

Pentesting


Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de, Raum 149B
Version: 1.0



Folien: <https://delors.github.io/sec-pentesting/folien.de.rst.html>
<https://delors.github.io/sec-pentesting/folien.de.rst.html.pdf>
Fehler melden: <https://github.com/Delors/delors.github.io/issues>

1. Einführung

Bedrohungen^[1]

- Angriffsarten:
 - Ransomware
 - Wirtschaftsspionage
 -  *Advanced Persistent Threats*
 - (Distributed) Denial of Service (DoS/DDoS)
 - Spam und Phishing
 - Unterscheidung der Angreifer:
 - Hacker
 - Cracker („kriminelle Hacker“ oder Insider)
 - Script Kiddies
-

[1] [\[BSI_Bedrohungslage\]](#)

Pentest(ing)[2]

- Sicherheitstest von einzelnen Rechnern oder von Netzwerke jeglicher Größe.
- Prüft die Sicherheit von Systembestandteilen und Anwendungen.
- Durchführung mit Hilfe des Einsatzes von Mitteln und Methoden, um unautorisierten Zugriff zu erhalten.
(D. h. mit Methoden, die auch Angreifer verwenden!)
- erfordert Kenntnisse der Zielsysteme und der Zielumgebung
- wesentliche Schritte:
 1. Planung und Informationssammlung
 2. Auswahl der passenden Methoden und Werkzeuge
 3. Durchführung
 4. Analyse der Ergebnisse und Erstellung eines Berichts

Ein einfacher Scan nach Schwachstellen ist kein Pentest.

[2] Pentests machen nur Sinn, wenn ein IT Sicherheitskonzept existiert.

Ziele des Pentesting

- Identifikation von Schwachstellen:
 - technischer Natur
 - organisatorischer Natur
- Erhöhung der Sicherheit
- Zertifizierung der IT Sicherheit durch einen Dritten

Warnung

It wasn't raining when Noah built the ark.

—Howard Ruff

Der erste Schritt ist es vorbereitet zu sein. Ein Angriff wird kommen und wird zu einem Sicherheitsproblem führen!

Arten von Pentests

Black-Box

- Keine Informationen über das Zielsystem
- Informationsgewinnung ist Teil der Aufgabe
- „Simuliert einen Cyberangriff“

White-Box

- Umfangreiche Informationen werden bereitgestellt
- „Simuliert ggf. einen Insiderangriff“

Gray-Box

- Informationen, die ein normaler Nutzer sich erarbeiten kann, werden bereitgestellt
- „Simuliert einen Cyberangriff“
- ggf. besseres Kosten-Nutzen-Verhältnis

Nicht Teil dieser LV

- Pentests, die auf Social-Engineering basieren.
- Red Team vs. Blue Team

Red Team: Experten, die ein System angreifen.

Blue Team: IT Security Experten eines Unternehmens, die ein System verteidigen und dabei von entsprechenden Beratern unterstützt werden.

Ziel ist es, die Sicherheit des Systems zu erhöhen und festzustellen:

1. ob bzw. wie lange es gedauert hat bis der Angriff erkannt wurde,
2. wie lange es danach gedauert hat die Bedeutung des Angriffs einzuschätzen
3. und wie lange es abschließend gedauert hat bis das System wiederhergestellt und gesichert war.

Am Ende einer Übung müssen sich beide Teams austauschen, um den maximalen Lerneffekt zu erzielen!

Aufbau von Pentests nach BSI[3]

Klassifikationsschema des BSI:

Informationsbasis: Black-Box ↔ White-Box

Aggressivität: passiv scannend (keine Ausnutzung von Schwachstellen) ↔ aggressiv (Ausnutzung von Schwachstellen)

Umfang: Punktuelle Tests oder vollständige Tests

Vorgehensweise: verdeckt oder offensichtlich

Technik: Netzwerkzugang, physischer Zugang, Social Engineering

Ausgangspunkt: von außen oder innen

[3] [BSI_Penetrationstests]

Achtung!

Pentests können zu Störungen der normalen IT Prozesse führen.

Technische Risiken:

- DoS Attacken
- Systemabstürze

Achtung!

Pentester können auf unternehmenskritische Daten Zugriff erhalten.

Warnung

Advanced Persistent Threats (APT) sind schwer zu erkennen und klassische Pentests helfen nur bedingt.

2. Rechtliche Aspekte

Computerkriminalität und Strafrecht

- Computerkriminalität nimmt immer mehr zu
- Schaffung neuer Straftatbestände zwecks Generalprävention bisher nicht erfolgreich
- Strafrechtliche Verfolgung von Computerkriminalität ist schwierig; Beweisführung ist aufwendig und schwierig

Rechtslage^[4]

- „[...] sich unbefugten Zugang zu einem System zu verschaffen ist in Deutschland strafbar.“
(D.h. Pentests ohne explizite Erlaubnis sind illegal!)
- Pentests verlangen explizite schriftliche Erlaubnis zwischen Auftraggeber und Auftragnehmer
- Ein Auftraggeber kann nur für Systeme Pentests vergeben, für die er die Verantwortung trägt
- Pentests sind gesetzlich nicht vorgeschrieben
- Pentests sind jedoch geeignet um nachzuweisen, dass gesetzliche Vorgaben in Hinblick auf die IT Sicherheit eingehalten werden

Beim Einsatz von Cloud-Diensten ist es wichtig, dass der Auftraggeber die Erlaubnis hat, einen Pentest durchzuführen.

^[4] Es handelt sich hierbei um keine Rechtsberatung!

Rechtliche Vorschriften und Pentests

Pentests sind geeignet, um ggf. *nachzuweisen*, dass die rechtlichen Anforderungen in den folgenden Bereichen eingehalten werden:

- Handelsgesetzbuch (HGB)
 - Bestimmungen zu internen Kontrollsystemen (Abschnitt 4 GoBS)
 - Bestimmungen zur Datensicherheit (Abschnitt 5 GoBS)
 - Bestimmungen in Hinblick auf den Schutz vor Verlust und unberechtigte Veränderung
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

—§ 91 Abs 2 AktG

- Kreditwesengesetz

Nach § 44 Abs. 1 KWG kann der Themenbereich Internet-Sicherheit zum Gegenstand einer Prüfung gemacht werden, wenn Finanzdienstleistungen über das Internet zur Verfügung gestellt werden.

- Bundesdatenschutzgesetz (BDSG)

Datenschutzaudit[#]

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.

- Telekommunikationsgesetz (TKG)

Wer Telekommunikationsanlagen betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, hat bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze [...]

1. der [...]systeme gegen unerlaubte Zugriffe, [...]
2. gegen äußere Angriffe [...] zu treffen

—87 Abs. 1 TKG

GoBS: Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme AktG: Aktiengesetz

[5] Vergleichbare Aussagen finden sich auch im Staatsvertrag für Mediendienste (MDStV)

Pentests und strafrechtliche Vorschriften

■ Zugangskontrolldiensteschutzgesetz

Verbot von gewerbsmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten

Verboten sind 1.) die Herstellung, die Einfuhr und die Verbreitung von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, 2.) der Besitz, die technische Einrichtung, die Wartung und der Austausch von Umgehungsvorrichtungen zu gewerbsmäßigen Zwecken, 3.) die Absatzförderung von Umgehungseinrichtungen.

—§ 3 ZKDSG

■ Telekommunikationsgesetz

Einsatz von Netzwerk-Sniffen und das Abhören von Netzwerkverkehr ist ggf. strafbar, wenn keine Erlaubnis eingeholt wurde.

■ Betriebsverfassungsgesetz

Pentests sind ggf. dazu geeignet Überwachung und Leistungsbeurteilungen der Mitarbeiter (implizit oder explizit) durchzuführen. Eine Einbindung des Betriebsrats ist deswegen im Vorfeld erforderlich; auch wenn keine Intention oder Auswertung bzgl. Leistungsorientierung existiert!

Achtung!

Der Auftragnehmer hat die allgemeine Sorgfaltspflicht!

(Wenn er „aus Versehen“, die falschen IP Adressen angreift, ist der Pentester schuldig.)

Beauftragung von Pentests

- typischerweise handelt es sich um *eine entgeltliche Geschäftsbesorgung mit Dienstleistungscharakter*
- Vertragsgegenstand:
 - Zielsetzung (z. B. Identifikation von Schwachstellen, Erlangung einer Zertifizierung, Erhöhung der technischen Sicherheit)
 - Art des Pentests (z. B. siehe **Klassifikationsschema**)
 - Einzusetzende und auszuschließende Methoden
 - Aufwand (z. B. in Personentage) und Umfang bzw. Zeitraum in dem die Tests durchgeführt werden.
- ggf. durchführende Personen benennen (insb. bei Social-Engineering-Pentests)
- nur ein vertretungsberechtigter des Auftraggebers (z. B. Prokurist, Geschäftsführer) kann den Vertrag wirksam abschließen

Der Aufwand muss nicht deckungsgleich mit dem Zeitraum sein. Insbesondere wenn umfangreiche, automatisierte Scans eingesetzt werden, kann der Zeitraum sehr viel länger sein.

Referenzen

- [BSI_Penetrationstests] BSI Penetrationstests 2020
- [BSI_Bedrohungslage] BSI Lagebericht 2023