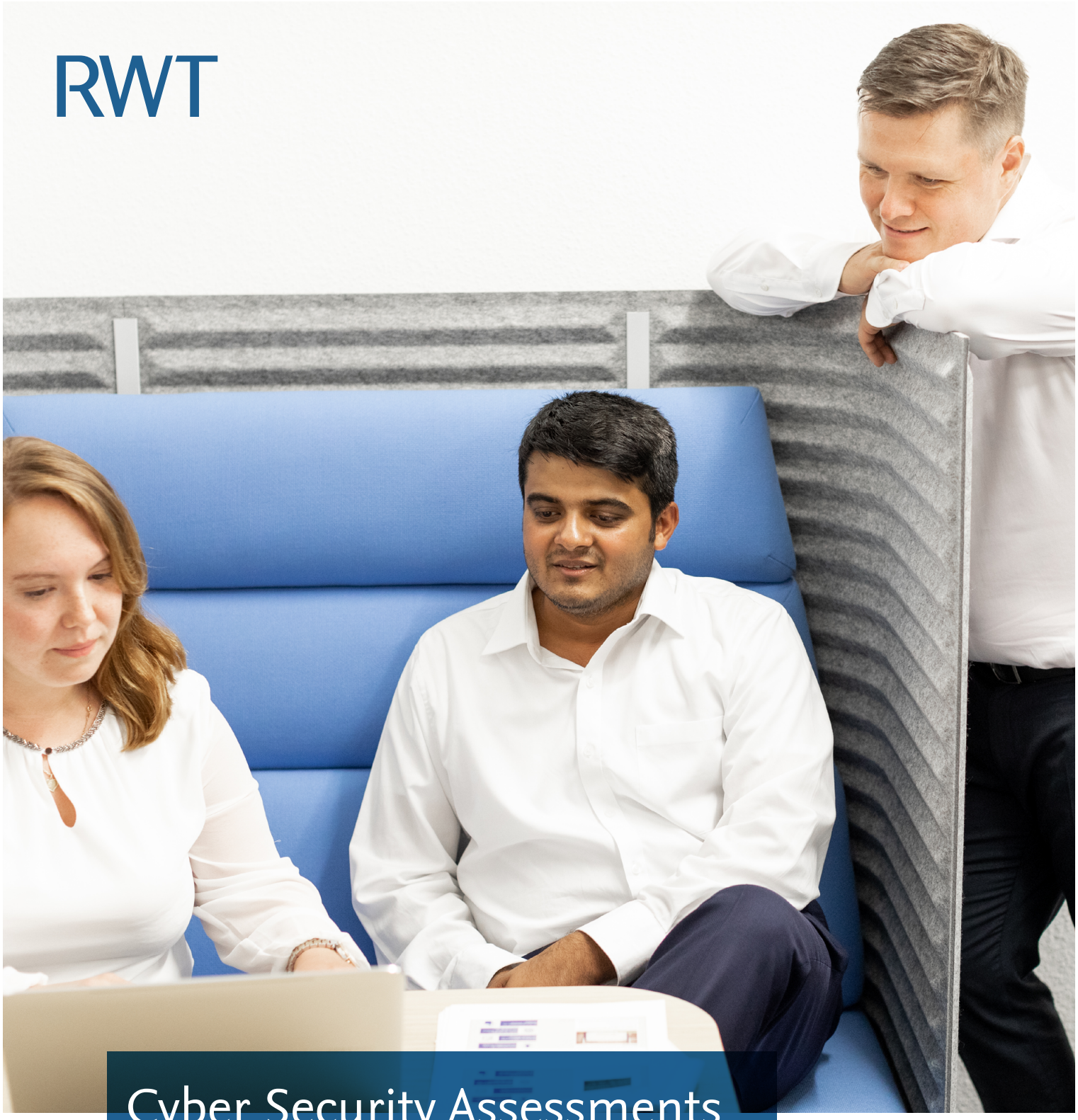
RWT



Cyber Security Assessments

Ihr Start in eine abgesicherte Digitalisierungsstrategie

bis zu 6.000 Euro* Zuschuss zur Verbesserung Ihrer IT-Sicherheit

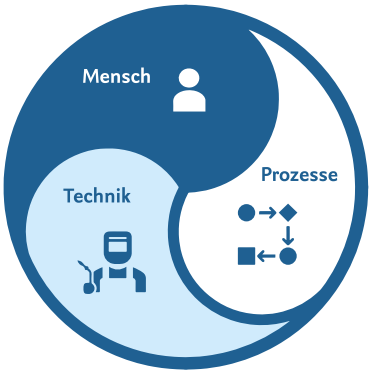
** bei einer Investitionssumme von 12.000 Euro gibt es die „Digitalisierungsprämie Plus", einen Zuschuss i.H.v. 50 % (max. 6.000 Euro). Zu weiteren Kriterien der L-Bank und Details beraten wir Sie!*

RWT – *besser beraten*

Global presence through Crowe

RWT

Mit der zunehmenden Digitalisierung Ihres Unternehmens wird das Zusammenspiel von Mensch, Technik und betrieblichen Prozessen und Methoden nicht nur komplexer, sondern auch anfälliger für Risiken aus dem Cyber-Raum.



Um die Chancen der neuen Welt zu nutzen und gleichzeitig Ihre Unternehmenswerte zu sichern, ist es notwendig, Informationssicherheitskonzepte zu etablieren, diese tagtäglich zu leben und regelmäßig zu überprüfen.

Wir unterstützen Sie bei der Wahl des Cyber Security Modells welches Sie in allen Bereichen der Technik, der Einbindung Ihrer Mitarbeiter sowie in der Definition von Prozessen und Methoden begleitet und entwickeln eine passgenaue Lösung.

Unser gemeinsames Ziel ist es, alle Einflussbereiche und Risiken zu erfassen, diese zu strukturieren und so Ihr Unternehmen abzusichern. Nur wenn alle Komponenten bestmöglich ineinandergreifen, können wir das verbleibende Restrisiko kosteneffizient adressieren.

Unser Beratungsansatz geht von diesen zentralen Leitfragen aus:

1. Wo stehen Sie heute?
2. Welches Sicherheitsniveau ist wo angebracht?
3. Welche Sicherheitsstrategie ist für Sie die passende?
4. Welche Maßnahmen sollen und können wann und wo eingesetzt werden?

Orientiert an den Rahmenwerken des BSI, ISIS12, ISO sowie weiteren erprobten Regelwerken ergründen wir im Rahmen eines Projektes Ihr derzeitiges Sicherheitsniveau, identifizieren Ihre primären schützenswerten Systeme, betrachten neben den technischen Komponenten auch die physischen und evaluieren das Bewusstsein bei Ihren Mitarbeitern für Cyber-Sicherheit.

Der Mensch, mag er bestens durch Ihre Absicherungssysteme und Prozesse in Ihrem Unternehmen unterstützt werden, ist der Schlüssel zum Erfolg Ihrer Cyber-Sicherheitsstrategie.

Cyber Security Assessments

Sicherheitsanalyse und Penetrationtests

- Wie sind Systeme und die IT abgesichert?

  I. Aufnahme und Evaluation bereits getroffener Sicherheitsmaßnahmen

  II. Durchführung von Penetrationstests auf Webseiten, IT-Infrastruktur, Firmennetzwerken nach einem abgestuften nutzenorientierten Modell

  III. Überprüfung von Sicherheitsmaßnahmen auf Effektivität im Unternehmensprozess

Überprüfung des Bewusstseins von Mitarbeitern auf Cyber-Risiken

- Wo steht der Mitarbeiter als Akteur im Sicherheitssystem?

  I. Evaluation der Verhaltensweisen der Mitarbeiter zur Schärfung des Bewusstseins (z.B. Phishing, Spear-Phishing) bei Nutzung von Applikationen

  II. Abgleich der Sicherheitsrichtlinien mit tatsächlichen Arbeitsabläufen

  III. Wissensabgleich bzgl. Daten- und Informationsschutz

RWT

Physische Überprüfung der Infrastruktur

- Wie sicher ist die Infrastruktur gegen Eindringlinge von außen tatsächlich geschützt?

  I. Validierung der Sicherheitsmaßnahmen durch bewusste Versuche in sensible Bereiche vorzudringen (z.B. „Der-zu-freundliche-Mitarbeiter-Check“)

  II. Überprüfung von baulichen Sicherheitsmaßnahmen, Netzwerkübergängen und Videoüberwachung

  III. Checks bei ausgelagerten Applikationen und Systemen bei Dienstleistern

Schwerpunkte, Tiefe sowie Inhalte der Sicherheitsüberprüfung schneiden wir individuell auf Sie zu.

Unser Leitmotiv: Cyber-Risiken transparent, verständlich, praktisch und zielgenau adressieren

Standards zur Analyse und Methodik

IT Standards	
BSI	BSI Grundschutz
ISIS12	Informationssicherheit in 12 Schritten
ISO 2700x	Information Security Management Systeme
ISO 13335	Guidelines for the Management of IT Security
ISO 18028	Network Security
ISO 18043	IDS
ISO 18044	SIM / SIEM
ISO 18045	IT Sec Evaluation
NIST	Cyber Security Framework

Bei der Analyse Ihrer Systeme und IT-Infrastruktur setzen wir auf eigens entwickelte Bash-(Linux)- und Powershell-(Win)-Scripte und bei Ports- bzw. Vulnerability Scans auf geeignete Werkzeuge, u.a. auf das Metasploit Framework, Nessus, OpenVAS, nmap, sowie Burpsuite. Bei Applikationstests greifen wir auf OWASP als auch speziell dafür konfigurierte Hardware Devices zurück.

Unsere 5-stufige Methodik für einen ganzheitlichen Cyber Security Ansatz

1. **Verstehen des Unternehmens:** Der erste Schritt zu einem effektiven Cyber Security Management ist es, Ihre Unternehmenswerte und -prozesse zu verstehen, um Ihre individuellen Bedürfnisse zu berücksichtigen.

2. **Programmplanung definieren:** Wir unterstützen Sie bei der Programmplanung, wie z.B. der Erfassung der technischen Anforderungen, der Definition des Projektzeitplans (in Abstimmung) und der Bildung des Projektteams mit kurz- und langfristigen Projektzielen.

   Erhalten Sie bis zu 6.000 Euro* Zuschuss zur Verbesserung Ihrer IT-Sicherheit

   ** bei einer Investitionssumme von 12.000 Euro gibt es die „Digitalisierungsprämie Plus“, einen Zuschuss i.H.v. 50 % (max. 6.000 Euro). Zu weiteren Kriterien der L-Bank und Details beraten wir Sie!*

3. **Programmentwicklung:** Wir unterstützen Sie bei der Definition der funktionalen Fähigkeiten und Kontrollen im Zusammenhang mit der IT-Sicherheit und dem Risikomanagement, einschließlich der Sammlung von Informationen, der Bedrohungsmodellierung, der Schwachstellenanalyse, der Ausnutzung, der Nachnutzung, der Berichterstattung und des Trainings.

4. **Festlegung von Risikomanagement-Frameworks und Benchmarks:** Wir bieten verschiedene Werkzeuge und Techniken zur qualitativen und quantitativen Analyse der aktuellen Reifegradmodelle, KPIs und anderer Benchmarks für die Leistungsüberwachung des IT-Risikomanagements von Unternehmen. Wir begleiten Sie bei der Erstellung geeigneter Risikomanagement-Rahmenwerke oder -Richtlinien (NIST, ISO2700x, ISIS12, BSI etc.).

5. **Implementierung, Überwachung und Kontrolle:** Wir unterstützen Sie bei der Implementierung von Cyber Security Risikomanagement-Frameworks und Richtlinien.

Unabhängig vom Stand Ihrer Maßnahmen zur Absicherung Ihrer Systeme, Mitarbeiter und Prozesse, stehen wir Ihnen zur Seite und unterstützen Sie individuell und zielorientiert.

RWT

Kontakt

Rafael Gawenda
Geschäftsführer

T +49 711 319 400 138
rafael.gawenda@rwt-gruppe.de

Dirk Peter
Head of Cyber Security

T +49 711 319 400 144
dirk.peter@rwt-gruppe.de

rwt@rwt-gruppe.de
www.rwt-gruppe.de

Standorte

Reutlingen
Charlottenstraße 45 - 51
72764 Reutlingen
+49 7121 489-201

Stuttgart
Olgastraße 86
70180 Stuttgart
+49 711 319400-00

Albstadt
Schmiechastraße 72
72458 Albstadt
+49 7431 1326-0