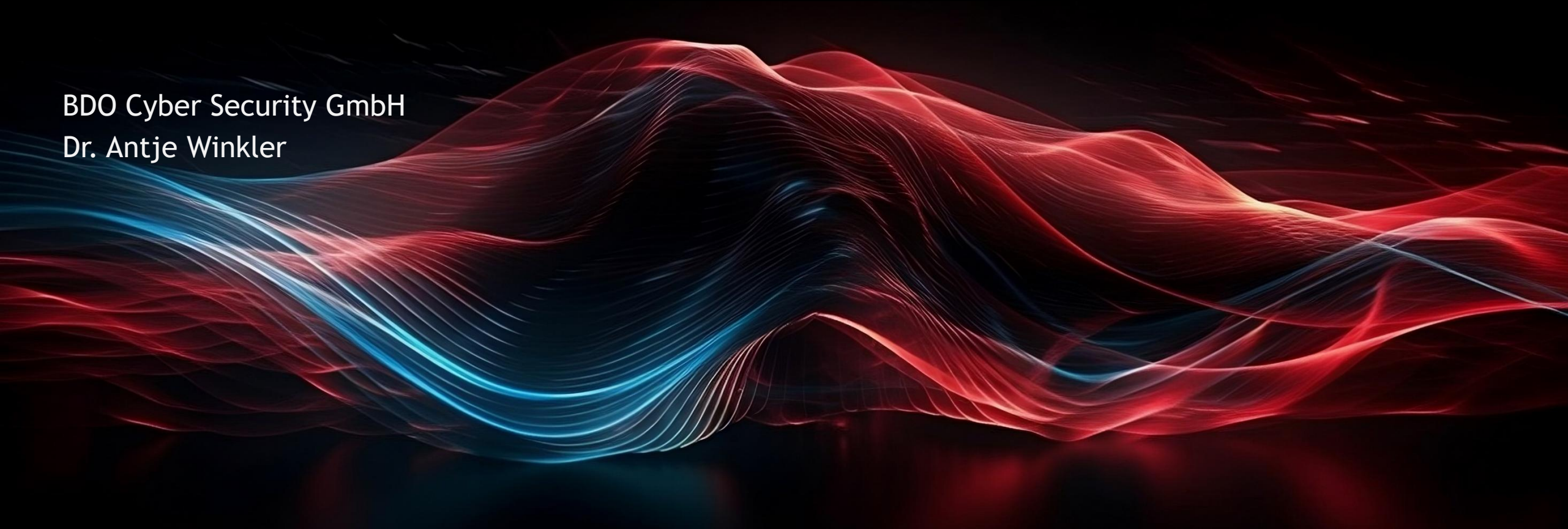


Penetrationstest

Vom Hacking zum rechtmäßigen Sicherheitstest

BDO Cyber Security GmbH
Dr. Antje Winkler

The background of the slide features a large, abstract graphic of flowing, wavy lines in shades of red and blue. These lines create a sense of movement and depth, resembling a digital landscape or a network flow. The colors transition from a deep red on the right to a bright blue on the left, with white highlights that give the lines a three-dimensional appearance.

Motivation - Warum Penetrationstests gebraucht werden

Cyberangriffe in Zahlen

Statistiken zeigen einen beunruhigenden Trend



9 von 10 Unternehmen in Deutschland wurden im Jahr 2025 mindestens einmal Opfer von Diebstahl, Industriespionage oder Sabotage
(2024: 4 von 5 Unternehmen)

289 Mrd. €

289 Mrd. € Gesamtschaden deutscher Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage (2025)
(2024: 266 Mrd. €)

202 Mrd. €

202 Mrd. € (70 %) des Gesamtschadens kann auf Cyberattacken zurückgeführt werden
(2024: 178 Mrd. € / 67 %)



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



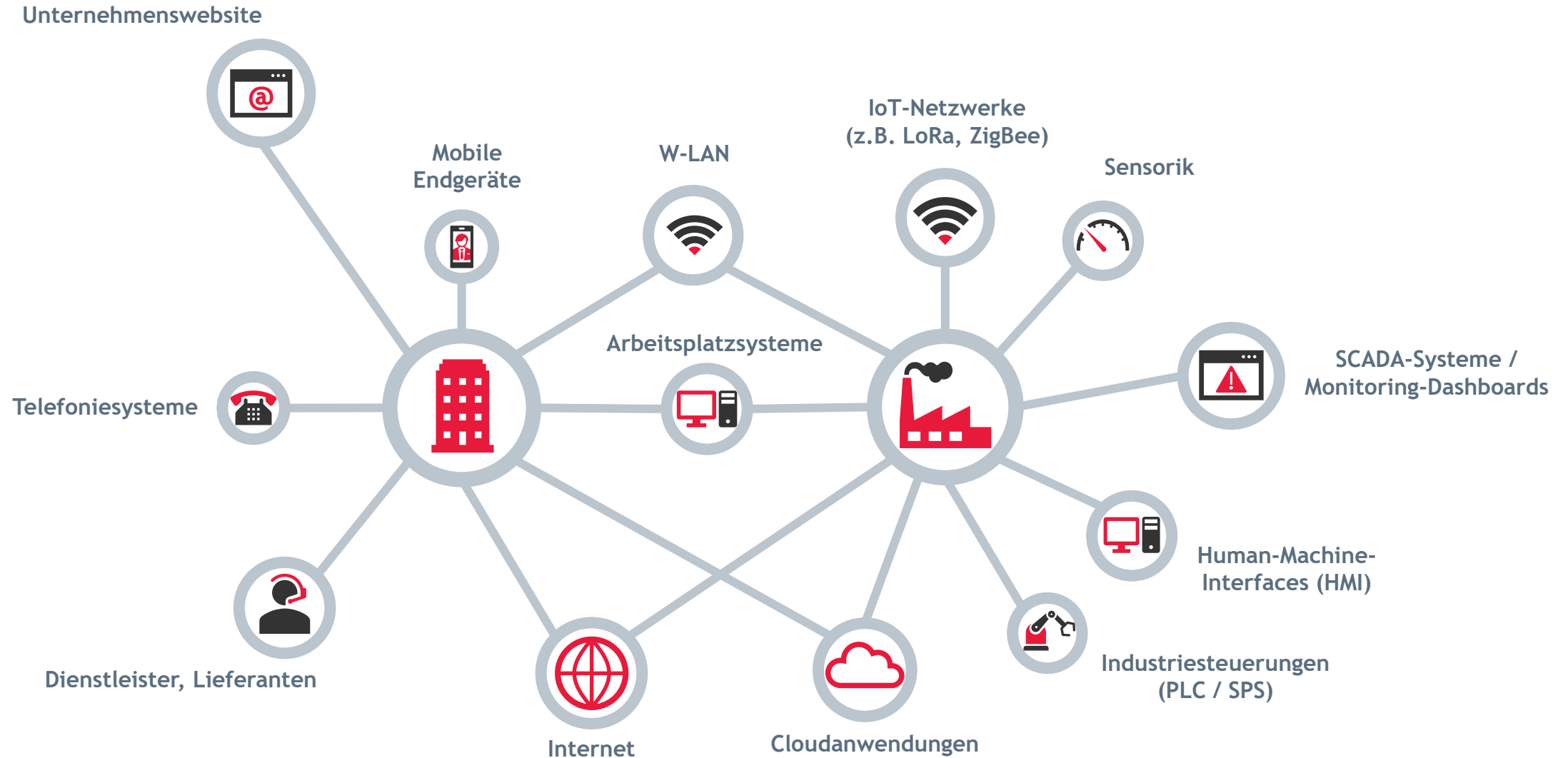
59 % der Unternehmen fühlen sich durch Cyberangriffe in ihrer Existenz bedroht
(2024: 65 %)



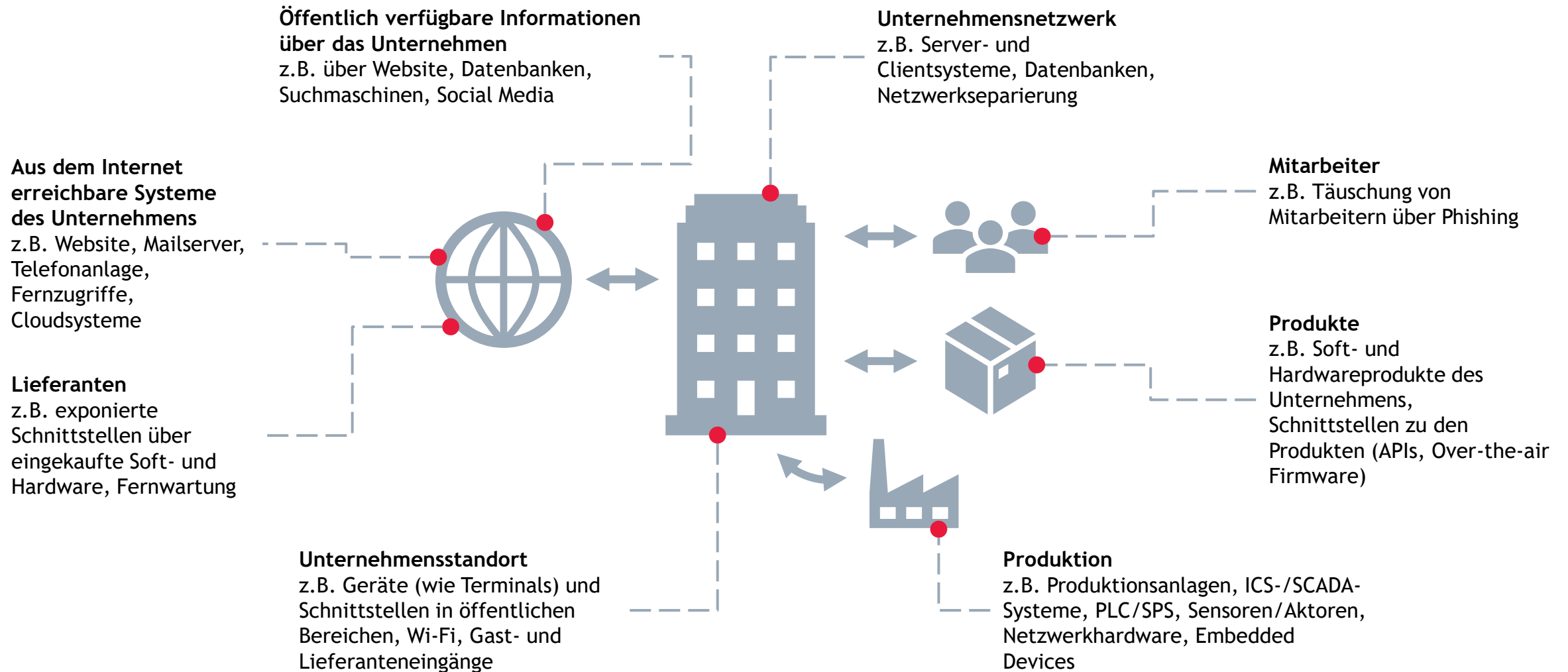
Richtlinien und Vorgaben durch den Gesetzgeber

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

Zunehmende Vernetzung - Erhöhung der Komplexität



Angriffsfläche von Unternehmen



Aktuelle Bedrohungen

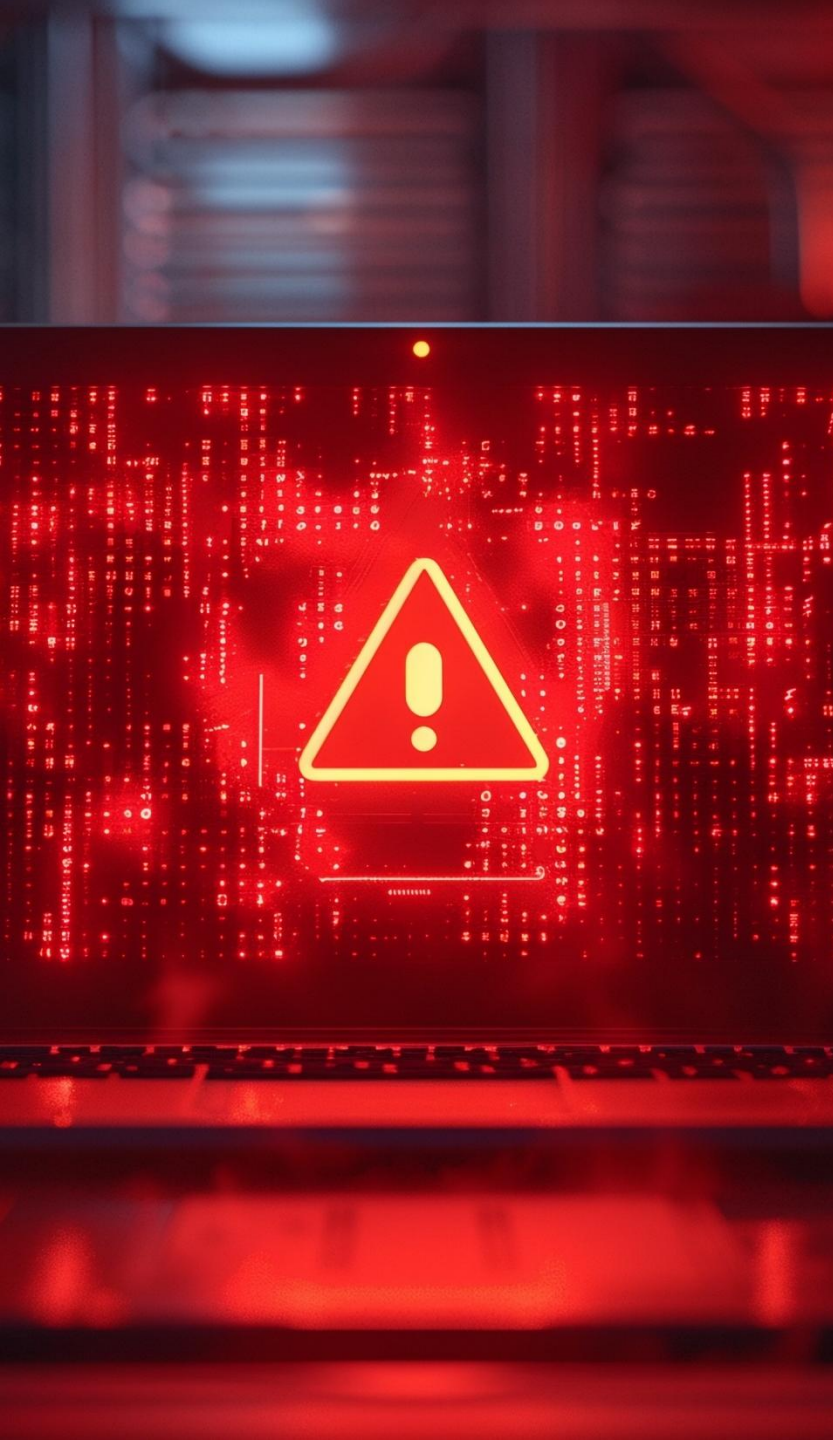
Häufigste Bedrohungsszenarien

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 zugekaufte 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:
 - ▶ hallo
 - ▶ 1234567890
 - ▶ 1234567
 - ▶ password
 - ▶ password1
 - ▶ target123
 - ▶ iloveyou
 - ▶ gwert123
- ▶ Teilen von sensiblen privaten Informationen im Internet / sozialen Netzwerken
- ▶ Installation / Herunterladen von fragwürdigen Programmen oder Apps
- ▶ Phishing-Mails, USB-Sticks
- ▶ Standard-Konfigurationen
 - ▶ Shodan
 - ▶ Insecam - World biggest online cameras directory



Hacking vs. Penetrationstest

Hacker - Begriff und Motivation

Einteilung nach Motivation und Legalität

Typ	Motivation	Rechtliche Einordnung
White Hat	Sicherheitslücken im Auftrag finden und schließen	Erlaubt, mit Einwilligung des Systeminhabers
Grey Hat	Handelt ohne Auftrag, oft mit guter Absicht	Rechtliche Grauzone, meist strafbar
Black Hat	Cyberkriminelle, Spammer, Erpresser	Strafbar
APT-Gruppen	Langfristige Spionage und Sabotage	Strafbar, oft staatlich motiviert
Script Kiddies	Nutzen fertige Tools ohne eigenes Verständnis	Häufig strafbar, schnell entdeckt



Hacking in Deutschland

Gesetzeslage

Grundsatz: Verboten

- ▶ § 202a StGB: Ausspähen von Daten, insbesondere Überwindung einer Zugangssicherung
- ▶ § 202b StGB: Abfangen von Daten bei nichtöffentlicher Übermittlung
- ▶ § 202c StGB: Vorbereitung, etwa durch Herstellen oder Verbreiten von Tools oder Zugangscodes, mit Zweckbestimmung für eine Straftat
- ▶ §§ 303a und 303b StGB: Datenveränderung und Computersabotage

Die Rechtsgrundlage des Penetrationstests

- ▶ Einwilligung des Systeminhabers, nachweisbar dokumentiert
- ▶ Schriftlicher Auftrag mit Scope, Zeitraum, Testmethoden und Ansprechpartnern
- ▶ Freigabe durch Verantwortliche (z. B. IT-Leitung, Geschäftsführung)
- ▶ Befugnis prüfen, wenn Dienstleister, Hosting oder Cloud-Anbieter betroffen sind
- ▶ Bei personenbezogenen Daten: Datenschutz klären (DSGVO, ggf. Auftragsverarbeitung)
- ▶ Bei Mitarbeiter-Tests (z. B. Phishing): Betriebsrat einbinden



Hacking vs. Penetrationstest

Vergleich

Kriterium	Hacking (ohne Auftrag)	Penetrationstest (im Auftrag)
Rechtsgrundlage	Keine; Strafbarkeit möglich	Einwilligung des Systeminhabers, Vertrag
Ziel	Schaden, Datenabfluss, eigener Vorteil	Risiken erkennen und Maßnahmen ableiten
Umfang	Selbst gewählt	Vorab festgelegt (Scope und Out-of-Scope)
Methoden und Werkzeuge	Teilweise identisch	Identisch, aber kontrolliert
Umgang mit Funden	Ausnutzen, verschleiern	Verifizieren, dokumentieren, melden
Ergebnis	Kein Nutzen für den Eigentümer	Bericht mit Bewertung und Empfehlungen
Abbruch	Nicht vorgesehen	Stopp-Kriterien und Notfallkontakt



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
• Ziele, Umfang und Vorgehen festlegen • Testumgebung, Testvoraussetzungen definieren • Rechtliche bzw. organisatorische Aspekte klären • Risiken und erforderliche Notfallmaßnahmen abstimmen	• Übersicht über installierte Systeme und Anwendungen • Recherche benötigter Informationen • Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel	• Analyse und Bewertung der gesammelten Informationen • Priorisierung und Auswahl der relevanten Testmodule • Auswahl von Testfällen	• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme • Verifikation und Dokumentation der identifizierten Schwachstellen	• Erstellung der Abschlussdokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Phase 2 - Informationsbeschaffung

Vorbereitung	Informations- beschaffung	Bewertung der Informationen	Aktive Eindring- versuche	Abschlussanalyse und Clean-Up
• Ziele, Umfang und Vorgehen festlegen • Testumgebung, Testvoraussetzungen definieren • Rechtliche bzw. organisatorische Aspekte klären • Risiken und erforderliche Notfallmaßnahmen abstimmen	• Übersicht über installierte Systeme und Anwendungen • Recherche benötigter Informationen • Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel	• Analyse und Bewertung der gesammelten Informationen • Priorisierung und Auswahl der relevanten Testmodule • Auswahl von Testfällen	• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme • Verifikation und Dokumentation der identifizierten Schwachstellen	• Erstellung der Abschlussdokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Phase 3 - Bewertung der Informationen

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
• Ziele, Umfang und Vorgehen festlegen • Testumgebung, Testvoraussetzungen definieren • Rechtliche bzw. organisatorische Aspekte klären • Risiken und erforderliche Notfallmaßnahmen abstimmen	• Übersicht über installierte Systeme und Anwendungen • Recherche benötigter Informationen • Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel	• Analyse und Bewertung der gesammelten Informationen • Priorisierung und Auswahl der relevanten Testmodule • Auswahl von Testfällen	• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme • Verifikation und Dokumentation der identifizierten Schwachstellen	• Erstellung der Abschlussdokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Phase 4 - Aktive Eindringversuche

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
• Ziele, Umfang und Vorgehen festlegen • Testumgebung, Testvoraussetzungen definieren • Rechtliche bzw. organisatorische Aspekte klären • Risiken und erforderliche Notfallmaßnahmen abstimmen	• Übersicht über installierte Systeme und Anwendungen • Recherche benötigter Informationen • Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel	• Analyse und Bewertung der gesammelten Informationen • Priorisierung und Auswahl der relevanten Testmodule • Auswahl von Testfällen	• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme • Verifikation und Dokumentation der identifizierten Schwachstellen	• Erstellung der Abschlussdokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Phase 5 - Abschlussanalyse und Clean-Up

Vorbereitung	Informationsbeschaffung	Bewertung der Informationen	Aktive Eindringversuche	Abschlussanalyse und Clean-Up
• Ziele, Umfang und Vorgehen festlegen • Testumgebung, Testvoraussetzungen definieren • Rechtliche bzw. organisatorische Aspekte klären • Risiken und erforderliche Notfallmaßnahmen abstimmen	• Übersicht über installierte Systeme und Anwendungen • Recherche benötigter Informationen • Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel	• Analyse und Bewertung der gesammelten Informationen • Priorisierung und Auswahl der relevanten Testmodule • Auswahl von Testfällen	• Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme • Verifikation und Dokumentation der identifizierten Schwachstellen	• Erstellung der Abschlussdokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Vorgehen im Penetrationstest - Phase 1

Scope definieren



Phase 1 - Scope definieren

- ▶ Angreiferperspektive
- ▶ Testtiefe
- ▶ Testabdeckung
- ▶ Teststart



Angreiferperspektive

Gegen welche Art Angreifer soll das System geschützt werden?

Angreifer	Zugang	Privilegien
Anonymer Angreifer	Extern, ohne Zugang	Keine
Endnutzer oder Kunde	Extern	Standardrechte
Gast im Gebäude	Physisch vor Ort	Minimal
Mitarbeitende	Intern	Normale Benutzerrechte
Administrator	Intern	Erhöhte Rechte
Entwickler oder Architekt	Intern	Kenntnis des Systems

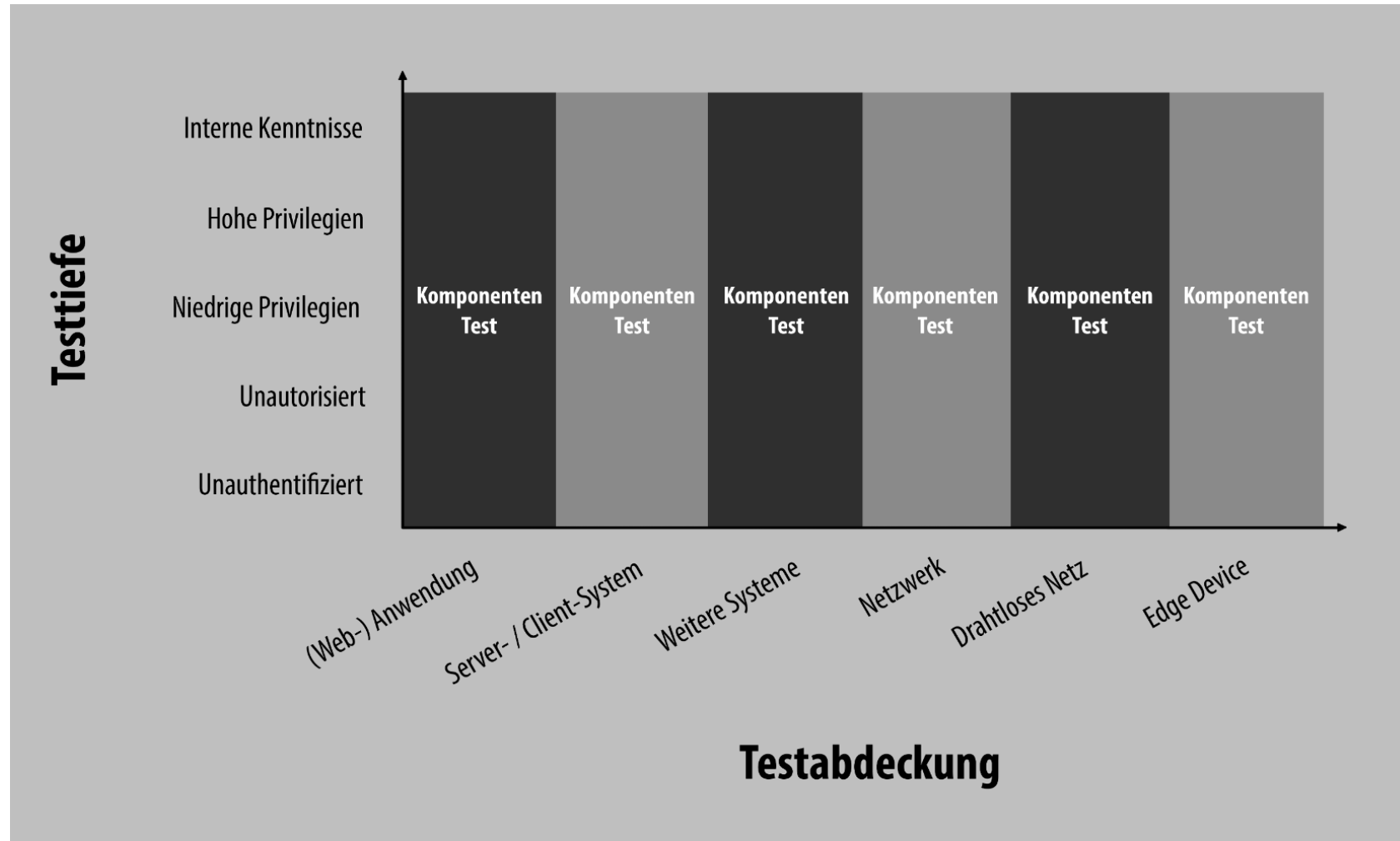


Testtiefe

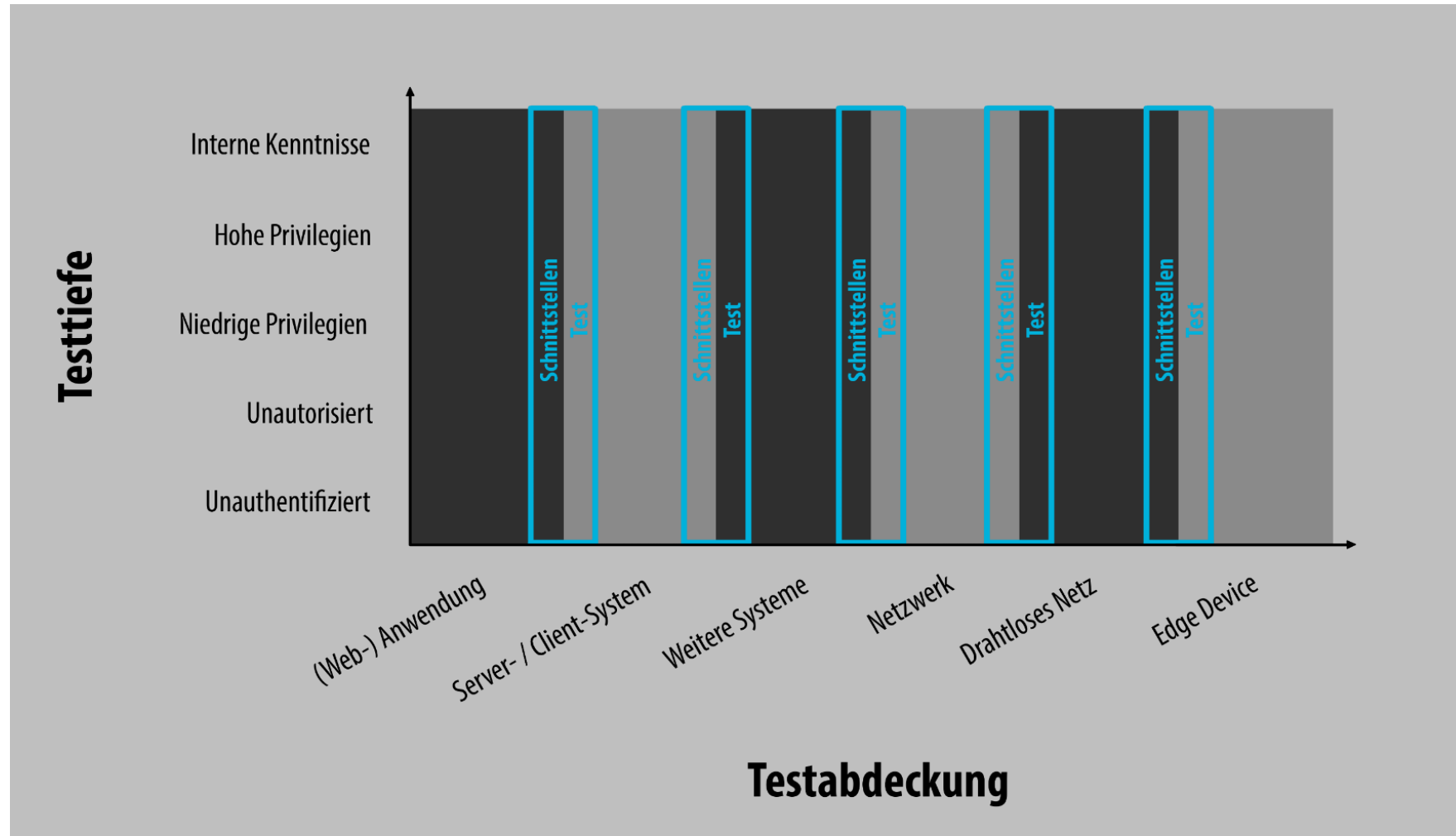
Festlegung, wie detailliert das Testobjekt untersucht werden soll?

Variante	Vorwissen des Testers	Typischer Einsatz
Black-Box	Keines, unauthentifiziert	Realistische Außensicht auf Internetdienste
Grey-Box	Teilweise, z. B. Testkonten	Anwendungen mit Login und Rollen
White-Box	Vollständig, z. B. Quellcode	Tiefe Prüfung, Architektur und Code
Explorativ / time-boxed	Tester entscheidet während des Tests	Begrenzte Zeit, flexibles Vorgehen

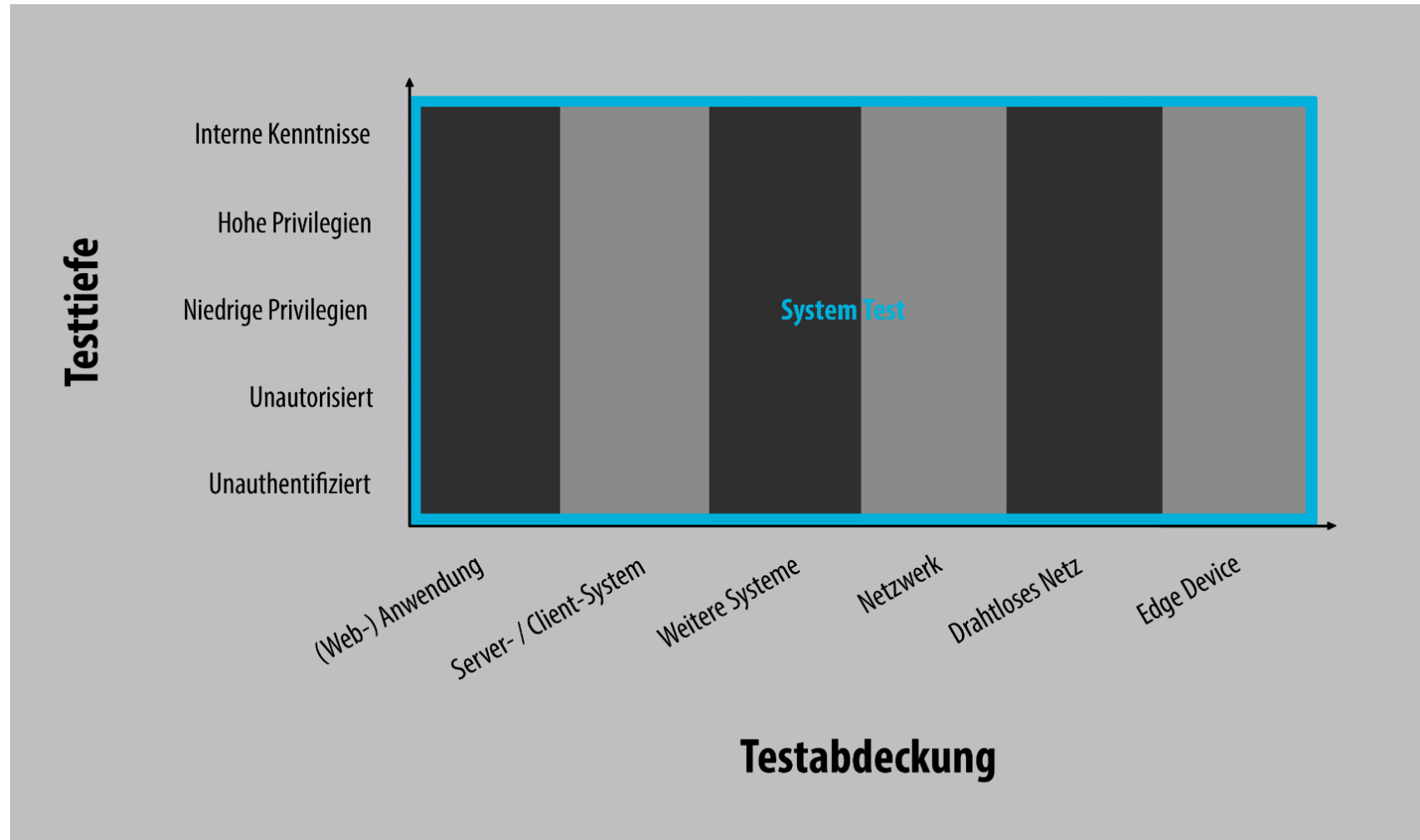
Testabdeckung - Komponententest



Testabdeckung - Schnittstellentest



Testabdeckung - Ende-zu-Ende Test





Testabdeckung

Vergleich

Ansatz	Gegenstand	Stärke	Schwäche
Komponententest	Einzelne Komponente oder Funktion	Früh möglich, gezielt	Wechselwirkungen fehlen
Schnittstellentest	APIs und Datenübergaben	Hohe Relevanz durch Vernetzung	Workflows müssen nachgebaut werden
Ende-zu-Ende-Test	Gesamtsystem	Realitätsnah	Aufwendig, zeitintensiv
Delta-Test	Änderung zwischen zwei Versionen	Schnell, kosteneffizient	Auswirkungen können übersehen werden

Testart

Vergleich

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

Vorgehen im Penetrationstest - Phase 2-4

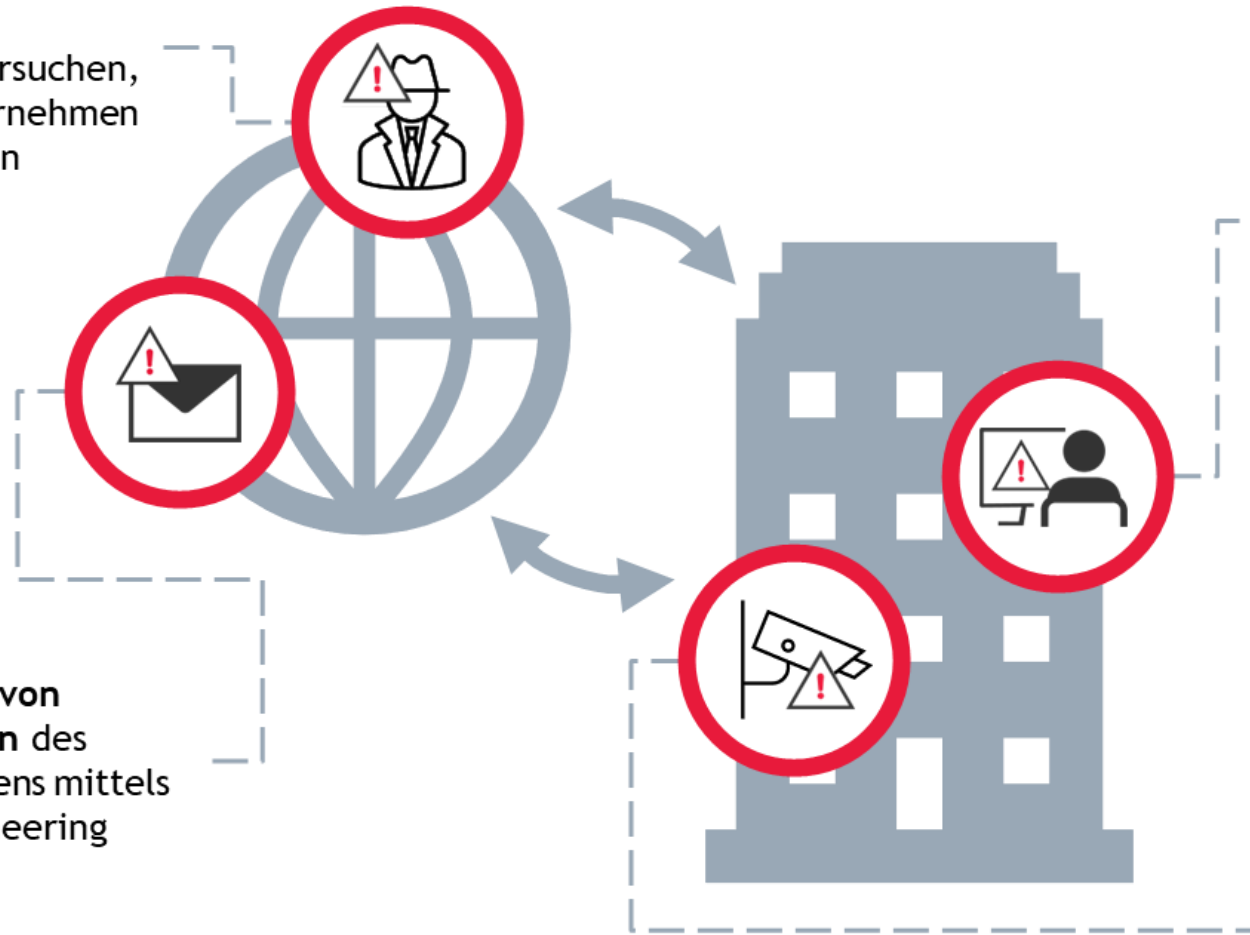
Perspektiven im Penetrationstest

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

**Täuschung von
Mitarbeitern** des
Unternehmens mittels
Social Engineering

Angriffe aus dem
**internen
Netzwerk** durch
kompromittierte
Geräte oder
Innentäter

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



Angriffe aus dem Internet

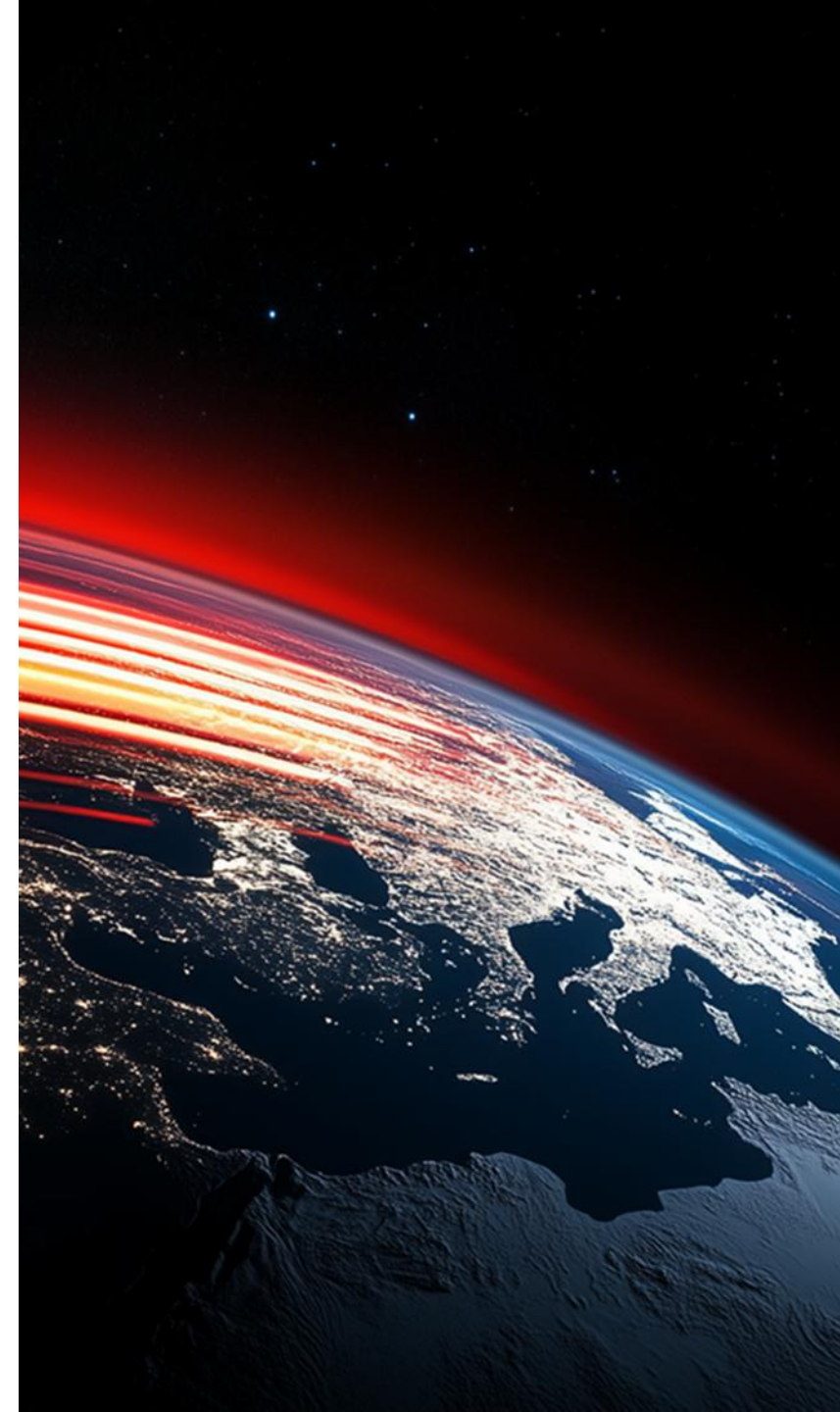
Bedrohungen aus aller Welt



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

Dazu zählen unter anderem:

- ▶ Internetauftritte und Onlineportale
- ▶ 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

Suchmaschinen

- ▶ Beispiele für Suchanfragen (Exploit-DB): <https://www.exploit-db.com/google-hacking-database>
 - ▶ Directory Listing
 - ▶ vertrauliche Dokumente
 - ▶ Private Key

Shodan:

- ▶ <https://www.shodan.io> → Verschiedene im Internet exponierte Dienste
- ▶ <https://github.com/jakejarvis/awesome-shodan-queries>
- ▶ Über das Remote Desktop Protocol (RDP) erreichbare Systeme:
 - ▶ Hospital has screenshot:true
 - ▶ Norwegischer Energieversorger
- ▶ Und vieles mehr...



Angriffe vor Ort

Angriffsfläche des Unternehmensstandorts



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

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



Angriffe aus dem internen Netzwerk

Ausbreitung innerhalb des Unternehmens



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
- ▶ PCs von höher privilegierten Mitarbeitern
- ▶ Applikations-, Datenbank- und Dateiserver
- ▶ Systeme für die Gebäudeautomatisierung



Beispiel

Angriffe am Unternehmensstandort

Ein Fallbeispiel aus der Vergangenheit:

- ▶ Manipulation von Bankaccounts durch einen internen Angreifer

Weitere Angriffsvektoren:

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



Testfälle

Strukturiertes Testvorgehen

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

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

OWASP-Testschwerpunkte Web (Auswahl)

Bereich	Beispiele für Prüfpunkte	Warum relevant
Authentifizierung	Standardzugänge, Passwort-Reset, Multi-Faktor	Zugang zu fremden Konten
Autorisierung	Umgehung von Rollen, unsichere Objektreferenzen	Zugriff auf fremde Daten
Eingabevalidierung	SQL-Injektion, Befehlsinjektion, Cross-Site-Scripting	Ausführung fremder Befehle
Session-Management	Token-Handhabung, Cross-Site Request Forgery	Übernahme von Sitzungen
Konfiguration	Verzeichnislisting, alte Backups, Fehlermeldungen	Preisgabe interner Informationen

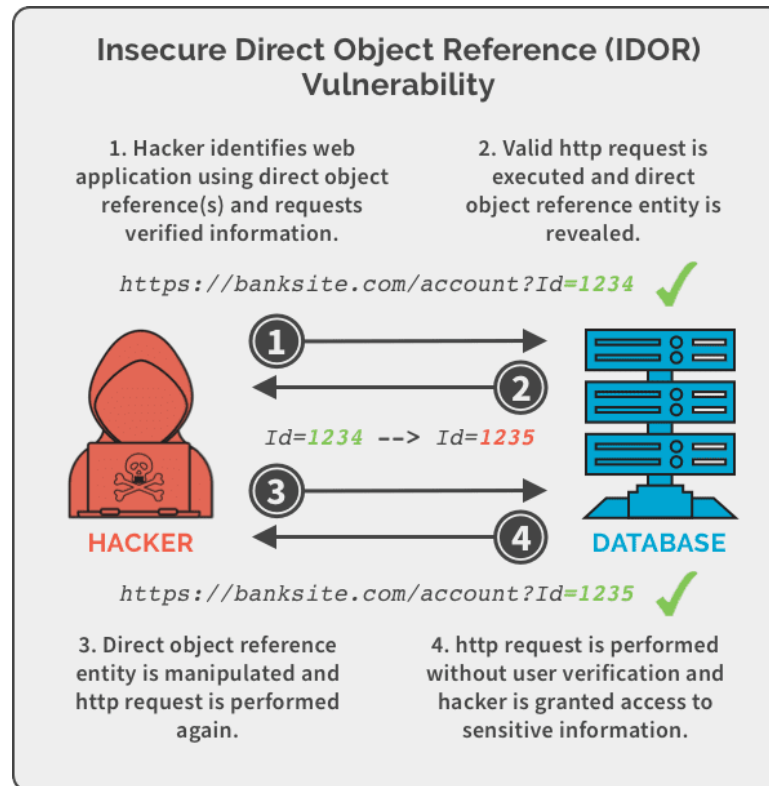


Testschwerpunkte und Testfälle

OWASP-Testschwerpunkte Web (Auswahl)

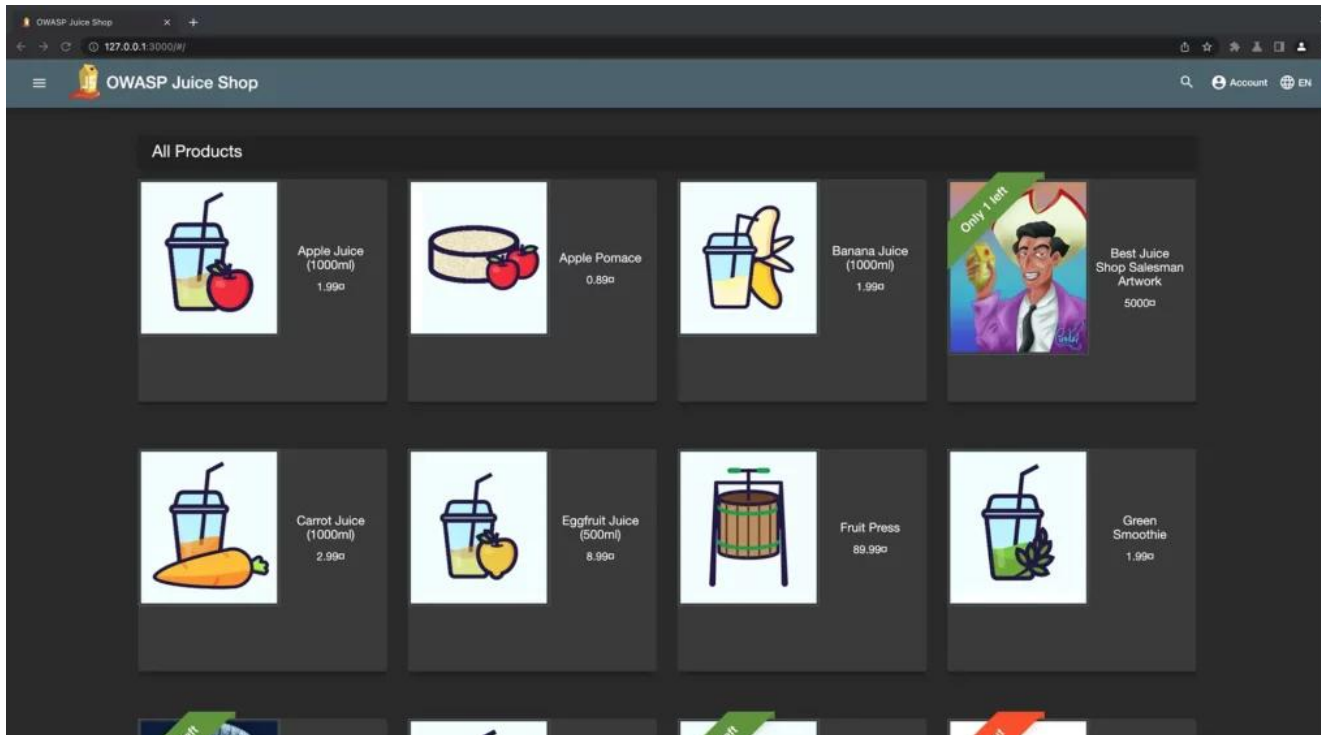
Testfall - Authorization Testing

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



Beispiel

Testing for Insecure Direct Object References



[OWASP Juice Shop - Insecure Web Application for Security Training | OWASP Foundation](https://owasp.org/www-project-juice-shop/)



Besondere Vorsicht beim Testen

Bitte beachten

Stopp-Kriterien: Wann ein Test abgebrochen wird:

- ▶ Betriebsstörungen oder ungewöhnliches Systemverhalten
- ▶ Zugriff auf personenbezogene Daten, die nicht zum Testumfang gehören
- ▶ Zufallsfund außerhalb des Scopes
- ▶ Vorgehen: Test stoppen, Ereignis dokumentieren, Notfallkontakt informieren

Social Engineering im Penetrationstest:

- ▶ Durchführung nur mit ausdrücklicher Freigabe und klaren Regeln
- ▶ Auswertung anonymisiert, keine Bloßstellung einzelner Personen
- ▶ Betriebsrat und Datenschutz vorab einbinden

OT und Produktion:

- ▶ Tests nur in Testumgebungen oder nach ausdrücklicher Freigabe und Abstimmung
- ▶ Passive Analyse vor aktiven Scans, kein Denial-of-Service
- ▶ Stopp-Kriterien und Notfallpläne sind vor Testbeginn festzulegen
- ▶ Ältere Systeme lassen sich oft nicht patchen; Fehlfunktionen können Anlagen und Menschen gefährden



Vorgehen im Penetrationstest - Phase 5

Abschlussanalyse und Clean-Up



Der Testbericht

Ergebnisse verständlich machen

Kernbotschaft: Der Bericht dokumentiert alle Ergebnisse nachvollziehbar und zeigt Entscheidungsträgern, wie dringend und wie einfach die Probleme zu beheben sind.

Inhalt des Berichts:

- ▶ Zusammenfassung des Testansatzes und der Ergebnisse
- ▶ Gesamtbewertung des Sicherheitsniveaus des Testobjekts
- ▶ Detailbeschreibung jeder Schwachstelle mit Proof of Concept und Screenshots, inkl. Bewertung nach Schweregrad
- ▶ Allgemeine Empfehlungen zu Behebung und Mitigation

Hinweise:

- ▶ Flughöhe: Kurz, verständlich und nicht zu technisch formulieren.
- ▶ Einstieg: Gesamtbewertung mit einem Überblick über das Sicherheitsniveau beginnen und positive Aspekte hervorheben
- ▶ Business-Sicht: Wichtigste Probleme und ihre Auswirkungen auf Geschäftsprozesse, Daten und Reputation zusammenfassen
- ▶ Schwärzung: Sensible Daten in Screenshots und Proof of Concept vor der Weitergabe unkenntlich machen



Der Testbericht

Aufbau eines guten Findings

Element	Inhalt
Titel	Kurz und eindeutig, z. B. „Fehlende Zugriffsprüfung auf Kundendatensätze“
Befund	Was wurde festgestellt, und warum ist es ein Problem? Hinweise: ▶ Formulierung und Flughöhe: Findings verständlich und zielgruppengerecht beschreiben. ▶ Folgende Fragen beantworten: ▶ WER (authentifizierter/unauthentifizierter Nutzer, Rolle, Tennant, ...) hat ▶ WO (Systemname, URL, IP, ...) ▶ WAS und WIE (Angriffsvektor, Vorgehen, beobachtetes Verhalten, ...) gemacht? ▶ Was hat das für AUSWIRKUNGEN?
Nachweis	Minimaler, reproduzierbarer Nachweis; keine Datenabzüge
Auswirkung	Betroffene Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit
Bewertung	Schweregrad nach CVSS, ergänzt um Kontext
Empfehlung	Konkrete Maßnahme, Priorität und Verantwortliche



Der Testbericht

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

Ein kleiner Überblick

- ▶ 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

Ein kleiner Überblick

Ausbildung

- ▶ [eLearnSecurity - Junior Penetration Tester \(eJPT\)](#)
- ▶ [HackTheBox](#)
- ▶ [TryHackMe](#)
- ▶ [LetsDefend](#)
- ▶ [TCM Security Academy](#)

Hacking Labs

- ▶ [HackTheBox](#)
- ▶ [OWASP Juice Shop](#)
- ▶ [PortSwigger Academy](#)

Konferenzen

- ▶ [DEFCON](#)
- ▶ [OffensiceCon](#)
- ▶ [Blackhat](#)
- ▶ ...



Ein kurzer Exkurs

Penetrationstest im Zeitalter von KI

Aktuelle Entwicklung

- ▶ Vom manuellen, stichtagsbezogenen Test zur kontinuierlichen, kontextgesteuerten Schwachstellenanalyse über alle Phasen der Angriffskette

Warum vollautonome KI-Penetrationstests (noch) scheitern

- ▶ Halluzinationen: Erfundene CVEs, Netzwerk-Timeouts werden als Exploit gewertet
- ▶ Kollateralschäden: Außerhalb des Scopes liegende Systeme oder produktive Datenbanken können beschädigt werden
- ▶ Kontext-Verlust: Bei langen, mehrstufigen Angriffen gehen Erkenntnisse verloren, Schleifen entstehen
- ▶ Datenschutz und OPSEC: Kundendaten, Quellcode oder Passwort-Hashes dürfen nicht in öffentliche Cloud-LLMs abfließen

Fazit

- ▶ Für Hacking bereits nutzbar und im Einsatz, für den kontrollierten Penetrationstest noch schwierig
- ▶ Human-in-the-Loop als Qualitätsgarant



Ein kurzer Exkurs

Penetrationstest im Zeitalter von KI

Human-in-the-Loop als Qualitätsgarant

- ▶ KI arbeitet das Grundrauschen bekannter Schwachstellen in Minuten ab
- ▶ Der Mensch konzentriert sich auf komplexe Kreativ- und Architekturaufgaben

Aufgaben des Testers

- ▶ Geschäftslogik: Mehrstufige Prozessfehler aufdecken, die Domänenwissen erfordern
- ▶ Validierung und Freigabe: KI-Findings auf echte Ausnutzbarkeit prüfen, kritische Exploits freigeben
- ▶ Physisches und Social Red Teaming: Technische Angriffe mit zwischenmenschlicher Manipulation kombinieren





Portfolio BDO Cyber Security

Cyber-Resilienz auf die Sie vertrauen können

Unternehmenswerte angemessen schützen und auf Notfälle vorbereitet sein



Cyber Strategieberatung

Cyber-Resilienz denken, entwickeln und steuern.

- ▶ Reifegradanalysen
- ▶ Cyber-Strategie und -Governance Beratung
- ▶ Informationssicherheitsmanagement (ISMS)
- ▶ Business Continuity Management (BCM)
- ▶ Security-Audits



Cyber Academy

Cyber-Kompetenz entwickeln, trainieren und festigen.

- ▶ Ganzheitliche Cyber-Security-Trainings
- ▶ Stärkung von Awareness & Resilienz
- ▶ Tabletop & Krisenübungen
- ▶ Showhacking
- ▶ Schulungen & BSI-Zertifizierungsvorbereitung



Offensive Security

Angreifen immer einen Schritt voraus sein.

- ▶ Penetration Testing
- ▶ OT Penetration Testing
- ▶ IoT & Embedded Penetration Testing
- ▶ Red Teaming
- ▶ Threat Analysis and Risk Assessment (TARA)



Defensive Security

Digitale Werte schützen und Notfälle meistern.

- ▶ Incident Response und
- ▶ Digitale Forensik
- ▶ Security Operation Center (German SOC)
- ▶ Notfallmanagement / Notfallübungen
- ▶ Secure Design / Hardening
- ▶ Cyber Academy

Unsere Offensive Security Services

Mit uns sind Sie Angreifern einen Schritt voraus

Consulting

IT-Lösungen sicher gestalten

- ▶ Erstellung von Sicherheitskonzepten sowie Management und Priorisierung von Sicherheitsanforderungen
- ▶ Konzeption sicherer Hardware- und Netzwerkarchitekturen
- ▶ Durchführung von Bedrohungs- und Risikoanalysen
- ▶ Prüfung und Bewertung der Konformität Ihrer Produkte und Netzwerke gegenüber aktuellen Standards und regulatorischen Vorgaben

[ZU UNSERER WEBSITE](#)

Penetration Testing

Sicherheitslücken finden, bevor es andere tun

- ▶ Aufdeckung von Schwachstellen in Unternehmensnetzwerken, Anwendungen, Systemen und Geräten aus der Perspektive realer Angreifer
- ▶ Bewertung des bestehenden Sicherheitsniveaus und Ableitung priorisierter, wirksamer Gegenmaßnahmen
- ▶ Modernes Testlabor für hardwarebezogene Sicherheitsprüfungen

[ZU UNSERER WEBSITE](#)

Red Teaming

Angriffssimulation unter realen Bedingungen

- ▶ Bewertung technischer und organisatorischer Aspekte der Cyberabwehr durch realistische Angriffsszenarien
- ▶ Aktive Einbindung des Krisenmanagements und der Cyberabwehr-Teams in Übungen
- ▶ Stärkung präventiver und reaktiver Cyberabwehrmaßnahmen durch gezielte Anpassungen

[ZU UNSERER WEBSITE](#)

Einstieg in den Beruf Penetrationstester

Was muss ich mitbringen?

Mindset

- ▶ Interesse an Hacking und IT-Sicherheit
- ▶ Experimentierfreude und Neugier: „Was passiert, wenn ...?“
- ▶ Querdenken und kreatives Kombinieren
- ▶ Technik auch außerhalb ihres Verwendungszwecks denken

Technische Basis

- ▶ Grundverständnis für Netzwerke, Betriebssysteme und Programmierung
- ▶ Sicherer Umgang mit Linux und Kommandozeile
- ▶ Bereitschaft zum Selbstlernen, da sich Technik und Angriffsmethoden schnell ändern
- ▶ Sorgfältige Dokumentation als Kernkompetenz

Soft Skills

- ▶ Kommunikationsfähigkeit für Kundengespräche und Berichte
- ▶ Teamarbeit und selbstständiges Arbeiten
- ▶ Ethisches Verantwortungsbewusstsein, besonders im Umgang mit sensiblen Daten und Systemen





Dr. Antje Winkler

Division Lead

Offensive Security

+49 351 26352-157

antje.winkler@bdosecurity.de

www.bdosecurity.de

