Welchen Nutzen hat ein Penetrationstest?

Mit der Beauftragung einer Sicherheitsüberprüfung der IT und den dazugehörigen Sicherheitsmaßnahmen ergeben sich für Sie mehrere Vorteile:

- Überprüfen und Sicherstellen der Wirksamkeit bereits eingeführter Sicherheitsmaßnahmen
- Lagebild über das derzeitige Sicherheitsniveau
- Identifikation von aktuell bestehenden Sicherheitslücken
- Grundlage zum Schließen der aktuellen Sicherheitslücken durch gezielte Maßnahmen
- Grundlage für zukunftsorientierte Planungen im Bereich der IT-Sicherheit und IT-Infrastruktur
- Mögliche Kostenreduktion durch die Anpassung der Sicherheitsmaßnahmen auf das tatsächlich benötigte Niveau
- Reduktion der durch die Nutzung von IT entstehenden Risiken und deren mögliche Auswirkungen auf Ihren Geschäftsbetrieb

Weitere Informationen zum Thema finden Sie auf unserer Webseite unter:

www.consectra.de

Sie haben Fragen zum Thema oder wollen sich diesbezüglich beraten lassen? Kontaktieren Sie uns telefonisch unter:

+49.781.203588-00

oder per E-Mail an:

info@consectra.de

Unsere Firmenadresse:

consectra GmbH

Im Unteren Angel 13

77652 Offenburg

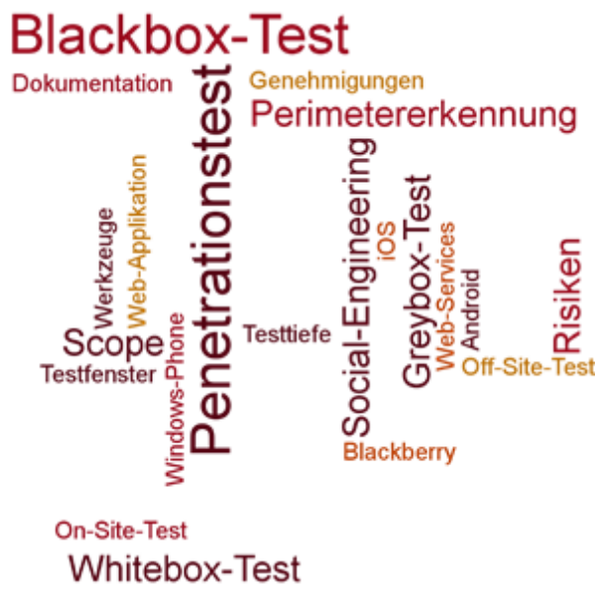
Partner der Bundesrepublik Deutschland
Mitglied der Allianz für Cyber-Sicherheit
Bundesverband IT-Sachverständige & Gutachter
Auditoren für ISO 27001, ISO 20000, FitSM
Traininginstitut ITIL®, FitSM, ISO 27000, IT-Sec, ISIS12

consectra

mIT-Sicherheit ein guter Partner

Penetrationstest

Ihre Sicherheit auf dem Prüfstand



Zielgerichtetes Überprüfen von IT-Sicherheitsmaßnahmen

consectra

mIT-Sicherheit ein guter Partner

Was ist ein Penetrationstest?

Eines der effizientesten und effektivsten Mittel, um vorhandene Sicherheitsmaßnahmen auf ihre korrekte Implementierung und Funktionsweise zu überprüfen. Die daraus resultierenden Ergebnisse liefern eine aktuelle Übersicht der möglichen Angriffspunkte und bieten somit die Möglichkeit, Verbesserungen zielorientiert und effizient durchführen zu können.

Wozu braucht man das?

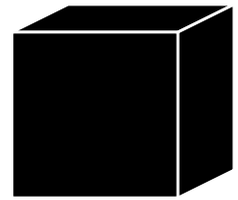
Die Notwendigkeit dieser Tests ergibt sich aus dem Unterschied zwischen theoretischer und praktischer Sicherheit, denn auch die besten und teuersten Sicherheitsmaßnahmen bieten keinen Schutz, wenn sie nicht korrekt implementiert, genutzt und gewartet werden. Daher müssen Sicherheitsmaßnahmen geprüft werden, bevor ein Angreifer eine Schwachstelle ausnutzen kann.

Wer macht sowas?

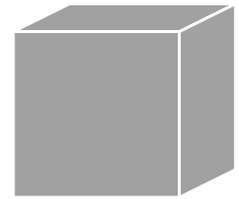
Hacker, also böswillige Angreifer, und Penetrationstester. Während Hacker Sicherheitslücken in Systemen finden wollen, um diese auszunutzen, wollen Penetrationstester diese Lücken finden und schließen. Dabei setzen beide Parteien in weiten Teilen die gleichen Techniken ein. Letztendlich unterscheidet beide Parteien die Absicht und das Ziel ihrer Tätigkeit.

Welche Arten von Penetrationstests gibt es?

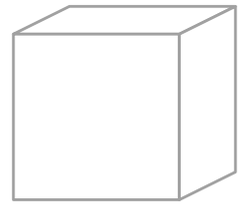
Es werden drei Arten von Penetrationstests unterschieden:



Blackbox-Test
Keine Vorkenntnisse und daher einem realen Hackerangriff am nächsten.



Greybox-Test
Ein Mix aus Black- und Whitebox und dadurch besonders effizient.



Whitebox-Test
Umfangreiche Informationen stehen bereits vor Testbeginn zur Verfügung, was den Aufwand deutlich reduziert.

Was kann getestet werden?

Der Testgegenstand kann individuell abgestimmt werden und die folgenden Bereiche umfassen:

- Perimeter Erkennung
  Welche Schnittstellen (Internetzugänge, eigen- und fremdgehostete Dienste, usw.) sind von außen sichtbar und auch erreichbar?
- Off-Site-Test
  Welche Schwachstellen lassen sich über das Internet in den erreichbaren Systemen finden und ausnutzen?
- On-Site-Test
  Wie weit kommt ein interner Angreifer, wenn er Zugriff auf das LAN/WLAN hat?
- Web Applications & Webservices
  Auch über das Internet oder Intranet erreichbare Anwendungen können Schwachstellen enthalten. Wie kann ein Angreifer diese ausnutzen und wie weit kommt er im System?
- Mobile Devices
  Smartphones (Android, iOS, Windows) sind tragbare Datenspeicher mit teils brisantem Inhalt. Sind sie daher auch ausreichend geschützt?
- Social Engineering
  Die Schwachstelle Mensch. Inwieweit schafft es ein Angreifer, sich auf zwischenmenschlicher Ebene sensible Informationen zu erschleichen?

Weiterführende Informationen finden Sie im Whitepaper Penetrationstest auf unserer Webseite.