Rödl & Partner

GEMEINSAM
ERFOLGREICH

IT-SECURITY IN DER SCHNELLLEBIGEN WELT AM BEISPIEL VON O365

Werner Merl & Falk Hofmann

Mannheim, den 23.07.2019

10.1 IHRE ANSPRECHPARTNER

Falk Hofmann (Berlin)

- Über 20 Jahre Berufserfahrung als Informationssicherheitsberater
- Dipl. Ing. (Universität) Informatik / Nachrichtentechnik
- ITIL Service Manager / Cisco CCNA, Akkreditierter ISO27001 Auditor und DSB
- TISAX® -Assessment & Kritis-Prüfung gemäß § 8a (3) BSIG
- M: Falk.Hofmann@roedl.com T: 0163 7788806

Werner Merl (Eschborn)

- 30 Jahre Berufserfahrung als Unternehmensberater / (Re-)Organisation / Prozesse
- Dipl.-Wirtsch.-Ing. (TH) ET / IT / Recht
- Datenschutzbeauftragter /DSB, Neuausrichtung von Unternehmensprozessen bei der Einführung von Datenschutzmanagementsystemen (DSMS)
- M: Werner.Merl@roedl.com T: 0619 / 76 11 47 11

1.1 WIR SIND UNVERWECHSELBAR:

ERFOLGSGESCHICHTE AUS DEUTSCHLAND

- 1977 Gründung als Ein-Mann-Kanzlei in Nürnberg
- 2019 weltweit 4.900 Mitarbeiterinnen und Mitarbeiter in 50 Ländern mit 111 eigenen Niederlassungen
- EIN Unternehmen, kein Netzwerk oder Franchise-System
- Alles aus einer Hand:
  Wirtschaftsprüfung, Steuerberatung, Steuerdeklaration und BPO, Rechtsberatung, Unternehmens- und IT-Beratung
- Spezialisiert auf deutsche, international tätige Unternehmen

1.3 UNSERE DIENSTLEISTUNGEN IM ÜBERBLICK

Wirtschaftsprüfung

- Jahres- und Konzernabschlussprüfung, Quartalsreviews
- Gutachten, Sonderprüfungen und Bestätigungsleistungen
- Financial und Performance Audit
- Internationale Rechnungslegung, Reporting
- IT-Audit
- Compliance und Risikomanagement

Rechtsberatung

- „Full-Service“ Wirtschaftsrecht
- Gesellschaftsrecht
- Arbeitsrecht
- Transaktionen
- Unternehmensnachfolge
- Gesellschafterkonflikte
- Rechtsdurchsetzung
- Compliance, Prävention und Verteidigung
- Öffentliches Recht

Steuerberatung

- Internationale Steuerplanung
- Verrechnungspreise
- Transaktionen
- Laufende Steuerberatung
- Umsatzsteuer
- Rechtsdurchsetzung und Verteidigung
- Beratung der Unternehmerfamilie
- Vermögende Privatpersonen, Spitzensportler

IT GRC Beratung / Digital GRC

- IT-Audit & Assurance
- Digital Advisory
- Digital Transformation

Unternehmens- und IT-Beratung

- Geschäftsprozessberatung
- Unternehmensfinanzierung
- Mergers & Acquisitions
- ERP Lösungen SAP und Microsoft Dynamics AX
- IT Outsourcing und Cloud Computing
- CRM Lösung Targenio

Steuerdeklaration und Business Process Outsourcing (BPO)

- Finanzbuchhaltung
- Lohnbuchhaltung
- Jahresabschluss und Deklaration
- Laufende Beratungsleistungen
- Tax Accounting

1.4 UNSERE DIENSTLEISTUNGEN IM ÜBERBLICK

Leistungsportfolio Team Digital GRC

IT-Audit & Assurance

- Ordnungsmäßigkeitsprüfungen für Prozesse und Systeme / IT-Prüfung
- Projekt- und IT-Revision
- Umsetzungsprüfung für den Datenschutz, KRITIS, GoBD
- Datenanalysen
- SAP Prüfung / Berechtigungen

Digital Advisory (operativ)

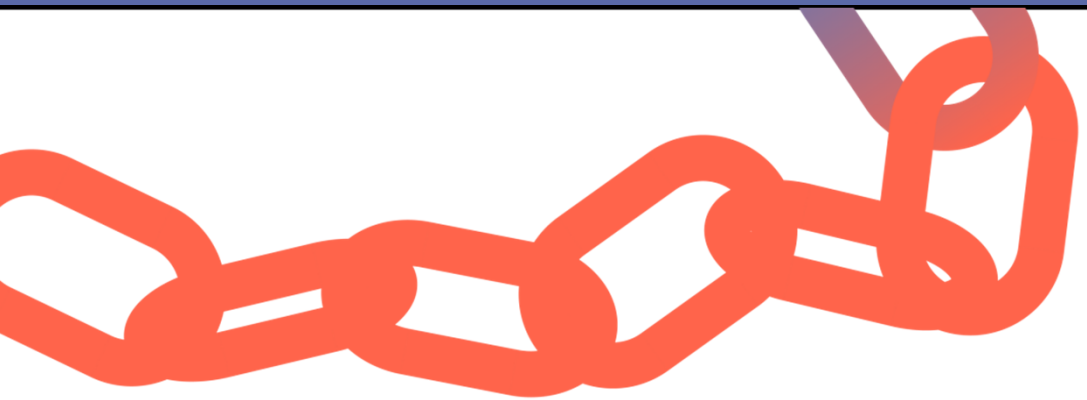
- IT-Servicemanagement
- Steuerungsoptimierung der IT-Prozesse
- Notfallmanagement / BCM
- Informationssicherheit und Datenschutzmanagement
- Systemauswahl und -einführung

Digital Transformation (strategisch)

- IT-Strategie
- IT- und Digital Due Diligence
- Cybersecurity
- Process Mining / Big Data
- Digitalisierung von Geschäftsprozessen

Nutzen von Chancen / Bewältigung von Risiken

IT-SECURITY IN DER SCHNELLLEBIGEN WELT – AM BEISPIEL VON O365



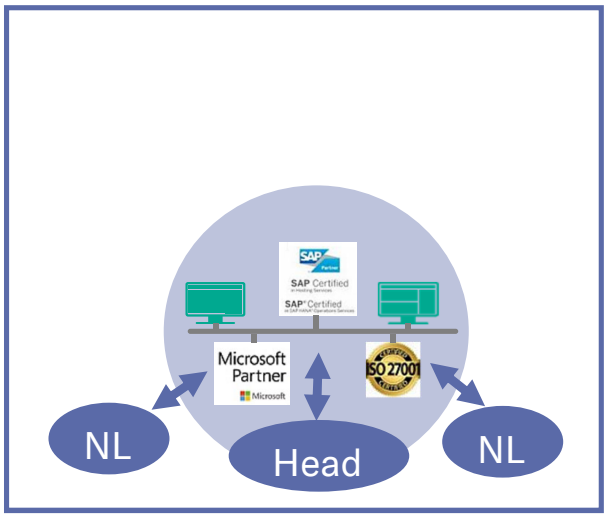
IT-Security aus der Sicht der Audits.

Welche Stützpfeiler für Prüfungen braucht die moderne IT.

Verwenden Sie doch sinnvolle Unterlagen für Ihr Unternehmen.

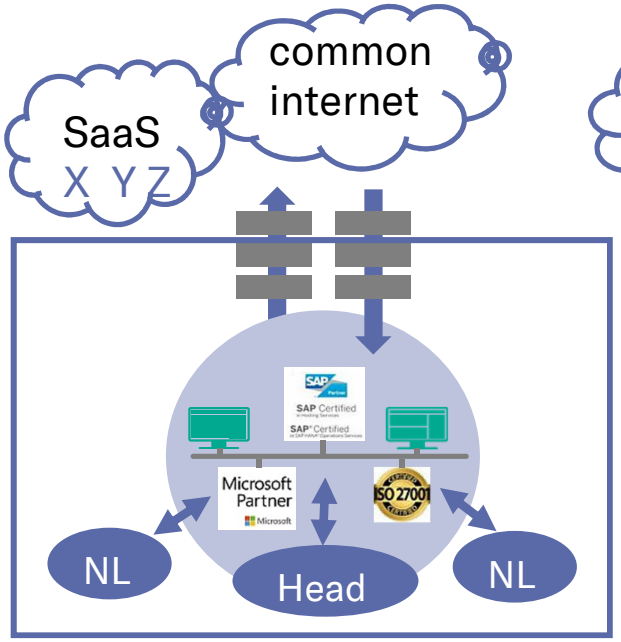
DIE HERAUSFORDERUNG: SCHNELLER – OFFENER - SICHERER

Network gestern



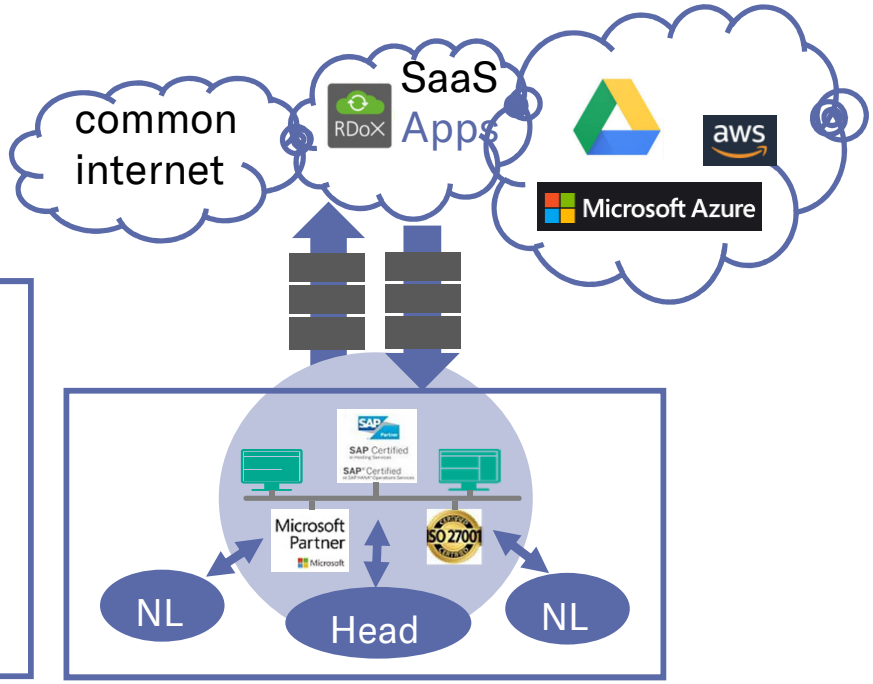
Selbstständige Sicherung
eigene Daten
und Infrastrukturen

Internet



Vernetzung extern + mobil
Traffic outbound + inbound
Sicherheitsbedarf steigt

Cloud heute



Verlagerung in cloud(s)
Zwang zur Öffnung (+IoT)
Security for & by cloud

IT-SECURITY AUS DER SICHT VON AUDITS

Was bedeutet der Paradigmenwechsel für die AUDIT-Seite? Folgende Aspekte werden noch wichtiger:

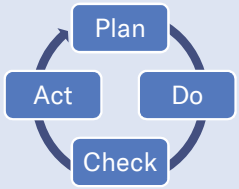
1. Umsetzung von herstellerspezifischen Hinweisen bei der Implementierung und Verwendung von Cloud-Applikationen
2. Monitoring und Scanning → Erstellung von Protokollen und deren Auswertung
3. „helfende Strukturen“ / Standardisierung / richtlinienorientiertes Handeln

Security Roadmap zur Implementierung von Office 365

	Security Administration	Threat Protection
30 Tage	• Protokollierung für Office 365 einrichten • Nutzer mit Sicherheitseinstellungen einrichten	• Verbinden von Office 365 mit der Microsoft Cloud-App-Sicherheit • Dedizierte Administratorkonten einrichten • Multi Faktor Authentifizierung (MFA) für Administratorkonten einrichten.
90 Tage	• Einrichtung Compliance-Manager, u.a. Erstellung von Regeln zum Umgang mit pbD, aber auch allen anderen Daten	• Konfiguration von Zugriffsrechten für „Privileged Access Workstations“ (PAWs) • Konfiguration von Privileged Identity Management (PIM)
Nach 90 Tagen	• Attack Simulator: Spear-Phishing-, Password-Spray- und Brute-Force-Kennwortangriffe • Microsoft Secure Score	• App-Überwachung und Berichterstellung (Shadow IT)

Security Roadmap zur Implementierung von Office 365

	Identity- and Access Management	Data Protection
30 Tage	• Account-Sicherheit (Kennwortlänge, Alter, Komplexität usw.) einrichten	1. Compliance-Manager: Anzeigen der gesetzlichen Anforderungen 2. Klassifizieren, Schützen und Überwachen von pbD (Content Search) 3. Definition von Aufbewahrungsbezeichnungen (Löschanforderungen) 4. Maßnahmenumsetzung für pbD 5. Überwachung der Einhaltung von Datenschutz-Compliance-Regeln über Security Center und Compliance Center
90 Tage	• Azure Active Directory Identity Protection aktivieren	
Nach 90 Tagen	• Einbindung von eDiscovery in Recherchen zu Bedrohungssituationen	



IT-SECURITY – OFFICE 365

MONITORING UND SCANNING -- ERSTELLUNG VON PROTOKOLLEN UND DEREN AUSWERTUNG

Der Blick von außen mit einem Cybersecurity-Rating-System

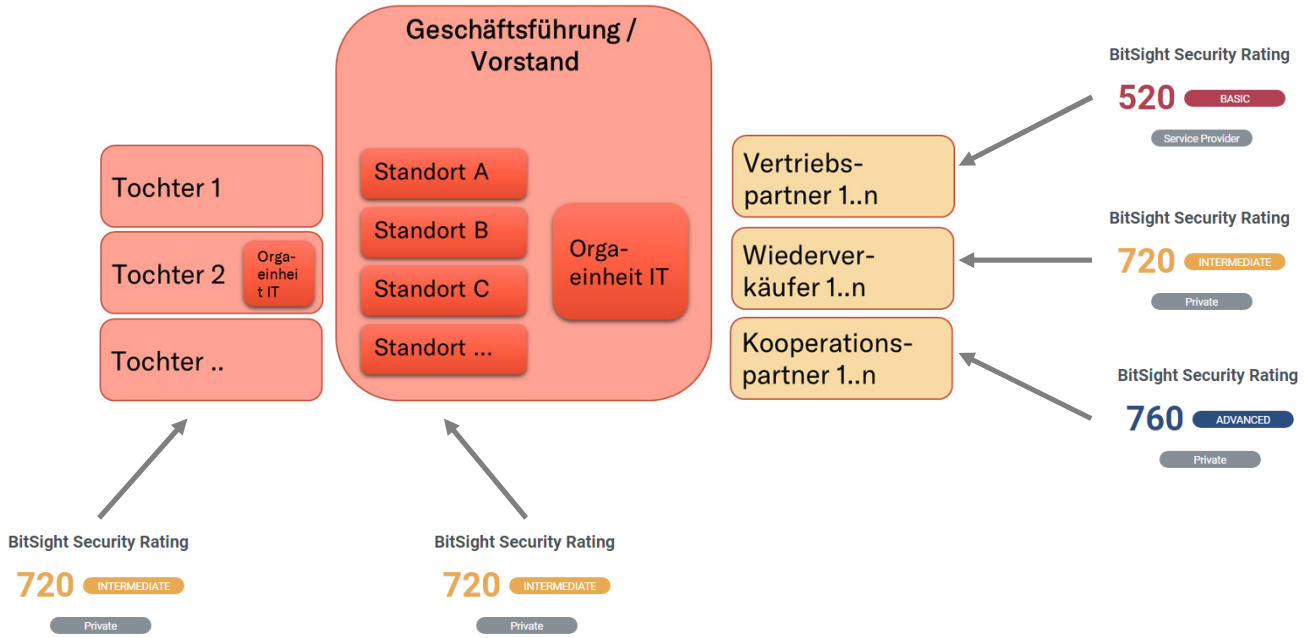
Der Blick von innen mit einem Vulnerability-Assessment and Managementlösung

Der Blick bei Verdacht mit einem APT-Scanner (Advanced Persistent Threats)

Die Überwachung der Infrastruktur, um Auffälligkeiten im Zuge der Cloud-Nutzung zu erkennen ist wichtiger denn je.

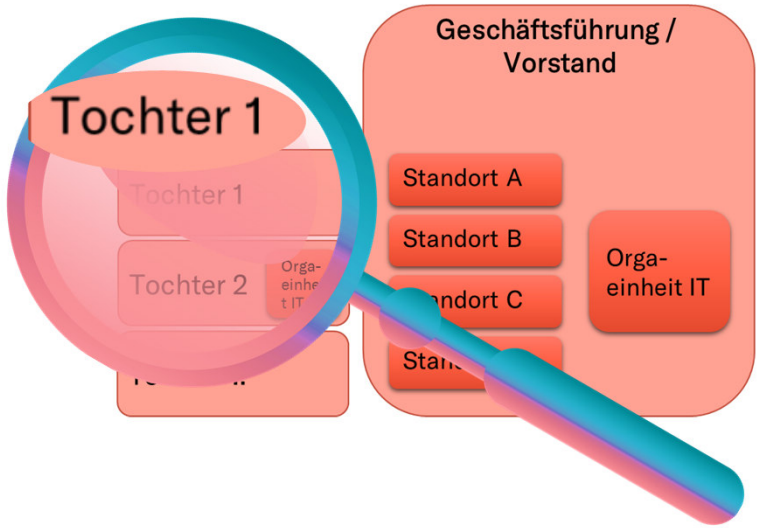
DER BLICK VON AUßEN MIT EINEM CYBERSECURITY-RATING-SYSTEM

Jedes Unternehmen hinterlässt Spuren im Cyber-Raum. Durch ein Rating-System, welches auf öffentliche Daten und Informationen zurück greift, wird das unternehmensspezifische Cybersecurity-ÖKO-System eines Unternehmens bzgl. der Informationssicherheit bewertbar!



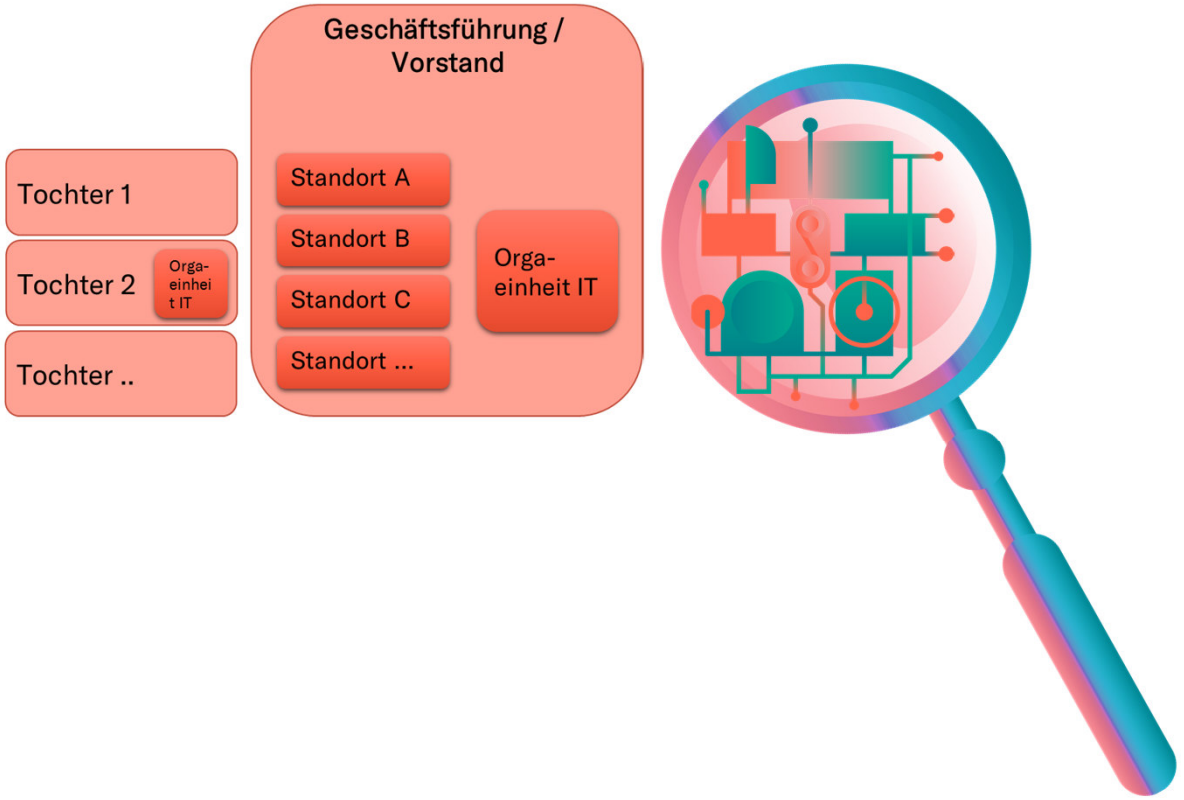
DER BLICK VON INNEN MIT EINEM VULNERABILITY-ASSESSMENT

Die Komplexität der IT-Komponenten in einer Unternehmensgruppe ist enorm. Die gängigen Sicherheitsmaßnahmen können nicht zu 100% schützen. Eine sinnvolle Erweiterung ist, zu wissen, **wo** man verwundbar ist.



DER BLICK BEI VERDACHT MIT EINEM APT-SCANNER

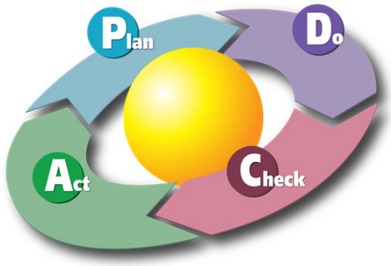
APT (Advanced Persistent Threats) sind Angriffe, welche in der Regel über Firewalls und Endpoint-Protection-Instrumente nur schwer aufzudecken sind. Ob ein APT vorliegt, ist mit herkömmlichen Instrumenten nicht möglich. Die Entscheidung jedoch, was im Angriffsfalle zu tun ist, hat in Regel enorme finanzielle Auswirkungen.

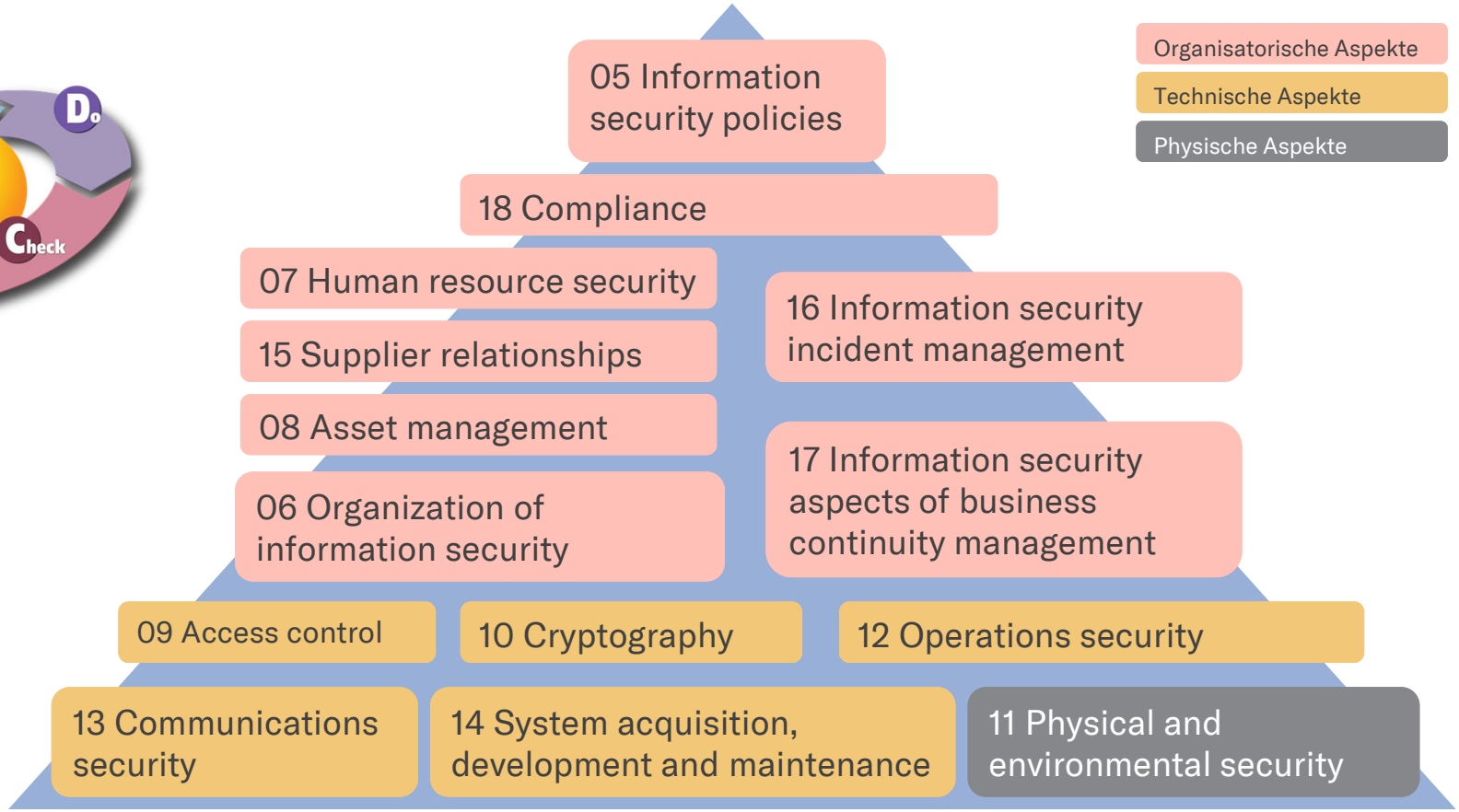


IT-SECURITY – OFFICE 365

„HELFENDE STRUKTUREN“ / STANDARDISIERUNG / RICHTLINIENORIENTIERTES HANDELN

4. Scope
5. Führung
6. Planung
7. Unterstützung
8. Umsetzung
9. Leistungsauswertung
10. Verbesserung (KVP)





Ein Managementsystem hilft Standardfehler zu vermeiden und eine Standard-Audit-Kultur zu etablieren

IT-SECURITY – OFFICE 365

„HELFENDE STRUKTUREN“ / STANDARDISIERUNG / RICHTLINIENORIENTIERTES HANDELN

Technische Aspekte

Einrichtung folgender O365 Services / Dienste:

- Verhinderung von Datenverlust (DLP)
- E-Mail-Verschlüsselung in Office 365
- Aktivierung von Exchange Online Protection (EoP)
- Einrichten von Email-Authentifizierung (SPF, DKIM)
- Office 365 Advanced Threat Protection (ATP) einrichten (u.a. Angriffs- Simulation & Analyse)
- Reaktion auf Sicherheitsvorfälle in Office 365
- Compliance Center: Durchsuchen von Überwachungsprotokollen
- …..

IHRE FRAGEN

RÖDL & PARTNER WELTWEIT

Aserbaidschan • Äthiopien • Belarus • Brasilien • Bulgarien • China • Dänemark
Deutschland • Estland • Finnland • Frankreich • Georgien • Großbritannien • Hongkong
Indien • Indonesien • Italien • Kasachstan • Kenia • Kroatien • Lettland • Litauen • Malaysia
Mexiko • Moldau • Myanmar • Österreich • Philippinen • Polen • Portugal • Rumänien
Russische Föderation • Schweden • Schweiz • Serbien • Singapur • Slowakei • Slowenien
Spanien • Südafrika • Thailand • Tschechische Republik • Türkei • Ukraine Ungarn • USA
Usbekistan • Vereinigte Arabische Emirate • Vietnam • Zypern

Alle Länder inkl. Kooperationsstandorte finden Sie auf www.roedl.de/standorte