



Penetrationstest eines Internet-Portals

„In jedem Fall ist zu beachten, dass sich durch Einbruchsversuche nur Unsicherheit zeigen lässt, keine Sicherheit. Wenn der Versuch misslingt, kann das System trotzdem unsicher sein. Daher ist bei Penetrationstests immer Vorsicht angebracht.“

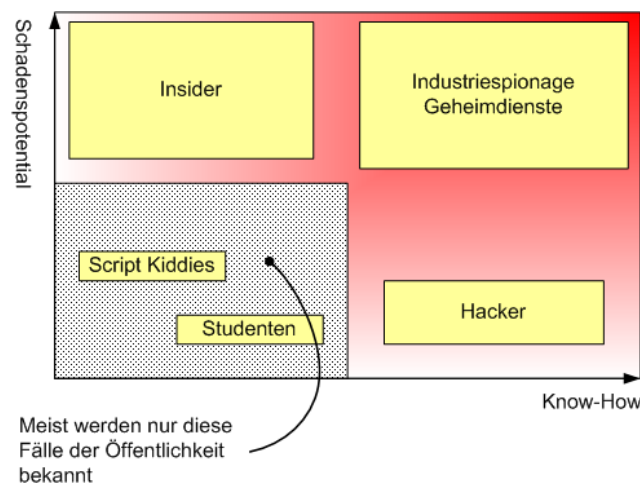
Chaos Computer Club, Berlin

Das Testen von Programmen ist sehr nützlich, um die Anwesenheit von Fehlern zu zeigen, nie aber die Abwesenheit.

Edsger W. Dijkstra

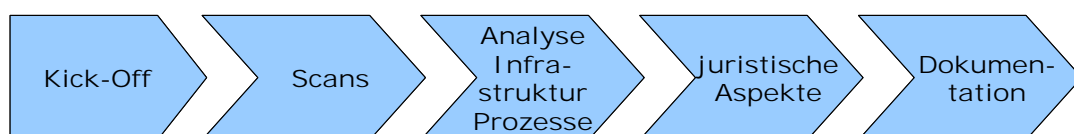
Mittels Penetrationstests können IT-Systeme, Anwendungen und Prozesse auf Angriffsmöglichkeiten durch diverse Täterkreise oder auch gegen (ungewollte) Fehler normaler Benutzer beim Gebrauch überprüft werden.

Die folgende Abbildung zeigt eine Klassifikation von Täterkreisen nach Schadenspotential und Know-how.



Da Penetrationstests zum einen schon aus rechtlichen Gründen eine äußerst sensible Angelegenheit sind und zum anderen immer nur eine stichprobenartige und zeitliche begrenzte Möglichkeit zur Feststellung des erreichten Sicherheitsniveaus des Untersuchungsgegenstandes bieten, sollte bei der Durchführung besonders streng auf Nachvollziehbarkeit und Vergleichbarkeit der Ergebnisse geachtet werden. Es empfiehlt sich deshalb die Orientierung der Vorgehensweisen an anerkannten Standards.

Das Projekt wird in 3 Phasen, optional 5 Phasen gegliedert, welche im Folgenden detailliert beschrieben werden.





Phase 1: Kick-Off und Vorbereitung

Im Vorfeld des eigentlichen Penetrationstest wird im Rahmen eines Kick-Offs vor Ort die Vorgehensweise im Projekt mit dem Kunden abgestimmt:

- Bestimmung der Verantwortlichkeiten auf Seiten des Kunden und der eSolve
- genaue Definition der Penetrationsziele
- genaue Definition der Penetrationsquelle (IP-Adressbereich) (Dies ist vor allem wichtig, falls der Kunde ein Intrusion Detection System (IDS) betreibt)
- Definition der Angriffsmethoden, insbesondere der Ausschluss bestimmter Angriffsmethoden und Informationsquellen (z.B. Denial of Service, Einsatz von Scannern und Tools, intrusive, non-intrusive)
- Festlegung der Zeiten für die Durchführung der Penetrationstests, da bei diesen Versuchen die Funktionalität des penetrierten Systems beeinträchtigt werden kann
- Einholen aller nötigen Informationen im Rahmen des Whitebox Penetrationstest über den Aufbau der Internet Portal Infrastruktur und Applikationsstruktur

Dazu gehören u.a.:

- § eine Liste der installierten Software (inkl. Version),
- § eine Aufstellung der angebotenen Dienste,
- § einen vollständigen Netzwerkplan,
- § alle vorhandenen Betriebs- und Installationshandbücher

Vorarbeit zu einem erfolgreichen Penetrationstest ist die Bewertung der Informationen und Daten bzgl. ihrer Gefährlichkeit.

Phase 2: Scans

Im Rahmen dieser Phase des Projektes wird durch Scans, d.h. durch den Einsatz von kommerziellen und frei verfügbaren Standard-Tools (z.B. ScanDo, ApplicationDetective, nmap, Nessus, ISS, ...) untersucht, ob die Netzwerkarchitektur und die eingesetzten Soft- und Hardware Komponenten mit den zuvor erhaltenen Informationen übereinstimmen. Die gesammelten Informationen lassen sich mit der erhaltenen Skizze der Netzwerkarchitektur und Applikationsarchitektur vergleichen. Ebenso wird die Liste der Systeme mit installierter Software überprüft.

Die Scans können des Weiteren auch schon erste Sicherheitslücken aufdecken.

Anhand der Liste der Systeme und der installierten Software wird systematisch untersucht, ob zu diesen Produkten Sicherheitslücken bekannt sind und ob diese Sicherheitslücken in der spezifischen Konfiguration ausgenutzt werden. Weiter wird untersucht, ob für die Sicherheitslücke bereits Exploits existieren. Dazu werden sämtliche öffentlich zugängliche Quellen der Informationsbeschaffung genutzt und verwendet.

Die gefundenen Angriffsmöglichkeiten werden nach Erfolgsaussichten für die folgenden Schritte des Penetrationstest priorisiert.

Auf der Basis der Erkenntnisse dieser "Standardscans" werden nun gezielte Angriffe auf den zu untersuchenden Webserver und die URL durchgeführt. Dies geschieht unter Hinzuziehung geeigneter kommerzieller Werkzeuge und selbstgeschriebener Skripte.



Insbesondere werden in Absprache mit dem Kunden Schwachstellen untersucht wie z.B.:

- Prüfung der Infrastruktur (Webserver) des Kunden
- Einschleusen eines Trojaners über das Web
- Prüfung spezieller Portale
- Prüfung der Systeme auf dem Kommunikationspfad zum Webserver, wie Firewall, Loadbalancer und Router

Nach Absprache können gezielte Denial of Service Attacks durchgeführt werden, die im Besonderen festgelegt werden müssen. Zeitpunkt und Stärke dieser DoS Attacks müssen im Einzelnen abgesprochen werden.

Falls Registrierungen an den Anwendungen für die Penetrationen notwendig sind, teilt eSolve dies dem Kunden mit. Der Kunde stellt dann einen entsprechenden Zugang zur Verfügung.

Der Penetrationstest wird mit z.T. selbstentwickelten Werkzeugen durchgeführt. Die Überlassung dieser Werkzeuge gehört nicht zu den Leistungen der eSolve, dem Kunden werden hieran keinerlei Nutzungsrechte eingeräumt. Die Überlassung einer CD-ROM mit der Sammlung aller verwendeten, frei verfügbaren Standardtools ist möglich.

Phase 3a: Untersuchung der Infrastruktur (optional)

Um eine vollständige Untersuchung des Internetportals durchzuführen, wird zusätzlich ein Penetrationstest von Innen angeboten. Dabei werden Scans innerhalb der Internet Portal DMZ durchgeführt, wodurch weitere Schwachstellen gefunden werden können, die durch die Firewall verdeckt bleiben. Bei einem Penetrationstest innerhalb der DMZ, wodurch mehrere Systeme gescannt werden, kann festgestellt werden, welche Möglichkeiten ein Hacker hat, wenn er die erste Hürde überwunden hat und freien Zugriff auf den Webserver hat.

Phase 3b: Untersuchung der Prozesse (optional)

Neben den Penetrationstests ist es sinnvoll alle Prozesse, die das Internetportal betreffen, zu untersuchen. Für das Management des Internetportals ist entscheidend

- ob ein Logging vorhanden ist und ob es ausgewertet wird,
- ob und wie Internetseiten einer Qualitätssicherung unterliegen und freigegeben werden,
- wie die Rechteverwaltung geregelt ist,
- ob Notfallpläne vorhanden sind,
- wie Eskalationsprozesse gelebt werden,
- ...

Phase 4: Hilfestellung bei juristischen Aspekten (optional)

Zusätzlich wird eine Analyse der Kunden Webseiten unter datenschutzrechtlichen und nutzungsrechtlichen Aspekten durch den Juristen des eSolve-Partners secaron angeboten. Die Webseite wird auf datenschutz- und nutzungsrechtlichen Auffälligkeiten hin untersucht, wobei Vorlagen zur Diskussion mit der Rechtsabteilung des Kunden erstellt



werden. Es handelt sich bei unserer Unterstützung nicht um eine Rechtsberatung, sondern lediglich um eine Hilfestellung zur Identifikation von vorhandenen Schwachstellen, die insbesondere angesichts der aktuellen Abmahnungswellen juristisch bedenklich sein könnten.

Die Analyse beinhaltet insbesondere folgende Punkte:

- Anbieterkennzeichnung / Impressum nach TDG
- Zweckbestimmung personenbezogener Daten
- Unterrichtung des Nutzers über die Verarbeitung personenbezogener Daten nach TDDSG (Datenschutzerklärung)
- Datenschutzrechtliche Einwilligungserklärung
- Datenschutzrechtliche Aspekte im Zusammenhang mit dem Vertriebszugang
- Datenschutzrechtliche Aspekte im Zusammenhang mit dem Kundenzugang

Phase 5: Dokumentation und Abstimmung der Ergebnisse

Die gewonnenen Informationen und Ergebnisse des Penetrationstests werden in einem Dokument beschrieben. Im Einzelnen enthält der Bericht folgende Abschnitte:

- Management Summary
- eingesetzte Methoden und ermittelte Informationen
- die ermittelte Netz- und Webserverstruktur des Kunden
- die durchgeführten Angriffe und deren Ergebnisse
- die ermittelten Schwachstellen und die damit verbundenen Risiken

Die aufgedeckten Sicherheitsprobleme werden in Risikoklassen (niedrig, mittel, hoch) eingeteilt. Für jedes Sicherheitsproblem wird, soweit möglich, eine Gegenmaßnahme aufgezeigt. Die Einteilung orientiert sich an den Prinzipien der Common Criteria, speziell den „Evaluation Techniques“, welche ein Teil der „Common Evaluation Methodology (CEM-99/045 Version 1.0 Annex B)“ sind.

Auf Wunsch können die Ergebnisse des Projektes in einer abschließenden Präsentation vor Ort zusammengefasst werden und vor dem Management und dem IT Sicherheitsteam des Kunden diskutiert werden.

ungefähre Aufwände für einen Penetrationstest

| Aktivitäten | Aufwände in Arbeitertagen (MT) |
|-------------------------------------------------------------|----------------------------------------------------------|
| Phase 1: Kick-Off und Vorbereitung | ca. 2 MT |
| Phase 2: Scans | ca. 3 - 10 MT je nach Funktionalität des Internets |
| Phase 3a: Untersuchung der Infrastruktur (optional) | ca. 3 - 5 MT |
| Phase 3b: Untersuchung der Prozesse (optional) | ca. 3 - 5 MT |
| Phase 4: Hilfestellung bei juristischen Aspekten (optional) | ca. 2 MT |
| Phase 5: Dokumentation und Abstimmung | ca. 2- 4 MT |