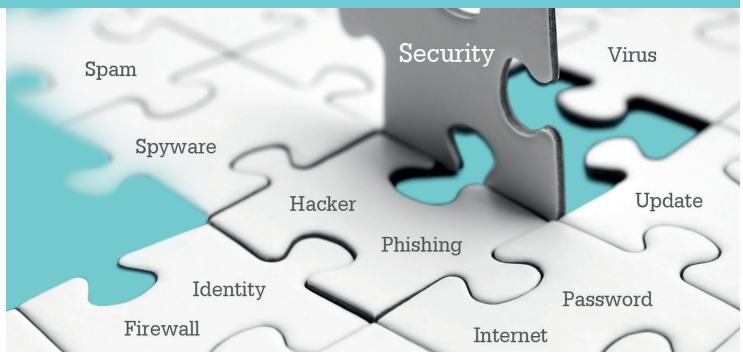
lippe]
computersyteme Lösungen für Unternehmen



IT Security / Mobile Security

Im Zuge der globalisierten Vernetzung und der steigenden Zahl mobiler Nutzer wird der Schutz der eigenen IT-Infrastruktur, der gespeicherten Unternehmensdaten und der eingesetzten Anwendungen immer wichtiger. Um der Vielzahl an Bedrohungen entgegenwirken zu können, unterstützen wir Sie dabei, Ihre Unternehmenswerte durch das richtige Maß an Schutz abzusichern. Unser Portfolio bezieht sich neben stationären IT-Systemen auch auf mobile Endgeräte.

Wir bieten Ihnen:

- Individuelle Sicherheits- und Datenschutzberatung
- Entwicklung eines Reports über den IST-Zustand
- Durchführung von Risiko- und Schwachstellenanalysen
- Durchführung von Disaster Recovery Tests
- Erstellen von Risikobewertungen
- Erarbeitung von Sicherheitskonzepten in strategischer, organisatorischer und technischer Hinsicht
- Entwicklung von Notfallhandbüchern im Rahmen des IT-Notfallmanagements
- Penetrationstest zur Überprüfung der Angreifbarkeit Ihrer IT-Systeme
- Forensische Analysen zur Aufdeckung unternehmensschädlicher Handlungen
- Implementierung gängiger Sicherheitskomponente wie Virenschutz, Spamschutz, Web Security, Firewall, VPN, Verschlüsselung, Authentifizierung
  etc.

Wir begleiten Sie auf Ihrem Weg
zu mehr Sicherheit ...

Beratung → **Analyse** → **Entwicklung** → **Implementierung** → **Support**

Wozu IT-Sicherheit?

GRÜNDE:

22 Mio. Nutzerdaten gestohlen

Manipulation von Daten bei über 38 Mio. Nutzern in Deutschland

50 Mrd. €/Jahr Schaden durch Cyberwar oder Wirtschaftsspionage

65 Mio. Virenalarme in Deutschland

1,2 Mrd. Zugangsdaten gestohlen

Manipulierte Anwendungen

Schwachstellen in Software

9.000+ schadhafte Webseiten pro Tag

Nachweis über Sicherheit und Datenschutz ist im Umgang mit personenbezogenen Daten nach BDSG, HGB, KonTraG und StGB eine unternehmerische Verpflichtung

Verantwortung übernehmen

Aktuelle Bedrohungen für Unternehmen

- Hackerangriffe (gezielt, aus Spaß etc.)
- Identifikationsdiebstahl (z.B. E-Mail)
- Malware
- Botnetze
- Spionage
- Sabotage
- Fake Websites
- Fake Apps
- Mitarbeiter (Verlust, Diebstahl, Unbedarftheit, Unwissenheit, Fehlverhalten)
- Social Engineering (Ausnutzung der Schwachstelle Mensch)
- Schadsoftware über Wechseldatenträger oder externe Hardware
- Einbruch über Fernwartungszugänge
- Internetverbundene Steuerkomponente
- Technisches Fehlverhalten
- Höhere Gewalt (wie z.B. Feuer, Hochwasser, Explosion etc.)
- Kompromittierung von Smartphones im Unternehmen
- Kompromittierung von Extranet und Cloud
- DDos-Angriffe (Lahmlegen von Servern mittels Botnetz)
- Datenabfluss (Verlust von Know-How)

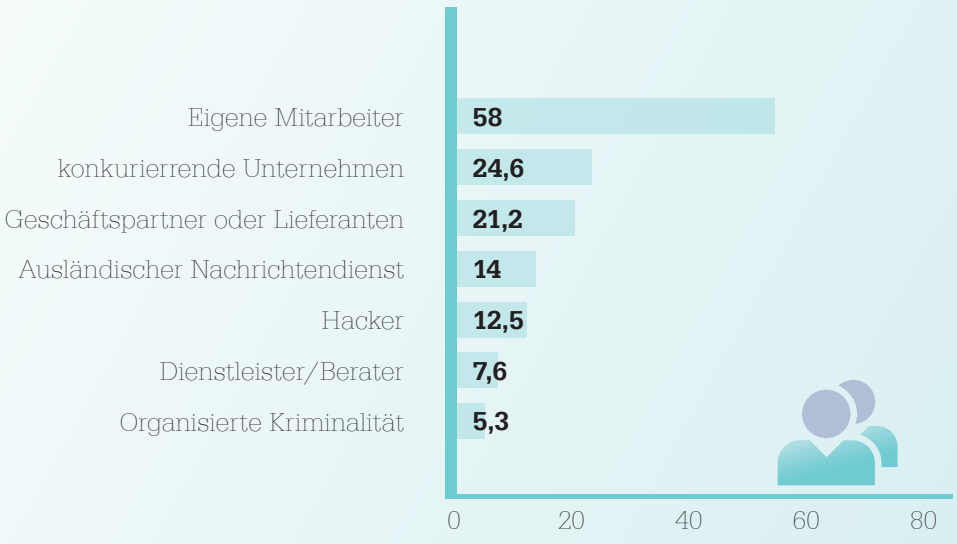
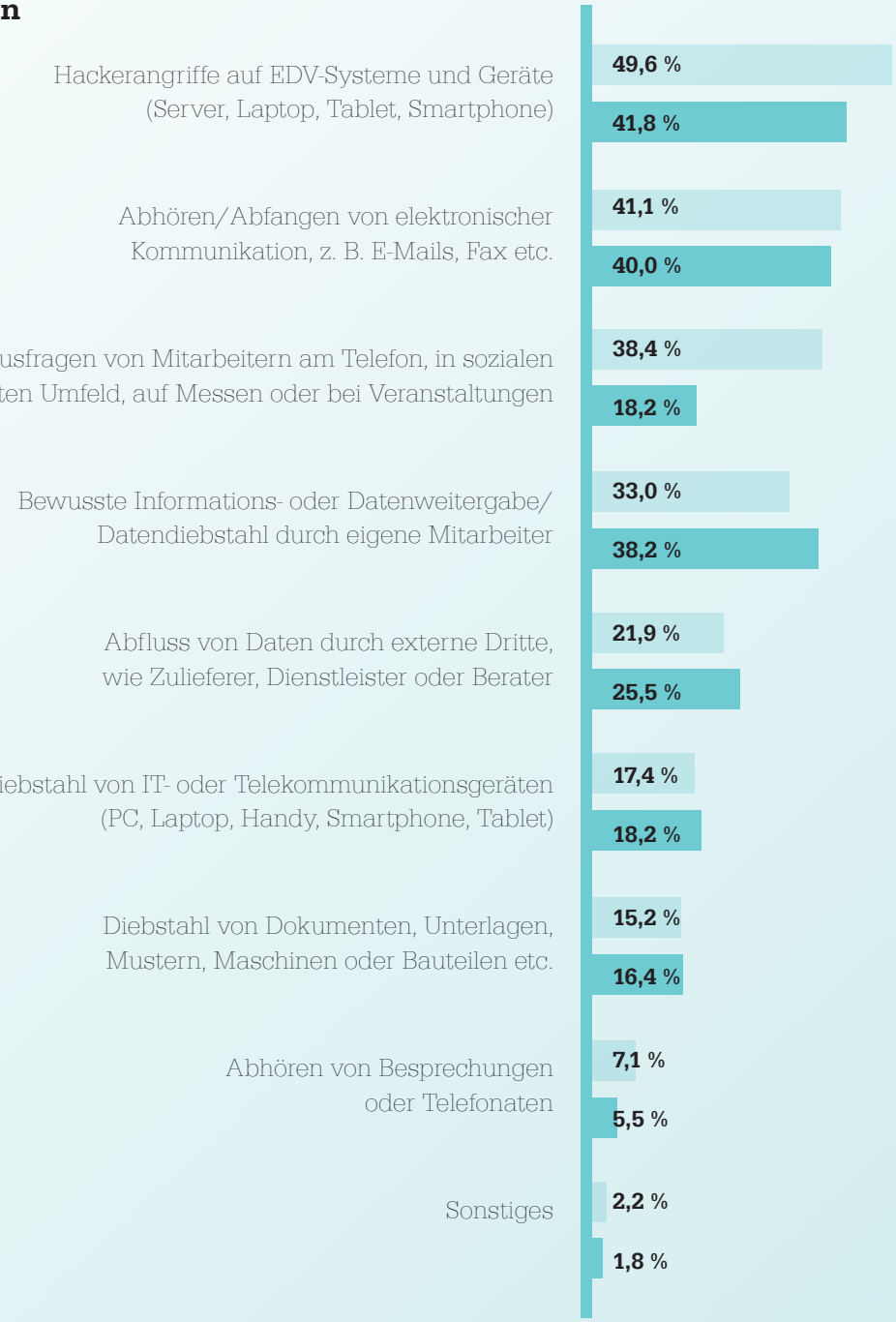


Abbildung: Hinweise auf Täter in % (Quelle:Corporate Trust 2013)

Welche konkreten Handlungen fanden (vermutlich) statt?

(Mehrfachnennungen möglich)



Quelle: Corporate Trust 2014

Folgeangriffe

- Auslesen von Zugangsdaten
- Unberechtigter Zugriff auf interne Systeme
- Eingriff in Steuerungskomponente (USB, Tastatur, Webcam. Micro etc.)
- Manipulation von Netzwerkkomponenten

Gründe ...

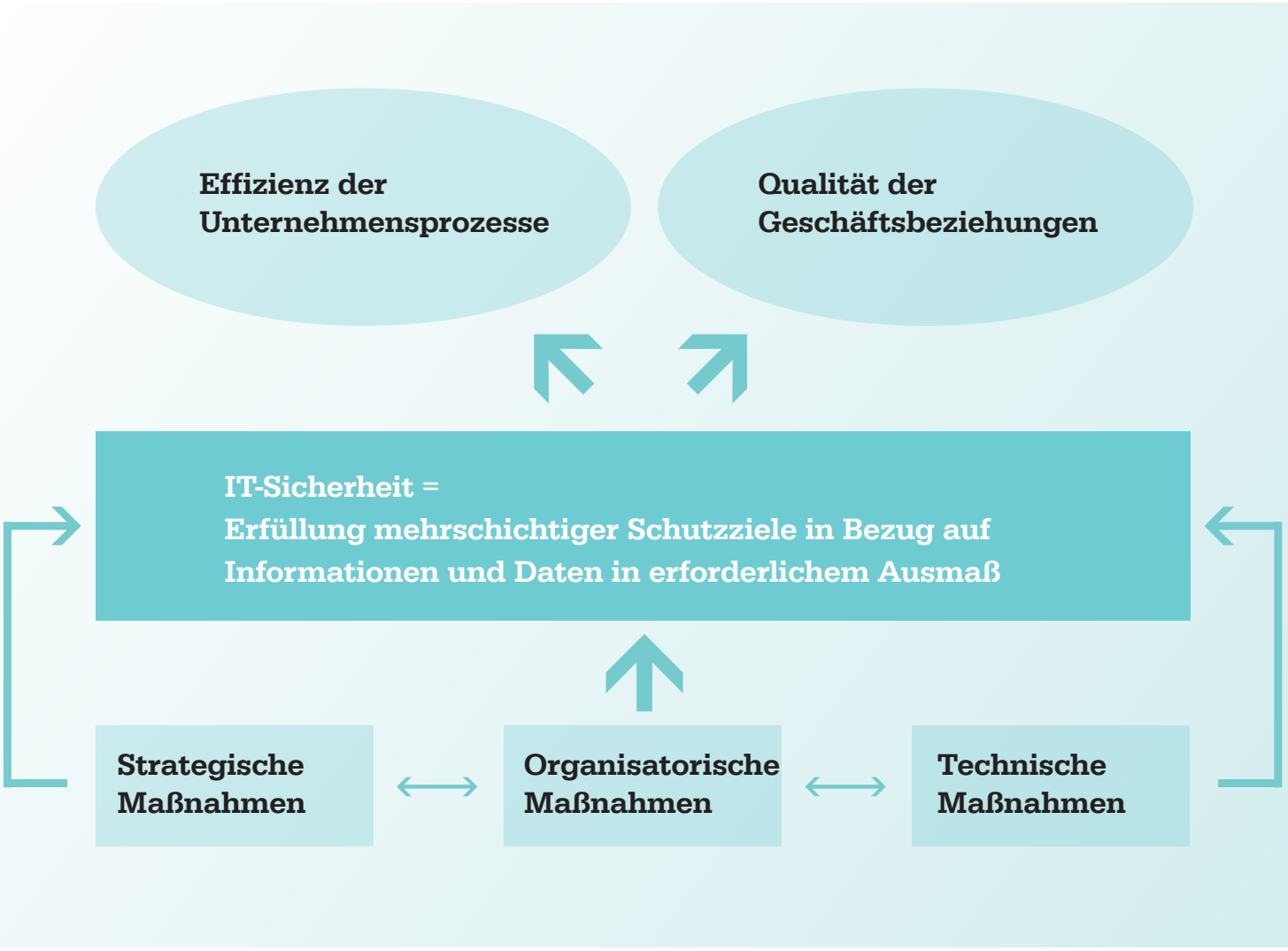
- Abgreifen von Informationen und Innovationen (wertvolles Unternehmensgut)
- Reger illegaler Handel mit Daten auf dem Schwarzmarkt
  - Kreditkarteninformationen
  - Namen von Benutzerkonten
  - Passwörter
  - Produktinnovationen
  - Geistiges Eigentum
- Schädigung des Firmenimages durch konkurrierendes Unternehmen, Mitarbeiter etc.

Lösung: IT-Sicherheitsstrategie

Warum?

- IT-Risiko- und Sicherheitsmanagement ist für Unternehmer eine juristische Pflicht
- Informationen sind ein wichtiger Vermögenswert
- Unzureichender Schutz kann das Unternehmensimage dauerhaft aufs Spiel setzen
- Einhaltung von Sicherheitsstandards sind gesetzlich gefordert
- Schutz personenbezogener Daten nach BDSG (Bundesdatenschutzgesetz)

Individuelle Maßnahmen durch eine individuelle Strategie



Maßnahmenkatalog

Strategischer Rahmen

- Berücksichtigung und Einbindung bestehender Unternehmensprozesse
- Berücksichtigung bestehender Gesetze und Normen (BSI,ISO etc.)
- Orientierung an ITIL-Standards und Best-Practice-Ansätzen
- Einbindung und Anpassung der Unternehmensstrategie (IT-Strategie)
- Risikoanalyse/Beschreibung der IST-Situation
- Risikobewertung

Organisatorischer Rahmen

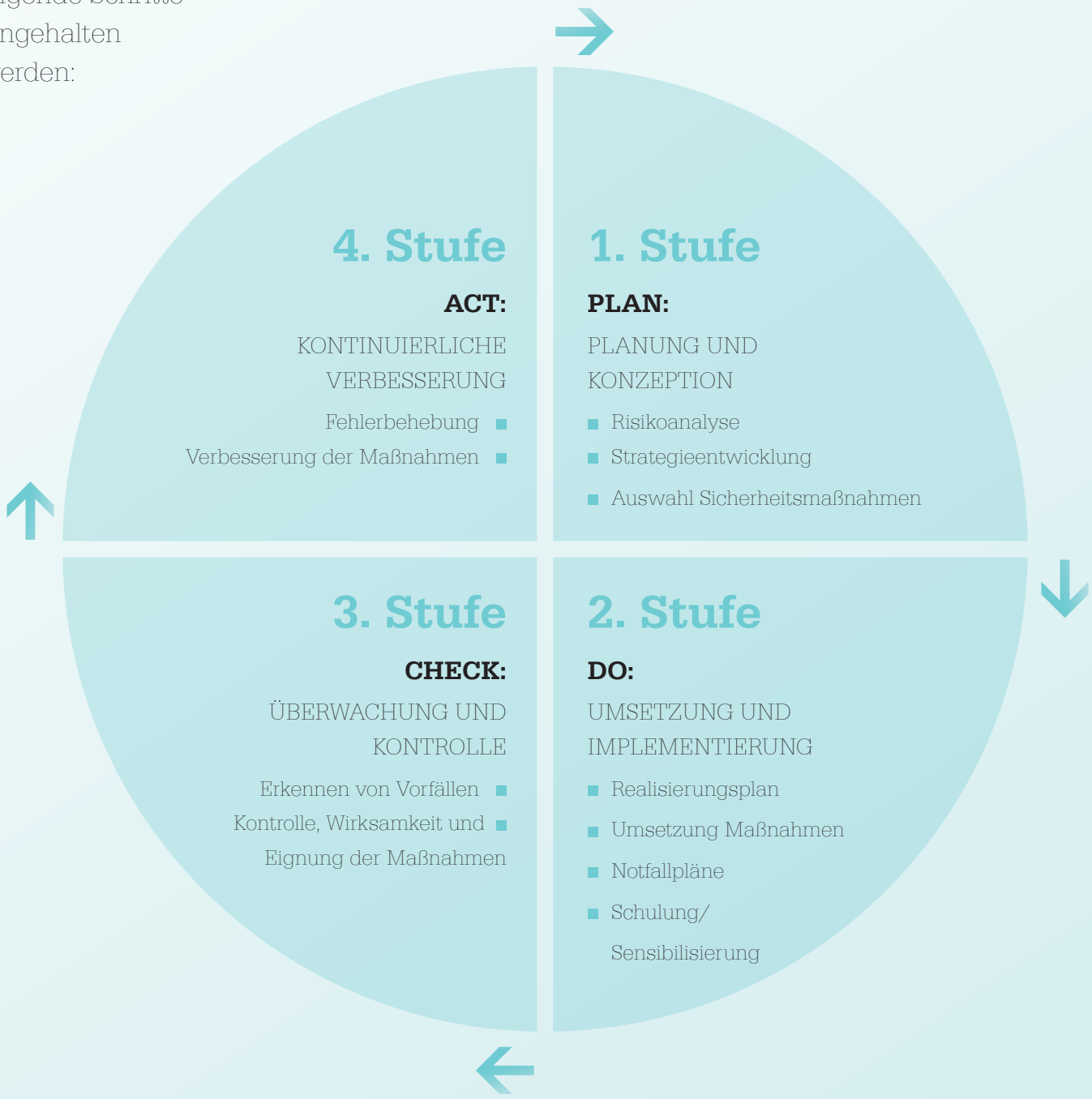
- Sicherheitsleitlinien/-policies (Regelungen für den User/Anforderung an IT)
- Gesetzliche Vorgaben/-richtlinien (KonTraG, SOX, KWG, HGB, BDSG, AO, GoBS, GDPdU, LDSG, SGB X, TKG, TMG etc.)
- Betriebsvereinbarung
- Verpflichtungserklärung
- IT-Sicherheitsmanagement, Support, Zuständigkeiten
- Mitarbeitersensibilisierung durch Schulungen & Workshops
- Notfallplan, Krisenmanagement, Umgang mit Restrisiken
- Systemmanagement
- Dokumentations- und Berichtspflicht

Technischer Rahmen

- Verschlüsselungstechniken (E-Mails, Netzwerke, Cloud etc.)
- Speicherkonzepte
- Virenschutz
- Firewall
- Authentifizierungsverfahren
- Autorisierung
- Sicherheit in Mobilfunknetzen
- Härtung
- Containerisierungsverfahren
- Zugangs- und Zugriffskontrollen
- Anonymisierung der Daten
- Managementsysteme
- Virtualisierung

Lifecycle der IT-Sicherheit

IT-Sicherheit sollte dem Bundesamt für Informationssicherheit (BSI) nach zufolge dem Plan-Do-Check-Act-Zyklus gemäß ISO 2700x folgen. Dabei sollten folgende Schritte eingehalten werden:



Strategieablauf

Risikomanagement

- Business Impact Analyse
- Risikoanalyse
- Schwachstellenanalyse
- Risikobewertung

IT-Sicherheitskonzept

- Strategische Maßnahmen
- Organisatorische Maßnahmen
- Technische Maßnahmen

Mobiles Sicherheitskonzept

- Strategische Maßnahmen
- Organisatorische Maßnahmen
- Technische Maßnahmen

Notfallmanagement

- Wiederanlaufplan/ Wiederherstellungsplan
- Geschäftsfortführungsplan
- Notfallhandbuch
- Notfall-/Krisen-kommunikationsplan