Penetrationstest

BDO Cyber Security GmbH

Dr. Antje Winkler

Was ist unsere Motivation?

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 %)

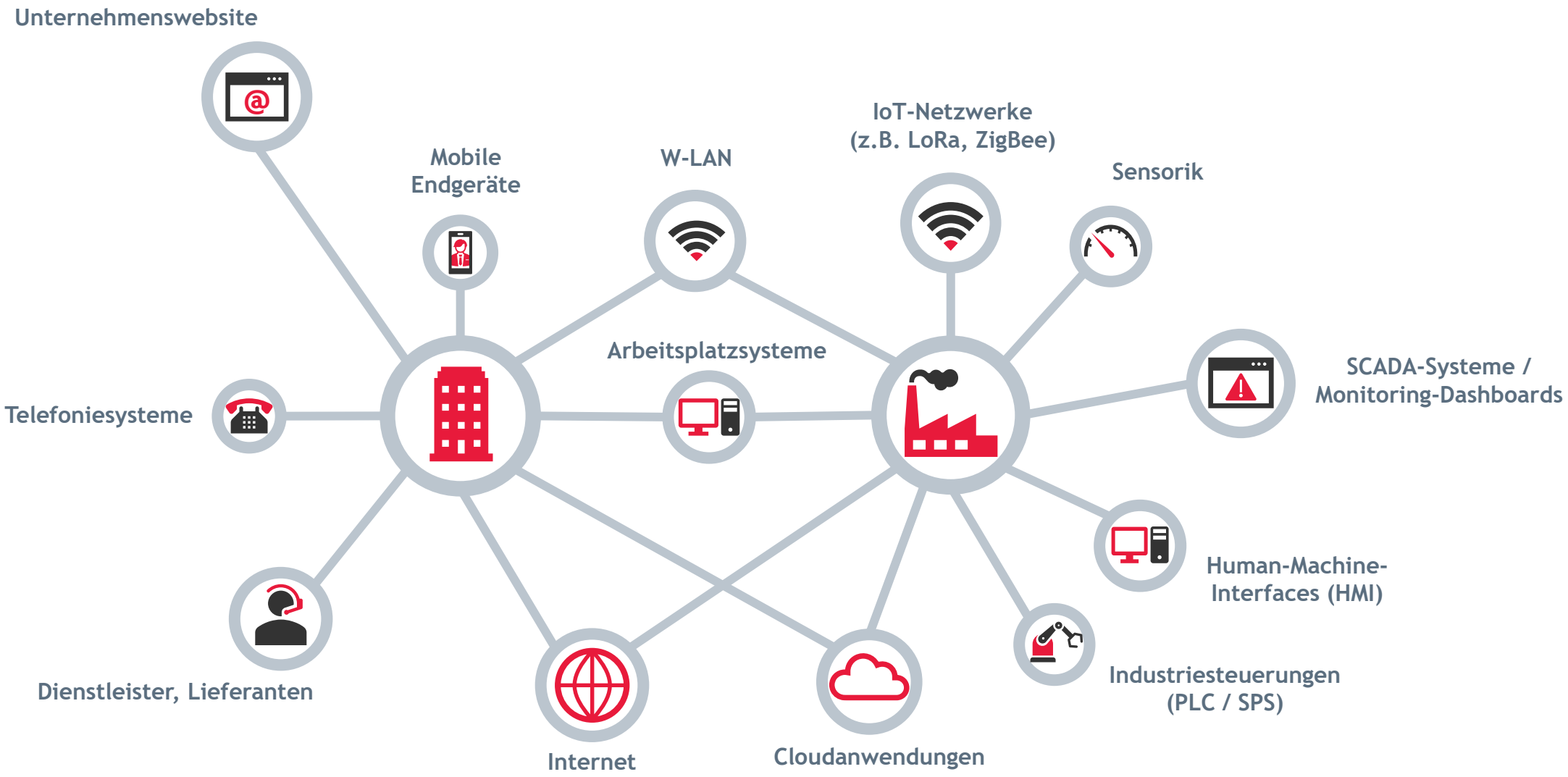
3+ Monate bis zur Rückkehr zum Normalbetrieb, wie z.B. im Fall von ca. 103 westfälischen Kommunen oder dem Frankfurter Uniklinikum

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



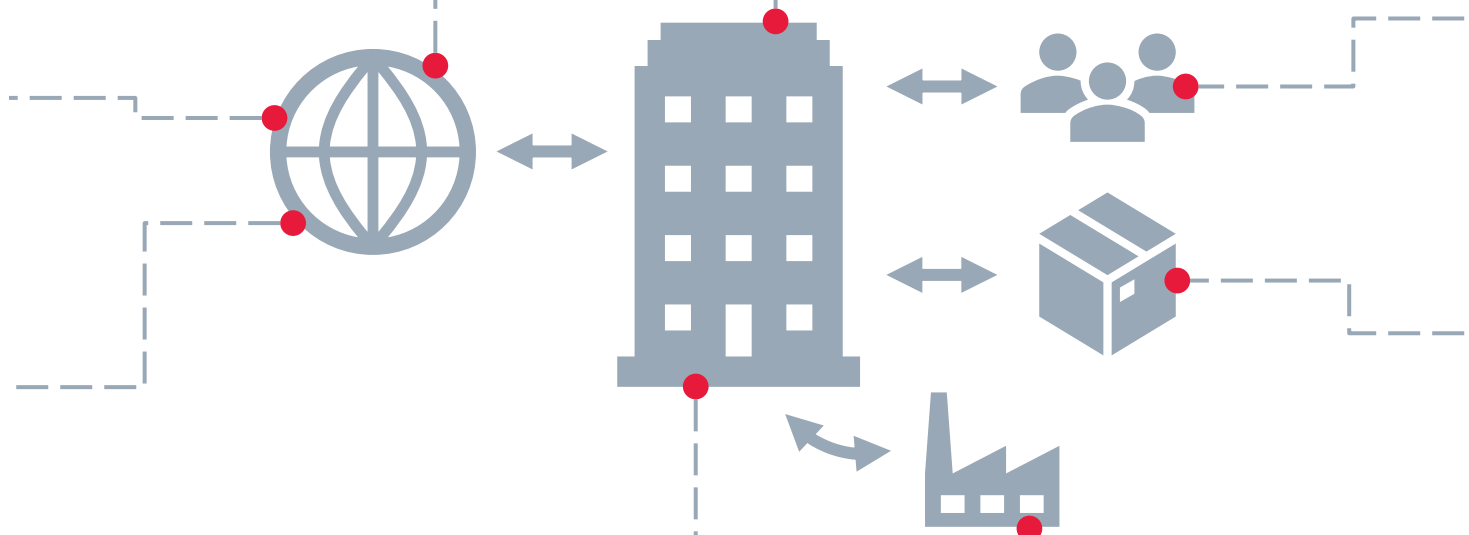
Angriffsfläche von Unternehmen

Angriffe von innerhalb und außerhalb des Unternehmens

Öffentlich verfügbare Informationen über das Unternehmen
z.B. über Website, Datenbanken, Suchmaschinen, Social Media

Unternehmensnetzwerk
z.B. Server- und Clientsysteme, Datenbanken, Netzwerkseparierung

Aus dem Internet erreichbare Systeme des Unternehmens
z.B. Website, Mailserver, Telefonanlage, Fernzugriffe, Cloudsysteme



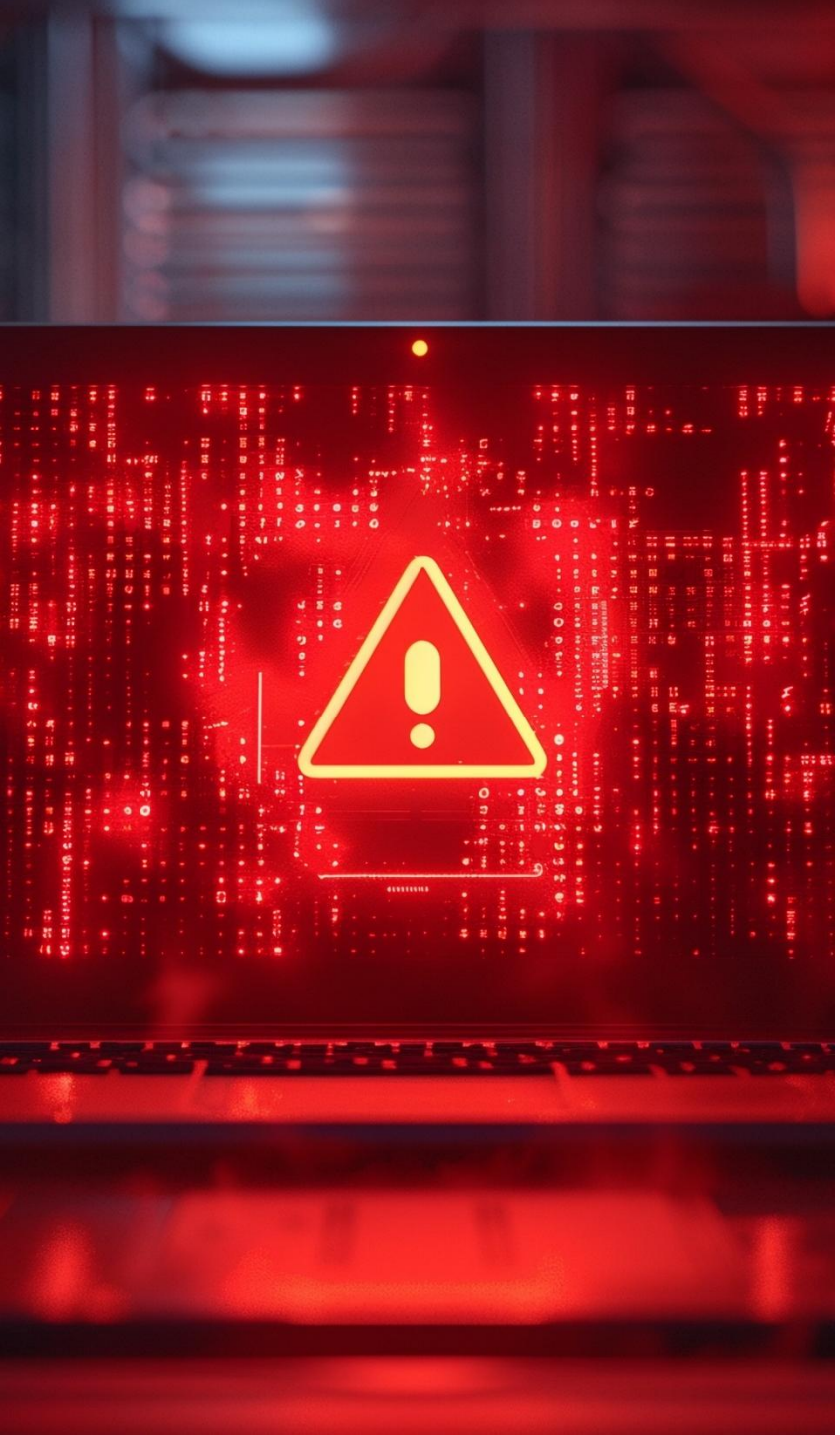
Mitarbeiter
z.B. Täuschung von Mitarbeitern über Phishing

Produkte
z.B. Soft- und Hardwareprodukte des Unternehmens, Schnittstellen zu den Produkten (APIs, Over-the-air Firmware)

Lieferanten
z.B. exponierte Schnittstellen über eingekaufte Soft- und Hardware, Fernwartung

Unternehmensstandort
z.B. Geräte (wie Terminals) und Schnittstellen in öffentlichen Bereichen, Wi-Fi, Gast- und Lieferanteneingänge

Produktion
z.B. Produktionsanlagen, ICS-/SCADA-Systeme, PLC/SPS, Sensoren/Aktoren, Netzwerkhardware, Embedded Devices



Aktuelle Bedrohungen

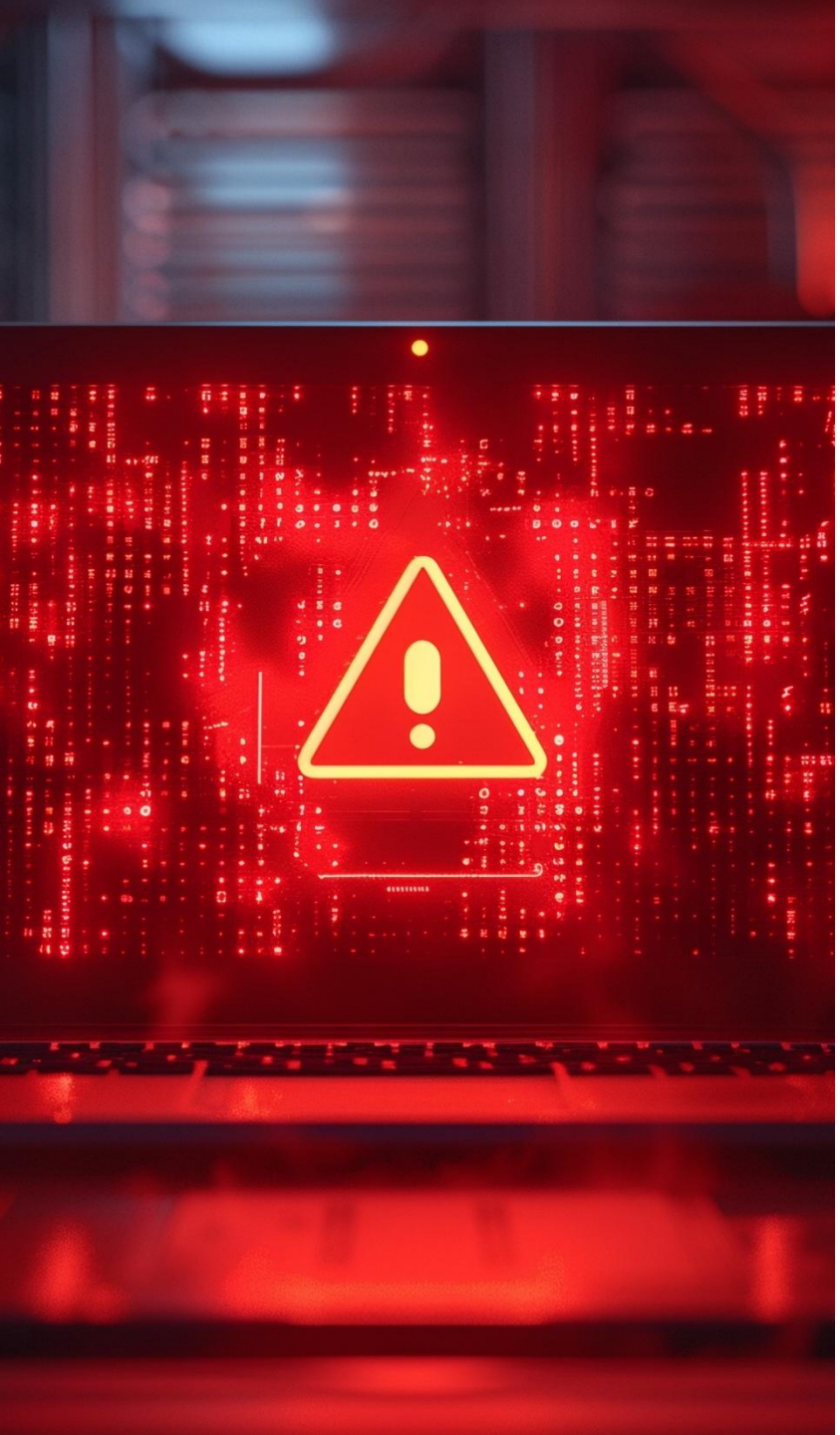
Häufigste Bedrohungsszenarien

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

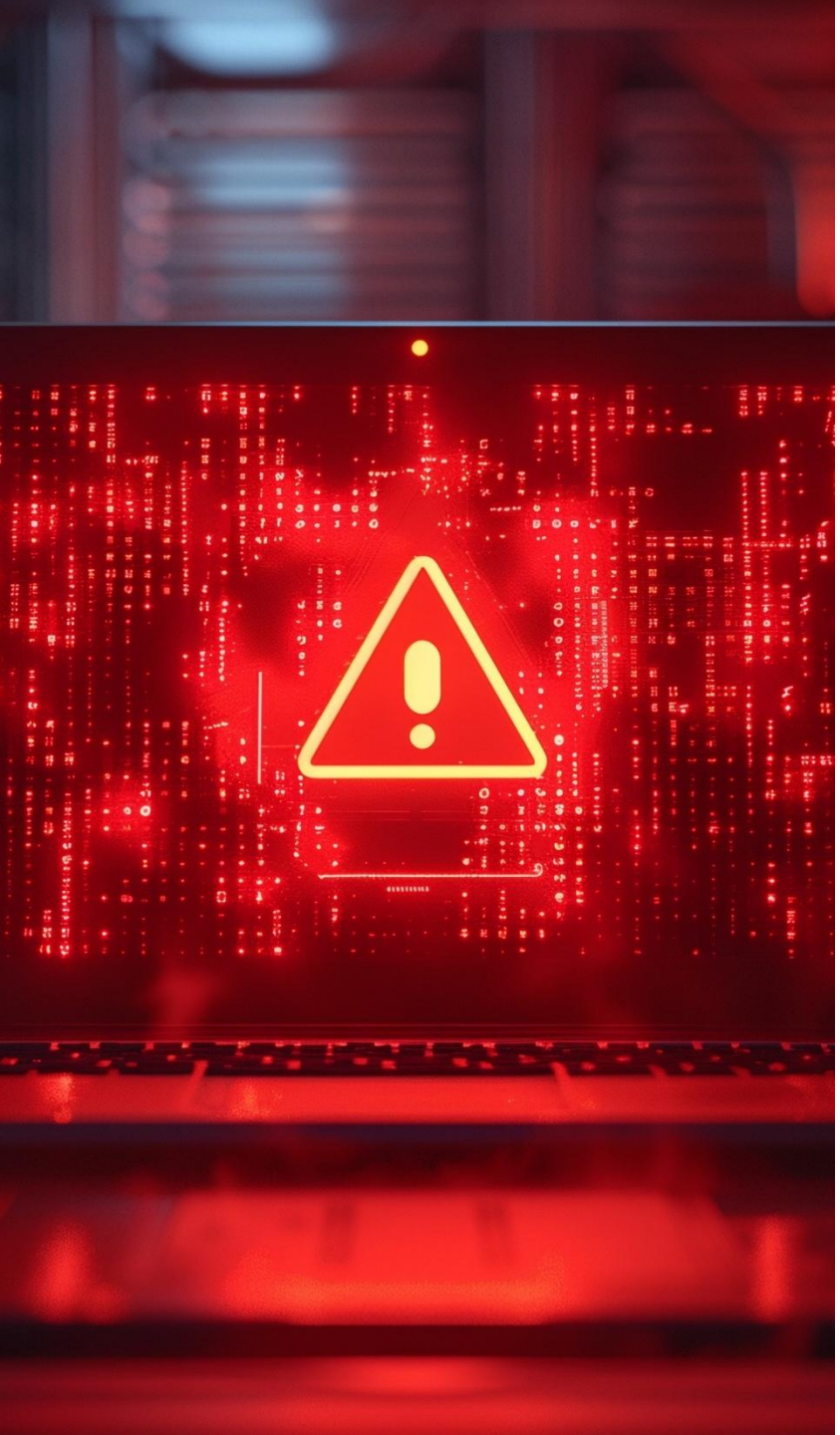
Häufigste Bedrohungsszenarien

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: https://www.youtube.com/watch?v=opRMrEfAIiI
  - hallo
  - 1234567890
  - 1234567
  - password
  - password1
  - target123
  - iloveyou
  - gwerty123
- 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
- Einteilung nach „Hats" (Motivation & Legalität)

White-Hat

- Agieren innerhalb der Gesetze (inkl. Grauzonen)
- Führen Penetrationstests im Auftrag von Unternehmen durch
- Ziel: Sicherheitslücken vor Missbrauch aufdecken
- Fachkompetente Sicherheitsexperten mit konstruktivem Ansatz

Black-Hat

- Handeln mit krimineller Energie
- Ziele: Systeme beschädigen oder Daten stehlen
- Cyber-Kriminelle
- Spammer / Adware
- APT-Gruppen

Gesetzeslage: Hacking in Deutschland

Grundsatz: Verboten

- Hacking ist strafbar nach §§ 202a, 202b, 202c, 303a StGB
- Bereits der unbefugte Zugriff allein ist strafbar – unabhängig von entstandenem Schaden

Problem:

- Kein Unterschied zwischen „gut" und „böse„
- Gesetz unterscheidet nicht zwischen White-Hat und Black-Hat
- Sicherheitsforscher bewegen sich in einer rechtlichen Grauzone

Ausnahmen: Wann ist es erlaubt?

- Eigene Systeme testen → legal
- Penetrationstests → nur mit schriftlicher Genehmigung des Systeminhabers
- Besitz von Hacker-Tools → legal, solange keine kriminelle Absicht nachweisbar

Fazit: Ohne explizite Erlaubnis des Systeminhabers ist jede Form von Hacking in Deutschland strafbar – auch gut gemeintes

Offensive Security

Wir finden Schwachstellen, bevor andere es tun.

Realistische Angriffssimulation

Wir versetzen uns in die Perspektive realer Angreifer und analysieren die Sicherheitsmaßnahmen Ihrer Systeme und Netzwerke.

Gezielte Schwachstellenanalyse

Wir identifizieren und bewerten Sicherheitslücken in diversen Anwendungen, Systemen und Netzwerken – ganz nach Ihrem Bedarf.

Ermittlung nachhaltiger Maßnahmen

Im Anschluss an die Analyse unterstützen wir Sie 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 Sie bei allen Fragestellungen rund um das Thema Cybersicherheit auf technischer Ebene – von der Konzeption über die Entwicklung bis zum Betrieb. Gern vernetzen wir Ihre Fachabteilungen direkt mit unseren Experten.

Vorgehen im Penetrationstest

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

Phase 1 - Vorbereitung

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 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	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 4 - Aktive Eindringversuche

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 5 - Abschlussanalyse und Clean-Up

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

Vorgehen im Penetrationstest – Phase 1

Scope definieren

Phase 1 – Scope definieren

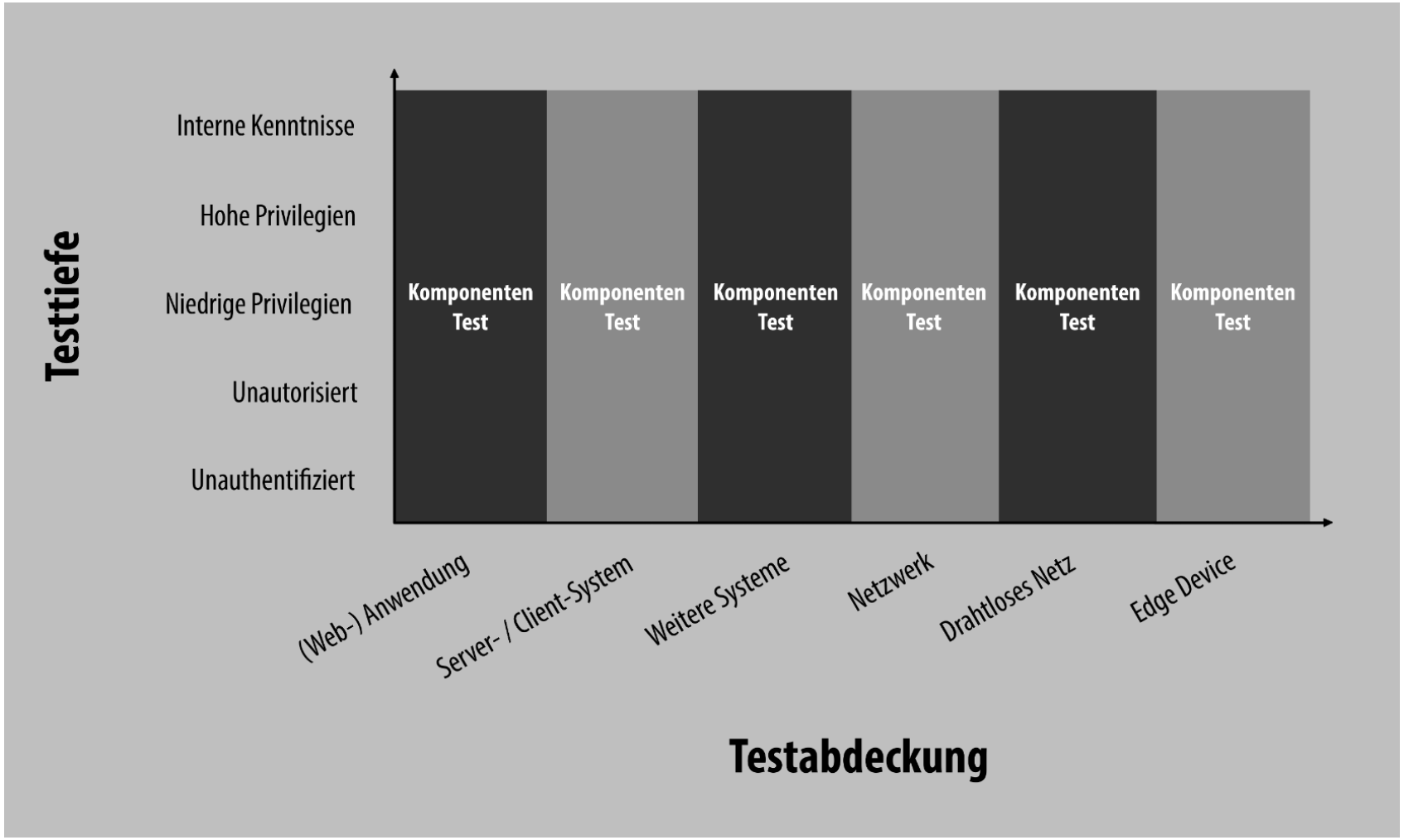
- Angreiferperspektive
- Testabdeckung
- Testart
- Testtiefe
- Testschwerpunkte

Angreiferperspektive

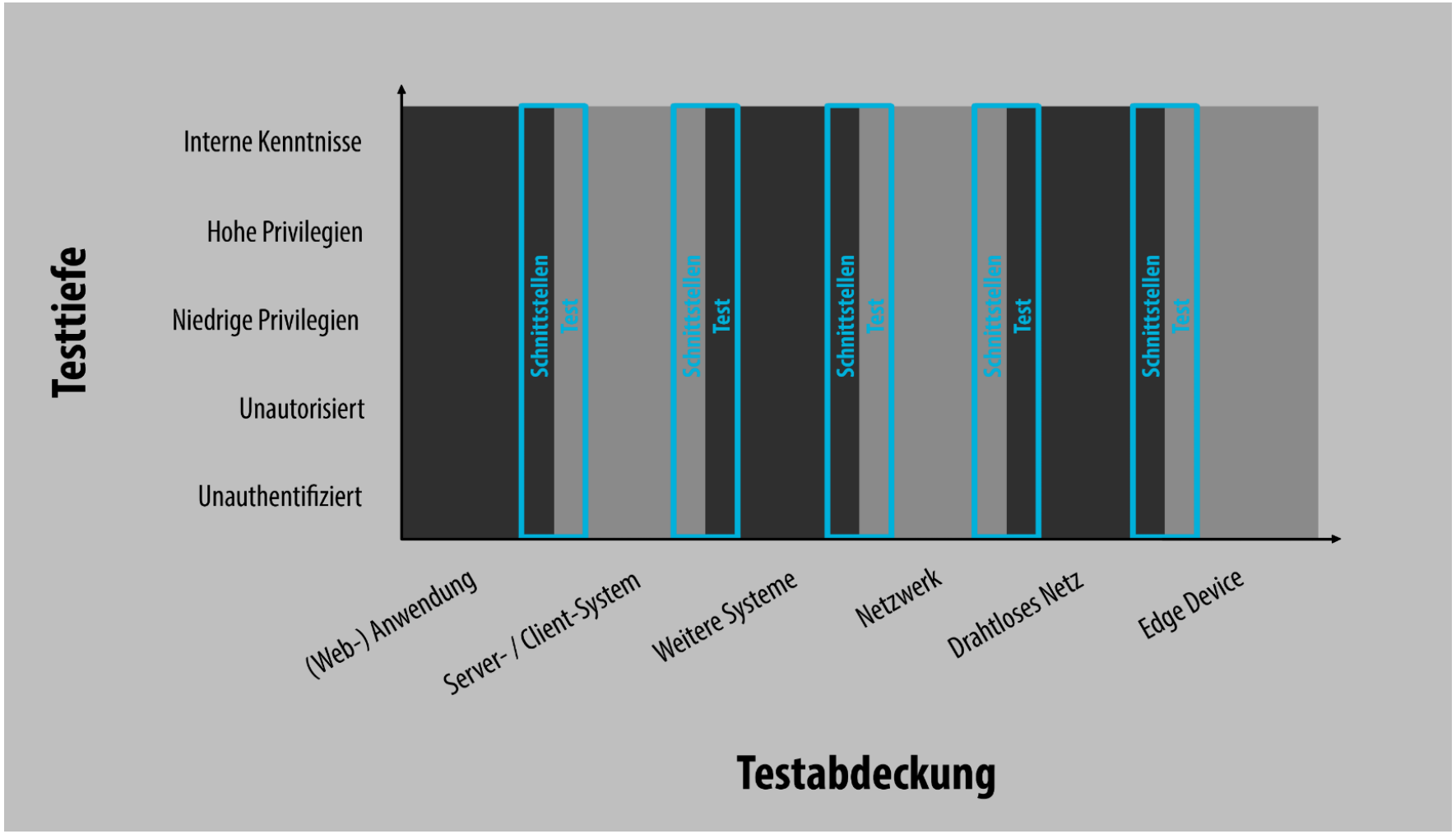
Klärung der Frage: Gegen welche Art Angreifer soll das System geschützt werden?

- 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)

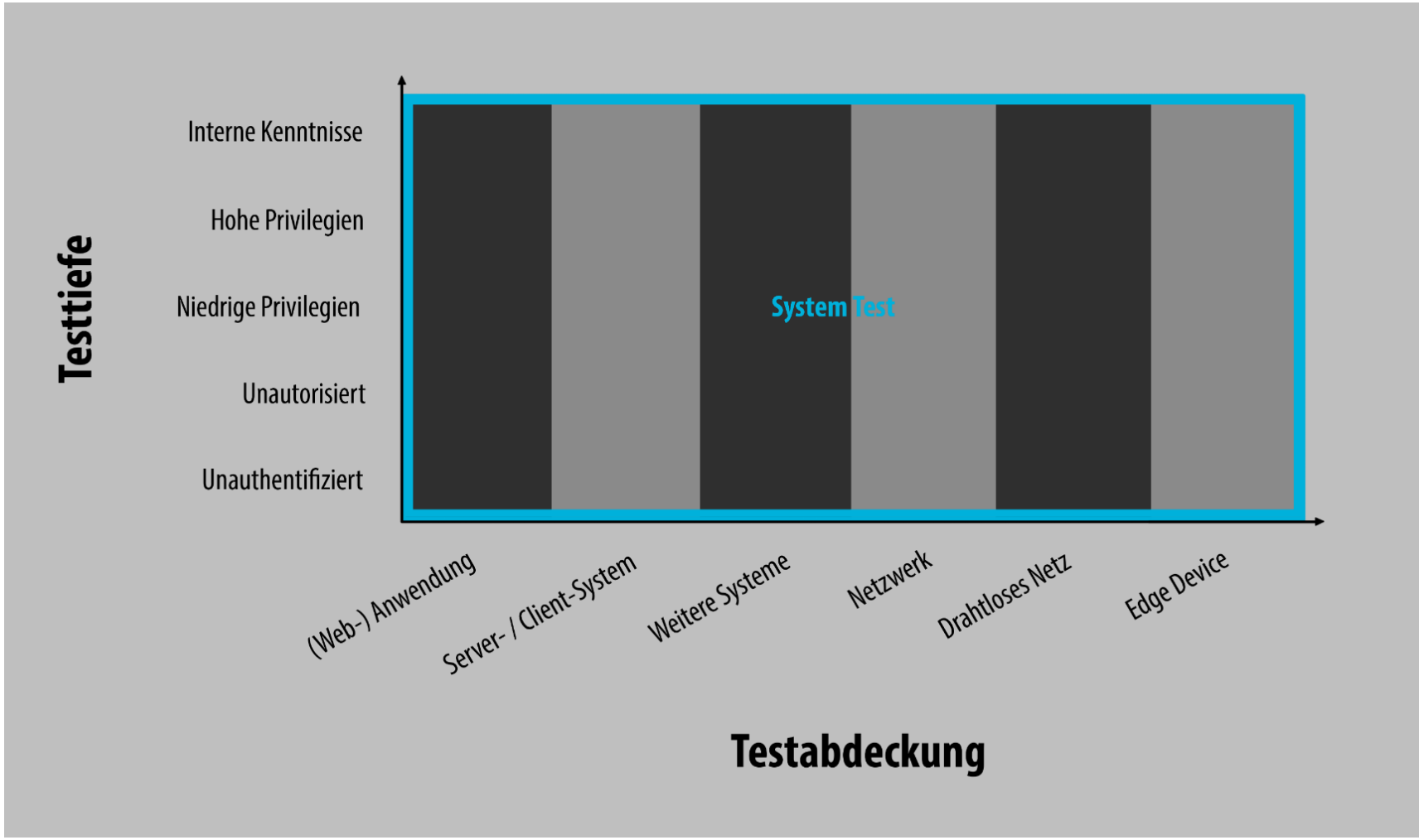
Testabdeckung - Komponententest



Testabdeckung - Schnittstellentest



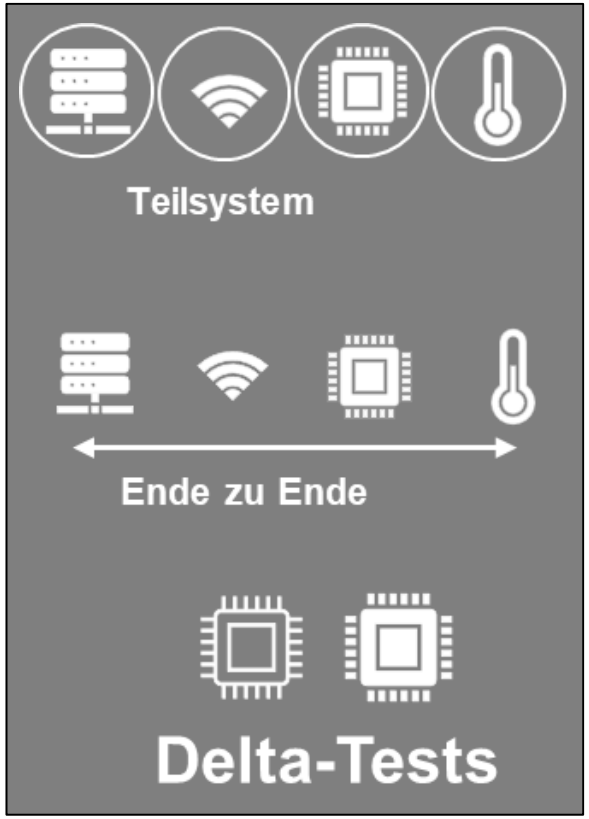
Testabdeckung - Ende-zu-Ende Test



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

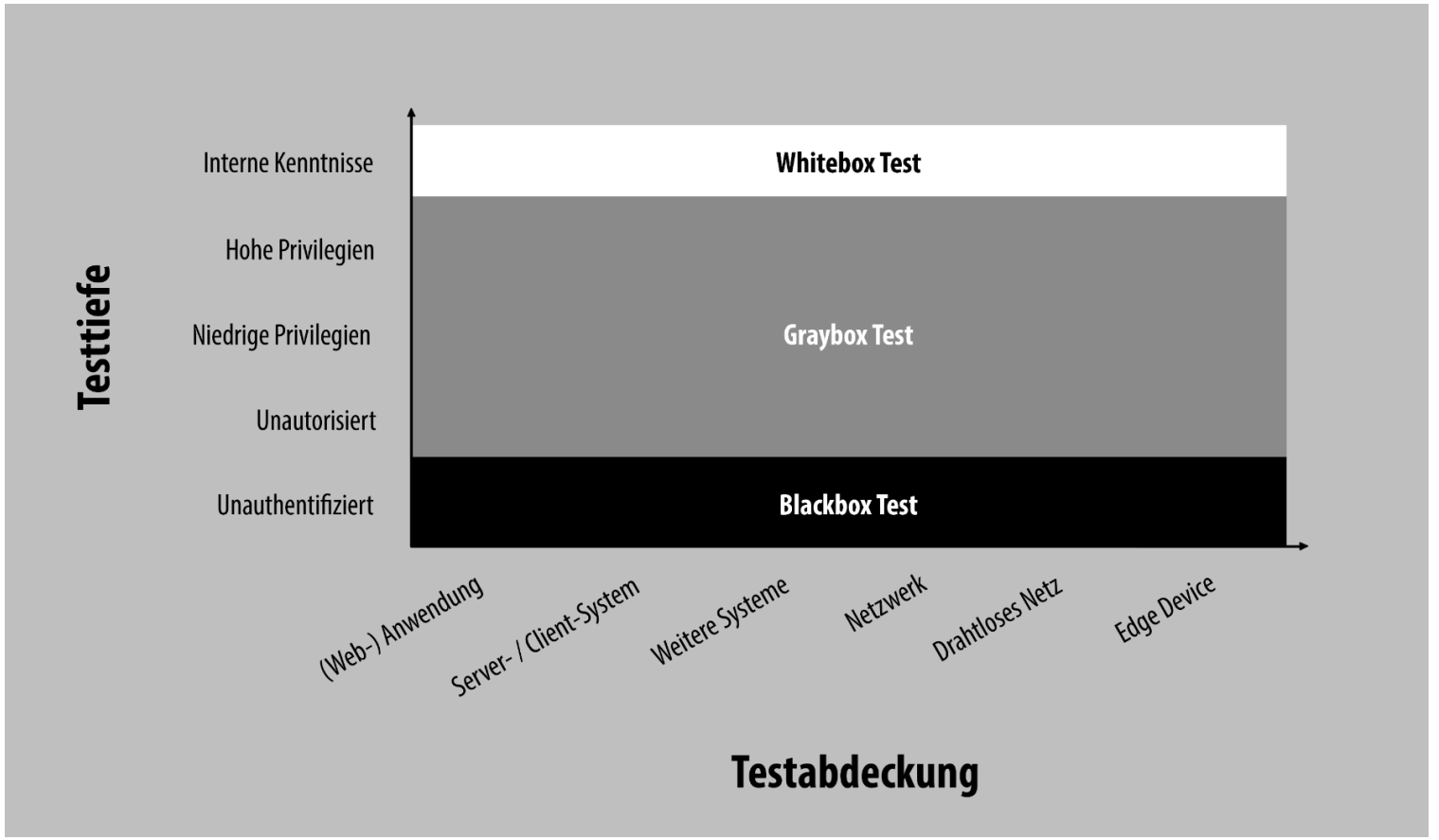
Source Code Analyse

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



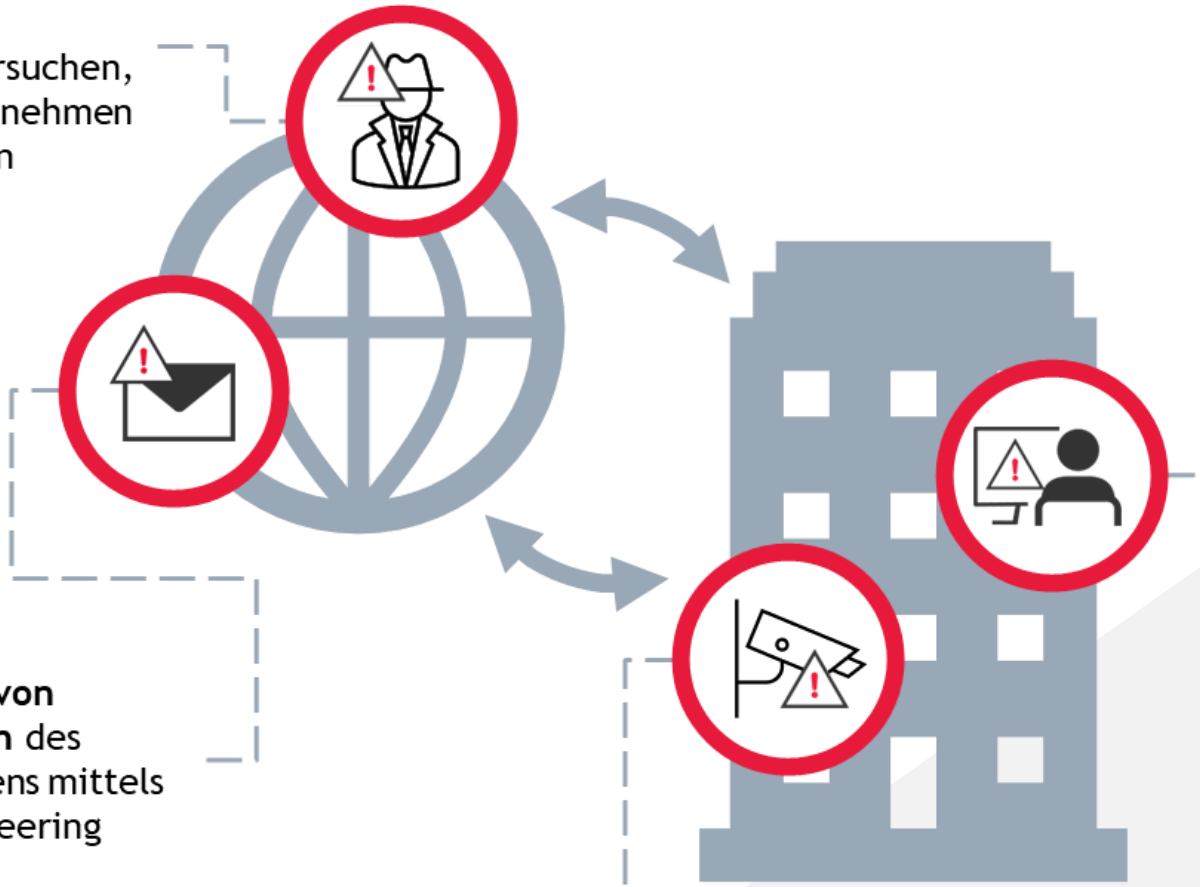
Das Angebot

- 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 Innentäter

Täuschung von Mitarbeitern des Unternehmens mittels Social Engineering

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

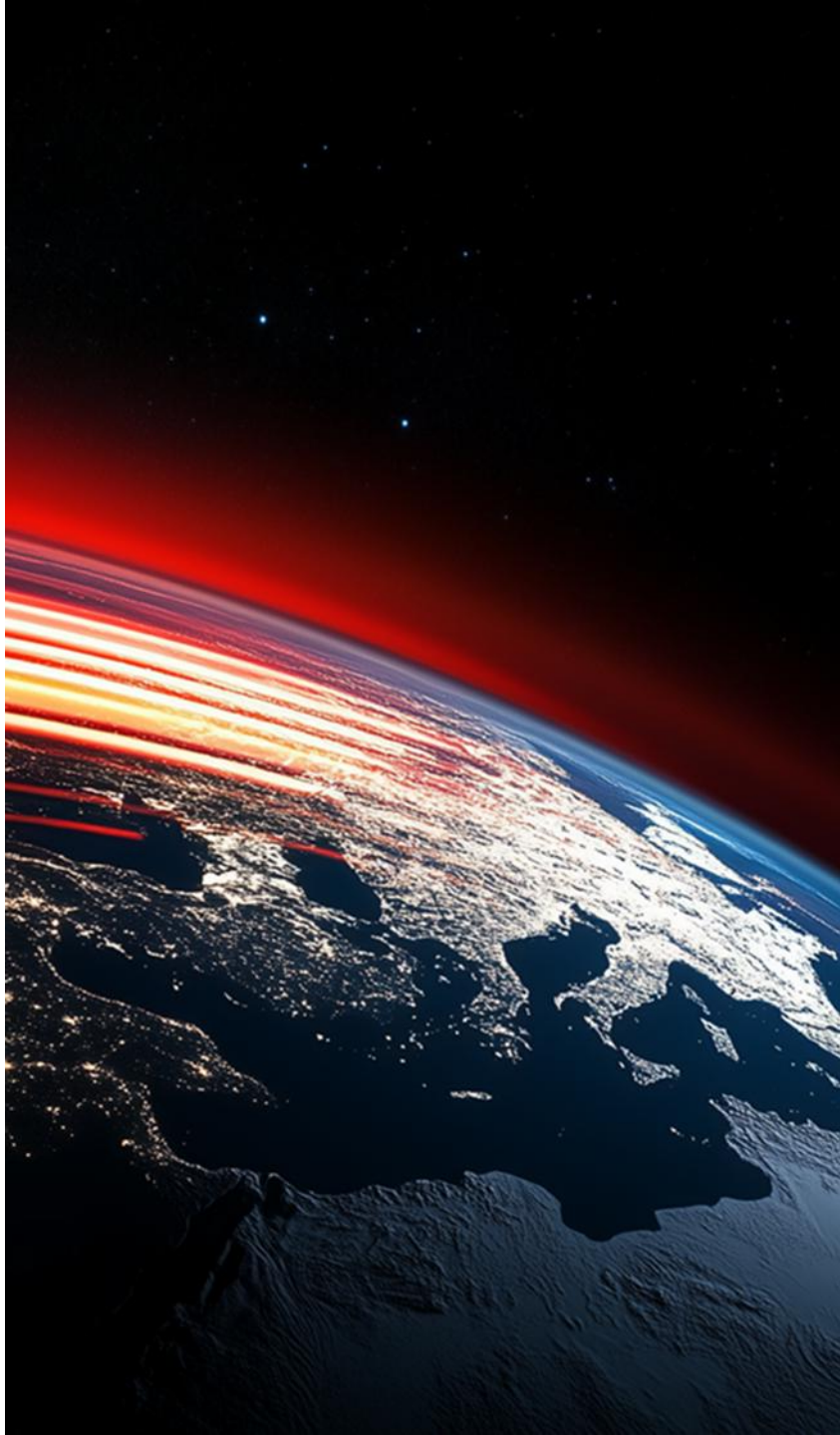
Angriffe aus dem Internet

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
- Kamera Büro China
- Über das Remote Desktop Protocol (RDP) erreichbare Systeme:
  - Hospital has_screenshot:true
  - Norwegischer Energieversorger
  - Klinik in Pinneberg

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

Beispiele

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

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

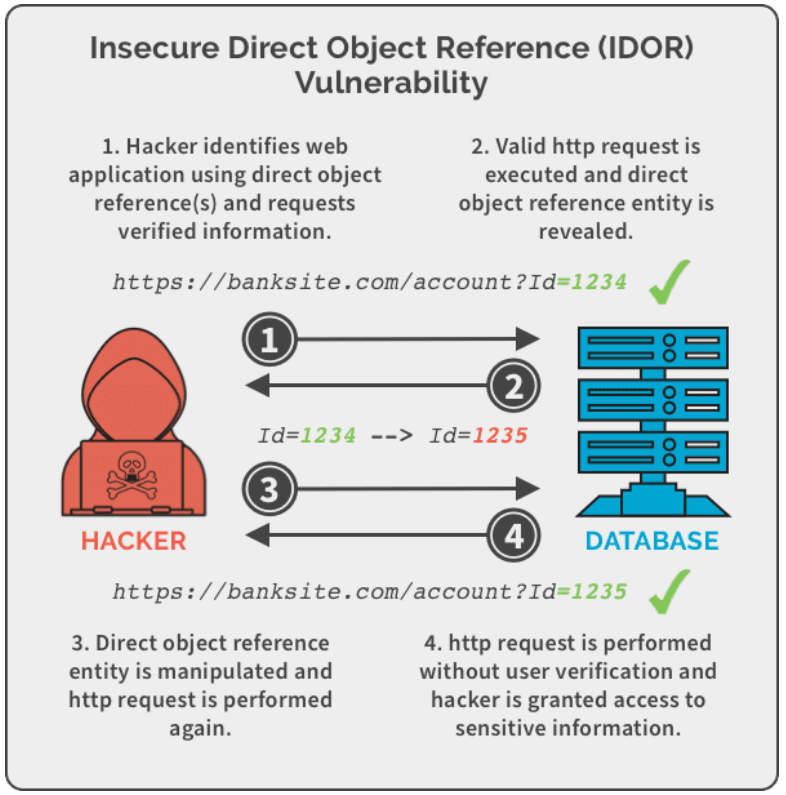
Testschwerpunkte Webanwendung

- 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



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
- Beipiele:
  - 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/
- OffensiceCon: https://www.offensivecon.org
- Blackhat: https://www.blackhat.com/...

Portfolio BDO Cyber Security

Cyber-Resilienz auf die Sie vertrauen können

Unternehmenswerte angemessen schützen und auf Notfälle vorbereitet sein.

Security Management

- Risiken erkennen und managen
- Cyber Strategie und Governance-Struktur etablieren
- Compliance herstellen und kontrollieren
- Cyber Sicherheit zertifizieren lassen

Defensive Security

- Reaktionsfähigkeit der Organisation trainieren
- Schnell und angemessen auf Cyber Angriffe reagieren
- Geschäftsfähigkeit sicherstellen
- Ursachen und Auswirkungen von Incidents aufklären

Offensive Security

- Angriffsoberfläche identifizieren
- Mit realen Angriffsmethoden Schwachstellen finden
- Ganzheitliche Sicherheitsbewertung
- Zielgerichtet Maßnahmen ableiten

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

Warum ist der Beruf so spannend?

Vielfalt & Abwechslung

- Web, IT/OT, Hardware, Automotive, Healthcare …
- Perspektiven: Außentäter, Innentäter, physisch vor Ort
- Kein Test wie der andere – kein Ziel wie das andere
- Nie langweilig – ständig neue Herausforderungen

Kombination vieler Tätigkeiten

- Technischer Test – allein oder im Team
- Kundenkontakt & Beratung
- Recherche, Analyse & Dokumentation
- Tool-Entwicklung & Programmierung

Gesellschaftliche Relevanz

- Aktiver Beitrag zur Sicherheit von Unternehmen
- „Hacking für das Gute" – legal Schwachstellen finden

Ständiges Lernen

- Neue CVEs, Exploits & Tools entdecken
- Aktive Community & Wissensaustausch

Was muss ich mitbringen?

Mindset

- Interesse an Hacking & IT-Sicherheit
- Experimentierfreude & Spieltrieb
- Grenzen austesten – „Was passiert, wenn …?"
- Querdenken & kreatives Kombinieren
- Dinge außerhalb ihres Verwendungszwecks nutzen

Technische Basis

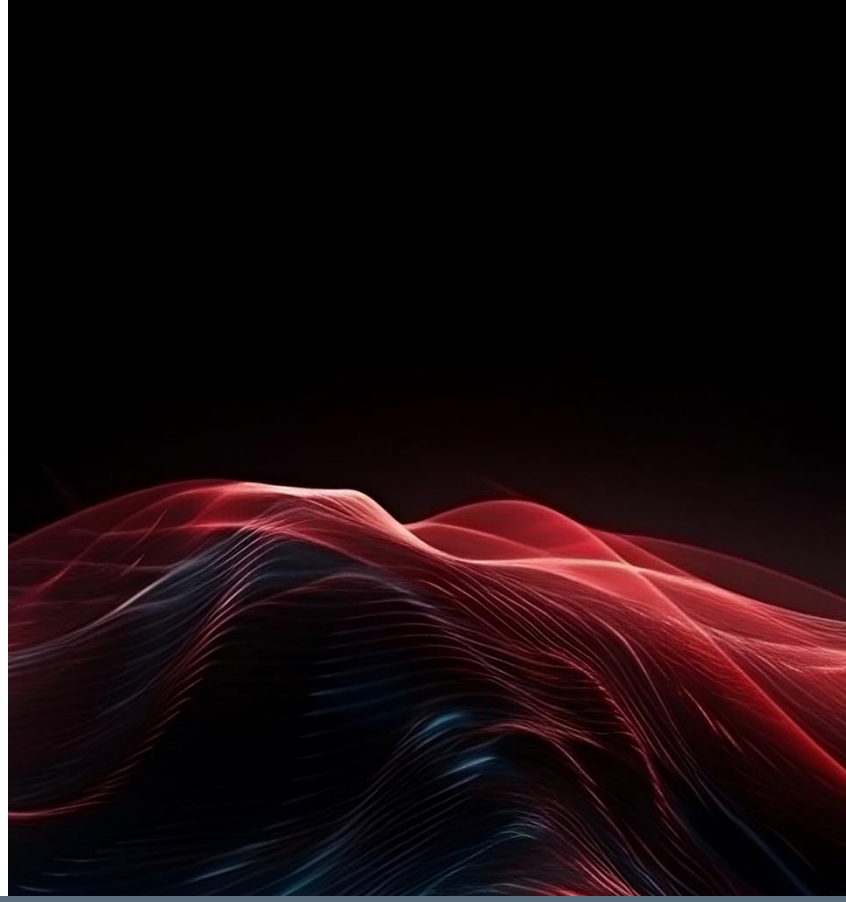
- Grundverständnis: Netzwerke, Betriebssysteme, Programmierung
- Linux & Kommandozeile
- Bereitschaft zum Selbstlernen
- Sorgfältige Dokumentation

Soft Skills

- Kommunikationsfähigkeit für Kundengespräche
- Team- & Einzelarbeit
- Ethisches Verantwortungsbewusstsein

Dr. Antje Winkler

Division Lead
Offensive Security
+49 351 26352-157
antje.winkler@bdosecurity.de



www.bdosecurity.de