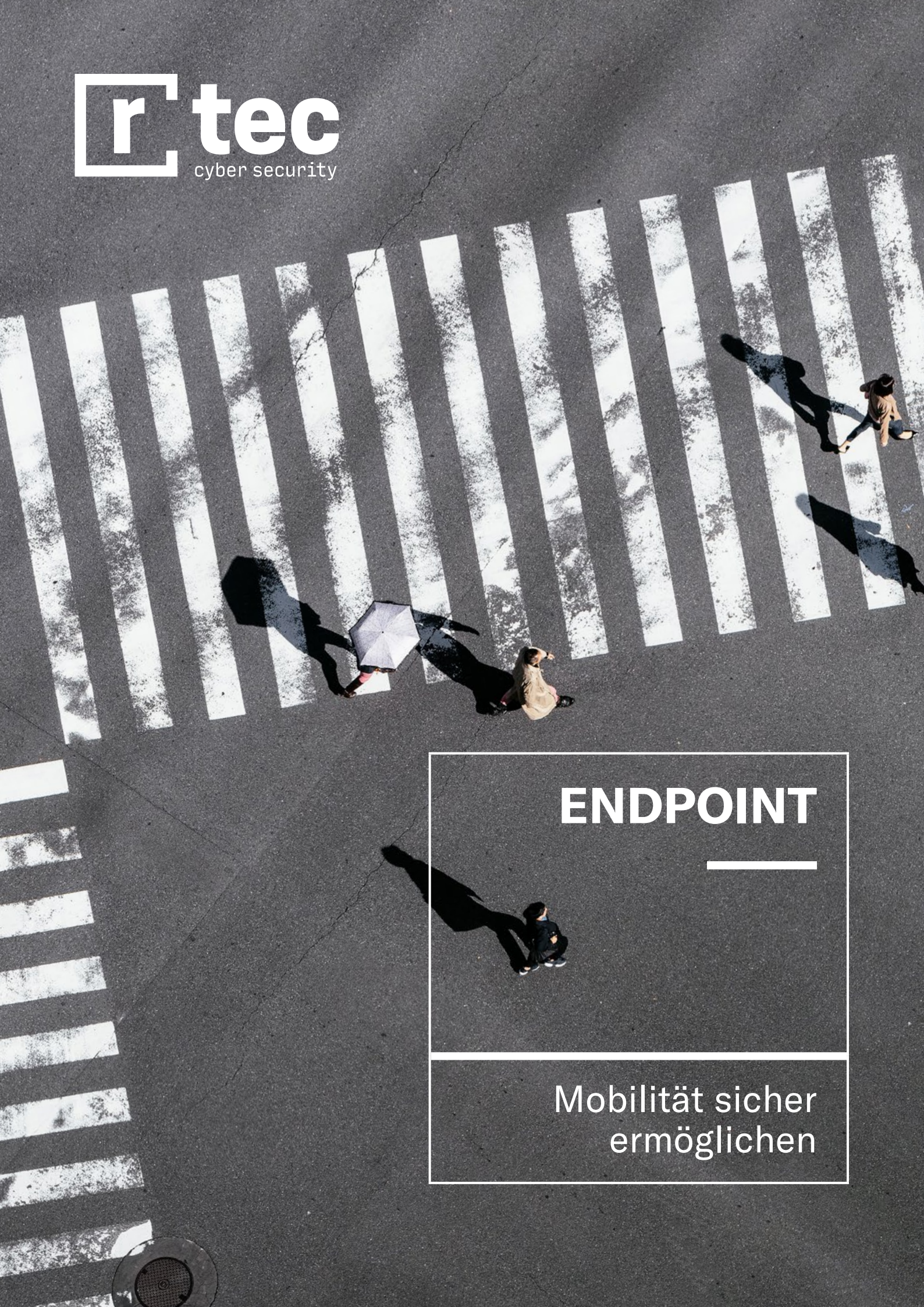
r tec
cyber security



ENDPOINT

Mobilität sicher ermöglichen

Endpoint.

Die Realität

Tausende Geräte in hundert verschiedenen Modellen mit Dutzenden unterschiedlichen Betriebssystemen, Server, PCs, Notebooks, Smartphones, Tablets, Barcode-Scanner, Point-of-Sales Terminals, das ist in vielen Unternehmen Alltag und mit der boomenden IoT-Welt wird die Anzahl weiter rapide wachsen. All diese Endpoints sind die zentralen Einfallstore für Angriffe auf die IT-Infrastruktur von Institutionen und Unternehmen und müssen verwaltet, kontrolliert und richtig abgesichert werden.

Die Zunahme an Ransomeware-Angriffen, Phishing-Mails, APT oder gezielter Industriespionage zeigt dies drastisch. Endpoint-Schutz muss jedoch mehr können, als Viren und Malware zu erkennen. Er muss offline und online Schutz bieten, Bedrohungen erkennen und schnelle Gegenmaßnahmen ermöglichen. Eine Strategie und ein unternehmensspezifisches Sicherheitskonzept sind unerlässlich.

Mobile Endgeräte bieten höchste Flexibilität in der Arbeitswelt und stellen gleichzeitig eines der größten Risiken für Datenverlust und Malwarevorfälle dar.

Die Lösung – Endpoint Data Protection

Der Schutz der Endgeräte lässt sich nicht allein durch technische Schutzmaßnahmen realisieren. Umfassender Schutz erfordert einen ganzheitlichen Ansatz, der alle Blickwinkel der Informationssicherheit berücksichtigt.

Im ersten Schritt gilt es, die möglichen Angriffstore und typischen Angriffswege sowie die businesskritischen Anwendungen, Systeme und Daten, schlicht die unternehmensspezifischen Werte, zu identifizieren, die im Fokus der Angreifer stehen. Darauf aufbauend muss ein unternehmensspezifisches Sicherheitskonzept entwickelt werden, das die Punkte

- Endpoint Management & Protection
- Endpoint Detection & Response
- Mobile Security
- Faktor Mensch: Schulung und Sensibilisierung umfasst.

Und ... wirksame Endpoint-Security sollte immer branchenspezifisch sein.

Wir erarbeiten mit Ihnen ein unternehmens- und branchen-spezifisches Sicherheitskonzept für Ihre Endpoints.

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 Anlagen-Netze und aller verbundenen Systeme auf sicherheitsrelevante Hinweise und Ereignisse
- Konzeption für den Umgang mit Vorfällen, Datensicherungskonzept, erprobtes Notfallkonzept

Herausforderungen und Lösungen im Detail.

MALWARE

Wie stark ist Ihr Immunsystem?

Malwareschutz

- Architekturreview Malwareschutz und Ransomware
- Endpoint Next Generation (EDR, Threat Intelligence, Threat Emulation)
- Device und Application Control
- Cyber-Threat-Analyse

SICHERHEITSLÜCKEN

Kennen Sie Ihre Verwundbarkeiten?

Schwachstellenmanagement

- Security Ratings
- Vulnerability Scan
- Threat Information Service
- Remediation Manager
- Pentest

IDENTITÄTSMISSBRAUCH

Sind Sie sicher, dass die Richtigen Zugriff haben?

Identity & Access Management

- Multi-Faktor-Authentifizierung
- Directory Federation und Single Sign-on
- Mobile Device Management
- Zero-Trust-Architektur
- Passwortmanagement

DATENVERLUST UND SPIONAGE

Haben Sie Ihre Daten unter Kontrolle?

Datensicherheit

- Datenklassifizierung
- DLP am Perimeter und in der Cloud
- Digital Rights Management
- Datei- und Geräteverschlüsselung
- Secure Data Exchange

SICHERHEITSLÜCKE MENSCH

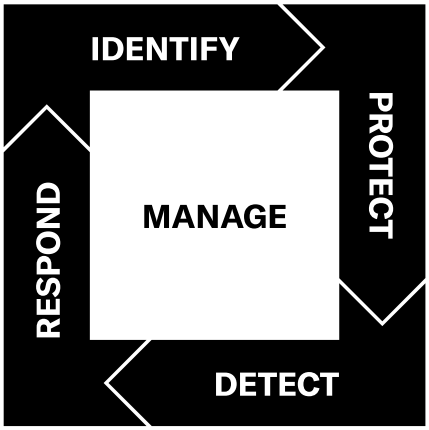
Kennen Sie jeden Enkeltrick?

Security Awareness

- Social-Engineering-Kampagnen
- Schulungen und Live-Hacking
- Awareness-Plattform
- Vorgaben- und Richtlinienerstellung

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.

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