Penetration Tests auf Netzwerk- und Systemebene

Penetrations-Tests werden je nach Ziel der Tests auf Netzwerk- und Systemebene oder auf Applikationsebene durchgeführt. Auf Netzwerk- und Systemebene stehen die IT-Systeme, wie z.B. Betriebssysteme, Middleware, Datenbanken, im Fokus der Tests. Bei den Tests auf Applikationsebene sind Webanwendungen, Webshops, Portal o. ä. die Zielobjekte.

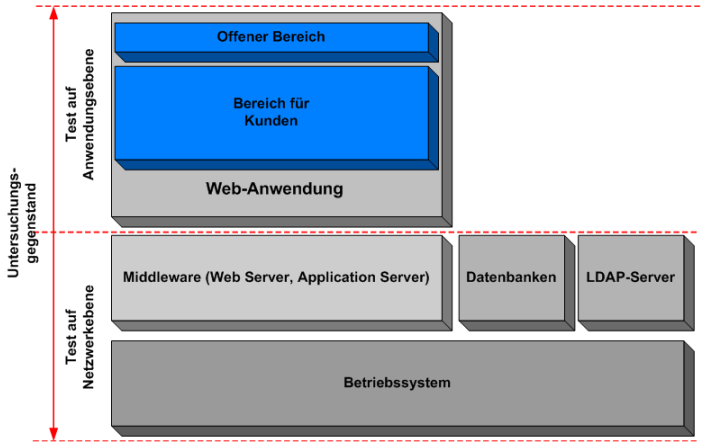

Abbildung 1: Exemplarische Abgrenzung der Angriffsziele (Netzwerk-/Systemebene bzw. Applikationsebene)

Mittels Penetrationstests auf Netzwerk- und Systemebene untersucht die Accuris AG die vom Auftraggeber benannten Zielsysteme aus dem Internet oder lokalen Netz hinsichtlich möglicher technischer Schwachstellen. Voraussetzung für die Durchführung der Tests ist, dass die Systeme auf IP-Ebene erreichbar sind.

Exemplarisch für solche Tests sind:

- die Ermittlung und der Versuch der Ausnutzung von Implementierungsschwächen des im Zielsystem eingesetzten Betriebssystems,
- die Ermittlung und der Versuch der Ausnutzung fehlerhafter Konfigurationen des Zielsystems (z.B. Zugriff auf beliebige Dateien auf einem IIS-Server),
- die Untersuchung auf unerwünscht zulässige Dienste (z.B. durch fehlerhafte Konfiguration oder unzureichende Filterregeln) und
- der Versuch, eingesetzte Dienste (nach Absprache mit dem Kunden) durch Denial-of-Service-Attacken außer Kraft zu setzen.

Ein Ziel eines Penetration Tests ist es, Schwachstellen in IT-Systemen oder Software (z.B. durch fehlende Patches) oder deren Konfiguration zu identifizieren, die von einem Hacker potenziell ausgenutzt werden können, um Zugriff auf die Systeme zu erhalten, sensible Informationen zu kompromittieren oder die Verfügbarkeit von Systemen oder Anwendungen einzuschränken.

Anders als ein von einem böswilligen Hacker durchgeführter Angriff, hat der durch die Accuris AG durchgeführte Penetration Test nicht die Ausnutzung von Schwachstellen, sondern deren Identifikation und Verifikation zum Ziel. Dadurch werden auch solche Schwachstellen erkannt, die sich derzeit noch nicht ausnutzen lassen.

Ein Penetration Test stellt daher eine wesentlich effizientere und kostengünstigere Form der Sicherheitsanalyse dar, als etwa ein vollständiges Systemaudit.

Die accuris AG folgt bei der Durchführung eines Penetration Tests dem folgenden Vorgehensmodell:

1. Informationsbeschaffung: Auswertung von öffentlich zugänglichen Informationen über die Zielsysteme (z.B. aus DNS- und WHOIS-Datenbanken und Google-Hacking-Techniken) sowie durch Mitschneiden des Netzwerkverkehrs (Sniffing).
2. Portscans: Identifikation von offenen TCP- und UDP-Ports.
3. Enumeration: Identifikation von Betriebssystem- und Softwareversionen mittels Banner-Grabbing und Software-Fingerprints.
4. Schwachstellenidentifikation und -verifikation: Die identifizierten Netzwerkdienste und Betriebssystemversionen werden hinsichtlich bekannter Schwachstellen überprüft. Dies beinhaltet die Verwendung von automatisierten Schwachstellenscannern (kommerziellen und Open Source). Mittels manueller Überprüfungen werden die Ergebnisse der eingesetzten Scanner verifiziert (z.B. um „False Positives“ zu eliminieren) und ggf. das Vorhandensein zusätzlicher Schwachstellen überprüft.
5. Denial-of-Service-Angriffe werden explizit NICHT durchgeführt, außer der Auftraggeber wünscht dies.

Auch ohne die explizite Durchführung von Denial-of-Service-Angriffen kann ein Penetration Test zum Verlust der Verfügbarkeit von Systemen führen, z.B. durch einen Systemabsturz der einen manuellen Neustart des betroffenen Systems durch einen lokalen Administrator erforderlich macht.
Auch Datenverlust kann eine unbeabsichtigte Folge eines Penetrationstests darstellen. Je nach der Beschaffenheit der Zielumgebung können diese Gefahren ein nicht zu akzeptierendes Risiko (z.B. bei Produktionssystemen) für den Kunden darstellen. Die Accuris AG kann daher in Absprache mit dem Kunden, bestimmte Systeme von riskanten Tests ausnehmen, oder ganz auf diese Art von Tests verzichten.

Auch wenn riskante Tests explizit von der Testdurchführung ausgenommen werden, kann ein Restrisiko für die untersuchten Systeme und Daten nicht vollständig ausgeschlossen werden. Aus diesem Grund werden Penetrationstests vorab sehr gründlich mit den Kunden geplant und während der Durchführung laufend mit einem technischen Ansprechpartner beim Kunden koordiniert.

Der Verzicht auf bestimmte Tests mindert jedoch auch immer die Aussagekraft eines Penetration Tests, da kritische Schwachstellen dadurch möglicherweise übersehen werden. Um das Schadenspotenzial zu minimieren, kann die Testdurchführung auch außerhalb der normalen Geschäftszeiten erfolgen um den möglichen Schaden für Produktivsysteme im Falle eines Ausfalls zu verringern.

Durchführungsoptionen für den PEN-Tests

White Box oder Black Box

Penetration Tests können sowohl in Form von „Black-Box“ als auch „White-Box“ Tests durchgeführt werden. Im Falle des Black-Box-Tests gibt der Kunde lediglich die notwendigsten Informationen (z.B. nur einen IP-Adressbereich) an die accuris AG. Die accuris AG versucht die fehlenden Informationen mittels passiver Informationsbeschaffung, Portscans etc. aufzubauen. Diese Art von Tests wird angewandt, um die Möglichkeiten eines externen Angreifers möglichst realistisch nachzustellen. Auch die Überprüfung der Funktionsweise von beim Kunden installierter IDS/IPS-Systeme sowie das Reaktionsverhalten und -Geschwindigkeit der eigenen Mitarbeiter kann ein Teilziel eines Black-Box-Tests darstellen. Die accuris AG kann hierzu Techniken einsetzen um IDS/IPS-Systeme zu täuschen.

Bei der zweiten Variante, dem „White-Box“ Verfahren, stellt der Kunde der accuris AG ausführliche Informationen über die zu testenden Systeme sowie Netzwerkinfrastruktur zur

Verfügung. Die Accuris AG kann dadurch in der begrenzten Zeit, wesentlich effizienter arbeiten und dadurch Schwachstellen identifizieren, die möglicherweise durch einen Black-Box-Test nicht erkannt werden würden. Zusätzlich muss davon ausgegangen werden, dass potenziellen Angreifern beliebige Zeit für die Durchführung eines Angriffs zur Verfügung steht und Social Engineering Methoden zur Informationsbeschaffung einsetzen. Dieser Vorteil, gegenüber dem in einem begrenzten Zeitrahmen durchgeführten Penetration Test der accuris AG, kann durch das White-Box-Verfahren ausgeglichen werden.

On-Site oder Off-Site

Penetration Tests können grundsätzlich über das Internet oder aus dem internen Netz beim Kunden durchgeführt werden. Der erste Fall wird als Off-Site-, der zweite als On-Site-Penetrationstest bezeichnet.

Off-Site Penetration Tests haben den Vorteil, dass sie sehr kostengünstig sind und dem Angriffsvektor eines potenziellen Angreifers aus dem Internet entsprechen. Auf der anderen Seite ist die Aussage solcher Tests nur sehr eingeschränkt. Ein verwundbarer Dienst etwa, der während des Tests von einer vorgelagerten Firewall geblockt wurde, kann durch einen Off-Site-Test nicht identifiziert werden.
Zudem ermöglicht die Durchführung On-Site, etwa aus der DMZ des Kunden, das Szenario zu simulieren, indem ein Angreifer bereits ein System des Kunden (z.B. einen Webserver) übernommen hat. Im Falle einer solchen mehrstufig aufgebauten Sicherheit, mit einer Firewall zwischen Internet und DMZ sowie zwischen DMZ und Office, lässt sich die Sicherheit wesentlich umfassender prüfen. Eine hiernach verifizierte Defense-In-Depth-Sicherheit, bietet auch bei der Kompromittierung eines Systems aus der Sicherheitskette noch ausreichenden Schutz zur Abwehr eines Angreifers. Schließlich lassen sich über On-Site-Tests auch die Möglichkeit von Innentätern oder Insidern prüfen.
Den wirkungsvollsten und umfassendsten Ansatz bietet schließlich die Kombination aus Off-Site und On-Site-Tests, mit dem sich verschiedene Bedrohungsszenarien abdecken lassen.

Die Durchführung des PEN-Tests wird wie folgt angeboten:

- Grey Box Penetration Test auf Netzwerk-/Systemebene,
- Manuelle Penetration einzelner, erkannter Dienste und Prüfung von Authentisierungs- und Autorisierungsmechanismen
- Die Durchführung des PEN-Tests ist MANUELL durch einen ZERTIFIZIERTEN Penetration Tester/Ethical Hacker (CEH, CE Council, BSI) MANUELL vorzunehmen. Kommerzielle (automatische) Scanner dürfen unterstützend zum Einsatz kommen.

Die accuris AG weist darauf hin, dass die Durchführung von Penetrationstests die Verfügbarkeit und Integrität der Zielsysteme beeinträchtigen kann. Es ist möglich, dass der ordnungsgemäße Betrieb nur durch manuellen Zugriff auf das Zielsystem wiederhergestellt werden kann.
Für Schäden, die bei der Durchführung von Angriffen im Rahmen von Penetrationstests entstehen, die zuvor vom Auftraggeber genehmigt wurden, übernimmt die accuris AG keinerlei Haftung, insoweit solche Schäden nicht auf grobe Fahrlässigkeit oder Vorsatz zurückzuführen sind und der Haftungsausschluss gesetzlich zulässig ist.

Ergebnisbericht des PEN-Tests

Nach Abschluss des Penetration Tests wird ein detaillierter Bericht geliefert, welcher folgende Informationen beinhaltet:

- Beschreibung der angewandten Verfahren

- Darstellung der konkreten Vorgehensweisen
- Darstellung der Ergebnisse (Schwachstellen, Sicherheitslücken)
- Wertung der Ergebnisse (Darstellung der Risiken und Risikoeinschätzung)
- Richtlinien und Empfehlungen zur Abstellung der Schwachstellen und Angriffspunkte (Handlungsempfehlungen) gemäß der Risikoeinschätzung nach Prioritäten
- auf Wunsch alle während des Penetrationstestes angefallenen Scannerprotokolle in dem jeweils vom Tool erzeugten Dateiformat