CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

PENETRATION TESTING

Was genau ist Penetration Testing und warum ist es wichtig für mein Unternehmen?

Penetration Testing, kurz Pentesting, ist ein simulierter Angriff auf Ihre IT-Systeme, um Schwachstellen aufzudecken, die von Angreifer:innen ausgenutzt werden könnten.
Es gibt verschiedene Art von Pentests, dazu mehr hier. Eine technische Wirksamkeitsprüfung eines Pentests gibt Ihnen und Ihren Mitarbeiter:innen die Sicherheit, dass die gesetzten Verteidigungsmaßnahmen realen Angriffen standhalten.

WELCHE RISIKEN BESTEHEN IN IT-SYSTEMEN FÜR UNTERNEHMEN?

RISIKO RANSOMWARE

Wahrscheinlichkeit: Mittel bis hoch, da Ransomware-Angriffe in den letzten Jahren zugenommen haben und viele Unternehmen betroffen sind.

Schaden: Hoch, da die Auswirkungen eines Ransomware-Angriffs erhebliche finanzielle Verluste und Betriebsstörungen verursachen können.

RISIKO DATENLECKS

Wahrscheinlichkeit: Mittel, Datenlecks treten regelmäßig auf, aber nicht alle Unternehmen sind gleichermaßen betroffen.

Schaden: Hoch, da die Freisetzung sensibler Daten zu erheblichen Bußgeldern, Reputationsverlust und potenziellen Rechtsstreitigkeiten führen kann.

RISIKO COMPLIANCE

Wahrscheinlichkeit: Gering bis mittel, viele Unternehmen haben Verfahren zur Einhaltung der Compliance, jedoch können unbeabsichtigte Verstöße auftreten.

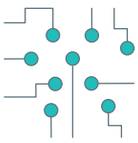
Schaden: Hoch, da Non-Compliance zu finanziellen Strafen und Reputationsschäden führen kann.

pentest.ait.ac.at

PENETRATION TESTING

AUSTRIAN INSTITUTE OF TECHNOLOGY

WELCHE TECHNISCHEN SICHERHEITSTESTS BIETET DAS AIT AN?

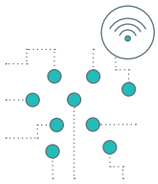


NETZWERK-PENETRATIONTEST

Hierbei werden die Netzwerkinfrastruktur und die Systeme auf Schwachstellen untersucht, um festzustellen, ob Angreifer:innen Zugang zu sensiblen Daten oder Systemen erhalten könnten.

ANWENDUNGS-PENETRATIONTEST

Dieser Test konzentriert sich auf die Sicherheit von Anwendungen, einschließlich Webanwendungen, mobilen Apps oder Desktop-Software. Ziel ist es, Schwachstellen in der Anwendungslogik, Authentifizierungsmechanismen und Datenverarbeitung aufzudecken.



WIRELESS-PENETRATIONTEST

Hierbei werden drahtlose Netzwerke und deren Sicherheitsmechanismen überprüft, um festzustellen, ob unautorisierte Benutzer:innen Zugriff auf das Netzwerk erlangen könnten.

SOCIAL ENGINEERING-TEST

Dieser Test zielt darauf ab, die Reaktion der Mitarbeiter:innen auf soziale Manipulation oder Täuschung zu überprüfen, um festzustellen, wie gut das Unternehmen gegenüber Social Engineering-Angriffen geschützt ist.

PHISHING-TEST

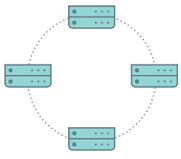
Hierbei wird simuliert, wie gut Mitarbeiter:innen auf Phishing-E-Mails oder gefälschte Websites reagieren. Dies hilft, das Bewusstsein für Phishing-Angriffe zu schärfen und die Schulungsbedürfnisse zu identifizieren.

PHYSICAL SECURITY-TEST

Dieser Test befasst sich mit der physischen Sicherheit eines Unternehmens, indem er versucht, unbefugten Zugang zu sensiblen Bereichen zu erhalten oder Geräte zu stehlen.

RED TEAM-TEST

Hierbei handelt es sich um eine umfassendere Form des Penetrationtests, bei dem ein Team von Sicherheitsexpert:innen versucht, das Unternehmen anzugreifen. Dies simuliert einen realen Angriff und hilft, die Gesamtsicherheit zu bewerten.



IOT-PENETRATIONTEST

Bei diesem Test werden vernetzte Geräte und das Internet der Dinge (IoT) auf Schwachstellen untersucht, um potenzielle Angriffsvektoren zu identifizieren.

CLOUD-PENETRATIONTEST

Hierbei werden Cloud-Infrastrukturen, -Dienste und -Anwendungen auf Sicherheitsmängel geprüft, da Unternehmen zunehmend Cloud-Plattformen nutzen.

Da Standards und Regulatorien sich ändern und auch unterschiedlich interpretiert werden können, prüfen wir gerne den aktuellen Stand und Ihren speziellen Fall.

Kontaktieren Sie uns.

pentest.ait.ac.at

PENETRATION TESTING

AUSTRIAN INSTITUTE OF TECHNOLOGY

WIE LÄUFT EIN PENTEST AB?

Wir haben die Phasen eines Pentests, wie vom AIT durchgeführt, in folgendem Bild auf hoher Flugebene für Sie zusammengestellt: Die technischen Schritte und Subphasen erklären wir Ihnen gerne bei einem kostenlosen Erstgespräch.

PLANUNG

In der Planungs- und Vorbereitungsphase werden der Umfang des Penetration Testings (z.B. Anwendungen, Systeme) und die erforderlichen Ressourcen (z.B. Benutzer:innen-Accounts mit unterschiedlichen Berechtigungen), Kontakte zu Kund:innen sowie der Testzeitraum festgelegt.

VORBEREITUNG

Informationsgewinnung über das Ziel, Analyse möglicher Angriffsvektoren und Entwicklung einer auf Kund:innen zugeschnittenen Teststrategie.

DURCHFÜHRUNG

Ausnutzung identifizierter Schwachstellen. Nach Möglichkeit Fortsetzung der Angriffe auf nun erreichbare Systeme im Netz.

PRÄSENTATION

Umfassender Abschlussbericht mit Schwachstellenfunden und Verbesserungsmaßnahmen. Abschlusspräsentation, Festlegung der nächsten Schritte und Unterstützung bei der Umsetzung.

WIE OFT SOLLEN SICHERHEITSTESTS DURCHGEFÜHRT WERDEN?

Die Empfehlungen der Standards und Regulierungen gehen auseinander und hängen vom spezifischen Kontext und den Anforderungen an Ihre Organisation oder Ihr Produkt ab. Allgemein empfehlen wir jährliche Penetrationtests, sowie Tests bei größeren Änderungen. Automatisierte Schwachstellenscans sollten laufend durchgeführt werden, oder aber zumindest einmal pro Quartal. Wir haben hier eine Übersicht der verschiedenen Standards zusammen gefasst.

STANDARD / KATALOG	SCHWACHSTELLENSCAN	PENETRATIONTEST	RED-TEAMING / PURPLE-TEAMING
PCI DSS	Vierteljährlich Jährlich	Nicht spezifiziert	Empfohlen, aber nicht spezifiziert
NIS2-Richtlinie	Nicht spezifiziert	Periodisch	Nicht spezifiziert
DSGVO	Nicht direkt spezifiziert	Empfohlen für Verarbeitungstätigkeiten mit hohem Risiko	Nicht spezifiziert
ISO/IEC 27001	Empfohlen als Teil des kontinuierlichen Risikomanagementprozesses	Empfohlen basierend auf Risikobewertung	Nicht spezifiziert
Sarbanes-Oxley Act/SOC2	Nicht direkt spezifiziert	Empfohlen	Nicht spezifiziert
TISAX**	Mindestens jährlich	Mindestens alle 3 Jahre	Nicht spezifiziert
Cyber Resilience Act	Nicht direkt spezifiziert	Empfohlen	Nicht spezifiziert
Microsoft Cloud	Empfohlen	Empfohlen	Nicht spezifiziert

**Die Angaben basieren auf den allgemeinen Best Practices und Richtlinien für industrielle Sicherheitssysteme.

Die Frequenz kann basierend auf der Größe der Organisation, der Art der verarbeiteten Daten und der Risikolandschaft variieren. Insbesondere sollten externe Faktoren, wie eine Änderung in der Bedrohungslandschaft, aber auch interne Faktoren, wie die Änderungen ihrer IT/OT-Umgebung berücksichtigt werden.

pentest.ait.ac.at

PENETRATION TESTING

WARUM SIND DIE KOSTEN FÜR PENETRATIONTESTS SO UNTERSCHIEDLICH?

UMFANG UND KOMPLEXITÄT
Je umfassender und komplexer der Umfang des Penetrationtests ist, desto mehr Zeit und Ressourcen werden benötigt. Tests, die mehr Systeme, Anwendungen oder Netzwerke abdecken, erfordern zusätzliche Arbeit und können teurer sein.

ART DES TESTS
Verschiedene Arten von Penetrationtests haben unterschiedliche Anforderungen und Kosten. Ein einfacher Netzwerk-Penetrationtest kann weniger kosten als ein umfassender Red Team-Test, der mehrere Angriffsszenarien simuliert.

QUALIFIKATION DER EXPERT:INNEN
Die Erfahrung und Qualifikation der Sicherheitsexpert:innen, die den Test durchführen, können die Kosten beeinflussen. Hochqualifizierte Expert:innen verlangen möglicherweise höhere Honorare.

TECHNISCHE ANFORDERUNGEN
Manche Tests erfordern spezielle Tools, Hardware oder Infrastrukturen, die zusätzliche Kosten verursachen können.

BRANCHENSPEZIFISCHE ANFORDERUNGEN
Bestimmte Branchen wie Finanzwesen oder Gesundheitswesen haben spezielle Sicherheitsanforderungen, die die Kosten erhöhen können.

REISE- UND VOR-ORT-KOSTEN
Wenn der Test vor Ort durchgeführt wird oder Reisen erforderlich sind, um physische Standorte zu überprüfen, können Reisekosten und Zeitaufwand die Kosten erhöhen.

WIEDERHOLTE TESTS
Ein regelmäßig durchgeführter Penetrationtest kann möglicherweise günstigere Konditionen bieten.

WAS PASSIERT, NACHDEM EIN PENETRATIONTEST ABGESCHLOSSEN IST?

Nach einem Penetrationtest erhalten Sie einen umfassenden Bericht mit den identifizierten Schwachstellen und Empfehlungen zur Behebung. Wir helfen Ihnen die Schwachstellen zu beheben und prüfen anschließend mit Ihnen gemeinsam, ob diese auch wirklich geschlossen sind.

Unsere Spezialist:innen sind bereit alle Ihre Fragen zu beantworten.

Wenden Sie sich bitte an unseren Pentest Team Lead:

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
Manuel Kern MSc
Tel +43 50550 4170
+43 50550 4150
manuel.kern@ait.ac.at