Designing Education
Connecting People

Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen

Lernfeld 04

Das erwartet Sie:

- Ausblick auf die Sicherheit
- Kerngrundlagen der Sicherheit

Die Themen

Einführung

Lernziele

Verantwortung, Zuständigkeit, Zertifizierung, Informationssicherheit

Kerngrundlagen

Lernziele

Datenschutz, Datensicherheit, IT-Sicherheit, weitere Rechte

IT-Grundschutz

Lernziele

Grundlagen zum IT-Grundschutz und dessen Bausteinen

Risikomanagement

Lernziele

Risiko, Risikoanalyse, Risikomanagement

©Urheber

Einführung

Lernziele

Verantwortung

Zuständigkeit

Zertifizierung

Informationssicherheit

Vorstellung des Lernfeldes

Kerngrund-lagen der Sicherheit

Datenschutz, Datensicherheit, IT-Sicherheit, Schutzziele, Grundschutz, Informationssicherheit, Risikoanalyse

Angriffs-szenarien

Social Engineering, Malware, Angriffsarten, PW-Angriffe

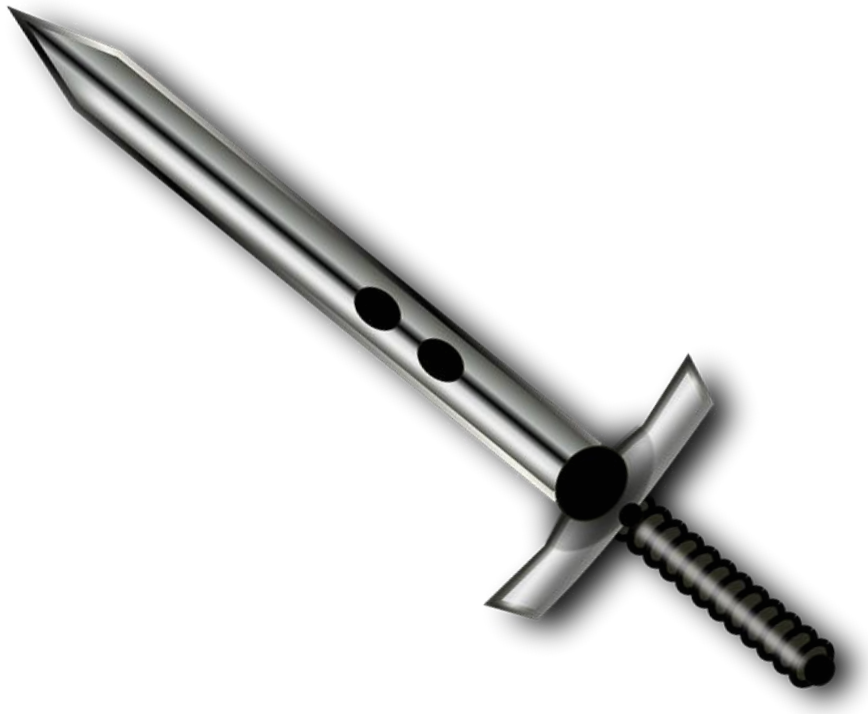
Verteidi-gungsmög-lichkeiten

Kryptographie, Passwörter, Schutzbedarfsfeststellung, Sicherheitsrichtlinien, Sicherheitskonzepte, Strukturanalyse, Schutzbedarfsfeststellung

Warum Sicherheit?

Wächter

Angreifer



Mitarbeiterstimmen

"Es spielt keine Rolle, was andere bei mir am Arbeitsplatz sehen."

Klaus Peter, Personalabteilung

"Nur 100 % Sicherheit zählt hier!"

Alexander Martin, Sicherheitsbeauftragter

"Jedes System muss 24/7 verfügbar sein."

Ian Hansson, Technischer Leiter

Mitarbeiterstimmen

Ich habe die größte Macht im Unternehmen!

Susi Sorglos, Putzkraft

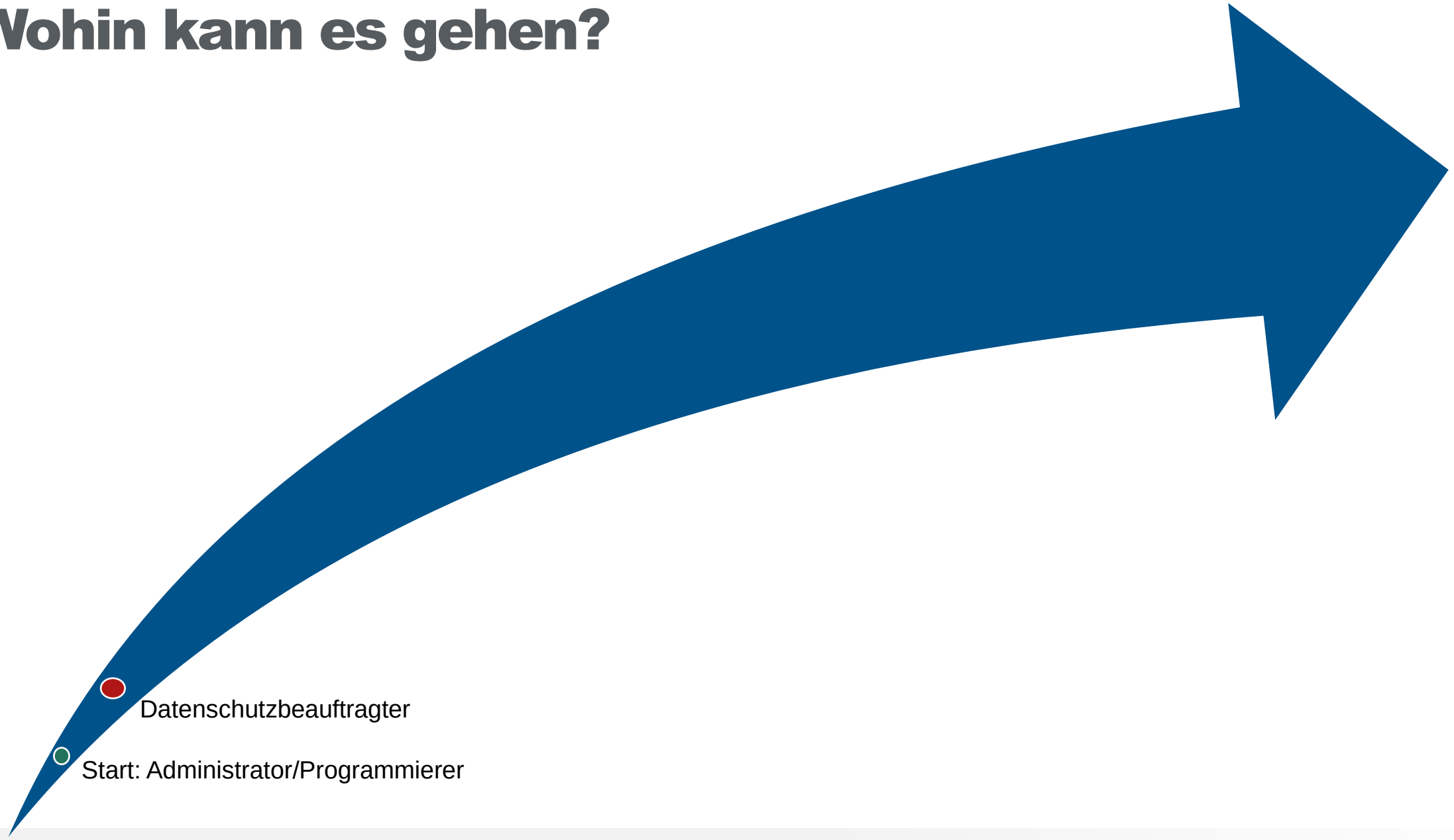
Meinen Arbeitsplatz im Verkaufsraum kann ich ungeschützt für einen Kaffee verlassen.

Alexander Martin, Verkauf

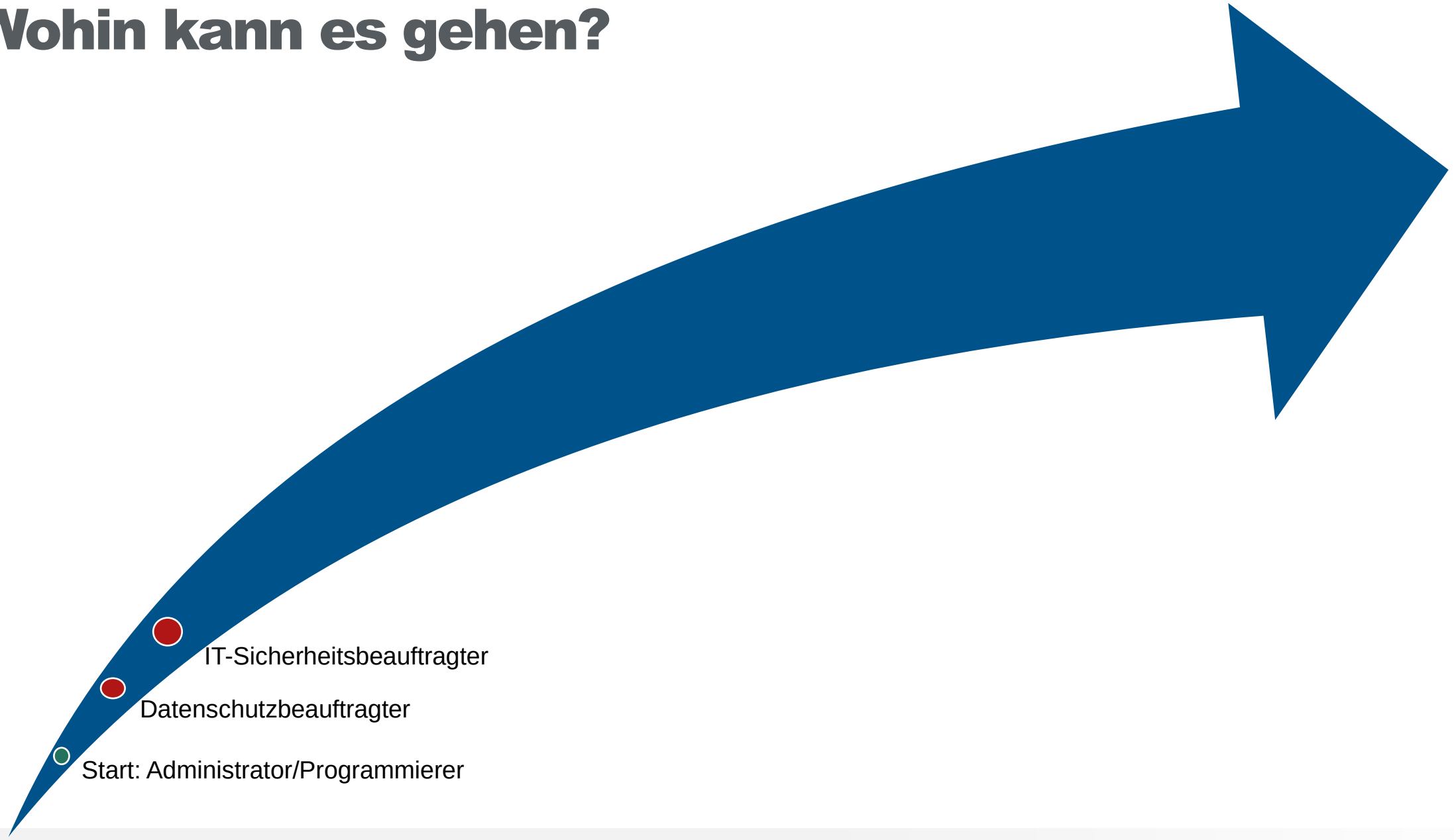
Sicherheit darf nichts, oder nur sehr wenig Kosten!

Alice Hanssen, Chef

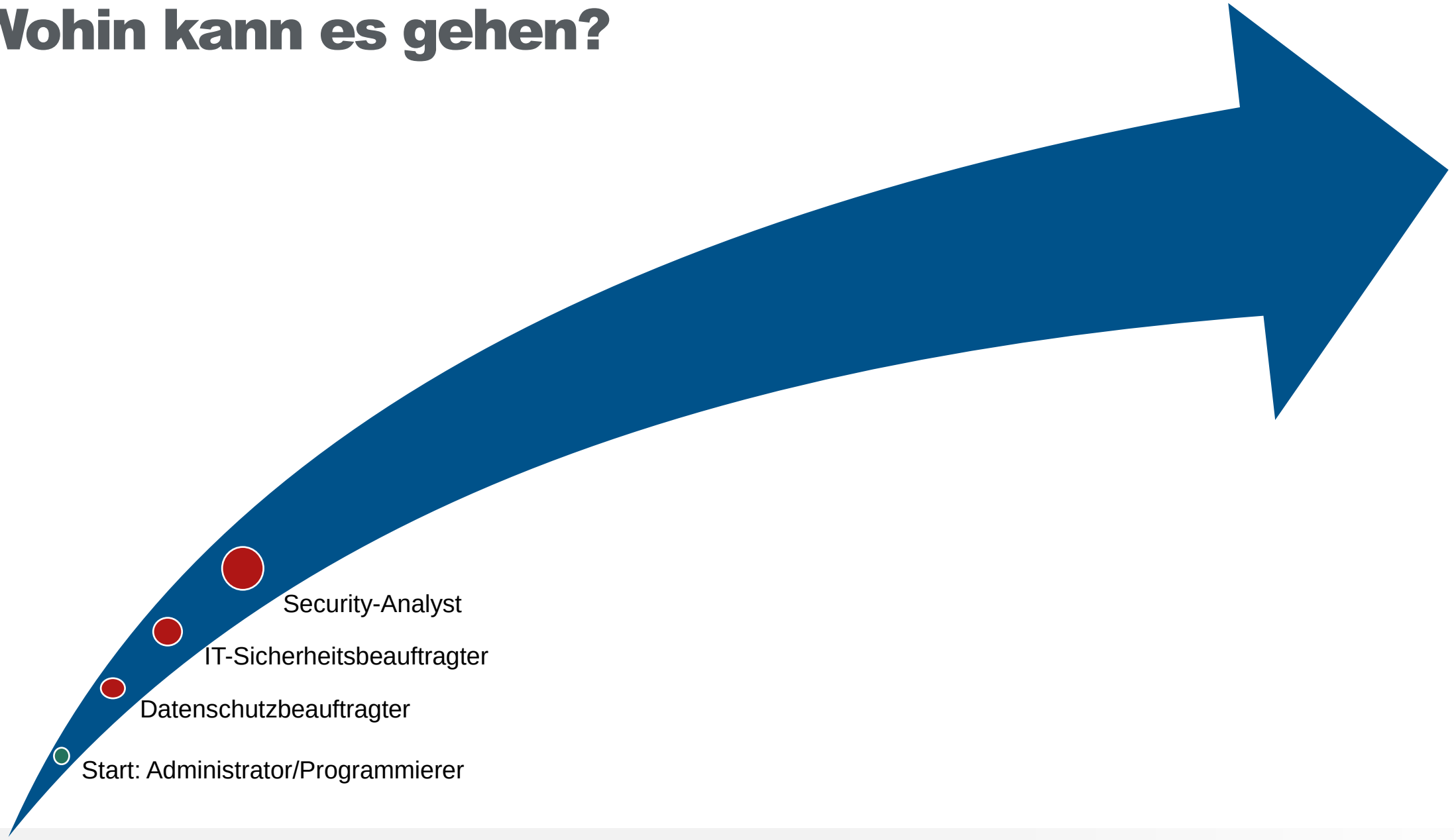
Wohin kann es gehen?



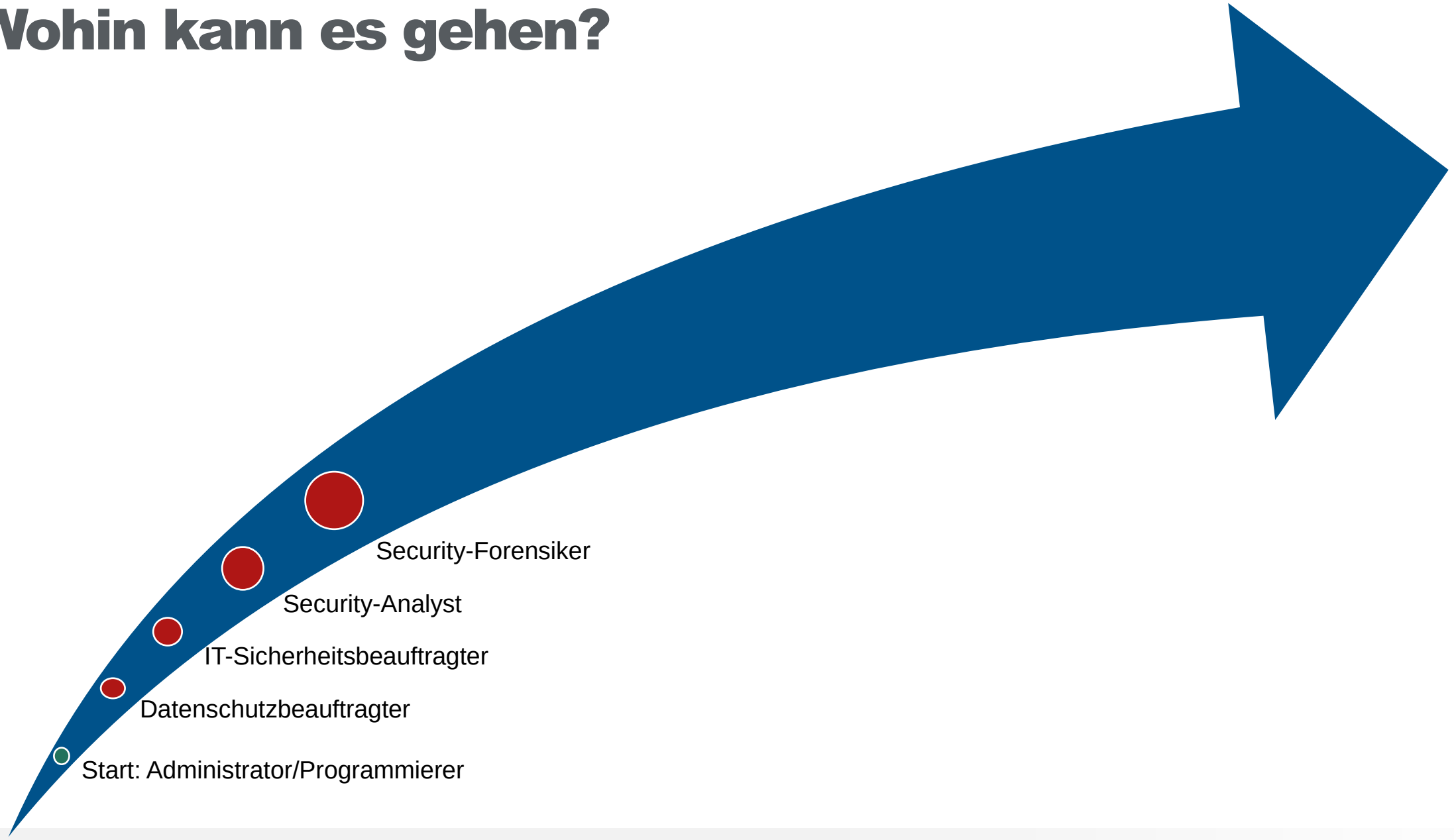
Wohin kann es gehen?



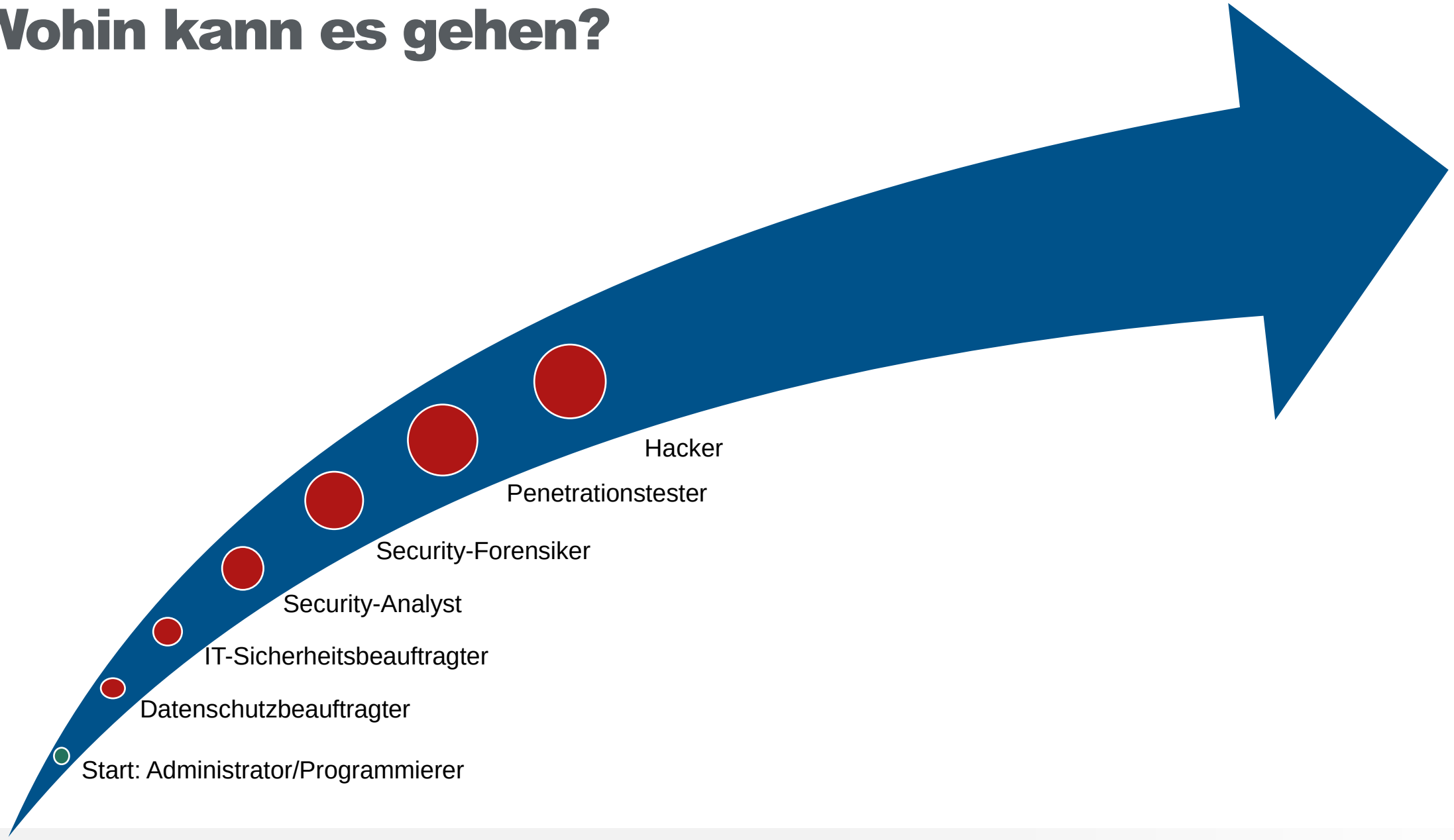
Wohin kann es gehen?



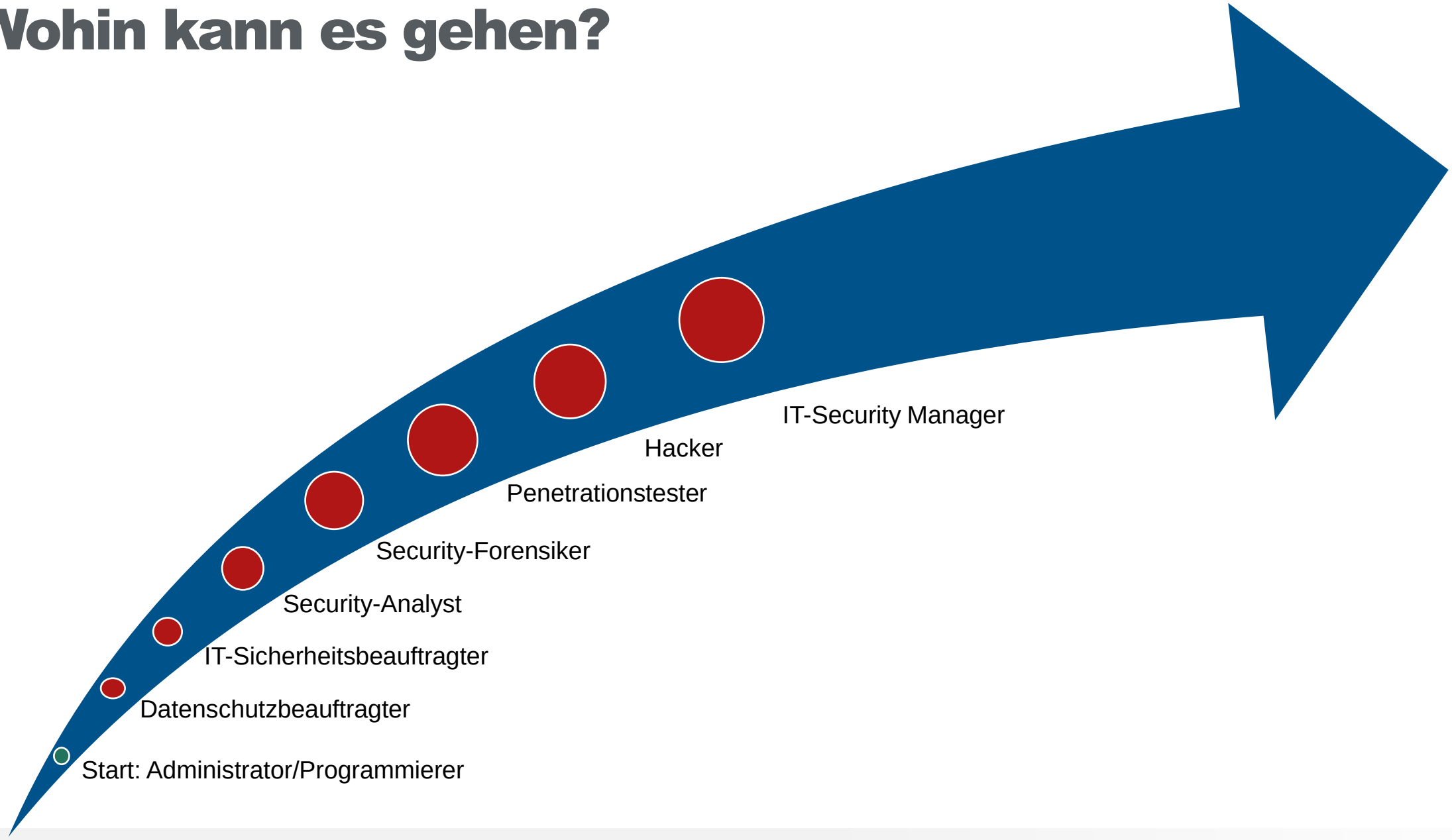
Wohin kann es gehen?



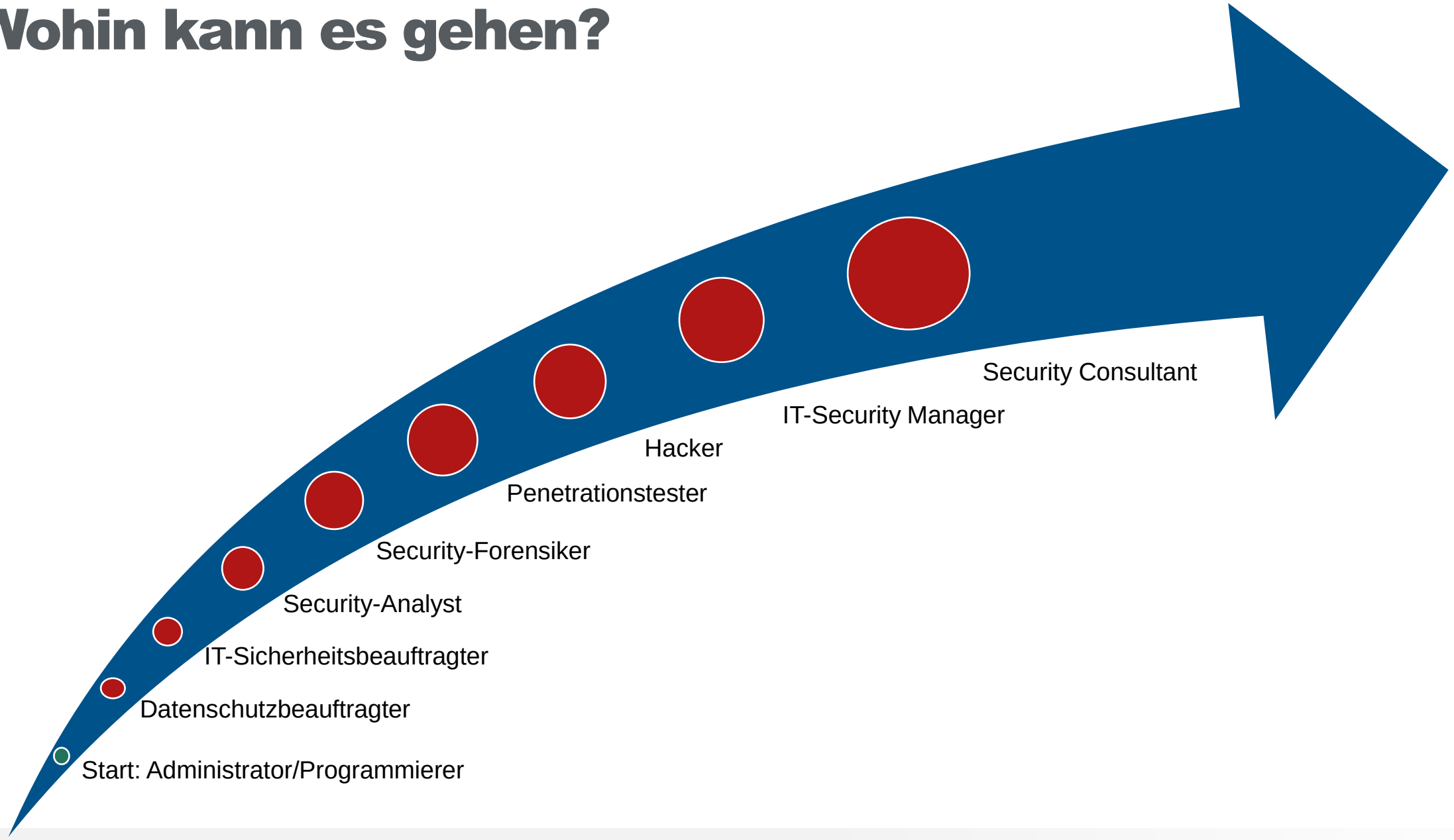
Wohin kann es gehen?



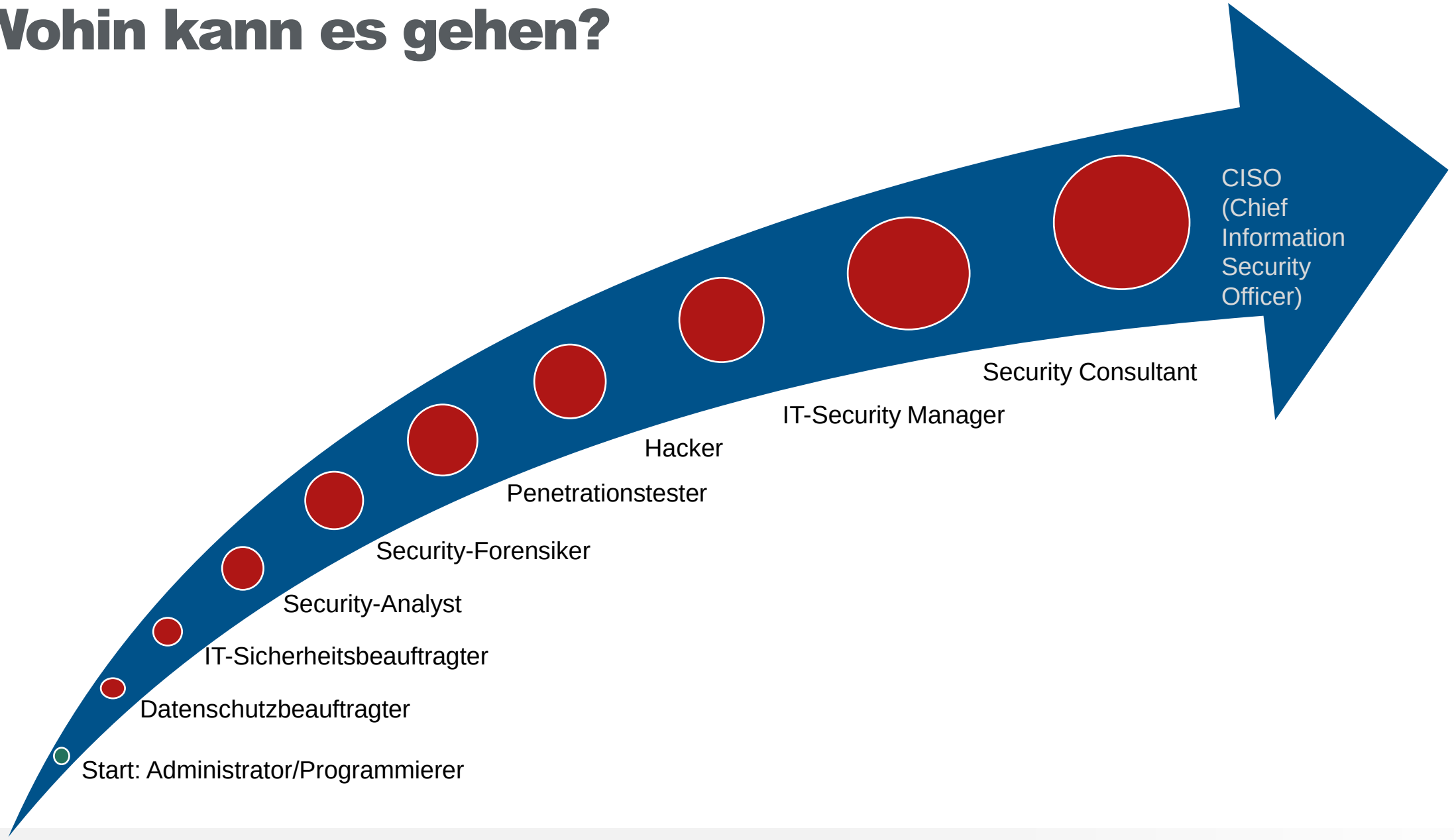
Wohin kann es gehen?



Wohin kann es gehen?



Wohin kann es gehen?

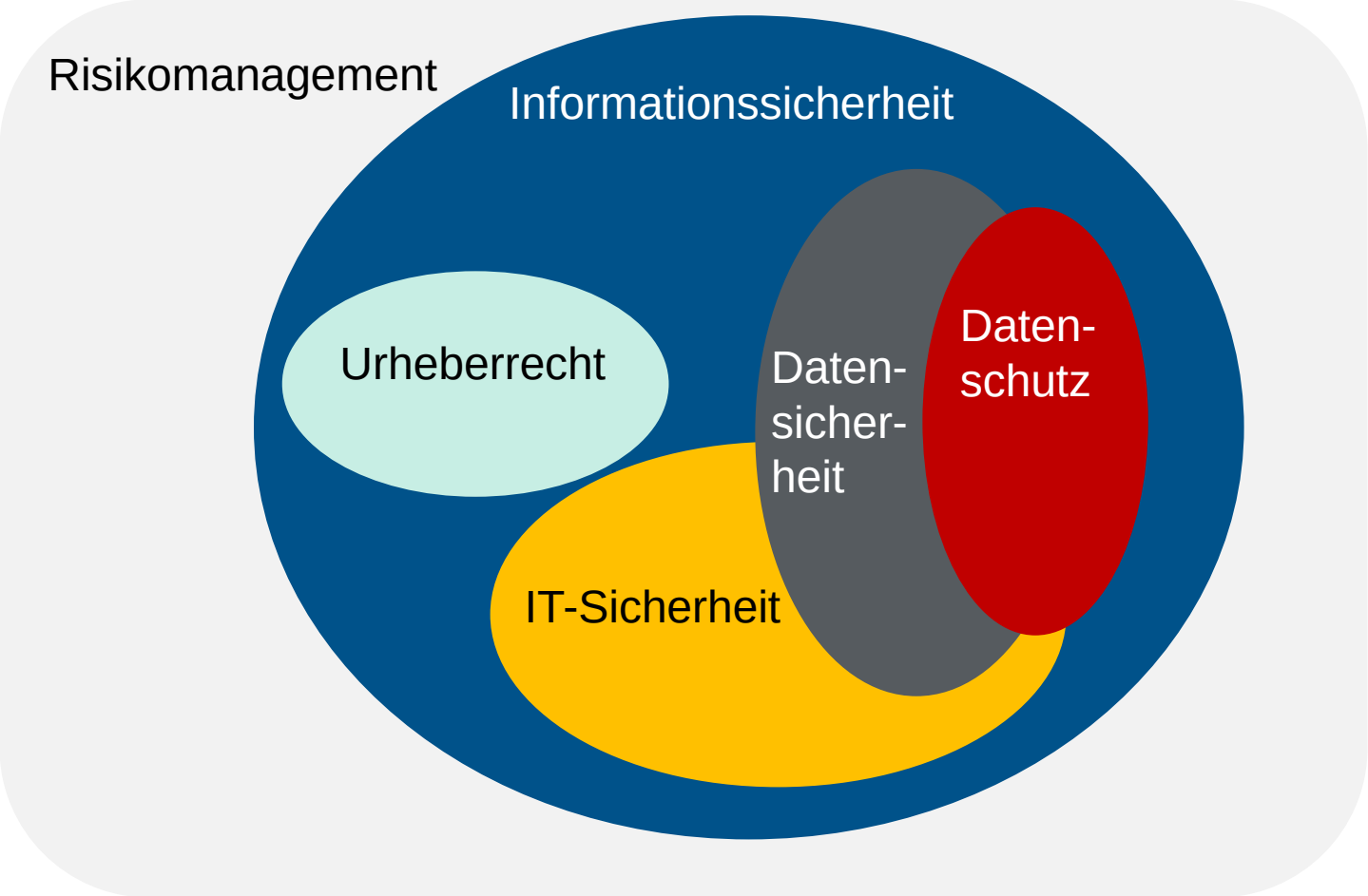


Die Zertifizierungsmöglichkeiten

- CISSP
  - Certified Information Systems Security Professional
- CCSP
  - Certified Cloud Security Professional
- CEH
  - Certified Ethical Hacker
- CompTIA Security+
- CISM
  - Certified Information Security Manager
- CHFI
  - Computer Hacking Forensic Investigator
- CISA
  - Certified Information Systems Auditor
- ISO/IEC 27000-Reihe

Informationssicherheit

Informationssicherheit, Gesetze und Aufsichtsbehörden



Gesetze:
- IT-Sicherheitsgesetz (IT-SiG)
- BSI-Gesetz (BSIG)
- EU-DSGVO
- BDSG

Standards/Zertifikate:
- BSI-Standards
- ISO 27001:2013
- Bußgelder:
  Bis 20 Mio. / 4 % Umsatz

Aufsicht:
- Bundesamt für Sicherheit und Informationstechnik (BSI)
- Bundesdatenschutz-beauftragte
- Landesdatenschutz-beauftragte
- Strafverfolgungs-behörden

©Urheber

Datenschutz

Lernziel

Information zum
Datenschutz
(Analog und Digital)

Private-/ Öffentliche-/
Personenbezogene-/
Gesundheits-Daten

Rechte

Verbote

Datenschutz - Definition

Definition: **Schutz personenbezogener Daten**

„Datenschutz ist Personenschutz“

- Schutz vor missbräuchlicher Datenverarbeitung
- Schutz des Rechts auf informationelle Selbstbestimmung
- Schutz des Persönlichkeitsrechts bei Datenverarbeitung
- Schutz der Privatsphäre

Daten

private

- Persönliche Daten (Einzelangaben)
  - Körperliche Merkmale
  - Geistige Zustände
  - Verhaltensweisen
  - Negative Angaben
  - Verbindung/Beziehung
  - Namen

public

- Daten im Interesse der Allgemeinheit
  - Lehrmaterial
  - Geodaten
  - Statistiken
  - Fakten

Personen-bezogene

- Daten, die Personen direkt zugeordnet werden können
  - Max Mustermann hat blaue Augen
  - Name
  - Geburtstag
  - Rentenversicherungsnummer

Gesundheits-daten

- Daten über physischen und psychischen Zustand eines Menschen
  - Unfälle
  - Selbsthilfegruppen
  - Allergien
  - Raucher
  - Krankheiten

Datenschutz – Rechte / Verbote

Rechte
(Rechte der Betroffenen)

- Anspruch auf Information
- Auskunftsrecht
- Widerspruchsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Vergessenwerden“)
- Recht auf Sperrung der Daten
- Recht auf Datenübertragbarkeit
- Anrufung der Aufsichtsbehörden
- Anspruch auf Schadenersatz

Verbote
(Verbotsprinzip – Verbot mit Erlaubnisvorbehalt)

- Jegliche Datennutzung ist grundsätzlich verboten
- Zulässig nur durch Erlaubnis durch Gesetze oder schriftliche Einwilligung des Betroffenen
- Angabe von Datenerhebung, -Verarbeitung und -nutzung

Datenschutz - Prinzipien

1.) Prinzip: Rechtmäßigkeit

2.) Prinzip: Zweckbindung

3.) Prinzip: Datenminimierung

4.) Prinzip: Richtigkeit

5.) Prinzip: Speicherbegrenzung

6.) Prinzip: Integrität und Vertraulichkeit

7.) Prinzip: Rechenschaftspflicht

Datenschutzgesetze

EU-DSGVO

EU-Datenschutz-Grundverordnung

Datenschtz-Grundverordnung für alle EU Länder

BDSG

Bundesdatenschutzgesetz

Konkretisiert und spezifiziert Vorgaben der DSGVO

Länderabhängig

ePVO

ePrivacy-Verordnung

- Ab etwa 2023
- Ersetzt TKG und TMG
- Schutz Personenbezogener Daten in öffentlichen elektronischen Kommunikation und Werbung

TMG

Telemedien-gesetz

Zentrale Vorschrift des Internetrechts

TKG

Telekommunika-tionsgesetz

Schutz durch den Telekommunikations-anbieter

Datenschutz - Aufgabe

	Aussage	Ziffer
1 – Rechtmäßigkeit	Die Richtigkeit der Datenverarbeitung muss gewährleistet sein und es besteht ein Aktualisierungsanspruch bei Fehlern	
2 – Transparenz	Die Zwecke der Datenverarbeitung müssen bereits bei der Erhebung festgelegt, eindeutig und legitim sein	
3 – Zweckbindung	Die verantwortliche Stelle muss jederzeit umfassende Informationen an die betroffene Personen geben können, welche Daten durch wen und zu welchen Zwecken verarbeitet werden und wurden	
4 – Datenminimierung	Dem Zweck angemessen und auf das notwendige Maß beschränkt	
5 – Richtigkeit	Die Verarbeitung der Daten beruht auf Einwilligung der betroffenen Person	
6 – Speicherbegrenzung	Die Speicherung von Daten unterliegt einer zeitlichen Begrenzung	

©Urheber

Datensicherheit

Lernziel

Unterscheidung zum Datenschutz

Technisch-Organisatorische Maßnahmen

Datensicherheit - Definition

- hat das primäre technische Ziel, Daten jeglicher Art gegen Manipulation, Verlust, unberechtigte Kenntnisnahme und andere Bedrohungen zu sichern

- befasst sich mit dem generellen Schutz von Daten, unabhängig davon, ob diese einen Personenbezug haben oder nicht (z. B. Konstruktionspläne)

- es geht sowohl um Daten in digitaler als auch in analoger Form (Papier)

- ist ein angestrebter Zustand, welcher durch eine Vielzahl an Maßnahmen erreicht werden soll (TOM = technische und organisatorische Maßnahmen)

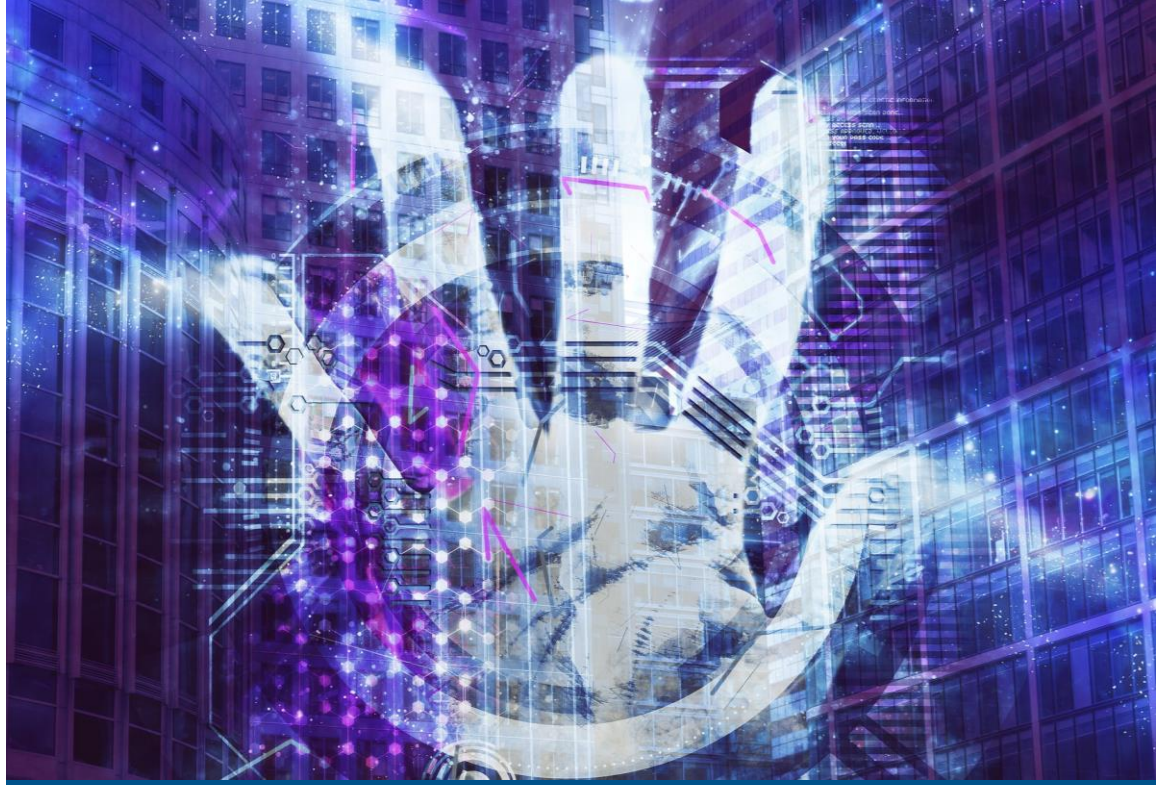
- ist die Voraussetzung für effektive Datenschutzmaßnahmen:
Datenschutz und **Datensicherheit** gehen Hand in Hand

Datensicherheit - TOM

- Zugangskontrolle
- Zugriffskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Datensicherheit / Datenschutz - Aufgabe

Sachverhalt (Verstoß gegen Datensicherheit / Datenschutz)	Datensicherheit	Datenschutz
Die Kundendaten eines IT-Unternehmens werden an den Arbeitgeber eines Kunden weitergeleitet.		
Die Buchung der letzten Woche sind durch einen technischen Defekt verloren gegangen.		
Der Server mit den technischen Daten ist wegen eines Stromausfalls im ganzen Gebäude ausgefallen.		
Die JIKU IT-Solution übersendet einem Personaldienstleister Kundendaten, die er für eine Werbemaßnahme verwendet.		
Eine unberechtigte Person arbeitet mit dem PC des Azubis und speichert sich Kunden- und Firmendaten auf einem Stick.		
Die JIKU IT-Solution setzt gegen zunehmender Diebstähle Videoüberwachung in Ihren Schulungsräumen ein.		
Die JIKU IT-Solution sendet all ihre Daten zwecks Arbeitslosenforschung mithilfe einer KI-Lösung an eine Universität.		
Ein Teilnehmer beschafft sich die Sicherheitscode des Zentralcomputers um an die Kontaktdaten einer Assistenz zu kommen.		
Eine fremde Person hat sich ohne Erlaubnis Zutritt zum Serverraum verschafft.		



©Urheber

IT-Sicherheit

Lernziel

Unterscheidung zum Datenschutz + Datensicherheit

Security Controls + Functions

Definition/Abgrenzung

Wo beginnt IT-Sicherheit?

Schutz der Organisation vor Bedrohungen und Angriffen

Bezug nicht nur auf IT-Systeme, sondern auch auf physikalische Objekte

Security Controls

Administrative

Maßnahme des Unternehmens zur IT-Sicherheit

Gesetze, Richtlinien, Leitfäden, Best Practices

Technische

Maßnahme IT-Systeme zur IT-Sicherheit

Computer, Firewalls, Passwörter, Authentifizierung, Verschlüsselung

Physische

Maßnahme in der realen Welt

Tore, Wachen, Schlüssel, Man Traps

Security Functions

Deterrent

(Abschreckung)

Hält davon ab, die Bedrohung zu versuchen

Preventative

(Vorbeugung)

Hält davon ab, die Bedrohung auszuführen

Detective

(Überwachung)

Die Bedrohung erkennen

Corrective

(Korrekt)

Minimiert die Auswirkung einer vorhanden Bedrohung

Compensating

(Kompensierung)

Bietet eine alternative Korrektur der anderen Funktionen

Aufgabe

	Administrativ Control	Technical Control	Physical Control
Deterrent			
Preventative			
Detective			
Corrective			
Compensating			

- Hintergrundcheck
- Mitarbeiterschulung
- Firewall
- Backup
- Warnschild
- Videoüberwachung

- Zaun
- Logfiles
- Wachhund
- Sicherheitspersonal
- Loch in der Wand und ein Sicherheitspersonal sitzt davor

©Urheber

Urheberrecht

Lernziel

Urheberrecht,
Copyright,
Markenrecht und
Lizenzen

Sonstige Rechte

Urheber-recht
(UrhG)

Schutz des geistigen Eigentums

Marken-recht
(MarkenG)

Schutz von Bezeichnungen von Produkten im geschäftlichen Verkehr

Lizenz-recht
(Lizenz)

Genehmigung oder Erlaubnis eines Rechtssubjektes zur wirtschaftlichen Nutzung

Copyright
©

Recht am vervielfältigen eines Werkes

Nutzungs-recht

Recht eines Rechtssubjekts aus einem Vertrag, fremde Sachen oder Rechte zu nutzen

Urheberrecht vs. Copyright

Urheber-recht
(UrhG)

Werk untrennbarer Teil der Autorenperson

- Verzicht auf Urheberrecht unmöglich
- Hauptsächlich im deutschsprachigen Raum

Copyright
©

Öffentliches Wohl durch wirtschaftlichen Anreiz

- Verzicht auf Copyright möglich
- Kann vom Autor vollständig übertragen werden

Markenrecht

Marken-recht
(MarkenG)

Schutz

- Geschäftliche Bezeichnungen
- Geografische Herkunftsangaben
- Besondere Wörter
- Personennamen
- Abbildungen
- Buchstaben
- Zahlen
- Klänge
- Dreidimensionale Gestaltungen

Beispiele

- Schuhhersteller: Nike, Adidas, Puma usw.
- IT-Unternehmen: Microsoft (Auch Produkte), Apple, Google usw.
- Andere Hersteller: Ferrero, Gucci usw.

Nutzungsrecht

Nutzungs-recht

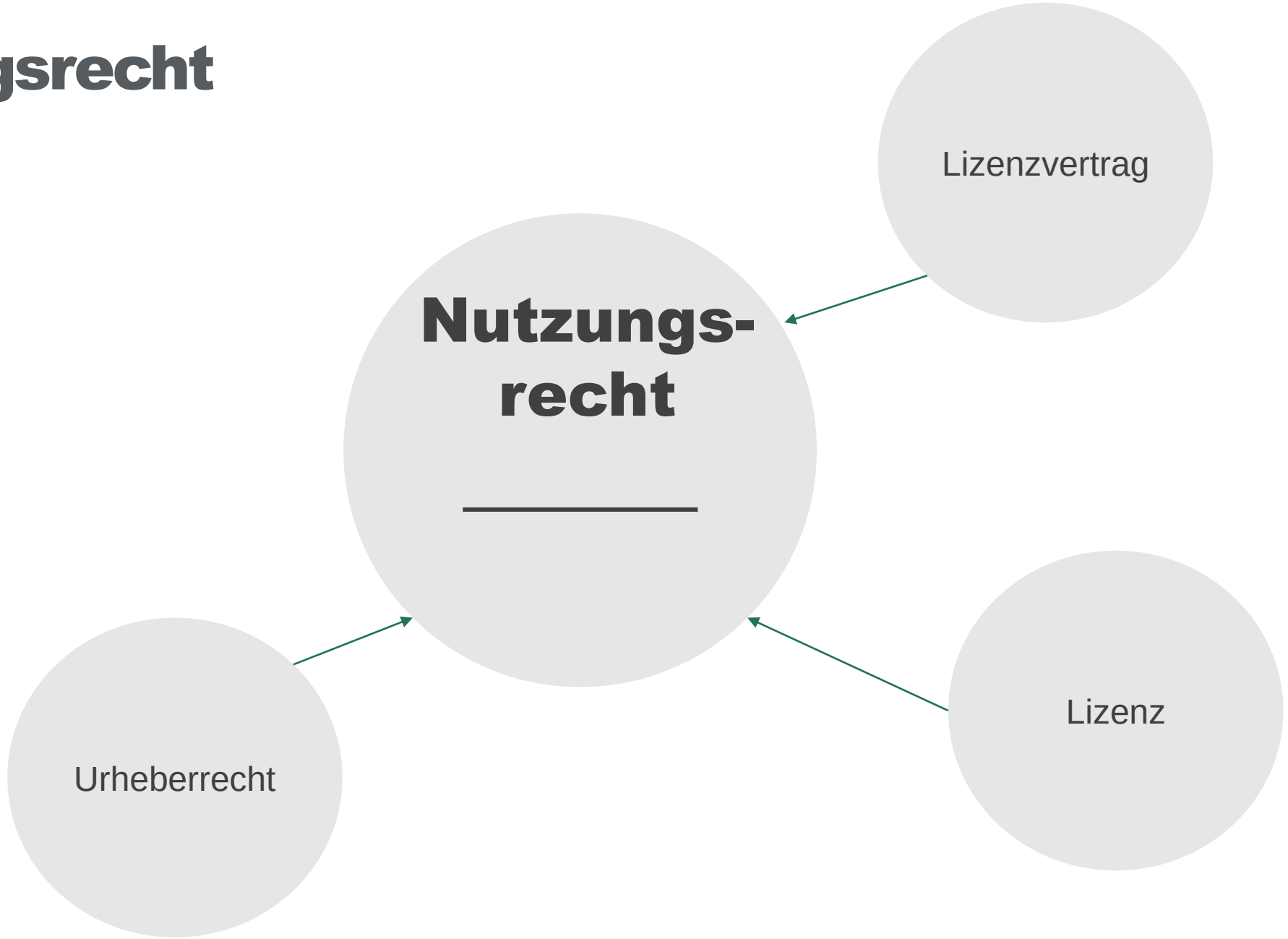
Einfaches Nutzungsrecht

Berechtigung des Dritten neben dem Urheber

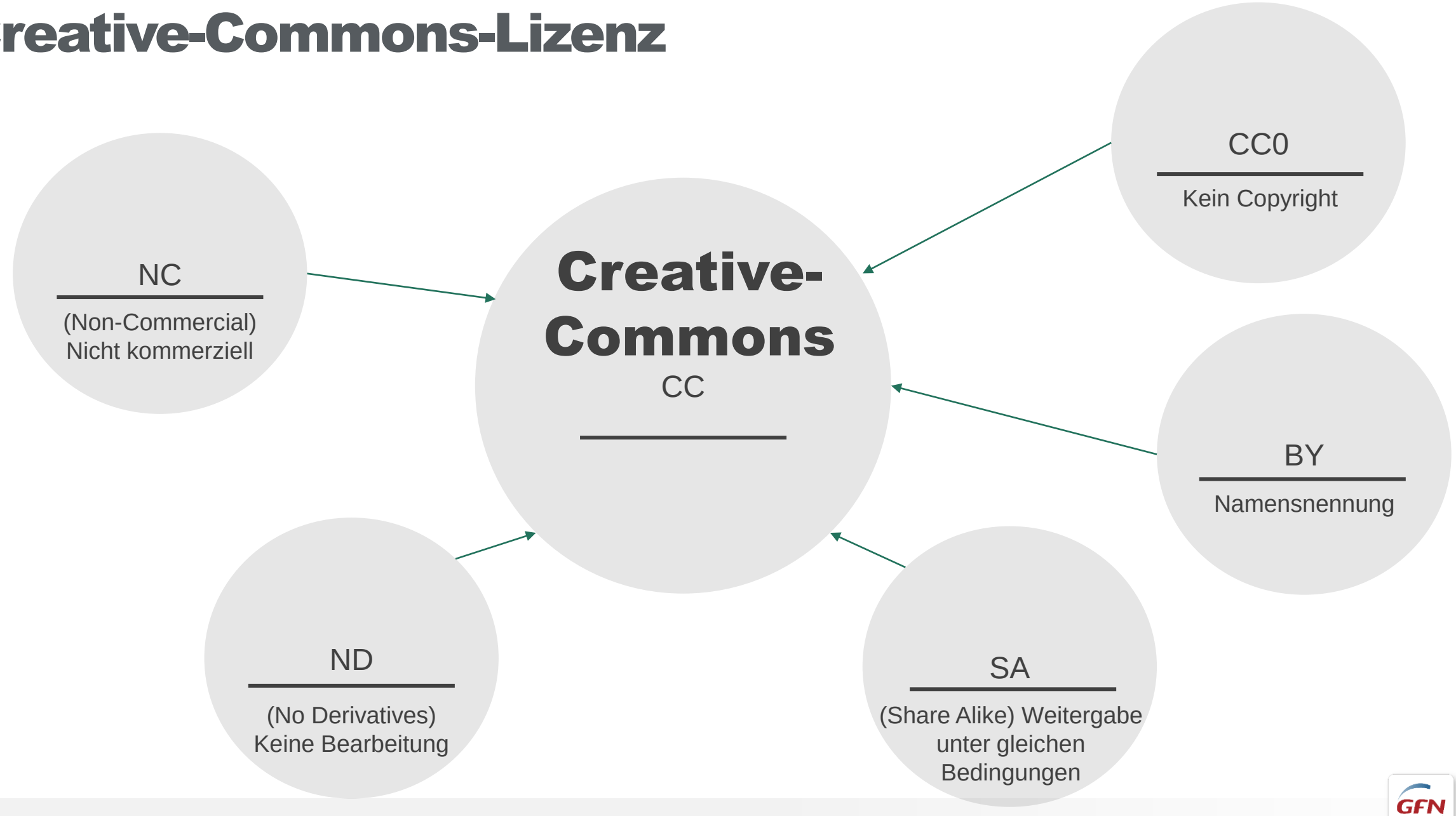
Ausschließ-liches Nutzungsrecht

Berechtigung des Dritten unter Ausschluss auch des Urhebers

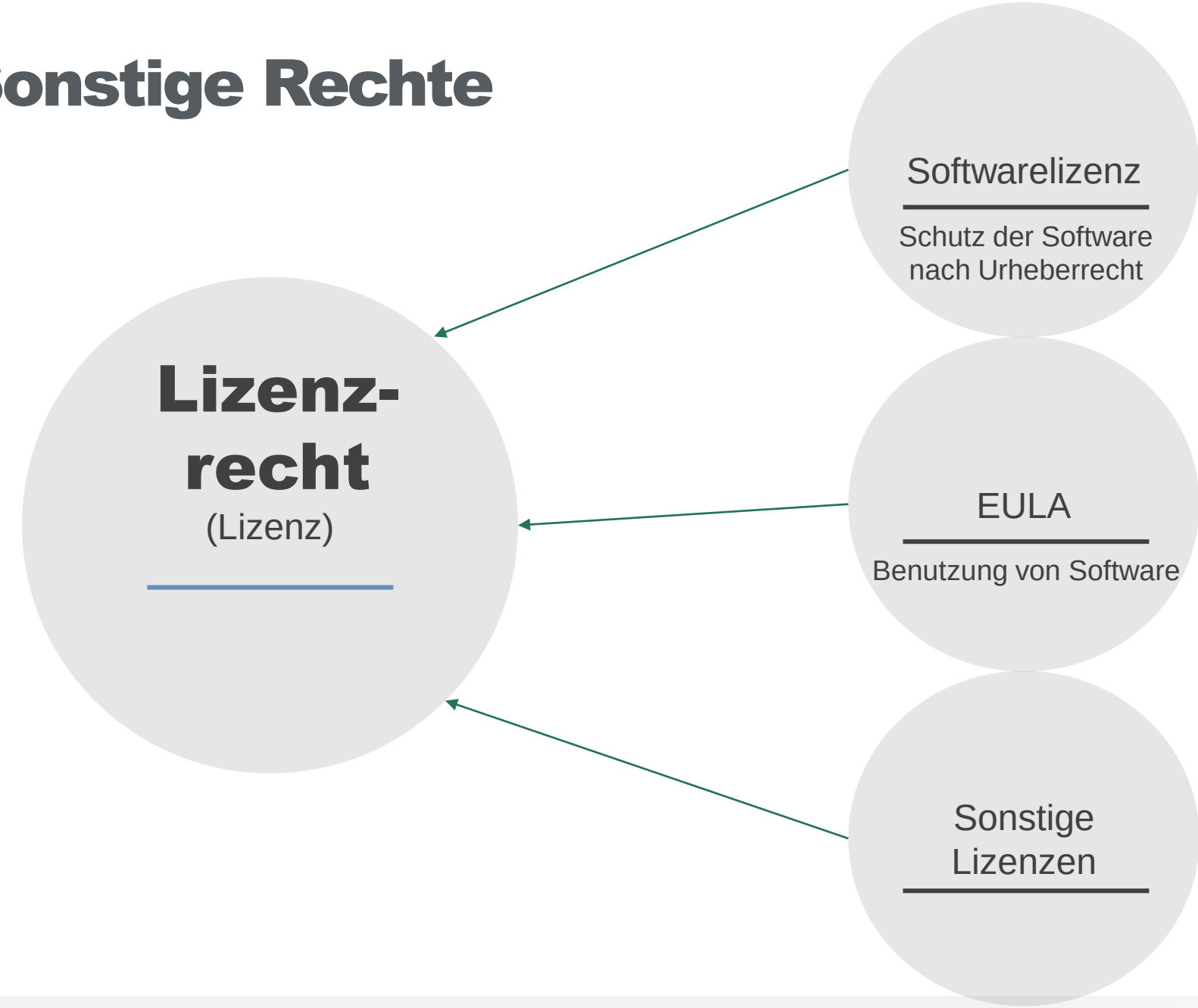
Nutzungsrecht



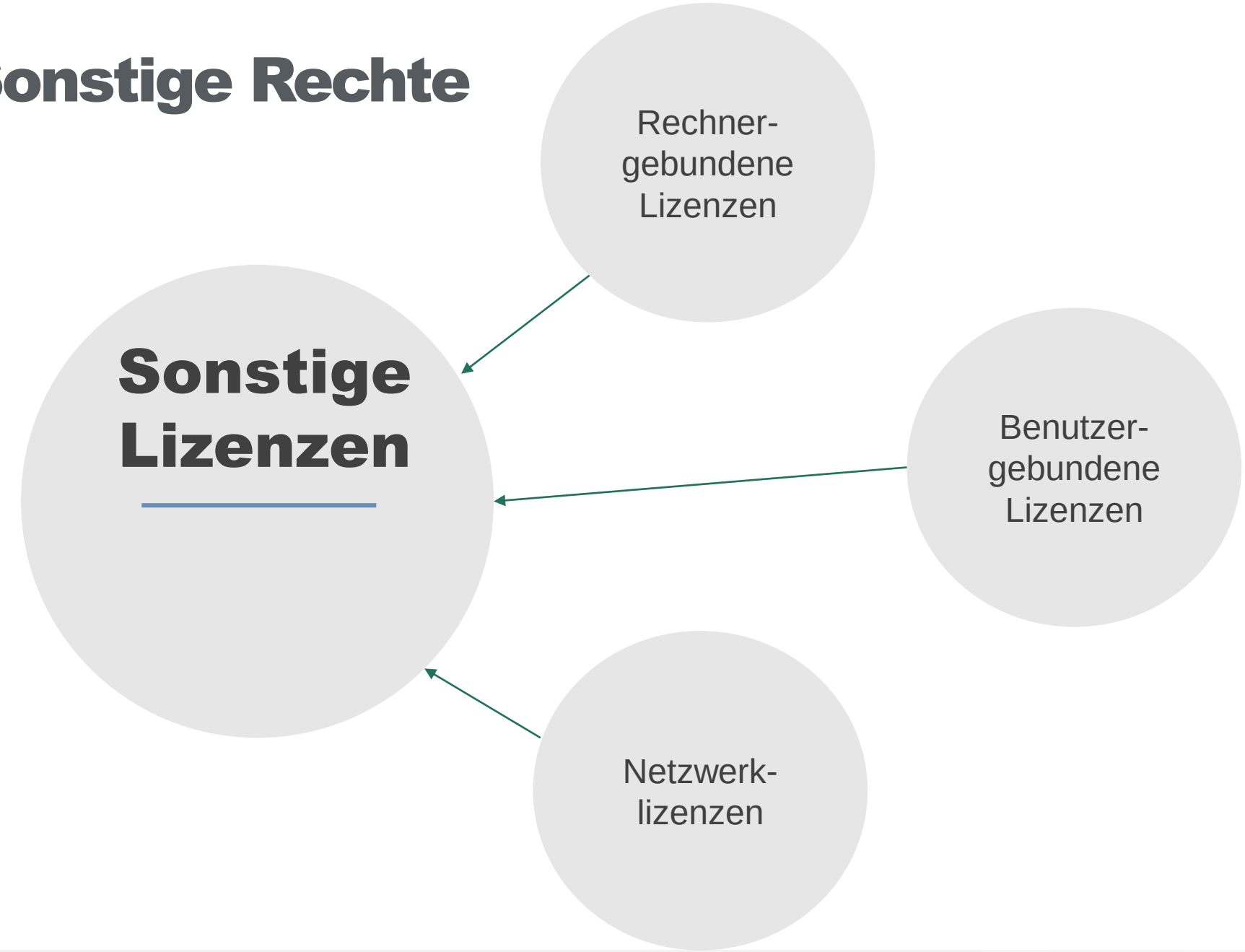
Creative-Commons-Lizenz



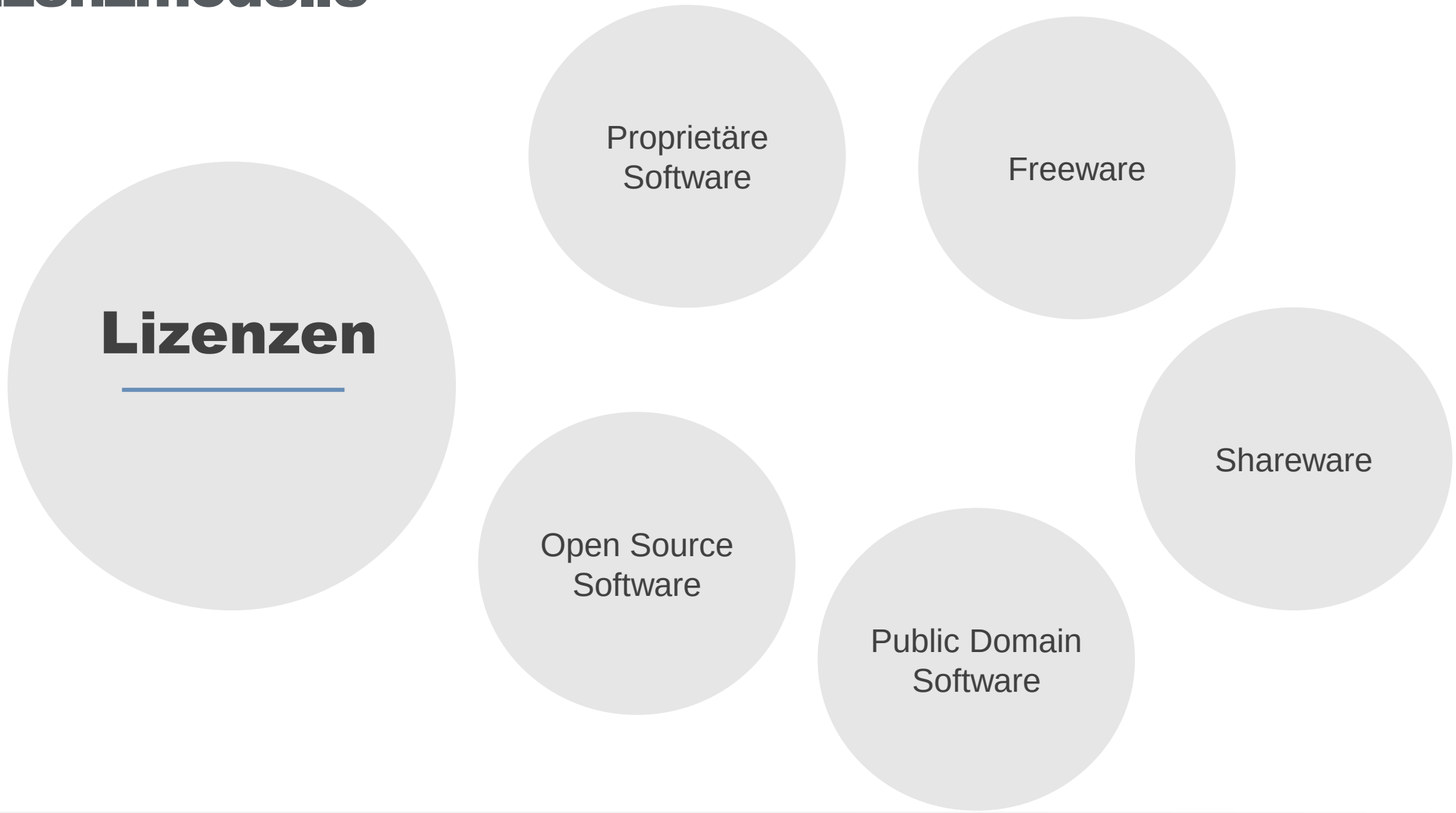
Sonstige Rechte



Sonstige Rechte



Lizenzmodelle



Fachbegriffe

Nutzer-/User-Lizenzen

Client Access License

Named User License

Concurrent Access License

Key Management Service

CPU-Klauseln

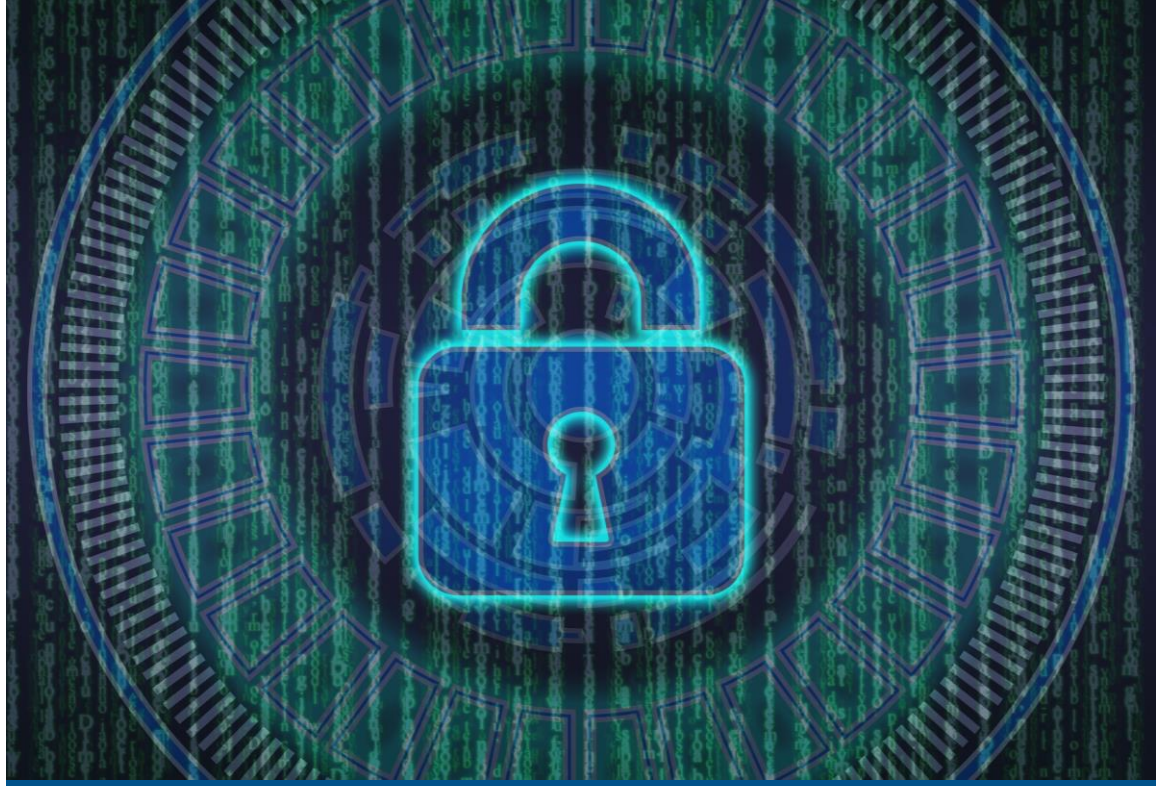
OEM

Maintenance

SPLA von CSP

Zweitkopie Recht

LTS



©Urheber

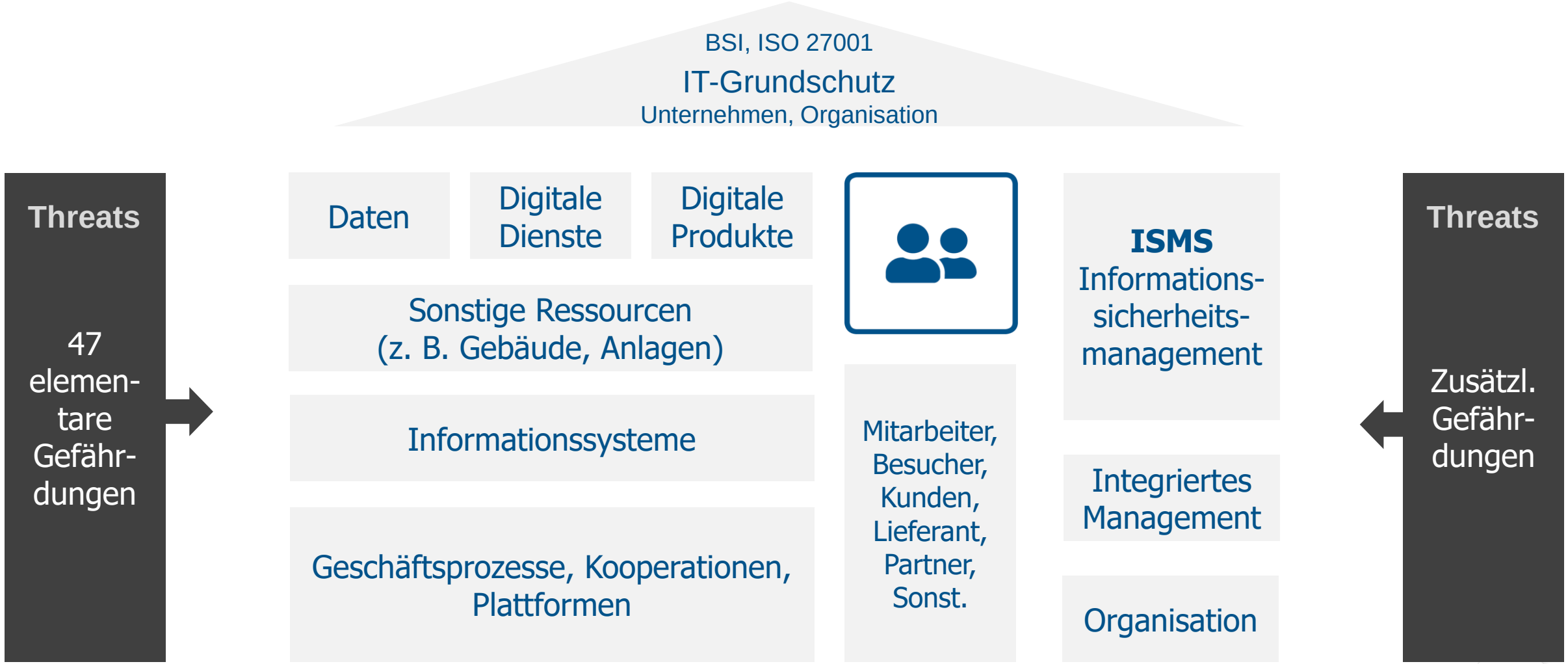
IT-Grundschutz

Lernziel

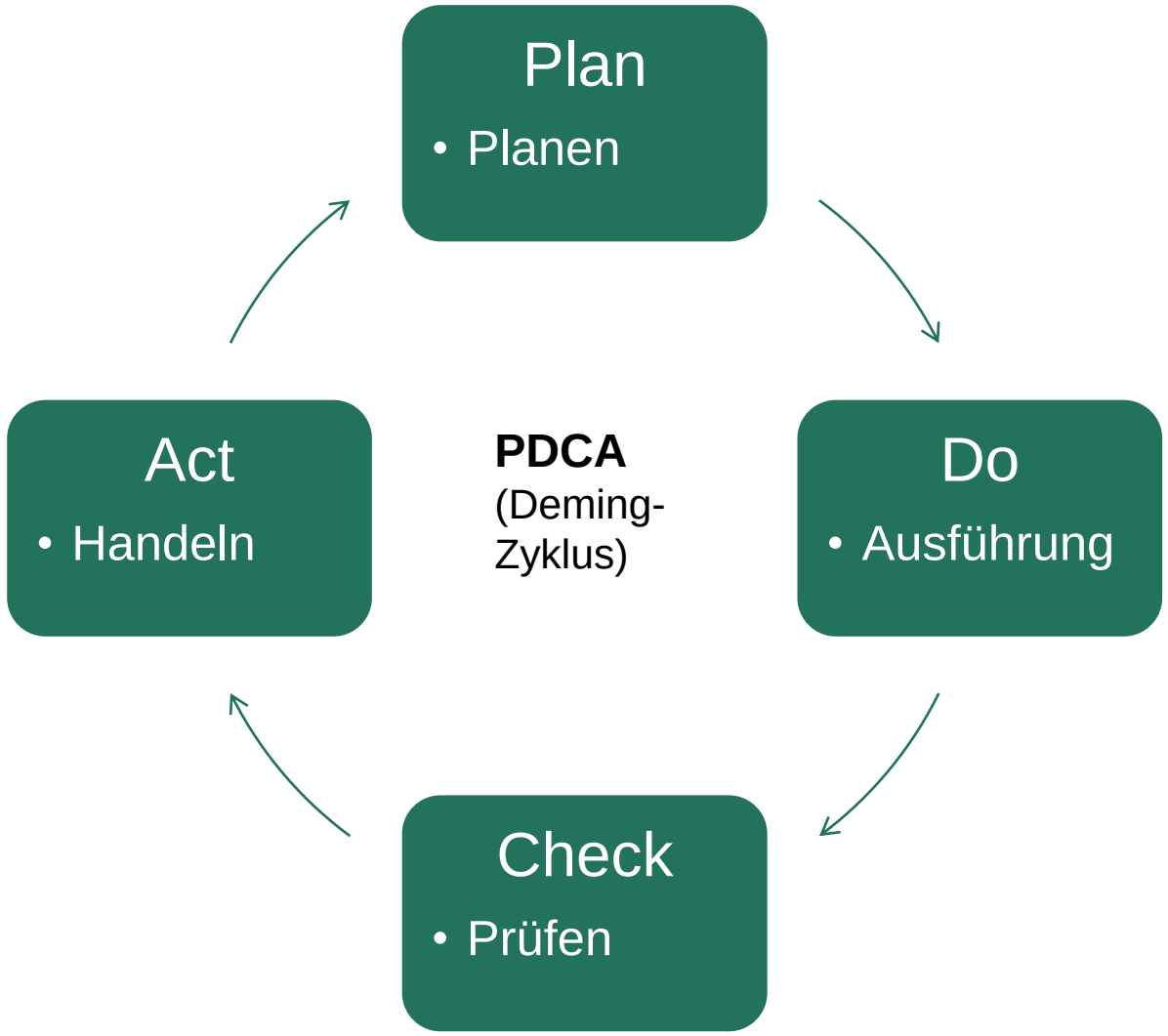
IT-Grundschutz

Schutzziele

IT-Grundschutz



Prozess


Plan
• Planen
Do
• Ausführung
Check
• Prüfen
Act
• Handeln
PDCA
(Deming-Zyklus)

Schutzziele

C

Confidentiality

(Vertraulichkeit)

Personenbezogene Daten, digitale Werte

I

Integrity

(Integrität)

Korrektheit von Informationen

A

Availability

(Verfügbarkeit)

Ressourcen und Informationen

Authentizität

Echtheit, Überprüfbarkeit, Vertrauenswürdigkeit

Verbindlichkeit

Kein unzulässiges Abstreiten durchgeführter Handlungen

Zurechenbarkeit

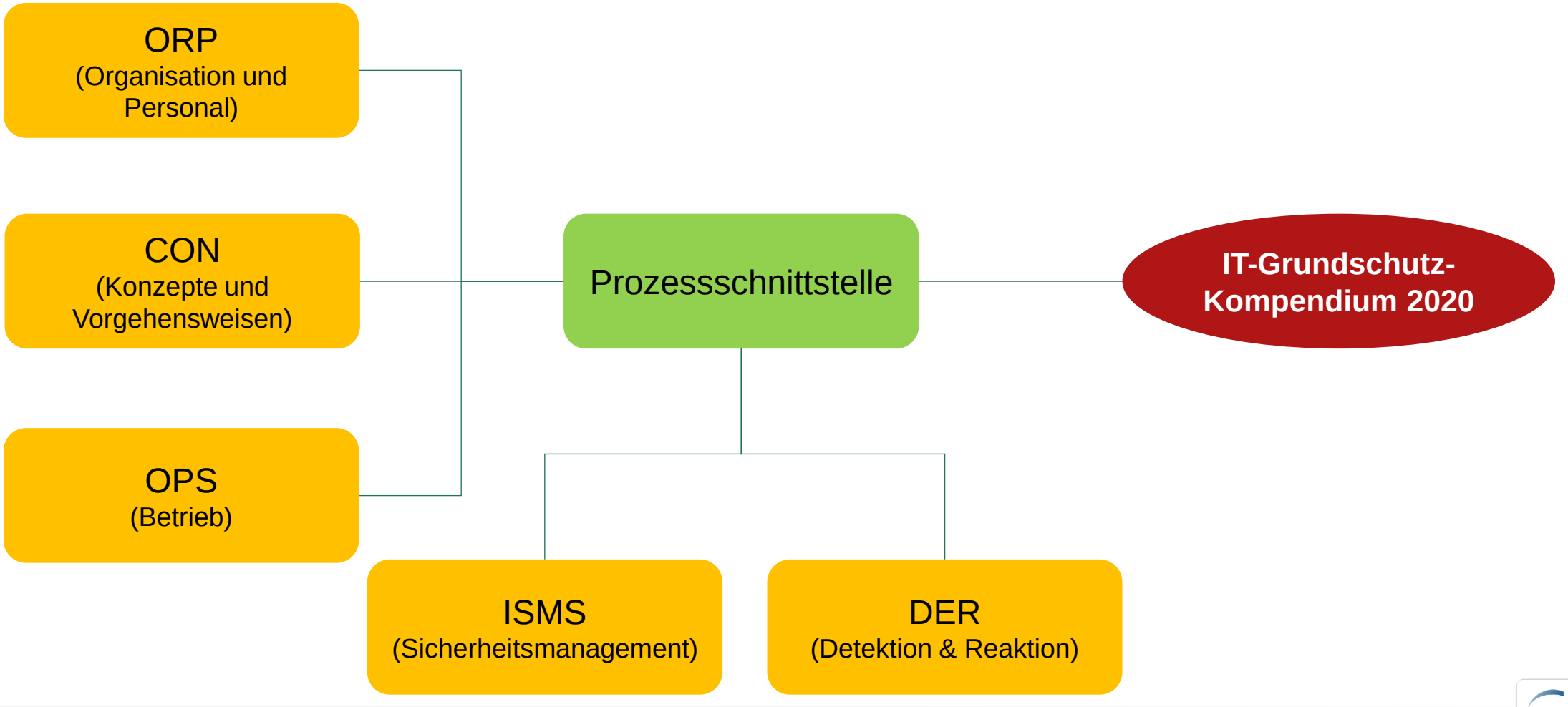
Handlung kann Partner eindeutig zugeordnet werden

Anonymität

Anzeigen von Informationen

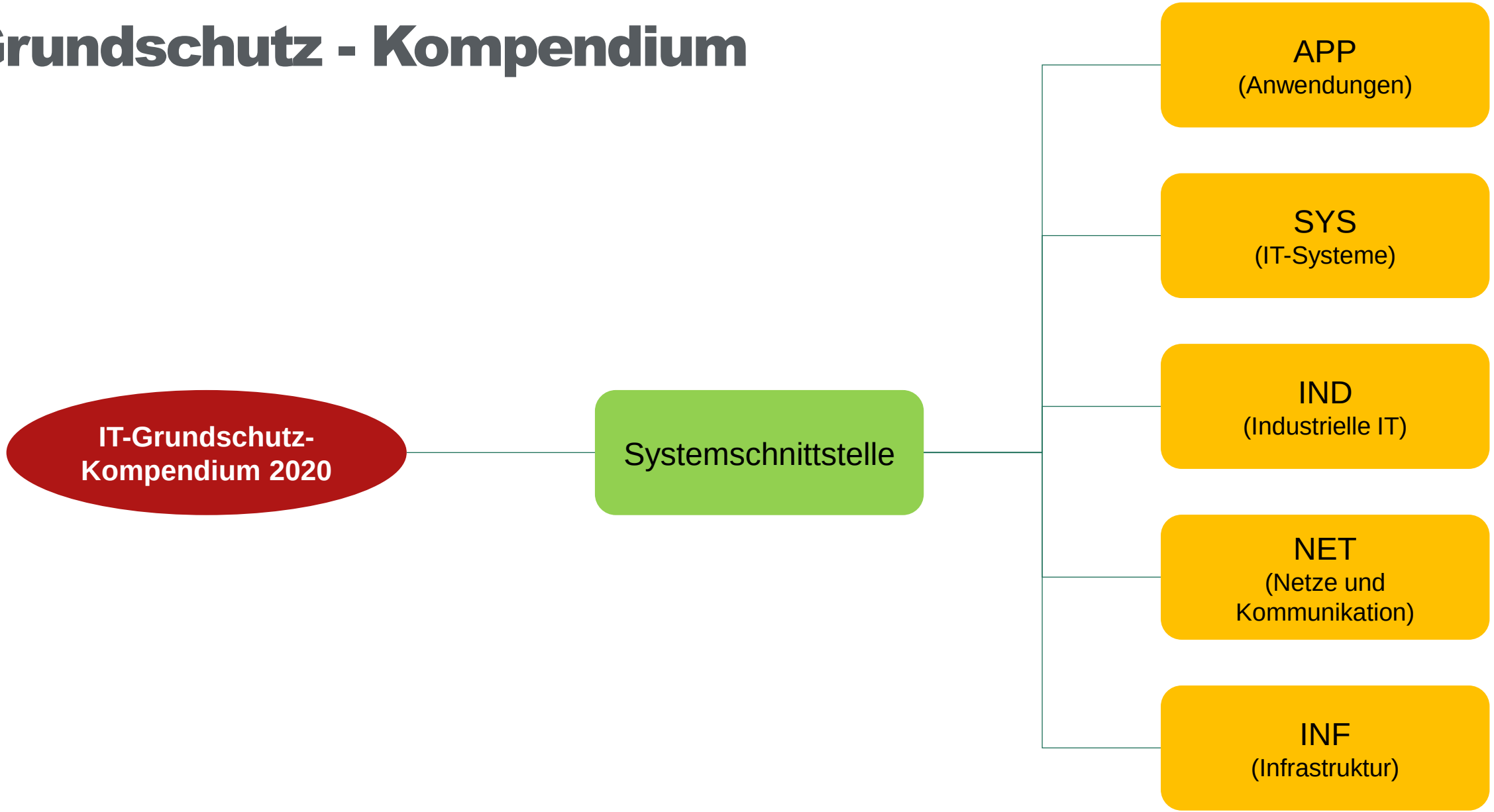
Grundschutz - Kompendium

Grundschutz - Kompendium



Grundschutz - Kompendium

Grundschutz - Kompendium



Checklistenerstellung - Aufgabe

- BSI-Kompendium mit technisch-organisatorische Maßnahmen

TOM

- Zugangskontrolle
- Zugriffskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Zuverlässigkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Kompendium

- INF – Allgemeines Gebäude
- INF – Büroarbeitsplatz
- INF – Häuslicher Arbeitsplatz
- INF – Mobiler Arbeitsplatz
- INF – Besprechungs-, Veranstaltungs- und Schulungsraum
- OPS – Telearbeit
- OPS – Cloud-Nutzung
- SYS – Allgemeiner Client
- SYS – Allgemeine Smartphones und Tablets
- SYS – Drucker, Kopierer und Multifunktionsgeräte
- SYS – Wechseldaten-träger
- APP – Office-Produkte
- CON – Auswahl und Einsatz von Standardsoftware

Checklistenerstellung - Aufgabe

1. Zutrittskontrolle (Gebäude, Räume)
2. Zugangskontrolle Unbefugter zu IT-Systemen/Peripherie
3. Zugriffskontrolle vor Zugriff nicht Berechtigter
4. Weitergabe- /Transportkontrolle von personenbezogenen Daten
5. Überprüfung der Wirksamkeit der Maßnahme (TOM)

©Urheber

Risikomanagement

Lernziel

Grundlagen Risiko

Grundlagen Risikomanagement

Kategorisieren von Risiken

Definitionen

Risiko

Risikoanalyse

Risikomanagement

Hauptteile

Objekt
(Assets)

Nützlicher Teil eines Unternehmens

Schwach-stelle
(Vulnerability)

Schwäche eines Objektes

Bedrohung
(Threats)

Negative Aktion, die eine Schwachstelle ausnutzt

Prozentsatz einer Bedrohung

- Wahrscheinlichkeit (Likelihood)

Quantitativ

Chance

Qualitativ

Nummer / Level

Einschlag (Impact)

- Schaden durch Bedrohung

Quantitativ

Messbar

Qualitativ

Nicht direkt Messbar

Risiko

Risiko = Bedrohung x Schwachstelle

Dokument für alle Bedrohungen und Schwachstellen:

BSI-Kompendium

Risikomanagement

Risiko-Identifikation / Bewertung

1. Katalogisieren und Definieren aller Objekte
   - Schwachstellen-Bewertung

2. Mehr aktive Tools
   - Schwachstellen-Bewertungstools

3. Bedrohungsbewertung

Bedrohungsbewertung

- Elementare Gefährdungen

Adversarial
Kontrovers

Schlechte Dinge

Accidental
Versehentlich

Falsche oder zu viele Rechte

Structural
Strukturell

Kann abstürzen

Environ-mental
Umwelt

Potentielle Probleme

Risikominimierung

- Ziel: Was ist zu tun
- Minimierung der Wahrscheinlichkeit

Mitigation
Minimierung

Minimierung des Risikos

Transference
Transferierung

Verschieben der Wahrscheinlichkeit, Risiko und Bedrohung an Dritte

Acceptance
Akzeptieren

Wahrscheinlichkeit und Eintritt des Risikos sind geringer, als die Kosten, um das Risiko zu minimieren

Avoidance
Vermeidung

Die Kombination aus Wahrscheinlichkeit und Eintritt ist so hoch, dass man die Auseinandersetzung damit vermeidet