Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Handreichung Penetrationstests

2026

Danksagung

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung im TeleTrusT-Arbeitskreis "PenTests" sowie für die aktive Mitgestaltung dieser Handreichung.

Projektleitung

Kirchhoff, Jan-Tilo

Autoren und mitwirkende Experten (Auszug)

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Döringer, Georg - go-IT-Security
Di Filippo, Marco - whitelisthackers
Gladisch, Alexander - Deutsche Telekom MMS
Glemser, Tobias - secuvera
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Oppelland, Vincent - Haufe Lexware
Probst, Christian W. - RMTP IT-Beratung und Service
Schröder, Dennis - TÜV Informationstechnik
Franz, Tobias - TÜV Austria
Söbütay, Ersin - itWatch
Wojzechowski, Chris - Aware7

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Desweiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
E-Mail: info@teletrust.de
https://www.teletrust.de

© 2026 TeleTrusT

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Mit Hilfe von Penetrationstests können Organisationen Aspekte ihrer IT-Sicherheit systematisch prüfen und verbessern. Da IT-Systeme immer komplexer werden, die Gefahr durch Angriffe steigt und immer mehr spezifische Compliance-Anforderungen Penetrationstests einfordern, gewinnen diese zunehmend an Bedeutung. Sie zeigen frühzeitig auf, wo IT-Systeme und Anwendungen anfällig sind. Einmal aufgedeckt, können diese Schwachstellen behoben werden, bevor sie von Angreifern ausgenutzt werden.

Diese Handreichung des TeleTrusT-Arbeitskreises "PenTests" richtet sich an Firmen, Behörden und Dienstleister, die Penetrationstests planen, durchführen lassen oder in Auftrag geben möchten. Sie gibt praktische Ratschläge und hilft dabei, Penetrationstests gut zu organisieren und Gesetze sowie Standards zu beachten.

Ziel des Dokuments ist es, bei allen Beteiligten ein gemeinsames Verständnis dafür zu schaffen, wie Penetrationstests geplant und durchgeführt werden können. Die Handreichung ist als zusätzliches Hilfsmittel zu den bestehenden gesetzlichen Vorgaben gedacht und stellt keinen Ersatz für individuelle technische oder rechtliche Beratung dar.

Zur Unterstützung einer besseren Lesbarkeit wird, wie in anderen Handreichungen des Bundesverband IT-Sicherheit, das generische Maskulinum, verwendet. Die verwendete männliche Form bezieht sich gleichermaßen auf weibliche, männliche und diverse Personen.

Die einzelnen Abschnitte des Dokuments wurden von Autoren bzw. Autorengruppen mit unterschiedlichen beruflichen Hintergründen und Fachkenntnissen erstellt. Die sich daraus ergebenden sprachlichen Unterschiede spiegeln dies wider, sind jedoch keine Zeichen mangelnder inhaltlicher Abstimmung. Die Mitglieder des Arbeitskreises stehen gemeinsam hinter dem vollen Umfang der Texte.

1.1 Warum dieses Dokument?

Es gibt mittlerweile eine Vielzahl von Dokumenten, die versuchen zu beschreiben, was ein Penetrationstest ist. Die Praxis aus vielen Anfragen und Ausschreibungen zeigt, dass die Definitionen nicht geeignet sind, ein ausreichendes Verständnis für Penetrationstestprojekte aufzubauen. Penetrationstest ist kein geschützter Begriff. Somit gibt es mittlerweile eine Vielzahl von Anbietern am Markt, die in sehr unterschiedlicher Güte und mit sehr unterschiedlicher Expertise Penetrationstests anbieten.

Im TeleTrusT-AK "PenTests" hat sich eine Vielzahl von Experten aus renommierten Penetrationstestanbietern mit in Summe vielen 1.000 Projekttagen Erfahrung zusammengefunden, um eine praxisnahe Handreichung zu liefern. Das Ziel ist es, alle Interessierten, die Penetrationstests in einer methodisch sinnvollen Art und Weise durchführen wollen, sowie Auditoren, die die zielführende Ausführung von Penetrationstests bewerten müssen, zu unterstützen. Nicht zuletzt soll das Dokument auch angehende Penetrationstester aufklären und umfassende Informationen bereitstellen.

1.2 Was ist ein Penetrationstest?

Wie eingangs beschrieben, gibt es Unmengen an Quellen. Es wurden unter anderem die drei einschlägigen Dokumente des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwendet (Leitfaden Penetrationstests[1], IS-Penetrationstest[2], IS-Webcheck[3]). Andererseits gibt es in vielen Guides des National Institute for Standardisation (NIST) unterschiedliche Definitionen. Es wurde die ausführlichste im NIST SP 800-53[4] zu Rate gezogen.
Penetrationstests sind im Idealfall professionell durchgeführte Dienstleistungen, die sich Hackermethoden zu eigen machen. Sie unterscheiden sich signifikant von "Live-Hacking-Shows". Penetrationstests

[1] Praxis-Leitfaden: IT-Sicherheits-Penetrationstest https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html
[2] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html#doc454152bodyText1
[3] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html#doc454152bodyText1
[4] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

und Penetrationstester sind professionell ausgebildet und beherrschen auch Projektmanagement und Risikoaufklärung.

Der Begriff "Hacker" bezieht sich ursprünglich auf einen Tüftler im technischen Kontext. Alltagssprachlich - und insbesondere in den Medien - ist der Begriff jedoch meist negativ konnotiert und wird häufig als Synonym für Personen verwendet, die illegal in IT-Systeme eindringen.

Zur Abgrenzung hiervon, wird in diesem Dokument ausschließlich von Angreifern gesprochen.

In den Medien liest man heute fast täglich von Angriffen auf IT-Systeme. Ein Angreifer kann beinahe jede Organisation ins Visier nehmen. Er könnte dabei auf verschiedene Arten und Weisen vorgehen. Vielleicht versucht er, Zugangsdaten zu erraten. Oder er sendet E-Mails, um die Mitarbeiter zu täuschen (Phishing-Angriffe). Möglicherweise nutzt er gerade erst bekannt gewordene Schwachstellen in extern erreichbaren Systemen gezielt aus. Oder er kommt sogar vor Ort in das Firmengebäude. All diese Angriffsvektoren und mehr ließen sich auch mit einem Penetrationstest prüfen. "Wie viel kostet es, unsere Organisation zu testen?" ist eine übliche Anfrage. Allerdings ist diese so nicht zu beantworten. Es ist nicht sinnvoll, alle vorstellbaren Angriffsvektoren in einem einzigen Penetrationstest zu prüfen. Je nach Komplexität der Organisation sollten Penetrationstests unterschiedlicher Teilbereich oder sogar einzelner Anwendungen als separate Projekte geplant und beauftragt werden. So lassen sich Aufwände und Kosten besser strukturieren und kontrollieren. Schließlich müssen auch die im abschließenden Ergebnisbericht zusammengefassten Erkenntnisse in Korrekturen und Verbesserungsmaßnahmen umgesetzt werden können, ohne die Auftraggeber zu überfordern.

1.3 Grundsätzliche Attribute eines Tests

Im Gegensatz zum echten Angreifer haben Auftraggeber und die Penetrationstestanbieter einen großen Vorteil: Sie können miteinander sprechen, um die Voraussetzungen für eine effizienten und gleichzeitig möglichst tiefgehende Prüfung mit hohem Erkenntnisgewinn zu erarbeiten. Man nennt das Scoping, also Planung der Prüfung. Ziel des Scopings eines Penetrationstests ist es, einen möglichst gut ausdefinierten Rahmen für den Penetrationstest zu schaffen, um den explorativen Charakter eines solchen Tests genau zu definieren.

Für jeden Test sollten folgende Attribute festgelegt werden (ausgewählte Beispiele finden sich im Abschnitt8 "Module"):

Ein Experte führt einen Angriff durch

- gegen ein definiertes Ziel

Was soll getestet werden? Die im Internet stehenden Systeme? Eine oder mehrere Webanwendungen? Ein WLAN-Gastzugang? Die neue Produktionslinie mit Cloud-Anbindung? Der Auftraggeber sollte die Prüfziele möglichst klar und eindeutig formulieren. So wäre "unsere Webanwendungen" nicht ausreichend. "Unser Onlineshop" wäre schon viel besser.

- auf Grundlage einer sinnvollen Informationsbasis

Die etablierten Begriffe "Black Box" und "White Box" werden seit vielen Jahren um "Grey Box" ergänzt. Sie beschreiben, auf welcher Informationsbasis ein Test durchgeführt wird. Für die Beschreibung von Angreifermodellen ist diese Einordnung grundsätzlich sinnvoll: Externe Angreifer haben häufig wenige oder keine internen Kenntnisse, während Innentäter oder sehr gut vorbereitete Angreifer über umfangreiche Informationen verfügen können.

Für die praktische Durchführung eines Penetrationstests ist jedoch nicht die abstrakte Box-Kategorie entscheidend, sondern die Frage, welche Informationsbasis für das jeweilige Testziel sinnvoll und effizient ist. Diese kann je nach Prüfmethode und Testmodul unterschiedlich ausfallen. Es wird daher bewusst auf eine pauschale Einordnung in Black-, Grey- oder White-Box-Tests verzichtet. Stattdessen beschreibt das Dokument in den einzelnen Testmodulen konkret, welche Informationen für eine zielgerichtete, aussagekräftige und wirtschaftliche Prüfung benötigt werden.

- mit definierter Berechtigung

Wer ist der Angreifer, der simuliert werden soll? Beispiel Onlineshop: Hier können es möglicherweise ein anonymer Angreifer und Kunden des Onlineshops sein; ggf. auch Dritte, die gemäß Rollen und Berechtigungskonzept Zugriff auf Supportfunktionen haben, oder die eigenen Mitarbeiter, die den Onlineshop pflegen.

- von einem festgelegten Ausgangspunkt

Von wo greifen der oder die Angreifer zu, deren Berechtigung zuvor definiert wurde? Es muss sichergestellt werden, dass die Penetrationstester vergleichbare Ausgangspunkte nutzen. So kann zum Beispiel bei internen Prüfungen ein interner Netzwerkzugang oder ein Standardarbeitsplatz notwendig sein, andere Module bringen andere Voraussetzungen mit sich. Für den Onlineshop wäre ein Angriff aus dem Internet am wahrscheinlichsten.

- für einen definierten Zeitraum mit festgelegtem Aufwand

Da den Penetrationstestern in der Regel weniger Zeit zur Verfügung steht als realen Angreifern, sollte der Anspruch auf Realismus nicht übertrieben werden. Es ist daher üblich, den Zeitraum, den Aufwand oder beides abzustimmen und Tester mit breiten Informationen über die Prüfobjekte auszustatten, Zugangsdaten bereitzustellen und Schutzmechanismen zu deaktivieren. Mit entsprechendem Aufwand wird es einem Penetrationstester wie einem realen Angreifer gelingen, diese Informationen zu erhalten, um zum Beispiel etwaige Firewall und Filter zu umgehen. Diese Zeit steht dann jedoch nicht mehr für Tests am eigentlichen Prüfobjekt zur Verfügung. Zusätzlich ändert sich der Dokumentationsaufwand mit der Anzahl und Komplexität der gefundenen Schwachstellen. Daher spricht man von "Time Boxed" Testing. In einer definierten Zeit werden möglichst risikoorientiert Schwachstellen aufgedeckt und dokumentiert.

- zu einem bestimmten Zeitpunkt

Ein Penetrationstest ist eine Momentaufnahme, die den Zustand im Zeitraum der Durchführung feststellt. Es ist also wichtig, den richtigen Zeitpunkt im Lebenszyklus des Prüfobjekts festzulegen - bei der Einführung einer neuen Komponente oder Lösung beispielsweise nach Fertigstellung aller geplanten Funktionen und so weit vor dem Einführungstermin, dass genügend Zeit bleibt, notwendige Korrekturen vorzunehmen. Da Anwendungen und IT-Systeme, aber auch die Vorgehensweise der Angreifer permanenter Veränderung unterliegen, sollten Penetrationstests außerdem in angemessenen Zeiträumen wiederholt werden.

- mit den gleichen technischen Methoden wie reale Angreifer

Angreifer nutzen öffentlich bekannte oder neu entdeckte Schwachstellen aus, um ihre Ziele zu erreichen. Penetrationstester nutzen idealerweise die gleichen Werkzeuge und Methoden, um dieselben Schwachstellen identifizieren zu können, nach einer abgestimmten Vorgehensweise. Hierbei können technische Schwachstellen oder Berechtigungsschwachstellen des Zielsystems ausgenutzt oder auch weitere Komponenten gezielt angegriffen werden

- mit erwartbaren Ergebnissen

Das Auffinden von neuen Schwachstellen, sogenannter "Zero-Days", ist meist nicht im Umfang eines Penetrationstests vorgesehen. Es handelt sich entweder um Zufallsfunde, deren weitere Behandlung im Anhang "Responsible Disclosure" weiter diskutiert wird, oder um spezielle Formen von entwicklungsnahen Sicherheitsuntersuchungen oder Produktprüfungen, bei denen ein entsprechender Aufwand für explorative Untersuchungen von vornherein kalkuliert werden muss.

Es gibt, je nach Prüfobjekte, unterschiedliche Vorgehensweisen, die eingesetzt werden können. So könnte bei einer Prüfung des Webshops der Shop auf technische Schwachstellen und Fehler im Berechtigungsmodell geprüft werden. Es könnte auch geprüft werden, wie widerstandsfähig der Shop gegen Massenanfragen (Distributed Denial-of-Service, DDoS) ist - gleicher Prüfgegenstand, zwei Vorgehensmodelle. Insofern gibt es nicht den einen richtigen Testaufwand. Details dazu sind in den Folgekapiteln zu finden. Auf jeden Fall sollte ein klarer Zeitplan mit dem Dienstleister vereinbart werden.

Die folgende Abbildung liefert eine Übersicht der hier angesprochenen Attribute und setzt sie in Beziehung zur Abbildung 1 auf S. 13 der BSI-Studie "Durchführungskonzept für Penetrationstests"[5]:

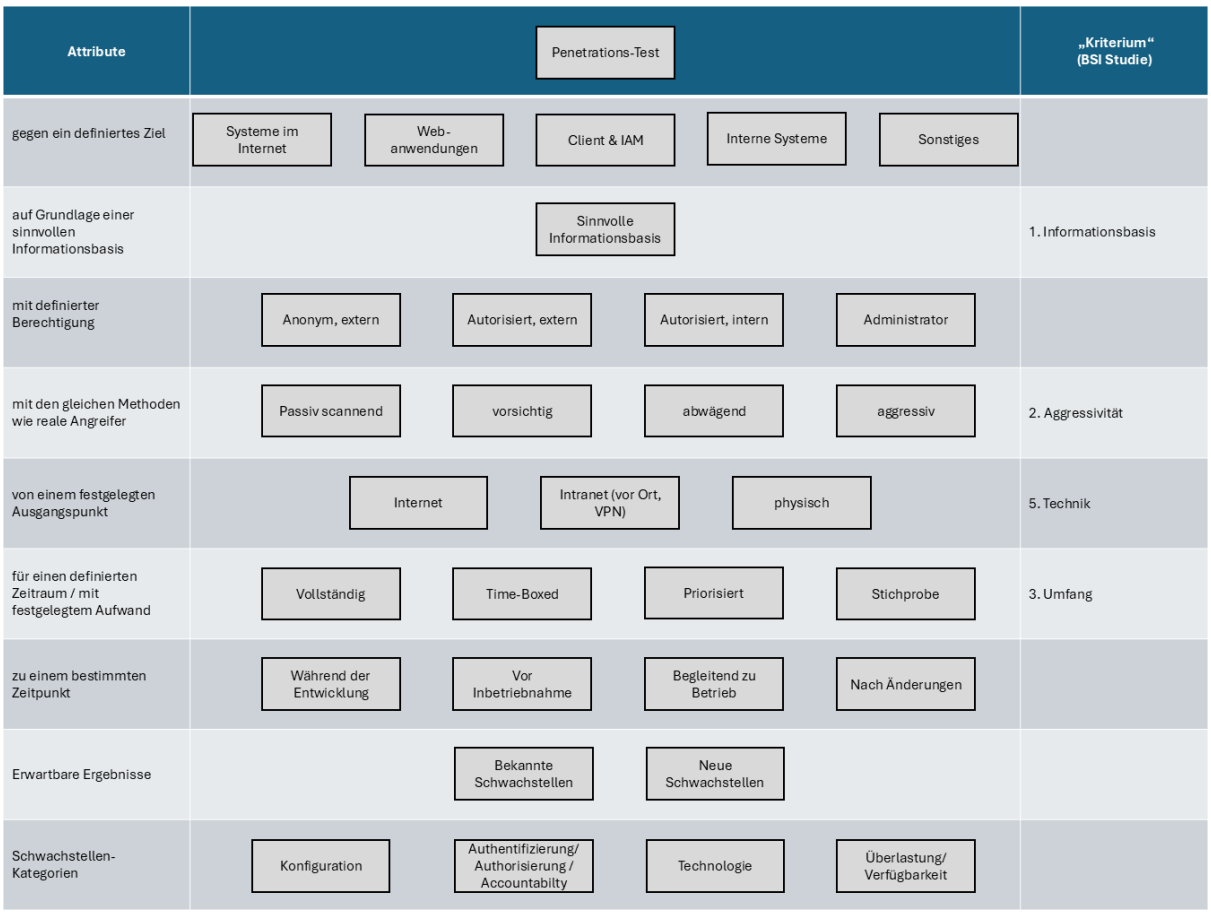

Abbildung 1: Attribute eines Penetrationstests

1.3.1 Abgrenzung zu verwandten Dienstleistungen

Vulnerability Scan
Ein Vulnerability Scan ist ein rein automatisierter Prozess, der IT-Systeme auf bekannte Schwachstellen überprüft. Dabei werden Scanner-Tools eingesetzt, um Netzwerkkomponenten, Server, Anwendungen und andere digitale Assets auf Sicherheitslücken wie veraltete Software, Fehlkonfigurationen oder schwache Passwörter zu analysieren. Ziel ist es, eine umfassende Übersicht über potenzielle Risiken zu erhalten, die anschließend priorisiert und behoben werden können.

Eine rein automatisierte Schwachstellenanalyse mit generierten Berichten ist kein echter Penetrationstest. Bei einem Penetrationstest werden die potenziellen Schwachstellen weiter analysiert: Es erfolgen eine Eliminierung von False Positives und eine kontextsensitive Bewertung auf potenzielle Auswirkungen durch erfahrene Experten.

Vulnerability Assessment
Ein Vulnerability Assessment ist ein umfassender Prozess zur Identifikation, Bewertung und Priorisierung von Schwachstellen in IT-Systemen, Netzwerken und Anwendungen. Es kombiniert in der Regel automatisierte Vulnerability-Scanning-Tools mit manueller Analyse, um die Ergebnisse zu validieren, False Positives zu eliminieren und Schwachstellen in ihrem Kontext besser zu bewerten. Im Gegensatz dazu ist ein rein automatisiertes Vulnerability Scanning auf die maschinelle Identifikation von Schwachstellen beschränkt, ohne eine tiefere Analyse oder Priorisierung durchzuführen. Ein Penetrationstest geht noch einen Schritt weiter, indem er Schwachstellen aktiv ausnutzt, um die tatsächliche Ausnutzbarkeit und potenzielle Auswirkungen zu bewerten. Während ein Vulnerability Assessment breiter

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=2

angelegt ist und auf die Identifikation und Bewertung abzielt, liefert ein Penetrationstest praktische Erkenntnisse zur realen Sicherheitslage durch simulierte Angriffe.

Attack Surface Management
Attack Surface Management (ASM) ist ein kontinuierlicher, automatisierter Prozess zur Identifikation, Überwachung und Reduzierung der gesamten digitalen Angriffsfläche einer Organisation. Es umfasst die Erkennung aller digitalen Assets sowie die Bewertung und Priorisierung von Risiken, um potenzielle Schwachstellen frühzeitig zu beheben. Im Gegensatz zu zeitlich begrenzten Sicherheitsüberprüfungen, wie Penetrationstests, liegt der Fokus von ASM auf der dauerhaften, proaktiven Überwachung und Minimierung von Angriffsvektoren. Meist steht dabei die aus dem Internet erreichbare Infrastruktur von Unternehmen im Fokus. Vulnerability Scans sind häufig Teil von ASM-Lösungen.

Red Teaming
Red Teaming geht über den traditionellen Penetrationstest hinaus, indem es die Reaktionsfähigkeit und Abwehrmechanismen einer Organisation gegen fortgeschrittene und gezielte Angriffe bewertet. Ein Red Teaming ermöglicht die vollumfängliche und vor allem realistische Analyse, wie verwundbar Organisationen gegenüber Aktionen professioneller Gruppierungen und Cyber-Kriminellen wirklich sind. Red Teaming umfasst oft längerfristige und umfassendere Angriffe, während ein Penetrationstest spezifische Ziele in einem begrenzten Zeitraum untersucht. Das Ziel eines Red Teamings ist, das Blue Team zu trainieren. Insofern gilt eine einfache Regel: Wenn kein Blue Team vorhanden ist, braucht es kein Red Teaming. Eine Organisation benötigt einen hohen Reifegrad, damit das mit einem Red Teaming prinzipbedingt einhergehende Risiko gemeinsam durch eine geprüfte Organisation, deren Blue Team und das Red Teaming beherrscht werden kann. Wenn ein Unternehmen über die Einführung von Red Teaming nachdenkt, sollten regelmäßige Penetrationstests bereits ein etablierter Prozess sein und kein Neuland. Im Vergleich zu einem typischen Penetrationstest geht es nicht darum, möglichst viele Schwachstellen in einem definierten Scope aufzudecken, sondern einen Weg zur Erreichung des Angriffsziels zu finden.

Audit
Ein Audit ist eine systematische Überprüfung und Bewertung von Prozessen, Systemen und Kontrollen, um die Einhaltung von Standards und Richtlinien wie z.B. der ISO 27001 oder auch technischer Common-Practices wie den CIS-Benchmarks sicherzustellen. Im Unterschied zum Penetrationstest erfolgt ein Audit in der Regel auf Basis von Dokumenten und Interviews. Im Einzelfall wird er ergänzt durch die in Augenscheinnahme von Konfigurationsdaten und Überwachungs- sowie Wartungsprotokollen. Weitergehende technische Prüfungen sind nicht Bestandteil von Audits.

Threat Led Penetration Testing (TLPT)
TLPT ist ein Begriff, der in der Regulierung der Finanzwelt[6] definiert wurde. Nach DORA, Art. 3 (17) Definitionen beschreibt TLPT "einen Rahmen, der Taktik, Techniken und Verfahren realer Angreifer, die als echte Cyber-Bedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht." Im Zuge der DORA-Einführung wurde auch das TIBER-EU[7]-Rahmenwerk überarbeitet, das zahlreiche Hinweise und Best Practices für die Durchführung von TLPT beinhaltet. Weitere Hinweise zu regulatorischen Vorgaben sind im Abschnitt "Gesetzgebungen und Normen, die Penetrationstests fordern oder nahelegen" zu finden.

Social Engineering
Social Engineering konzentriert sich auf die Manipulation von Menschen, um Zugang zu vertraulichen Informationen zu erhalten. Diese Manipulation ist ein sehr sensibler Punkt. Ethisch ist eine Prüfung auf individuelle Fehler von Mitarbeitern oft schwer zu verargumentieren. Im Regelfall prüft ein Penetrationstest technische Schwachstellen. Die Erkenntnisse aus Social-Engineering-Kampagnen lassen sich häufig mit Audits ebenfalls erzielen. In speziellen Fällen kann - erneut einen hohen Reifegrad der Organisation vorausgesetzt - aber auch Social Engineering zu Erkenntnissen führen.

Weiterhin wird Social Engineering im Rahmen von Angriffssimulationen (Red Teaming) oder im Umfeld von Awareness Trainings angewendet.

[6] BaFin - Testen der digitalen operationalen Resilienz einschließlich Threat-Led Penetration Testing (TLPT)
[7] What is TIBER-EU?

1.3.2 Weitere Begrifflichkeiten

Lateral Movement
Lateral Movement bezieht sich auf Techniken, die Angreifer verwenden, um sich von System zu System durch ein Netzwerk zu bewegen, nachdem sie initialen Zugang erlangt haben. Entsprechend der Eingangsdefinition hat ein Penetrationstest einen Ausgangspunkt und ein Ziel. Beim Lateral Movement verschiebt sich der Ausgangspunkt. Aus Planungssicht entsteht ein neues Szenario. Ein Beispiel: Testet man z.B. VPN-Server, würden sich echte Angreifer auf die Lauer legen und warten, bis Schwachstellen auftreten und gezielt angreifen. Das lässt sich mit einem Penetrationstest nicht simulieren. Daher wäre zunächst der VPN-Server zu prüfen. Sofern das Risiko "was passiert, wenn ein VPN-Server übernommen wird" geprüft werden soll, ist das auch prüfbar - aber nicht mit einem "Wenn-dann-Ablauf" wie bei einem Lateral Movement. Lateral Movement ist daher als Teilaufgabe eines internen Penetrationstests mit dem Ausgangspunkt Active Directory oder in Red Teaming sinnvoll.

Exploiting
Exploiting ist das gezielte Ausnutzen von identifizierten Schwachstellen, um Kontrolle über Systeme zu erlangen. Meist geht vom Exploiten der Schwachstellen kein relevanter Erkenntnisgewinn aus. Manche Exploits funktionieren auch nicht direkt, sodass man Zeit für das Anpassen von Exploits aufwenden müsste. Das vollständige Entwickeln von Exploits auf Basis einer im Rahmen eines Tests erstmals identifizierten Schwachstelle (Zero-Day) ist sehr zeitaufwendig und daher im begrenzten Zeitrahmen eines Penetrationstests in der Regel nicht möglich. Das Schließen einer Schwachstelle sollte im Vordergrund stehen. Es gibt eine begrenzte Anzahl von Fällen, in denen das Ausnutzen einen Erkenntnisgewinn bietet, z.B., um Angriffspfade im Rahmen eines Lateral Movements nachzustellen. Das genaue Vorgehen muss im Einzelfall mit dem Auftraggeber abgestimmt werden.

Static Application Security Testing (SAST)
SAST ist eine Form der Sourcecode-Analyse, die den Quellcode einer Anwendung auf Sicherheitslücken und Schwachstellen überprüft. Im Gegensatz dazu ist ein Penetrationstest dynamisch und testet die Anwendung im laufenden Betrieb, ohne Zugriff auf den Quellcode zu benötigen. SAST ist insbesondere für Individualsoftware ein wertvoller Blick. Manchmal wird SAST auch als "White-Box-Penetrationstest" klassifiziert.

2 Motivationsfaktoren für Penetrationstests

Mittlerweile ist ein Alltag ohne die Nutzung von vernetzten Computern und Smartphones kaum noch vorstellbar. Ob bewusst oder unbewusst, sind damit auch Prozessabläufe in den meisten Unternehmen von einer funktionierenden und sicheren IT-Infrastruktur abhängig. Leider fällt die Kritikalität der IT-Infrastruktur häufig erst dann auf, wenn einmal etwas nicht funktioniert und der Regelbetrieb kurz- oder mittelfristig gestört wird. Sicherlich hat fast jeder schon einmal zusätzliche Arbeit gehabt, weil eine wichtige Datei nicht mehr lesbar war und neu erstellt werden musste. Im Vergleich dazu sind die Schäden, die durch gezielte Angriffe auf IT-System verursacht werden, exponentiell größer und im schlimmsten Falle existenzbedrohend. Eigentlich sollte das genug Motivation bieten, sich mit dem Thema IT-Sicherheit auseinanderzusetzen. Erfahrungen von Dienstleistern im Bereich Penetrationstests zeigen jedoch, dass häufig erst ein Schadensfall eingetreten sein muss, um das Bewusstsein dafür zu schärfen. Dabei sind Penetrationstests an sich ein hervorragendes Mittel, um verdeckte Mängel in der Sicherheit aufzudecken und Korrektur- und Gegenmaßnahmen zu ergreifen, um potenzielle Angriffe zu erschweren.

2.1 Gesetzgebungen und Normen, die Penetrationstests fordern oder nahelegen

Nachfolgend eine Übersicht über gesetzliche Regelungen, Richtlinien und Standards, die eine Verpflichtung zu einem Penetrationstest entweder direkt vorsehen oder diesen im Rahmen angemessener technischer und organisatorischer Maßnahmen nahelegen. Penetrationstests gelten dabei häufig als "Best Practice", um Sicherheitsanforderungen nachvollziehbar umzusetzen und zu dokumentieren. Sofern eine oder mehrere dieser Regelungen Anwendungen finden, müssen diese bei der in Abschnitt "3.3" beschriebenen Festlegung von Art und Umfang der Tests berücksichtigt werden.

1. Datenschutz-Grundverordnung (DSGVO / GDPR)
- Art. 32 DSGVO verlangt "angemessene technische und organisatorische Maßnahmen" (TOMs) zur Sicherung personenbezogener Daten. Ein Penetrationstest kann eine solche Maßnahme darstellen, insbesondere zur Risikobewertung und Schwachstellenanalyse. Erwägungsgrund 83 hebt hervor, dass Systeme regelmäßig auf Schwachstellen geprüft werden sollen.

Fazit: Kein Pflicht-Penetrationstest, aber sinnvoll bei Datenpannen oder Prüfungen

2. IT-Sicherheitsgesetz (IT-SiG 2.0, Deutschland)
Gilt für KRITIS-Betreiber (kritische Infrastrukturen), z.B. Energie, Gesundheit, Finanzen. Verpflichtet Unternehmen zur Umsetzung von angemessenen Schutzmaßnahmen. Penetrationstests sind eine bewährte Methode, um die Wirksamkeit solcher Maßnahmen zu überprüfen.

Fazit: Spätestens bei der BSI-Kontrolle ist es sehr hilfreich, auf einen dokumentierten Penetrationstest verweisen zu können.

3. ISO/IEC 27001
International anerkannter Standard für Informationssicherheits-Managementsysteme (ISMS). Verlangt regelmäßige Bewertung von Sicherheitsrisiken und Prüfungen der Wirksamkeit von Sicherheitsmaßnahmen. Penetrationstests sind typischerweise Bestandteil dieser Prozesse.

Fazit: Zwingend, wenn ein Unternehmen nach ISO 27001 zertifiziert ist oder sich zertifizieren will

4. NIS2-Richtlinie (EU)
Richtet sich an systemrelevante Unternehmen in der EU, auch außerhalb von KRITIS. Erfordert u. a. regelmäßige Sicherheitsüberprüfungen, Incident Response und Risikomanagement.

Fazit: In der Umsetzung kann ein Penetrationstest notwendig sein, um die Anforderungen zu erfüllen.

5. Digital Operational Resilience Act (DORA)
Durch DORA regulierte Unternehmen müssen gem. Art. 25 Abs. 1 als Teil ihres Programms, mit dem die digitale Resilienz getestet wird, u. a. auch Schwachstellen- sowie Penetrationstests durchführen. Die Aufsichtsbehörden können von ihr bestimmten Finanzunternehmen auferlegen, sog. "Threat-Led Penetrationstests" (TLPT) durchzuführen (Art. 26 Abs. 1 DORA). Diese müssen mindestens alle drei

Jahre durchgeführt werden, und jeder dritte Test muss durch einen externen Tester durchgeführt werden (Art. 26 Abs. 8, S. 2). Bedeutsame Kreditinstitute (Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013) müssen immer externe Tester einsetzen (Art. 26 Abs. 8, S. 3). Die Anforderungen an die Tester sind in Art. 27 geregelt.

Fazit: In der Praxis wird von der BaFin regelmäßig ein Nachweis über durchgeführte Penetrationstests verlangt.

6. TISAX (für die Automobilindustrie)
Teilnehmer der TISAX-Zertifizierung müssen die Angemessenheit der Sicherheitsmaßnahmen nachweisen.

Fazit: Penetrationstests sind hier Best Practice, wenn nicht sogar Voraussetzung.

7. Cyber Resilience Act (CRA, EU) - seit Dezember 2024 in Kraft
Der Cyber Resilience Act verpflichtet Hersteller und Anbieter digitaler Produkte mit "digitalen Elementen" - etwa Software, IoT-Geräte oder eingebettete Systeme - zur Umsetzung und Nachweisführung angemessener Cyber-Sicherheitsmaßnahmen über den gesamten Lebenszyklus ihrer Produkte hinweg.

Der CRA unterscheidet dabei zwischen zwei Risikoklassen:

a) Allgemeine Produkte ("non-critical")
Kein ausdrücklicher Penetrationstestzwang - aber faktisch notwendig, um die Sicherheitsanforderungen nachweisbar und revisionssicher zu erfüllen, insbesondere bei kritischen Produkten.

b) Kritische Produkte der Klasse I und II
Es bestehen erhöhte Anforderungen an technische Dokumentation, Bedrohungsanalysen und Schutzmechanismen. Es gibt eine verpflichtende Konformitätsbewertung durch eine benannte Stelle für viele Produkte der Klasse II. Umfassende Sicherheitsprüfungen sind unerlässlich - darunter explizit Penetrationstests und Code-Analysen.

Fazit: Kein ausdrücklicher Penetrationstestzwang - aber faktisch notwendig, um die Sicherheitsanforderungen nachweisbar und revisionssicher zu erfüllen, insbesondere bei kritischen Produkten.

8. Weitere Normen und Rahmenwerke, in denen Penetrationstests empfohlen werden:

- BSI IT-Grundschutz (DE)
- OWASP ASVS / SAMM
- PCI-DSS (für alle, die Kreditkartendaten verarbeiten)
- HIPAA (USA, Gesundheitsdaten)
- SOC 2 (USA, IT-Dienstleistungen)

Fazit: Wer nach branchenspezifischen oder internationalen Standards arbeitet, wird um regelmäßige Penetrationstests kaum herumkommen.

3 Voraussetzungen von Penetrationstests, insbesondere zu Dokumentation, Scope und Risikoabschätzung

Der primäre Zweck eines Penetrationstests liegt in der Identifikation von Schwachstellen und Sicherheitslücken innerhalb eines Systems, einer Applikation oder einer IT-Infrastruktur. Diese Tests zielen darauf ab, die Wirksamkeit vorhandener Sicherheitsmaßnahmen zu bewerten und potenzielle Angriffsvektoren zu identifizieren. Ein wichtiger Aspekt dieser Tests ist die Sicherstellung der Compliance mit gesetzlichen und regulatorischen Anforderungen, was das Risiko rechtlicher Konsequenzen verringert. Außerdem ist es wichtig, diese Tests mit der Auftragslage und dem täglichen Geschäft abzustimmen, so dass das Risiko einer Beeinträchtigung des Geschäftsbetriebs minimiert wird.

3.1 Rechtliche Genehmigungen

Vor dem Beginn eines Penetrationstests müssen alle relevanten rechtlichen Aspekte geklärt sein. Dies umfasst eine mögliche Einbeziehung von Softwareherstellern und anderen Drittanbietern, deren Systeme getestet werden oder indirekt betroffen sein könnten. Zudem sind alle Anforderungen aus Branchenstandards, Verträgen, Richtlinien und Vorschriften zu berücksichtigen, die für das Unternehmen verbindlich sind.

Um rechtliche Konflikte zu vermeiden und die Vertraulichkeit der Testergebnisse zu gewährleisten, ist es unerlässlich, schriftliche Genehmigungen einzuholen und Vertraulichkeitsvereinbarungen mit beteiligten Firmen und Mitarbeitern abzuschließen. Darüber hinaus sollte bei Vertragsabschluss bereits festgelegt werden, wer in welchem Umfang Zugang zu den Testergebnissen erhält (z.B. interne Teams, Hersteller). Diese Klärung kann nur der Auftraggeber herbeiführen.

Weitere Details zu vertraglichen und rechtlichen Aspekten sind unter Abschnitt 5 "Vertragliches" zu finden.

3.2 Technische Voraussetzungen

Bei der Vorbereitung auf einen Penetrationstest gibt es unterschiedliche technische Voraussetzungen, wie z.B. Netzwerkzugang, Systeminformationen, Testumgebung, Zugangsdaten, Sicherheitsrichtlinien, Backup-Systeme, Monitoring, Logging, Ressourcenverfügbarkeit und Patch-Management, die Kunden beachten sollten, um sicherzustellen, dass der Test effektiv durchgeführt werden kann.

3.3 Art und Umfang der Tests

Der Umfang eines Penetrationstests muss klar definiert sein, um sicherzustellen, dass alle relevanten Systeme und Netzwerke abgedeckt werden. Mögliche Varianten von Penetrationstests wurden bereits im Abschnitt 1.3 genauer beschrieben. Im dort angesprochenen, dem Test vorausgehenden Scoping müssen darüber hinaus die zu prüfenden Systeme und Netzwerke genau definiert werden. Dabei ist es wichtig, auch möglicherweise auszuschließende Angriffsvektoren und Ziele festzulegen.

3.4 Bereitstellung von Informationen und Zugängen

Eine detaillierte technische Vorbereitung ist in jedem Fall entscheidend für den Erfolg eines Penetrationstests. Dies umfasst die Dokumentation der aktuellen Systemarchitektur und der spezifischen Konfigurationen, wie z.B. Netzwerkdiagramme, IP-Adressenbereiche, Quellcodes und die Bereitstellung aller notwendigen Zugangsdaten für das Penetrationstestteam, entsprechend der für den konkreten Penetrationstest ausgewählten Attribute (siehe Abschnitt 1.3).
Diese Dokumentation ist auch wesentlich, um die Ergebnisse eines einzelnen Tests sowie die zeitliche und qualitative Entwicklung von Testergebnissen zu dokumentieren und bewerten zu können.

3.5 Risikobewusstsein

In Verbindung hiermit muss eine sorgfältige Risikoabschätzung erfolgen, um die möglichen Auswirkungen des Tests auf den Betrieb zu bewerten und sicherzustellen, dass die Risikotoleranz des Unternehmens nicht überschritten wird. Wichtige Aspekte sind hier die Risikotoleranzstufen des Unternehmens, kritische Vermögenswerte, insbesondere eine Folgenabschätzung für den Geschäftsbetrieb während des Tests und insbesondere danach als Folge von möglichen Systemausfällen oder Datenschäden. Selbst bei sorgfältigster Planung und ausschließlichem Einsatz von qualifiziertem Personal können Störungen des Regelbetriebs im Rahmen der Tests nicht ausgeschlossen werden, Details dazu sind in Abschnitt "Haftungsfreistellung" zu finden. Dies gilt insbesondere dann, wenn Tests in der produktiven Umgebung durchgeführt werden müssen, sei es, weil keine gesonderten Testsysteme zur Verfügung stehen oder andere Gründe dies zwingend erforderlich machen. Die Durchführung von Tests auf Entwicklungs- oder Staging-Systemen erlaubt es den Penetrationstestern, offensiver vorzugehen, da etwaige Fehlfunktionen nicht zu einer Störung des laufenden Betriebs führen. Damit valide Ergebnisse erzielt werden, ist es zwingend erforderlich, dass die getesteten Prüfobjekte mit der Konfiguration des Produktivsystem (ggf. auch der Hardware) übereinstimmen. Datenbanken sollten in diesem Falle immer mit anonymisierten oder pseudonymisierten Testdaten gefüllt werden, um Datenschutzvorfälle durch den Test zu vermeiden. Für vermeintlich bekannte Schwachstellen und Sicherheitslücken muss hierbei bewertet werden, in welchem Umfang diese vorab dokumentiert und an das Testteam kommuniziert werden. Ein Vorteil einer offenen Kommunikation ist eine eventuelle umfassendere Erfassung des Umfangs vorhandener Lücken. Ein Nachteil ist unter anderem, dass die durchgeführten Tests bei Kenntnis solcher Lücken eventuell nicht in dem erwarteten Umfang durchgeführt werden.

Schließlich sollte in die Risikobewertung auch der Umgang mit den Ergebnissen der Tests einbezogen werden. In der Regel erfordert die Beseitigung der aufgedeckten Schwachstellen einen gewissen Aufwand, im schlimmsten Fall müssen einzelne Funktionen oder Dienste vorübergehenden deaktiviert werden, was zu Beeinträchtigung der regulären Geschäftsprozesse führen kann.

3.6 Testplan

Vor der Durchführung des Tests muss das Penetrationstestteam einen Testplan erstellen. Der Testplan sollte detailliert die geplanten Testmethoden, Werkzeuge und Zeitpläne beschreiben. Inwieweit dieser Testplan mit dem Betreiber der getesteten Systeme über die Benennung der Systeme und den Zeitplan hinaus geteilt wird, hängt von der Zielsetzung des Tests und den Systemen ab und muss im Einzelfall geklärt werden.

3.7 Kommunikation

Vor, während und nach der Durchführung des Tests ist eine effektive Kommunikation zwischen dem Penetrationstestteam und dem Unternehmen unerlässlich. Ein zentraler Ansprechpartner sollte benannt werden, der als Schnittstelle zwischen beiden Parteien fungiert. Zusätzlich sollte ein Notfallplan vorhanden sein, um auf unerwartete kritische Vorfälle während des Tests reagieren zu können. Hierfür ist es unerlässlich, die entsprechenden Kontaktdaten auszutauschen und Erreichbarkeitszeiten mit den Arbeitszeiten der Tester abzugleichen. Bei Tests an produktiven oder besonders kritischen Systemen ist zu empfehlen, auch eine Stellvertretungsregelung oder Eskalationsstufen zu definieren, sollte die geplante Erreichbarkeit doch einmal nicht gegeben sein (siehe auch Abschnitt "Verfügbarkeit und Erreichbarkeit").

3.8 Dokumentationen

Der Bericht fasst die Ziele (Scope), Verlauf und Ergebnisse der durchgeführten Tests zusammen und ist damit das wichtigste Element des gesamten Penetrationstestauftrags. Daher wird diesem wichtigen Thema ein eigener Abschnitt "Bericht (Mindestanforderungen)" gewidmet. In der Regel stellt der Bericht eine Mängelbeschreibung dar. Das heißt, Testfälle ohne Auffälligkeiten werden nicht aufgeführt. Sollte eine vollständige Dokumentation aller Testfälle gewünscht sein, muss dies vom Auftraggeber im Rahmen des Scopings mitgeteilt werden, um den Mehraufwand korrekt zu berücksichtigen.

4 Wie finde ich einen Dienstleister?

Einen geeigneten Anbieter für Penetrationstests zu ermitteln, kann eine Herausforderung sein. Aus diesem Grund werden nachfolgend einige wichtige Merkmale und Kriterien aufgezeigt, welche die Entscheider für ihre jeweilige Organisation beachten sollten. Im Vorfeld des Auswahlprozesses sollten idealerweise der IT-Sicherheits-Reifegrad der eigenen Organisation sowie die Ziele, die Budgetgrenzen und weitere organisatorische Rahmenbedingungen für den zu beauftragenden Penetrationstest klar sein.

4.1 Technische Kompetenz, Erfahrung und Zertifizierungen

Für die Auswahl eines passenden Anbieters von Penetrationstests sind die technische Kompetenz, die Erfahrung und die Zertifizierungen wichtige Qualifikationsmerkmale.

4.1.1 Zertifizierungen

Unternehmens- und Personenzertifikate sind ein gutes und leicht vergleichbares Merkmal eines Anbieters. Sie allein reichen jedoch nicht aus, da sie für die jeweilige Organisation möglicherweise nicht entscheidend sind. Penetrationstests folgen einem kreativen Prozess, bei dem auch Erfahrung, Branchenkenntnisse und technische Kompetenz eine wichtige Rolle spielen. Zertifikate können aber als objektiver Nachweis für Qualifikation und Kompetenz dienen.

Unternehmenszertifikate bezogen auf die Dienstleistung

- Ein BSI-IT-Sicherheitsdienstleister-Zertifikat bescheinigt für den definierten Geltungsbereich, dass der Anbieter bestimmte Anforderungen an IT-Sicherheitsdienstleistungen erfüllt und entsprechend wirksame Prozesse zum Risikomanagement, der Qualität der IT-Sicherheitsdienstleistungen, der Kompetenz und der Qualifikation des Personals, zum kontinuierlichen Verbesserungsprozess, zu Einhaltung von rechtlichen und regulatorischen Anforderungen, zur Mitarbeitersensibilisierung und zur Handhabung von Sicherheitsvorfällen etabliert hat. Jeder Anbieter muss mindestens über zwei Penetrationstester mit Kompetenzfeststellung durch das BSI verfügen.
- CREST ist eine international anerkannte, im deutschsprachigen Raum jedoch nicht weit verbreitete Akkreditierung für Unternehmen, die Dienstleistungen in den Bereichen Penetrationstests, Sicherheitsbewertungen und Reaktion auf Sicherheitsvorfälle anbieten. Unternehmen, die eine CREST-Zertifizierung erhalten, erfüllen strenge technische und ethische Standards. Die Akkreditierung stellt sicher, dass der Anbieter über qualifizierte und erfahrene Sicherheitsfachleute verfügt, die regelmäßig durch CREST evaluiert werden. Zudem überprüft CREST die organisatorischen Abläufe und ethischen Richtlinien der zertifizierten Unternehmen, um sicherzustellen, dass diese höchsten Qualitätsansprüchen genügen.
- Die Akkreditierung nach ISO/IEC 17025 bestätigt für den definierten Geltungsbereich, dass eine Prüfstelle die fachlichen, organisatorischen und technischen Anforderungen an die Durchführung von Prüf- und Kalibrierleistungen erfüllt. Wenn diese Norm auf den Bereich des Penetrationstests angewandt wird, geht es darum, die Qualität, Verlässlichkeit und Glaubwürdigkeit der von einem Penetrationstestdienstleister erbrachten Ergebnisse zu gewährleisten. Die Akkreditierung bescheinigt, dass qualifiziertes Personal, geeignete Prüfmethoden, validierte Verfahren, kalibrierte Messmittel sowie wirksame Prozesse zur Qualitätssicherung und Rückverfolgbarkeit etabliert sind. Darüber hinaus müssen Maßnahmen zum Risikomanagement, zur Sicherstellung der Unparteilichkeit und Vertraulichkeit sowie zur Einhaltung gesetzlicher und regulatorischer Anforderungen umgesetzt sein. Damit wird sichergestellt, dass Prüfergebnisse innerhalb des akkreditierten Geltungsbereichs zuverlässig, reproduzierbar und international anerkannt sind.

Unternehmenszertifikate Informationssicherheit

- Ein ISO/IEC 27001, BSI-IT-Grundschutz bzw. BSI-IT-Grundschutz auf Basis von ISO/IEC 27001-Zertifikat bescheinigt für den definierten Geltungsbereich, dass der Anbieter selbst ein Informationssicherheitsmanagementsystem (ISMS) betreibt und entsprechend wirksame Prozesse zum Risikomanagement, zu Sicherheitsmaßnahmen, zum kontinuierlichen Verbesserungsprozess, zu Einhaltung von rechtlichen und regulatorischen Anforderungen, zur Mitarbeitersensibilisierung und zur Handhabung von Sicherheitsvorfällen etabliert hat. Abhängig von den für die betroffene

Organisation relevanten Compliance-Vorschriften kann eine entsprechende Unternehmenszertifizierung des An-bieters im Auswahlverfahren relevant sein.

Personenzertifikate
Für den Nachweis von Penetrationstestkompetenzen gibt es eine große Zahl von Anbietern von Trainings und Zertifizierungen. Auf Grund des sich schnell wandelnden technologischen Umfelds besteht zudem eine hohe Dynamik im Angebot. Hier wird bewusst darauf verzichtet, eine eigene Liste zu erstellen und stattdessen auf die vom BSI unter der Überschrift "Kompetenzfeststellung von Penetrationstestern" im Internet bereitgestellte und permanent aktualisierte Übersicht, der vom BSI anerkannten Zertifikate verwiesen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Personen/Penetrationstester/penetrationstester_node.html

Einen weiteren Überblick über verfügbare Zertifizierungen und deren Einordnung bietet die Security Certification Roadmap von Paul Jeremy: https://pauljerimy.com/security-certification-roadmap/

Personenzertifikate aus diesen Quellen können Indikatoren sein. Die dort benannten Zertifikate schwanken naturgemäß in Qualität, Tiefe und Praxisrelevanz.

Hochschulabschlüsse
Seit einigen Jahren gibt es auch Universitäten und andere Hochschulen, die Abschlüsse im Bereich IT-Sicherheit anbieten. Zum einen muss man hier zwischen verschiedenen Schwerpunkten wie Sicherheitsmanagement, sicherer Softwareentwicklung, Secure Computing etc. unterscheiden, zum anderen überwiegt in allen Studiengängen die Vermittlung theoretischer Grundlagen. In der Regel müssen die Absolventen zunächst also die entsprechende praktische Erfahrung sammeln (oder bereits während des Studiums gesammelt haben), um eigenständig Penetrationstests durchführen zu können.

4.2 Reputation, Branchenerfahrung und technische Kompetenz

Der Nachweis von Qualifikationen ohne Unternehmens- und Personenzertifikate ist möglich, gestaltet sich aber sowohl für die Anbieter als auch für die Auftraggeber von Penetrationstests im Rahmen des Anbietervergleichs weitaus schwieriger und zeitaufwändiger. In diesem Fall sind beispielsweise die Entscheidungsmerkmale Erfahrung in der Durchführung von Penetrationstests, spezifische Branchenkenntnisse, Technologieverständnis und auch die gelebte Weiterbildungspraxis von Mitarbeitern wichtig, da sich Personen selbstverständlich auch im Selbststudium mit öffentlichen Quellen und/oder mit Zugriff auf kostenpflichtige Lernplattformen weiterbilden und qualifizieren können. Die Art und Güte der Qualifizierung wurde in diesem Fall jedoch nicht in einer Prüfungssituation unter Beweis gestellt, so dass hier ein gewisses Restrisiko bzgl. des Qualifikationsnachweises bleibt.

4.2.1 Erfahrung in der Durchführung von Penetrationstests

Ein etablierter Anbieter für Penetrationstests sollte mehrere Jahre Erfahrung in der Durchführung von Penetrationstests haben und entsprechend lang am Markt agieren. Dabei kann die Unternehmenserfahrung gemäß des Dienstleistungsangebots über die Jahre in den verschiedenen Sicherheitsdisziplinen, Branchen und Technologien durchaus unterschiedlich ausfallen. Neben der Unternehmenserfahrung ist insbesondere auch die Erfahrung der für die Durchführung des geplanten Penetrationstest relevanten Personen wie der eingesetzten Führungskräfte, Projektleiter, Qualitätssicherheitsbeauftragte und selbstverständlich der Penetrationstester selbst für die Qualität des Penetrationstests von Belang.

4.2.2 Technische Kompetenz

Ein Anbieter für Penetrationstests mit entsprechendem Leistungsangebot für spezifische Sicherheitsdisziplinen und Technologien hat den Vorteil, dass dieser sich aus technischer Sicht nicht neu in die Sicherheitsdisziplin und die Technologie einarbeiten muss und das notwendige Toolset, bestehend aus Hard- und Software (inkl. Lizenzen), zur Durchführung des Penetrationstests vorhält und im Umgang damit geübt ist. Die Sicherheitsdisziplinen und die Technologien unterliegen stetig neuen Änderungen und auch Anbieter von Penetrationstests wollen ihr Dienstleistungsportfolio und Technologieverständnis ausweiten, so dass durchaus auch Anbieter ohne ausgewiesene Expertise in der Sicherheitsdisziplin und Technologie allein durch ihre Erfahrung und Qualifikation mit Penetrationstests gute Leistungen erbringen können. Gleichwohl müssen derartige Anbieter in das zur Durchführung des Penetrationstest notwendige Toolset und die Qualifikation ihrer Mitarbeiter investieren.

4.2.3 Branchenkenntnis

Da sich die technologischen Grundlagen von Netzwerken, Systemen und Applikationen zwischen unterschiedlichen Branchen kaum unterscheiden, spielen entsprechende Kenntnisse nach Einschätzung der Autoren dieser Handreichung eine nachgeordnete Rolle. Sie können hilfreich sein, um die Vorgehensweise an betriebliche Anforderungen anzupassen und bei der Einordnung der Ergebnisse in einen größeren Kontext (z.B. im Rahmen eines KRITIS Audits durchgeführten Penetrationstests) zu unterstützen. Bei spezifischen Compliance-Anforderungen (z.B. DORA im Bankenkontext) müssen die Anbieter zudem über die geforderten nachweisbaren Kenntnisse verfügen. Mit wachsender Komplexität der abgebildeten Geschäftsvorfälle kann bei einer Anwendungsprüfung die Anforderung an das entsprechende Fachwissen steigen.

4.2.4 Community Engagement

Die Mitgliedschaft in einem oder mehreren Branchenverbänden durch den Anbieter beweist sein Engagement, seine Verbundenheit und seine Marktexpertise in der IT-Sicherheitsbranche. Damit unterstreicht der Anbieter, dass er über neuste Trends und Entwicklungen in der Branche informiert und an einer stetigen Qualitätssteigerung aktiv involviert ist. Die aktive Mitarbeit in Standardisierungsgremien, bei Dokumenten wie dem vorliegenden oder in einschlägigen Open-Source-Projekten sind weitere Beispiel für positive Beiträge zur Entwicklung des Themenfeldes.

4.2.5 Referenzen

Empfehlungen, Kundenbewertungen und Unternehmensreferenzen sorgen für eine gewisse Reputation eines Anbieters am Markt und können ein Indikator für die Qualität und Kundenzufriedenheit sein. Gleichwohl ist es für Anbieter von Penetrationstest bzw. für Anbieter im IT-Sicherheitsbereich oft gar nicht einfach, Referenzen und Kundenstimmen öffentlich auszuweisen, da dieses Marketinginstrument oft auf Grund von Verschwiegenheitserklärungen etc. nicht ohne Weiteres genutzt werden darf.

4.2.6 Veröffentlichungen

Im Rahmen der Kompetenzentwicklung unterstützen die meisten Anbieter ihre Mitarbeiter auch bei der Durchführung eigener Forschungsprojekte. Hieraus entstehen häufig Veröffentlichungen im Blog des Unternehmens, in Fachzeitschriften oder als Vorträge auf Fachkonferenz. Darüber hinaus werden identifizierte Schwachstellen in weit verbreiteten Lösungen häufig im Rahmen eines "Responsible Disclosure"-Verfahrens auch in entsprechenden Datenbanken als "CVEs" (Common Vulnerabitilities and Exposures) veröffentlicht.

4.3 Dienstleistungsspektrum, Methodik und Vorgehens-weise

Abhängig vom jeweiligen Leistungsspektrum des Anbieters wird dieser verschiedene Arten von Penetrationstests anbieten. Netzwerktests, Systemtests, Webanwendungstests, sind hier nur einige Beispiele. Das Leistungsspektrum des Anbieters sollte für das Ziel des Penetrationstests geeignet sein.

Idealerweise wird sich der Anbieter auch flexibel an die Bedürfnisse und Anforderungen sowie den Reifegrad der IT-Sicherheit (Maturity-Level) der betroffenen Organisation anpassen. Dabei ist es möglich, dass ggf. auch über das Ziel des zu beauftragenden Penetrationstests hinaus weitere Ziele erreicht werden. Das können z.B. die Berücksichtigung von technologie- und branchenspezifische Testanforderungen sein, Leistungen zur Unterstützung bei der Schwachstellenbeseitigung, Leistungen in Form von Re-Tests, um die Wirksamkeit der Schwachstellenbeseitigungen festzustellen, oder auch eine formale Anerkennung des Anbieters als Konformitätsbewertungsstelle für einen spezifischen Bereich, sodass der Penetrationstest als Nachweis für eine angestrebte Zertifizierung anerkannt werden kann.

Gleichwohl sind ggf. Interessenkonflikte und eine eingeschränkte Lösungsauswahl vorprogrammiert, wenn derselbe Anbieter sowohl die Identifikation von Schwachstellen sowie die Behebung der zuvor identifizierten Schwachstellen als auch die Wirksamkeitsprüfung der beseitigten Schwachstellen durch angepasste und neu implementierte Sicherheitsmaßnahmen durchführt.

Im Zuge des Anbietervergleichs sollte sichergestellt werden, dass der angefragte Penetrationstest auch bei allen Anbietern in gleicher Art und Weise kommuniziert wird. Dabei sollten die Methodik und die Vorgehensweise von allen Anbietern dargestellt und vergleichbar sein. Wie im Abschnitt "Grundsätzliche Attribute eines Tests" beschrieben, entspricht die reine Durchführung von automatisierten Schwachstellenscans ohne manuelle Tests beispielsweise nicht der hier vertretenen Definition eines Penetrationstests.

4.4 Zuverlässigkeit und Professionalität

Die Zuverlässigkeit und Professionalität des Anbieters ist entscheidend für den Erfolg des zu beauftragenden Penetrationstests. Durch die in Abschnitt 4.1.1 aufgeführten Zertifizierung kann dies zumindest in Teilen nachgewiesen werden. Darüber hinaus erfordert der Austausch von sensiblen Informationen, Testergebnissen und Schwachstellen besondere Sorgfalt, insbesondere wenn es um vertrauliche oder sicherheitskritische Daten geht. Eine reibungslose, sichere und transparente Kommunikation ist daher unerlässlich. Der folgende Abschnitt beschreibt die wesentlichen Aspekte, die im Rahmen eines Penetrationstests ebenfalls berücksichtigt werden sollten.

4.4.1 Verschlüsselter Kommunikationsaustausch

Die Kommunikation zwischen dem Auftraggeber und dem Anbieter sollte grundsätzlich verschlüsselt erfolgen, um die Vertraulichkeit und Integrität der übermittelten Daten zu gewährleisten. Der Anbieter sollte hierzu geeignete technische Lösungen anbieten, darunter:

- **E-Mail-Verschlüsselung**: Der Anbieter sollte den Einsatz von E-Mail-Verschlüsselung mittels PGP (Pretty Good Privacy) oder S/MIME (Secure/Multipurpose Internet Mail Extensions) unterstützen. Dies bietet Schutz vor unberechtigtem Zugriff auf E-Mails, die vertrauliche Informationen enthalten.

- **Digitaler Datenraum**: Für den sicheren Austausch größerer Datenmengen, wie z.B. Testergebnisse, empfiehlt sich die Bereitstellung eines verschlüsselten digitalen Datenraums. Dies kann ein gesicherter Cloud-Speicher oder ein speziell dafür eingerichteter Datenraum sein, der den Zugang nur für autorisierte Personen ermöglicht und den Transfer protokolliert.

- **Zugriffsberechtigungen:** Der Zugriff auf den Bericht sollte auf autorisierte Personen beschränkt werden. Hierzu sind geeignete Authentifizierungsmaßnahmen zu ergreifen.

4.4.2 Projektsprache

Abhängig von den spezifischen Anforderungen des Auftraggebers kann die Projektsprache ein kritischer Faktor sein. Für internationale Projekte sollte der Anbieter in der Lage sein, die Dokumentation, Kommunikation und Berichterstattung in der gewünschten Sprache (z.B. Englisch oder Deutsch) anzubieten. Zusätzlich sollten die eingesetzten Penetrationstester über ausreichende Sprachkenntnisse verfügen, um sicherzustellen, dass Missverständnisse während des Projekts vermieden werden.

4.4.3 Verfügbarkeit und Erreichbarkeit

Während der Durchführung eines Penetrationstests ist es essenziell, dass der Anbieter jederzeit erreichbar ist, um mögliche Rückfragen oder unvorhergesehene Situationen schnell zu klären. Der Anbieter sollte klar definierte Kommunikationswege und Kontaktpersonen benennen, die sowohl per E-Mail als auch telefonisch erreichbar sind. Besonders wichtig ist dies während kritischer Phasen des Penetrationstests, wie der finalen Berichterstellung oder bei der Identifizierung schwerwiegender Schwachstellen.

- **Kontaktwege**: Die Hauptansprechpartner des Projekts sollten leicht und vor allem während der vereinbarten Zeiten erreichbar sein und bei Bedarf Updates liefern. Die Kommunikationswege (E-Mail, Telefon, Webkonferenz) sollten vorab festgelegt werden.

- **Postalische oder physische Übertragungen**: Falls physische Testobjekte oder Dokumente per Post oder Kurier versandt werden müssen, sollten die Adressen und Verfahrensweisen klar definiert sein, um Verzögerungen oder Datenverlust zu vermeiden.

- **Notruf:** Sofern entsprechende Arbeitszeiten für die Durchführung vereinbart wurden oder die Ausführung (teil-)automatisierter Tests außerhalb der regulären Arbeitszeiten im 24-Stunden-Betrieb notwendig ist, muss eine entsprechende Erreichbarkeit von Auftraggeber und Auftragnehmer gewährleistet sein.

4.4.4 Dokumentationsqualität

Der Bericht zum durchgeführten Penetrationstest sollte qualitativ den Ansprüchen des Auftraggebers genügen und vollständige Transparenz gewährleisten (siehe Abschnitt "Bericht (Mindestanforderungen)"). Öffentlich verfügbare oder vom Anbieter individuell bereitgestellte Musterberichte können die Auswahl in jedem Fall unterstützen. Der Anbieter sollte einen klaren Prozess für das Reporting festlegen, der auf Wunsch regelmäßige Status-Updates während des Tests sowie einen Abschlussbericht umfasst. In diesem Zuge können wöchentliche oder projektphasenbezogene Reports vereinbart werden, um über Fortschritte und erste Testergebnisse zu informieren. Des Weiteren sollten Eskalationswege definiert werden, falls kritische Sicherheitslücken gefunden werden oder unvorhergesehene Probleme bei der Testdurchführung auftreten.

4.4.5 Eskalationsmanagement

Bei schwerwiegenden Problemen, wie dem Auffinden kritischer Schwachstellen, die sofortige Aufmerksamkeit benötigen, sollte ein vordefinierter Eskalationsweg genutzt werden, um Maßnahmen zu koordinieren. Dieser kann neben direkten Kontakten zu den Sicherheitsverantwortlichen der Organisation auf Auftraggeberseite auch die ergänzende Einbindung unterbeauftragter Dienstleister und externer Spezialisten umfassen.

4.4.6 Responsible Disclosure

Auf Grundlage eines sogenannten Responsible-Disclosure-Verfahrens können der Auftraggeber und der Auftragnehmer des Penetrationstests eine klare Regelung zum Umgang mit im Penetrationstest identifizierten Sicherheitslücken sicherstellen. Weitere Details zu diesem Thema sind in Abschnitt "Responsible Disclosure"**Fehler! Verweisquelle konnte nicht gefunden werden.** im Anhang zu finden.

4.4.7 Ausgangspunkt der Testdurchführung

Die Flexibilität von Penetrationstestanbietern unterscheiden sich beispielsweise in der Durchführung von Penetrationstests im internen Netzwerk (LAN). Die Testdurchführung erfolgt typischerweise vor Ort bei am Standort der betroffenen Organisation, remote über das Internet über eine von der Organisation zur Verfügung gestellte VPN-Verbindung oder mittels einer seitens des Anbieters postalisch versendeten VPN-Box. Diese Ansätze unterscheiden sich im Wesentlichen in Bezug auf Sicherheit, Flexibilität, Kosten und Aufwand.

Nachfolgend werden die spezifischen Vor- und Nachteile der Ansätze dargestellt.

4.4.7.1 Testdurchführung vor Ort beim Auftraggeber

Vorteile:	**Nachteile:**
Höhere Sicherheit und Kontrolle: Da die Tests im internen Netzwerk des Auftraggebers durchgeführt werden, entfallen potenzielle Sicherheitsrisiken, die mit der Übertragung von Daten über das Internet oder externe Netzwerke einhergehen.	Höhere Kosten und Logistik: Die Anreise und der Aufenthalt vor Ort verursachen in Form von Reisezeiten und Reisekosten zusätzlichen Aufwand, was anhängig vom Angebot zu höheren Gesamtkosten für den Auftraggeber führen kann.
Echter Einblick in die Infrastruktur: Der Penetrationstester kann das Netzwerk und die Umgebung direkt analysieren, was oft detailliertere Einblicke ermöglicht und auch die Erkennung physischer Schwachstellen (z.B. unsichere Geräteplatzierungen, Zutrittskontrollen, etc.) einschließt. Solche Zufallsfunde können einen wesentlichen Mehrwert für den Auftraggeber liefern.	Organisatorischer Aufwand: Der Auftraggeber muss möglicherweise spezielle Vorkehrungen treffen, wie die Zuweisung von Projekträumen und Arbeitsplätzen, temporäre Zugangskarten, Sicherheitsüberprüfungen und andere Maßnahmen, was zusätzliche Aufwände auf seitens des Auftraggebers verursacht.
Stabile Verbindung: Die Tests sind unabhängig von Internetverbindungen, VPN-Stabilität oder Netzwerkbandbreite, was die Genauigkeit und Geschwindigkeit der Tests erhöhen kann.	Zeitaufwand: Die zeitliche Flexibilität ist eingeschränkt, da der Penetrationstester physisch vor Ort sein muss. Kurzfristige Anpassungen oder Nachtests, welche von der ursprünglichen Planung abweichen, sind schwieriger umzusetzen.

4.4.7.2 Testdurchführung remote über eine VPN-Verbindung des Auftraggebers

Vorteile:	**Nachteile**:
Kostenersparnis: Da keine Anreise oder Logistik erforderlich ist, entfallen Reisezeiten und Reisekosten für den Anbieter des Penetrationstests und der organisatorische Aufwand für den Auftraggeber.	Sicherheitsrisiko durch unzureichend konfigurierte VPN-Zugänge: Der VPN-Zugang, der extern bereitgestellt wird, stellt ein Sicherheitsrisiko dar, wenn er nicht ordnungsgemäß geschützt ist. Unzureichend konfigurierte VPNs könnten den Angriffsvektor erweitern und potenziell neue Risiken schaffen.
Flexibilität: Remote-Tests im Vergleich leichter planbar und können flexibler an die Verfügbarkeit des Penetrationstestanbieters und die Anforderungen des Auftraggebers angepasst werden.	Abhängigkeit von Internetverbindung und Bandbreite: Die Qualität der Tests hängt stark von der Stabilität und Geschwindigkeit der Internetverbindung ab. Eine langsame Verbindung kann die Tests verlangsamen oder sogar behindern.
Schnelle Bereitstellung: Wenn der Auftraggeber bereits über eine VPN-Infrastruktur für Remote-VPN-Zugriffe verfügt, können Tests schnell gestartet werden, ohne dass seitens des Auftraggebers zusätzliche Hardware benötigt wird.	Potenzielle Begrenzung des ausgewählten Untersuchungsgegenstands: Manche VPN-Konfigurationen ermöglichen nur den Zugang zu bestimmten Netzwerksegmenten, was die Testmöglichkeiten einschränken könnte oder dem Penetrationstestanbieter zu weitreichende Zugriffsmöglichkeiten auf die IT-Infrastruktur ermöglicht.

4.4.7.3 Testdurchführung remote über eine VPN-Box des Penetrationstestanbieters

Vorteile:	**Nachteile**:
Einfache und flexible Konnektivität: Die VPN-Box kann meist einfach in das Netzwerk des Kunden integriert werden. ohne dass eine VPN-Konfiguration seitens des Auftraggebers erforderlich ist.	Logistik: Die VPN-Box muss erst an den Kunden versandt und installiert werden, was zu Verzögerungen führen kann, insbesondere wenn der Kunde in einer anderen Region oder einem anderen Land ansässig ist. Manipulationsrisiko während des postalischen Versands: Der Versand der Box birgt das Risiko, dass sie während des Transports manipuliert wird. Außerdem besteht für beide Vertragsparteien das Risiko des unbefugten Zugriffs auf die in Betrieb genommene Box und die damit verbundene IT-Infrastruktur. Durch entsprechende Gegenmaßnahmen (Versand in plombierten und nummerierten Containern) lassen sich diese Risiken hinreichend minimieren.

Jeder Ansatz hat spezifische Stärken und Schwächen. Die Wahl hängt stark von den Sicherheitsanforderungen, der Infrastruktur und den Ressourcen des Auftraggebers ab.

4.4.8 Near- / Offshore / Freelance Penetrationstester

Im Sinne der Internationalisierung und Globalisierung kann der Einsatz von sogenannten Nearshore-, Offshore- oder Freelance-Penetrationstester seitens des Penetrationstestanbieters sowohl wirtschaftliche als auch operative Vorteile haben, gleichwohl auch einige Herausforderungen und Nachteile mit sich bringen.

Die wesentlichen Vorteile lassen sie wie folgt zusammenfassen.

- **Kosteneffizienz**
  Offshore- und Nearshore-Tester sowie Freelancer arbeiten oft in Regionen mit niedrigeren Lebenshaltungskosten, was dazu führt, dass ihre Dienstleistungen kostengünstiger sind. Der Penetrationstestanbieter kann diese Einsparungen an den Kunden weitergeben, was das Penetrationstestangebot insgesamt günstiger macht.

- **Zugang zum globalem Talentpool**
  Die Zusammenarbeit mit Freelancern und internationalen Testern ermöglicht es dem Anbieter, auf ein breiteres Spektrum an Fachwissen und Erfahrung zuzugreifen. Tester aus verschiedenen Regionen können spezifische Kenntnisse haben, die für bestimmte Technologien oder Angriffsvektoren nützlich sind.

- **Skalierbarkeit und Flexibilität**
  Freelancer und Near-/Offshore-Teams ermöglichen es, Projekte schnell aufzustocken oder abzuschließen. Der Anbieter kann bei Bedarf zusätzliche Ressourcen hinzuziehen, um auf plötzliche Anforderungen oder besonders umfangreiche Tests zu reagieren.

- **Zeitliche Flexibilität und 24/7-Verfügbarkeit**
  Durch die verschiedenen Zeitzonen und die flexible Verfügbarkeit von Freelancern können Tests rund um die Uhr durchgeführt werden. Dies kann insbesondere bei dringenden Sicherheitsüberprüfungen oder großen Projekten von Vorteil sein, da Schwachstellen schneller aufgedeckt werden können.

- **Spezialkenntnisse und Nischenkompetenzen**
  Freelancer und Near-/Offshore-Tester bringen oft spezifische Fachkenntnisse mit, die bei komplexen Systemen oder spezialisierten Technologien nützlich sein können. Diese Expertise ist oft schwer zu finden und kann besonders wertvoll für Nischenprojekte sein.

Die wesentlichen Nachteile von eingesetzten Nearshore-, Offshore- oder Freelance-Testern durch den beauftragten Penetrationstestanbieter lassen sie wie folgt zusammenfassen.

- **Kommunikations- und Kulturbarrieren**
  Unterschiedliche Zeitzonen, Sprachbarrieren und kulturelle Unterschiede können die Kommunikation und Zusammenarbeit erschweren. Missverständnisse sind häufiger und können zu Fehlern oder Verzögerungen führen.

- **Sicherheits- und Datenschutzrisiken**
  Die Einbindung von Near-/Offshore- und Freelance-Testern kann Risiken im Hinblick auf den Datenschutz und die Datensicherheit mit sich bringen. Besonders bei sensiblen Daten oder strategisch wichtigen Projekten und Innovationsprojekten kann dies problematisch sein, da die gesetzlichen Bestimmungen in verschiedenen Ländern variieren und möglicherweise nicht dieselben Sicherheitsstandards gelten.

- **Compliance-Probleme und Strafzahlungen**
  Der Einsatz von Near-/Offshore- und Freelance-Testern ist aus rechtlicher Sicht durch den Auftraggeber hinsichtlich möglicher Compliance- und Vertragsverstößen zu überprüfen, um Strafzahlungen zu vermeiden. Besonders bei Offshore-Testern kann es zu Problemen mit rechtlichen und regulatorischen Anforderungen kommen, da bestimmte Compliance-Standards, wie die DSGVO oder ISO-Normen, eventuell nicht eingehalten werden. Dies ist besonders für Unternehmen in stark regulierten Branchen relevant.

- **Schwierige Qualitätskontrolle und Konsistenz**
  Bei Freelancern oder Teams in anderen Regionen ist die Qualität der Arbeit schwerer direkt zu kontrollieren. Unterschiedliche Standards, Arbeitsweisen und Methoden können dazu führen, dass die Testergebnisse uneinheitlich oder nicht auf dem erwarteten Niveau sind.

- **Mangel an langfristiger Verfügbarkeit und Kontinuität**
  Freelancer und kurzfristig eingesetzte Tester sind möglicherweise nicht langfristig verfügbar. Der Wechsel von Testern kann die Konsistenz beeinträchtigen, da sich neue Tester erst einarbeiten müssen und möglicherweise nicht dasselbe Maß an Kontext oder Kundenkenntnis mitbringen.

- **Geringere Unternehmensbindung**
  Freelancer und Near-/Offshore-Teams sind oft weniger eng an den Penetrationstestanbieter und an deren Auftraggeber gebunden, was die Loyalität und das Verantwortungsbewusstsein verringern. Dies könnte dazu führen, dass die Motivation oder die Bemühung nachlassen, insbesondere, wenn es um die Einhaltung von Unternehmenswerten und -standards geht.

Ein Penetrationstestanbieter, der Nearshore-, Offshore- oder Freelance-Tester einsetzt, kann zusammengefasst wirtschaftliche und operative Vorteile bieten, da er flexibler, skalierbarer und kostengünstiger arbeiten kann. Jedoch sind diese Vorteile oft mit erhöhten Risiken verbunden, wie Datenschutz- und Compliance-Problemen sowie möglichen Kommunikations- und Qualitätsherausforderungen. Organisationen sollten diese Faktoren sorgfältig bei der Auswahl eines Penetrationstestanbieters abwägen und gegebenenfalls zusätzliche Sicherheits- und Qualitätskontrollen einführen, um eine hohe Qualität und Datensicherheit sicherzustellen.

4.4.9 Einsatz Künstlicher Intelligenz

Der Einsatz von Künstlicher Intelligenz (KI) im Kontext von Penetrationstests wird zunehmend ein Thema, das intensiv in der Fach-Community und den Medien diskutiert wird. Die Entwicklung schreitet - wie im gesamten KI-Sektor - sehr schnell voran. Neben möglichen Effizienzgewinnen entstehen aber auch neue Herausforderungen. Daher werden KI-Technologien aktuell (zum Zeitpunkt der Veröffentlichung dieser Handreichung) eher noch punktuell als Unterstützung bestehender Methoden und Vorgehensweisen eingesetzt.

4.4.9.1 Chancen und Nutzen

Der Einsatz von KI bietet insbesondere in der Vorbereitung, Durchführung und Auswertung von Penetrationstests erhebliche Potenziale:

- **Effizienzsteigerung und Automatisierung**
  KI kann große Datenmengen (z. B. Scan-Ergebnisse, Logs, Konfigurationsdaten) schneller analysieren und priorisieren als klassische Ansätze. Dadurch lassen sich insbesondere wiederkehrende Prüfungen, Basisanalysen und das Berichtswesen (die Dokumentation der Testergebnisse) beschleunigen.

- **Persönliche Assistenz für erfahrene Penetrationstester**
  KI kann als Assistenzsystem für erfahrene Tester bei der Durchführung von explorativen Penetrationstests dienen. Sie ersetzt jedoch nicht die fachliche Bewertung durch Experten, die für eine fundierte Sicherheitseinschätzung essenziell ist.

4.4.9.2 Risiken und Herausforderungen

Trotz der genannten Vorteile bringt der Einsatz von KI in Penetrationstests auch relevante Risiken mit sich:

- **Transparenz und Nachvollziehbarkeit**
  KI-gestützte Entscheidungen sind nicht immer vollständig erklärbar (Black-Box-Problematik). Für regulatorische Anforderungen und Berichte kann dies eine Herausforderung darstellen.

- **False Positives und False Negatives**
  Wie bei automatisierten Verfahren generell besteht das Risiko, dass KI-basierte Analysen unzutreffende Ergebnisse liefern. Die manuelle Validierung durch erfahrene Penetrationstester bleibt daher zwingend erforderlich.

- **Fehlende Kontextsensitivität**
  KI-Modelle können technische Schwachstellen erkennen, sind jedoch häufig nicht in der Lage, diese vollständig im organisatorischen oder geschäftlichen Kontext zu bewerten. Dies kann zu Fehlpriorisierungen führen.

- **Gefahr der Überautomatisierung**
  Ein rein KI-gestützter Ansatz widerspricht dem Charakter eines Penetrationstests als qualitativ hochwertige, explorative und kontextbezogene Dienstleistung. Eine zu starke Automatisierung kann dazu führen, dass wesentliche Angriffsszenarien nicht ausreichend berücksichtigt werden.

- **Unbeabsichtigte Auswirkungen auf das Testobjekt**
  Der Einsatz von KI kann das Risiko unbeabsichtigter Auswirkungen auf das Testobjekt erhöhen. Durch automatisierte, hochskalierbare und teilweise adaptive Testverfahren können Systeme stärker und weniger vorhersehbar belastet werden als bei rein manuellen Ansätzen. Dies kann zu Nebenwirkungen wie Performanceeinbußen, Systeminstabilitäten oder im Einzelfall zu Ausfällen oder Datenverlusten führen.

- **Unbeabsichtigter Datenabfluss und Compliance- Verstöße**
  So wie dem Anbieter, also dem beauftragten Auftragnehmer des Penetrationstests, vertraut wird, so muss auch dem KI-Anbieter bzw. dem zugrundeliegenden Cloud-Anbieter vertraut werden. Sowohl die identifizierten Schwachstellen als auch etwaige Zugangs- sowie Nutzdaten sind den KI-Anbietern bekannt. Des Weiteren ist für den Einsatz der gängigen KI-Lösungen aus der Cloud stets eine Datenverbindung über das Internet zum Backend der KI-Lösung notwendig, damit die KI effizient arbeiten und weiter trainiert werden kann. Dies kann zu unbeabsichtigten Datenabflüssen und ggf. zu Compliance-Verstößen führen.

- **Kostenfaktor Token-Verbrauch**
  Mit der Größe und Mächtigkeit der Modelle wachsen auch Tokenverbauch und damit die Kosten. Ein wirtschaftlich sinnvoller Einsatz von KI bedarf daher einer vorangestellten Analyse des Prüfobjektes und einer detaillierten Planung, um die Risiken das Testbudget durch unkontrollierten Token-Verbrauch zu minimieren.

4.4.9.3 Einordnung

Zusammenfassend ist KI als unterstützende Technologie zu verstehen, die klassische Methoden für Penetrationstests sinnvoll ergänzt, jedoch nicht ersetzt. Der größte Mehrwert entsteht in hybriden

Ansätzen, bei denen automatisierte und KI-gestützte Verfahren mit der Erfahrung und Kreativität menschlicher Experten kombiniert werden.

4.4.9.4 Weitere Anforderungen

Der Anbieter und die eingesetzten Mitarbeiter sollten selbst auch ein gewisses Mindestmaß an Sicherheits- und Datenschutzstandards einhalten. Neben den externen Compliance-Vorgaben sind in diesem Zusammenhang ggf. noch ergänzende interne Vorgaben bei der Anbieterauswahl zu berücksichtigen. In diesem Sinne sollte sichergestellt werden, dass der Anbieter beispielsweise die Anforderungen der DSGVO, den geltenden Mindestlohn und den Nachhaltigkeitsvorgaben genügt.

In diesem Zusammenhang sind auch die bereits genannten Unternehmenszertifikate ein gut vergleichbarer Nachweis, dass die Einhaltung entsprechender Sicherheits- und Datenschutzanforderungen überprüft und eingehalten werden. Beim Anbietervergleich können sich bei der Einhaltung von Sicherheits- und Datenschutzstandards auch Unterschiede in der zugrundeliegenden Unternehmensstruktur des Anbieters bemerkbar machen. Für Selbstständige, Vereinigungen von selbstständigen Anbietern sowie für kleinere Unternehmen ist die Umsetzung und die Bestätigung zur Einhaltung von Sicherheits- und Datenschutzstandards in Teilen nicht konsequent einheitlich in der Praxis umsetzbar und die Evaluierung samt Zertifizierung im Erfolgsfall zu teurer.

Da im Rahmen des zu beauftragenden Penetrationstests sensible Informationen und Schwachstellen aufdeckt werden können, sollten über die Sicherheitsgarantien hinaus entsprechende Verschwiegenheitserklärungen mit dem Anbieter abgeschlossen werden. Im Zuge der Ausweisung von Unternehmensreferenzen durch den Anbieter sind hier ggf. entsprechende Ausnahmen in den Vereinbarungen zu berücksichtigen.

4.5 Preisgestaltung

Der Anbieter sollte im Rahmen seines Angebots die fachliche Leistung transparent darstellen und mindestens die folgenden Aspekte aufgreifen und beschreiben:

- Projektspezifische Zielsetzung
- Darstellung der einzelnen Leistungsbestandteile und Vorgehensweisen
- Qualifikation des eingesetzten Personals und Einsatzort

Die Preisgestaltung des Anbieters sollte transparent und verständlich sein. Es sollte klar erkennbar sein, welche konkreten Leistungsbestandteile von den jeweilig ausgewiesenen Preisen abgedeckt werden.

Die Vertragsbedingungen sollten neben den oben genannten Aspekten insbesondere auch transparent über die Haftung, etwaige Versicherungssummen, die jeweiligen Verantwortungsbereiche der Vertragsparteien und ggf. etwaige Unterauftragsnehmerverhältnisse aufklären.

4.5.1 Entscheidungsmatrix

Die Entscheidungsmatrix greift die beschriebenen Merkmale auf und dient als Vorschlag. Sowohl die Kriterien, die Fragestellung und die Bewertung als auch die Punkte und Gewichtung sind in dieser Form eine solide Grundlage für viele Situationen. Selbstverständlich muss am Ende jede Organisation entschieden, welche Kriterien wichtig sind, welche nicht und in welcher Gewichtung sie zueinanderstehen.

Kriterium	**Fragestellung**	**Bewertung**	**Punkte**	**Gewichtung**
Qualität	Hat der Bieter die geplanten Tests ausreichend beschrieben?	Nur Titel, keine näheren Angaben	0	**50%**
		Die Aufgaben und Unteraufgaben sind genannt. Prüfmethodik, Projektplan oder Zuständigkeiten sind mit keinen oder wenig Details beschrieben. Die Vorgehensweise passt bedingt zur Erwartungshaltung (z.B. Automatisierungsgrad)	5	
		Die Aufgaben und Unteraufgaben sind genannt. Prüfmethodik, Projektplan oder Zuständigkeiten sind detailliert beschrieben. Die Vorgehensweise passt zur Erwartungshaltung (z.B. Automatisierungsgrad).	10	
		Die Aufgaben und Unteraufgaben sind genannt. Prüfmethodik, Projektplan oder Zuständigkeiten sind detailliert vollständig beschrieben. Die Vorgehensweise passt sehr gut zur Erwartungshaltung (z.B. Automatisierungsgrad).	20	
	Einheitliche Testprozesse in der Firma	Keine Angaben	0	
		Prozessbeschreibung zu Einheitlichkeit und Weiterentwicklung im Team werden genannt, aber mit keinen oder wenig Details beschrieben.	5	
		Prozessbeschreibung zu Einheitlichkeit und Weiterentwicklung im Team werden genannt und detailliert zum Prozess beschrieben.	10	
	Qualitätsmanagement-Prozesse	Keine Angaben	0	
		Einheitliche Qualitätsmanagement-Prozesse werden genannt, aber mit keinen oder wenig Details beschrieben.	2	
		Einheitliche Qualitätsmanagement-Prozesse werden genannt und mit Details beschrieben, QM-Zertifikat vorhanden.	5	

Extra-Punkte	BSI-zertifizierte IT-Sicherheitsdienstleister	ja/nein	10	**10%**
	CREST	ja/nein	3	
	Relevante Personenzertifizierungen laut BSI-Liste	1 Punkt je Zertifizierung, maximal 5		
	Referenzen im passenden technischen Umfeld	1 je Referenz, maximal 3		
	Anbieter sichert zu, Nearshoring- oder Offshoring-Personal nur entsprechend der Projektanforderungen einzusetzen.	ja/nein	10	
	Zertifiziertes ISMS nach ISO 27001 oder BSI-Grundschutz	ja/nein	5	
	Community-Engagement	ja/nein	2	
	Veröffentlichungen, Schulungen und Vorträge	je 1, maximal 5		
	Teamgröße Penetrationstestteam	je FTE 1 Punkt, mind. 3. maximal 10		
Preis	Preis Modul 1 Preis Modul 2	? EUR ? EUR		**40%**
Ausschusskriterien (bei Fehlen folgender Punkte): Datenschutzerklärung und TOMs liegen vor NDA unterschrieben Verschlüsselter Datenaustausch Erreichbarkeit während der Testzeiträume zugesichert Nur festangestelltes Personal Mind. 2 Tester je Modul verfügbar				

Tabelle 1: Entscheidungsmatrix

5 Vertragliches

Eine saubere vertragliche Regelung von Penetrationstests ist sowohl für den Auftraggeber als auch für den Dienstleister unerlässlich. Laut §202c StGB ist schon das "Vorbereiten des Ausspähens und Abfangens von Daten" strafbar. Erst durch die Begründung des BVerfG für die Abweisung einer Verfassungsbeschwerde gegen diesen Paragrafen konnte geklärt werden, dass dies nicht für das Erbringen entsprechender Dienstleistungen gilt, wenn sie durch den Eigentümer bzw. Betreiber des jeweiligen IT-Systems beauftragt werden[8].

Ein wesentlicher Bestandteil des Vertrages ist damit der "Scope", also der genaue Umfang der durchzuführenden Prüfung, sowie eine Abklärung der Rechte des Auftraggebers und etwaiger Dritter an den zu prüfenden Systemen und Daten. Daneben sind Regelungen zur jeweiligen Haftung von Auftraggeber und Auftragnehmer bzw. Haftungsfreistellungen essenziell für eine vollständige vertragliche Vereinbarung.

5.1 Was sollte im Vertrag stehen

Neben Deckblatt, Dokumentenmanagement (Erstellungsdatum, Versionierung, Änderungsliste) und Inhaltsverzeichnis sollte ein Vertrag über einen Penetrationstest mindestens folgende Informationen enthalten:

- Einleitung/Übersicht
- Zu erreichende Ziele
- Rechtliche Rahmenbedingungen
    - Rechte Dritter an den zu prüfenden Systemen und Diensten
        - Ist der Auftraggeber tatsächlich Eigentümer der Systeme?
        - Liegt die Zustimmung des Eigentümers zum Test vor?
    - Sorgfaltspflichten des Dienstleisters
    - Mitwirkungspflichten des Auftraggebers, u. a. Klärung, ob er tatsächlich Eigentümer der zu prüfenden Systeme ist
    - Datenschutzrechtliche Abwägungen (Sollen Art. 9-Systeme getestet werden?)
    - Meldung von Sicherheitslücken
    - Verwertung von Ergebnissen aus dem Bericht

- Umfang der geplanten Tests (Scope)
    - Welche Systeme und/oder Dienste sollen getestet werden?
    - Welche Ausschlüsse werden vom Auftraggeber vorgegeben?
    - In welchem Zeitrahmen sollen die Prüfungen durchgeführt werden?
    - Welche Testtiefe ist zu erreichen?
    - Sollen Schwachstellen lediglich dokumentiert oder auch ausgenutzt werden?
        - Hier sollte jeweils auch eine Risikoabwägung in direkter Abstimmung zwischen Tester und Auftraggeber erfolgen.

- Zeitplan
    - Wann findet ein Vorgespräch statt?
    - Wann sollen die Tests durchgeführt werden?
    - Bis wann soll der Bericht vorliegen?

- Prozess für und Folgen von Vertragsänderungen
- Umfang der Rechteeinräumung: Vom Auftragnehmer eingesetzte Tools und Skripte verbleiben in dessen Eigentum bzw. Rechteinhaberschaft; Rechte an den Ergebnissen und dem Bericht gehen auf den Auftraggeber über, jedoch nur für den vereinbarten Verwendungszweck. Eine weitergehende Verwertung - etwa die Einreichung gefundener Schwachstellen bei Bug-Bounty-Programmen - muss gesondert geregelt werden.

[8] Dennoch kann weiterer gerichtlicher Klärungsbedarf bestehen, wenn es Uneinigkeit über den Umfang der erteilten Berechtigungen bzw. die Eigentumsrechte an Daten und Systemen gibt, wie dieser Fall zeigt: https://www.heise.de/news/Warum-ein-Sicherheitsforscher-im-Fall-Modern-Solution-verurteilt-wurde-9601392.html

- Haftungsklausel
    - Allgemeine Bestimmungen
    - Verzug, Projektabbruch
    - Schäden an Systemen einschließlich Folgeschäden

- Kommerzielles
    - Welche Kosten werden in Rechnung gestellt?
        - Erfolgt die Abrechnung pauschal oder nach Zeitaufwand?
        - Welche Nebenkosten werden ggf. zusätzlich verrechnet?
            - Lizenzkosten für projektbezogene Software
            - Reisezeiten
            - Übernachtungs- und Verpflegungskosten

5.2 Werkvertrag oder Dienstvertrag

Im Bereich von Penetrationstests kommen sowohl Dienst- als auch Werkverträge zum Einsatz, je nach Leistungsumfang und Vereinbarung mit dem Dienstleister. Ein Dienstvertrag liegt in der Regel dann vor, wenn der Auftragnehmer sich dazu verpflichtet, innerhalb eines bestimmten Zeitraums Tätigkeiten wie das Auffinden und Dokumentieren von Schwachstellen durchzuführen, ohne jedoch einen bestimmten Erfolg - etwa die vollständige Beseitigung der Schwachstellen oder einen verbindlichen Prüfbericht - zu schulden. Es wird also das Bemühen, nicht aber ein konkretes Ergebnis garantiert. Die Abrechnung erfolgt hier meist auf Basis der geleisteten Arbeitszeit, unterstützt durch einen Stundennachweis; ein Abschlussbericht kann zur Dokumentation dienen, ist aber nicht zwingend geschuldet.

Ein Werkvertrag hingegen liegt dann vor, wenn ein bestimmtes Arbeitsergebnis geschuldet ist. Dies kann beispielsweise der Fall sein, wenn neben der Identifikation auch die Behebung der Schwachstellen vereinbart wird oder ausdrücklich ein abschließender, detaillierter Prüfbericht als vertraglich geschuldetes Ergebnis festgelegt ist. Die Vergütung erfolgt hierbei üblicherweise nach Abnahme des vereinbarten Werks, also beispielsweise nach Übergabe und Anerkennung des Prüfberichts durch die Auftraggeber.

Hiervon kann allerdings durch Vereinbarung zwischen Auftraggeber und Auftragnehmer abgewichen werden, so dass es z.B. auch zulässig wäre, dass der Auftragnehmer einen Teil der Vergütung als Vorauszahlung oder die gesamte Vergütung vor Erbringung der Leistung erhält.

5.3 Geheimhaltungsvereinbarung (mNDA)

Penetrationstests sind Vertrauenssache. Schließlich erhalten die Penetrationstester unter Umständen Zugriffe auf sensible Unternehmensinformationen und IT-Systeme. Sofern der Auftraggeber keinen Standard-NDA nutzt, sollte der Anbieter eine Vorlage übergeben können. Je nach der Sensibilität der Informationen, die bereits im Vorfeld beim "Scoping" ausgetauscht werden sollen, kann es sinnvoll sein, dieses Thema bereits im Rahmen der ersten Kontaktaufnahme zu klären. Idealerweise sollte ein mNDA (mutual Non-Disclosure Agreement) geschlossen werden, der die Vertraulichkeit für beide Parteien wechselseitig regelt.

5.4 AVV

Ein Penetrationstest stellt an sich nicht zwangsläufig eine Auftragsdatenverarbeitung dar, da der Auftrag des Penetrationstesters (Auftragnehmer) in der Regel nicht darin besteht, gezielt personenbezogene Daten (pbD) auf eigenen Systemen zu speichern oder zu verarbeiten. Die Notwendigkeit eines Auftragsverarbeitungsvertrages (AVV) sollte daher vor der Beauftragung dezidiert geprüft werden.

Die Notwendigkeit eines AVV kann insbesondere anhand folgender Fragen geprüft werden:

- Werden produktive Systeme oder Echtdaten in den Test einbezogen oder wird ausschließlich in einer isolierten Testumgebung gearbeitet, in der sich keine personenbezogenen Daten befinden?

- Welche Datenkategorien könnten dem Auftragnehmer zugänglich werden? Sind besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO (z.B. Gesundheitsdaten, biometrische Daten) betroffen?
- Ist der Auftragnehmer angewiesen, Daten, auf die er im Testverlauf stößt, zu dokumentieren oder in den Abschlussbericht aufzunehmen?

Sollte eine Frage mit " Ja" beantwortet werden, spricht dies für die Notwendigkeit eines AVV. Eine rechtliche Beratung im Einzelfall ist hier angezeigt.

Sollte die Prüfung ergeben, dass ein AVV geschlossen werden soll, sind bei der Beauftragung eines Penetrationstests festzulegen, welche personenbezogenen Daten der Auftragnehmer bei seiner Tätigkeit verarbeiten darf. Dies dient der Rechtsklarheit und begrenzt den Verarbeitungsumfang auf das Notwendige.

Folgende Angaben sind erforderlich:

- Gegenstand und Zweck der Verarbeitung
  Es müssen Gegenstand und Zweck der Verarbeitung genannt werden. Diese können z.B. die Durchführung eines Sicherheitsaudits/Penetrationstests und die Identifikation von Schwachstellen in IT-Systemen sein.

- Art der personenbezogenen Daten
  Die betroffene Organisation benennt, soweit möglich, konkret, welche Datenarten verarbeitet werden können, z.B. Zugangsdaten (Benutzernamen, Passwort-Hashes), Netzwerkdaten (IP-Adressen, MAC-Adressen) und etwaige weitere Daten. Falls zutreffend: besondere Kategorien nach Art. 9 DSGVO (z.B. Gesundheitsdaten bei Tests von Gesundheitsanwendungen)

- Kategorien betroffener Personen
  Die betroffene Organisation benennt, soweit möglich, welche Kategorien von Personen von den Tests und etwaigen Datenverarbeitungen betroffen sein können. Dies können z.B. Mitarbeiter des Unternehmens, Kunden/Vertragspartner, Website-Besucher oder andere relevante Personengruppen sein.

- Dauer der Verarbeitung
  Die betroffene Organisation benennt den Zeitraum der Testdurchführung und eine Aufbewahrungsfrist für Testdaten und Berichte. So werden an dieser Stelle auch die Einhaltung von Lösch- und Auskunftspflichten gemäß DSGVO vertraglich geregelt und das Risiko für den Auftraggeber minimiert.

5.5 Haftungsfreistellung

Der Auftraggeber sollte den Auftragnehmer von Schäden freistellen, die durch die Durchführung des Tests entstehen, es sei denn, dass die Schäden vorsätzlich oder grob fahrlässig durch den Tester verursacht worden sind. Eine solche Haftungsfreistellung sollte zunächst bezüglich etwaiger Schäden gelten, die unmittelbar beim Auftraggeber entstehen, z.B. durch den Ausfall von Systemen infolge der Tests.

Mit einem Test können aber auch unabsichtlich Systeme angegriffen werden, die zwar im Scope des vereinbarten Testings sind, von denen sich aber im Laufe der Tests herausstellt, dass sie gar nicht dem Auftraggeber, sondern einem Dritten gehören. Der Auftragnehmer kann nicht wissen, in wessen Eigentum die zu testenden Systeme stehen. Diese Klärung kann nur der Auftraggeber verbindlich durchführen. Es ist daher sachgerecht, dass der Auftraggeber den Auftragnehmer von Ansprüchen freistellt, die der Dritte gegen den Auftragnehmer erhebt. Schließlich ist darauf hinzuweisen, dass aus der durch den Auftragnehmer vorgenommene Einstufung des Schweregrads der aufgedeckten Schwachstellen keine Haftungsansprüche ableiten lassen, da eine Bewertung konkreter Risiken nur durch den Auftraggeber selbst vorgenommen werden kann. Die Haftungsfreistellung zugunsten des Auftragnehmers sollte sich also auch auf diesen Punkt erstrecken. In diesem Zusammenhang sollte durch den Auftragnehmer auch geregelt werden, dass keine Haftung für die vorgenommene Kritikalitätsbewertung übernommen wird.

6 Bericht (Mindestanforderungen)

Ein Penetrationstest ist ein wesentlicher Bestandteil der Sicherheitsüberprüfung von IT-Systemen, bei der Schwachstellen systematisch identifiziert und bewertet werden. Ein detaillierter und strukturiert erstellter Bericht stellt das zentrale Ergebnis eines Penetrationstests dar und dient als Grundlage für die weitere Sicherheitsstrategie der geprüften Organisation.

6.1 Aufbau

Ein Penetrationstest-Bericht sollte präzise und vollständig die Ergebnisse des Tests dokumentieren. Folgende Mindestanforderungen sind zu beachten:

- **Format (PDF, PPT, etc.):**
  Der Bericht muss in einem standardisierten und allgemein akzeptierten Format bereitgestellt werden, das die Integrität und Authentizität der Informationen gewährleistet. Das PDF ist hierbei das bevorzugte Format, da es unveränderbar ist und eine hohe Akzeptanz genießt. Sofern eine Abschlussbesprechung vor Management geplant ist, kann ergänzend eine Übersicht in einem Präsentationsformat (z.B. PPT) zur Verfügung gestellt werden. Sofern ein Ticketsystem für die Weiterbearbeitung der identifizierten Schwachstellen im Einsatz ist, sollte der Auftraggeber vorab definieren, in welchem maschinenlesbaren Format die Daten konkret bereitgestellt werden sollen.

- **Detailgrad:**
  Der Detailgrad des Berichts ist entscheidend für dessen Nutzbarkeit. Ein guter Bericht sollte sowohl technische als auch nicht-technische Aspekte abdecken und den unterschiedlichen Informationsbedürfnissen der Leser gerecht werden. Technische Details sind unerlässlich, um die Schwachstellen nachvollziehbar darzustellen und zu bewerten. Gleichzeitig sollte der Bericht Management-Empfänger in einer verständlichen Weise über die wesentlichen technischen Schwachstellen und empfohlenen Maßnahmen informieren. Dabei sollte der Bericht auch den Hinweis enthalten, dass die vom Testunternehmen vorgenommene Einstufung hinsichtlich des Schweregrads von Schwachstellen den Auftraggeber nicht von der Pflicht entbindet, im Hinblick auf seinen internen Schutzbedarf diesbezüglich noch einmal eine eigene Bewertung vorzunehmen. Weitere Details dazu sind in Abschnitt "Haftungsfreistellung" zu finden. Dies ist insbesondere auch erforderlich, um Zertifizierungen und Testate wie ISAE 3000/3402 nach BSI C5 zu erlangen oder aufrechterhalten, vgl. z.B. Kriterium OPS-19 "Umgang mit Schwachstellen, Störungen und Fehlern - Penetrationstests" im BSI C5:2020.

- **Länge:**
  Die Länge des Berichts ergibt sich aus der Anzahl der identifizierten Schwachstellen. Ziel ist es, alle relevanten Informationen zu vermitteln. Dabei sollten Redundanzen im Bericht vermieden werden, um diesen nicht aufzublähen.

- **Zielbeschreibung:**
  Die Zielbeschreibung stellt den Ausgangspunkt des Berichts dar. Sie muss klar definieren, welche Systeme, Anwendungen oder Netzwerke Gegenstand des Penetrationstests waren. Dies umfasst eine detaillierte Auflistung der zu prüfenden Systeme und deren sicherheitsrelevanter Aspekte. Die Zielbeschreibung sollte zudem die Zielsetzung des Penetrationstests erläutern, beispielsweise die Identifikation kritischer Schwachstellen oder die Überprüfung der Wirksamkeit bestehender Sicherheitsmaßnahmen.

6.1.1 Management Summary

Das Management Summary ist ein integraler Bestandteil des Berichts und sollte darin als erstes Kapitel erscheinen. Es fasst die wesentlichen Ergebnisse des Penetrationstests in kurzer und prägnanter Form zusammen. Dabei ist es wichtig, technische Details auf ein Minimum zu reduzieren und den Fokus auf die strategischen Risiken und Handlungsempfehlungen zu legen. Die zentrale Frage, die das Management Summary beantworten muss, lautet: "Welche Gefahren bestehen für die Organisation und wie können diese reduziert werden?"

Inhalte des Management Summarys

- **Einleitung: Wer, was, wann, wo?**
- **Haupterkenntnisse:** Übersicht über die kritischsten Schwachstellen.
- **Bewertung**[9]**:** Eine qualitative Bewertung der Schwachstellen nach ihrer Kritikalität.
- **Empfohlene Maßnahmen:** Kurzfassung der wesentlichen Empfehlungen zur Risikominderung. Dabei sollten die Maßnahmen priorisiert werden, die entweder die schwerwiegendsten Risiken mindern oder einen hohen QuickWin versprechen.
- **Vergleich zu ähnlichen Organisationen (optional):** Wenn möglich, sollte das Ergebnis des Penetrationstestes in Relation zu vergleichbaren Organisationen gesetzt werden. Damit kann es Entscheidungsträgern erleichtert werden, das Ergebnis besser zu verstehen und notwendige Entscheidungen herbeizuführen.

Hinweis: Insbesondere, wenn Manager aus nicht-technischen Bereichen zur Zielgruppe des Berichts gehören, sollte der Auftraggeber dem Penetrationstester dies spätestens beim Kick-Off Meeting mitteilen, um sicherzustellen, dass hinreichend allgemeinverständliche Formulierungen verwendet werden.

6.1.2 Übersicht der Schwachstellen (Tabelle / Grafik)

- **Tabelle**: Übersicht geordnet nach Kritikalität (ID / Risikoeinstufung / Kapitel / Seite / Bezeichnung)
- **Grafische Übersicht**: z.B. Balkendiagramm (kritisch / hoch / mittel / gering / Empfehlung)

6.1.3 Testplan und Methodik

Der Testplan beschreibt den strukturellen Ablauf des Penetrationstests. Er sollte eine detaillierte Darstellung der geplanten und durchgeführten Testaktivitäten enthalten. Dies umfasst:

- **Zeitplan:** Eine Übersicht über den zeitlichen Ablauf des Penetrationstests.
- **Umfang:** Definition des Umfangs des Penetrationstests, d. h. welche Systeme, Anwendungen und Netzwerke untersucht wurden.
- **Vorgehensweise / Testbedingungen**: Auf welche Weise fand der Zugriff statt? Mit / ohne Bereitstellung von Zugangsdaten

Grundlagen und Methodik
Eine detaillierte Beschreibung der Methodik und der eingesetzten Tools ist unerlässlich, um die Nachvollziehbarkeit der Ergebnisse sicherzustellen. Die Methodik sollte sich an anerkannten Standards orientieren, wie z.B. der OWASP Testing Guides.

Methodik:
- **Angriffsszenarien:** Beschreibung der simulierten Angriffsszenarien, die auf die spezifischen Risiken der Zielumgebung abgestimmt sind.
- **Testmethoden:** Erläuterung der eingesetzten Testmethoden, z.B. Netzwerkscans, Schwachstellenanalyse, Exploitation etc.

6.1.4 Schwachstellen

Die Dokumentation der identifizierten Schwachstellen ist der Kern des Berichts. Jede Schwachstelle sollte detailliert beschrieben werden, einschließlich:

- **Allgemeine Beschreibung:** Eine umfassende Darstellung der Schwachstelle inklusive der betroffenen Komponenten und der spezifischen Sicherheitslücken.

[9] An dieser Stelle wird in Berichten teilweise von Risikobewertungen gesprochen. Formal muss diese, ggf. mit Unterstützung des Penetrationstestanbieters, vom Auftraggeber selbst durchgeführt werden. Im Rahmen eines Penetrationstests stehen in der Regel nicht alle notwendigen Informationen (Einordnung des Prüfobjekts im Unternehmenskontext, finanzielle Auswirkungen, ...) zur Verfügung, um das konkrete Risiko zu ermitteln.

- **Auswirkung (optional):** Bewertung der potenziellen Auswirkungen auf die Organisation, wenn die Schwachstelle ausgenutzt wird. Dies umfasst eine Analyse der möglichen Schäden für Vertraulichkeit, Integrität und Verfügbarkeit.
- **Proof-of-Concept (PoC):** Ein technischer Nachweis, der belegt, dass die Schwachstelle real existiert und ausnutzbar ist. Dies sollte durch reproduzierbare Schritte unterstützt werden, einschließlich Screenshots, Logs oder Skripten. Bei den genutzten Tools sollte die genutzte Version mit aufgeführt sein.
- **Bewertung:** Die Schwachstelle sollte anhand eines **nachvollziehbaren** Bewertungsschemas, wie dem Common Vulnerability Scoring System (CVSS), dem Exploit Prediction Scoring System (EPSS), oder einer **sonstigen nachvollziehbaren, klar definierten Metrik** (z.B. Festlegung von vereinfachten Kategorien wie "kritisch", "hoch", "mittel", "niedrig") bewertet werden. Diese Bewertung hilft dabei, die Dringlichkeit der Behebung einzuschätzen.
- **Empfehlung:** Für jede Schwachstelle sollten konkrete Handlungsempfehlungen gegeben werden. Diese sollten sowohl technische Maßnahmen (z.B. Patches, Konfigurationsänderungen) als auch organisatorische Maßnahmen (z.B. Schulungen, Prozessanpassungen) umfassen.

6.2 Umgang mit Rohdaten

Im Rahmen des Penetrationstests fallen zahlreiche Rohdaten an, wie z.B. Logs, Scans oder Debug-Informationen. Diese Daten sind für die Erstellung des Berichts unerlässlich, sollten jedoch nicht im Bericht selbst enthalten sein. Rohdaten können für den Leser schwer verständlich sein und das Verständnis des Berichts erschweren. Zudem verursachen sie einen erheblichen Mehraufwand bei der Verarbeitung und Analyse.

Empfehlungen für den Umgang mit Rohdaten:

- **Zusammenfassung:** Statt Rohdaten sollte der Bericht eine Zusammenfassung der wesentlichen Erkenntnisse enthalten.
- **Anhang:** Falls erforderlich, können ausgewählte Rohdaten in einem separaten Anhang bereitgestellt werden, um technische Nachweise zu unterstützen oder ggf. den jeweiligen Fachverantwortlichen in der IT zur weiteren Evaluierung der Schwachstelle zu dienen.
- **Archivierung:** Rohdaten sollten sicher archiviert und bei Bedarf zur weiteren Analyse bereitgestellt werden.
- **Zeitliche Begrenzung:** Rohdaten sollten nur zeitlich begrenzt vorgehalten werden, um die Sicherheit des Unternehmens nicht zu gefährden.

7 Projektablauf Penetrationstest

7.1 Vorbereitung und Planung

Der Erfolg eines Penetrationstests hängt maßgeblich von der richtigen Vorbereitung ab. Dessen Planung kann bestimmte Merkmale aufweisen, die einen Penetrationstest besonders effektiv machen können.

1. Reifegrad des Unternehmens:
Alle Branchen und Unternehmen sind so einzigartig wie die Menschen, die bei ihnen arbeiten. So verhält es sich zumeist auch bei dem zugrundeliegende IT-Sicherheitsniveau und der Wirksamkeit des Maßnahmenmixes. Grundsätzlich ist die Durchführung von Penetrationstests unabhängig vom Reifegrad des Unternehmens zur Erhöhung des IT-Sicherheitsniveaus immer sinnvoll.

- **Geringer IT-Sicherheitsreifegrad**
  Entgegen einiger Meinungen kann die Durchführung eines Penetrationstests auch bei Unternehmen mit einem geringen Reifegrad der IT-Sicherheit bereits sinnvoll sein. Häufig sind bei diesen Unternehmen bereits erste Sicherheitsmaßnahmen und -prozesse in der Praxis etabliert, jedoch noch nicht einheitlich standardisiert, umfassend und nachvollziehbar dokumentiert. Folglich fällt es den Verantwortlichen oft schwer, den Fokus für einen Penetrationstest zu definieren und abzugrenzen. In einem solchen Fall kann vor einem Penetrationstest eine zusätzliche Bestandsaufnahme der IT-Sicherheit, z.B. durch einen ISACA Cyber-Sicherheits-Check oder vergleichbarer ISMS Gap-Analyse-Dienstleistungen, hilfreich sein, um den Scope des Penetrationstests festzulegen. Im Zuge des Penetrationstests werden Schwachstellen auf technischer Basis überprüft, Schwachstellen identifiziert und die Wirksamkeit der zugrundeliegenden Sicherheitsmaßnahmen und -prozesse bestätigt oder widerlegt, so dass im Nachgang eine fokussierte Nachbesserung zur Erhöhung des Sicherheitsniveaus ermöglicht wird. In Abhängigkeit der Testergebnisse lassen sich häufig neben den technischen Maßnahmen auch prozessuale und strukturelle Verbesserung zur IT-Sicherheit ableiten.

  Die Ausgangsbasis und typischen Leistungsmodule für Penetrationstests von Unternehmen mit einem geringen IT-Sicherheitsreifegrad lassen sich typischerweise wie folgt zusammenfassen. Beispiele für Module finden sich im Abschnitt 8.

Dokumentationsgrad:	• niedrig
Prozessgrad:	• niedrig
Maßnahmenmix:	• niedrig bis mittel
Anzahl involvierter Dienstleister:	• niedrig
Gesamtkomplexität:	• niedrig
Exemplarische Leistungsabrufe:	• Tests auf Netzwerkebene von extern gegen alle im Internet erreichbaren Systeme • Tests auf Anwendungsebene von extern gegen eine ausgewählte Webanwendung • Tests auf Netzwerkebene von intern gegen alle Server- und ausgewählte Client-Systeme • Tests auf Netzwerk- und Systemebene von intern gegen den zentralen Microsoft Active Directory Server

- **Fortgeschrittener Reifegrad**
  Bei einem fortgeschrittenen Reifegrad der IT-Sicherheit eines Unternehmens sind die Sicherheitsprozesse meist ausreichend gut dokumentiert und weitgehend standardisiert. Penetrationstests sollten jetzt integraler Bestandteil der Sicherheits- und Compliance-Prozesse sein und regelmäßig durchgeführt werden, um die implementierten Sicherheitsmaßnahmen kontinuierlich auf ihre Robustheit hin zu überprüfen. Unternehmen können hier bereits häufig besser bestimmen, auf welche Sicherheitsaspekte des Unternehmens bzw. welche Angriffsvektoren der Penetrationstest abzielen soll, und die notwendigen Informationen für einen Penetrationstest wie Netzpläne und Systemarchitekturen bereitstellen, um den Penetrationstest möglichst effizient zu gestalten. Sind regelmäßige Penetrationstests bereits etabliert, kann zudem auch über Themen wie automatisierte Schwachstellenscans und weiterführende Tests, wie z.B. Red Teaming Assessments, nachgedacht werden.

Die Ausgangsbasis und typische Leistungsmodule für Penetrationstests von Unternehmen mit einem fortgeschrittene IT-Sicherheitsreifegrad lassen sich typischerweise wie folgt zusammenfassen:

Dokumentationsgrad:	• mittel bis hoch
Prozessgrad:	• mittel bis hoch
Maßnahmenmix:	• mittel bis hoch
Anzahl involvierter Dienstleister:	• niedrig bis hoch
Gesamtkomplexität:	• mittel bis hoch
Exemplarische Leistungsabrufe:	Testkategorien für Unternehmen mit geringem Sicherheitsreifegrad zuzüglich: • Tests auf Netzwerkebene von ausgewählten Netzbereichen gegen ausgewählte Systeme und Netzwerkperipherie • Tests von Release-Versionen auf Anwendungsebene • Spezifische Tests nach Migrationen und Enrollments von neuen Systemen • Spezielle Insider-Angriffe (Lateral Movement, Data Loss Prevention) • Tests von mobilen Client-Systemen wie Notebooks, Tablets und Smartphones • Red Teaming Assessments (inkl. Social-Engineering-Angriffsvektoren)

2. Teststrategien

Zur Minimierung von unternehmerischen Risiken ist ein Penetrationstest zu jedem Zeitpunkt und aus jedem Beweggrund sinnvoll. In der Praxis haben sich für die Momentaufnahme durch einen Penetrationstests folgende Merkmale als besonders geeignet herausgestellt:

- **Nach einer signifikanten Änderung an der Infrastruktur:**
  Wenn wesentliche Änderungen an der Infrastruktur, Software oder den Systemkonfigurationen vorgenommen werden, wie z.B. das Hinzufügen neuer Komponenten (z.B. Migration von Firewalls) oder zentraler IT-Infrastrukturdienste oder das Ändern der Netzwerkarchitektur (z.B. Netzwerksegmentierung, Anbindung von neuen Standorten oder Cloud-Diensten), sollte ein Penetrationstest durchgeführt werden, um sicherzustellen, dass die kontinuierliche Anpassung der IT-Infrastruktur gemäß der Geschäftserfordernisse aus sicherheitstechnischer Sicht nicht zu Schwachstellen, Compliance-Verstößen und unnötigen unternehmerischen Risiken führt.

- **Vor dem Go-Live eines neuen Systems oder einer Anwendung:**
  Bevor eine neue Anwendung, ein System oder eine Infrastruktur in Betrieb genommen wird, ist ein Penetrationstest unerlässlich, um potenzielle Sicherheitslücken zu identifizieren und zu beheben. Beispiele hierfür sind die Einführung neuer IT-Technologien, die Migration auf ein neues Produkt oder die Anbindung eines neuen Unternehmensstandortes.

- **Bei Verdacht eines Sicherheitsvorfall / Nach einem Sicherheitsvorfall (Post-Incident-Tests):**
  Wenn der Verdacht einer Sicherheitsverletzung oder eines Angriff besteht, ist es ratsam, zusätzlich zu den typischen Dienstleistungen der Digitalen Forensik und Incident Response (DFIR) auch ein sogenanntes Compromise Assessment und einen Penetrationstest durchzuführen, um festzustellen, ob die ursprünglichen Schwachstellen zur Kompromittierung nach wie vor durch Angreifer ausnutzbar sind und ob ggf. weitere potentielle Möglichkeiten zur Kompromittierung oder Wahrung des unbefugten Zugriffs eröffnet wurden. Um sicherzustellen, dass sich nicht ein Dienstleister selbst überprüft und ggf. bereits betriebsblind ist, sollte hier im Idealfall ein anderer Dienstleister gewählt werden.

- **Regelmäßigkeit:**
  Es ist wichtig, regelmäßige Penetrationstests durchzuführen, um sicherzustellen, dass das System auch weiterhin sicher bleibt. Penetrationstest sind immer eine Momentaufnahme. Sowohl Bedrohungen als auch Anwendungen, Systeme und IT-Infrastrukturen entwickeln sich ständig weiter, so dass diese Feststellung des Ist-Zustandes regelmäßig erneuert werden muss. Typischerweise werden im Sinne der Regelmäßigkeit feste Zeiträume wie beispielsweise die jährliche, halbjährliche oder quartalsweise Durchführung von Penetrationstests empfohlen. Alternativ zu iterierenden

Zeitfenstern hat sich auch die Durchführung in Anlehnung von Meilensteinplänen, Entwicklungsstufen und des Releasemanagement etabliert.

3. **Fokus und Umfang festlegen (Scoping)**:
Wie in Abschnitt 1.3 bereits erwähnt, ist der klar definierte Umfang (Fokus / Scope) des Penetrationstests entscheidend. Dazu gehört die Auswahl der Angriffsszenarien, die Spezifikation der zu testenden Systeme, aber auch die Entscheidung, welche technischen und organisatorische Teile des Unternehmens von der Prüfung ausgenommen sind (z.B. Produktionssysteme oder andere sensible / kritische Infrastruktur, die nicht gestört werden darf). Es wird auch festgelegt, welche Angriffstechniken verwendet werden dürfen bzw. welche ggf. ausgeschlossen werden müssen.

Im Abschnitt "Module" sind übliche Tests definiert und können als Grundlagen für eine Ausschreibung verwendet werden. Sofern die Module aufgrund sehr individueller Gegebenheiten nicht direkt anwendbar sind, umso eher sind Gespräche mit Dienstleistern sinnvoll, um ein zielgenaues Scoping der Tests zu erhalten.

4. **Budget und Ressourcen**:
Das Unternehmen sollte sicherstellen, dass die finanziellen Mittel und Ressourcen für die Durchführung eines Penetrationstests vorhanden sind. Dazu gehört sowohl die Finanzierung des externen Sicherheitsexperten zur Durchführung des Penetrationstests als auch die Bereitstellung von internen IT-Ressourcen zur Unterstützung des Penetrationstests (Vorbereitung, Ansprechpartner während des Tests) sowie für die danach zu erwartenden Arbeiten zur Behebung der Schwachstellen. Im Sinne des Best-Effort-Ansatzes und immer knapper werdender Budgets wird der risikobasierte Ansatz empfohlen, um die für das betroffene Unternehmen am gefährlichsten erscheinenden Angriffsvektoren mit einem Penetrationstest abzubilden. Ein risikobasierter Ansatz berücksichtigt die Art der Bedrohungen, denen jedes Unternehmen individuell ausgesetzt ist. Eine Branche bzw. ein Unternehmen, das im Vergleich zu anderen vermehrt Compliance-Anforderungen ausgesetzt ist, da kritische Finanzdaten oder personenbezogene Daten verarbeitet werden, sollte entsprechend häufiger und umfassendere Penetrationstests durchführen, um den Marktanforderungen zu genügen. Der Fokus des Penetrationstests sollte auf den Bereichen liegen, die das höchste Risiko für das Unternehmen darstellen.

7.2 Durchführung des Penetrationstests

Sobald die Planungsphase abgeschlossen ist, beginnt die eigentliche Durchführung des Penetrationstests. Die Durchführung kann sich dabei an verschiedenen Vorgehensmodellen, wie z.B. dem "Durchführungskonzept für Penetrationstests" des BSI orientieren. Typischerweise ergeben sich damit folgende Best Practices für den Ablauf:

1. **Vorbereitungsgespräch**
   In diesem Gespräch sollten noch einmal alle Details zum Penetrationstest zwischen Auftraggeber und Auftragnehmer besprochen werden. Genaueres zum Ablauf und Inhalt dieses Gesprächs ist in Abschnitt 3 und 4 festgehalten.

2. **Verbindungstests (Dry Run)**
   Vor Beginn der Testdurchführung wird zumeist ein sogenannter Verbindungstest seitens des Penetrationstestanbieters durchgeführt. Im Rahmen der Verbindungstests werden beispielsweise die Verbindung zu untersuchenden IP-Adressen, URLs oder zu nutzenden Testkonten ausprobiert. Nur wenn die Verbindungstests erfolgreich sind, kann der Penetrationstest wie zuvor geplant durchgeführt werden. Falls es hier zu Problemen kommt, müssen beide Vertragsparteien in die Problemanalyse einsteigen, um die notwendigen Voraussetzungen zur Testdurchführung herzustellen. Die fristgerechte Lieferung der Beistellleistungen obliegt dem Auftraggeber. Falls es dabei zu Problemen kommt, führt das meist unweigerlich zu einer Verschiebung der ursprünglich vereinbarten Zeitpläne. Um Projektverschiebungen und unnötige Kosten zu vermeiden, wird empfohlen, diese wichtige Vorbereitungsphase ca. eine bis zwei Wochen vor der Testdurchführung anzugehen.

3. **Testdurchführung**

- **Informationsbeschaffung (Reconnaissance / passiver Penetrationstest)**: Der erste Schritt in der Durchführung ist die Sammlung von Informationen. Dies kann z.B. im Fall eines Penetrationstests der IT-Infrastruktur mittels automatisierter Port- und Schwachstellenscans erfolgen. Im Fall einer Webseite wäre das z.B. ein Walkthrough des Testers durch die Anwendung, ggf. gepaart mit automatisierten Webseiten-Crawlern. Mit der Informationssammlung verschafft sich der Tester erste

Anhaltspunkte zur Angriffsfläche, um zu entscheiden, welche Aspekte er wie im weiteren Projektverlauf testet.

- **Aktive Angriffe**: In diesem Schritt wird versucht, die in der Informationsbeschaffung identifizierten potenziellen Schwachstellen zu verifizieren (um False Positives auszuschließen), und es werden weitere Prüfpunkte durchgeführt, beispielsweise zum Umgehen von Authentifizierungsmechanismen oder zum Erlangen von Administratorrechten.

- **Optional Post-Exploitation und lateral movement**: Nachdem ein Angriffspunkt erfolgreich ausgenutzt wurde, prüft der Tester, wie weit er sich im Netzwerk des Unternehmens bewegen kann. Dies geschieht im Rahmen der vorher abgesteckten Grenzen (Scope des Tests). Dies umfasst das Erlangen von Zugriffsrechten auf weitere Systeme und das Ausweiten des Angriffs, z.B. mit dem Ziel, Domänenadministratorrechte zu erlangen.

- **Auswertung und Dokumentation der Ergebnisse**
  Die Erkenntnisse des Penetrationstests werden nun detailliert in einem Bericht dokumentiert und dem Auftraggeber zur Verfügung gestellt. Das Thema Berichterstellung ist im Abschnitt 6 detailliert ausgeführt.

- **Clean-UP**
  Etwaige Spuren, die durch den Penetrationstest verursacht wurden, müssen aufgeräumt werden, um kein Einfallstor für Angreifer zurückzulassen (z.B. Remoteshells, Test-Accounts, etc.).

Das Vorgehensmodell kann abhängig vom Fokus des Penetrationstest auch abweichen. Das oben skizzierte Vorgehensmodell wird zumeist bei einem Penetrationstest von IT-Infrastrukturkomponenten und Netzen angewendet.

4. Nachbereitung und Implementierung der Maßnahmen

Nach Abschluss des Penetrationstests gilt es, die identifizierten Schwachstellen wirksam zu beseitigen. Diese wichtige Phase erfolgt häufig in enger Zusammenarbeit mit der internen IT-Abteilung oder externen Dienstleistern. Die nachfolgenden Aktivitäten sind besonders wichtig:

- **Ergebnisse analysieren und priorisieren**: Ein Penetrationstest liefert einen detaillierten Bericht, der die Schwachstellen aufzeigt und Empfehlungen zur Behebung gibt. Dabei ist es wichtig, die Prioritäten richtig zu setzen. Nicht jede Schwachstelle hat die gleiche Dringlichkeit. Die Abarbeitung sollte daher auf Basis des Schweregrads der Schwachstellen und einer internen Risikobewertung erfolgen (falls ein ISMS/BCM vorhanden ist). Kritische Sicherheitslücken, die sofortigen Zugriff auf sensible Daten ermöglichen, sollten vorrangig behandelt werden, während weniger schwerwiegende Lücken mit weniger Dringlichkeit angegangen werden können.

- **Externe Hilfe**: In vielen Fällen kann es sinnvoll sein, externe Experten hinzuzuziehen, um komplexe Schwachstellen zu beheben, insbesondere, wenn interne Ressourcen fehlen oder spezielle Expertise erforderlich ist. Dies gilt insbesondere bei der Behebung von Schwachstellen, die tief in der Architektur des Unternehmenssystems verwurzelt sind oder wenn spezielle und tiefgehende Produktkenntnisse erforderlich sind.

- **Regelmäßige Tests und Monitoring**: Ein einmaliger Penetrationstest reicht nicht aus, um die Sicherheitslage eines Unternehmens langfristig zu gewährleisten. Es sollte ein kontinuierlicher Prozess etabliert werden, der regelmäßige Tests und Monitoring umfasst. Dies hilft, neue Schwachstellen schnell zu identifizieren und frühzeitig Gegenmaßnahmen zu ergreifen.

8 Module

8.1 Penetrationstest aus dem Internet erreichbarer IP-Adressen

8.1.1 Einleitung und Zielsetzung:

- Es werden alle extern erreichbaren IP-Adressen auf offene Ports und bekannte Schwachstellen in den erreichbaren Diensten (Prüfung des Perimeters) ohne Authentisierung geprüft. Ergänzend folgen manuelle Prüfungen und die Verifikation der automatisiert ermittelten Scanergebnisse (Toolergebnisse) durch Experten.
- Die Prüfung sollte regelmäßig (z.B. jährlich) erfolgen. Somit ist das Angriffsszenario, dass Angreifer bekannte Schwachstellen ausnutzen können, deutlich reduziert.

8.1.2 Fokus und Umfang

Automatisierte Scan und Analyse, z.B.:

a. Durchführen von Portscans (TCP fullscan, UDP-definierte Ports)
b. Durchführen von toolgestützten Schwachstellenscans (z.B. OpenVAS, Nessus, Qualys)

Auswertung und Verifikation der Scan-Ergebnisse, z.B.:

c. Ausschließen von False Positives
d. Kontextspezifische Bewertung des Schweregrads der Schwachstellen

Manuelle Tests, z.B.:

e. Durchführen protokollspezifischer Testfälle auf Basis der Scan-Ergebnisse (z.B. DNS, SNMP, etc. Jedoch keine manuelle tiefergehende Prüfung von Webanwendungen/APIs)
f. Umgehung von dynamischen Angriffserkennungsfunktionen (z.B. Firewall, IDS/IPS)
g. Prüfen von Authentifizierungsmechanismen

8.1.3 Abgrenzung

- Prüfung IDS/IPS/WAF; Diese Technologien sind dynamische Angriffserkennungssysteme. Sie erkennen anhand von Parametrisierung Angriffsmuster und sperren dann meist Quelladressen aus. Da Penetrationstests effizient ablaufen sollen, sind sie "laut" und damit sehr einfach erkennbar. Ein echter Angreifer hätte aber im Vergleich mehr Zeit. Daher sollten die dynamischen Angriffserkennungsfunktionen für die Quelladressen der Tester deaktiviert werden, um das Firewall-Regelwerk und die erreichbaren Dienste auf Korrektheit und bekannte Schwachstellen zu prüfen.

- OSINT: Im Regelfall sollte einer Organisation bekannt sein, welche IP-Adressen im Internet erreichbar sind. Diese Adressen werden an die Prüfer übergeben. Sollte Unsicherheit herrschen, kann auch eine OSINT-Analyse erreichbarer IP-Adressen zum Abgleich mit internen Informationen sinnvoll sein. Für diesen Fall sollte ein sinnvoller Aufwand für die OSINT-Analyse vereinbart und ggf. eine OSINT-Analyse beauftragt werden.

- Exploiting: Im Regelfall genügt die Information, dass eine potenzielle Schwachstelle erkannt wurde. Exploiting liefert im Regelfall keinen zusätzlichen Erkenntnisgewinn und verursacht Mehraufwände.

8.1.4 Notwendige Angaben für eine sinnvolle Ausschreibung

- Wie hoch ist die Anzahl zu prüfender IP-Adressen / bzw. IP-Netze, die Anzahl der aktiven IP-Adressen?
- Werden dynamische Angriffserkennungsfunktionen wie IDS / IPS eingesetzt? Können die dynamischen Angriffserkennungsfunktionen für die Penetrationstest-Quell-IPs deaktiviert werden?

8.2 Penetrationstest ausgewählter Adressen / Netzbereiche aus dem internen Netzwerk

8.2.1 Einleitung und Zielsetzung

Im Rahmen des internen Penetrationstests sollen zuvor definierte, aus dem internen Unternehmensnetz erreichbare IP-Adressen bzw. Netzbereiche (z.B. Server-VLANs) ohne interne Nutzerkennung (ohne Authentisierung) auf bekannte Schwachstellen geprüft werden. Ergänzend folgen manuelle Prüfungen und die Verifikation der automatisiert ermittelten Scanergebnisse (Toolergebnisse). Zudem wird geprüft, ob Ziele in anderen internen Netzwerkbereichen vom definierten Ausgangspunkt des Tests (z.B. Client- oder Server-VLAN) erreicht werden können (Segmentierungstest). Typische Beispiele für Segmentierungstests sind sensible Netzbereiche wie DMZ, Managementnetze oder Netzwerke mit Produktionsanlagen.

Der interne Penetrationstest sollte regelmäßig erfolgen. Ein übliches Intervall ist mindestens einmal jährlich. Weitere Anforderungen können durch Regulierungs-Frameworks wie NIS2 oder ISO27001 erfolgen. Sofern bereits ein Vulnerability Management mit regelmäßigen Schwachstellen-Scans etabliert ist, können die Prüfungen ggf. auch in größeren Abständen erfolgen (z.B. alle zwei Jahre).

Somit sind viele der üblichen internen Angriffsszenarien ohne spezielle Rechte (z.B. Innentäter, Dienstleister) geprüft.

8.2.2 Fokus und Umfang

Für den Umfang des Tests sollten vorab insbesondere zwei Aspekte besprochen werden:

1. Aus welcher Perspektive bzw. mit welchem Ausgangspunkt des Testers der Test durchgeführt wird. Die Frage kann auch lauten: "Welches Angriffsszenario möchte ich nachstellen?". Je nachdem, ob z.B. aus dem Client-, Server- oder Managementnetz getestet wird, werden sich die Ergebnisse des Tests unterscheiden. Typische Ausgangspunkte für einen Test sind entweder das Clientnetzwerk (Angriffsszenario: übernommener Client im Firmennetz) und / oder aus dem Servernetz (Annahme: der Angreifer hat den ersten Verteidigungsperimeter bereits überwunden). Es ist auch möglich, mehrere Sichtweisen zu kombinieren, was entsprechend zu höheren Aufwänden führt. Auch die Kombination mit weiteren internen Modulen (z.B. AD-Test) kann sehr sinnvoll sein und wird von den Autoren empfohlen.

2. Welche Teststrategie wird verfolgt? Insbesondere bei größeren Netzwerken, die einen vollumfänglichen Penetrationstest schnell sehr aufwändig und teuer machen können, ist es empfehlenswert, eine der folgenden Strategien zu nutzen:
   a. Auswahl einer geeigneten Menge an Beispielsystemen aus der Gesamtmenge und vollumfänglicher Test dieser Systeme (kein exploratives Testen). Die Auswahl der Samples für den Test sollte so erfolgen, dass sie die wichtigsten Systeme und Systemtypen abdecken, z.B. besonders kritische Systeme (Bsp.: Domain-Controller, Business-kritische Server) und mehrfach vorkommende, sich stark ähnelnde Systeme (Clients, Netzkomponenten, Server-Images). Auch einzelne Unternehmensstandorte können eine geeignete Teilmenge sein. Diese ausgewählten Sample-Systeme werden im Rahmen des Penetrationstests geprüft. Bei gefundenen Schwachstellen ist es wahrscheinlich, dass diese auch auf identischen oder ähnlichen Systemen auftreten. Auch Standorte können in ihrer Netzstruktur ähnlich aufgebaut sein. Ein Nachteil dieser Variante ist, dass im Rahmen des durchgeführten Tests die Gesamtsicht aufs Netzwerk fehlt. Manche Systeme, die der Auftraggeber als identisch oder ähnlich betrachtet, unterscheiden sich

ggf. dennoch und dieser Unterschied kann bereits ein Risiko / eine unidentifizierte Schwachstelle ausmachen. Ein Vorteil ist, dass die gewählte Teilmenge der Systeme jedoch vollumfänglich geprüft ist und der Test daher eine gute Aussage über die Sicherheit dieser Systeme liefert.

b. Es wird das gesamte Netzwerk mit allen darin enthaltenen Systemen geprüft, dabei wird aber ein explorativer Testansatz in Kombination mit einem Time-Box-Ansatz gewählt. Dies bedeutet, dass hierbei in Absprache zwischen Auftraggeber und Auftragnehmer vorab ein Budget für Testzeit festgelegt wird. Der Auftragnehmer wird hierzu auf Basis seiner Erfahrungswerte eine Empfehlung aussprechen, welches Budget eine möglichst gute Testabdeckung und einen hohen Erkenntnisgewinn gewährleistet. Anschließend werden im Rahmen der zur Verfügung stehenden Testzeit auf Basis etablierter Testvorgehensmodelle, aber auch auf Basis der Erfahrung des Testers, die wichtigsten Angriffsvektoren priorisiert und anschließend im Rahmen des Tests überprüft. Der Test endet nach dem definierten Zeitbudget. Dabei kann es sein, dass nicht alle Prüfpunkte auf allen Systemen innerhalb des Netzwerks geprüft werden können - der Tester geht explorativ vor und konzentriert sich auf besonders kritische Komponenten oder Schwachstellen. Ein Nachteil dieser Variante ist, dass niedriger priorisierte Systeme, Angriffsvektoren, oder Schwachstellen (Bsp.: SSL/TLS) ggf. ungeprüft bleiben und in den Testeinschränkungen vermerkt werden müssen. Ein Vorteil ist, dass trotz knappen Budgets die wichtigsten Sicherheitsaspekte im gesamten Netz geprüft werden und sich der Auftraggeber im Nachgang auf schwerwiegendsten Risiken und Schwachstellen konzentrieren kann.

Die Testdurchführung ist sowohl onsite als auch remote möglich. Im beiden Fällen müssen entsprechende Zugangsvoraussetzungen für den Tester geschaffen werden. Für einen Remote-Test muss z.B. VPN-Zugriff auf eine Kali-VM, die im zuvor definierten Ausgangspunkt platziert ist, bereitgestellt werden. Für Onsite-Tests muss der Tester mit seinem Testnotebook Zugriff auf das interne Netzwerk erhalten (NAC-Freischaltung) und sich mit seinem Notebook am zuvor definierten Ausgangspunkt für den Test befinden.

Im Rahmen des internen Penetrationstests sollten folgende Testschwerpunkte überprüft werden:

Automatisierte Scan und Analyse, z.B.:
- Durchführen von Portscans (TCP fullscan, UDP-definierte Ports) auf die definierten Netzbereiche
- Durchführen von toolgestützten Schwachstellenscans (z.B. OpenVAS, Nessus, Qualys) auf die definierten Netzbereiche

Auswertung und Verifikation der Scan-Ergebnisse, z.B.:
- Ausschließen von False Positives
- Kontextspezifische Bewertung des Schweregrads der Schwachstellen

Manuelle Tests, z.B.:
- Durchführen protokollspezifischer Testfälle auf Basis der Scan-Ergebnisse (z.B. DNS, SNMP, etc., jedoch keine manuelle tiefergehende Prüfung von Webanwendungen/APIs)
- Umgehung von dynamischen Angriffserkennungsfunktionen (z.B. Firewall, IDS/IPS)
- Prüfen von Authentifizierungsmechanismen (Standardpasswörter, Nutzerpasswörter, …)
- Versuch, Zugriff auf sensitive Daten / Systeme zu erlangen (z.B. SMB, SNMP, …)

Prüfung der Netzwerksegmentierung, z.B.
- Durchführen von Erreichbarkeitstests gegen definierte Zielbereiche
- Überprüfung der Möglichkeit zur Umgehung von Erreichbarkeitsbeschränkungen (Firewall)

8.2.3 Abgrenzung

- Zuvor muss mit dem Auftraggeber geklärt werden, ob der interne Penetrationstest eine Prüfung zur Ausbreitung eines Angriffes (Lateral Movement) beinhalten soll. Technologien wie IPS und IDS werden häufig zur Erkennung und Verhinderung von Angriffen eingesetzt. Sie erkennen Angriffsmuster und sperren dann meist Quelladressen aus. Da Penetrationstests effizient ablaufen sollen, sind sie "laut" und damit für IDS/IPS sehr einfach erkennbar. Ein echter Angreifer hätte aber im Vergleich mehr Zeit und würde "leiser" vorgehen. Daher kann er ggf. unerkannt bleiben.
    - Die dynamischen Angriffserkennungsfunktionen sollten zunächst für die Quelladressen der Tester deaktiviert werden (Whitelisting), um den Test effizient durchführen zu können. Nach Abschluss der ersten Testphase sollte überlegt werden, in einer zweiten Testphase mit

aktivierter IDS/IPS zu testen, um auch die Wirksamkeit dieser Systeme mit einzubeziehen. Hinweis: Dieses zweistufige Vorgehen erzeugt höhere Aufwände, und muss daher zwischen Auftraggeber und Auftragnehmer während der Angebotsphase berücksichtigt werden.

- Active Directory ist ein separates Testmodul und daher sind AD-spezifische Testfälle nicht Bestandteil dieses Moduls.
- Bei großer Anzahl von Systemen sollte aus Effizienzgründen neben den hochpriorisierten Systemen nur eine exemplarische Prüfung niedrig priorisierter Systeme (z.B. Client-Systeme) stattfinden
- Es wird keine Prüfung von Netzwerken mit Produktionsanlagen oder ähnlich sensiblen Systemen im Rahmen eines internen Penetrationstests durchgeführt. Hier erfolgt ein interner Penetrationstest mit besonderen Anforderungen im Rahmen eines extra Prüfmoduls.
- Keine Ausführung von Exploits

8.2.4 Notwendige Angaben für eine sinnvolle Ausschreibung

- Anzahl zu prüfender IP-Adressen/bzw. IP-Netze,
    - Anzahl der aktiven IP-Adressen in den zuvor definierten Netzbereichen (z.B. x aktive IP-Adressen im Servernetz und y aktive IP-Adressen im Client- oder Druckernetz)
    - Wie viele Systeme davon sind Server (VMs)?
- Nach welchem Prinzip erfolgt die Netzsegmentierung (z.B. nach Funktion wie Management, Server, Client, Drucker, nach Standorten, …)?
- Ist Firewalling zwischen den Netzsegmenten aktiv? Falls ja, welches Netz soll Ausgangspunkt des Penetrationstests sein? Sollen ggf. mehrere Ausgangspunkte eingenommen werden?
- Werden dynamische Angriffserkennungsfunktionen wie IDS / IPS eingesetzt? Sollen diese im ersten Testschritt deaktiviert und in einem zweiten Testschritt mitgeprüft werden? Wenn ja, können die dynamischen Angriffserkennungsfunktionen für die Penetrationstest-Quell-IPs deaktiviert werden?

8.3 Active Directory Penetrationstest (Assumed Breach)

8.3.1 Einleitung und Zielsetzung

Das Active Directory verwaltet Benutzerkonten und Berechtigungsstrukturen in großen Umgebungen. Gelingt es einem Angreifer, Zugriff auf ein privilegiertes Benutzerkonto zu erlangen, so stehen diesem weitreichende Berechtigungen auf sensible Daten zur Verfügung. Mit diesen Zugriffen ist es möglich, eine große Menge an Daten zu exfiltrieren und Infrastrukturen im Nachgang zu verschlüsseln. In der Vergangenheit zeigte sich das Active Directory regelmäßig als primäres Ziel von Angreifern, denen bereits ein initialer Zugriff auf eine interne Infrastruktur gelungen war. Um die Umgebung prüfen zu können, sollten für die Durchführung eines Penetrationstests folgende Voraussetzungen erfüllt sein:

- Den Testern wird ein Arbeitsplatzrechner in einer typischen Konfiguration und Netzwerkzugriff bereitgestellt, sodass die Kommunikation mit den Domain Controllern, dem Client- und dem Servernetzwerk möglich ist. Der ebenfalls zur Verfügung gestellte Benutzer hat eine Berechtigungsstufe, die üblicherweise von Mitarbeitern des Unternehmens genutzt wird.
- Geprüft wird, wie ein Angreifer mit Zugang zu einem (kompromittierten) Benutzerkonto auf einfache Weise mehr Privilegien erlangen oder Zugriff auf sensitive Systeme oder Daten erhalten kann.
- Zur Verbesserung der Analysemöglichkeiten ist es sinnvoll, neben dem niedrig privilegierten Benutzerkonto ein weiteres mit lokalen Administrationsrechten bereitzustellen, um auf relevante Konfigurationsparameter zuzugreifen, Testsoftware zu installieren und ohne Einschränkungen ausführen zu können.
- Ergänzend sollte es den Penetrationstestern möglich sein, einige der Überprüfungen von einem eigenen Testsystem durchzuführen, um den Aufwand durch die Installation von Testsoftware zu minimieren. Die Durchführung der Tests ohne vorkonfigurierten Arbeitsplatzrechner ist ebenfalls möglich, wobei die für das Unternehmen typische Systemkonfiguration in diesem Fall nicht mitgeprüft werden kann.

8.3.2 Fokus und Umfang

- Versuch der (unautorisierten) Enumeration des Active Directory sowie Analyse der durch Domänencontroller bereitgestellten Informationen
- Identifikation privilegierter und sicherheitskritischer Konten sowie Analyse von Berechtigungsstrukturen, Gruppenmitgliedschaften und Delegationen
- Aufdeckung sicherheitsrelevanter Fehlkonfigurationen im Active Directory, einschließlich der Überprüfung von Vertrauensstellungen zwischen Domänen oder Forests sowie der Active Directory Certificate Services (AD CS), sofern vorhanden
- Prüfung der Authentifizierungsmechanismen auf Schwachstellen, beispielsweise durch Passwort-Spraying, die Identifikation schwacher Passwörter oder die Bewertung möglicher NTLM-oder Kerberosangriffe
- Identifikation und Validierung von Möglichkeiten zur Privilege Escalation und Lateral Movement innerhalb der Domäne mit dem Ziel, privilegierte Berechtigungen (z.B. Domänenadministratorrechte) oder andere kritische Nutzerkonten (z.B. Geschäftsführung, IT-Mitarbeiter) zu erlangen
- Überprüfung der Wirksamkeit von Sicherheitsmechanismen (z.B. Tiering, Administrative Separation, Credential Guard, LAPS, Windows LAPS, Protected Users), sofern vorhanden
- Überprüfung von Netzwerkfreigaben (Shares), Dateiverzeichnissen und weiteren für den Testbenutzer zugänglichen Ressourcen auf sicherheitsrelevante oder vertrauliche Informationen sowie auf unzureichend geschützte Berechtigungen
- Sofern mit dem vereinbarten Testumfang vereinbart, Prüfung, ob ausführbare Skripte oder Programme in freigegebenen Bereichen abgelegt oder verändert werden können, um potenzielle Risiken durch unsichere Berechtigungen oder Ausführungsmechanismen aufzuzeigen

8.3.3 Abgrenzung

- Interne Active-Directory-Strukturen werden immer häufiger durch Cloud-basierte Lösungen (Microsoft Entra ID) ergänzt oder abgelöst. Während bei der Prüfung solcher hybrider oder reiner Cloud Infrastrukturen ähnliche Ziele verfolgt werden, weicht die Vorgehensweise von der hier beschriebenen ab und wird in einem zukünftig zu erstellenden alternativen Modul dokumentiert.
- Die detaillierte Prüfung etwaiger Dienste (SQL-Server, Webserver, ...), die das AD zur Autorisierung nutzen, ist nicht im Umfang dieses Moduls enthalten und muss separat betrachtet werden.
- Prüfhandlungen aus dem internen Penetrationstest (**Fehler! Verweisquelle konnte nicht gefunden werden.**) sind nicht Teil einer Analyse des Active Directory und sollten separat betrachtet werden.

8.3.4 Notwendige Angaben für die Angebotserstellung

- Architektur der Domäne(n)
    - Anzahl der Domänencontroller und Domänen
    - Beschreibung der Vertrauensstellungen zwischen den Domänen
    - Art und Anzahl von auf AD-Berechtigungen vertrauenden Diensten
    - Anzahl der in die Domäne eingebundenen Systeme und Nutzer
- Übersicht über das Rechte- und Rollenmodell

8.4 Entra ID-Analyse

8.4.1 Einleitung und Zielsetzung

- Anstelle von Active Directory kommt insbesondere bei KMUs immer häufiger Microsoft Entra ID als zentrale Lösung für das Identity und Access Management (IAM) zum Einsatz. Während sich wesentliche Grundkonzepte in Bezug auf die Zuweisung von Rechten und Rollen zu Benutzern und Diensten ähneln, unterscheiden sich die verwendeten Technologien stark, so dass andere Werkzeuge und Herangehensweisen für die Prüfung der Sicherheit notwendig sind.

- In der Regel ist zur Überprüfung ein Review der entsprechenden Einstellung im Microsoft M365 Tennant einem reinen Penetrationstest aus Perspektive eines Benutzers vorzuziehen. Letzteres sollte ergänzend im Umfang der Prüfung enthalten sein.

Damit wird das Angriffsszenario privilegierter Nutzer auf die Entra-ID-Umgebung geprüft.

8.4.2 Fokus und Umfang

- Der Fokus der Untersuchung liegt auf dem implementierten Rechte- und Rollenkonzept sowie der Aufdeckung möglicher Eskalationspfade vom einfachen Benutzer oder einer Managed Identity zu weiterreichenden Rechten. Ein wesentlicher Faktor ist dabei die Delegation von Berechtigung.
- Darüber hinaus gilt es, die grundlegende Sicherheit des verwendete Microsoft M365 Tennant zu überprüfen und eine angemessene Protokollierung sicherzustellen.

8.4.3 Abgrenzung

- Die Prüfung der Entra-ID-Einstellung umfasst nicht die Integration des Identity and Accessmanagements in (eigenentwickelte) Applikationen
- Auch die detaillierte Prüfung weitere Microsoft-Dienste und -Applikationen (Office365, Sharepoint, ...) muss separat an den Bedarf des Auftraggebers angepasst werden.
- Bei hybriden Umgebungen ist es abhängig von der Gesamtarchitektur sinnvoll, zusätzlich eine vollständige Analyse der AD-Infrastruktur durchzuführen.

8.4.4 Notwendige Angaben für die Angebotserstellung

- Grobe Architekturbeschreibung (inkl. Angaben zu hybrid oder cloud only)
- Anzahl der zu prüfenden Tennants
- Anzahl der verwendeten Benutzerrollen und etwaiger Custom Roles

8.5 Mobile App (inkl. Backend API)

8.5.1 Einleitung und Zielsetzung

- Derzeit sind iOS und Android die verbreitetsten Betriebssysteme und bilden daher die Grundlage für dieses Modul. Detaillierte Testbeschreibungen finden sich in den OWASP Mobile Application Security Testing Guide (MASTG).
- Die Backend APIs sind in der Regel auf Basis typischer Webschnittstellen implementiert, daher wird hier auf die detaillierte Beschreibung der entsprechenden Tests verzichtet und auf das entsprechende Modul verwiesen. Bei der Planung des Testumfangs sollten diese Tests auf jeden Fall berücksichtigt werden.
- Im Wesentlichen gilt es, vier Angriffsszenarien zu überprüfen:
    - Angriffe auf die App über das Netzwerk
    - Angriffe auf die App durch andere auf dem gleichen Gerät installierte Apps
    - Angriffe auf die Kommunikation mit den Backend Systemen (APIs)
    - Angriffe auf die App auf dem mobilen Endgerät im Fall von Gerätverlust

8.5.2 Fokus und Umfang

- In der Regel müssen alle Tests auf allen unterstützten Betriebssystemen separat durchgeführt werden. Beim Einsatz von Multiplattform-Frameworks bei der Entwicklung der Apps können ggf. einige Tests zusammengefasst werden. Alle von der App genutzten Funktion, die mit OS-spezifischen Schnittstellen interagieren, müssen in jedem Fall separat untersucht werden.

- Prüfung der Datenhaltung, Zugriffberechtigungen und Interprozesskommunikation auf Sicherheit. Dies beinhaltet Caches, Logdateien, Datenbanken und weitere interne und externe Datensenken. Neben der Speicherung personenbezogener Daten sind hier insbesondere sensitive Nutz- und Zugangsdaten zu berücksichtigen.
- Prüfung der Sicherheit der Anbindung an die Backend APIs mit Fokus auf die sichere Übertragung von Daten und die wechselseitige Authentifizierung.

8.5.3 Abgrenzung

- Die hier beschriebenen Tests sind auf die Überprüfung der Sicherheit der Applikationen und der vom Auftraggeber gespeicherten und verarbeiteten Daten bei der Verwendung auf "regulären" mobilen Geräten ausgerichtet. Das heißt, es wird davon ausgegangen, dass die Geräte und Betriebssystem auf dem aktuellen Sicherheitslevel betrieben werden.
- Für die effiziente Durchführung der Tests ist es unerlässlich, den Testern auch Versionen der App mit deaktivierten Sicherheitsmaßnahmen wie Root-/Jailbreakdetection und Certificate Pinning bereitzustellen.

8.5.4 Notwendige Angaben für die Angebotserstellung

- Zielplattformen (Betriebssystemversion und Gerätetypen)
- Verwendete Frameworks und Entwicklungsumgebungen
- Kann eine Testversion der App bereitgestellt werden, die eine Untersuchung vereinfacht / ermöglicht (Deaktivierung von Sicherheitsmaßnahmen wie Root-/Jailbreak Detection, Certificate Pinning oder alternativ die Instrumentierung der App mit Testwerkzeugen)? Wenn dies nicht der Fall ist, entsteht ggf. zusätzlicher Aufwand oder der Testumfang muss reduziert werden.
- Testkonten mit realistischen Testdaten und Anbindungen
- Sonstige Besonderheiten der App (notwendige zusätzliche Hardware, komplexe Rechte-/Rollenmodelle, spezielle Kommunikationsprotokolle, zusätzliche Verschlüsselung)

8.6 Endgerät ("Pre-Assumed Breach")

Es können verschiedene Hardware- und Softwareplattformen getestet werden (z.B. Windows-Laptops, Android-Tables, iOS-Mobiltelefone). Im Folgenden wird der Standardfall der Analyse eines Windows-Laptops beschrieben.

8.6.1 Einleitung und Zielsetzung

Es wird ein **Standardarbeitsplatz (Client) auf Basis von Windows** auf Schwachstellen untersucht, um das Risiko von Angriffen auf Endgeräte zu bewerten. Der Test simuliert zwei Perspektiven:

- **Externer Angreifer (anonym):** Ziel ist es, Zugriff auf das Gerät, die Festplatte oder gespeicherte Daten zu erlangen.
- **Interner Angreifer (mit begrenzten Zugangsdaten):** Ziel ist es, ohne administrative Rechte Zugriff auf sensible Daten zu erhalten, Berechtigungen zu erweitern oder Schadcode auszuführen.

Durch die Prüfung werden **typische Angriffsszenarien** abgedeckt, wie z.B.:

- Umgehung von Festplattenverschlüsselung oder BIOS-Passwörtern,
- Ausnutzung von Konfigurationsfehlern (z.B. in Windows-Schutzmechanismen),
- Missbrauch von Schwachstellen in installierter Software zur Rechteerweiterung,
- Umgehung von Endpoint-Protection-Lösungen (z.B. durch In-Memory Execution oder AMSI-Bypasses),
- Prüfung der Datenübertragung auf unverschlüsselte Kommunikation.

Die Prüfung sollte **regelmäßig** (z.B. bei Änderungen der Client-Konfiguration oder jährlich) durchgeführt werden, um neue Bedrohungen zu adressieren.

8.6.2 Fokus und Umfang

Prüfungen aus Sicht eines anonymen Angreifers:

- **Physische und technische Schutzmechanismen:**
  - Vorhandensein und Wirksamkeit von Festplattenverschlüsselung (z.B. BitLocker), Boot-Passwörtern, BIOS-Passwörtern
  - Möglichkeit, die Festplattenverschlüsselung zu umgehen oder zu brechen (z.B. durch Cold Boot Attacks)
  - Auslesen von Daten aus dem Arbeitsspeicher
- **Hinweis:** Die Prüfungen können zur **Zerstörung von Daten** auf dem Gerät führen. Es muss sich daher um ein **dediziertes Testgerät** handeln.

Prüfungen aus Sicht eines internen Angreifers (mit Nutzerrechten):

Hinweis: Sofern keine Prüfung mit Hardware erfolgen soll, können diese Prüfungen auch remote erfolgen.

- **Analyse der Systemkonfiguration**:
  - Installierte Software und Betriebssystemversion und bekannte Schwachstellen
  - Zugriff des Benutzers auf sensible Daten (z.B. über Autostart-Einträge, Dienste, Login-Skripte, freigegebene Ordner oder Verzeichnisse anderer Benutzer)
- **Rechteerweiterung**:
  - Möglichkeit, Benutzerrechte durch Konfigurationsfehler (z.B. Boot-Optionen, Benutzerverwaltung) oder Missbrauch installierter Software zu erweitern
  - Umgehung von Schutzmaßnahmen wie Anti-Malware-Software oder Endpoint-Protection
- **Schutzmechanismen**:
  - Prüfung von Windows-Schutzmechanismen (z.B. Application Whitelisting, PowerShell-Restrictions) auf Konfigurationsfehler
  - Analyse der Netzwerkkommunikation auf unverschlüsselte Übertragung sensibler Daten
  - Wirksamkeit von Data Loss Prevention (DLP)-Maßnahmen und deren Umgehbarkeit

8.6.3 Abgrenzung

- **Keine Prüfung der Netzwerkinfrastruktur:** Der Fokus liegt auf dem **lokalen Client**. Netzwerkbasierte Angriffe (z.B. Man-in-the-Middle) sind nicht Teil dieses Moduls.
- **Keine Zerstörung von Produktivsystemen:** Das Testgerät muss **exklusiv für den Penetrationstest** bereitgestellt werden.
- **Kein Social Engineering:** Physische oder psychologische Angriffe (z.B. Phishing) sind nicht enthalten.
- **Keine Prüfung von Servern oder Backend-Systemen:** Der Test beschränkt sich auf den **Client-Arbeitsplatz**.

8.6.4 Notwendige Angaben für eine sinnvolle Ausschreibung

- **Testgerät:**
  - Bereitstellung eines **Standardarbeitsplatzes** (Windows-basiert) mit typischer Konfiguration (Software, Berechtigungen, Schutzmechanismen).
  - Technische Daten des Testgeräts (Modell, BIOS-Version, Windows-Version)
  - Klärung, ob das Gerät **physisch oder remote** (z.B. per RDP/VPN) zugänglich gemacht wird.
- **Zugangsdaten:**
  - Bereitstellung von **Nutzerdaten** (keine administrativen Rechte) für die Prüfung aus interner Sicht
  - Idealerweise für die Installation und Ausführung von Prüfwerkzeugen lokale administrative Rechte zur Effizienzsteigerung
- **Technische Rahmenbedingungen:**
  - Gibt es **Restriktionen** (z.B. keine Deaktivierung von Schutzsoftware)?

    - Werden **sensible Daten** auf dem Testgerät gespeichert, die besonders geschützt werden müssen?
- **Organisatorische Rahmenbedingungen:**
    - Zeitfenster für den Test (z.B. keine Prüfungen während der Kernarbeitszeit)
    - Ansprechpartner für technische Rückfragen
- **Dokumentation:**
    - Soll der Bericht **technische Details** (z.B. konkrete Exploits) oder eine **zusammengefasste Risikobewertung** sowie **empfohlene Maßnahmen und deren Priorisierung** enthalten?

8.7 Web-Anwendung

8.7.1 Einleitung und Zielsetzung

Web-Anwendungen zählen zu den am häufigsten angegriffenen Systemen, da sie typischerweise aus dem Internet erreichbar sind und gleichzeitig geschäftskritische Funktionen sowie sensible Daten verarbeiten.

Ziel eines Penetrationstests von Web-Anwendungen ist die systematische Identifikation und Bewertung von Schwachstellen, die eine unbefugte Nutzung, Manipulation oder Offenlegung von Daten und Funktionen ermöglichen könnten. Dabei wird insbesondere geprüft, ob die implementierten Sicherheitsmechanismen geeignet sind, typische Angriffe wirksam abzuwehren und die definierten Schutzbedarfe umzusetzen. Im Fokus steht insbesondere die Bewertung:

- der Authentifizierungs- und Autorisierungsmechanismen,
- der Sicherheit von Datenverarbeitung und -übertragung,
- sowie der korrekten Umsetzung von Geschäftsprozessen und Zugriffsbeschränkungen.

Ein Penetrationstest von Web-Anwendungen sollte insbesondere in folgenden Situationen durchgeführt werden:

- Idealerweise nicht erst in der finalen Version, sondern schon in einem möglichst frühen Stadium der Softwareentwicklung,
- vor dem Go-Live neuer Anwendungen oder wesentlicher Funktionserweiterungen,
- nach signifikanten Änderungen an Architektur, Authentifizierung oder Geschäftslogik,
- bei erhöhtem Schutzbedarf, z.B. bei Verarbeitung sensibler oder geschäftskritischer Daten,
- sowie regelmäßig im Betrieb, um neue Schwachstellen oder geänderte Bedrohungslagen zu berücksichtigen.

Als Orientierung gelten in der Praxis wiederkehrende Prüfungen in jährlichen oder risikobasiert kürzeren Intervallen. Zusätzlich sollten anlassbezogene Tests erfolgen, wenn sich wesentliche Rahmenbedingungen ändern.

8.7.2 Fokus und Umfang

Der Fokus der Prüfung liegt auf der Webanwendung selbst, einschließlich direkt angebundener Komponenten, insbesondere:

- Frontend (Web-Oberfläche)
- Anbindung der Authentifizierungs- und Autorisierungssysteme
- zugehöriger API-Endpunkte

Die Prüfung orientiert sich an etablierten Best Practices, insbesondere dem OWASP Web Security Testing Guide (WSTG), und umfasst strukturierte Tests entlang typischer Angriffspfade und Prüfkategorien.

Hinweis zu OWASP Top 10
Die OWASP Top 10 werden in vielen Compliance-Vorgaben gefordert. Nach ihrem eigenen Verständnis sind die OWASP Top 10 jedoch ausdrücklich ein Sensibilisierungsdokument und kein Testkatalog. Sie sind außerdem keine Liste einzelner Schwachstellen, sondern eine Übersicht zentraler Risiken.

Der WSTG enthält dagegen eine sehr umfangreiche Sammlung konkreter Testfälle. Er eignet sich daher deutlich besser als verbindliche Testvorgabe.

Der Test kann aus verschiedenen Perspektiven erfolgen:

- Externer Angreifer ohne Zugangsdaten
- Authentifizierter Benutzer mit regulären Rechten
- Authentifizierter Benutzer mit erweiterten Rechten / Privilegierter Benutzer

Auf dieser Basis werden typischerweise folgende Prüfschwerpunkte abgedeckt:

- Kryptographie (z.B. verwendete Ciphers, eingesetzte Zertifikate)
- Authentifikation & Autorisierung (z.B. Prüfung des Anmeldeprozesses, Passwortrichtlinien, Berechtigungsprüfungen, Zugriffsschutz)
- Identitätsmanagement (Prüfen des Registrierungsprozesses, Aktivierungs- und Sperrmechanismen, Authentifizierungsmerkmale)
- Session Management (eingesetzte Session-Cookies oder Token und deren Validierung)
- Konfigurations- und Deployment-Management
- Datenvalidierung (Eingabevalidierung und typische Injection-Angriffe)
- Anwendungslogik (anwendungsspezifische Prozesse, Dateiupload, eingabeabhängige Ressourcenbindung, etc.)
- Fehlerbehandlung (Informationspreisgabe durch Fehler, Resilienz ggü. provozierten Fehlern)
- Clientseitiges Testen
- Technologiespezifische Testfälle (bekannte Schwachstellen der eingesetzten Technologien)

Je nach Zielsetzung des Tests und bei hoher Komplexität der Anwendung, die einen vollumfänglichen Test sehr aufwändig machen können, können zudem unterschiedliche Teststrategien eingesetzt werden:

- Fokussierter Anwendungstest: detaillierte Prüfung einzelner Komponenten, Anwendungs- oder Funktionsbereiche bei größeren Anwendungen
- End-to-End-Test von Geschäftsprozessen (Analyse von kompletten Nutzungsszenarien und Abläufen)
- Zeitlich begrenzter Ansatz (Time-Boxed, Priorisierung relevanter Angriffsvektoren innerhalb des gegebenen Zeitbudgets)

8.7.3 Abgrenzung

Dieses Modul fokussiert sich ausschließlich auf die Sicherheit der Web-Anwendung und ihrer direkt zugehörigen Komponenten. Nicht Bestandteil des Moduls sind insbesondere:

- allgemeine Netzwerkinfrastruktur des Betreibers
- Cloud- oder Plattformanalysen (z.B. Infrastruktur-Konfiguration)
- Source-Code-Analysen (SAST)
- Social Engineering oder Red-Team-Szenarien

Zusätzlich gilt:

- Tests mit produktionsgefährdenden Auswirkungen sind in der Regel ausgeschlossen oder müssen individuell abgestimmt werden.
- Externe Dienste (Identitätsdienste, Zahlungsdienste) werden nur im Kontext ihrer Integration in die Anwendung betrachtet.
- Abhängige Drittsysteme werden nicht vollumfänglich geprüft.

Die Aussagekraft der Testergebnisse kann je nach gewählter Testumgebung variieren. Tests in Produktivumgebungen liefern in der Regel realitätsnahe Ergebnisse, können jedoch Einschränkungen im Testumfang erfordern. Tests in isolierten Test- oder Staging-Umgebungen ermöglichen häufig eine tiefere Prüfung, spiegeln jedoch nicht immer die reale Betriebsumgebung vollständig wider.

Bei zugekauften bzw. Standardanwendungen sind Penetrationstests insbesondere dann sinnvoll, wenn die Anwendungen angepasst werden. So kann beispielsweise die Prüfung eines Standard-Outlook-Webaccess ggf. im Rahmen eines Risikomanagements nicht im Scope sein.

8.7.4 Notwendige Angaben für eine sinnvolle Ausschreibung

Für eine valide Angebotserstellung und zielgerichtete Durchführung sollten mindestens folgende Informationen bereitgestellt werden:

- Testgegenstand:
  - Beschreibung der Webanwendung / Zweck der Anwendung
  - URLs, Domains, Subdomains und API-Endpunkte (mit API-Dokumentation)
  - Eingesetzte Technologien, Frameworks oder Plattformen
  - Abgrenzung Frontend, Backend, API

- Funktionsumfang, Architektur und Kontext:
  - Grobe Systemarchitektur
  - Funktionalitäten (z.B. Upload, E-Mail-Versand, …) / abgebildete Prozesse
  - Vorhandene Mandanten- / Benutzerstruktur, z.B. Kunde, interner Mitarbeiter, Administrator oder Support
  - Gibt es externe Abhängigkeiten (z.B. Zahlungsdienstleister oder Identitätsprovider)?
  - Sind Sicherheitsmechanismen (z.B. WAF, CAPTCHA) vorhanden? Wenn ja, können diese selektiv deaktiviert werden für notwendige Massenprüfungen?

- Testumgebung:
  - Handelt es sich um eine Produktiv-, Staging- oder Testumgebung?
  - Ist die Anwendung über das Internet erreichbar? Wenn nein, wie soll der Zugriff erfolgen?

9 Anhang

9.1 Responsible Disclosure

Im Responsible-Disclosure-Verfahren werden Sicherheitslücken und Schwachstellen in Soft- oder Hardware von dem beauftragten Penetrationstestanbieter verantwortungsbewusst und unabhängig voneinander sowohl an den Auftraggeber des Penetrationstests als auch an die betroffenen Hersteller oder Entwickler gemeldet, bevor die Informationen über die identifizierten Schwachstellen seitens des Penetrationstestanbieters veröffentlicht werden, um Anwender der betroffenen Lösung die Möglichkeit zu geben, Sicherheitsupdates einzuspielen oder andere geeignete Schutzmaßnahmen zu ergreifen, bis dies möglich ist.

Globales Ziel des Verfahrens ist es, Soft- und Hardware für die Endanwender aus IT-sicherheitstechnischer Sicht sicherer zu machen, Missbrauch zu verhindern und die Zusammenarbeit zwischen allen Marktteilnehmern (insbesondere zwischen Herstellern von Soft- und Hardware und Ethical Hackern wie Anbietern von Penetrationstests) zu fördern. In diesem Sinne wird den Herstellern und Entwicklern ein festgelegtes Zeitfenster gegeben, die Schwachstellen zu beseitigen, bevor sie öffentlich bekannt gemacht und folglich auch durch andere Angreifer ausgenutzt werden können. Ein Responsible-Disclosure-Verfahren ist folglich ein optionaler, aber wichtiger Ansatz zur Steigerung des globalen IT-Sicherheitsniveaus.

Ein Responsible-Disclosure-Verfahren ersetzt also keine Verschwiegenheitsregelung zwischen den Vertragsparteien zur Durchführung eines Penetrationstests. Es handelt sich bei dem Verfahren vielmehr um eine Ergänzung, welche standardmäßig oder optional seitens der Anbieter von Penetrationstests im Angebot zugrunde gelegt wird und klar regelt, wie entdeckte Sicherheitslücken den Herstellern und den Entwicklern, dem Auftraggeber des Penetrationstests und der Öffentlichkeit gemeldet werden. Hersteller und Entwickler von Soft- und Hardware bieten mittlerweile oft Meldeverfahren für identifizierte Sicherheitsschwachstellen in ihren Produkten an und loben im Rahmen von sogenannten Bug-Bounty-Programmen dafür auch teilweise finanzielle Prämien aus. Responsible-Disclosure-Vereinbarungen können mit einigen Vor- und Nachteilen verbunden sein.

Die Vorteile eines Responsible-Disclosure-Verfahrens sind im Wesentlichen:

Schutz der Endanwender: Die verantwortungsvolle Meldung von Sicherheitslücken gibt Herstellern die Chance, rechtzeitig zu reagieren und Schwachstellen zu schließen, bevor sie möglicherweise missbräuchlich ausgenutzt werden. Gleichwohl wird folglich auch der Druck auf die betroffenen Hersteller erhöht, die Schwachstellen zu beseitigen, um dem Endanwender einen möglichst hohen Schutz zu bieten.

- **Transparenz und Vertrauen:** Eine Responsible-Disclosure-Vereinbarung macht transparent, dass der Anbieter des Penetrationstests den Umgang mit identifizierten Schwachstellen klar geregelt hat und diese dem Hersteller aus ethischen Gründen mitteilt, um das IT-Sicherheitsniveaus bzw. das Vertrauen in Soft- und Hardware im Allgemeinen zu erhöhen.

- **Eindringliches Risikomanagement:** Wenn der Anbieter von Penetrationstests ein standardisiertes Vorgehen für die Meldung und Veröffentlichung von identifizierten Sicherheitslücken hat, wissen die betroffenen Hersteller, dass Schwachstellen nicht sofort veröffentlicht werden und sie die Kontrolle über den Prozess zur Behebung der Schwachstelle verantworten.

- **Reputation und Image:** Das Responsible-Disclosure-Verfahren ermöglicht es Anbietern von Penetrationstests, ihre Leistungsfähigkeit durch entsprechende Veröffentlichungen von Schwachstellen positiv darzustellen.

Die Nachteile eines Responsible-Disclosure-Verfahrens sind im Wesentlichen:

- **Fremdbestimmung und potenzielle Compliance-Probleme:** Nach Ablauf der festgelegten Frist zur Behebung der identifizierten Schwachstelle wird diese veröffentlicht. Falls Hersteller und Entwickler die Schwachstelle innerhalb der Frist nicht wirksam durch einen Patch oder Update beseitigt haben, erhöht sich die Gefahr, dass die Schwachstelle aufgrund der Veröffentlichung vermehrt, missbräuchlich ausgenutzt wird. Im Sinne der Produktsicherheit drohen Hersteller und Entwickler

abhängig vom Gerichtsstand auch Compliance-Probleme und Regressansprüche. Abhängig von der konkret zugrundeliegenden Responsible-Disclosure-Klausel kann der Penetrationstestanbieter auch auf die Veröffentlichung der Schwachstelle bestehen, obwohl diese seitens des Herstellers und Entwicklers innerhalb der Frist behoben wurde. Abhängig vom Endanwender können historische Informationen über vergangene Schwachstellen für den Hersteller und Entwickler zu einem Imageschaden oder positiven Image führen.

An dieser Stelle sei ebenfalls angemerkt, dass auch für den Penetrationstestanbieter und den Auftraggeber des Penetrationstests abhängig von den Nutzungs- und Lizenzbedingungen potenzielle Compliance-Verstöße im Raum stehen können.

- **Zeitdruck und Ressourcenaufwand:**
  Eine Responsible-Disclosure-Klausel setzt Hersteller und Entwickler unter Druck, Schwachstellen innerhalb einer fremd- oder mitbestimmten Frist (schneller) zu beheben, da ansonsten eine Veröffentlichung droht. Organisationen, die nicht über die notwendigen Ressourcen zur schnellen bzw. fristgerechten Behebung der identifizierten Schwachstelle verfügen, könnten dadurch in Schwierigkeiten geraten.

- **Abhängigkeit vom Dienstleister:**
  Hersteller und Entwickler könnten sich verpflichtet fühlen, weitere IT-Sicherheitsdienstleistungen beim Penetrationstestanbieter zu beauftragen, um beispielsweise bei der Behebung der entdeckten Schwachstellen zu helfen oder die Wirksamkeit der Schwachstellenbeseitigung durch einen Re-Test zu überprüfen, was Zusatzkosten verursacht.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.