FORUM

Penetrationstest

präsentiert von MORGENSTERN

MORGENSTERN

Whitepaper

Penetrationstest

Inhalt

01
Einführung und Überblick

02
Irrtümer in Bezug auf Penetrationstests

03
Arten von Penetrationstests

04
Durchführungsmethoden

05
Phasen eines Penetrationstests

06
Beispielbericht

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.
...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung und Überblick

Im Idealfall wird jede Software und jedes IT-System von vornherein so konzipiert, dass gefährliche Sicherheitslücken vermieden werden – aber das ist eben nur der Idealfall, die Realität sieht meist anders aus. Mit Hilfe eines Penetrationstests, kurz Pentest genannt, kann jedoch unmittelbar nach der Anschaffung einer neuen IT-Komponente und auch in den Folgejahren regelmäßig festgestellt werden, inwieweit Schwachstellen vorhanden sind.

Ein Penetrationstest ist ein autorisierter simulierter Angriff auf ein Computersystem, der durchgeführt wird, um dessen Sicherheit zu bewerten, indem erlaubterweise im Rahmen der getroffenen vertraglichen Regelung versucht wird, vorhandene Schwachstellen zu finden und auszunutzen. Hier wird festgelegt, ob ein System robust genug ist, um Angriffen von authentifizierten und nicht authentifizierten Positionen sowie einer Reihe von Systemrollen standzuhalten. Somit kann die Wirksamkeit der eingesetzten Sicherheitsmaßnahmen evaluiert werden. Penetrationstests sind jedoch im Allgemeinen keine einmalige Prozedur. Aufgrund der sich häufenden Sicherheitsvorfälle und der kontinuierlich neu auftretenden Schwachstellen in IT-Produkten stellen Organisationen zunehmend Sicherheitsexperten ein, die in regelmäßigen Abständen Penetrationstests durchführen. Für mehr Transparenz und Objektivität werden oft auch externe Dienstleister beauftragt.

Penetrationstester verwenden in der Regel dieselben Tools, Techniken und Prozesse wie Angreifer, um die Auswirkungen von Schwachstellen in einem System zu finden und zu demonstrieren. Hier werden verschiedene Angriffspunkte wie Server, Netzwerke, Mobilgeräte und Webanwendungen betrachtet, um Zugang zu internen Ressourcen und hochsensiblen Daten zu erhalten.

Das grundlegende Ziel von Pentests ist es, die Wirksamkeit der von der Organisation eingerichteten Abwehrmechanismen und die potenziell daraus resultierenden Verluste zu bewerten. Daher wird auch nach Durchführung ein Bericht mit Maßnahmenempfehlungen zur Optimierung des Sicherheitsniveaus vorgelegt und anhand eines sogenannten Retests kann geprüft werden, ob die Schwachstellen tatsächlich behoben wurden.

Brauchst du Rat? Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hoch spezialisiertes Team bestehend aus Anwälten & Anwältinnen, Datenschutz- und IT-Sicherheitsexpert*innen!

contact@morgenstern-privacy.com
+49 (0) 6232 - 100119 44

Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

Die Hauptgründe, warum sich eine Organisation für die Beauftragung von Pentests entscheiden sollte, lassen sich wie folgt zusammenfassen:

- **Unterstützung der Einhaltung von Datenschutz- und Compliance-Anforderungen**
  Viele Branchen, wie das Gesundheitswesen und Finanzwesen, haben strenge Compliance-Anforderungen, die regelmäßige Sicherheitstests vorschreiben. Penetrationstests helfen Unternehmen, diese Anforderungen zu erfüllen, ihre Sicherheit zu erhöhen und Verstöße zu vermeiden.

- **Sicherheitsrisiken frühzeitig identifizieren und entsprechend priorisieren**
  Auf diese Weise kann die Organisation proaktive Maßnahmen ergreifen, um die Schwachstellen zu beseitigen und das Risiko eines erfolgreichen Angriffs zu verringern.

- **Absicherung sensibler Daten, Wahrung der Loyalität der Kunden und somit die Pflege eines gutes Unternehmensimage**
  Geistiges Eigentum, Kundeninformationen und Finanzdaten müssen sicher und vertraulich behandelt werden. In einer digitalisierten Arbeitsweise ist es leider möglich, dass einem kleinen technische Fehlkonfiguration oder Unaufmerksamkeit zu einem unbefugten Zugriff auf diese Daten führen kann. Mit regelmäßige Penetrationstests kann das Risiko deutlich verringert werden.

- **Bestimmung der Robustheit von Kontrollen und Bereitstellung qualitativer und quantitativer Beispiele für die aktuelle Sicherheitslage**
  Penetrationstests können wertvolle Einblicke in die allgemeine Sicherheitslage eines Unternehmens geben, einschließlich seiner Richtlinien, Verfahren und Technologien. Diese Informationen können verwendet werden, um gezielte Verbesserungen vorzunehmen und sicherzustellen, dass Vermögenswerte effektiv geschützt werden.

02. Irrtümer in Bezug auf Penetrationstests

Leider kursieren auch heute noch viele Irrtümer und Halbwahrheiten, wenn es um Penetrationstests geht.
Daher möchten wir im Folgenden einige davon aufgreifen und versuchen, diesen Irrtümern entgegen zu wirken.

1. „Penetrationstests sind für kleine Organisationen nicht relevant."

Unabhängig von der Größe einer Organisation können Sicherheitsvorfälle langfristige Schäden verursachen, die nur durch sorgfältige Maßnahmen verhindert werden können. Cyberkriminellen ist es egal, wie groß oder klein deine Organisation ist: Ein leichtes Ziel ist ein leichtes Ziel.

Ausreichende – und vor allem tatsächlich wirksame – Schutzmaßnahmen sind zudem gesetzlich vorgeschrieben. So fordert z.B. die Datenschutz-Grundverordnung (DS-GVO) „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen" (Art. 32 Abs. 1d).

Darüber hinaus ist diese Überprüfung der Wirksamkeit ebenfalls Voraussetzung für die Einhaltung der Vorgaben der IT-Sicherheitsstandards ISO 27001 und IT-Grundschutz nach BSI, Bundesamt für Sicherheit in der Informationstechnik.

2. „Penetrationstests sind nur für Regierungs- bzw. Finanzinstitutionen wichtig."

Sicherheit ist ein integraler Bestandteil jeder Organisation, unabhängig von der Branche, in der sie tätig ist. Es ist wichtig, die Kontinuität der Geschäftstätigkeit zu gewährleisten und vor allem Reputations- und finanzielle Verluste zu vermeiden.

3. „Penetrationstests sind das gleiche wie eine Schwachstellenbewertung."

Organisationen verwechseln häufig Penetrationstests mit Schwachstellenanalysen. Schwachstellenanalysen basieren auf automatisierten Tools mit vordefinierten Signaturen, die bekannte Sicherheitsprobleme und Patch-Ebenen (Programmversionen) überprüfen, ohne zu validieren, ob die Schwachstelle ausnutzbar ist. Sie decken daher nur Schwachstellen auf, die in ihren Datenbanken vorhanden sind.

Penetrationstests hingegen verwenden sowohl manuelle als auch automatisierte Techniken, um jede Schwachstelle zu validieren. Diese Tests verlassen sich also nicht nur auf Werkzeuge, sondern auch auf die Kreativität, den Einfallsreichtum, die Erfahrung und das Wissen des Testers, um alle „Puzzleteile" zusammenzufügen und so die vordefinierten Ziele zu erreichen.

03. Arten von Penetrationstests

Basierend auf unterschiedlichen Rahmenbedingungen und dem Prüfobjekt selbst werden Penetrationstests in verschiedene Arten kategorisiert, wie z.B. externe Penetrationstests, interne Penetrationstests, Web Application Penetrationstests, Cloud Penetrationstests, Social Engineering und physische Penetrationstests.

Externer Penetrationstest

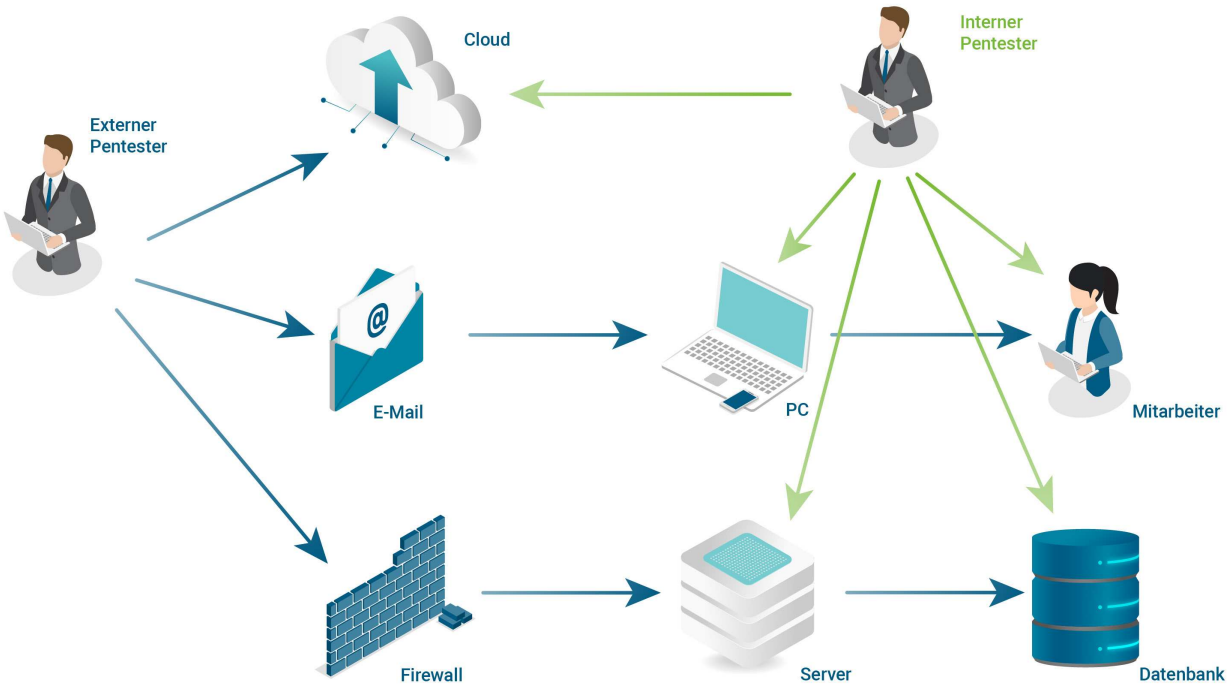
Ein externer Penetrationstest ist der traditionellere und häufigere Ansatz, da die Rahmenbedingungen denen eines echten Hackerangriffs sehr ähnlich sind. Dabei werden die Tests von außerhalb der Organisation durchgeführt, ohne die ordnungsgemäße Autorisierung und Berechtigungen zu missbrauchen. Diese Art von Tests wird normalerweise über das Internet durchgeführt. Der Tester kann über die Infrastruktur der Organisation Bescheid wissen oder auch ohne Wissen starten. Die Offenlegung von Informationen in diesem Zusammenhang liegt vollständig im Ermessen der Organisation.

Der Test beginnt mit der Auflistung von Informationen, die bereits öffentlich verfügbar sind, um extern erreichbare Systeme ausfindig zu machen, die eventuell Angriffsfläche sein könnten. Solche Systeme können zum Beispiel die Webseite, CMS-Systeme, E-Mail-Server, Datenbanken, SSH-Schnittstellen oder auch Firewalls sein. Diese wird unter anderem mit einer DNS-Enumeration (Auflistung) und eines Port-Scans erreicht. Im Anschluss werden gezielte Angriffsversuche simuliert, deren Art und Weise von den eingesetzten Technologien abhängt.

Interner Penetrationstest

Obwohl die Techniken für interne und externe Pentests ähnlich sind, können die Ergebnisse sehr unterschiedlich sein. Der interne Pentest wird innerhalb der Organisation simuliert. Er ist vergleichbar mit einem Insider-Angriff, hinter dem beispielsweise ein unzufriedener Mitarbeiter oder ein Gast mit Standardbenutzerrechten stecken könnte. In diesem Fall hat der Tester mehr Informationen und somit gute Kenntnisse über die Endpunkte, über die der Angriff erfolgen soll. Aus diesen Gründen hat ein Angriff von innen das Potenzial, größeren Schaden anzurichten.

Bei der Durchführung eines internen Penetrationstests analysiert ein Cybersicherheitsteam Netzwerke, Server, Computersysteme und andere Geräte, Firewalls, Angriffserkennungssysteme (IDS, Intrusion Detection System), Angriffsabwehrsysteme (IPS, Intrusion Prevention System) und sogar das Verhalten der Mitarbeiter. Dabei werden die tiefgreifenden Sicherheitsmaßnahmen überprüft und festgestellt, ob diese vorhanden und fehlerfrei konfiguriert sind. Sobald die Schwachstellen in diesen Komponenten identifiziert sind, wird versucht, sie auszunutzen, um das Ausmaß des potenziellen unbefugten Zugriffs und der daraus resultierenden Schäden zu ermitteln.



Webanwendungs-Penetrationstest

Grundsätzlich kannst du dir Web-Anwendungen als offene Türen zu deinem Haus oder deinem Unternehmen vorstellen. Sie umfassen alle Softwareanwendungen, bei denen die Benutzeroberfläche oder die Aktivität online stattfindet. Daher ist ein Penetrationstest für Webanwendungen eine Sicherheitsmaßnahme, auf die angesichts der heutigen Bedrohungslage nicht mehr verzichtet werden kann. Dabei werden die kritischsten und am häufigsten ausgenutzten Schwachstellen bzw. die OWASP Top-10 Angriffsfaktoren untersucht.

Das OWASP (Open Web Application Security Project) ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen und Diensten im Internet zu verbessern. Der Fokus liegt unter anderem auf folgenden Bereichen:

- **Zugriffskontrolle und Autorisierung:** Es wird versucht, Zugriffskontrollprüfungen zu umgehen, z. B. durch Änderung der aufgerufenen URL (Parametermanipulation oder Forced Browsing), Änderung des http-Antwortstatus oder der HTML-Seite.

- **Eingabe- und Ausgabevalidierung:** Mittels gezielter und moderner Injection-Attacken werden alle URL-Parameter, HTTP-Header, Registrierungs-, Anmelde- und Kontaktformulare auf Schwachstellen wie XSS (Cross-Site-Scripting), SQL-Injection (Einschleusen von SQL-Datenbankbefehlen), XXE (XML External Entity Attack, XML-Objekt-Attacke, Manipulation eines externen XML-Objekts), RCE (Remote Code Execution, Ausführen von Code/Befehlen auf entfernten Rechnern/Servern) etc. untersucht. untersucht. Abhängig davon, ob und wie die Benutzereingaben validiert werden, werden unterschiedliche Methoden zur Umgehung eingesetzt.

- **Sicherheitsrelevante Fehlkonfiguration:** Es wird geprüft, ob alle Software und Komponenten auf dem aktuellen Stand sind, ob Standardkonten und deren Passwörter noch aktiv und unverändert sind, ob unnötige Funktionen aktiviert oder installiert sind (z.B. unnötige Ports, Dienste, Seiten, Konten oder Berechtigungen), ob Fehlermeldungen sensible Informationen wie Quellcodebestandteile oder Versionsnummern enthalten, etc.

- **Offenlegung von sicherheitsrelevanten Informationen:** Beispielsweise wird in JavaScript-Bibliotheken oder Github-Repositories nach eingebetteten Kommentaren gesucht. Diese weisen oft auf versteckte Endpunkte oder Anmeldeinformationen hin.

- **Authentifizierung und Session Management:** Um die Identität anderer Nutzer oder eines Administrators zu übernehmen, wird das Verhalten der Anwendung vor und nach dem An- und Abmelden untersucht und beispielsweise die Gültigkeit und Funktionsweise von Cookies oder Session-IDs analysiert.

- **Kryptographie und Datensicherheit:** Hier wird festgestellt, ob Daten im Klartext übertragen werden, ob Standard- oder schwache kryptographische Algorithmen oder Protokolle verwendet werden, ob veraltete Hash-Funktionen wie MD5 oder SHA1 oder überhaupt kryptographische Hash-Funktionen verwendet werden.

- **Geschäfts- und Anwendungslogik:** Hier geht es mehr um Schwachstellen im Zusammenhang mit dem eigentlichen Geschäftsprozess. Dazu gehören z.B. das Überbrücken des Bezahlvorgangs, Preismanipulationen, die unendliche Verlängerung von Testphasen, die automatische Verzerrung von Umfrageergebnissen etc.

- **Datenschutz:** Während des Tests prüfen unsere Experten die Datenschutzkonformität auf Basis der EU-DSGVO, indem sie die Verarbeitung der personenbezogenen Daten von Seitenbesuchern bewerten.

Cloud-Penetrationstest

Cloud-Infrastrukturen und -Dienste entwickeln sich rasch zu einer dominierenden Anlageklasse für Unternehmen aller Größen. Viele Unternehmen integrieren zunehmend eine Vielzahl von Anwendungen, Diensten und Daten in die Cloud, z. B. Anwendungen zur gemeinsamen Nutzung von Dateien und zur Steigerung der Geschäftsproduktivität, Daten aus mobilen Anwendungen, Netzwerküberwachungsdaten und -protokolle, Backups sowie Mitarbeiter- und Kundendaten. Das bedeutet, dass die Cloud-Ressourcen eines Unternehmens immer wertvoller werden und ein höheres Risiko darstellen. So tauchen nicht nur immer wieder Datenschutzbedenken auf, da der Dienstanbieter jederzeit auf die Daten in der Cloud zugreifen oder sie an Dritte weitergeben kann, sondern die Cloud ist auch ein beliebtes Ziel für Angreifer. Ein Cloud-Penetration-Test liefert den besten Beweis dafür, dass ein Unternehmen über eine solide betriebliche Widerstandsfähigkeit verfügt und vor Cyberangriffen, erzwungenen Unterbrechungen, unbefugtem Zugriff, Datendiebstahl und Schadsoftware geschützt ist.

Jede Cloud hat ihre eigenen Besonderheiten, aber im Allgemein werden die folgenden Aspekte beim Testen einer Cloud-Umgebung überprüft:

- Identitäts- und Zugriffsverwaltung
- Cloud-Fehlkonfiguration
- Externe Dienste, Schnittstellen und Anwendungen einschließlich APIs
- Offengelegte sensible Informationen, Daten und Dokumente
- Internes Testen von Cloud-Servern und -Diensten

Social Engineering

Social Engineering ist eine Strategie, die sich hauptsächlich auf menschliche Interaktion stützt. Dabei konzentriert sich der Tester auf die psychologischen und physiologischen Aspekte sowie das technische Know-how einer Person, um Sicherheitspraktiken zu durchbrechen. Der Mensch wird somit als das vermeintlich schwächste Glied in der Sicherheitskette betrachtet.

Social Engineering umfasst im Allgemeinen drei Methoden: Phishing, Vishing (Voice Phishing) und Identitätsdiebstahl. Wobei der Klassiker, der Anruf eines vermeintlichen Bankmitarbeiters, der Informationen zum Firmenkonto benötigt, kein Trend mehr ist. Vielmehr nutzen Kriminelle neue Techniken, um sich Zugang zu digitalen Systemen oder sensiblen Informationen zu verschaffen.

Mitarbeiter wollen ihrem Arbeitgeber in der Regel keinen Schaden zufügen. Wenn sie jedoch nicht gut geschult sind, machen sie Fehler – das ist menschlich. Es ist daher allerdings sehr ratsam, den Hackern einen Schritt voraus zu sein, indem man eine Zwischenbewertung der aktuellen Situation vornimmt und die Testergebnisse überwacht.

Die Mitarbeiterinnen und Mitarbeiter müssen geschult werden, um beispielsweise verdächtige E-Mails, die täuschend echt aussehen können, zu erkennen und damit richtig umzugehen. Es sollte auch erklärt werden, warum es wichtig ist, eingehende Anweisungen, zum Beispiel per Telefon, zu hinterfragen und gegebenenfalls durch einen Rückruf sicherzustellen, dass es sich nicht um Betrug oder irgendeine Art von Manipulation handelt. Die festgelegten Kommunikationsrichtlinien des Unternehmens werden dadurch verständlicher. So kann der effektivste Weg zur Erreichung der gewünschten Cyber-Awareness eingeschlagen werden.

„Jeder Mensch macht Fehler. Das Kunststück liegt darin, sie zu machen, wenn keiner zuschaut." (Peter Ustinov)

Physischer Penetrationstest

Während immer mehr Unternehmen ihre Netzwerke und Anwendungen hervorragend gegen die Bedrohung durch virtuelle Cyber-Angriffe schützen, wird das Risiko eines möglichen physischen Angriffs auf ihre Standorte häufig vernachlässigt.

Ein physischer Penetrationstest ist ein Offline-Test, bei dem die Sicherheit von Firmengebäuden, Messeständen usw. überprüft wird. Dabei wird versucht, Zutrittskontrollen zu umgehen und in Bereiche von besonderem Interesse einzudringen, um an interne Informationen zu gelangen.

Im Folgenden werden einige zentrale Schritte und Methoden zur Durchführung eines physischen Penetrationstests beschrieben:

- **Mapping:** Dies entspricht der Erkundungsphase, die bei allen Arten von Penetrationstests durchgeführt wird, und beinhaltet eine detaillierte Analyse der Umgebung, Gebäude und Räumlichkeiten deiner Organisation. Alle Türen, Fenster, Notausgänge, Kellerzugänge usw. werden kartiert und untersucht, um mögliche ungesicherte oder unbewachte Angriffspunkte zu identifizieren.
- **Lock-Picking:** Das Knacken von Schlössern ist eine so beliebte Methode, dass das SANS Institute (SysAdmin, Audit, Networking and Security) einen Kurs über physische Penetrationstests und Werkzeuge zum Öffnen von Schlössern anbietet. Die Hauptgründe dafür sind sowohl mechanische als auch elektromagnetische Schlösser, die sich im Laufe der Zeit nicht wesentlich weiterentwickelt haben und mit ein wenig Training leicht zu knacken sind.

- **Telephotography:** Der einfache Versuch, von außerhalb des Büros Fotos von den Computerbildschirmen der Mitarbeiterinnen und Mitarbeiter zu machen, reicht aus, um zu testen, ob dieser Angriff auf dein Unternehmen erfolgreich sein kann.
- **Dumpster Diving:** Müllcontainer werden durchsucht, um Quellen sensibler Informationen wie Rechnungen, Papierdokumente und Kontoauszüge zu finden, die die Sicherheit des Unternehmens gefährden könnten.
- **Trusted Authority:** Der Tester gibt sich als vertrauenswürdige Person aus, z. B. als Lieferant, Dienstleister usw., um sich Zugang zu vertraulichen Informationen zu verschaffen.

Durch das Testen all dieser und anderer Szenarien kann die Widerstandsfähigkeit gegen physisches Eindringen realistisch eingeschätzt werden. Beachten sollte man auch, dass diese Verbrechen nicht so kompliziert sind, wie es oft in Filmen den Anschein hat. Die Berücksichtigung der physischen Seite der Cyberkriminalität ist ein wesentlicher Bestandteil der Cybersicherheitsstrategie einer jeden Organisation.

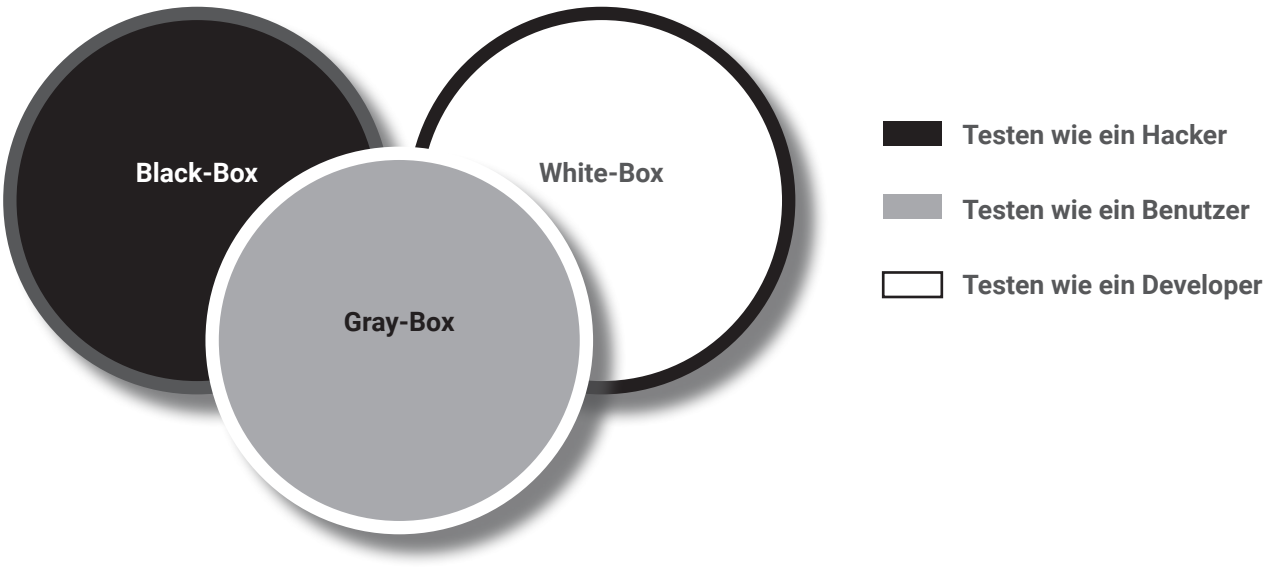
04. Durchführungsmethoden

Die oben aufgeführten Penetrationstests können mit drei verschiedenen Methoden durchgeführt werden, je nach Kenntnisstand und Zugang, der dem Pentester zu Beginn der Aufgabe gewährt wird.

- **Black-Box-Pentest:** Der Tester hat keine spezifischen Kenntnisse über die interne Funktionsweise des Systems. Er hat auch keinen Zugang zum Quellcode und kennt die Architektur nicht. Ein Black-Box-Pentest identifiziert Schwachstellen in einem System, die von außen ausgenutzt werden können. Das bedeutet, dass diese Art von Test auf einer dynamischen Analyse der aktuell laufenden Programme und Systeme im Netzwerk basiert.

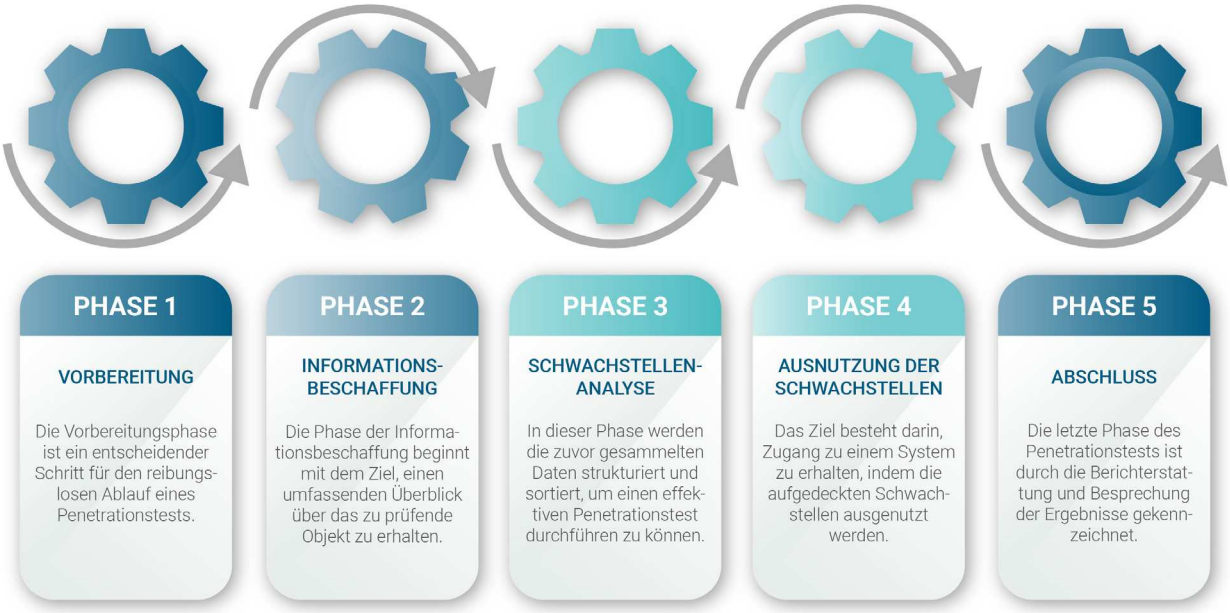
- **White-Box-Pentest:** Hier verfügt der Tester über umfassende Systemkenntnisse und hat Zugriff auf das gesamte Netzwerk. Dieses Wissen ermöglicht es dem Tester, Schwachstellen schneller zu identifizieren. Das kann die Kosten eines Pentests senken.

- **Gray-Box-Pentest:** Hierbei handelt es sich um eine Kombination aus Black- und White-Pentest. Der Tester hat zumindest einige Kenntnisse über die Interna des Zielsystems, z.B. über den Zugang und die Rechte eines Benutzers. Ziel dieser Methode ist es, eine fokussiertere und effizientere Bewertung des Sicherheitsniveaus zu ermöglichen.



05. Phasen der Penetrationstests

Penetrationstests bestehen typischerweise aus den folgenden Phasen:



In der Praxis können der Umfang, die Relevanz und möglicherweise die konkrete Reihenfolge dieser Phasen je nach Art des Tests und des Testobjekts, des Testumfangs sowie der festgelegten Ziele variieren. Je nach Bedarf können einzelne Phasen reduziert, erweitert und miteinander kombiniert werden.

Phase 1 | Vorbereitung – Planung

Die Vorbereitungsphase ist ein entscheidender Schritt für den reibungslosen Ablauf eines Penetrationstests. In einem ersten Gespräch werden alle notwendigen Vereinbarungen zwischen dem Auftraggeber und dem Penetrationstester getroffen. Dabei werden sowohl technische als auch regulatorische Anforderungen berücksichtigt, um sicherzustellen, dass der Test den geltenden Standards entspricht. Außerdem werden der Testumfang und die zu erreichenden Ziele festgelegt. Dazu gehört auch die Auswahl der Test- und Auswertemethoden, einschließlich der Entscheidung, welche Methoden ausgeschlossen werden sollen. Der Schwerpunkt liegt auf der Diskussion der Risiken und möglichen Nebenwirkungen der Prüfung und wie diese vermieden werden können. Auf der Grundlage dieser Informationen wird ein Arbeitsplan erstellt, der alle Schritte und Meilensteine des Projekts enthält. Dazu gehören auch die festgelegten Fristen, die beteiligten Personen und deren Kontaktdaten.

Phase 2 | Informationsbeschaffung - Reconnaissance

Die Phase der Informationsbeschaffung beginnt mit dem Ziel, einen umfassenden Überblick über das zu prüfende Objekt zu erhalten. Zunächst werden so viele Informationen wie möglich gesammelt. Dazu gehören Hosts, Subdomänen, offene Ports, verwendete Protokolle, Softwarekomponenten und deren Versionen etc. Genau so, wie ein Hacker sich an das Zielsystem herantastet. Diese Phase wird oft auch als „Recon“ oder „Reconnaissance“ bezeichnet und kann auf zwei verschiedene Arten durchgeführt werden:

- Passive Reconnaissance: Dieser Ansatz erfordert keine direkte Interaktion mit dem System. Der Penetrationstester verwendet hauptsächlich sogenannte „Open Source Intelligence“ (OSINT), die in öffentlich zugänglichen Quellen automatisiert nach relevanten oder vertraulichen Informationen sucht. Dazu gehören Techniken wie Google Hacking oder „Dorking“, Suchmaschinen für Server und IoT-Geräte wie Shodan oder Censys.
- Aktive Reconnaissance: Bei der aktiven Reconnaissance kommt es tatsächlich zu Interaktionen mit dem System. Dies trägt dazu bei, die Struktur des Testobjekts besser zu verstehen und mögliche Einfallstore zu identifizieren. Typische Methoden sind Port-Scanning, Subdomain-Auflistung, Verzeichnis-Brute-Forcing etc.

Phase 3 | Informationsbewertung – Schwachstellenanalyse

In dieser Phase werden die zuvor gesammelten Daten strukturiert und sortiert, um einen effektiven Penetrationstest durchführen zu können. Dabei werden Subdomains nach ihrem Statuscode, Schnittstellen nach ihrem Schutzbedarf und den vergebenen Zugriffsrechten sowie Ressourcen und Dateien nach ihrem Typ und der verwendeten Programmiersprache klassifiziert. Im nächsten Schritt werden verschiedene Tools eingesetzt, um verschiedene Payloads zu testen und bekannte Sicherheitslücken oder CVEs (Common Vulnerabilities and Exposures) zu identifizieren. Diese Scanner sind oft signaturbasiert und können daher nur bekannte Schwachstellen identifizieren. Obwohl die Ergebnisse dieser Scans wertvolle Informationen liefern, stellen sie nur den ersten Schritt in der Schwachstellenanalyse dar. Scanner können keine neuen oder unbekannten

Schwachstellen entdecken. Daher ist eine manuelle Überprüfung notwendig, die sich nicht nur auf die Ergebnisse der Scanner beschränkt, sondern auch die Besonderheiten und spezifischen Funktionsweisen des zu testenden Systems berücksichtigt.

Phase 4 | Exploitation – Ausnutzung

Die vorhergehenden Phasen bereiten die Basis für die Ausnutzung vor. Das Ziel besteht darin, Zugang zu einem System zu erhalten, indem die aufgedeckten Schwachstellen ausgenutzt werden.

Der Pentester muss in dieser Phase sehr vorsichtig und professionell vorgehen, um sicherzustellen, dass die Geschäftsfunktionen nicht beeinträchtigt oder behindert werden. Dennoch ist es ratsam, "Exploits" (to exploit, "ausnutzen") auszuschließen, die beispielsweise zu einem Denial of Service (auch "DoS" abgekürzt) führen.

Phase 5 | Berichterstattung – Abschlusspräsentation

Die letzte Phase des Penetrationstests ist durch die Berichterstattung und Besprechung der Ergebnisse gekennzeichnet. Der Umfang und die Bestandteile des Berichts hängen dabei maßgeblich von den zuvor getroffenen Vereinbarungen zwischen Auftraggeber und Auftragnehmer ab.

Neben einer ausführlichen Darstellung der Ergebnisse mit detaillierten Erläuterungen zu den gefundenen Schwachstellen, Maßnahmen zur Reproduzierbarkeit sowie einer Charakterisierung nach Risikostufe und damit Dringlichkeit des Handlungsbedarfs und insbesondere der Abhilfemaßnahmen zur Behebung sollten in der Regel folgende Bestandteile vorhanden sein:

- Vertraulichkeitserklärung: Diese enthält Informationen wie den Namen des Testers, seine Kontaktdaten und die während des Tests verwendete IP-Adresse. Der Tester verpflichtet sich, die Ergebnisse streng vertraulich zu behandeln und die während des Tests gesammelten personenbezogenen oder sonstigen sensiblen Informationen unverzüglich zu löschen.

- Management Summary: Diese Zusammenfassung ermöglicht es dem Management, wichtige Erkenntnisse aus dem Bericht zu ziehen, ohne zu sehr auf technische Details einzugehen.
- Informationen über die Durchführung des Penetrationstests: Dazu gehören die verwendeten Werkzeuge und Methoden, eine Erläuterung der Vorgehensweise und Priorisierung sowie eventuell festgestellte Probleme, die während oder durch den Penetrationstest aufgetreten sind.

Retest (optional)

Bei einem Retest werden die im Bericht empfohlenen und umgesetzten Abhilfemaßnahmen und Korrekturen zur Behebung der festgestellten Schwachstellen erneut überprüft. Diese Phase wird nach einem angemessenen Zeitraum durchgeführt, um der IT-Abteilung und sonstigen Beteiligten genügend Zeit für die Umsetzung der empfohlenen Maßnahmen zu geben.

Der Aufwand für die Retest-Phase variiert je nach Zielsetzung: Entweder wird gezielt ausschließlich die Wirksamkeit der neu umgesetzten bzw. angepassten Maßnahmen überprüft oder es wird zusätzlich aktiv nach neuen Schwachstellen gesucht, die durch die vorgenommenen Konfigurationsänderungen entstanden sein könnten.

06. Beispielbericht

Du bist neugierig, wie das konkrete Ergebnis eines Pentests aussehen könnte? Dann frag bei uns einfach einen Beispielbericht an!

MORGENSTERN Penetrationstests:
Unser Angebot für deinen sicheren Webauftritt

1 | Quick-Check

Mit unserem Quick-Check möchten wir dir einen ersten Überblick über das Sicherheitsniveau deiner Webseite und gleichzeitig eine Kostprobe unserer Services anbieten. Wir führen eine oberflächliche Überprüfung durch, um offensichtliche Sicherheitsrisiken zu identifizieren.

Dabei liegt unser Fokus auf folgenden Bereichen:

- Patchmanagement
- Prüfung auf bekannte Sicherheitslücken (CVEs)
- TLS/SSL-Anordnung
- Phishing- und Spam-Schutz

2 | Basis-Check

Basierend auf dem Durchführungskonzepts des Bundesamts für Sicherheit in der Informationstechnik (BSI) und den Richtlinien des Open Web Application Security Project (OWASP) untersuchen wir deine Webpräsenz mit automatisierten und manuellen Techniken auf die sogenannten OWASP-Top 10 Sicherheitslücken. Diese stellen ein Ranking der bedeutendsten Bedrohungen, Risiken, Angriffsvektoren und Schwachstellen dar, welche in der (Weiter-) Entwicklung und Absicherung von Webseiten berücksichtigt werden sollten.

Wir stellen dabei u.a. sicher, dass folgende Punkte dem aktuellen Stand der Technik und den empfohlenen Absicherungsmaßnahmen entsprechen:

- Zugriffsmanagement
- Behandlung sensibler Daten
- Verschlüsselungsmechanismen
- Eingabevalidierung / Ausgabe-Maskierung
- Fehlerbehandlung
- Registrierungs- und Login/Passwort-Richtlinien
- Phishing- und Spam-Schutz
- Sicherheitskonfiguration
- Patchmanagement
- Identifizierung und Authentifizierung
- Softwareintegrität
- Systemüberwachung

MORGENSTERN Penetrationstests:
Unser Angebot für deinen sicheren Webauftritt

3 | Advanced-Check

Mit unserem Advanced-Check gehen wir über die grundlegende Sicherheitsanalyse im Rahmen des Basis-Checks hinaus und bieten dir erweiterte Leistungen und maßgeschneiderte Optionen, um deine spezifischen Sicherheitsanforderungen zu erfüllen:

Umfangreicher Support bei der Behebung von Schwachstellen:
Wir stehen dir bei technischen Fragen zur Behebung der identifizierten Schwachstellen und Umsetzung von Abhilfemaßnahmen zur Seite.

Bestätigung der Schwachstellenbehebung:
Nachdem du die Schwachstellen behoben hast, führen wir ein Retest (Nachtest) durch, um sicherzustellen, dass die Abhilfemaßnahmen erfolgreich umgesetzt und Schwachstellen wirksam geschlossen wurden.

Empfehlungen zu "Security Best Practices":
Wir unterstützen dich mit bewährten Methoden bei der kontinuierlichen Verbesserung des Sicherheitsniveaus deiner Webseite.

+ Optionale Services für alle Packages

Bewertung der physischen Sicherheitsaspekte:
Unsere Überprüfung umfasst die Sicherstellung, dass der Schutz deiner physischen Ressourcen den geltenden Sicherheitsstandards entspricht, einschließlich Aspekten wie Zutrittskontrolle, Büroanordnung und sicherer Entsorgung vertraulicher Unterlagen.

Bewertung des Sicherheitsbewusstseins:
Durch gezielte Social-Engineering-Simulationen analysieren wir den Reifegrad des Sicherheitsbewusstseins deiner Mitarbeitenden und stellen dir auch hier gezielte Abhilfemaßnahmen durch unsere Awareness Trainings zur Verfügung – alles aus einer Hand!

Alle Packages inkl. Berichterstattung

Für alle Packages werden nach der Durchführung die Ergebnisse in einem detaillierten Bericht festgehalten. Dieser ist so gestaltet, dass er eine umfassende Analyse der gefundenen Schwachstellen bietet, inklusive ihrer Ausnutzbarkeit und des Schweregrades des damit verbundenen Risikos. Zudem werden detaillierte Handlungsgrundlagen zur Behebung der identifizierten Schwachstellen geliefert.

Das MORGENSTERN Magazin

the future is yours.

No. 3 | Ausgabe 2024

HINTER DEN KULISSEN DER E-LEARNING MAGIE

TOP AKTUELLE THEMEN ZU

DIGITAL LEARNING & E-LEARNING

DATENSCHUTZ, DATENSICHERHEIT & KI

IT-SICHERHEIT, CYBERSICHERHEIT & KI

IT-RECHT & RECHTLICHE ASPEKTE

MORGENSTERN consecom GmbH
Große Himmelsgasse 1
DE - 67346 Speyer

Telefon
+49 (0) 6232 - 100119 44

E-Mail
contact@morgenstern-privacy.com

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere **ISO-Zertifizierungen nach 9001 und 21001** unterstreichen dies. Jetzt informieren

Dieses Whitepaper wurde Ihnen von unserem Content-Partner präsentiert.
sichern Sie sich jetzt eine individuelle und zielgenaue Beratung.

MORGENSTERN legal | Dein Partner in Sachen IT-Recht & Digitalisierung
morgenstern-legal.com

MORGENSTERN privacy | Dein Partner in Sachen Datenschutz & IT-Sicherheit
morgenstern-privacy.com

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de