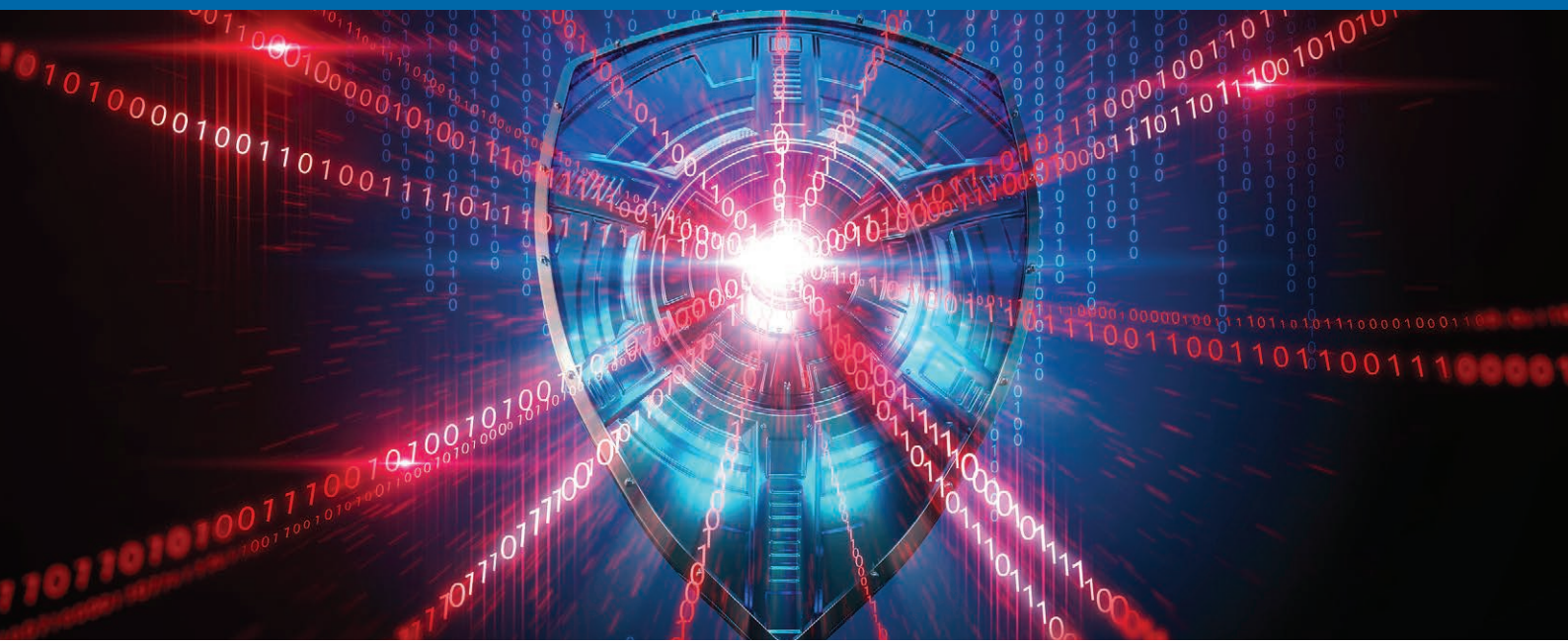
DigiTrace

PENETRATIONSTEST IHRER IT
AUS SICHT EINES INNENTÄTERS




DigiTrace

PENETRATIONSTEST IHRER IT
AUS SICHT EINES INNENTÄTERS

Die Führung eines Unternehmens ist für dessen reibungslosen Ablauf verantwortlich. IT-Systeme spielen dabei eine wichtige Rolle. Im digitalen Zeitalter kann ein Ausfall dieser Systeme zum völligen Stillstand und im schlimmsten Fall sogar zur Insolvenz des Unternehmens führen. Auch drohen langfristige Probleme wie etwa Imageschäden oder der Verlust von Zertifizierungen. Daraus resultieren möglicherweise Kundenverlust sowie Gesetzesverstöße mit kaum vorhersehbaren Folgen. Dabei bestehen IT-Systeme aus komplexen, meist heterogenen und voneinander abhängigen Systemen. Interne sowie externe Einflüsse, sogar kleine Sicherheitslücken oder fehlerhaft konfigurierte Teilkomponenten können verheerende Folgen haben.

Warum bei Penetrationstests Innentäter besonders betrachten?

Ein wichtiger und noch immer oft übersehener Punkt ist der Schutz vor Innentätern. Die äußere Sicherheit kann noch so gut sein, oft lassen sich durch einfache Mittel von innen unbefugt z.B. Daten abgreifen.

Fallbeispiel

Ein kleiner Hersteller von Zylinderlaufbahnbeschichtungen verfügt über eine geheime Technik, welche ihm einen erheblichen Wettbewerbsvorteil ermöglicht. Plötzlich verfügt auch ein Konkurrent im Ausland über dasselbe Beschichtungsverfahren und kann dieses zu einem günstigeren Preis anbieten. Zunächst ist unklar, wie dies passieren konnte. Die Entwicklungsabteilung mit der Geheimrezeptur verfügt über keinen Zugang zum Internet und ist nur lokal vernetzt. Bald stellt sich heraus, dass ein gekündigter Mitarbeiter zu eben diesem Konkurrenten gewechselt ist. IT-Forensiker konnten den Datenabgriff aufklären und letztlich den Mitarbeiter überführen. Dieser legte ein Geständnis ab: Obwohl die Entwicklungsabteilung vom Internet abgeschirmt ist, war es dem abteilungsfremden Mitarbeiter aufgrund fehlerhaft gesetzter Rechte möglich, auf die interne Datenfreigabe der Entwicklungsabteilung zuzugreifen. Trotz außergerichtlicher Einigung bleibt das Unternehmen dennoch auf einem Restschaden sitzen.

Damit Ihnen nichts entgeht und Sie eine gute Einschätzung des aktuellen Standes Ihrer Sicherheitslage haben, bieten wir Ihnen unseren Penetrationstest (kurz: Pentest) aus Sicht eines Innentäters an. Dabei untersuchen unsere Experten Ihre Unternehmenstechnik ausgehend von einem regulären Büro-Netzwerkanschluss. Aus der Perspektive eines internen IT-Systems prüfen wir gründlich, welche Zugriffsmöglichkeiten Ihr Netzwerk und die angeschlossenen Geräte bieten und ob sich eventuelle Sicherheitslücken ausnutzen lassen.

Sie entscheiden, wie im Falle eines Handlungsbedarfs weiter verfahren wird.

Aus unserer langjährigen Tätigkeit in den Bereichen Incident Response, IT-Forensik und als Gutachter für IT-Systeme wissen wir genau, welche Probleme später zu Sicherheitsvorfällen führen. Diese umfassende Erfahrung bringen wir für Sie in unsere Pentests und andere präventive Projekte ein.

Vorteile eines Pentests aus Sicht eines Innentäters

» Bietet einen guten Gesamtüberblick aus interner Sicht auf Ihre IT-Infrastruktur
» Bei kleinen Infrastrukturen vergleichsweise wenig Vorbereitung und Ressourcen notwendig
» Findet schon mit begrenztem Aufwand aus „Tätersicht“ Mängel in der IT-Sicherheit und zugehörigen Prozessen
» Mündet in konkrete Handlungsempfehlungen

Was passiert bei einem Pentest aus Sicht eines Innentäters?

Den Pentest führen unsere erfahrenen IT-Sicherheitsexperten für Sie durch. Dabei testen sie Ihre IT-Systeme auf typische Probleme und Schwachstellen, können aber bei Bedarf auch ins Detail gehen. Dies vermittelt im Ergebnis einen Gesamteindruck über den bei Ihnen vorherrschenden IT-Sicherheitszustand (Reifegrad) aus Sicht eines Innentäters. Wir arbeiten unvoreingenommen und unabhängig. Handlungsempfehlungen zeigen Ihnen leicht verständlich auf, welche Maßnahmen Sie ergreifen müssen oder sollten, um die gefundenen Probleme zu beheben.

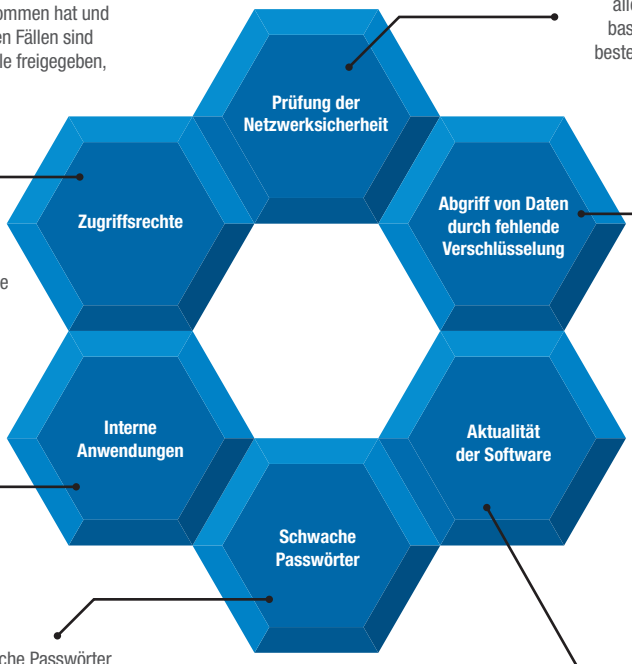
Grundbausteine des Pentests aus Sicht eines Innentäters sind:

Ein nicht restriktiv geführtes Rechtemanagement ermöglicht unberechtigten Personen oft den Zugriff auf sensible Daten (Überberechtigungen). Ebenso lässt sich bei durch mehrere Personen gemeinsam genutzten Benutzerkonten schwer nachvollziehen, wer welche Zugriffe vorgenommen hat und ob diese jeweils berechtigt waren. In seltenen Fällen sind auch sensible Daten fälschlicherweise für alle freigegeben, ohne Zutun des Nutzers.

06

Sind Ihre Netzwerke ausreichend voneinander getrennt? Ist das verwendete WLAN-Netzwerk auch wirklich sicher? Ist Ihr Netzwerk ausreichend gegen unbefugten Zugriff geschützt? Ein Netzwerkscan spürt alle aktiven IT-Systeme im Unternehmen auf. Darauf basierend lässt sich prüfen, ob Zugriffsmöglichkeiten bestehen, welche sich unberechtigt nutzen lassen, z.B. durch Konfigurationsfehler.

01



05

Interne Webanwendungen wie CRM-Systeme (Customer-Relationship-Management), Intranet-Lösungen und anwendungsspezifische Server wie lokale Fibu-Umgebungen beinhalten meist sensitive Daten und sind deshalb ebenfalls in unserem Prüfplan enthalten.

02

Viele Arten von Daten werden in internen Netzwerken ausgetauscht. Ein Beispiel dafür ist VoIP (Voice over IP), eine moderne Möglichkeit des Telefonierens, z. B. über das Internet. Solche Daten lassen sich ggf. „mithören“, wenn diese unverschlüsselt übertragen werden.

04

Verwenden Sie sichere Passwörter? Schwache Passwörter lassen sich durch automatisierte Abfragen schnell ermitteln, Standard-Passwörter schnell ausprobieren. Dies gilt für alle mit Netzwerken verbundene Systeme – etwa auch für Netzwerkdrucker, Router und sonstige Steuerungssysteme.

03

Betriebssysteme, Sicherheitsanwendungen, allgemeine Software und auch Firmware auf Geräten wie einem Router müssen aktuell gehalten werden. Bekannte Sicherheitslücken werden von Tätern automatisiert und systematisch gesucht und ausgenutzt.

IHRE **VARIANTEN**

Wir führen den gesamten Pentest vor Ort durch. Dabei nehmen wir Ihre Technik selbst in Augenschein und können so auch auf Details und nicht so offensichtliche Schwachstellen achten. Unsere Experten können dabei vor Ort selbst überprüfen, wie die IT-Systeme tatsächlich konfiguriert sind.

Üblicherweise werden Pentests umfassend und mit individueller Vorabplanung durchgeführt. Dementsprechend umfangreich fallen regelmäßig die durchzuführenden Arbeiten aus, mit entsprechenden Kosten.

Komplexe IT-Infrastrukturen mit vielen Systemen und vielschichtigen Netzwerken erfordern einen umfassenden Pentest aller Systeme, mit einem individuellen Prüfplan. Diesen stimmen wir vor Beginn mit Ihnen ab. Dabei sind auch Schwerpunktsetzungen und besonders tiefgehende Prüfungen möglich (z. B. intensiver Pentest Ihrer Webanwendungen).

Als kostengünstige Alternative bieten wir Quick-Check-Pentests an. Diese ermöglichen, mit begrenztem Aufwand die typischen Bereiche und Probleme abzudecken. Diese untergliedern sich in zwei Varianten: Die kleine Variante eignet sich beispielsweise für kleinere Arztpraxen oder Bürogemeinschaften. Die mittlere Variante richtet sich an mittelständische Unternehmen aus allen Branchen, welche über mehrere Server und 1-2 Teilnetze verfügen.

ENTSCHEIDUNGSMATRIX

	Quick-Check klein	Quick-Check mittel	Umfassender Pentest
Anzahl der Standorte	1	1-2	Individuell, typischerweise mehrere
Anzahl der Netzwerke	1	1-2 (z. B. LAN und DMZ oder Außenstelle)	Individuell, typischerweise mehrere oder ein besonders großes
Anzahl der IT-Systeme	ca. 5-25 Clients und ca. 1-5 Server	ca. 10-100 Clients und ca. 2-10 Server	Viele und/oder komplexe Systeme
Zeitlicher Aufwand	1 Tag	2 Tage	Individuell
Fixpreis	1.400 €	2.800 €	individuell

Die Preise verstehen sich zuzüglich Umsatzsteuer. Reisekosten und Reisezeit fallen individuell nach Entfernung an.

Gut zu wissen!

Die Experten von DigiTrace führen nicht nur Pentests durch. Zu unserem Leistungsangebot im Bereich IT-Sicherheit gehören auch: Beratungsprojekte und Schulungen, Erstellung von Konzepten zur Informationssicherheit, Incident Response, Aufklärung von IT-Sicherheitsvorfällen und umfassende IT-Sachverständigen-Gutachten. Wir beraten Sie gerne!

KOMBINIERTE **EXPERTISE**

DigiTrace ist ein Spezialanbieter, der Expertise zum Kompetenzbereich IT-Forensik zu Ihrem Nutzen mit IT-Sicherheit und allgemeinen Themen der IT verbindet.

Dank dieser verschiedenen Perspektiven und fachlichen Hintergründe verstehen wir Sachverhalte zu IT-Systemen nicht nur wie IT-Profis und beurteilen diese als IT-Sachverständige – z. B. hinsichtlich ihrer Ordnungsmäßigkeit, Konfiguration oder der Optimierung ihrer Leistung, diagnostizieren Fehlerursachen und begutachten IT-Schäden und -Werte.

Vielmehr bringen wir die besonderen Blickwinkel der Untersuchung von IT-Systemen durch IT-Forensiker und durch IT-Sicherheitsexperten zusammen, die dabei ihre langjährige Erfahrung sowie tiefe Systemkenntnis einbringen.

DigiTrace

DigiTrace GmbH

Zollstockgürtel 59,
50969 Köln

0221-6778695-0

info@digitrace.de

www.digitrace.de