Cyber- und Datensicherheit durch IT-Compliance

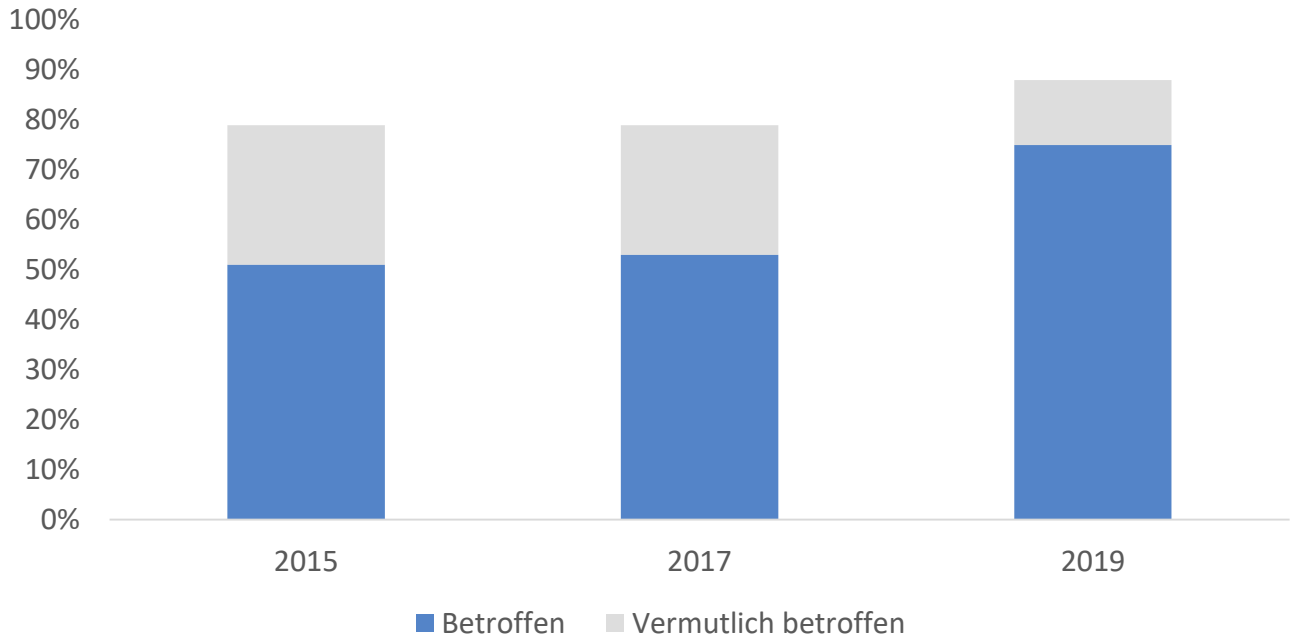
Moderation: WP/StB Anke Düsterloh

Referenten: Philipp Becker
Niklas Himmighofen
David Zaißmann

Cyber- und Datensicherheit durch IT-Compliance

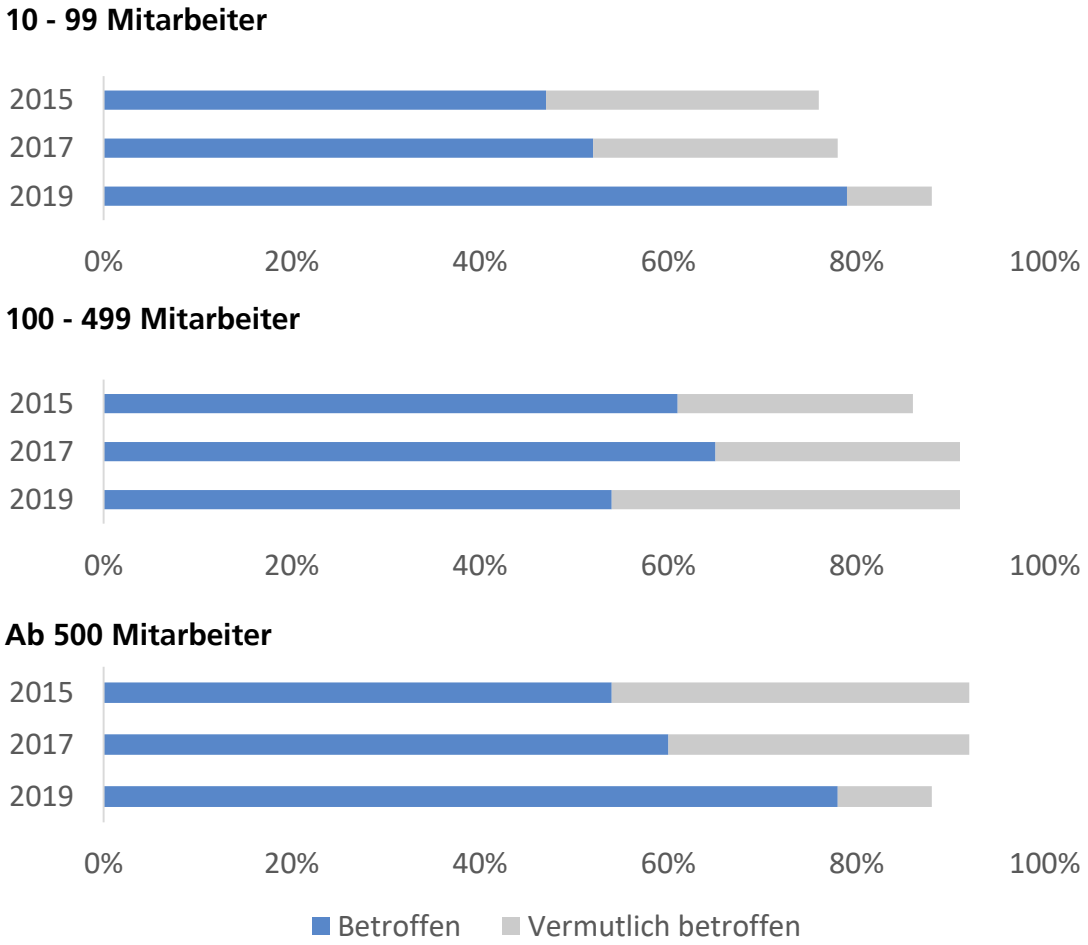
1. **IT-Gefahrenquellen**
2. Interne IT-Compliance
3. Datenschutz und Datensicherheit

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen?



Quelle: Bitkom Research, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt (Studienbericht 2020).

Betroffene Unternehmen nach Betriebsgrößenklasse



Quelle: Bitkom Research, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt (Studienbericht 2020).

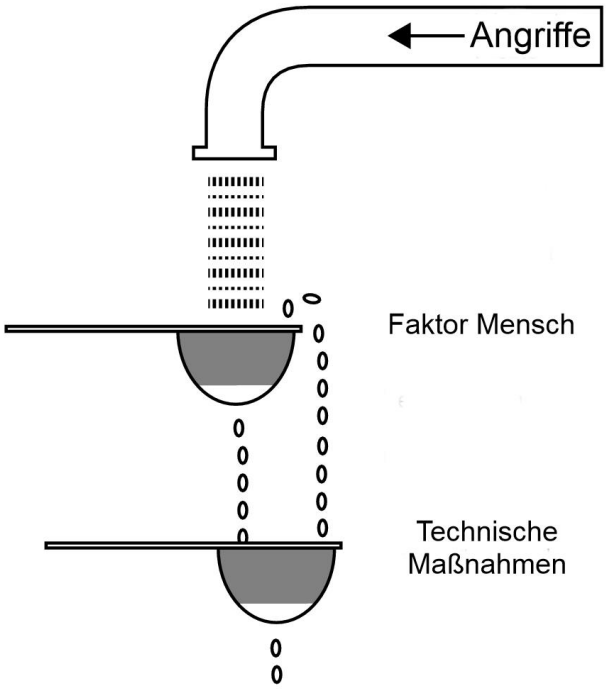
Einrichtung von technischen Maßnahmen

- Unternehmen verfügen über die üblichen Schutzmaßnahmen
  - Endpoint-Solution, Firewall etc.
- Mindestumfang zur Cyber-Security: BSI-Grundschutz
  - www.bmi.bund.de
- Maßnahmen müssen nicht nur eingerichtet sein, sondern verstanden und überwacht werden
- Regelungen zur Verantwortlichkeit, Verständnis, Überwachung müssen eingerichtet sein
  → Interne IT-Compliance

Gefahrenquelle Faktor „Mensch“

- „Direkte“ Angriffe sind heutzutage selten bzw. die Erfolgsaussichten geringer
- Schadsoftware gelangt in das Unternehmensnetzwerk oft durch menschliche Fehler (Phishing)
- Externe versuchen durch gefälschte E-Mails Überweisung durch Mitarbeiter zu veranlassen (Social Engineering)

Gefahrenquelle Faktor „Mensch“



- Durch Schulung und Sensibilisierung der Mitarbeiter kann Zahl der möglichen Angriffe deutlich gesenkt werden
  - Richtlinien zum Umgang mit E-Mails, Web & Endgeräten

Neue Gefahrenquellen durch Home-Office

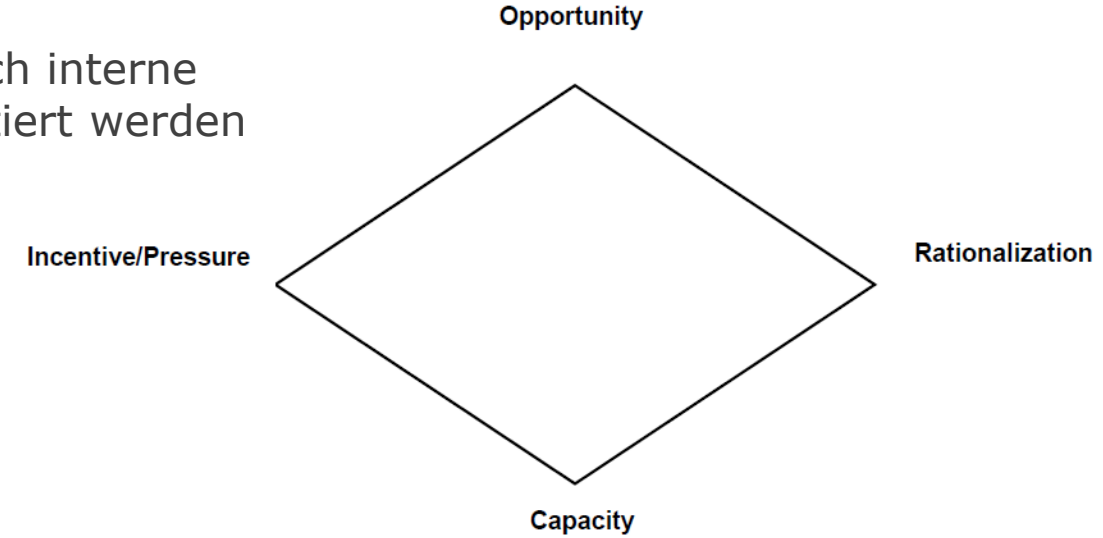
- Trend zum Home-Office/Mobiles Arbeiten schafft Nährboden für Cyberkriminalität

- Neue Einfallstore für Cyberangriffe entstehen
  - Zugriff auf Firmennetzwerk von außerhalb
  - ggf. Zugriff von private Endgeräten

- Im Unternehmen eingerichtete Sicherheitsmaßnahmen sind Mitarbeitern nicht bewusst und sind im Home-Office nicht eingerichtet
  - Physische Sicherheit
  - Clean Desk

Neue Gefahrenquellen durch Home-Office

- Gefahr krimineller Handlungen gewinnt im Home-Office deutlich an Bedeutung:
  - Kriminelle Handlungen werden durch Bedürfnis oder Druck, Fähigkeiten, Rechtfertigung und Möglichkeit getrieben
  - Im Home-Office sind bei unzureichender Datensicherheit insbesondere die Bereiche „Möglichkeit" (intern Akteure) und „Fähigkeit" (externe Akteure) relevant
  - Ziel: Verhindern, dass Daten durch interne oder externe Akteure kompromittiert werden

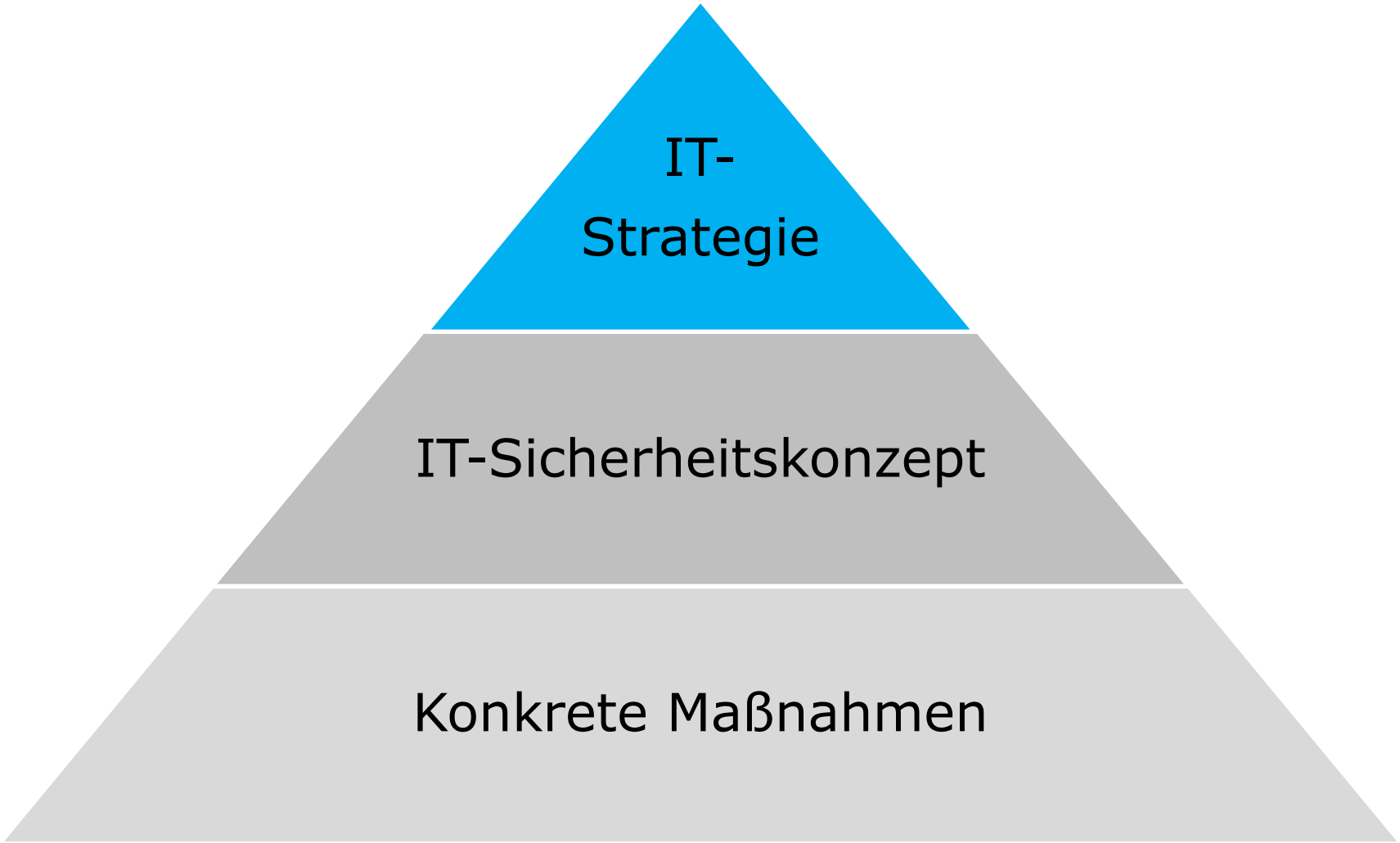


Fraud Diamond nach Wolfe und Hermanson (2004)

Cyber- und Datensicherheit durch IT-Compliance

1. IT-Gefahrenquellen
2. **Interne IT-Compliance**
3. Datenschutz und Datensicherheit

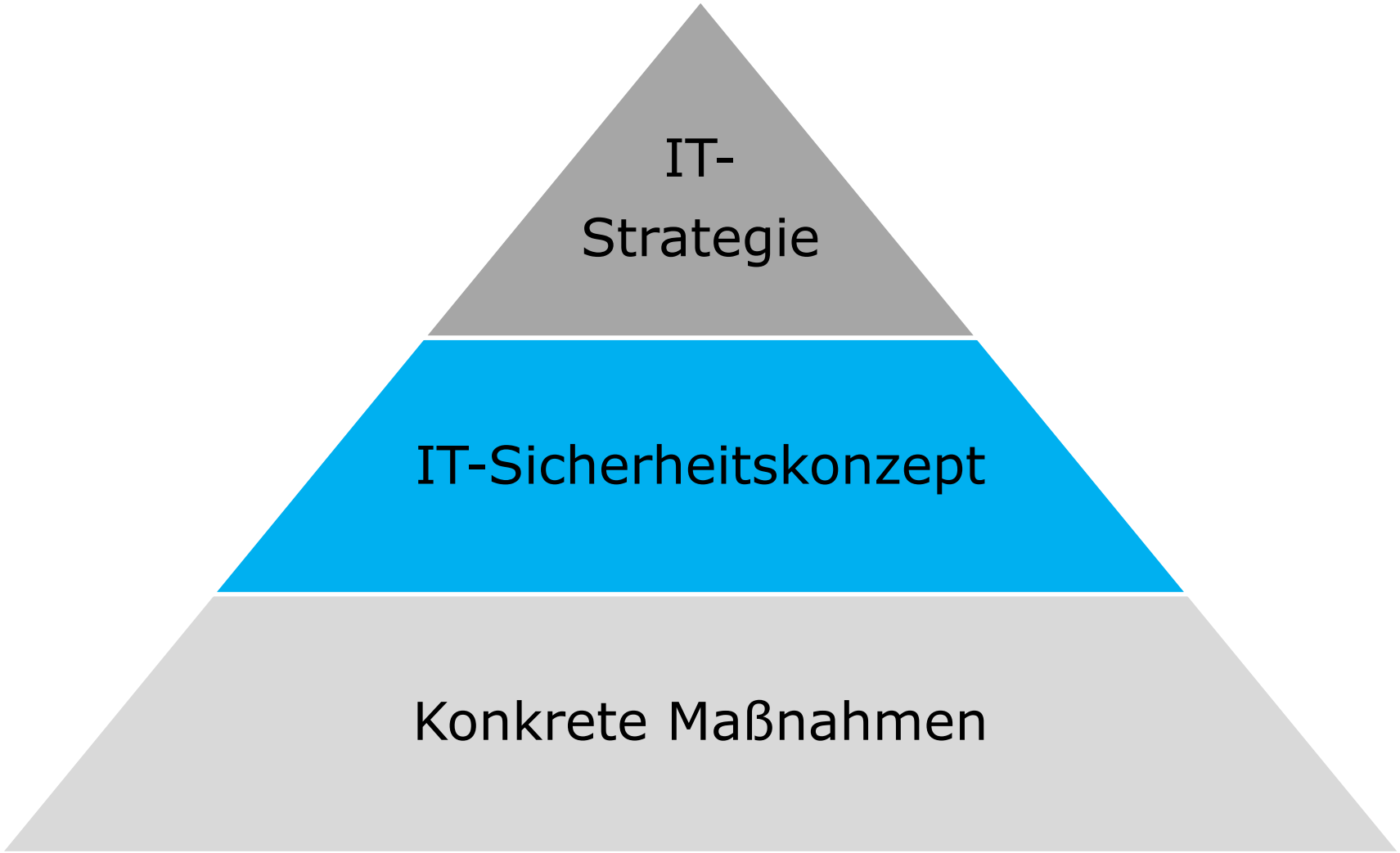
IT-Compliance



IT-Strategie

- IT- und Datensicherheit obliegen als Bestandteil der gesamten Unternehmensstrategie der Verantwortung der Geschäftsführung
  - Kontrolle, Überwachung sowie Dokumentation der sicherheitstechnischen Organisation
  - Berücksichtigung von zukünftigen Entwicklungen der IT
  - Verwendung von messbaren Zielen zur Überprüfung der Wirkungsweise der Strategie

IT-Compliance



IT-Sicherheitskonzept

- IT-Richtlinien als verbindliche Vorgaben für alle Mitarbeiter des Unternehmens für die Entwicklung und Benutzung von IT Systemen und Applikationen

- Häufige Vernachlässigung des Faktors „Mensch“
  - Angreifbarkeit von Sicherheitsmaßnahmen durch Unachtsamkeit oder Fehlverhalten

IT-Sicherheitskonzept - Sicherheitsbeauftragter

- IT- bzw. Informationssicherheitsbeauftragter
  - steht in ständigem Austausch mit der Geschäftsführung
  - kriegt ausreichende Ressourcen zur Verfügung gestellt
  - Identifikation von Schwachstellen in der IT und Informationssicherheit
  - Expertenstellung und zentrale Anlaufstelle
- Einbeziehung des Sicherheitsbeauftragten bei der Anschaffung bzw. Implementierung von IT
- Koordinierung von sicherheitsrelevanten Projekten sowie Sensibilisierungs- und Schulungsmaßnahmen

IT-Risikomanagement

- Strukturierte Vorgehensweise für Risikovorsorge und -management – keine „Brandbekämpfung“
- Identifikation von Risiken nicht nur aufgrund öffentlich zugänglicher Vorgaben, sondern zusätzlich den Bedürfnissen des Unternehmens entsprechend
- Orientierung an der IT-Strategie

IT-Risikomanagement

- Kommunikation zwischen IT-Abteilung und Geschäftsführung
  - keine Isolierung der IT-Abteilung, sondern Weiterleitung von Risiken bzw. akuten Vorfällen
- Kommunikation von IT-Risiken mit Aufsichtsorgan (z.B. Beirat)
- Kommunikation zwischen Mitarbeitern und Geschäftsführung
- Konkrete Maßnahmen:
  - Schulungen, die den Umgang mit IT-Risiken und IT-Sicherheit behandeln

IT-Organisation

- Erstellung eines Organigramms anhand von Kriterien:
  - Verzeichnis aller Mitarbeiter mit Tätigkeits- und Funktionsbeschreibungen
    - ➢ Laufende Anpassung
  - Klare Vertretungsregelungen mit Verantwortungen
- Verzeichnis über Zugangsberechtigungen von allen Mitarbeitern
  - Benutzerberechtigungskonzept
  - Laufende Anpassung bei Wechsel der Funktion bzw. des Tätigkeitsbereichs
  - Insbesondere relevant bei Verlassen des Unternehmens sowie Eintritt

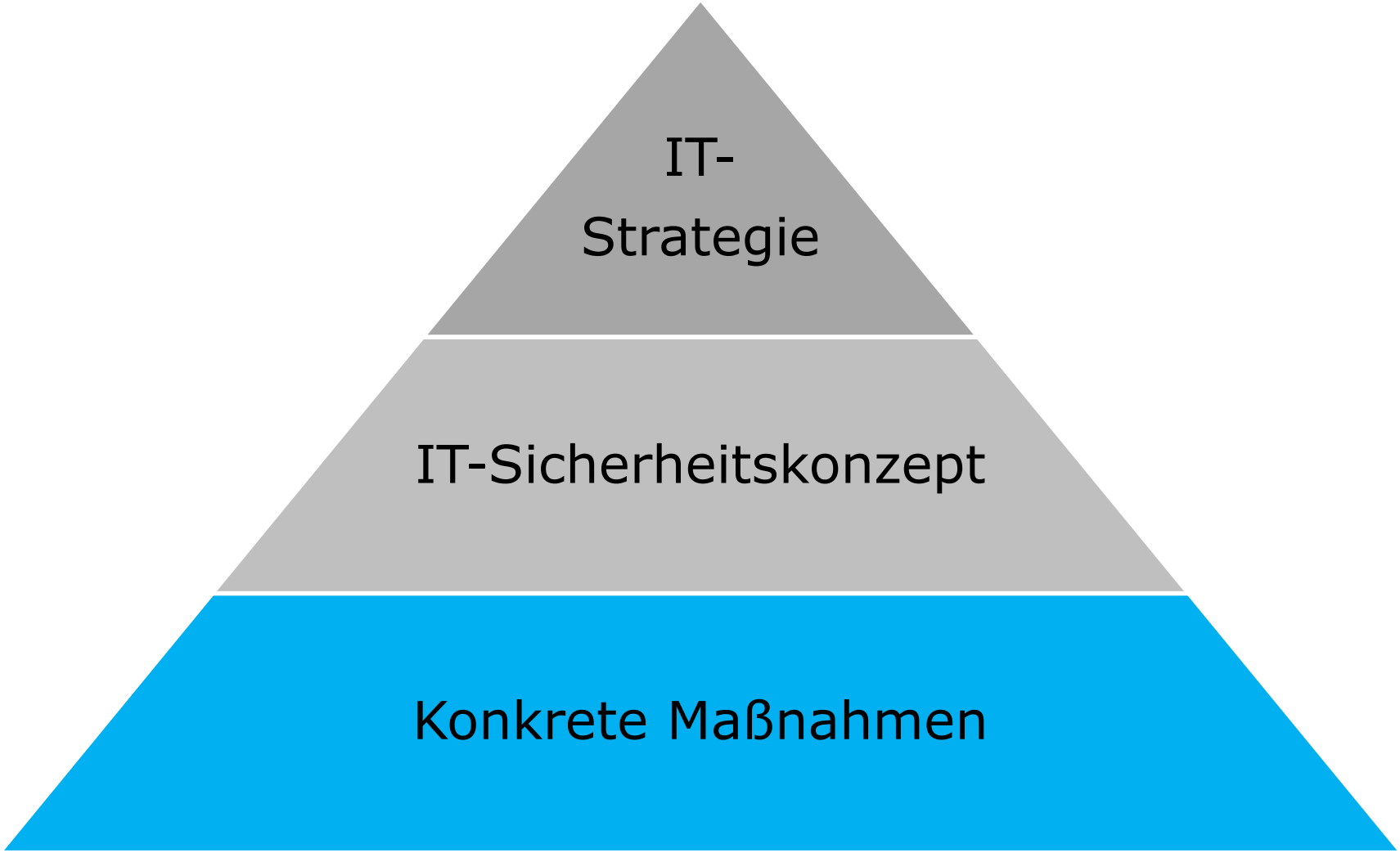
IT-Organisation

- Kommunikation mit Personalabteilung bei Änderung der Funktion (z.B. Beförderung) des Mitarbeiters oder bei Verlassen des Unternehmens

- Konkrete Maßnahme:
  - Unmittelbare Aktualisierung der Zugriffsberechtigungen bzw. Löschen bei Ausscheiden aus dem Unternehmen

  - Insbesondere Deaktivierung Zugang mobiler Geräte

IT-Compliance



Richtlinie Archivierung/Datenschutz

- Datensicherung in regelmäßigen Abständen
  - Richtlinie zu Häufigkeit und Umfang sowie Zuständigkeit
- Beschränkung des Zugriffs auf gesicherte Daten
  - ebenfalls schriftliche Fixierung der Zugriffsberechtigten
- Überprüfung der Datensicherung in regelmäßigen Abständen
  - Dokumentation der Überprüfung
  - Richtlinie zu Zuständigkeit und Turnus

IT-Compliance im Home-Office

- Erhöhtes Risiko durch privates Netzwerk
- Zusätzliche Richtlinien zu Umgang im Home-Office
  - **Welche** Informationen dürfen in IT-Systemen nach Hause transportiert werden?
  - **Wer** darf diese Informationen mitnehmen?
  - **Welche** besonderen Schutzvorkehrungen sind dafür zu treffen?

IT-Compliance im Home-Office

- Bisherige organisatorische Regelungen und technische Sicherheitsmaßnahmen meist unzureichend
- Deshalb besondere Sensibilisierung der Mitarbeiter für Gefahren des Arbeitens im Home-Office
- Insbesondere bei Verwendung von Laptops im Alltag höhere Gefahr durch physische Schäden als am stationären Arbeitsplatz
  - Datensicherung in kürzeren Abständen, um Datenverlust zu minimieren
  - **keine** lokale Speicherung von Daten

Umsetzung der Richtlinien

- Richtlinien formulieren ist zwar wichtig, aber vor allem Überprüfung der Umsetzung notwendig
- Verständnis, aber auch Kontrolle der Mitarbeiter muss gegeben sein
- Richtlinien müssen „gelebt" werden
- Unterzeichnung der zusätzlich ausgehändigten Richtlinien zum Home-Office
- Einhaltung der Richtlinien sowie Organisation relevant für Cyber-Versicherung

Cyber- und Datensicherheit durch IT-Compliance

1. IT-Gefahrenquellen
2. Interne IT-Compliance
3. **Datenschutz und Datensicherheit**

Datenschutz und Datensicherheit

- Datenschutzgrundverordnung (DSGVO) regelt insbesondere die Erhebung, Verarbeitung und Speicherung **personenbezogener** Daten

- Umsetzung im Unternehmen ist verpflichtend und wird kontrolliert
  - bspw. Datenschutzkonzepte, Prozessdokumentationen

- Im Home-Office gelten die gleichen Regeln
  - Aber viele im Unternehmen eingesetzten Sicherheitsmaßnahmen können im Home-Office nur eingeschränkt umgesetzt werden

Datenschutzgrundverordnung

- Wesentliche Ziele des Datenschutzes und der DSGVO
  - Zweckgebundene Verwendung von Daten
  - Datenminimierung: Nur Erhebung und Speicherung erforderlicher Daten
  - Schutz der Daten vor Bekanntwerden an unberechtigte Dritte
  - Richtige und sichere Archivierung, Speicherung und Löschung von Daten

Zusätzlicher Schutzbedarf

- Im Bereich Home-Office ergeben sich zusätzliche (Sicherheits-) Erfordernisse durch z.B. folgende Risiken:
  - (versehentliche) Einsichtnahme durch Unberechtigte (z.B. Familienmitglieder, Handwerker, …)
  - Physischer Diebstahl (z.B. Einbruch beim Mitarbeiter, Hardware im Kfz)
  - Diebstahl von Daten (z.B. auf Grund mangelnder Netzwerksicherheit beim Mitarbeiter)

Zusätzlicher Schutzbedarf

- Im Home-Office ist darüber hinaus der Schutz weiterer Daten sicherzustellen:
  - Interne Dokumentationen
  - Finanzzahlen
  - Projektinformationen (z.B. Forschungsfortschritte)
  - …

- Umsetzung von Schutzmaßnahmen im Unternehmen ist nicht durch bspw. die DSGVO verpflichtend

- Zum Schutz des Unternehmens aber zwingend erforderlich
  - Entsprechende Governance- und Compliancemaßnahmen sollten vorhanden sein und im Unternehmen gelebt werden

Maßnahmen zur Erreichung von Schutzzielen

- Maßnahmen und Überlegungen zum Schutz und zur Sicherung von Daten sollten z.B. umfassen:
  - Regelungen zum lokalen Speichern
  - Backup-Maßnahmen (hier insbesondere für lokal gespeicherte Daten)
  - Regelungen zum Umgang mit Wechseldatenträgern (bspw. USB-Sticks)
  - Verwendung von VPN-Tunneln
  - Umgang mit unternehmensfremder Hardware (BYOD)
  - Verwendung neuer Software

Regelungen zum lokalen Speichern von Daten

- Lokal gespeicherte Daten werden regelmäßig nicht im Backup berücksichtigt
- Idealerweise Speichern nur auf den Datenservern erlauben
- Festplattenverschlüsselung (Schutz lokaler Daten bei Verlust oder Diebstahl)

Backup-Maßnahmen (hier insbesondere für lokal gespeicherte Daten)

- Prozesse und Richtlinien, die manuelle Übertragung von lokal gespeicherten Daten erfordern sowie entsprechende Kontrollen
- Automatische Festplattenspiegelungen oder anderweitige Datenübertragung bei Verbindung mit dem Netzwerk
- Regelmäßige Backups sowie Recovery-Tests

Regelungen zum Umgang mit Wechseldatenträgern (bspw. USB-Sticks)

- Wechseldatenträger sind praktisch, bergen aber ein wesentliches Sicherheitsrisiko

- Insbesondere USB-Sticks sind für viele Szenarien anfällig:
  - Einbringung von Schadsoftware ins Unternehmen
  - Verlust oder Diebstahl vertraulicher Daten
  - Regelmäßig nicht in Backup-Prozeduren eingeschlossen

Verwendung von VPN (Virtual Private Network)-Tunneln

- VPN-Tunnel verschlüsseln die Datenflüsse auf dem Weg zwischen Unternehmensnetzwerk und angeschlossenem Endgerät
- Der Datenfluss durch das Internet gilt grundsätzlich als „nicht sicher" hinsichtlich der Vertraulichkeit und Integrität von Daten
- Die Verwendung eines VPN-Tunnels ist daher unbedingt zu empfehlen!

Umgang mit unternehmensfremder Hardware (BYOD)

- Hardware sollte zwingend durch die IT angeschafft oder überprüft und freigegeben werden
  - Kompatibilität der Geräte zur IT-Landschaft
- Insbesondere USB-Geräte enthalten oft Schadsoftware
  - Mit Malware versehener USB-Bilderrahmen
  - Keylogger in einer USB-Tastatur
- VPN-Zugang über private PCs stellt ein hohes Sicherheitsrisiko dar
  - Anderer (schwächerer) Schutz des PCs erhöht die Gefahr, Schadsoftware ins Unternehmensnetzwerk einzuspielen
  - Auf den privaten PC heruntergeladene Dateien sind ggf. schlechter gegen Fremdzugriffe geschützt
  - Entsprechend hohe Schutzanforderung, falls private PCs genutzt werden

Verwendung neuer Software

- Laut Art. 32 DSGVO muss auch für die Datenverarbeitung verwendete Software ein angemessenes Sicherheitsniveau erfüllen
- Programme wie Teams, Zoom etc. weisen teilweise Sicherheitsmängel auf
  - Lösungen sind häufig bereits in Arbeit bzw. umgesetzt
- Bei Verwendung neuer Software sollte die Einhaltung von Datenschutz- und Sicherheitsstandards vorab überprüft und insbesondere bei Bedenken laufend evaluiert werden

- Vielen Dank für Ihre Aufmerksamkeit
- Beantwortung von Fragen
- Für spezielle Fragen zu Einzelsachverhalten stehen Ihnen Ihre gewohnten Ansprechpartner wie immer gerne zur Verfügung.