Penetrationstest

Dr. Antje Winkler
BDO Cyber Security GmbH

BDO CYBER SECURITY

Was ist unsere Motivation?

BDO CYBER SECURITY

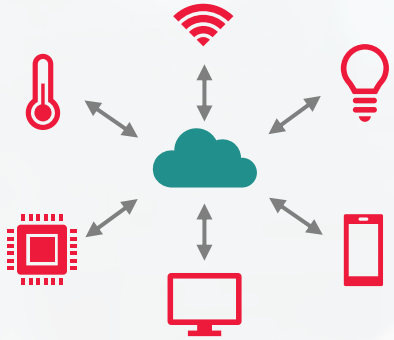
Gründe für die meisten erfolgreichen Angriffe

- schlechte Passwörter: https://www.youtube.com/watch?v=opRMrEfAIiI

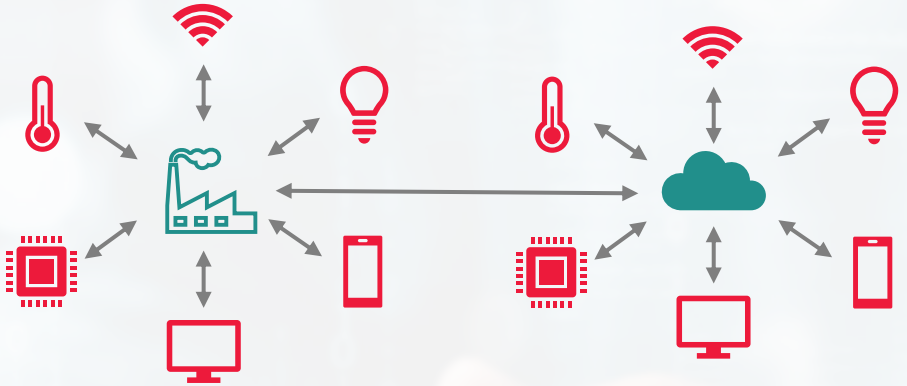
Password123	Lieblingsband
Hallo123	Haustiername
Lol123	Schule
123456	Crush
Abc123	Beziehungsdatum

- Teilen von sensiblen privaten Informationen im Internet / sozialen Netzwerken
- Installation / Herunterladen von fragwürdigen Programmen oder Apps
- Phishing-Mails
- Standard-Konfigurationen und Unwissenheit: https://www.shodan.io/search?query=webcamxp

Zunehmende Vernetzung - Erhöhung der Komplexität



Internet of Things
„intelligente“ Gegenstände mit „smarten“ Funktionen



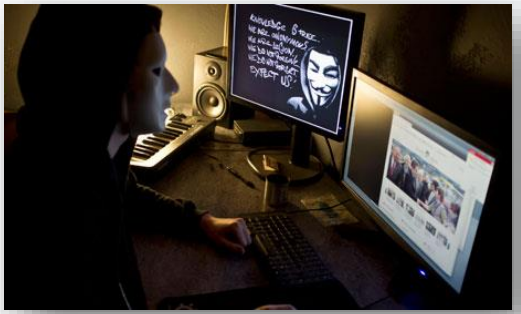
Industrial IoT
Industrielle Ausprägung des IoT

BDO CYBER SECURITY

Was macht ein Penetrationstester?

BDO CYBER SECURITY

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

Bunte Hüte

White-Hat

- halten sich an Vorschriften, Gesetze und die “Hackerethik”
- "Ethical Hackers"

→ **Penetrationstester**

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 …

BDO CYBER SECURITY

Was ist ein Penetrationstest?

- **Aufspüren** von Sicherheitslücken in IT-Ökosystemen, bevor andere sie ausnutzen
- **Bewertung** des Sicherheitsniveaus
- Erstellung eines detaillierten **Maßnahmenkataloges** mit Empfehlungen

- rechtliche Absicherung
- definierter Scope
- definierter Testprozess
  - abgestimmte Prüfpunkte
  - reproduzierbare Ergebnisse

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.

Testvorgehen Penetrationstest

BDO CYBER SECURITY

Vorgehensmodell nach BSI

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

1. Vorbereitung
2. Informationsbeschaffung und -auswertung
3. Bewertung der Informationen / Risikoanalyse
4. Aktive Eindringversuche
5. Abschlussanalyse

Penetrationstest - Prozess -Phase 1

Vorbereitung	Informations-beschaffung	Bewertung	Aktive Eindring-versuche	Abschlussanalyse
• 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 Abschluss-dokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Penetrationstest – Prozess –Phase 2

Vorbereitung	Informations-beschaffung	Bewertung	Aktive Eindring-versuche	Abschlussanalyse
• 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 Abschluss-dokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Penetrationstest - Prozess -Phase 3

Vorbereitung	Informations-beschaffung	Bewertung	Aktive Eindring-versuche	Abschlussanalyse
• 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 Abschluss-dokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Penetrationstest - Prozess -Phase 4

Vorbereitung	Informations-beschaffung	Bewertung	Aktive Eindring-versuche	Abschlussanalyse
• 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 Abschluss-dokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Penetrationstest - Prozess -Phase 5

Vorbereitung	Informations-beschaffung	Bewertung	Aktive Eindring-versuche	Abschlussanalyse
• 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 Abschluss-dokumentation • Bewertung der Ergebnisse • Darstellung der Risiken • Definition von Maßnahmen

Phase 1: Scope definieren

BDO CYBER SECURITY

Angreiferperspektive

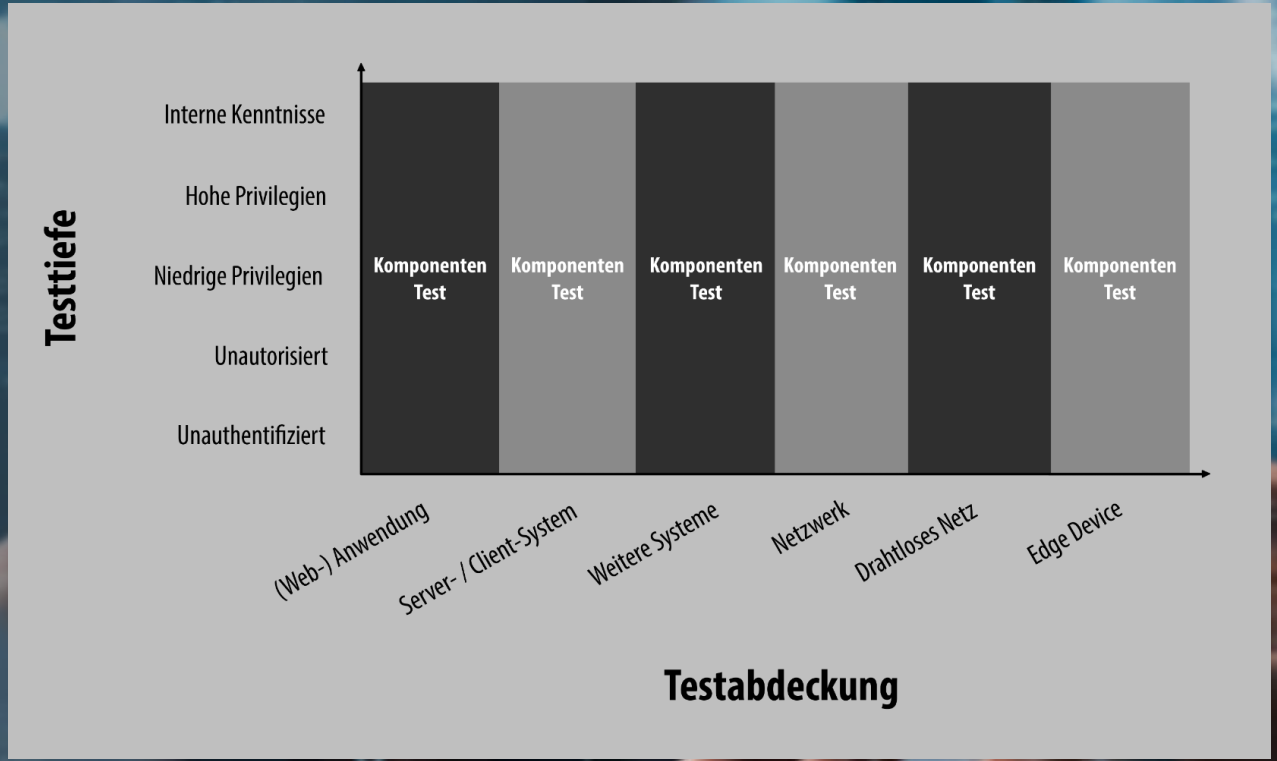
- Klärung der Frage: Gegen welche Art Angreifer soll das System geschützt werden?
  - Beispiele:
    - externer, nicht privilegierter Angreifer (z.B. jemand mit Zugang zum Gerät aber ohne Zugriff auf Gerätefunktionen)
    - externer, privilegierter Angreifer (z.B. Käufer, Endnutzer)
    - interner, nicht privilegierter Angreifer (z.B. Gastzugang)
    - interner, niedrig privilegierter Angreifer (z.B. Mitarbeiter)
    - interner, hoch privilegierter Angreifer (z.B. Administrator)

Testabdeckung

- Definition der Testobjekte, welche im Rahmen des Tests untersucht werden
- Beispiele:
  - **Komponenten** (z.B. Webanwendungen, Server)
  - **Schnittstellen** (z.B. APIs, Funkschnittstellen)
  - **Ende-zu-Ende Test** (vom Gerät über die API bis zur Webanwendung)

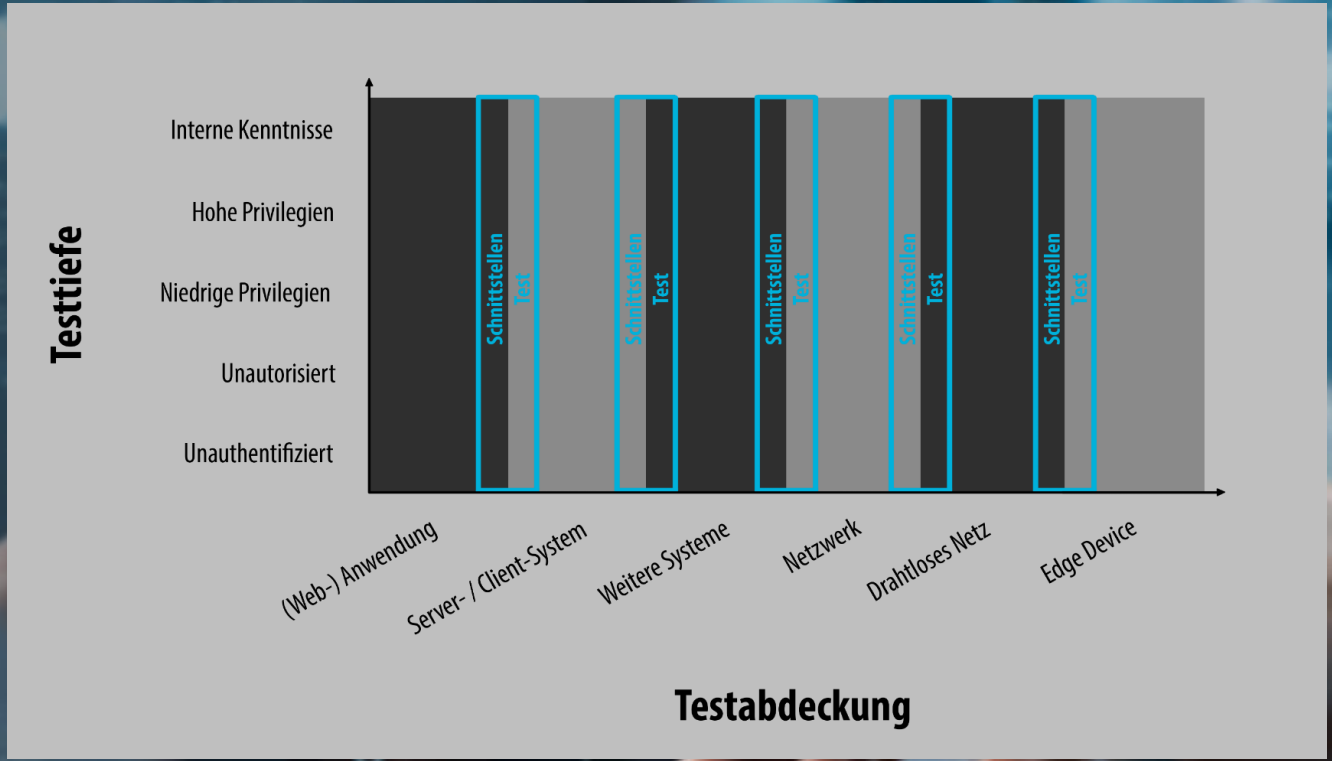
- zunehmende Vernetzung führt zu mehr Schnittstellen und zur vermehrten Öffnung dieser (Zugriff über das Internet)

Testabdeckung - Komponententest



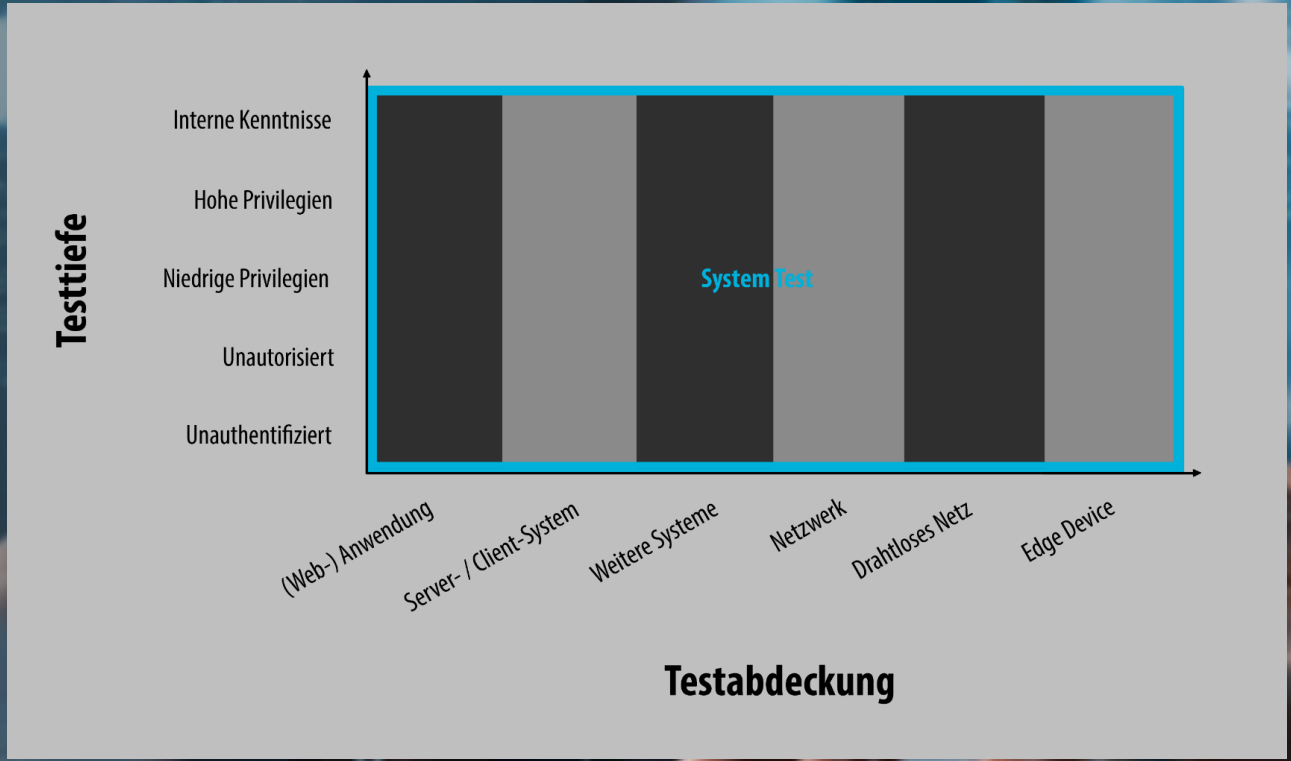
BDO CYBER SECURITY

Testabdeckung - Schnittstellentest



BDO CYBER SECURITY

Testabdeckung - Ende-zu-Ende Test

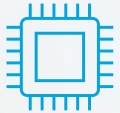


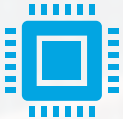
BDO CYBER SECURITY

Testabdeckung - Deltatest

Delta-Tests

Vergleich zwischen zwei verschiedenen Systemversionen

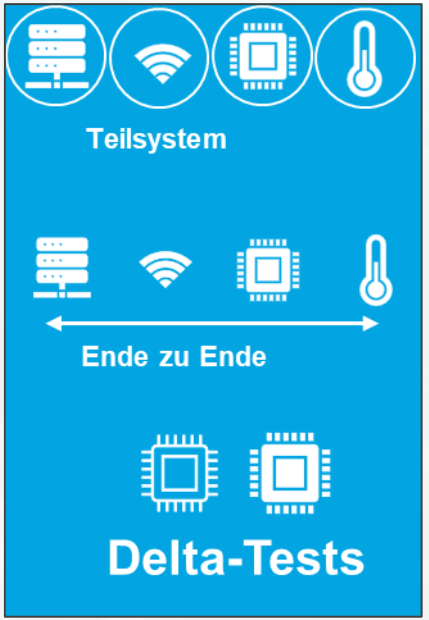




Testabdeckung

Vergleich

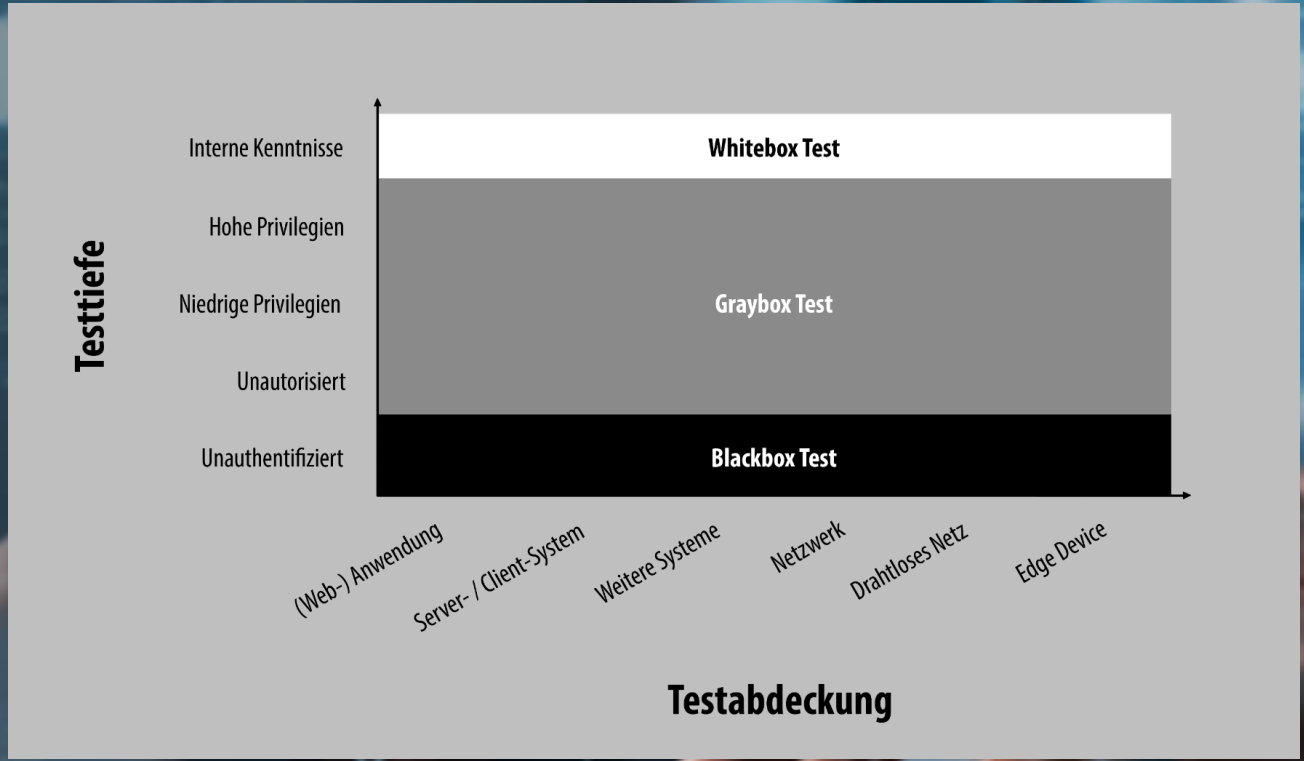
- Komponententest z.B. wichtig bei verschiedenen Zulieferern;
  Betrachtung aber nicht ganzheitlich
- Ende-zu-Ende Test betrachtet das System ganzheitlich;
  aufwendiger und kostenintensiver
- Delta-Tests eignen sich bei weniger großen Updates



Testtiefe

- legt fest, wie detailliert das Testobjekt betrachtet werden soll
- Eingrenzung der Testfälle und der Einzelkomponenten
- 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



BDO CYBER SECURITY

Testtiefe

Blackbox

- realitätsnah, vergleichsweise wenig Aufwand
- Probleme können übersehen werden
- relativ geringe Testabdeckung und hohes Risiko, dass tieferliegende Schwachstellen nicht entdeckt werden

Whitebox

- besserer Soll-Ist Vergleich
- aufgrund der Dokumentenlage können schon Probleme erkannt werden
- aufgrund hoher Abdeckung meist auch höhere Kosten

Testtiefe

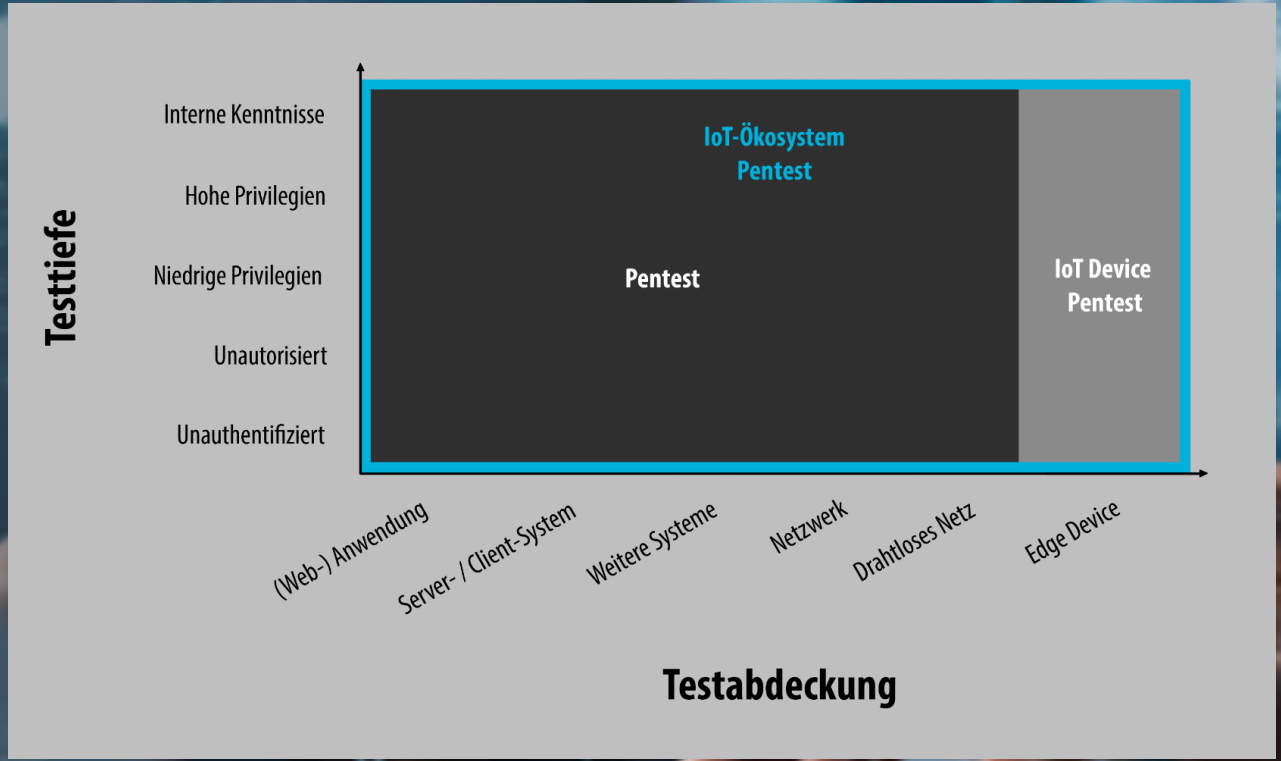
Greybox

- stellt eine Mischform aus Black- und Whitebox-Test dar
- entsprechend geringere Kosten als bei Whitebox
- nicht vollumfänglich wie Whitebox

Explorativ

- fokussiert auf das Wesentliche
- meist festgelegter Zeitrahmen
- besonders geeignet bei großen Systemen

Testschwerpunkte



BDO CYBER SECURITY

Testart

Schwachstellen-Scan

- 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

Testart

Penetrationstest

- zielgerichteter Versuch, mit den Mitteln eines Angreifers innerhalb einer gegebenen Zeitspanne Lücken in der Sicherheit aufzudecken
- realitätsnaher Ansatzes, 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
  - Web: z. B. https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/

Testart

Source Code Analyse

- Untersuchung von Quelltexten
- 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

Das Angebot

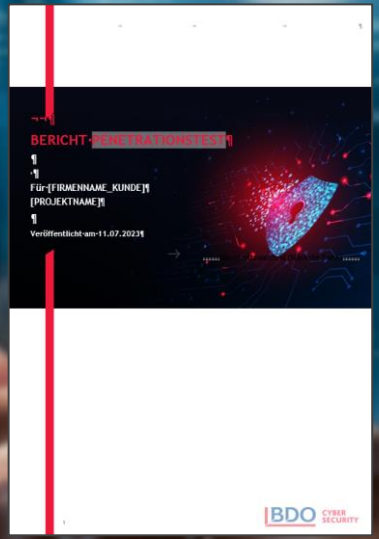
- Testart (Scan, Penetrationstest,…)
- Testobjekt und Testumfang (Scope und Out-of-Scope)
- Whitebox oder Blackboxtest, Innen- oder Außenperspektive, verdeckt oder offen
- Mitwirkungspflichten des Kunden
- Planung der Testdurchführung
  - Testzeitraum
  - Ort der Durchführung
  - Testzugänge, Testaccounts
  - Mitwirkung des Kunden

Phase 5: Testdokumentation

BDO CYBER SECURITY

Testbericht Penetrationstest

- Nach der Durchführung des Tests erhalten Sie einen Testbericht, der folgendes beinhaltet:
  - eine Zusammenfassung des Testansatzes und der Testergebnisse, einschließlich einer allgemeinen Bewertung des Gesamtsicherheitsniveaus des Testobjekts,
  - eine detaillierte Beschreibung der gefundenen Schwachstellen, einschließlich eines Proof of Concept und Screenshots,
  - eine Bewertung jeder Schwachstelle hinsichtlich ihres Schweregrades,
  - allgemeine Empfehlungen für Gegenmaßnahmen zur Behebung oder Mitigation der festgestellten Schwachstellen



BDO CYBER SECURITY

Bewertung von Findings

Bewertung: nach CVSS 3.1 (Base Score):
https://www.first.org/cvss/calculator/3.1

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**	

Score: 7,6 (High)

Weitere Infos

BDO CYBER SECURITY

Testwerkzeuge

- je nach zu untersuchemden 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/
- **Hacking Labs**
  - HackTheBox: https://www.hackthebox.eu/
  - OWASP Juice Shop: https://github.com/bkimminich/juice-shop
  - PortSwigger Academy https://portswigger.net/web-security
- **Konferenzen**
  - DEFCON: https://media.defcon.org/
  - OffensiceCon: https://www.offensivecon.org
  - Blackhat: https://www.blackhat.com/

Portfolio BDO Cyber Security

BDO CYBER SECURITY

Unser Portfolio

Embedded und IoT

- eingebettete Systeme und IoT-Geräte, inkl. aller Schnittstellen
- Hard- und Software aus dem Automobilbereich
- verschiedenste Funkprotokolle (z.B. WiFi, ZigBee, Bluetooth/BLE, LoRa), etc.

IT-Infrastrukturen und -komponenten

- Perimetersysteme
- Unternehmensnetzwerke
- Cloudumgebungen
- Hardening-Checks von Servern, etc.

Webanwendungen und Webdienste

- Webanwendungen
- REST APIs
- SOAP APIs, etc.

Mobile Applikationen

- Android Applikationen
- iOS Applikationen

Red-Teaming

- explorative Tests basierend auf definierten Angriffsszenarien
- Fokus auf Defensesysteme

Warum Ihr Euch für uns entscheiden solltet?

- **professionelles Testteam** (Zertifizierungen und langjährige Erfahrung)
- **Testlabor** für verschiedenste hardwarenahe Tests
- **thematisch breit aufgestellt**
- vorwiegend **manuelle Analyse** aus der **Perspektive eines realen Angreifers**

Sprecht uns gern an

Antje Winkler
Division Lead
Offensive Security
+49 351 86691-157
+49 173 6740786
antje.winkler@bdosecurity.de

BDO CYBER SECURITY