IT-SICHERHEIT BRAUCHT VERBÜNDETE

Wir helfen Ihnen exzellenten Schutz gegen Cyberbedrohungen jeder Ausprägung und Komplexität aufzubauen.

root IT-SECURITY

UNSERE MISSION

Wir stehen Ihnen als Verbündeter Ihrer IT-Sicherheit
loyal und **bedingungslos** zur Seite.

Wir begleiten Sie **persönlich** durch alle Prozessphasen und
übernehmen uneingeschränkt Verantwortung für Ihre IT-Sicherheit.

root IT-SECURITY

MOTIVATION FÜR IT-SICHERHEIT

Angst	Reaktion auf Vorfälle, Auditergebnisse, „Beinahe-Vorfall“
Compliance	Rechts-, Vertrags-, Versicherungsanforderungen
Weitblick	IT-Risiken sind Geschäftsrisiken, Sicherheitskonzepte ermöglichen Innovation

AUFGABEN DER IT-SICHERHEIT

Risikomanagement

- Identifizieren, bewerten, behandeln und überwachen
- Geeignete Maßnahmen ergreifen
- Geschäftskontinuität sicherstellen

Investitionsberater

- Budgets zielgerichtet investieren
- Ressourcen wirksam einsetzen
- Sicherheitsziele und -maßnahmen aktiv steuern
- Ausrichtung an den Geschäftszielen

Reporting

- Abgewendeten Schaden sichtbar machen
- Vertrauen von Kunden, Partnern und Mitarbeitern stärken

Technologietreiber

- Neue Technologien sicher implementieren
- Chancen schnell und sicher nutzen
- Ermöglicher neuer Geschäftsmodelle

root IT-SECURITY

IT-SICHERHEIT BRAUCHT STRUKTUR

Struktur macht

die Komplexität, Dynamik und Kritikalität moderner

IT-Sicherheit beherrschbar

– und vermeidet Fehler, blinde Flecken oder ineffiziente Maßnahmen.

IT-SICHERHEITS-ASSESSMENT

Transparenz schaffen. Risiken verstehen. Sicherheit gestalten.

Ihr Lagebild für fundierte Entscheidungen in der IT-Sicherheit.

root IT-SECURITY

IT-SICHERHEITS-ASSESSMENT

Ziel des Assessments:

- Sicherheitsrisiken identifizieren und priorisieren
- Transparenz schaffen über die aktuelle Sicherheitslage
- Grundlage für eine strukturierte Sicherheitsstrategie schaffen
- Ressourcen gezielt einsetzen und priorisieren

IT-SICHERHEITS-ASSESSMENT

Risikoeinschätzung

- Wert der Daten und Prozesse
- Attraktivität für Angreifer
- Art der Angreifer
- Zielgerichtetheit des Angriffs
- Angriffe in der Vergangenheit

IT-Sicherheits-Check

- Governance und Compliance
- Risikomanagement und Sicherheitsstrategie
- Netzwerk- und Systemhärtung
- Zugriffskontrollen und Identitätsmanagement
- Incident Response und Business Continuity
- Awareness und Schulungen

Schwachstellenscan

- Netzwerkscan
- System- und Softwareschwachstellen
- Fehlkonfigurationen in Betriebssystemen und Serverdiensten
- Benutzer- und Zugriffsrechte
- Web-Applikations-Check
- Risikobewertung

root IT-SECURITY

WAS WIR TUN

Offensive Security

- AD Assessment
- (Interne) Penetration Tests
- Red Teaming
- Personalisierte Assessments

Consulting

- IT-Security-Check
- IT-Security Konzepte
- IT-Security Kompass
- Begleitung
- Revision

Services

- SIEM / SOC
- Network Access Control
- Unterstützung bei der Härtung Ihrer IT

Compliance

- BSI CyberRisikoCheck
- NIS2
- Umsetzung IT Sicherheit nach ISO 27001 auf Basis BSI IT-Grundschutz
- Einführung eines ISMS

root IT-SECURITY

ANDERE SAGEN PARTNERSCHAFT.

WIR SPRECHEN VON VERBÜNDETEN.

Wir begleiten Sie persönlich durch alle Prozessphasen und übernehmen uneingeschränkte Verantwortung für Ihre IT-Sicherheit. Fordern Sie jetzt Ihren persönlichen Sicherheitscheck bei uns an.

Simon Weber | Operations Lead

Telefon: +49 2262 71722-203,
Mobilfunk: +49 151 7020 3942
E-Mail: simon.weber@root.security

Benjamin Schorre | Geschäftsführer (CTO)

Telefon: +49 2262 71722-202,
Mobilfunk: +49 151 40106080
E-Mail: benjamin.schorre@root.security

root IT-SECURITY