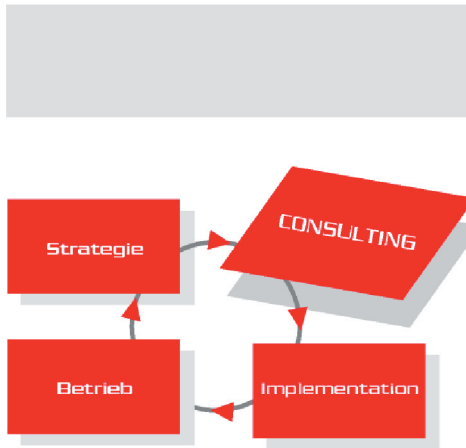


IT-Risikomanagement

@-yet Assessments Teil 3.2 - Security Audit

Unzureichende IT Security ist nicht nur ein Wettbewerbsrisiko, sondern kann auch finanzielle und strafrechtliche Risiken für Vorstand oder Geschäftsführung mit sich ziehen.



Erst durch mehrere Testangriffe können die bestehenden Sicherheitsvorkehrungen verifiziert werden.

Überblick: @-yet Sicherheit

Teil 3 - Sicherheitsanalyse

- ✓ Richtlinien für Sicherheitsvorkehrungen

Teil 3.1 - Security Scan: Erkennen

- ✓ Schneller Scan der IT Landschaft
- ✓ Hilfe zur Selbsthilfe

Teil 3.2 - Security Audit: Prüfen

- ✓ erweiterter Check (Organisation)
- ✓ abgestimmte Penetrationstests

@-yet Security Audit

- ✓ überprüft und verifiziert den aktuellen Sicherheitsstand der IT Infrastruktur und Organisation in den Bereichen
 - ✓ Anwendungen
 - ✓ Netzwerkinfrastruktur
 - ✓ Bereits existierende Sicherheitsvorkehrungen (Technologie, Organisation)
- ✓ Varianten
 - ✓ Black Box - Prüfung ohne Insider Information (Informationsbeschaffung)
 - ✓ White Box - Prüfung mit Kenntnissen der Landschaft (Revision)
- ✓ beinhaltet Prüfungsprotokolle, Bewertung und Optimierungsvorschläge für:
 - ✓ technische Sicherheit
 - ✓ physikalische Sicherheit
 - ✓ organisatorische Sicherheit

Sicherheitsüberprüfung gesetzlich verankert

z.B.: § 91 Aktiengesetz (AktG)

- ✓ (2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Die Verletzung der Organisationspflicht kann zu Schadensersatz führen.

Datenschutzerklärung

- ✓ @-yet garantiert die Geheimhaltung der Daten durch eine Datenschutzerklärung.

Ergebnisse eines Audits

Black Box

- ✓ Informationsbeschaffung und Verifizierung (Testattacken) des aktuellen Sicherheitsstands aus Sicht eines externen Angreifers

White Box

- ✓ Bewertung und Mängelliste in der IT Infrastruktur
- ✓ Zugang zum Rechenzentrum und Daten
- ✓ Organisation
- ✓ Verifizierung (Revision)
- ✓ Einstufung in Risikogruppen

Beide Varianten

- ✓ Protokolle und Verbesserungsvorschläge

@-yet-Vorgehen

Einführungs-Workshop

- ✓ Abstimmung des Vorgehens
- ✓ Aufnahme der Infrastruktur und bestehenden organisatorischen Vorkehrungen (White Box)

Checkup (von Außen, von Ihnen)

- ✓ automatisiert

abgestimmter Penetrationstest

- ✓ Testattacken (Black Box, White Box)
- ✓ Verifizierung der Umsetzung der Securityrichtlinien (White Box)

Protokolle erarbeiten

- ✓ Erklärung und Darstellung der Ergebnisse
- ✓ Identifizierung von Schwachstellen
- ✓ Darstellung der Gefahren
- ✓ Optimierungs- und Lösungsvorschläge

Präsentation der Ergebnisse

- ✓ Summary