splone

Penetrationstest

Leistungsübersicht

11. September 2024

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 Handlungsempfehlungen 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 uns

- ✓ Durchgeführt von Profis
- ✓ Priorisierung nach dem CVSS
- ✓ Enge Kommunikation
- ✓ Forschungsnähe

Unsere Penetrationstests werden von Profis durchgeführt. 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.

Welche Farbe darf es sein

- ✓ Bei Blackbox-Tests bekommen die Tester keinerlei Informationen
- ✓ Möglichst viele Informationen bekommen Tester bei Whitebox-Tests
- ✓ Red-Team Tests beschränken sich nicht auf eine Anwendung
- ✓ Mehr Informationen steigern die Qualität

Penetrationstest kommen in verschiedenen Variationen vor. Ausschlaggebend dabei ist, wieviel Informationen einem Tester vorab zur Verfügung gestellt werden. Intuitiv ist eine Sicherheitsüberprüfung dann am Besten, wenn sie möglichst nah an einem realen Szenario gestaltet ist. In Wahrheit kann es aber helfen, von dieser Prämisse abzuweichen. Werden Pentestern Informationen über die interne Funktionsweise wie Programmierschnittstellen (APIs) oder gar Nutzerzugang zur Verfügung gestellt, können diese die Testqualität stark verbessern. Denn anders als traditionelle, böse Angriffe sind simulierte Penetrationstests oft einem Zeitrahmen unterworfen. Ein tatsächlicher Angreifer ist eher dazu bereit, seinen Test über mehrere Tage oder gar Wochen vorzubereiten und zu strecken als es einem Penetrationstester möglich ist. Ebenso werden bei einem realen Angriff gerne Angriffsvektoren miteinbezogen, die bei Penetrationstests eher außen vor gelassen werden.)

Red

Aus dem militärischen Jargon haben die Begriff *Red Team* und *Blue Team* auch im IT-Sicherheitsbereich Eingang gefunden. Dabei sind Red Teams jene, die versuchen auf verschiedenste und kreative Weise Zugang zu Unternehmensinterna zu erlangen. Im Gegensatz zu klassischen Penetrationstests wird das Vorgehen nicht auf einene einzelne Anwendung begrenzt. Stattdessen kommen Social Engineering Kampagnen wie Phishing oder Telefon-Anrufe genauso zum Einsatz wie die technischen Tests. Red Team Tests erlauben eine weite Perspektive auf die Sicherheit eines Unternehmens. Während ein rotes Team oft aus externen Experten besteht, ist das blaue Team eher im Unternehmen verankert. Es versucht, die Angriffe zu erkennen und möglichen Schaden abzuwenden.

Black

Black Box Penetrationtests sind Penetrationstests bei denen vorab nur ein Minimum an Informationen an die Tester gegeben werden. Der Hintergedanke dabei ist, dass der Test so möglichst nah an einen realistischen Test herangeführt wird. In der Realität werden tatsächliche Angriffe sich anders als bei Penetrationstests nicht auf einzelne Anwendungen beschränken.

Gray

Wenn den Testern schrittweise einige Informationen zur Verfügung gestellt werden, spricht man in der Regel von einem *Gray Box* Penetrationstest. Anders als klassische White Box Tests werden hier noch Informationen zurückgehalten.

White

Hat ein Penetrationstester vollen Zugang zu Informationen spricht man von *White Box* Tests. Auch wenn ein tatsächlicher Angreifer nicht die Fülle an Informationen zur Verfügung hat, kann dadurch

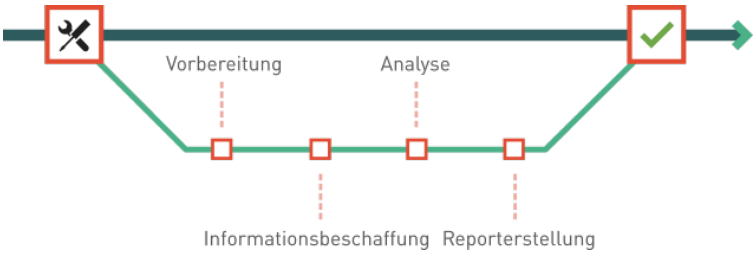
die Testqualität verbessert werden. Anders als klassische Angreifer, sind Penetrationstests einem begrenzten Zeitrahmen ausgesetzt und fokussieren sich auf eine bestimte Anwendung. Durch das Zurverfügungstellen der Informationen wird den Testern die Möglichkeit geschaffen, sich auf die wesentlichen Dinge zu konzentrieren.

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.

Nachbereitung und Schulung

- ✓ Intensive Betreuung
- ✓ Schulungen und Workshops für Mitarbeiter:Innen
- ✓ Nachtests nach Absprache
- ✓ Zusammenarbeit mit Expert:innen und Partner-Unternehmen

Unser Ziel ist es, Sie bis zum sicheren Produkt zu begleiten. Das heißt, dass wir Sie nach einem Penetrationstest oder Audit nicht einfach mit dem Report alleine lassen. Durch Workshops und Schulungen möchten wir Sie und Ihre Mitarbeiter:innen befähigen, Schwachstellen auch in Zukunft schnell zu erkennen und vorzubeugen.

Bei der Konfiguration von Netzwerkgeräten kann vieles schiefgehen. Unsere Expert:innen und Partner-Unternehmen arbeiten eng mit Ihnen zusammen, um Ihren Kolleg:innen beim Beheben der Schwachstellen zu helfen. Hierfür arbeiten wir eng mit spezialisierten Unternehmen zusammen, die auf Ihrem Gebiet Experten sind.

Sollte es Bedarf geben, testen wir gerne nach und verifizieren die umgesetzten Lösungen.

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 ein unabhängiger Dienstleister im Bereich der IT-Sicherheit. Als Teil der Assecor-Familie unterstützen wir unsere Kunden bei der Konzeption, Umsetzung und Überprüfung der Unternehmensinfrastruktur, Software oder Anwendungen. In Form von Audits, Red Team Tests oder Penetrationstests simulieren wir ganzheitliche oder risikoorientierte Angriffe. Gemeinsam mit unseren Kunden implementieren wir Prozesse und Managementsysteme für Informationssicherheit (ISMS) zum Beispiel nach ISO 27001 oder dem BSI IT-Grundschutz.

splone

splone UG (haftungsbeschränkt)
Storkower Str. 207
10369 Berlin

web: https://splone.de
mail: mail@splone.com