Arbeitsrichtlinie Penetrationstests

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Penetrationstests
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	08.11.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	08.11.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Review ohne inhaltliche Änderungen	Daniel Fürdauer
21.0	17.11.2021	Redaktionelle Anpassungen und Überarbeitung Kapitel 4.1.1; 4.1.5; 6.1.2 in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0; Aktualisierung zertifizierter Unternehmen	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. EINLEITUNG

Im technischen Sprachgebrauch versteht man unter einem Penetrationstest den kontrollierten Versuch, von „außen“ in ein bestimmtes Computersystem bzw. -netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen bzw. ähnliche Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. Die hierbei identifizierten Schwachstellen können dann durch entsprechende Maßnahmen behoben werden, bevor diese von unautorisierten Dritten genutzt werden können.
Typische Ansatzpunkte für einen Penetrationstest sind:

- Netzkoppelelemente (Router, Switches, Gateways)
- Sicherheitsgateways (Firewall, Paketfilter, Intrusion Detection System, Virenscanner, Loadbalancer etc.)
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.)
- Telekommunikationsanlagen
- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop)
- Clients
- Drahtlose Netze (WLAN, Bluetooth)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

Ein Penetrationstest kann nicht die üblichen IT-Sicherheitsprüfungen ersetzen. Auch ersetzt er nicht die üblichen Qualitätssicherungen, da im Rahmen von Penetrationstests keine funktionalen Aspekte getestet werden und diese zudem nur stichprobenartig erfolgen.

2. ANWENDUNGSBEREICH

Penetrationstests **müssen** durchgeführt werden, wenn

- Systeme neu eingeführt oder sicherheitsrelevant verändert[1] werden, sofern sie mit dem Internet direkt verbunden sind (Webserver, Webportale etc.),
- die Stabstelle Datenschutz und Informationssicherheit die Durchführung als zwingend notwendig erachtet.

Ungeachtet der vorgenannten Punkte sollte in regelmäßigen Abständen bei Systemen mit hohem Schutzbedarf ein Penetrationstest durchgeführt werden. Die Auswahl der zu überprüfenden Systeme ist durch den IT-Betrieb zu planen und einmal im Jahr mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen. In Abstimmung mit dem Informationssicherheitsbeauftragten können geplante Penetrationstests aufgeschoben werden.
Penetrationstests sollten ferner durchgeführt werden, wenn

- neue Unternehmensteile an das Netzwerk der VAV angeschlossen werden sollen,
- neue Netzwerkinfrastrukturen zur Verfügung gestellt werden oder wesentliche Änderungen durchgeführt wurden oder
- IT-Dienstleistungen ausgelagert werden, z.B. IT-Systeme von einem externen Dienstleister betrieben werden (z.B. Hosting)

Ein Penetrationstest kann zudem im Nachgang zu einem IT-Sicherheitsvorfall sinnvoll sein.

[1] z.B. bei der Einführung neuer Dienste, der Änderung von Zugangsmöglichkeiten oder Authentisierungsverfahren oder der Eröffnung zusätzlicher Schnittstellen.

3. ABGRENZUNG ZU ANDEREN IT-SICHERHEITSPRÜFUNGEN

3.1. Informationssicherheitsüberprüfungen

Informationssicherheitsprüfungen der Stabstelle Datenschutz und Informationssicherheit verfolgen das Ziel, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden sowie die bestehenden Sicherheitsmaßnahmen und Sicherheitsprozesse zu optimieren.
Während die internen Audits von der Stabstelle Datenschutz und Informationssicherheit – basierend auf den Anforderungen der ISO 27001 – das Ziel verfolgen, zu überprüfen, ob die vorher festgelegten Sicherheitsmaßnahmen wie vereinbart umgesetzt sind, geht der Penetrationstest einen Schritt weiter. Hierbei wird gezielt nach Wegen gesucht, die eingesetzten Sicherheitsmaßnahmen zu umgehen oder bisher nicht erkannte Schwachstellen oder Sicherheitslücken zu finden.

3.2. Code-Review

Bei einem Code-Review wird der Quellcode von Software systematisch auf Schwachstellen und Fehler untersucht. Der Code-Review ist ein Teilgebiet der Qualitätssicherung. Er kann aber auch gezielt eingesetzt werden, um gängige Sicherheitslücken zu finden. Hierzu wird der Quellcode beispielsweise gezielt nach zu gering ausgelegten Speicherbereichen oder nicht abgefangenen Fehlern untersucht. Bei einem Penetrationstest auf eine IT-Anwendung wird im laufenden Betrieb gezielt unerwartetes Verhalten provoziert und anhand des Verhaltens der IT-Anwendung auf Schwachstellen geschlossen.

4. ANFORDERUNGEN

4.1. Prüfmethoden

Vor jedem Penetrationstest müssen die Methoden des Vorgehens festgelegt werden. Das nachfolgende Schaubild verdeutlicht, auf welche Weise Penetrationstests durchgeführt werden können. Die linke Seite zeigt sechs Kriterien für die Unterscheidung von Penetrationstests. Auf der rechten Seite sind die unterschiedlichen Werte für die Kriterien aufgelistet, die den Penetrationstestspezialisten eine Leitlinie für den Umfang und die Methodik geben. Diese Kriterien sind im Dienstleistungsvertrag festzuhalten. Die orange eingefärbten Kriterien sind als Standardwerte zu verstehen, von denen allerdings im Einzelfall nach Abstimmung mit der Stabstelle Datenschutz und Informationssicherheit abgewichen werden kann.

	INFORMATIONSFLUSS		Black-Box	White-Box	
	AGGRESSIVITÄT	passiv scannend	vorsichtig	abwägend	aggressiv
	UMFANG	vollständig	begrenzt	fokussiert	
	SICHTBARKEIT		verdeckt	offensichtlich	
	TECHNIK	Netzwerk-zugang	Telekommunikationszugang	Physischer Zugang	Social En-gineering
	ANGRIFFSPUNKT		von außen	von innen	
	PRÜFORT		vor Ort	über das Internet	

Abbildung 1: Übersicht der Methoden eines Penetrationstests

4.1.1. Informationsfluss

Mit der Unterscheidung zwischen „Black-Box-Test“ und „White-Box-Test“ wird der Wissenstand des Penetrationstesters über das anzugreifende Objekt festgelegt, also mit oder ohne Insiderwissen:

- Bei einem **Black-Box-Test** stehen dem Penetrationstester keine weiteren Informationen oder Daten zur Verfügung. Er muss diese über verschiedene Wege selbst sammeln und analysieren, bevor er wie ein Hacker versucht in die IT des Unternehmens einzudringen.
- Bei einem **White-Box-Test** stehen dem Penetrationstester alle Informationen und Daten zu dem zu überprüfenden Objekt, wie Quellcode, Dienste, Softwareversionen zur Verfügung.

Es wird grundsätzlich empfohlen, einen White-Box-Test durchzuführen, da bei einem Black-Box-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können. Auch ist der Aufwand bei einem Black-Box-Test wesentlich größer. Zusätzlich besteht bei einem Black-Box-Test ein höheres Risiko unbeabsichtigt Schäden (z.B. Systemausfälle) zu verursachen.

Damit der Prüfer bei einem White-Box-Test einen schnellen Überblick über die zu testenden Prüfobjekte erhalten, sollten ihm die im Folgenden aufgelisteten Unterlagen vom Auftraggeber zur Verfügung gestellt werden:

- **Netzwerkpläne:** Mit allen Kommunikationsverbindungen zu anderen IT-Systemen und IT-Anwendungen. IP-Adressen sollten beinhaltet sein, sowie Schnittstellen, die von außen zu erreichen sind.
- **Beschreibung des Prüfobjekts:** Die mindestens beschreibt, welche Benutzer Zugriff auf das Objekt besitzen, zu welchen Zeiten Zugriffe erfolgen, welche Daten personenbezogen sind, sowie welche IT-Systeme für das Funktionieren der IT-Anwendung wichtig sind.
- **Liste der IT-Systeme mit Beschreibung der Härtungsmaßnahmen**
- **Beschreibung der Kommunikationsverbindungen:** Alle notwendigen Kommunikationsverbindungen sollten nachvollziehbar dokumentiert sein.
- **Sicherheitskonzepte:** Mit Beschreibung der Fachverfahren und Bewertung des Schutzbedarfs sind – sofern vorhanden – beizufügen.
- **Quellcode**
- **Eingesetzte Software mit Versionsnummer**

4.1.2. Aggressivität

Diese Anforderung beschreibt, wie aggressiv der Penetrationstester beim Testen vorgeht:

- **passiv, scannend**: Die Testobjekte werden nur passiv untersucht. Die gefundenen Schwachstellen werden nicht ausgenutzt.
- **vorsichtig**: Die gefundenen Schwachstellen werden durch den Penetrationstester nur dann ausgenutzt, wenn eine Beeinträchtigung des untersuchten Systems ausgeschlossen werden kann.
- **abwägend**: Es wird versucht die Schwachstellen auszunutzen, die auch zu Systembeeinträchtigungen führen können. Allerdings wird abgewogen wie stark die Konsequenzen im Vergleich zum möglichen Erfolg wären.
- **aggressiv**: Hierbei wird versucht alle potenziellen Schwachstellen auszunutzen. Dem Auftraggeber muss dabei bewusst sein, dass neben den zu untersuchenden Systemen auch benachbarten Systeme ausfallen können.

Grundsätzlich ist eine abwägende Angriffsstärke zu wählen. Ein Penetrationstest soll dafür so dimensioniert werden, dass Schwachstellen zwar nachgewiesen, aber nur aktiv ausgenutzt werden, wenn es nicht vermeidbar ist und die Exploits ausreichend getestet wurden.

4.1.3. Umfang

Der Testumfang bestimmt, welche Systeme getestet werden sollen:

- **vollständig:** Bei einem vollständigen Test werden alle erreichbaren Systeme geprüft.
- **begrenzt:** Alle Systeme in der DMZ (demilitarisierten Zone) können beispielsweise bei einem begrenzten Penetrationstest geprüft werden.
- **fokussiert:** Der fokussierte Penetrationstest prüft nur ein bestimmtes Teilnetz oder System. Dieser Test bietet sich z.B. nach Änderung der Systemlandschaft an.

Bei einem erstmaligen Penetrationstest für ein System oder eine Anwendung wird eine vollständige Überprüfung empfohlen, darüber hinaus sind fokussierte Penetrationstests im Rahmen der durchgeführten Systemänderungen empfohlen.

4.1.4. Sichtbarkeit

Die Sichtbarkeit legt fest, wie „sichtbar“ der Penetrationstester beim Testen vorgeht:

- **verdeckt:** Es sollen nur solche Methoden zum Einsatz kommen, die nicht direkt als Angriffsversuch erkannt werden.
- **offensichtlich:** Hierbei werden offensichtliche Methoden, wie umfangreiche Port-Scans, verwendet.

Die Sichtbarkeit sollte in aller Regel offensichtliche Methoden einschließen.

4.1.5. Technik

Hiermit wird festgelegt, welche Angriffstechnik beim Testen verwendet wird:

- **Netzwerkzugang:** Der Penetrationstest über das Netzwerk entspricht dem normalen Vorgehen und simuliert einen typischen Angriff.
- **Telekommunikationszugang:** Es existieren neben IP Netzwerken weitere Netze, die für Angriffe genutzt werden können (z.B. CAN im Automobilbereich, Fax-Dienste, Bluetooth-Verbindungen, Mobilfunknetze usw.).
- **Physischer Zugang:** Der Zugang erfolgt direkt über die Konsole auf das zu testende IT-System.
- **Social Engineering:** Diese Tests bieten sich nach Einführung von Sicherheitsrichtlinien an, um die Akzeptanz und Sensibilität der Mitarbeiter zu prüfen. Bei Social-Engineering-Attacken wird z.B. durch Telefonate oder direkten Kontakt zu Mitarbeitern versucht, an die Passwörter oder geschützte Daten zu gelangen.

Für den Test der IT-Systeme der VAV wird ein Test über die Netzwerkinfrastruktur in aller Regel empfohlen.

4.1.6. Angriffspunkt

Der Angriffspunkt legt fest, von wo aus der Penetrationstest durchgeführt wird:

- **von außen:** Die meisten Angriffe erfolgen über die Netzwerkanbindung an das Internet. Daher kann ein Angriff als „externer Täter“ die Risiken eines solchen Angriffs erfassen und bewerten. Hierbei werden meistens Router, Firewalls und Systeme in der DMZ untersucht.
- **von innen:** Hier liegt der Fokus auf Personen, die aufgrund einer erfolgreichen Attacke Zugriff zum internen Netzwerk erlangt haben. Es wird getestet, welche Möglichkeiten für Angriffe aus dem internen Netz heraus bestehen.

Der Angriffspunkt ist fallspezifisch mit der Stabstelle Datenschutz und Informationssicherheit festzulegen.

4.1.7. Prüfort

Mit dem Prüfort wird festgelegt, ob das Prüfobjekt über das Internet getestet wird oder ob der Penetrationstest vor Ort stattfindet.
Penetrationstests sollten vor Ort durchgeführt werden. Es sei denn, es handelt sich bei dem Prüfobjekt um eine Webanwendung, die sinnvollerweise über das Internet getestet wird oder die IT-Systeme stehen an einem entfernten Ort, für den die Reisekosten die geplanten Kosten des Tests überschreiten würden.

4.2. Auswahl und Beauftragung von Prüfern

4.2.1. Auswahl des Prüfers

Ein Prüfer erhält Zugang zu sensiblen Informationen über die Infrastruktur und deren Schwachstellen. Bei der Suche nach einer vertrauenswürdigen Firma für eine solche Aufgabe können die im Folgenden beschriebenen Kriterien herangezogen werden. Anbieter, die Penetrationstests anbieten, sollten möglichst als Prüfstelle zertifiziert sein (siehe Anhang). Sie sollten nachweislich die Grundsätze des Datenschutzes, der sicheren Datenhaltung und der IT-Sicherheit einhalten und ausschließlich qualifiziertes Personal beschäftigen.
Die Prüfer müssen umfangreiche fachliche Kenntnisse haben. Werden beispielsweise folgende Zertifikate vorgelegt, so kann von einer breiten fachlichen Qualifikation und Eignung ausgegangen werden:

- Personenzertifizierung des BSI:
  https://www.bsi.bund.de/dok/6617744
- Council for Registered Ethical Security Testers (CREST)-Zertifizierung:
  http://www.crest-approved.org/http://www.crestaustralia.org/approved.html
- Certified Ethical Hacker (CEH)-Zertifizierung (USA):
  http://www.eccouncil.org/Certification/certified-ethical-hacker

Sollte kein Zertifikat für die Prüfstelle bzw. deren Personal vorliegen, so wird empfohlen, dass der hauptverantwortliche Prüfer Berufserfahrung im Bereich IT-Penetrationstests besitzt und eine technische Ausbildung abgeschlossen hat. Der Projektverantwortliche muss in den letzten acht Jahren mindestens fünf Jahre Berufserfahrung (Vollzeit) im Bereich IT erworben haben, davon sollten mindestens zwei Jahre (Vollzeit) im Bereich Informationssicherheit absolviert worden sein. Zudem

sollte der Prüfer mindestens sechs Penetrationstests in den letzten drei Jahren durchgeführt haben. Dieses sollte möglichst vom Anbieter über entsprechende Referenzen nachgewiesen werden. Weiterhin sollte anhand des Prüfobjekts entschieden werden, welche Qualifikationen erforderlich sind. Ein versierter Prüfer im Webanwendungsbereich ist beispielsweise nicht zwangsläufig auch dafür geeignet, Gateways oder Infrastruktursysteme zu untersuchen.
Entsprechende Referenzen können Rückschlüsse auf die Eignung geben. Weiterhin sind Branchenerfahrungen unter Umständen von Vorteil.
Die Unabhängigkeit und die Neutralität der Prüfer ist ein wichtiger Aspekt. Das schließt in der Regel aus, dass Penetrationstests von eigenen Mitarbeitern durchgeführt werden. Ein weiterer Grund für die Verwendung von externen Spezialisten ist die notwendige Unvoreingenommenheit des Prüfers.
Der Auftraggeber sollte darauf achten, dass die Personen den Penetrationstest durchführen, deren Qualifikation im Angebot beschrieben werden. Es sollten nur Vertreter akzeptiert werden, wenn diese vergleichbare Qualifikationen nachweisen können.

4.2.2. Beauftragung

Die Beauftragung des Penetrationstesters erfolgt in der Regel durch das Projekt bzw. Maßnahme und muss im Projektbudget im Rahmen des Projektmanagementprozesses der VAV eingeplant werden.
Bei der Neueinführung von Systemen im Rahmen der Linientätigkeit des IT-Betriebs (z.B. Einführung eines WLAN) ist im Rahmen der Jahresbudgetplanung des IT-Betriebs ein entsprechendes Budget einzuplanen. Gleiches gilt für geplante Änderungen an Systemen, die einen Penetrationstests entsprechend Ziffer 2 erfordern.
Notwendige Wiederholungstests sind ebenfalls durch den IT-Betrieb in der Jahresplanung zu berücksichtigen.
Prüfer sollten regelmäßig gewechselt werden, um gegebenenfalls nicht erkannte Schwachstellen aufgrund von z.B. der Vorgehensweise durch einen anderen Dienstleister zu erkennen.

4.2.3. Vertragliche Inhalte

Notwendige Vertragsinhalte
Die Prüfer bzw. die Prüfstellen sollten nie ohne schriftlichen Auftrag eine IT-Anwendung bzw. IT-Systeme testen. Daher sollte immer ein Vertrag zwischen Prüfern und der VAV geschlossen werden. Sind Dienste bei einem Hoster ausgelagert, so muss auch dieser in den Vertrag einbezogen werden. Die Beauftragung erfolgt über den zentralen Einkaufsprozess.
Der Vertrag sollte Rahmenbedingungen wie Prüfzeitraum, Prüfobjekt und Prüftiefe spezifizieren, entsprechend der oben genannten Vorgaben. Hierdurch kann vermieden werden, dass Prüfer unbeabsichtigt zu tief testen oder IT-Systeme beeinflussen, die nicht beeinträchtigt werden dürfen. Andererseits können auch die Prüfer davor geschützt werden, dass sie nicht für zufällig während der Penetrationstests aufgetretene Fehler an anderen IT-Systemen zur Verantwortung gezogen werden.
Es sollte festgelegt werden, welche Kosten anfallen werden und was neben dem Test selbst erwartet wird, wie zum Beispiel eine Präsentation vor dem Management oder ein besonders umfangreicher Bericht. Außerdem müssen die Mitwirkungspflichten des Auftraggebers festgelegt werden.
Es sollten weiterhin Vereinbarungen bezüglich der Haftbarkeit und der Verschwiegenheit getroffen werden.

Die Art und der Umfang der Dokumentation sollten im Vertrag festgelegt werden. Der Auftragnehmer sollte dazu verpflichtet werden, seine Prüfungshandlungen genau zu dokumentieren. Damit wird sichergestellt, dass im Falle eines Schadens die Nachvollziehbarkeit der angewandten Techniken gewährleistet ist. Darüber hinaus ist die Form der Ergebnisdarstellung (Bericht, Präsentation, Reports und Analysen der eingesetzten Sicherheitstools) zu vereinbaren.
Es sollte ein Anfangs- und Enddatum des Auftrags festgelegt werden, innerhalb dessen der Penetrationstest zu erbringen bzw. autorisiert ist. Damit wird sichergestellt, dass über diesen Zeitraum hinausgehende Penetrationsversuche klar als tatsächliche Angriffe eines Dritten identifiziert werden können. Missverständnisse werden dadurch ausgeschlossen.
Weiterhin sollte geregelt werden, dass für den IT-Betrieb nachvollziehbare risikominimierende oder risikobeseitigende Maßnahmen im Abschlussbericht aufgeführt werden. Es ist festzulegen, welchem Personenkreis der Abschlussbericht zur Kenntnis vorgelegt werden soll. Die Stabstelle Datenschutz und Informationssicherheit ist obligatorisch aufzuführen.

Non Disclosure Agreement (NDA)
Im Vertrag sollte festgelegt werden, dass weder über die vorgefundenen Sicherheitsmängel, noch über die Organisationsstrukturen und die Struktur der überprüften IT-Systeme, noch über gesichtetes Firmen-Know-how gegenüber Dritten kommuniziert wird.

Speicherzeit von Daten
Die Prüfer müssen während der praktischen Tests Daten speichern, durch deren Auswertung sie erst einen Bericht erstellen können. Es sollte vor einem Penetrationstest vereinbart werden, welche Daten in welcher Form und auf welchen Datenträgern erhoben werden dürfen und nach welcher Zeit die Prüfer die erhobenen Daten löschen müssen und welche Nachweise dafür zu erbringen sind.

Datenschutz
Der Datenschutz muss zu jeder Zeit gewährleistet sein. Wenn personenbezogene Daten von einem Penetrationstest betroffen sind oder betroffen sein können, muss vor Beginn des Tests eine Vereinbarung zur Auftragsverarbeitung inklusive der notwendigen Anlagen mit dem Prüfer abgeschlossen werden. Hierfür sind die Musterverträge der VAV zu verwenden. Der Datenschutzbeauftragte ist bei der Prüfung der Verträge mit einzubeziehen.

5. SONSTIGE RAHMENBEDINGUNGEN

Durch einen Penetrationstest ist oft auch ein Personenkreis außerhalb des untersuchten Bereichs betroffen. Durch einen Test kann es unter Umständen zu Netzwerkbelastungen kommen oder Mitarbeiter oder Kunden werden zeitweise in ihrer normalen Arbeit beeinträchtigt. Die Penetrationstests sollten daher so geplant werden, dass möglichst wenig Beeinträchtigungen stattfinden. Weiterhin sollten die betroffenen Personenkreise vor einem Penetrationstest benachrichtigt und einbezogen werden. Dazu gehören z. B.:

- der Datenschutzbeauftragte,
- der Informationssicherheitsbeauftragte,
- der IT-Betrieb,
- das IT Service Continuity Management,
- der Business Continuity Manager,
- ggf. der Betriebsrat (sofern Mitarbeiterdaten betroffen sind) und
- ggf. weitere Betroffene je nach Prüfobjekt.

6. ABLAUF DES PENETRATIONSTESTS

Die praktische Durchführung des Penetrationstests erfolgt in der Regel nach dem skizzierten Schema:

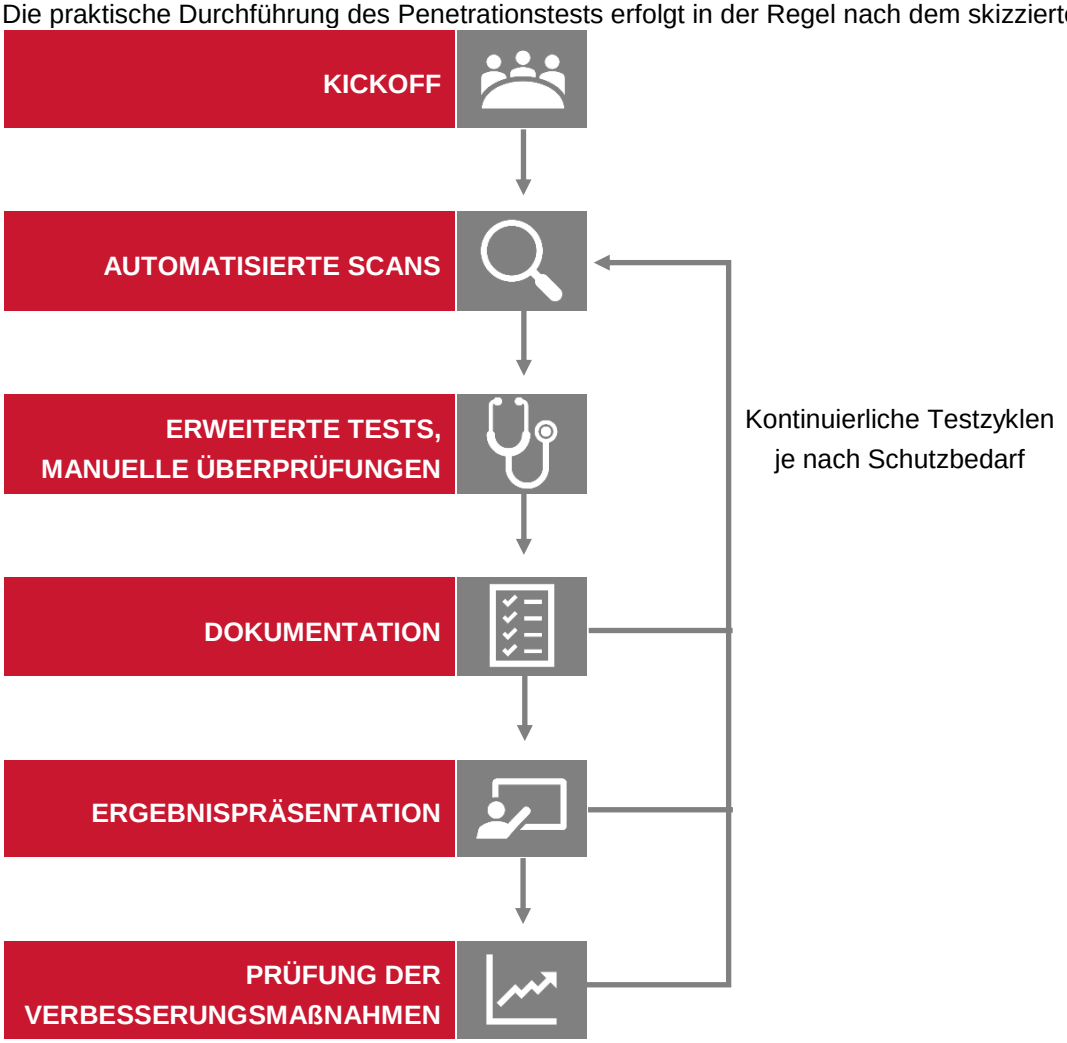

Abbildung 2: Übersicht der Durchführung eines Penetrationstests

6.1. Organisatorische Vorbereitung (Kick Off)

Im Vorgespräch werden die optimale Vorgehensweise für den Prüfgegenstand und organisatorische Einzelheiten festgelegt. Zu klären sind in diesem Zusammenhang mindestens:

- Ansprechpartner für Zwischenergebnisse und Besonderheiten
- Kommunikationswege
- Eskalationsprozedur und Ansprechpartner bzw. Kommunikationswege für Notfälle
- Abstimmung mit den betroffenen IT-Betriebseinheiten und Fachabteilungen, die über das Vorhaben unterrichtet werden müssen
- Zeitliche Vorgehensweise und Zeitpunkte der Tests in Abstimmung mit dem IT-Betrieb

Wenn die Zeiträume zur Durchführung des Penetrationstests ausgewählt werden, sollte darauf geachtet werden, dass nicht gleichzeitig Wartungsarbeiten an den betroffenen IT-Systemen durchgeführt werden. Ein Penetrationstest auf ein IT-System, welches gerade verändert wird, verliert an Aussagekraft.

6.1.1. Durchführung

Die Durchführung soll in Abstimmung mit dem IT-Betrieb und der Fachabteilung erfolgen, um negative Einflüsse auf den IT-Regelbetrieb zu vermeiden und gegebenenfalls ein differenziertes Systemverhalten im Rahmen des Incident-Prozesses erklären zu können.
Es wird empfohlen, dass ein Testteam aus mindestens zwei Personen für einen Penetrationstest eingesetzt wird, damit das Vier-Augenprinzip gewahrt bleibt. Letztendlich entscheidet der Kostenfaktor, wie viele Personen beauftragt werden. Es muss insbesondere bei kleinen Prüfobjekten zwischen Kosten und Nutzen abgewogen werden.

6.1.2. Abschlussbericht

Neben den Aufzeichnungen der einzelnen Prüfungsschritte sollte der Abschlussbericht auch eine Bewertung der gefundenen Schwachstellen in Form der potenziellen Risiken sowie verständliche und nachvollziehbare Empfehlungen zur Kompensation der Schwachstellen bzw. der Risiken enthalten. Der Bericht muss in jedem Fall die Nachvollziehbarkeit der Tests und der dadurch offen gelegten Schwachstellen sicherstellen.
Die Feststellungen im Abschlussbericht müssen für jede Prüfungsfeststellung eine Risikoklassifizierung aufweisen. Gängige Bewertungsmethoden basieren z.B. auf

- CVSS
- OWASP Risk Rating

und weisen zumindest eine Skalierung in den folgenden Stufen aus:

SCHADENPOTENZIAL	ERFORDERLICHE REAKTION	ERLÄUTERUNG
hoch	sofort	Fremdsteuerung des Prüfobjekts durch Angreifer möglich, Verlust von sensiblen Daten möglich, Veränderung des Prüfobjekts oder Auslesen von sensiblen Daten durch Angreifer möglich
mittel	kurzfristig	Schwachstellen, die schwerwiegende Angriffe ermöglichen können
gering	mittelfristig	Schwachstellen, die ein unbestimmtes Angriffspotenzial haben
zur Information	langfristig	Verbesserungspotenzial

Tabelle 1: Bewertungsskalierung des Abschlussberichts

Der Abschlussbericht ist aufgrund der darin eventuell vorhandenen sensiblen Informationen **vertraulich** zu behandeln. Er ist entsprechend zu klassifizieren und nur dem notwendigen Personenkreis zur Verfügung zu stellen. Der Abschlussbericht ist der Stabstelle Datenschutz und Informationssicherheit in jedem Fall zur Verfügung zu stellen. Abweichende Bewertungen seitens der Stabstelle Datenschutz und Informationssicherheit werden mit der IT-Abteilung abgestimmt.

6.1.3. Ergebnispräsentation

Die Ergebnispräsentation findet in einem vorbestimmten Personenkreis statt. Mindestens die „hoch“ eingestuften Schwachstellen werden besprochen und Wege zur Beseitigung mit den betroffenen Parteien diskutiert und festgelegt. Da das Ergebnisdokument des Penetrationstests, der Abschlussbericht, sehr technisch geprägt ist, muss im Einzelfall geprüft werden, ob eine Differenzierung zwischen Management Präsentation und technischer Präsentation erforderlich ist. Im Rahmen der Ergebnispräsentation werden wichtige Sachverhalte geklärt sowie Unstimmigkeiten und Verständnisprobleme bereinigt.
Die Ergebnispräsentation kann – insbesondere in Abhängigkeit der Menge an gefundenen Schwachstellen oder Komplexität der Beseitigung der Schwachstellen – entweder bei der VAV vor Ort oder im Rahmen einer Telefonkonferenz mit der beauftragten Firma erfolgen.
Der Teilnehmerkreis setzt sich mindestens wie folgt zusammen:

- der Penetrationstester, der die Tests durchgeführt hat,
- Projektverantwortlicher oder eine von diesem beauftragte, für die Nachverfolgung der Umsetzung im Projekt verantwortliche Person mit entsprechendem technischen Fachwissen,
- Vertreter der betroffenen IT-Betriebseinheiten und
- Mitarbeiter der Abteilung Stabstelle Datenschutz und Informationssicherheit

6.2. Bereinigung der Schwachstellen

Die Bereinigung der gefundenen Schwachstellen erfolgt bei Linientätigkeiten durch den IT-Betrieb. Bei Projekten erfolgt sie durch die vom Projekt-/Maßnahmenverantwortlichen beauftragten Personen. Die Stabstelle Datenschutz und Informationssicherheit ist über das Ergebnis zu informieren.
Der Penetrationstest gilt als beendet, wenn

- die Schwachstellen beseitigt sind bzw.
- etwaige Restrisiken behandelt worden sind (z.B. durch eine Risikoübernahme).

ANHANG: EMPFEHLUNGEN DES BSI

Leistungsbeschreibung zur Beauftragung

Die nachfolgende Übersicht dient als Leitfaden zur Erstellung einer Leistungsbeschreibung mit einem Prüfer auf Basis der Anforderungen dieser Richtlinie.

VORGABE	SPEZIFIZIERUNG	KONKRETE BESCHREIBUNG IM EINZELFALL – SOFERN RELEVANT
Grund für den Penetrationstest (siehe u. a. Ziffer 2)	Prüfung der Sicherheitsmaßnahmen, Verdacht auf Angriff, entdeckter Angriff, etc.	
Anforderung an Prüfer (siehe Ziffer 4.2.1)	Fachliche Anforderungen	
	Weitere Fähigkeiten	
	Technische Qualifikation / Zertifikate	
Rahmenbedingungen (siehe Ziffer 4.2.3)	Vertrag mit notwendigen Inhalten, NDA, Festlegung der Speicherzeit von Daten	
	Auftragsverarbeitungsvereinbarung nebst Anlagen zu TOM	
Festlegung des Prüfobjekts	z.B. Netzkoppelelemente (Router, Switches, Gateways), Sicherheitsgateways (Firewall, Paketfilter, Intrusion Detection System, Virenscanner etc.), Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.), Telekommunikationsanlagen, Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop), Clients, Drahtlose Netze (WLAN , Bluetooth etc.), Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)	

Festlegung des Prüfumfangs (siehe Ziffer 4.1.3)	Prüftiefe
	Prüfort
	Prüfzeitraum
	Prüfbedingungen
Verantwortlichkeiten	Ansprechpartner Dienstleister
	Ansprechpartner VAV
Ablauf des Tests	Zeitplan, Berichterstattung

Tabelle 2: Leistungsbeschreibung zur Beauftragung

Zertifizierte Unternehmen

Das BSI stellt eine Liste zertifizierter IT-Sicherheitsdienstleister für Penetrationstests unter der Adresse https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/IS_REV_PEN/IS_REV_Dienstleister/stellen_zertifizierung_pentester-is-revisoren.html bereit:

NAME	ERSTZERTIFIZIERUNG	ABLAUFDATUM
Atos Information Technology GmbH	01.08.2016	31.12.2022
datenschutz cert GmbH	12.05.2015	11.05.2021
Deutsche Telekom Security Services GmbH	01.08.2019	30.11.2021
Ernst & Young GmbH WPG	01.05.2021	14.10.2023
HiSolutions AG	15.10.2012	26.05.2023
Infodas GmbH	15.10.2019	31.05.2022
PwC Cyber Security Services GmbH	01.08.2019	14.08.2024
secunet Security Networks AG	30.07.2015	29.07.2022
secuvera GmbH	15.09.2013	31.03.2022
T-Systems Multimedia Solutions GmbH	01.04.2019	31.03.2022
TÜV Informationstechnik GmbH	15.10.2013	31.01.2023
TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria	15.04.2019	28.02.2022

Tabelle 3: Zertifizierte Unternehmen