splone

Penetrationstest

Leistungsübersicht

3. November 2016

Penetrationstest

"Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight "

- Sun Tzu, The Art of War

- ✓ Jedes zweite Unternehmen war Opfer von Angriffen
- ✓ Nur 20% treffen Sicherheitsvorkehrungen
- ✓ Penetrationstest simuliert Angriffe

Angriffe auf die digitale Infrastruktur von Unternehmen sind keine Seltenheit mehr. Die Bitkom schätzt, dass jedes zweite Unternehmen Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl ist. So wurde festgestellt, dass insbesondere der Mittelstand mit seinem hohen Innovationsgrad ein attraktives Ziel für Hacker ist. Trotz des großen Risikos greifen lediglich 20 Prozent der befragten Unternehmen auf adäquate Sicherheitsmaßnahmen wie Penetrationstests zurück. Mit einem solchen Penetrationstest werden zielgerichtete Angriffe, wie sie von Hacker ausgeführt werden, simuliert. Man spricht in diesem Zusammenhang von einer risikobasierten Sicherheitsüberprüfung.

Unsere Leistung

- ✓ Simulation eines Angriffes
- ✓ Schwachstellen und Risiken aufdecken
- ✓ Schutz verbessern

Ein Penetrationstest ist die Simulation eines Angriffes auf das Zielsystem. Im Gegensatz zu einem tatsächlichen Angriff wird bei einem Penetrationstest kein vorsätzlicher Schaden angerichtet. Wie bei einem realen Angriff auch, wird risikoorientiert versucht, Zugriff auf sensible Daten oder zentrale Systeme zu erhalten, also die Assets zu erreichen. Risikoorientiert bedeutet in diesem Zusammenhang, dass die Angriffsvektoren gründlicher überprüft werden, die den größten Erfolg versprechen. Durch einen Penetrationstest stellen wir das vorhandene Sicherheitsniveau fest, decken Schwachstellen auf, geben Handlungsemp- fehlungen zur Verbesserung der IT-Sicherheit und bewerten diese nach Aufwand und Dringlichkeit. So verbessern Sie den Schutz Ihrer IT-Systeme.

Ihr Nutzen

- ✓ Feststellen Ihres Sicherheitsniveaus
- ✓ Schwachstellen & Einfallstore identifizieren
- ✓ Risiko analysieren
- ✓ Schäden minimieren

Ein Penetrationstest bietet eine Vielzahl von Informationen. So sorgt diese Art der Überprüfung dafür, dass vorhandene Schwachstellen und Einfallstore identifiziert werden. Neben der Bewertung Ihres persönlichen Risikos, lernen Sie Maßnahmen kennen, die Ihnen helfen, den Bedrohungsszenarien zu begegnen. Diese Maßnahmen werden priorisiert, damit Sie auch schnell und kurzfristig reagieren können. Als Konsequenz verhindern Sie beispielsweise den Verlust oder die Manipulation Ihrer Assets. So schützt ein Penetrationstest Ihre (Kunden-)Daten und reduziert die Anzahl sowie das Ausmaß von erfolgreichen Angriffen. Als Nachweis der Überprüfung stellen wir Ihnen gerne ein einseitiges Dokument ohne sensible Informationen aus, mit dem Sie Ihre Kunden und Partner von der Qualität Ihrer Angebote überzeugen können.

Ihre Vorteile mit splone

- ✓ OSCP zertifizierte Experten
- ✓ Priorisierung nach dem CVSS
- ✓ Enge Kommunikation
- ✓ Forschungsnähe

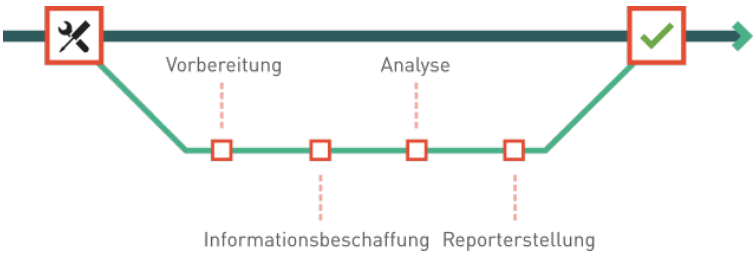
Unsere Penetrationstests werden von OSCP zertifizierten Auditoren begleitet. Wir berücksichtigen Ihre individuellen Anforderungen und passen unsere Leistungen flexibel an Ihre Rahmenbedingungen und Bedürfnisse an. Uns ist es wichtig, dass Sie während einer Überprüfung konstant auf dem aktuellen Stand sind. So pflegen wir eine enge Kommunikation, bei der Sie regelmäßig Fortschrittsberichte über den Testverlauf erhalten. Als Ergebnis erhalten Sie zudem einen Abschlussbericht mit einer gut verständlichen Zusammenfassung. In diesem abschließenden Gutachten sind alle Schwachstellen bewertet. Hierfür orientieren wir uns am Common Vulnerability Scoring System (CVSS). Zu jedem identifizierten Problem schlagen wir Maßnahmen vor, die konkrete Lösungen beschreiben und kurz in ihrem Aufwand abgeschätzt werden. Dank unserer guten Vernetzung mit der Freien Universität Berlin kennen wir den aktuellen Stand der Forschung und sind informiert über die neuesten Erkenntnisse.

Der Ablauf

- ✓ 4 Phasen des Penetrationstest

Ein typischer Penetrationstest besteht aus mehreren Phasen. Die Phasen können von Audit zu Audit einen unterschiedlichen Umfang aufweisen. Folgende Schritte werden durchgeführt:

1. Vorbereitung - In der Vorbereitung zu einem Audit werden wesentliche Kriterien wie beispielsweise Typ und Ziel des Audits besprochen.
2. Informationsbeschaffung - Während der Informationsbeschaffung werden zu einem Ziel relevante Informationen gesammelt. Dazu gehören technische Details genauso wie Daten, die mittels Internetrecherche gesammelt werden.
3. Analyse - Die gesammelten Informationen werden nach sicherheitsbezogenen Problemen analysiert und können über direkte Angriffe verifiziert werden.
4. Reporterstellung - Zum Abschluss eines Audits erhält der Kunde einen Report, der alle Informationen im Detail zusammenfasst. Zusätzlich wird der Report mit dem Kunden besprochen und gegebenenfalls durch eine Präsentation für verschiedene Zielgruppen aufbereitet.



Mögliche Überprüfungsgegenstände

- ✓ Webapplikationen
- ✓ IT-Infrastrukturen
- ✓ Eingebettete Systeme
- ✓ Industrielle Netzwerke
- ✓ Desktop- & Mobile Anwendungen

Penetrationstests lassen sich auf unterschiedlichste Bereiche anwenden. Neben den traditionellen Zielen wie Webapplikationen und der klassische IT-Infrastruktur bieten wir auch Tests für Spezialgebiete an. Dazu gehören Penetrationstests für eingebettete Systeme wie sie beispielsweise im Internet der Dinge eingesetzt werden und Penetrationstests für industrielle Netzwerke mit SCADA-Komponenten. Ein weiteres Ziel von Penetrationstests sind Desktop- und Mobile-Anwendungen.

Umfang

✓ Individueller Umfang

Der Umfang jedes Penetrationstests wird individuell bestimmt. Er ist abhängig vom jeweiligen Untersuchungsobjekt sowie von der Tiefe der Untersuchung. Das für Sie passende Paket erarbeiten wir gemeinsam mit Ihnen. Hierfür benötigen wir Informationen über Ihre Zielsysteme oder Anwendungen. Basierend darauf erstellen wir Ihnen gerne ein individuelles Angebot.

Kontaktieren Sie uns!

Wir haben Ihr Interesse geweckt? Sie haben Fragen zum Ablauf, zu Inhalten oder zum konkreten Umfang? Sie haben andere Wünsche oder spezielle Anforderungen? Dann treten Sie mit uns in Kontakt!

Wir beraten Sie ausführlich in einem persönlichen Gespräch.

splone ist eine unabhängiger Dienstleister im Bereich der IT-Sicherheit. Wir unterstützen unsere Kunden bei der Konzeption, Umsetzung und Überprüfung Ihrer Unternehmensinfrastruktur, Software oder Applikationen. In Form von Audits und Penetrationstest simulieren wir ganzheitliche oder risikoorientierte Angriffe auf Unternehmensnetzwerke. Gemeinsam mit unseren Kunden implementieren wir Prozesse und Managementsysteme der IT-Sicherheit (ISMS) zum Beispiel nach ISO 27001 oder dem BSI Grundschutzkatalog.

splone

splone UG (haftungsbeschränkt)
c/o Freie Universität Berlin
Malteserstr. 74-100
12249 Berlin

Robin Hahn
web: splone.com/de/
mail: robin.hahn@splone.com
tel: +49 30 1205 3264