# WAS IST EIN PENETRATION TEST?

Penetration Tests oder kurz Pentest(ing) sind simulierte Angriffe aus externen oder internen Quellen. Penetration Test ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner oder mehrerer Rechner oder Netzwerke jeglicher Größe. Durch diese Angriffe wird die Sicherheit von Webanwendungen, Anwendungen, Netzwerken und Infrastrukturen ermittelt. Mögliche Schwachstellen werden aufgedeckt. Durch methodische und manuelle Validierung der Wirksamkeit von Sicherheitsmechanismen werden mögliche Angriffspunkte in den Systemen erkannt und können so behoben werden.

## Warum sind Penetration Tests unerlässlich?

In einer sich ständig verändernden IT-Landschaft mit stets neuen Bedrohungen und immer besser organisierten Angreifern ist Sicherheit ein zentrales Thema. Immense Image-Schäden, Umsatzeinbußen oder Bußgelder von Datenschutzbehörden rücken immer stärker in das Bewusstsein der Unternehmen. Die Cybersicherheit ist inzwischen eine der wichtigsten Herausforderungen für alle Unternehmen.

## Gründe für einen Penetration Test

1. Aufdecken versteckter Schwachstellen – Ein Penetration Test bietet die Möglichkeit, die Wiederstandsfähigkeit Ihres Systems gegen externe und interne Angriffe zu testen. Er simuliert die Aktionen eines möglichen Eindringlings und versucht vorhandene Schwachstellen auszunutzen. Bei einem Penetration Test werden die Sicherheitsvorkehrungen den gleichen Belastungen ausgesetzt wie bei einem richtigen Angriff.
2. Vertrauen Ihrer Kunde in Ihr Unternehmen – Angriffe gefährden nicht nur die Verfügbarkeit Ihrer Infrastruktur, sie zerstören auch das Vertrauen Ihrer Kunden in Ihr Unternehmen. Dieser Schaden lässt sich nicht immer sofort mit Geld beziffern. Er geht aber, je nach Unternehmensgröße in die Millionen.
3. Einsparung durch reduzierte Ausfallzeiten – Die Ausgabe für Penetration Tests spart am Ende Geld. Penetration Tests zeigen die Punkte mit den größten Schwachstellen auf. Sie erfahren dadurch wo das Budget für IT-Sicherheit am sinnvollsten eingesetzt werden sollte. Ganz zu schweigen von den vorbeugenden Maßnahmen gegen Cybererpressung oder Bußgelder durch den Gesetzgeber. Auch der Prozess der Wiederherstellung nach einem Angriff kann in die Millionen gehen.
4. Einhaltung von Sicherheitsvorschriften – Ein Penetration Test ist eine Möglichkeit um der Nachweispflicht gemäß der DSGVO nachzukommen.
5. Entwicklung der richtigen Sicherheitsmaßnahmen – Ein Penetration Test unterstützt Sie bei der Entwicklung der richtigen Sicherheitsmasnahmen. Dadurch werden Sie in die Lage versetzt die richtigen Investitionen zielgerichtet zu tätigen. Weiterhin ist der Penetration Test in der Regel auch eine Anforderung von Cybersecurityversicherungen.