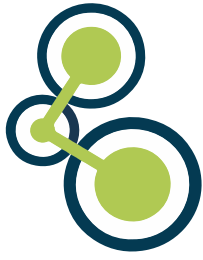


Connecting
Media



PENETRATIONTESTS

MIT KANONEN AUF SPATZEN SCHIESSEN

Ein Penetrationstest ist eine Prüfung Ihrer IT-Umgebung auf Sicherheitslücken und Schwachstellen. Letztendlich ist er nichts anderes als der Versuch, in Ihr IT-System einzubrechen - und zwar mit allen technischen Mitteln aus Sicht eines Angreifers. Er hat - je nach Vorgabe - unterschiedliche Ausprägungen, Schwerpunkte und Prüftiefen. So kann bspw. eine einzelne Applikation innerhalb eines Netzwerkes oder auch das gesamte Netzwerk das Ziel sein.

Gerade für mittelständische Unternehmen ist ein Penetrationstest zu Beginn wie mit Kanonen auf Spatzen zu schießen. Durch unser **Security Audit** erhalten Sie schnell einen objektiven Blick auf den aktuellen Zustand der IT Security in Ihrem Unternehmen. Mittels unserer Pentest Engine werden standardisierte und teilautomatisierte Test in Ihrem Netzwerk von echten Hackern durchgeführt. Gefundene Dokumente und Schwachstellen werden selbstverständlich streng vertraulich behandelt und nach Abschluss des Checks gelöscht.

WAS IHNEN DAS BRINGT?

Sie erhalten ein ehrliches Abbild des tatsächlichen Schutzniveaus Ihrer IT-Infrastruktur. Wir zeigen Ihnen die existierenden Schwachstellen und die daraus resultierenden „Baustellen“ auf - ohne Schönfärbungen, dem Einfluss von Dritten oder irgendwelchen Sicherheitsdokumenten. Neben technischen Informationen zu vorhandenen Schwachstellen und deren Behebung zeigen wir Ihnen außerdem die konkreten Gefahren für Ihr operatives Geschäft auf und liefern strategische Maßnahmenempfehlungen zur nachhaltigen Verbesserung Ihres Sicherheitsniveaus.

LASSEN SIE UNS TESTEN

Vereinbaren Sie ein kostenfreies und unverbindliches Beratungsgespräch unter
www.secaud.it#termin

Das Wichtigste zusammengefasst

- 
- ☒ Überblick über den aktuellen Zustand Ihrer IT-Umgebung und das Schutzniveau - verständlich und nachvollziehbar aufbereitet.
 - ☒ Konkrete Lösungswege, damit Sie die gefundenen Probleme kurzfristig und nachhaltig beheben können.
 - ☒ Geschulte, qualifizierte und zertifizierte Pentester, die sicher im Umgang mit vertraulichen Daten sind.
 - ☒ Kontinuierliche Weiterentwicklung unserer Fähigkeiten und Angriffsszenarien in unserem Labor.
 - ☒ Stetige Zusammenarbeit mit einer breiten IT-Sicherheitscommunity ermöglichen es uns, Ihr Unternehmen auf die neuesten Sicherheitslücken und Schwachstellen zu testen.

9 ENTSCHEIDENDE ASPEKTE

- ☐ Stellen Sie sicher, dass Sie im Vorfeld schon genau wissen was auf Sie zukommt. Denn Planbarkeit und transparente Leistungen sind die Schlüssel zu Ihrem Erfolg.
- ☐ Verschaffen Sie sich einen objektiven Überblick über Ihre IT-Infrastruktur und die verwendete Software aus der Brille eines Hackers.
- ☐ Halten Sie den Aufwand für Ihre Mitarbeiter in der IT so gering wie möglich.
- ☐ Ermöglichen Sie die kurzfristige und schnelle Umsetzbarkeit, mit der Option den Scan jederzeit zu stoppen oder zu beenden.
- ☐ Achten Sie darauf, dass auch unternehmensfremde Geräte beim Check gefunden und überprüft werden. (BYOD, Industrieanlagen, Smart-Home, Klimatisierung u.v.m.)
- ☐ Stellen Sie sicher, dass während des Schwachstellenscans der laufende Betrieb nicht gestört wird.
- ☐ Beachten Sie, dass schwache Passwörter ermittelt, aber nicht veröffentlicht werden.
- ☐ Lassen Sie bekannte Sicherheitslücken (CVEs) nicht nur aufzeigen, sondern auch validieren.
- ☐ Schaffen Sie klar formulierte und umsetzbare Handlungsempfehlungen auf der Managemententscheidungen gebildet werden können, statt nur eine rein technische Auflistung.

IHR KONTAKT

Connecting Media GmbH

Am Hardtwald 7
76275 Ettlingen

Telefon: +49 7243 99167 - 10
vertrieb@connectingmedia.de

www.connectingmedia.de
www.secaud.it

