IT SICHERHEIT 2025

Cyber Security Essentials: Penetrationstests und Schutzmaßnahmen verständlich erklärt!

Schwachstellen erkennen
Risiken minimieren
Angriffe verhindern

Inhaltsverzeichnis

Einleitung

Das E-Book rund um das Thema IT-Sicherheit. In einer digitalisierten Welt, in der nahezu jedes Unternehmen und jede Privatperson auf vernetzte Systeme und Cloud-Dienste angewiesen ist, gewinnt der Schutz sensibler Daten immer mehr an Bedeutung. Cyberangriffe sind längst kein Phänomen mehr, das nur große Konzerne betrifft – selbst kleine und mittlere Unternehmen (KMU) sowie Privatpersonen werden zunehmend zum Ziel.
Dieses E-Book soll Ihnen einen verständlichen Überblick über die Grundlagen der IT-Sicherheit bieten. Dabei gehen wir auf wesentliche Begrifflichkeiten, Konzepte und typische Angriffsszenarien ein. So können Sie erkennen, weshalb eine fundierte Sicherheitsstrategie unerlässlich ist, um sich in der heutigen Bedrohungslandschaft zu schützen.
Im ersten Kapitel befassen wir uns mit den Grundlagen und erläutern wichtige Begrifflichkeiten sowie typische Angriffstypen. Ob Sie bereits im IT-Sicherheitsumfeld tätig sind oder Einsteiger in dieses Thema: Unser Ziel ist es, Ihnen sowohl praktische als auch strategische Impulse zu geben, die Ihnen bei der Absicherung Ihrer IT-Umgebung helfen.

Wichtige Begriffe und Konzepte

IT-Sicherheit ist ein sehr umfangreiches Feld, in dem unterschiedlichste Fachbegriffe kursieren. Im Folgenden stellen wir Ihnen die wichtigsten Konzepte vor, die das Fundament für ein umfassendes Sicherheitsverständnis bilden.

Vertraulichkeit (Confidentiality)

Vertraulichkeit bedeutet, dass nur autorisierte Personen Zugang zu bestimmten Informationen oder Systemen haben. Ein Beispiel hierfür ist die Verschlüsselung von Daten oder der Einsatz sicherer Passwörter.

Integrität (Integrity)

Integrität stellt sicher, dass Daten nicht unbemerkt verändert oder manipuliert werden können. Technisch wird dies oft durch Hash-Verfahren oder Signaturen erreicht, die Veränderungen an Daten erkennen lassen.

Verfügbarkeit (Availability)

Verfügbarkeit bedeutet, dass Systeme und Dienste verlässlich funktionieren und Nutzern zur Verfügung stehen, wenn sie benötigt werden. Dazu zählen Maßnahmen wie Redundanzen, Lastverteilung oder regelmäßige Backups, um Ausfallzeiten zu vermeiden.

Authentifizierung und Autorisierung

Authentifizierung ist der Vorgang, bei dem überprüft wird, ob jemand wirklich die Person oder das System ist, für die/ das er sich ausgibt (z. B. Login mit Passwort oder Multi-Faktor-Authentifizierung).

Autorisierung entscheidet im Anschluss, welche Aktionen dieser Nutzer oder dieses System durchführen darf (z. B. Schreib-/Leserechte, Admin-Berechtigungen).

Bedrohung (Threat), Schwachstelle (Vulnerability) und Risiko (Risk)

Bedrohung: Jegliches Ereignis oder Objekt, das potenziell Schaden verursachen kann (z. B. Hacker, Malware, Naturkatastrophen).
Schwachstelle: Eine Lücke in einem System oder Prozess, die eine Bedrohung ausnutzen kann (z. B. unsichere Konfiguration, fehlendes Patch-Management).
Risiko: Kombination aus der Wahrscheinlichkeit, mit der eine Schwachstelle ausgenutzt wird, und den möglichen Schäden, die daraus entstehen.

Sicherheitsrichtlinien (Policies)

Unternehmensweite Vorgaben, die definieren, wie mit Daten und Systemen umgegangen werden darf. Dazu gehören unter anderem Passwort-Policies, Regelungen zu Bring Your Own Device (BYOD) oder Zugriffsrechten.

Sicherheitskonzepte (z. B. Zero Trust)

Moderne Konzepte wie Zero Trust gehen davon aus, dass jedes Gerät und jeder Dienst im Netzwerk potenziell unsicher ist. Das Prinzip lautet: „Vertraue niemandem, überprüfe jeden.“ Somit wird die komplette IT-Infrastruktur kontinuierlich überwacht und abgesichert.

Authentifizierung und Autorisierung

Defense in Depth“ beschreibt das Prinzip, Sicherheitsmaßnahmen nicht nur auf einer Ebene zu platzieren, sondern mehrstufig abzusichern: vom Perimeterschutz (z. B. Firewall) über Netzsegmentierung, sichere Konfigurationen bis hin zum Schutz einzelner Endgeräte und Anwendungen.

Diese Konzepte bilden die Grundlage für alle Maßnahmen der IT-Sicherheit. Ein tiefes Verständnis hilft Ihnen, die eigenen Risiken besser einzuschätzen und passende Schutzmaßnahmen gezielt umzusetzen.

Angriffstypen und aktuelle Bedrohungslage

Die digitale Welt entwickelt sich rasant – und mit ihr die Bedrohungslandschaft. Cyberkriminelle nutzen immer raffiniertere Methoden, um Unternehmen und Privatpersonen anzugreifen. Hier ein Überblick über verbreitete Angriffstypen und Trends.

Phishing

Bei Phishing-Angriffen versuchen Betrüger, über gefälschte E-Mails oder Webseiten an vertrauliche Informationen (z. B. Zugangsdaten, Kreditkartendaten) zu gelangen. Moderne Phishing-Mails wirken oft täuschend echt, weshalb insbesondere regelmäßige Mitarbeiterschulungen wichtig sind.

Malware (Viren, Würmer, Trojaner, Ransomware)

Malware steht als Sammelbegriff für bösartige Software, die unerwünschte Handlungen auf Geräten auslöst.
Ransomware gehört zu den größten Bedrohungen für Unternehmen: Daten werden verschlüsselt und erst gegen ein Lösegeld wieder freigegeben, was teils zu enormen finanziellen Schäden führt.

DDoS (Distributed Denial of Service)

Angriffe, bei denen eine Vielzahl kompromittierter Systeme (Botnetz) gezielt Anfragen an Server richtet, um diese zu überlasten und für legitime Nutzer unerreichbar zu machen. Solche Angriffe können Webseiten und Onlinedienste stunden- oder tagelang lahmlegen.

Advanced Persistent Threats (APT)

Hochentwickelte, oftmals staatlich unterstützte Gruppen (APT-Gruppen) schleusen sich schrittweise und über einen längeren Zeitraum in ein Netzwerk ein, um sensible Informationen abzuziehen oder gezielte Sabotage zu betreiben. Diese Angriffe sind sehr schwer zu erkennen, da die Angreifer sehr vorsichtig und verdeckt agieren.

Insider-Bedrohungen

Nicht immer stammt die Gefahr von außen: Gerade unzufriedene oder fahrlässige Mitarbeiter können zu einem Sicherheitsrisiko werden, indem sie absichtlich oder versehentlich Daten entwenden, löschen oder an Dritte weitergeben.

Social Engineering

Social Engineering umfasst alle Methoden, die versuchen, durch gezielte Manipulation von Personen Zugang zu vertraulichen Informationen zu bekommen. Das kann ein Anruf sein, in dem sich jemand als Kollege ausgibt und um das „schnelle Durchgeben“ eines Passworts bittet.

Cloud-Angriffe

Mit zunehmender Verlagerung von Daten in Cloud-Services und -Infrastrukturen entstehen neue Angriffspunkte, z. B. durch falsche Konfigurationen von Cloud-Speichern oder unzureichende Authentifizierungsmechanismen.

IoT-Angriffe

Im Internet der Dinge (IoT) ist jedes Gerät mit dem Netzwerk verbunden – von Smart-TVs bis hin zu industriellen Steuerungen. Häufig fehlt hier ein ausreichendes Sicherheitskonzept. Cyberkriminelle nutzen veraltete Firmware oder Standardpasswörter, um ganze IoT-Botnetze aufzubauen.

Die aktuelle Bedrohungslage lässt sich somit am besten als dynamisch und hochprofessionell beschreiben. Es genügt längst nicht mehr, nur eine Firewall und ein Antivirenprogramm einzusetzen. Vielmehr ist ein ganzheitliches Sicherheitskonzept erforderlich, das sowohl technische als auch organisatorische Maßnahmen umfasst und die Human-Firewall (sprich: geschulte Mitarbeiter) mit einschließt.

Was ist ein Penetrationstest?

Ein Penetrationstest (oft kurz „Pentest“ genannt) ist eine kontrollierte und geplante Angriffssimulation, bei der IT-Sicherheitsexperten bewusst versuchen, in ein System oder Netzwerk einzudringen. Das Ziel: **Sicherheitslücken aufdecken**, **Risiken bewerten** und konkrete Maßnahmen ableiten, um die Verteidigung zu verbessern.

Unterschiede zwischen Penetrationstests und anderen Sicherheitsmaßnahmen

In der IT-Sicherheit gibt es zahlreiche Maßnahmen, um die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen sicherzustellen. Penetrationstests stehen dabei meist am Ende einer langen Kette von Sicherheitsbemühungen – oder werden regelmäßig ergänzend eingesetzt.

Vulnerability Scans

Was ist das?
Ein automatisierter Scan, der Systeme (z. B. Server, Anwendungen) auf bekannte Schwachstellen wie veraltete Software oder Konfigurationsfehler untersucht.

Unterschied zum Pentest
Während ein Vulnerability Scan in der Regel nur registriert, dass eine Schwachstelle existiert, geht ein Penetrationstest einen Schritt weiter: Er zeigt auch praktisch, ob und wie sich diese Schwachstelle ausnutzen lässt und welche konkreten Schäden entstehen könnten.

Code Reviews / Sicherheitsaudits

Was ist das?
Dabei wird Quellcode (z. B. von Webanwendungen, Softwaremodulen) manuell oder automatisiert auf Sicherheitslücken und fehlerhafte Implementierungen überprüft. Sicherheitsaudits befassen sich zudem mit Prozessen, Richtlinien und organisatorischen Strukturen.

Unterschied zum Pentest
Ein Code Review bzw. Audit bewertet vor allem die Qualität des Codes oder Prozesses, während der Penetrationstest auf realen Angriffsszenarien basiert. Beide Ansätze ergänzen sich, da Pentests häufig „Black-Box“-Methoden nutzen (ohne detaillierte Code-Einsicht), während Code Reviews einen tiefen Einblick in die Software geben.

Intrusion Detection/Prevention Systems (IDS/IPS)

Was ist das?
Systeme, die Echtzeit-Überwachung von Netzwerkverkehr und Ereignissen leisten, um verdächtige Aktivitäten zu erkennen (IDS) oder zu blockieren (IPS).

Unterschied zum Pentest
IDS/IPS dienen der laufenden Überwachung und Abwehr. Ein Pentest ist hingegen ein zeitlich begrenztes Projekt, das Schwachstellen aufdeckt, bevor sie von echten Angreifern genutzt werden können. Der Pentester „spielt“ den Angreifer aktiv.

Security Information and Event Management (SIEM)

Was ist das?
Eine Plattform, die Daten aus verschiedenen Quellen (Logs, Netzwerkdaten etc.) sammelt, korreliert und auf Anomalien prüft.

Unterschied zum Pentest
Ein SIEM-System ist ein Dauerläufer, der das Netzwerk kontinuierlich im Blick behält. Ein Penetrationstest zeigt, ob ein SIEM-System Angriffe tatsächlich erkennt oder ob bestimmte Aktionen unbemerkt bleiben können.

Penetrationstests sind keine Ersatzmaßnahme für andere Sicherheitslösungen, sondern eine wichtige Ergänzung, um die Effektivität bestehender Maßnahmen praktisch zu überprüfen.
Sie liefern Erkenntnisse über tatsächliche Angriffsszenarien und Gesamtrisiken und können so Lücken aufdecken, die rein theoretische oder automatisierte Ansätze möglicherweise übersehen.

Typen von Penetrationstests

Penetrationstests lassen sich – je nach Ausgangspunkt und Zugriffsrechten – in unterschiedliche Kategorien einteilen. Die bekanntesten Testformen sind **White-Box**, **Black-Box** und **Grey-Box**.

White-Box-Test

Vollständige Transparenz:
Der Pentester erhält alle Informationen über das Zielsystem, darunter Quellcode, Netzwerkpläne, Architekturdiagramme und Zugriffsrechte.

Vorteil:
- Exakte und detaillierte Analyse von Schwachstellen.
- Besonders geeignet, wenn man sicherstellen will, dass jede potenzielle Lücke gefunden wird.

Nachteil:
- Nicht jeder reale Angreifer besitzt solch tiefe Einblicke.
- Test kann länger dauern und muss häufig mit besonderer Vorsicht durchgeführt werden, um das Unternehmen nicht zu beeinträchtigen.

Black-Box-Test

Keine Vorkenntnisse:
Der Tester weiß nur das Nötigste, z. B. die Domain oder IP-Adresse, ähnlich wie ein externer Angreifer.

Vorteil:
- Realitätsnahes Szenario, da ein echter Hacker in der Regel kaum Insiderinformationen besitzt.

Nachteil:
- Einige Schwachstellen bleiben möglicherweise unentdeckt, weil der Tester erst aufwendig recherchieren und „reverse-engineeren“ muss.
- Ergebnisse können weniger tiefgehend ausfallen als beim White-Box-Test.

Grey-Box-Test

Teileinblicke:
Eine Mischform aus White-Box und Black-Box. Der Pentester erhält bestimmte Informationen über die Struktur des Systems, aber nicht den vollständigen Quellcode oder sämtliche Netzwerkdetails.

Vorteil:
- Kompromiss zwischen Realitätsnähe und Effizienz.
- Tester kann zielgerichteter vorgehen, ohne im Dunkeln tappen zu müssen.

Nachteil:
- Je nachdem, wie viel Einblick gewährt wird, kann die Tiefe der Analyse variieren.

Weitere Testkategorien

External vs. Internal:
Externe Tests simulieren Angriffe von außen via Internet, während interne Tests von einem Standpunkt innerhalb des Unternehmensnetzwerks ausgehen (z. B. ein „Ex-Mitarbeiter“-Szenario).

Application Pentests:
Fokus speziell auf Webanwendungen, mobile Apps oder Desktop-Software.

Network Pentests:
Fokus auf Netzwerk-Infrastruktur, Router, Switches, Firewalls und Protokolle.

Physical Pentests:
Testen die physische Sicherheit (z. B. Zugangskontrollen in Gebäuden), sind aber eher eine Ergänzung zu klassischen IT-Pentests.

Je nach Ziel und Risikoprofil können verschiedene Pentest-Typen kombiniert werden. In vielen Fällen ist ein Grey-Box-Ansatz am sinnvollsten, da er den bestmöglichen Kompromiss zwischen Realitätsnähe und Tiefenanalyse bietet. Wichtig ist, den Testumfang und die Testbedingungen vorab klar zu definieren, damit die Erwartungen und Ziele sowohl für Auftraggeber als auch für den Tester transparent sind.

Phasen eines Penetrationstests (mit Praxisbeispielen)

Ein Penetrationstest läuft in der Regel in mehreren aufeinanderfolgenden Phasen ab. Jede Phase hat das Ziel, möglichst realistisch und systematisch vorzugehen, um Schwachstellen zu identifizieren und ihre Auswirkungen einzuschätzen. Im Folgenden stellen wir die wichtigsten Schritte vor und geben kurze Praxisbeispiele zur Veranschaulichung.

Informationsbeschaffung

Beschreibung

- In dieser Phase sammelt der Pentester alle öffentlich zugänglichen Informationen über das Zielsystem oder Unternehmen.
- Häufige Quellen sind Suchmaschinen, soziale Netzwerke, Unternehmenswebsites, Jobportale sowie technische Abfragen (z. B. DNS-Lookups oder Port-Scans).

Zweck

- Das Ziel ist, ein möglichst detailliertes „Bild“ des Ziels zu erhalten, um erste potenzielle Angriffspunkte zu identifizieren.
- Der Tester erfährt beispielsweise, welche Dienste online verfügbar sind, ob bestimmte Software-Versionen laufen oder ob Mitarbeiter sensible Informationen offen teilen.

Praxisbeispiel

- Ein Pentester entdeckt über die Google-Suche ein veraltetes Impressum, in dem noch der Name eines Administrators steht. Eine weitere Recherche auf sozialen Netzwerken zeigt, dass genau dieser Administrator sehr aktiv über technische Themen postet. So könnten E-Mail-Adressen, Vorlieben oder Kenntnisse aufgespürt werden, die später für Social-Engineering-Angriffe genutzt werden.

Schwachstellenanalyse

Beschreibung

- Aufbauend auf den gesammelten Informationen werden nun systematisch Schwachstellen gesucht.
- Dies geschieht mithilfe automatisierter Tools (z. B. Vulnerability Scanner) und manueller Überprüfung (z. B. Code-Reviews oder händische Tests von bestimmten Eingabeformularen).

Zweck

- Ziel ist es, eine Liste möglicher Sicherheitslücken zu erstellen und ihre Kritikalität einzuschätzen (z. B. durch Common Vulnerability Scoring System – CVSS).

Praxisbeispiel

- Der Pentester führt einen Port-Scan durch und entdeckt, dass auf einem Webserver ein veralteter Apache- oder IIS-Dienst läuft. Die Version ist bekannt für eine kritische Sicherheitslücke, die es Angreifern erlaubt, sich unbefugt Zugriff auf das System zu verschaffen. Diese Lücke wandert sofort in die Liste prioritärer Schwachstellen.

Exploitation

Beschreibung

- In dieser Phase versucht der Tester aktiv, die identifizierten Schwachstellen auszunutzen.
- Das kann das Ausführen von Schadcode, das Erweitern von Benutzerrechten oder das Abgreifen von Daten beinhalten.

Zweck

- Prüfen, ob und wie leicht sich eine Lücke in der Praxis ausnutzen lässt.
- Ermitteln, welche Auswirkungen ein Angriff hätte (z. B. Zugriff auf Datenbank mit Kundendaten, Übernahme von Administratorrechten).

Praxisbeispiel

- Die erwähnte alte Apache-Version enthält eine Remote Code Execution-Lücke. Der Pentester startet ein dafür konzipiertes Exploit-Skript, das ihm erlaubt, beliebige Befehle auf dem Server auszuführen. Innerhalb kurzer Zeit erhält er Administratorrechte (Root-Privilegien) und kann auf wichtige Daten zugreifen.

Post-Exploitation und Persistenz

Beschreibung

- Nachdem die erste Schwachstelle erfolgreich ausgenutzt wurde, geht es darum, den Zugriff zu festigen und weitere Systeme im Netzwerk zu kompromittieren.
- Hierbei werden oft Hintertüren (Backdoors) eingerichtet oder es wird versucht, in andere (höher privilegierte) Bereiche des Netzwerks vorzudringen.

Zweck

- Aufzuzeigen, wie tief ein Angreifer ins Unternehmensnetz vordringen und welche zusätzlichen Systeme er kontrollieren könnte, wenn der erste Zugang einmal geschaffen ist.
- Ebenso lässt sich herausfinden, ob es Abwehrmechanismen gibt, die den Angreifer aufhalten, sowie ob ein Eindringen überhaupt bemerkt würde.

Praxisbeispiel

- Nach dem erfolgreichen Hack des Webservers installiert der Pentester einen sogenannten Web-Shell. Dadurch kann er die Kontrolle behalten, selbst wenn die ursprüngliche Lücke geschlossen wird. Von diesem Server aus scannt er nun das interne Netz und entdeckt weitere Server mit Standardpasswörtern. Schritt für Schritt dehnt er seinen Zugriff aus.

Reporting und Maßnahmen

Beschreibung

- Am Ende des Penetrationstests fasst der Tester alle Ergebnisse in einem detaillierten Bericht zusammen.
- Der Bericht enthält eine Übersicht über die gefundenen Schwachstellen, den Schweregrad der Lücken und konkrete Handlungsempfehlungen, wie diese geschlossen werden können.

Zweck

- Dem Auftraggeber (Unternehmen, IT-Abteilung, Management) soll aufgezeigt werden, wo welche Risiken bestehen und wie dringlich diese sind.
- Das Unternehmen erhält einen konkreten Aktionsplan, um die Sicherheitslücken möglichst schnell zu beheben.

Praxisbeispiel

- Im Abschlussbericht ist aufgeführt, dass die Webserver-Software dringend auf eine aktuelle Version gebracht werden muss. Zudem wird empfohlen, Multi-Faktor-Authentifizierung für kritische Administrationszugriffe einzurichten und regelmäßige Sicherheitsüberprüfungen (z. B. Vulnerability Scans) durchzuführen. Der Pentester priorisiert alle Lücken nach Kritikalität – von „kritisch“ über „hoch“ bis „gering“ – damit das Unternehmen gezielt an die Problembehebung herangehen kann..

Die Phasen eines Penetrationstests sind strukturiert und basieren auf gängigen Standards (z. B. PTES, NIST, OWASP). Jeder Schritt dient dazu, die realistische Vorgehensweise eines Angreifers abzubilden. Das Hauptziel: Unternehmen und Organisationen sollen Schwachstellen erkennen und die notwendigen Maßnahmen treffen, um ihre IT-Umgebung abzusichern. Ein professionell durchgeführter Test endet daher niemals ohne einen umfassenden Bericht und klare Empfehlungen, damit der Fokus nicht nur auf dem Aufdecken, sondern auch dem Beseitigen von Sicherheitslücken liegt.

Verantwortlichkeiten und Haftung

Management und Geschäftsführung

- In vielen Fällen sind Vorstände, Geschäftsführer und leitende Angestellte persönlich dafür verantwortlich, IT-Sicherheitsrisiken zu minimieren und gesetzliche Anforderungen einzuhalten.
- Die Sorgfaltspflicht umfasst auch die Umsetzung angemessener Sicherheitsmaßnahmen. Wird diese vernachlässigt und entsteht ein Schaden, kann es zu zivil- oder strafrechtlichen Konsequenzen kommen.

Datenschutzbeauftragter

- Unternehmen, die eine gewisse Größe an Mitarbeitenden überschreiten oder besonders sensible Daten verarbeiten, müssen einen Datenschutzbeauftragten benennen.
- Er oder sie überwacht die Einhaltung der DSGVO und anderer Datenschutzgesetze, ist jedoch nicht für die tatsächliche Umsetzung verantwortlich (diese obliegt der Geschäftsführung).

IT-Abteilung und externe Dienstleister

- Interne IT-Abteilungen oder beauftragte Dienstleister tragen ebenfalls eine Mitverantwortung, da sie technische Sicherheitskonzepte umsetzen und pflegen müssen.
- Wurden Sicherheitslücken erkannt, aber nicht behoben, können im Schadensfall Ansprüche gegen die Verantwortlichen geltend gemacht werden. Bei externer Vergabe an Dienstleister sollte ein klarer Vertrag (Auftragsdatenverarbeitung, SLA) regeln, wer wofür haftet.

Mitarbeiter und Awareness

- Jeder Mitarbeiter trägt zur IT-Sicherheit bei. Fahrlässiger Umgang mit Passwörtern, Software-Downloads aus unsicheren Quellen oder die Weitergabe von Daten an Unbefugte können große Schäden verursachen.
- Arbeitgeber sind verpflichtet, Schulungen und Richtlinien anzubieten, während Mitarbeiter eine Mitwirkungspflicht haben, diese Vorgaben zu befolgen.

- Unternehmen, die diese Anforderungen ignorieren, riskieren hohe Bußgelder, Imageschäden und rechtliche Konsequenzen.
- Erfolgreiches IT-Sicherheitsmanagement setzt eine Teamleistung voraus: Von der Geschäftsführung über den IT-Verantwortlichen bis hin zum einzelnen Mitarbeiter sollte jeder wissen, welche Standards gelten und welche Verantwortung er trägt.
- Mit einer regelmäßigen Überprüfung (z. B. durch Penetrationstests, interne Audits oder Zertifizierungen nach ISO 27001) können Unternehmen sicherstellen, dass sie nicht nur auf dem Papier, sondern auch in der Praxis compliant sind.

Praktische Umsetzung eines Penetrationstests

Ein Penetrationstest ist weit mehr als nur das Ausführen einiger Tools. Um realistische Ergebnisse zu erzielen, braucht es ein gut strukturiertes Konzept, passende Werkzeuge sowie eine gründliche Dokumentation. Anschließend sollten die gewonnenen Erkenntnisse in konkrete Maßnahmen übersetzt werden, damit das Unternehmen tatsächlich von den Testergebnissen profitiert.

Erstellung eines Testkonzepts

Zieldefinition
Bevor der eigentliche Test beginnt, sollte klar sein, was getestet werden soll und warum.
Mögliche Ziele: Aufdecken kritischer Schwachstellen im Webshop, Überprüfung der internen IT-Infrastruktur, Sicherstellung von Compliance-Anforderungen.

Scope-Festlegung
Entscheiden Sie, welche Systeme, Netzwerke, Anwendungen oder Cloud-Dienste in den Test einbezogen werden.
Legen Sie fest, ob es sich um einen externen oder internen Penetrationstest handelt und welche Bereiche ggf. ausgeschlossen bleiben (z. B. Produktionssysteme mit hohen Verfügbarkeitsanforderungen).

Rollen und Verantwortlichkeiten
Bestimmen Sie, wer im Unternehmen als Ansprechpartner fungiert und wer das „Go“ für kritische Testschritte geben muss.
Internes Team, externe Pentester oder eine Kombination beider? Achten Sie auf klare Zuständigkeiten und kurze Kommunikationswege.

Zeitplanung und Genehmigungen
Erstellen Sie einen Zeitplan, der sowohl die Vorbereitung, den Test selbst als auch die Nachbereitung einschließt.
Holen Sie vorab Genehmigungen ein, um rechtliche Risiken zu vermeiden. Insbesondere bei Tests, die Dritte oder Cloud-Umgebungen betreffen, ist eine schriftliche Erlaubnis oft Pflicht.

Risikoabwägung und Sicherheitsnetze
Ein Penetrationstest kann Systeme beeinträchtigen oder sogar zum Absturz bringen, wenn kritische Exploits verwendet werden.
Planen Sie Notfallmaßnahmen ein: etwa Zeitfenster außerhalb der Hauptgeschäftszeiten oder eine sofortige Kontaktaufnahme, falls Störungen auftreten.

Durchführung und Dokumentation

Erstellung eines Testkonzepts

Testdurchführung

- Die eigentliche Angriffssimulation beginnt mit den Phasen der Informationsbeschaffung, Schwachstellenanalyse, Exploitation und ggf. Post-Exploitation (siehe Kapitel 4).
- Wichtig: Transparente Kommunikation mit den Projektverantwortlichen, um negative Auswirkungen auf das Tagesgeschäft zu minimieren.

Laufende Protokollierung

- Jeder Schritt sollte nachvollziehbar dokumentiert werden:
- Welche Tools wurden in welcher Konfiguration eingesetzt?
- Welche Schwachstellen konnten gefunden und ausgenutzt werden?
- Diese Informationen sind entscheidend, um später die richtigen Schlüsse zu ziehen und Gegenmaßnahmen einzuleiten.

Reporting

- Ein **Abschlussbericht** fasst alle Ergebnisse zusammen und beinhaltet:
- **Beschreibung der Schwachstelle**
- **Auswirkungen** auf das Unternehmen (finanziell, rechtlich, reputationsbezogen)
- **Empfehlungen** zum Schließen der Lücken
- **Priorisierung** nach Kritikalität (z. B. High, Medium, Low)
- Dieser Bericht ist meist für verschiedene Zielgruppen relevant: Technische Mitarbeiter benötigen Detailinformationen, das Management benötigt eine verständliche Zusammenfassung der Risiken und Kosten.

Nachbesprechung und Retest

- Nach dem Test und dem Erhalt des Berichts sollten Maßnahmen priorisiert und in einem Aktionsplan festgehalten werden.
- Ein anschließender Re-Test stellt sicher, dass die umgesetzten Korrekturen wirksam sind und keine neuen Lücken entstanden sind.

Umsetzungsstrategie für Unternehmen

Schrittweises Vorgehen

- Gerade in großen Organisationen ist es sinnvoll, mit Teilbereichen zu beginnen (z. B. kritische Webanwendungen oder Kernsysteme), bevor das gesamte IT-Ökosystem getestet wird.
- So lassen sich erste Erfolge erzielen, ohne das Unternehmen zu überfordern.

Regelmäßige Tests einplanen

- IT-Systeme und Bedrohungslagen verändern sich ständig. Ein einmaliger Penetrationstest spiegelt nur eine Momentaufnahme wider.
- Planen Sie regelmäßige oder anlassbezogene Tests (z. B. nach großen Updates, Systemmigrationen oder Sicherheitsvorfällen).

Integration in das Risikomanagement

- Die Ergebnisse des Pentests sollten Teil eines kontinuierlichen Risikomanagements sein.
- Wichtig ist es, die identifizierten Risiken mit anderen Unternehmensrisiken (z. B. finanzielle, strategische) zu verknüpfen, um klare Prioritäten für Investitionen in die IT-Sicherheit zu setzen.

Awareness und Schulung

- Nutzen Sie die Ergebnisse, um das Bewusstsein für IT-Sicherheit im Unternehmen zu erhöhen.
- Workshops, Schulungen und interne Informationskampagnen helfen, auch Mitarbeiter außerhalb der IT in das Thema einzubinden.

Zusammenarbeit mit externen Partnern

- Wenn das interne Know-how nicht ausreicht, lohnt sich die Zusammenarbeit mit spezialisierten Penetrationstest-Anbietern oder IT-Sicherheitsberatungen.
- Achten Sie auf Zertifizierungen (z. B. OSCP, CISM, CISSP) und Referenzen, um die Qualität der Dienstleistung sicherzustellen.

Maßnahmen zur IT-Sicherheit außerhalb von Pentests

Penetrationstests sind ein hervorragendes Instrument, um akute Schwachstellen aufzudecken und die Widerstandsfähigkeit Ihrer IT-Systeme regelmäßig zu überprüfen. Allerdings reicht ein gelegentlicher Pentest allein nicht aus, um ein ganzheitlich hohes Sicherheitsniveau zu gewährleisten. In diesem Kapitel stellen wir zentrale Maßnahmen vor, die parallel oder unabhängig von Pentests für eine robuste IT-Sicherheit sorgen.

Härtung von Systemen

Beschreibung
„System Hardening“ oder „Härtung“ bedeutet, Betriebssysteme, Anwendungen und Netzwerkkomponenten so zu konfigurieren, dass Angriffsflächen minimiert und Fehlkonfigurationen vermieden werden.

Beispiele und Vorgehensweisen
Deaktivieren unnötiger Dienste

- Standardmäßig sind in manchen Betriebssystemen oder Anwendungen Dienste aktiviert, die nicht benötigt werden. Jeder unnötige Dienst ist eine potenzielle Schwachstelle.

Sichere Konfiguration

- Absicherung von Servern und Diensten mittels Firewalls, Zugriffskontrolllisten (ACLs) und verschlüsselter Kommunikation (z. B. HTTPS/SSH statt unverschlüsseltes HTTP/Telnet).

Patch-Management

- Regelmäßige und zeitnahe Updates von Betriebssystemen, Anwendungen und Firmware.

Passwort- und Berechtigungsrichtlinien

- Durchsetzen starker Passwörter, Multi-Faktor-Authentifizierung und das Prinzip der geringsten Rechte (Least Privilege).

Vorteil

- Eine gute Basiskonfiguration reduziert das Risiko, dass Angreifer Erfolg haben, selbst wenn sie einzelne Schwachstellen ausnutzen wollen.

Zero-Trust-Strategie

Beschreibung
Das Zero-Trust-Modell geht davon aus, dass kein Gerät, Benutzer oder Netzwerkbereich per se vertrauenswürdig ist – unabhängig davon, ob er sich innerhalb oder außerhalb des Unternehmensnetzwerks befindet.

Kernprinzipien
Alles und jeden überprüfen

- Jeder Zugriff auf ein System oder einen Dienst wird grundsätzlich neu authentifiziert und autorisiert.

Least Privilege

- Auch innerhalb des Netzwerks oder der Anwendung werden Rechte strikt auf das notwendige Minimum beschränkt.

Mikrosegmentierung

- Das Netzwerk wird in viele kleine Bereiche aufgeteilt, sodass ein kompromittiertes System nicht automatisch Zugriff auf andere Bereiche bekommt.

Kontinuierliche Überwachung

- Zugriffe, Anomalien und verdächtige Aktivitäten werden in Echtzeit analysiert, um schnell reagieren zu können.

Vorteil

- Eine gute Basiskonfiguration reduziert das Risiko, dass Angreifer Erfolg haben, selbst wenn sie einzelne Schwachstellen ausnutzen wollen.

Sicherheitsschulungen für Mitarbeiter

Beschreibung
Mitarbeiterschulungen sind ein essentieller Teil jeder Sicherheitsstrategie, weil Menschen häufig das schwächste Glied in der Sicherheitskette sind (z. B. durch Phishing, Social Engineering, unsichere Passwörter).

Inhalte
Grundlagen des sicheren Arbeitens

- Erkennen von Phishing-Mails, Umgang mit verdächtigen Links oder Anhängen, Schutz sensibler Dokumente.

Passworthygiene

- Erstellen starker Passwörter, kein Wiederverwenden von Passwörtern, Nutzung von Passwortmanagern.

Vertraulichkeit und Datenschutz

- Sensibilisierung für den verantwortungsvollen Umgang mit personenbezogenen und unternehmenskritischen Daten.

Meldewege

- Wie verhalte ich mich bei einem Sicherheitsvorfall? An wen kann ich mich im Zweifel wenden?

Umsetzung

- Regelmäßige Schulungen (z. B. einmal pro Quartal, Halbjahr oder Jahr), damit das Wissen aktuell bleibt.
- Interaktive Formate (Workshops, Phishing-Tests, E-Learning-Plattformen) erhöhen die Lernmotivation.

Incident Response und Notfallpläne

Beschreibung

- Incident Response umfasst den strukturierten Umgang mit Sicherheitsvorfällen – von der Erkennung eines Angriffs bis zur Behebung und Wiederherstellung des Normalbetriebs.
- Notfallpläne oder Business Continuity Plans (BCP) konzentrieren sich darauf, zentrale Geschäftsprozesse auch im Krisenfall aufrechtzuerhalten.

Elemente eines Incident-Response-Plans

Erkennung und Alarmierung

- Klare Kriterien und Tools (z. B. Intrusion Detection Systems, SIEM) definieren, ab wann ein Ereignis kritisch ist.

Rollen und Zuständigkeiten

- Wer ist Teil des Incident-Response-Teams? Wer informiert wen (Geschäftsführung, externe Dienstleister, Behörden)?

Containment und Beseitigung

- Maßnahmen, um die Ausbreitung eines Angriffs zu stoppen (z. B. Netzwerksegmentierung, Trennung befallener Systeme).

Wiederherstellung

- Nutzung von Backups und neu aufgesetzten Systemen, um den Geschäftsbetrieb schnell zu normalisieren.

Dokumentation und Lessons Learned

- Aus jedem Vorfall sollte das Unternehmen lernen, um ähnliche Situationen künftig zu vermeiden.

Warum wichtig?

- Auch bei bester Prävention kann ein Sicherheitsvorfall nie ganz ausgeschlossen werden. Ein durchdachter und geübter Notfallplan minimiert Schäden, beschleunigt die Wiederherstellung und schafft Vertrauen bei Kunden und Partnern.

Pentest-Planung Checkliste

Zieldefinition
- Was wollen wir testen? (z. B. Webanwendungen, interne Netzwerke, Cloud-Dienste)
- Geht es primär um Compliance, Risikoerkennung oder Sicherheitsbewusstsein?

Scope-Festlegung
- Welche Systeme und IP-Bereiche sind im Test enthalten?
- Soll der Pentest intern, extern oder in hybrider Form stattfinden?
- Gibt es Bereiche, die explizit nicht getestet werden dürfen (z. B. Produktionssysteme)?

Testart und Vorgehensweise
- Black-Box-, White-Box- oder Grey-Box-Testing?
- Erlauben wir den Testern Einsicht in Code oder Systemdokumentation?
- Ggf. Social-Engineering-Aspekte einschließen?

Rollen und Verantwortlichkeiten
- Wer ist Hauptansprechpartner im Unternehmen (IT-Leitung, Sicherheitsbeauftragter)?
- Wer koordiniert den Test mit externen Dienstleistern?

Zeitplan und Ressourcen
- Festlegung eines realistischen Testzeitraums (ggf. außerhalb von Stoßzeiten).
- Sind interne Mitarbeiter verfügbar, um Rückfragen der Tester zeitnah zu klären?

Genehmigungen und Vertragliches
- Liegen schriftliche Genehmigungen vor, insbesondere bei externen Pentestern?
- Klare vertragliche Regelung: Haftung, Geheimhaltung, Datenschutz.

Risikoabwägung
- Notfallmaßnahmen definieren, falls es zu Systemausfällen während des Tests kommt.
- Kommunikationswege bei kritischen Funden: Wer wird wann informiert?

Reporting und Nachbereitung
- Wie soll der Endbericht aussehen, an wen wird er adressiert?
- Wie wird sichergestellt, dass gefundene Schwachstellen behoben werden (Re-Test)?

IT-Sicherheits-Checkliste für Unternehmen

Organisationsstruktur
Gibt es einen definierten Sicherheits- oder Datenschutzbeauftragten?

Sicherheitsrichtlinien
Existieren schriftliche Policies (Passwortvorgaben, BYOD, etc.)?

Zugriffs- und Berechtigungsmanagement
Werden Zugriffsrechte regelmäßig überprüft und angepasst?

Patch-Management
Gibt es einen Prozess, um OS- und Software-Patches zeitnah einzuspielen?

Backup-Strategie
Werden Backups regelmäßig erstellt, geprüft und auch offline gelagert?

Netzwerksegmentierung & Firewall
Sind geschäftskritische Systeme isoliert? Firewall-Regeln aktuell?

Endpoint Security
Sind Virenscanner, Endpoint-Protection und Verschlüsselung aktiv?

Logging & Monitoring
Werden sicherheitsrelevante Ereignisse protokolliert und ausgewertet?

Schulungen & Sensibilisierung
Werden Mitarbeitende regelmäßig zu IT-Sicherheit und Phishing geschult?

Notfallpläne & Incident Response
Sind Pläne dokumentiert und werden sie wiederkehrend geübt?

Test & Audits
Wird regelmäßig ein Pentest oder eine IT-Sicherheitsanalyse durchgeführt?

Datenschutz & Compliance
Werden gesetzliche Vorgaben (z. B. DSGVO) und Branchenstandards eingehalten?

Cloud- & Drittanbieter-Risiken
Sind Verträge & Sicherheitsanforderungen mit Dienstleistern klar geregelt?

Reaktionsplan für Cyberangriffe

Erkennung und Alarmierung

- Legen Sie fest, wer Angriffe erkennt (Monitoring-Team, SIEM-System).
- Definieren Sie klare Meldewege (z. B. IT-Leitung, Geschäftsführung, externe Sicherheitsdienstleister).

Analyse und Einstufung

- Einrichten eines Incident-Response-Teams (IT, Recht, Kommunikation, Datenschutz).
- Einstufung der Schwere des Vorfalls (gering, mittel, hoch) und der betroffenen Systeme.

Eindämmungsmaßnahmen

- Netzwerkzugriffe beschränken, kompromittierte Benutzerkonten sperren.
- Ggf. Systeme vom Netz trennen, um Ausbreitung zu verhindern.

Beseitigung der Ursachen

- Identifizieren der Einfallstore (z. B. fehlende Patches, unsichere Konfiguration).
- Schließen der Lücken, Patchen von Software oder Neuinstallation kompromittierter Systeme.

Wiederherstellung des Betriebs

- Restore aus sauberen Backups, falls erforderlich.
- Schrittweise Wiederinbetriebnahme, Test und Überprüfung, ob der Angriff tatsächlich beseitigt ist.

Kommunikation

- Informieren von Führungskräften, betroffenen Mitarbeitern, ggf. Behörden (z. B. Datenschutzaufsicht bei DSGVO-relevanten Datenlecks).
- Bei größeren Vorfällen: Offenlegung an Kunden oder öffentliche Stellungnahmen (PR).

Dokumentation und Lessons Learned

- Alle Schritte dokumentieren: Was wurde wann entdeckt, welche Maßnahmen wurden wann umgesetzt?
- Nach dem Vorfall: Analyse, wie ähnliche Angriffe in Zukunft frühzeitiger erkannt oder verhindert werden können.

Nachbereitung / Re-Test

- Überprüfung der neu eingeführten Maßnahmen durch einen Penetrationstest oder internes Audit.
- Sicherstellen, dass alle Verantwortlichen die aktualisierten Pläne kennen.

15Min.Tech TALK

www.15min.tech

info@15min.tech