicherheitsrelevante Hinweise und Ereignisse
- Konzeption für den Umgang mit Vorfällen, Datensicherungskonzept, erprobtes Notfallkonzept

Herausforderungen und Lösungen im Detail.

SCHNELLE BEDROHUNGSERKENNUNG

Kennen Sie die aktuellen Gefahren für Ihre Wertschöpfungskette?

Identifikation der Bedrohungen

- Industrial Cyber Security Audit (rICSA)
- Architekturreview Industrie 4.0
- Industrial IT Pentest
- Threat Information Service

TECHNISCHER ANLAGENSCHUTZ

Sind Sie ausreichend abgesichert?

Schutzmaßnahmen implementieren und betreiben

- Geräteverwaltung und SPS-Versionskontrolle
- Netzwerkseparierung und Netzwerkzugriffskontrolle
- Berechtigungsverwaltung und sicherer Fernzugriff
- Kapselung kritischer Produktionskomponenten
- Applikationskontrolle

SCHNELLE ANOMALIEERKENNUNG

Sehen Sie Abweichungen rechtzeitig?

Überwachung der Wertschöpfungskette auf sicherheitsrelevante Anomalien

- Anomalieerkennung
- Schwachstellenüberwachung
- Security Monitoring (SIEM)

INCIDENT RESPONSE

Wie reagieren Sie auf Vorfälle und Angriffe?

Vorfälle analysieren, Angriffe stoppen, Normalbetrieb wiederherstellen

- Incident Response Team
- Cyber-Threat-Analyse
- Remediation Manager

INDUSTRIAL CYBER SECURITY 4.0 MANAGEMENT

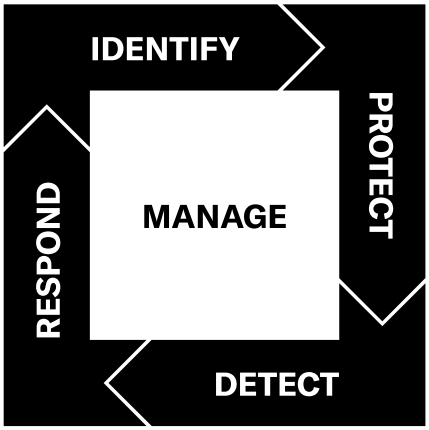
Halten Sie alle Fäden in der Hand?

Steuerungssystem implementieren und betreiben

- ISMS Industrie 4.0
- Risikomanagement
- Notfallmanagement
- Audit-Services
- Awareness-Trainings

Unser Ansatz.

Mit unserem Cyber Security Framework stellen wir Ihnen den aktuellen Standard zur Bewältigung Ihrer Cyber Security Herausforderungen vor. Wir bestimmen Stärken und Schwächen und liefern Ihnen die Services für Ihre Strategie und Sicherheitsarchitektur.



INDUSTRIE 4.0

CLOUD

DATACENTER

ENDPOINT

IDENTIFY_ Identifizierung der Bedrohungen und geschäftskritischer Anwendungen, Systeme und Daten. **PROTECT_** Design und Implementierung von Schutzmaßnahmen. **DETECT_** Überwachung zur frühzeitigen Erkennung drohender Vorfälle. **RESPOND_** Vorfallsanalyse, Angriffsabwehr, Wiederherstellung des Betriebs. **MANAGE_** Governance, Risk and Compliance umfassen alle Bausteine für ein erfolgreiches Cyber Security Management.

Warum r-tec.

Unsere Kernkompetenz

- Technisch voraus, menschlich auf Augenhöhe
- Passgenaue Servicelösungen, kurze Reaktionszeiten, schnelle Terminierung, direkter Expertenkontakt
- Schnelle Hilfe im Angriffsfall
- Spezialisiertes Cyber Security Unternehmen mit ausgeprägter Service-Struktur
- 20 Jahre Erfahrung in Konzeption, Aufbau und Betrieb von Cyber Security Lösungen
- Zertifiziert nach ISO 9001 und ISO 27001

For your objectives.

r-tec cyber security

Die r-tec IT Security GmbH, mit Sitz in Wuppertal, wurde 1996 von Dr. Stefan Rummenhöller gegründet. Als Wegbereiter und Wegbegleiter schaffen wir für unsere Kunden sichere Räume für die Entwicklung ihrer Organisationen und die Verwirklichung ihrer Visionen. Unsere Kunden aus dem gehobenen Mittelstand, Konzerne, kommunale Rechenzentren und Bundes- oder Landesbehörden vertrauen seit über 20 Jahren auf unsere hoch spezialisierten Experten.

Als Strategic Supplier für Cyber Security Services schützen wir die Werte unserer Kunden vor Bedrohungen und begleiten ihr Security Management von der Initiierung über die Einführung bis zum Betrieb auf allen Ebenen.

Wir leben Regeltreue, höchste Qualitätsstandards und Servicementalität. Unser Unternehmen haben wir nach den Strukturen und Richtlinien der DIN ISO 9001:2015 und der ITIL aufgebaut. Wir sind nach ISO 27001 zertifiziert.

r-tec IT Security GmbH | Hatzfelder Str. 167 | 42281 Wuppertal
www.r-tec.net | +49 (0) 202 31767–100