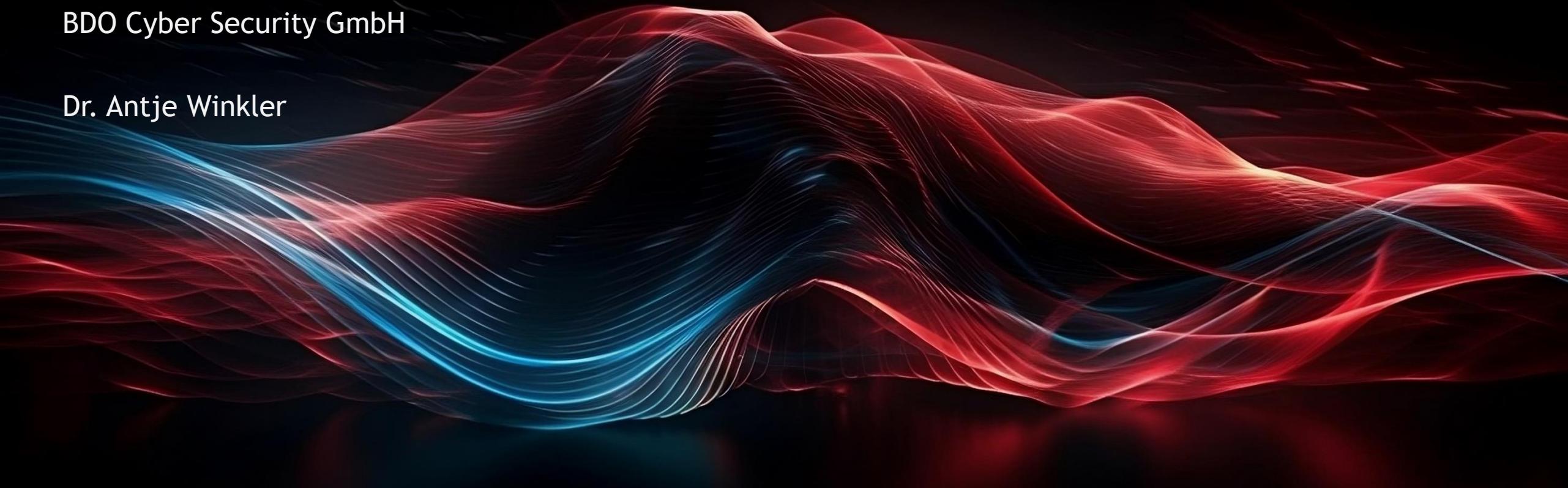


# Penetrationstest

BDO Cyber Security GmbH

Dr. Antje Winkler



Was ist unsere Motivation?

# Cyberangriffe in Zahlen



**4.500.000 €**

**3 von 5 Unternehmen** in Deutschland wurden im Jahr 2023 mindestens einmal Opfer einer Cyber-Attacke

**4,5 Mio. €** durchschnittlicher Schaden pro Vorfall

**206 Mrd. €** Gesamtschaden deutscher Unternehmen im Zusammenhang mit Diebstahl, Industriespionage und Sabotage (2023)



**3+ Monate** bis zur Rückkehr zum Normalbetrieb, wie z.B. im Fall von ca. 103 westfälischen Kommunen oder dem Frankfurter Uniklinikum

**52 % der Unternehmen** fühlen sich durch Cyberangriffe in ihrer Existenz bedroht



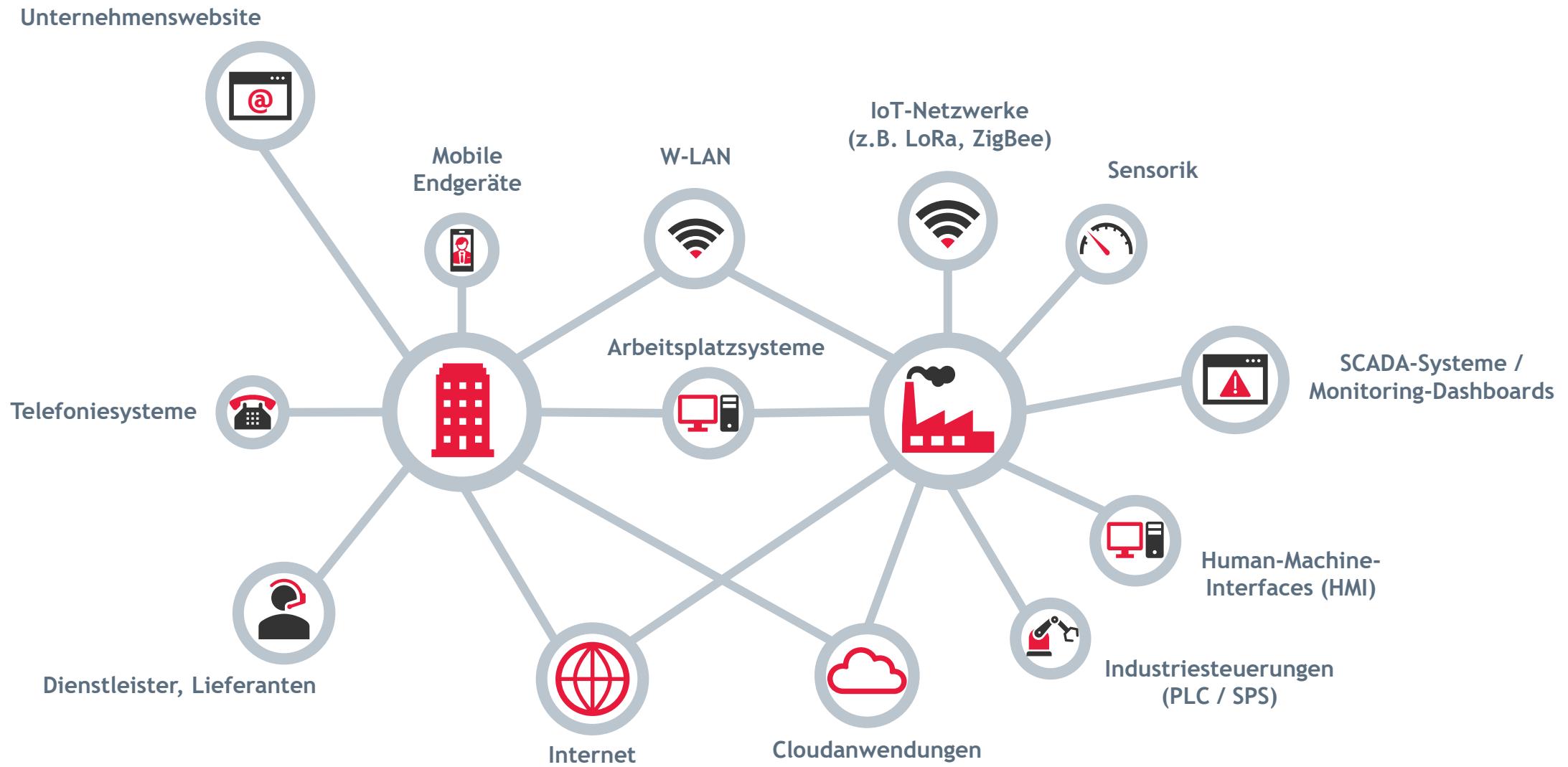
**ca. 20 % der Unternehmen** stehen dann am Rande der Insolvenz

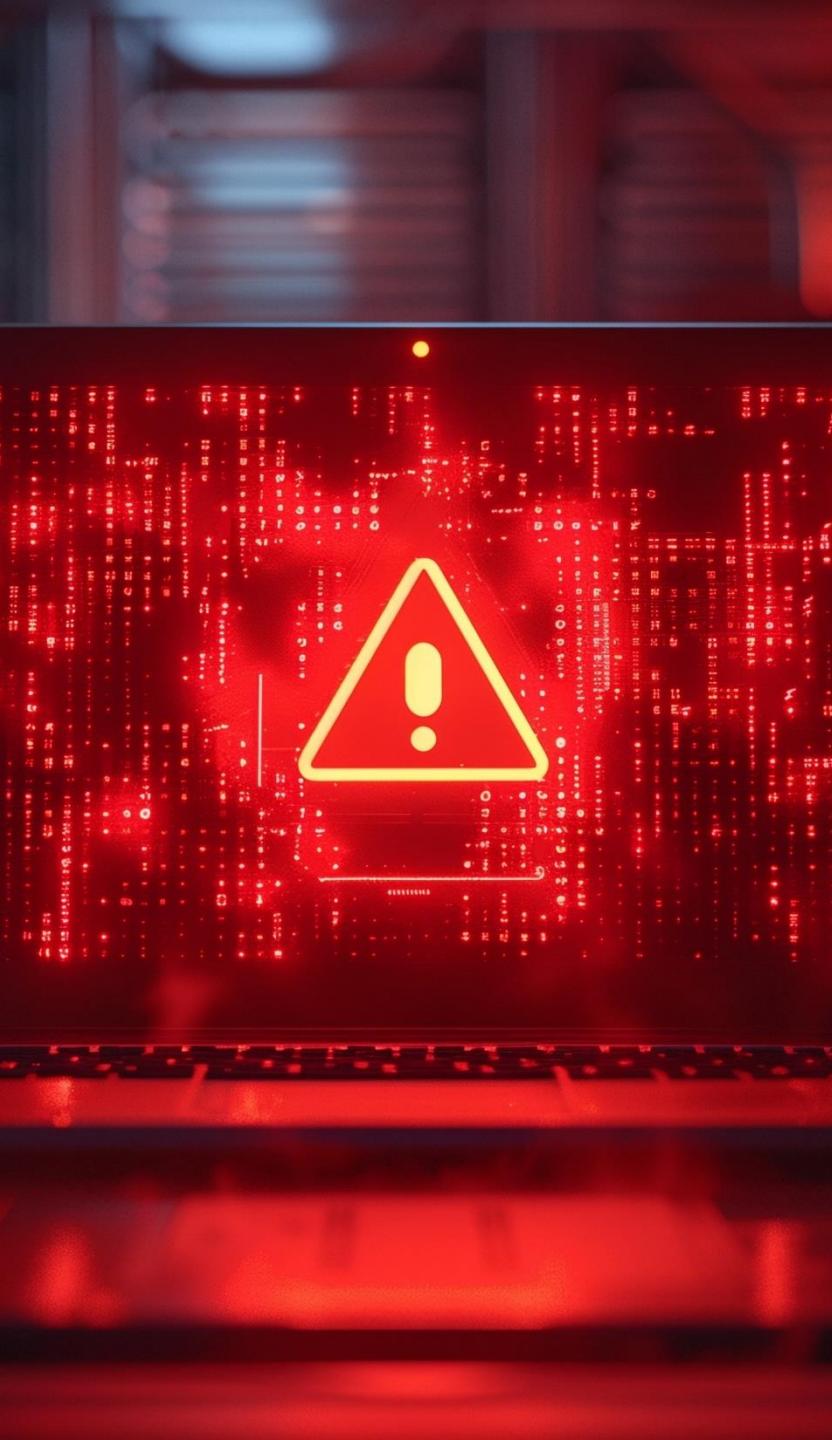


## Richtlinien und Vorgaben durch den Gesetzgeber

- ▶ DSGVO
- ▶ NIS2-Richtlinie
- ▶ BSI-Kritisverordnung
- ▶ ISO27001
- ▶ BSI-Grundschutz

# Zunehmende Vernetzung - Erhöhung der Komplexität





# Aktuelle Bedrohungen

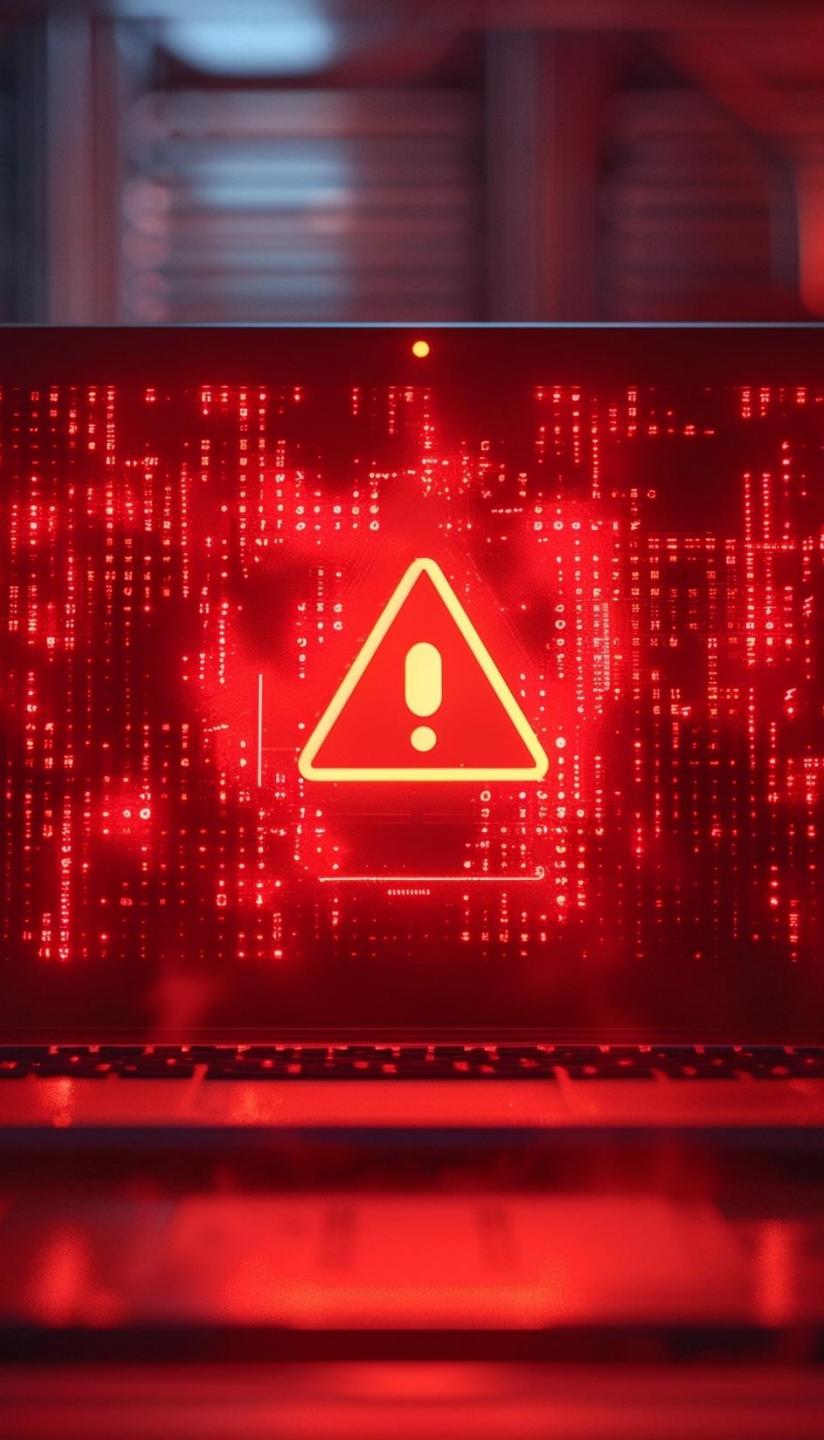
## Häufigste Bedrohungsszenarien

### Ransomware, Schadsoftware und Phishing

- ▶ Angriffe, bei denen Cyberkriminelle die Kontrolle über ein System übernehmen und Lösegeld für dessen Rückgabe verlangen
- ▶ **Achtung:** Daten liegen immer noch in den Händen der Angreifer, können auch jederzeit später und trotz Zahlung noch abfließen

### Wie kann man sich schützen?

- ▶ Absender prüfen
- ▶ Links nicht direkt anklicken
- ▶ Plausibilität prüfen
- ▶ Keine persönlichen Daten preisgeben
- ▶ Vorsicht bei vorgetäuschter Dringlichkeit
- ▶ Vorsicht bei Anhängen
- ▶ Im Zweifel lieber nicht bearbeiten



# Aktuelle Bedrohungen

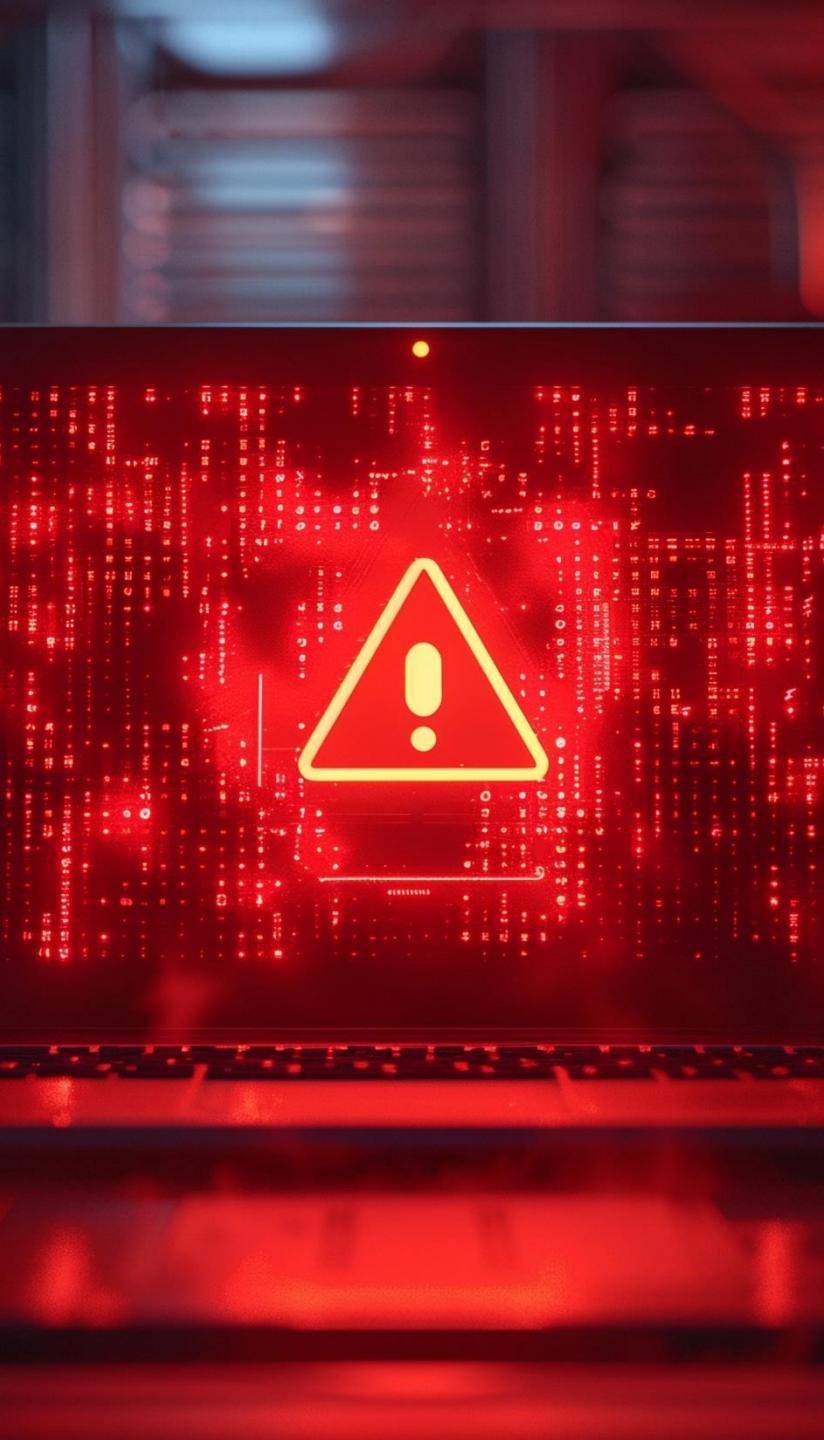
## Häufigste Bedrohungsszenarien

### Angriffe auf Lieferketten

- ▶ Vgl. Ransomware und Schwachstellen/Fehlkonfigurationen
- ▶ Ziel des Angriffs ist ein verbundenes Unternehmen bzw. ein Dienstleister
- ▶ Auswirkungen werden „weitergetragen“, z.B. durch infizierte Software/Dateien und vermeintlich vertrauenswürdige Kommunikationskanäle

### Wie kann man sich schützen?

- ▶ Dienstleister auditieren
- ▶ Auch zugekauft Soft- und Hardware prüfen



# Aktuelle Bedrohungen

## Häufigste Bedrohungsszenarien

### Schwachstellen und Fehlkonfigurationen

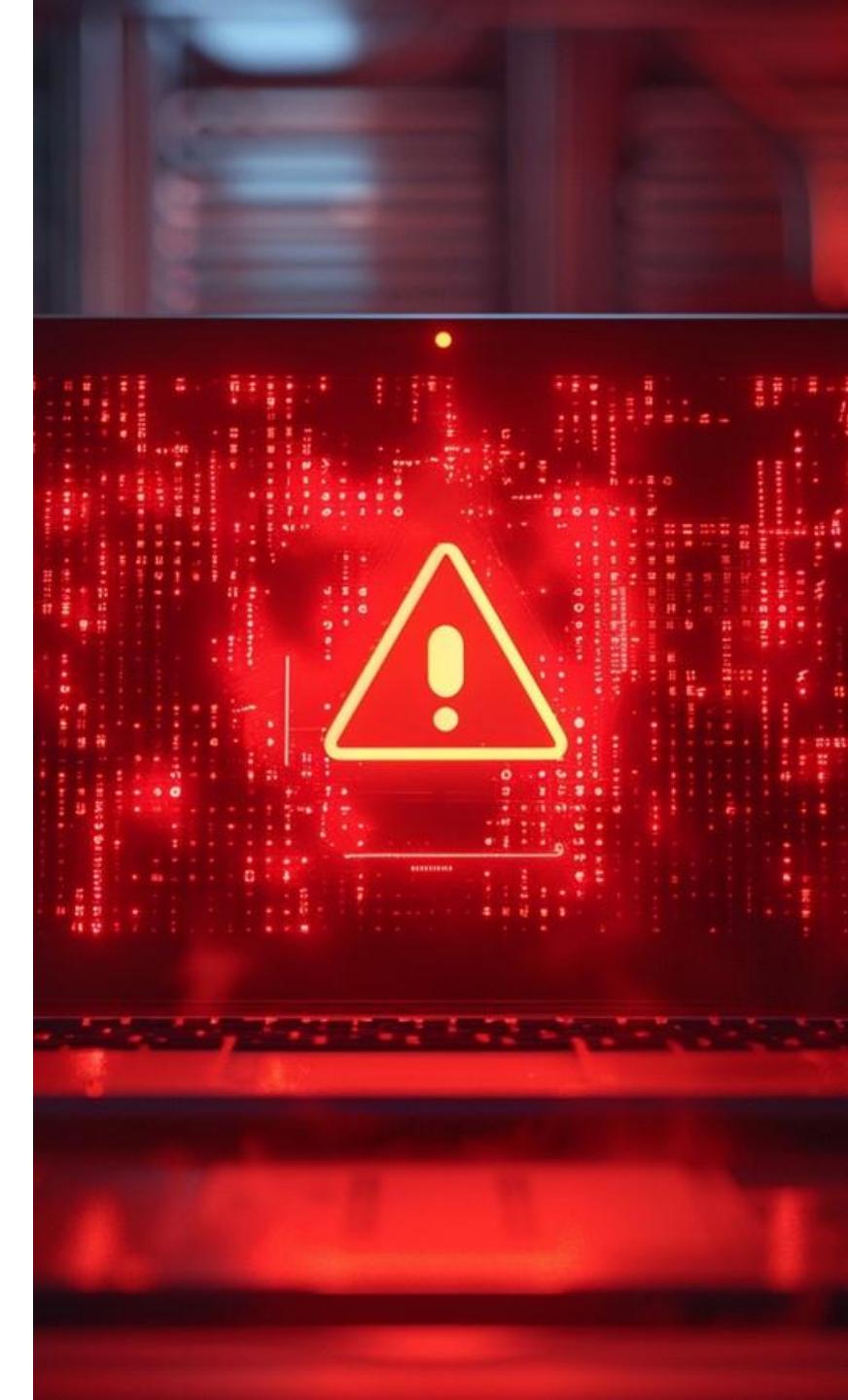
- ▶ IT-Systeme nicht auf aktuellem Stand der Technik
- ▶ Schnittstellen unbewusst exponiert
- ▶ Unklare Verantwortlichkeiten, fehlende Patch-Prozesse

### Wie kann man sich schützen?

- ▶ Angriffsfläche minimieren
- ▶ Systeme aktuell halten
- ▶ Gegen Brute-Force schützen

# Gründe für die meisten erfolgreichen Angriffe - Faktor Mensch

- ▶ Schlechte Passwörter: <https://www.youtube.com/watch?v=opRMrEfAII>
  - ▶ hallo
  - ▶ 1234567890
  - ▶ 1234567
  - ▶ password
  - ▶ password1
  - ▶ target123
  - ▶ iloveyou
  - ▶ gerty123
- ▶ Teilen von sensiblen privaten Informationen im Internet / sozialen Netzwerken
- ▶ Installation / Herunterladen von fragwürdigen Programmen oder Apps
- ▶ Phishing-Mails, USB-Sticks
- ▶ Standard-Konfigurationen
  - ▶ <https://www.shodan.io/search?query=webcamxp>
  - ▶ [Insecam - World biggest online cameras directory](#)



# Was macht ein Penetrationstester?

# Was ist ein Hacker?

Ein Hacker ist:

- ▶ Experimentierfreudiger Technologie-Enthusiast
- ▶ Expertise in einem bestimmten Themenfeld, welche er nutzt um Geräte/Apps usw. außerhalb des eigentlichen Verwendungszwecks einzusetzen



**White-Hat**

- ▶ Halten sich an Vorschriften, Gesetze und die "Hackerethik"
- ▶ "Ethical Hackers"



**Grey-Hat**

- ▶ Halten sich nicht immer an Gesetze
- ▶ Haben oft ein höheres Ziel
- ▶ Können nicht klar in "Gut" oder "Böse" eingeteilt werden



**Black-Hat**

- ▶ Kriminelle Personen / Gruppen
- ▶ Ziel: Schaden anrichten, Datendiebstahl, Erpressung ...



# Gesetzeslage

## Hackerparagraph §202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

## §202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

## §202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

## Reaktion des Rechtsausschusses des Deutschen Bundestages 2007

Hinweis, dass gutwillige Umgang mit Hackertools durch IT-Sicherheitsexperten nicht vom § 202c StGB erfasst werde.



# Offensive Security

Schwachstellen finden, bevor andere es tun



## Realistische Angriffssimulation

Wir versetzen uns in die Perspektive realer Angreifer und analysieren die Sicherheitsmaßnahmen von Systemen und Netzwerken.



## Gezielte Schwachstellenanalyse

Wir identifizieren und bewerten Sicherheitslücken in diversen Anwendungen, Systemen und Netzwerken.



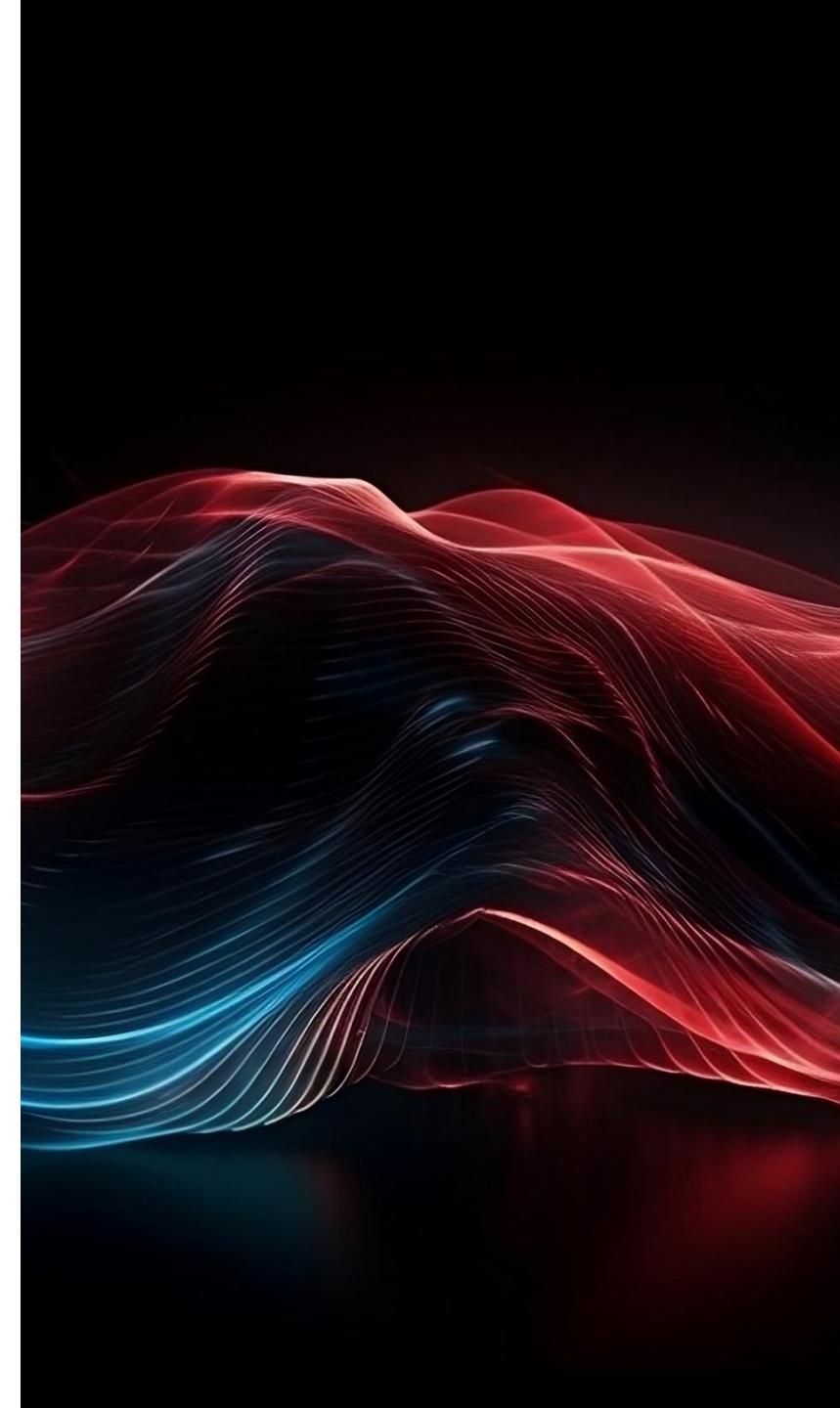
## Ermittlung nachhaltiger Maßnahmen

Im Anschluss an die Analyse unterstützen wir bei der Ermittlung geeigneter Maßnahmen. Auf Wunsch führen wir eine Re-Evaluierung der Systeme durch, um die Wirksamkeit der Maßnahmen zu bestätigen.



## Umfassende Beratung

Wir unterstützen bei allen Fragestellungen rund um das Thema Cybersicherheit auf technischer Ebene - von der Konzeption über die Entwicklung bis zum Betrieb.



# Vorgehen im Penetrationstest

## 5-Phasen Modell des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

# Phase 1 - Vorbereitung

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
<ul style="list-style-type: none"><li>• Ziele, Umfang und Vorgehen festlegen</li><li>• Testumgebung, Testvoraussetzungen definieren</li><li>• Rechtliche bzw. organisatorische Aspekte klären</li><li>• Risiken und erforderliche Notfallmaßnahmen abstimmen</li></ul>	<ul style="list-style-type: none"><li>• Übersicht über installierte Systeme und Anwendungen</li><li>• Recherche benötigter Informationen</li><li>• Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel</li></ul>	<ul style="list-style-type: none"><li>• Analyse und Bewertung der gesammelten Informationen</li><li>• Priorisierung und Auswahl der relevanten Testmodule</li><li>• Auswahl von Testfällen</li></ul>	<ul style="list-style-type: none"><li>• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme</li><li>• Verifikation und Dokumentation der identifizierten Schwachstellen</li></ul>	<ul style="list-style-type: none"><li>• Erstellung der Abschlussdokumentation</li><li>• Bewertung der Ergebnisse</li><li>• Darstellung der Risiken</li><li>• Definition von Maßnahmen</li></ul>

## Phase 2 - Informationsbeschaffung

Vorbereitung	Informations- beschaffung	Bewertung der Informationen	Aktive Eindring- versuche	Abschlussanalyse und Clean-Up
<ul style="list-style-type: none"><li>• Ziele, Umfang und Vorgehen festlegen</li><li>• Testumgebung, Testvoraussetzungen definieren</li><li>• Rechtliche bzw. organisatorische Aspekte klären</li><li>• Risiken und erforderliche Notfallmaßnahmen abstimmen</li></ul>	<ul style="list-style-type: none"><li>• Übersicht über installierte Systeme und Anwendungen</li><li>• Recherche benötigter Informationen</li><li>• Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel</li></ul>	<ul style="list-style-type: none"><li>• Analyse und Bewertung der gesammelten Informationen</li><li>• Priorisierung und Auswahl der relevanten Testmodule</li><li>• Auswahl von Testfällen</li></ul>	<ul style="list-style-type: none"><li>• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme</li><li>• Verifikation und Dokumentation der identifizierten Schwachstellen</li></ul>	<ul style="list-style-type: none"><li>• Erstellung der Abschlussdokumentation</li><li>• Bewertung der Ergebnisse</li><li>• Darstellung der Risiken</li><li>• Definition von Maßnahmen</li></ul>

# Phase 3 - Bewertung der Informationen

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
<ul style="list-style-type: none"><li>• Ziele, Umfang und Vorgehen festlegen</li><li>• Testumgebung, Testvoraussetzungen definieren</li><li>• Rechtliche bzw. organisatorische Aspekte klären</li><li>• Risiken und erforderliche Notfallmaßnahmen abstimmen</li></ul>	<ul style="list-style-type: none"><li>• Übersicht über installierte Systeme und Anwendungen</li><li>• Recherche benötigter Informationen</li><li>• Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel</li></ul>	<ul style="list-style-type: none"><li>• Analyse und Bewertung der gesammelten Informationen</li><li>• Priorisierung und Auswahl der relevanten Testmodule</li><li>• Auswahl von Testfällen</li></ul>	<ul style="list-style-type: none"><li>• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme</li><li>• Verifikation und Dokumentation der identifizierten Schwachstellen</li></ul>	<ul style="list-style-type: none"><li>• Erstellung der Abschlussdokumentation</li><li>• Bewertung der Ergebnisse</li><li>• Darstellung der Risiken</li><li>• Definition von Maßnahmen</li></ul>

## Phase 4 - Aktive Eindringversuche

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
<ul style="list-style-type: none"><li>• Ziele, Umfang und Vorgehen festlegen</li><li>• Testumgebung, Testvoraussetzungen definieren</li><li>• Rechtliche bzw. organisatorische Aspekte klären</li><li>• Risiken und erforderliche Notfallmaßnahmen abstimmen</li></ul>	<ul style="list-style-type: none"><li>• Übersicht über installierte Systeme und Anwendungen</li><li>• Recherche benötigter Informationen</li><li>• Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel</li></ul>	<ul style="list-style-type: none"><li>• Analyse und Bewertung der gesammelten Informationen</li><li>• Priorisierung und Auswahl der relevanten Testmodule</li><li>• Auswahl von Testfällen</li></ul>	<ul style="list-style-type: none"><li>• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme</li><li>• Verifikation und Dokumentation der identifizierten Schwachstellen</li></ul>	<ul style="list-style-type: none"><li>• Erstellung der Abschlussdokumentation</li><li>• Bewertung der Ergebnisse</li><li>• Darstellung der Risiken</li><li>• Definition von Maßnahmen</li></ul>

# Phase 5 - Abschlussanalyse und Clean-Up

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
<ul style="list-style-type: none"><li>• Ziele, Umfang und Vorgehen festlegen</li><li>• Testumgebung, Testvoraussetzungen definieren</li><li>• Rechtliche bzw. organisatorische Aspekte klären</li><li>• Risiken und erforderliche Notfallmaßnahmen abstimmen</li></ul>	<ul style="list-style-type: none"><li>• Übersicht über installierte Systeme und Anwendungen</li><li>• Recherche benötigter Informationen</li><li>• Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel</li></ul>	<ul style="list-style-type: none"><li>• Analyse und Bewertung der gesammelten Informationen</li><li>• Priorisierung und Auswahl der relevanten Testmodule</li><li>• Auswahl von Testfällen</li></ul>	<ul style="list-style-type: none"><li>• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme</li><li>• Verifikation und Dokumentation der identifizierten Schwachstellen</li></ul>	<ul style="list-style-type: none"><li>• Erstellung der Abschlussdokumentation</li><li>• Bewertung der Ergebnisse</li><li>• Darstellung der Risiken</li><li>• Definition von Maßnahmen</li></ul>

# Vorgehen im Penetrationstest - Phase 1

## Scope definieren



## Phase 1 - Scope definieren

- ▶ Angreiferperspektive
- ▶ Testabdeckung
- ▶ Teststart
- ▶ Testtiefe
- ▶ Testschwerpunkte und Testfälle



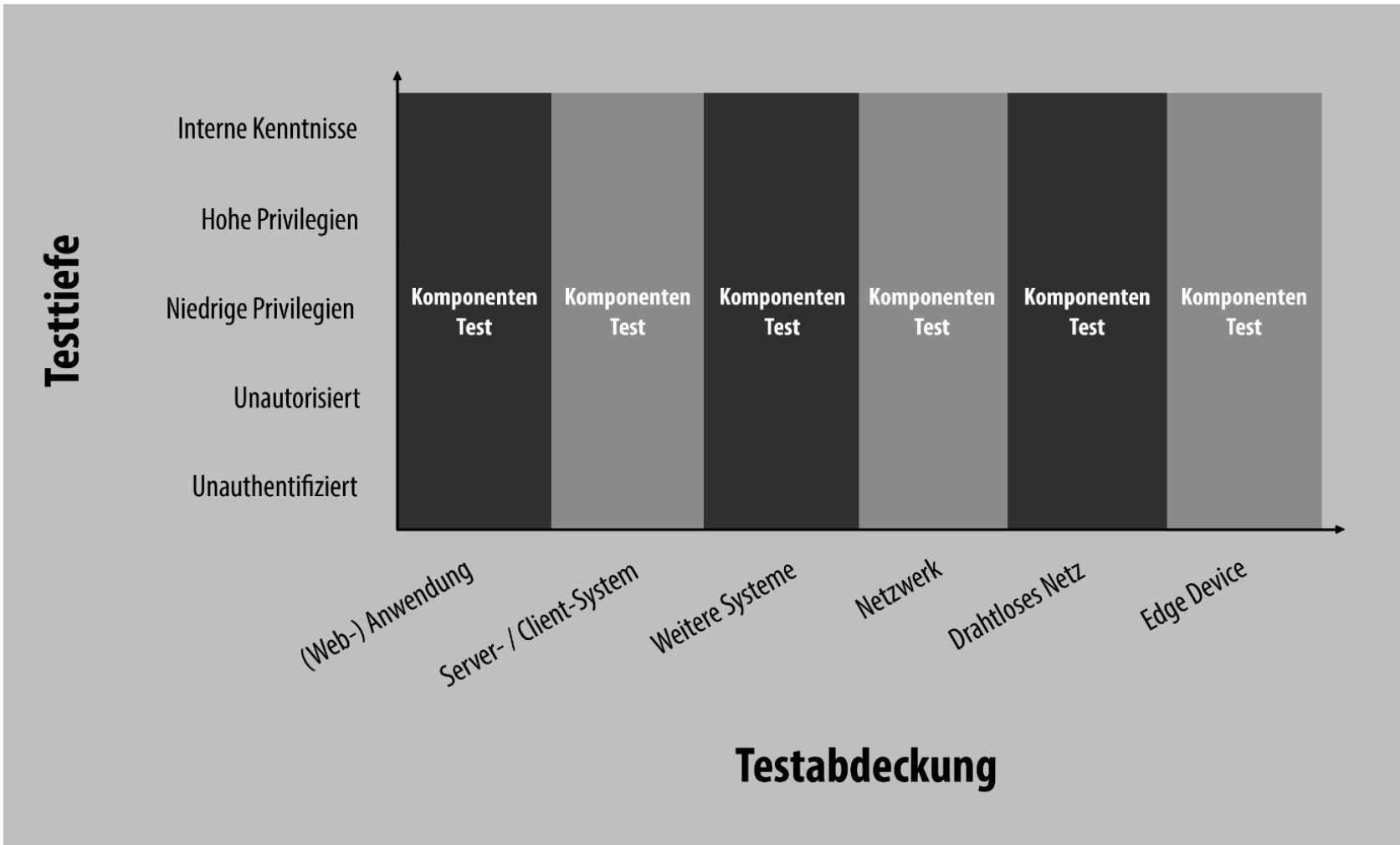
## Angreiferperspektive

Klärung der Frage: Gegen welche Art Angreifer soll das System geschützt werden?

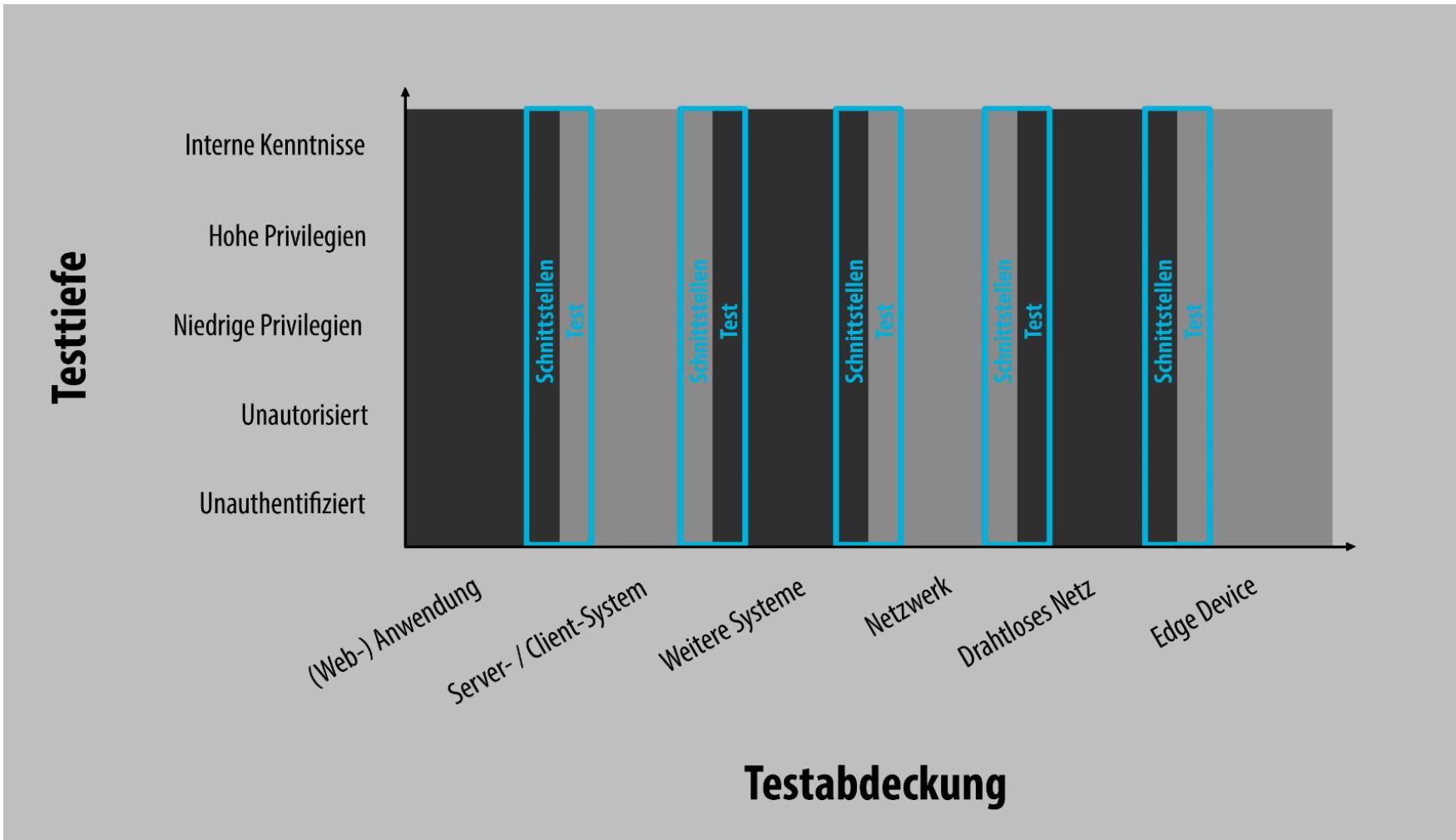
► Beispiele:

- ▶ externer, nicht privilegierter Angreifer (z.B. jemand mit Zugang zum Gerät aber ohne Zugriff auf Gerätefunktionen)
- ▶ externer, privilegierter Angreifer (z.B. Käufer, Endnutzer)
- ▶ interner, nicht privilegierter Angreifer (z.B. Gastzugang)
- ▶ interner, niedrig privilegierter Angreifer (z.B. Mitarbeiter)
- ▶ interner, hoch privilegierter Angreifer (z.B. Administrator)

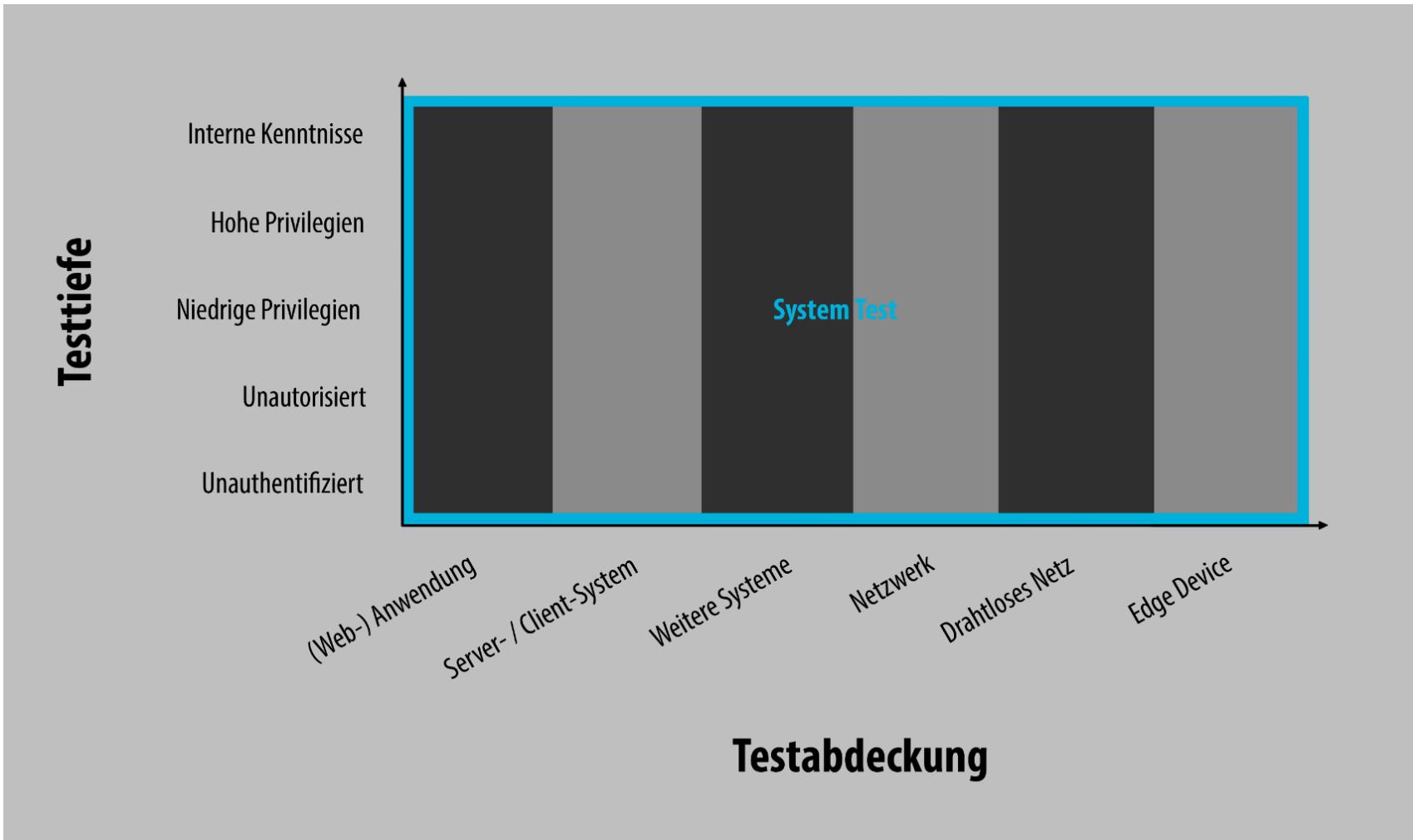
# Testabdeckung - Komponententest



# Testabdeckung - Schnittstellentest



# Testabdeckung - Ende-zu-Ende Test

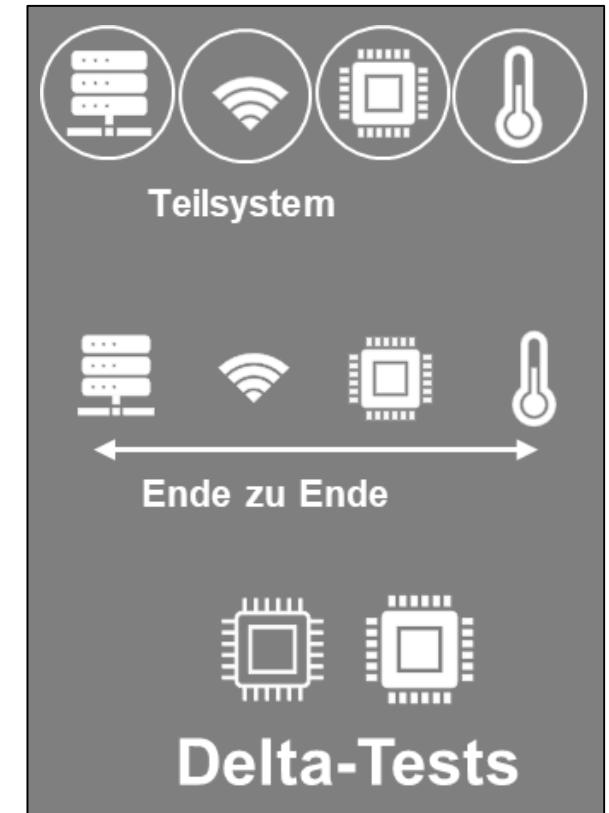




# Testabdeckung

## Vergleich

- ▶ Komponententest z.B. wichtig bei verschiedenen Zulieferern; Betrachtung aber nicht ganzheitlich
- ▶ Schnittstellentest überprüft Daten zwischen den (Software-)Komponenten
- ▶ Ende-zu-Ende Test betrachtet das System ganzheitlich; aufwendiger und kostenintensiver
- ▶ Delta-Tests (Vergleich zwischen zwei verschiedenen Systemversionen) eignen sich bei weniger großen Updates



# Testart

## Schwachstellen-Scan

### Fast vollständig automatisiert

- ▶ Mittels Portscanner und Schwachstellenscanner werden definierte IP-Adressen bzw. Anwendungen gescannt
- ▶ Ziel: bekannte Schwachstellen identifizieren (Profile und Pattern)
- ▶ Sollte manuell nachqualifiziert werden, um mögliche False-Positive-Ergebnisse zu filtern
- ▶ Guter Überblick über das Sicherheitsniveau, da typische Schwachstellen schnell identifiziert werden können

## Penetrationstest

### Hoher manueller Anteil

- ▶ Zielgerichteter Versuch, mit den Mitteln eines Angreifers innerhalb einer gegebenen Zeitspanne Lücken in der Sicherheit aufzudecken
- ▶ Realitätsnaher Ansatz, verwendet die gleichen Methoden und Werkzeuge wie ein realer Angreifer
- ▶ Agiert nur innerhalb vorgegebener, mit dem Kunden abgestimmter Grenzen
- ▶ Prüfpunkte: systematisches Vorgehen im Test, standardisierte Testfälle

## Source Code Analyse

### Untersuchung von Quellcode

- ▶ Dient der Verbesserung und Qualitätssicherung von Applikationen
- ▶ Automatische Analyse zur Überprüfung von Programmcode hinsichtlich besonderer Auffälligkeiten oder Verstößen gegen geltende Programmierrichtlinien
- ▶ Bedingung ist die Lieferung des kompilierbaren, vollständigen Quellcodes, inklusive aller verwendeten Frameworks und Bibliotheken sowie Konfigurationsdateien



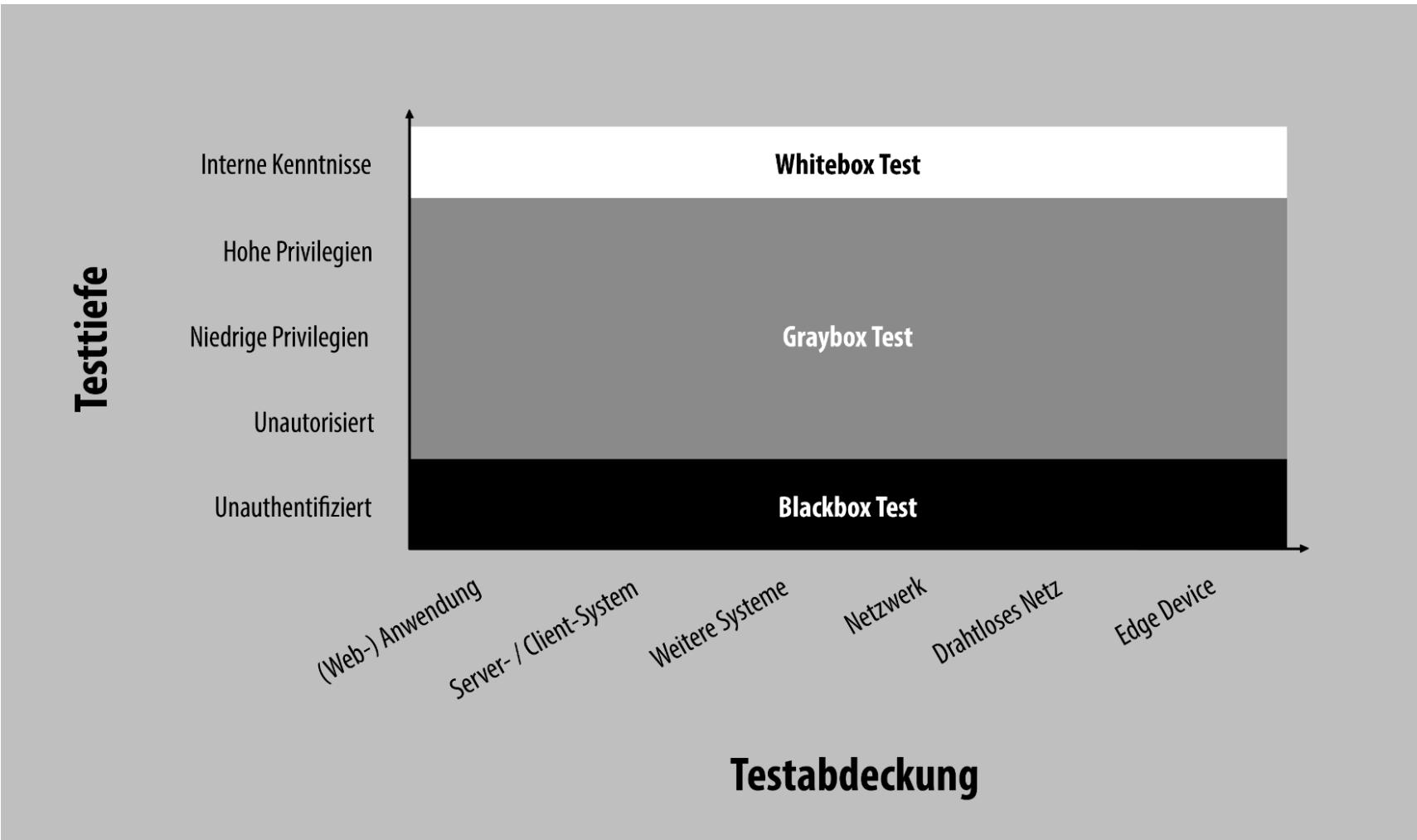
# Testtiefe

Festlegung, wie detailliert das Testobjekt untersucht werden soll

► Beispiele:

- ▶ Blackbox (wenige bis gar keine Informationen über den inneren Aufbau des Systems vorhanden, unauthentifiziert, unautorisiert)
- ▶ Greybox (Mischform, z.B. wenige Informationen über den inneren Aufbau des Systems vorhanden, es liegen aber Anmeldedaten für Authentifizierung und Autorisierung vor)
- ▶ Whitebox (Details über den inneren Aufbau des Systems sind bekannt, der Tester hat Zugriff auf alle Einzelkomponenten)
- ▶ explorativ oder time-boxed (der Tester entscheidet während des Tests, welche Einzelkomponenten in welcher Detailtiefe betrachtet werden)

# Testtiefe



# Testschwerpunkte und Testfälle

Testschwerpunkte = Aspekte und Prüfpunkte, die während des Tests betrachtet werden

- ▶ Schritt 1: Komponenten im Scope definieren
- ▶ Schritt 2: Prüfpunkte definieren

Analysen erfolgen basierend auf etablierten Frameworks:

- ▶ OWASP Web Security Testing Guide ([WSTG](#))
- ▶ OWASP Mobile Application Security Testing Guide ([MASTG](#))
- ▶ OWASP IoT Security Testing Guide ([ISTG](#)) sowie Testfallkatalog für Hardwaregeräte, welcher von der BDO Cyber Security GmbH entwickelt und gepflegt wird
- ▶ Testfallkatalog für IT-Infrastrukturen und Infrastrukturkomponenten, welcher von der BDO Cyber Security GmbH entwickelt und gepflegt wird
- ▶ [CIS Benchmarks](#) für Security Audits / Hardening Checks



# Testschwerpunkte und Testfälle

## Testschwerpunkte Webanwendung

- ▶ Informationsgewinnung, z.B.:
  - ▶ Identifizierung des Webservers
  - ▶ Prüfung der Webserver-Metadaten auf Informationspreisgabe
  - ▶ Testen des Konfigurations- und Deployment-Managements, z.B.:
    - ▶ Test der Plattformkonfiguration
    - ▶ Überprüfung alter Backups und nicht referenzierter Dateien auf sensible Informationen
- ▶ Prüfung des Identitätsmanagements, z.B.:
  - ▶ Test von Rollendefinitionen
  - ▶ Test der Registrierungsfunktion
  - ▶ Prüfung, ob sich Account-Namen ermitteln lassen
- ▶ Test der Authentifizierung, z.B.:
  - ▶ Prüfung auf Standard-Anmeldeinformationen
  - ▶ Prüfung auf Umgehung des Authentifizierungsschemas
  - ▶ Testen auf schwache Funktionen zum Ändern oder Zurücksetzen von Passwörtern
  - ▶ Testen der Multi-Faktor-Authentifizierung



# Testschwerpunkte und Testfälle

## Testschwerpunkte Webanwendung

- ▶ Test der Autorisierung, z.B.:
  - ▶ Testen von Directory Traversal File Include
  - ▶ Testen auf Umgehung des Autorisierungsschemas
  - ▶ Testen auf Eskalation von Privilegien
  - ▶ Testen auf Insecure Direct Object References
- ▶ Testen des Session-Managements, z.B.:
  - ▶ Testen auf Cross-Site Request Forgery
  - ▶ Testen von JSON Web Tokens
- ▶ Prüfung der Eingabevalidierung, z.B.:
  - ▶ Testen auf reflektiertes Cross-Site Scripting
  - ▶ Testen auf gespeichertes Cross-Site Scripting
  - ▶ Testen auf SQL-Injektion
  - ▶ Testen auf Code-Injektion
  - ▶ Testen auf Befehlsinjektion



# Testschwerpunkte und Testfälle

## Testschwerpunkte Webanwendung

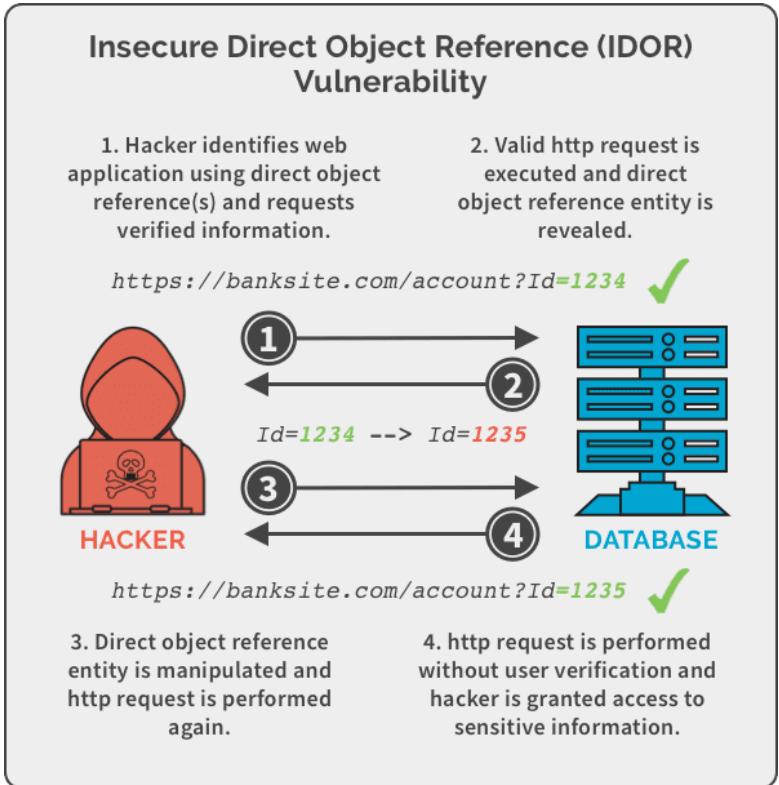
- ▶ Testen des Fehlerhandlings, z.B.:
  - ▶ Testen auf unsachgemäße Fehlerbehandlung
  - ▶ Testen auf Stack Traces
- ▶ Test der eingesetzten Kryptographie, z.B.:
  - ▶ Testen auf schwache Transportverschlüsselung
  - ▶ Prüfung auf sensible Informationen, die über unverschlüsselte Kanäle gesendet werden
- ▶ Testen der Anwendungslogik, z.B.:
  - ▶ Testen, wie oft eine Funktion maximal verwendet werden kann
  - ▶ Test auf die Umgehung von Arbeitsabläufen
  - ▶ Test des Uploads bösartiger Dateien
- ▶ Client-seitige Tests, z.B.:
  - ▶ Testen auf HTML-Injektion
  - ▶ Test auf Cross-Origin Resource Sharing



# Testschwerpunkte und Testfälle

## Testfall - Authorization Testing

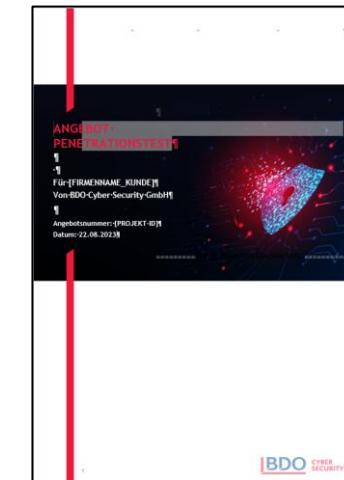
- ▶ [WSTG - Authorization Testing](#)
- ▶ [Testing for Insecure Direct Object References](#)
- ▶ [Insecure Direct Object Reference Prevention - OWASP Cheat Sheet Series](#)





## Das Angebot

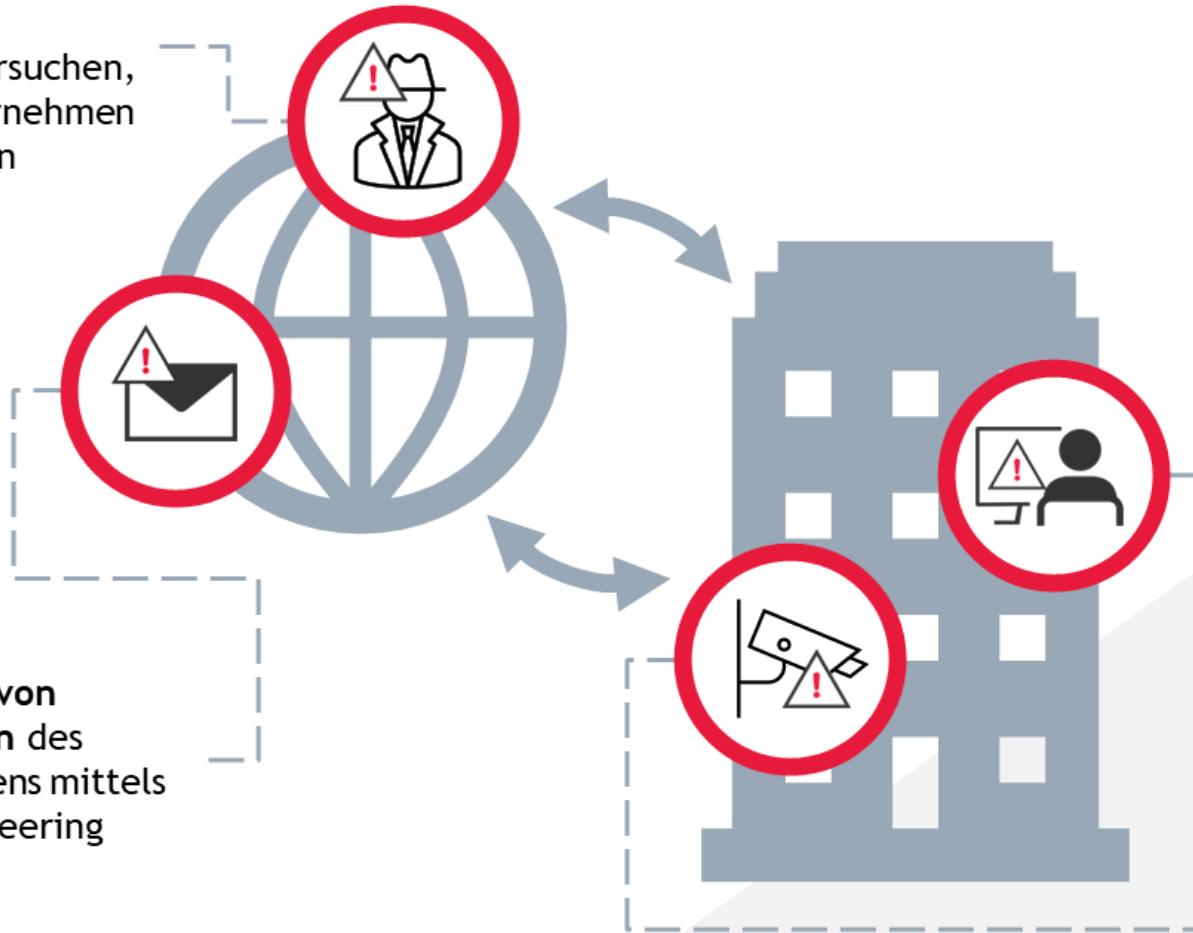
- ▶ Ergebnisse der Phase 1 werden in einem Vertrag dokumentiert, der als Rechtsgrundlage für die Beauftragung des Penetrationstests dient
- ▶ Geregelt werden u.a.:
  - ▶ Testobjekt und Testumfang (Scope und Out-of-Scope)
  - ▶ Allgemeine Teststrategie (Informationsbasis, Aggressivität, Vorgehensweise, Ausgangspunkt)
  - ▶ Mitwirkungspflichten des Kunden (z.B. Testzugänge, Testaccounts)
  - ▶ Planung der Testdurchführung, Testzeitraum
  - ▶ Ort der Durchführung



# Vorgehen im Penetrationstest - Phase 2-4

# Vorgehen im Penetrationstest

Angreifer, die über  
im Internet  
exponierte  
Systeme versuchen,  
in das Unternehmen  
einzudringen



Angriffe aus dem  
internen  
Netzwerk durch  
kompromittierte  
Geräte oder  
Innenräte

Täuschung von  
Mitarbeitern des  
Unternehmens mittels  
Social Engineering

Angriffe am  
Unternehmens-  
standort, z.B.  
über öffentliche  
Bereiche

# Angriffe aus dem Internet



Systeme, welche Daten aus externen Quellen empfangen und verarbeiten, sind potenzielle Einstiegspunkte für Angreifer.

Dazu zählen unter anderem:

- ▶ Internetauftritte und Unternehmensportale
- ▶ Cloud-Umgebungen
- ▶ Perimeter-Systeme (z.B. Firewalls, VPN-Gateways, Mailserver, Webserver)
- ▶ Arbeitsplatzsysteme und Mobiltelefone von Mitarbeitern (bspw. via Phishing)



# Beispiele

## Angriffe aus dem Internet - Externer Perimeter

### Ein Fallbeispiel aus der Vergangenheit:

- ▶ Ransomware-Angriff auf das Logistikunternehmen Maersk (2017)
  - ▶ Nahezu das gesamte Unternehmensnetzwerk wurde übernommen
  - ▶ Gesamte interne Kommunikation war gestört
  - ▶ Backups nicht vollständig (Netzwerk-Setup fehlte)
  - ▶ Wiederherstellung nur durch einen Standort möglich, der zur Zeit des Angriffes einen Stromausfall hatte

### Unternehmen mit aktuellen Angriffsvektoren:

- ▶ Kamera in einer [Produktionsanlage in Japan](#)
- ▶ Über das Remote Desktop Protocol (RDP) erreichbare Systeme:
  - ▶ [Norwegischer Energieversorger](#)
  - ▶ [Klinik in Pinneberg](#)
  - ▶ [Fabrik in Bangladesch](#)



# Angriffe am Unternehmensstandort



Der Unternehmensstandort selbst bietet Angreifern oft eine breite Angriffsfläche, sowohl im Gebäude als auch davor:

- ▶ Drahtlosnetzwerke und -geräte (z.B. Wi-Fi, Bluetooth)
- ▶ IoT-Netzwerke (z.B. LoRaWAN, ZigBee)
- ▶ Besucherterminals und Automaten
- ▶ Netzwerkanschlüsse in (semi-)öffentlichen Bereichen (z.B. Lobby, Cafeteria, Parkhaus, Konferenzraum)
- ▶ Ungesicherte Gebäudezugänge und Sicherheitsbereiche
- ▶ Ungesperrte Arbeitsplatzsysteme



# Angriffe aus dem internen Netzwerk



Angreifer können über verschiedene Wege in das interne Netzwerk eindringen - bspw. über das Internet, durch Überwindung von Sicherheitsmaßnahmen vor Ort oder die Kompromittierung von Mitarbeiteraccounts.

Von diesem Ausgangspunkt bieten sich verschiedene Möglichkeiten weiter ins Unternehmensnetzwerk vorzudringen:

- ▶ Weitere Anwendungen und Systeme im internen Netz
- ▶ Applikations-, Datenbank- und Dateiserver
- ▶ Produktionsanlagen und Steuerungen



# Beispiele

## Angriffe am Unternehmensstandort

### Ein Fallbeispiel aus der Vergangenheit:

- ▶ Manipulation von Bankaccounts durch einen internen Angreifer
  - ▶ Zugriff von einem ungeschützten internen PC sowie über das Unternehmens-VPN mittels validen Accounts
  - ▶ Nutzung einer Software-Schwachstelle zum Diebstahl von Sitzungs-Cookies
  - ▶ Manipulation der Privilegien von anderen Accounts

### Weitere Angriffsvektoren:

- ▶ Manipulierte USB-Geräte
- ▶ Zugekaufte Geräte mit Schwachstellen (z. B. Bluetooth Thermostat)



# Vorgehen im Penetrationstest - Phase 5

## Abschlussanalyse und Clean-Up



## Der Testbericht

- ▶ Alle in den vorangegangenen Phasen erzielten Ergebnisse werden in einem detaillierten Bericht zusammengefasst:
  - ▶ Eine Zusammenfassung des Testansatzes und der Testergebnisse, einschließlich einer allgemeinen Bewertung des Gesamtsicherheitsniveaus des Testobjekts
  - ▶ Eine detaillierte Beschreibung jeder entdeckten Schwachstelle, einschließlich eines Proof-of-Concept und Screenshots
  - ▶ Eine Bewertung jeder Schwachstelle hinsichtlich ihres Schweregrads
  - ▶ Allgemeine Empfehlungen für Gegenmaßnahmen zur Behebung oder Mitigation der festgestellten Schwachstellen





## Bewertung von Findings

- ▶ Bewertung: nach CVSS 3.1 (Base Score):  
<https://www.first.org/cvss/v3.1/specification-document>
- ▶ Der Wertebereich des CVSS Base Scores reicht von 0,0 bis 10,0 und gibt den Schweregrad einer Schwachstelle wie folgt an: 0.0 (Schweregrad „Hinweis“), 0.1 - 3.9 (Schweregrad „Niedrig“), 4.0 - 6.9 (Schweregrad „Mittel“), 7.0 - 8.9 (Schweregrad „Hoch“), 9.0 - 10.0 (Schweregrad „Kritisch“)
- ▶ Online Calculator: <https://www.first.org/cvss/calculator/3.1>
- ▶ Beispiel: Score: 7,6 (High)

Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low	High		
Privileges Required	None	Low	High	
User Interaction	None	Required		
Scope	Unchanged	Changed		
Confidentiality	None	Low	High	
Integrity	None	Low	High	
Availability	None	Low	High	

# Weiterführende Informationen

# Testwerkzeuge

- ▶ je nach zu untersuchendem Testobjekt kann Spezial-Soft- / Hardware benötigt werden
- ▶ Beispiele:
  - ▶ Kali Linux als Betriebssystem
  - ▶ Web Applikationen:
    - ▶ BurpSuite (BURP), Swagger
  - ▶ Infrastruktur:
    - ▶ nmap, Wireshark, Metasploit, John the Ripper
  - ▶ IoT:
    - ▶ Hardware wie Labornetzgeräte, Oszilloskope, Signalgenerator, eine HF-abschirmende Umgebung, SDR, Lötstation
    - ▶ verschiedene protokollspezifische Dongles und Adapter (z. B. für Bluetooth, Wi-Fi, ZigBee, RFID, NFC, CAN usw.)
- ▶ ...



# Nützliche Links

## Ausbildung

- ▶ eLearnSecurity - Junior Penetration Tester (eJPT): <https://elearnsecurity.com/product/ejpt-certification/>
- ▶ HackTheBox: <https://academy.hackthebox.com>
- ▶ TryHackMe: <https://tryhackme.com/>
- ▶ LetsDefend: <https://letsdefend.io/>
- ▶ TCM Security Academy: <https://academy.tcm-sec.com/>

## Hacking Labs

- ▶ HackTheBox: <https://www.hackthebox.eu/>
- ▶ OWASP Juice Shop: <https://github.com/bkimminich/juice-shop>
- ▶ PortSwigger Academy: <https://portswigger.net/web-security>
- ▶ VulnLab: <https://www.vulnlab.com/>

## Konferenzen

- ▶ DEFCON: <https://media.defcon.org/>
- ▶ OffenseCon: <https://www.offensivecon.org>
- ▶ Blackhat: [https://www.blackhat.com/...](https://www.blackhat.com/)





# Portfolio BDO Cyber Security

# Unsere Services

Unseren Expertinnen und Experten unterstützen Sie bei allen Themengebieten der Cyber Resilienz.

## Security Management

Cyber-Resilienz denken, entwickeln und steuern

- ▶ Informationssicherheitsmanagement
- ▶ Cyber Strategy und Governance
- ▶ Business Continuity Management
- ▶ Reifegradanalysen
- ▶ Security-Audits

## Offensive Services

Angreifern immer einen Schritt voraus sein

- ▶ Pентest von Anwendungen, (OT-) Infrastrukturen, Cloud Umgebungen und IoT-Geräten
- ▶ Red Teaming
- ▶ Krisensimulationen
- ▶ Threat Analysis and Risk Assessment (TARA)
- ▶ Phishing Kampagnen

## Defensive Services

Werte schützen, Krisen meistern

- ▶ Cyber Crisis Center für Incident Response und Notfallmanagement
- ▶ Digitale Forensik
- ▶ Security Operation Center
- ▶ Sicherheitskonzeption und Secure Design
- ▶ Trainings



# Warum ist der Beruf so spannend?

- ▶ Sehr vielfältige Themen und Projekte
  - ▶ Verschiedene „Perspektiven“, z.B. über das Internet von außen oder als „Innentäter“
  - ▶ Verschiedene Themen und Technologien (Webseiten, IT/OT-Systeme, Hardware, ...)
  - ▶ kein Test ist wie der andere, kein Testobjekt wie das andere
- ▶ Verschiedene Branchen (z.B. Automotive und Health Care)
- ▶ Nie langweilig, ständig neues lernen
- ▶ Kombination aus Kundenkontakt mit Beratung, Test (allein oder im Team), Recherche und Programmierung/Toolentwicklung
- ▶ Was muss ich mitbringen?
  - ▶ Interesse am Thema Hacking und IT
  - ▶ Experimentierfreude und Spieltrieb
    - ▶ Dinge außerhalb des eigentlichen Verwendungszwecks nutzen
    - ▶ Grenzen austesten
    - ▶ Um die Ecke denken, Dinge kombinieren



## Ihre Ansprechpartnerinnen und Ansprechpartner



**Dr. Antje Winkler**

Division Lead

Offensive Security

+49 351 26352-157

[antje.winkler@bdosecurity.de](mailto:antje.winkler@bdosecurity.de)



**Luca Pascal Rotsch**

Manager

Offensive Security

+49 351 26352-154

[lucapascal.rotsch@bdosecurity.de](mailto:lucapascal.rotsch@bdosecurity.de)



[www.bdosecurity.de](http://www.bdosecurity.de)

