SECURITY AUDITING

Sicherheit durch Transparenz

INTENSIV-CHECK SCHAFFT SICHERHEIT

In Zeiten wachsender Cyber-Kriminalität ist es unverzichtbar, das Sicherheitsniveau der eigenen Infrastruktur realistisch einzuschätzen. Mit welchem Aufwand können Angreifer zum Beispiel über ein Webportal in die Backend-Systeme eindringen? Wie gut sind Kunden- und Geschäftsdaten geschützt? Um diese Fragen zu beantworten, müssen Systeme heute regelmäßig und sachgerecht überprüft werden. Bei einem Sicherheitstest führen Experten eine Bestandsaufnahme durch und durchleuchten systematisch den aktuellen Sicherheitsstand eines IT-Systems.

SICHERHEITSSTANDARDS ERFÜLLEN

Für ein Risikomanagement, das ein realistisches Bild der System- und Anwendungssicherheit zeichnen will, sind Sicherheitstests unverzichtbar. Auch öffentliche Standards und Normen schreiben regelmäßige Prüfungen und die Dokumentation von Schwachstellen vor.

T · · Systems ·

CYBER-ANGRIFF IM KUNDENAUFTRAG

Wer wissen will, wie stabil und sicher seine Systeme sind, muss letztlich die Methoden der Angreifer anwenden. Deshalb führt T-Systems mit sogenannten Penetrationtests „Cyber-Attacken im Kundenauftrag“ durch. Indem sich Sicherheitsexperten in die Rolle von Angreifern versetzen und deren Denkweisen und Methoden übernehmen, können sie technische Schwachstellen am zuverlässigsten identifizieren, überprüfen und gezielte Gegenmaßnahmen ableiten.

NEUTRALER BLICK VON EXTERN

T-Systems verfügt als ICT-Dienstleister über die Expertise und die notwendige Unabhängigkeit, um den Sicherheitszustand der Systeme und Anwendungen kritisch zu analysieren. Haben Unternehmen bereits Tests und Prüfungen durchgeführt, baut T-Systems auf diesen Ergebnissen auf. Es wird großer Wert darauf gelegt, dass die Durchführung der Penetrationtests effizient und in klarer Abstimmung mit den Betriebsprozessen des Kunden erfolgt.

MANUELLE UND SEMIAUTOMATISCHE PRÜFUNG

Bei den Tests wenden die Experten eine Kombination aus automatisierten Werkzeugen und manuellen Tests an, um ein Optimum an Effizienz und Aussagekraft zu erzielen. Dabei orientiert sich T-Systems an aktuellen Best Practices für Penetrationtests. Für Webanwendungen sind dies zum Beispiel OWASP (Open Web Application Security Project) und für Systeme und Netze OSSTMM (Open Source Security Testing Methodology Manual). Kunden profitieren automatisch vom aktuellen Stand der Technik und von Innovationen auf diesem Gebiet.

EXPERTEN FÜR ALLE TECHNISCHEN DETAILS

Je nach Testszenario, Systemumgebung oder Art der technischen Schnittstellen sind bei Penetrationtests unterschiedliche Fähigkeiten und Erfahrungen gefragt. T-Systems verfügt über Experten für diverse Spezialfälle. Zum Beispiel unterschiedliche Testarten: Während Black-Box-Tests ausschließlich öffentlich verfügbare Informationen als Ausgangspunkt nehmen, greifen White-Box-Tests auch auf Systeminterna wie Netzpläne zurück. Darüber hinaus unterscheiden Penetrationtester zwischen netz- und anwendungsbasierten Checks. Im ersten Fall sucht der Tester nach Systemen im vereinbarten Netz. Er stellt fest, welche Betriebssysteme und Serversoftware zum Einsatz kommen und dokumentiert, wo es Schwachstellen gibt. Im zweiten Fall ist das Ziel, etwa in einer webbasierten Anwendung Fehler zu identifizieren, die zu einer Gefährdung von Vertraulichkeit, Integrität oder Verfügbarkeit führen können. Dies beginnt bei Angriffstechniken wie Cross Site Scripting, SQL-Injection oder Privilege-Escalation und umfasst ebenso Prüfung der realisierten Anwendungslogik. In speziellen Bereichen wie Cloud Computing, Mobile Communications und Unified Communication & Collaboration verfügen die Experten von T-Systems über besondere Kompetenzen.

KLASSIFIKATION

Anhand welcher Kriterien kann man einen Penetrationstest beschreiben, bzw. was unterscheidet einen Penetrationstest von einem anderen Penetrationstest? Die Unterscheidungsmerkmale wie Umfang der geprüften Systeme, die Vorsicht bzw. Aggressivität beim Testen etc., die einen bestimmten Penetrationstest charakterisieren, müssen an die Zielsetzung des Tests angepasst werden, um eine effektive und effiziente Durchführung mit kalkuliertem Risiko sicherzustellen. In Abbildung 1 (siehe Grafik auf der folgenden Seite) ist eine Klassifikation von möglichen Penetrationstests dargestellt. Auf der linken Seite sind sechs Kriterien aufgelistet, nach denen man Penetrationstests unterscheiden kann und auf der rechten Seite sind die unterschiedlichen Werte für die Kriterien in einem kompakten Baumdiagramm zusammengefasst.

Je nach Zielsetzung des Auftraggebers muss ein geeigneter Penetrationstest anhand der genannten Kriterien vereinbart werden. Dabei ist zu beachten, dass nicht alle möglichen Kombinationen sinnvolle Tests darstellen, obwohl bei der Klassifikation großer Wert auf die klare Trennung der Kriterien gelegt wurde. Ein aggressiver Test wird meistens sehr schnell erkannt und ist daher nicht optimal mit einer verdeckten Vorgehensweise kombinierbar. Analog ist ein offensichtlicher Penetrationstest nicht geeignet, um mittels Social-Engineering-Techniken z. B. vertrauliche Informationen von den vorgewarnten Mitarbeitern zu erlangen.

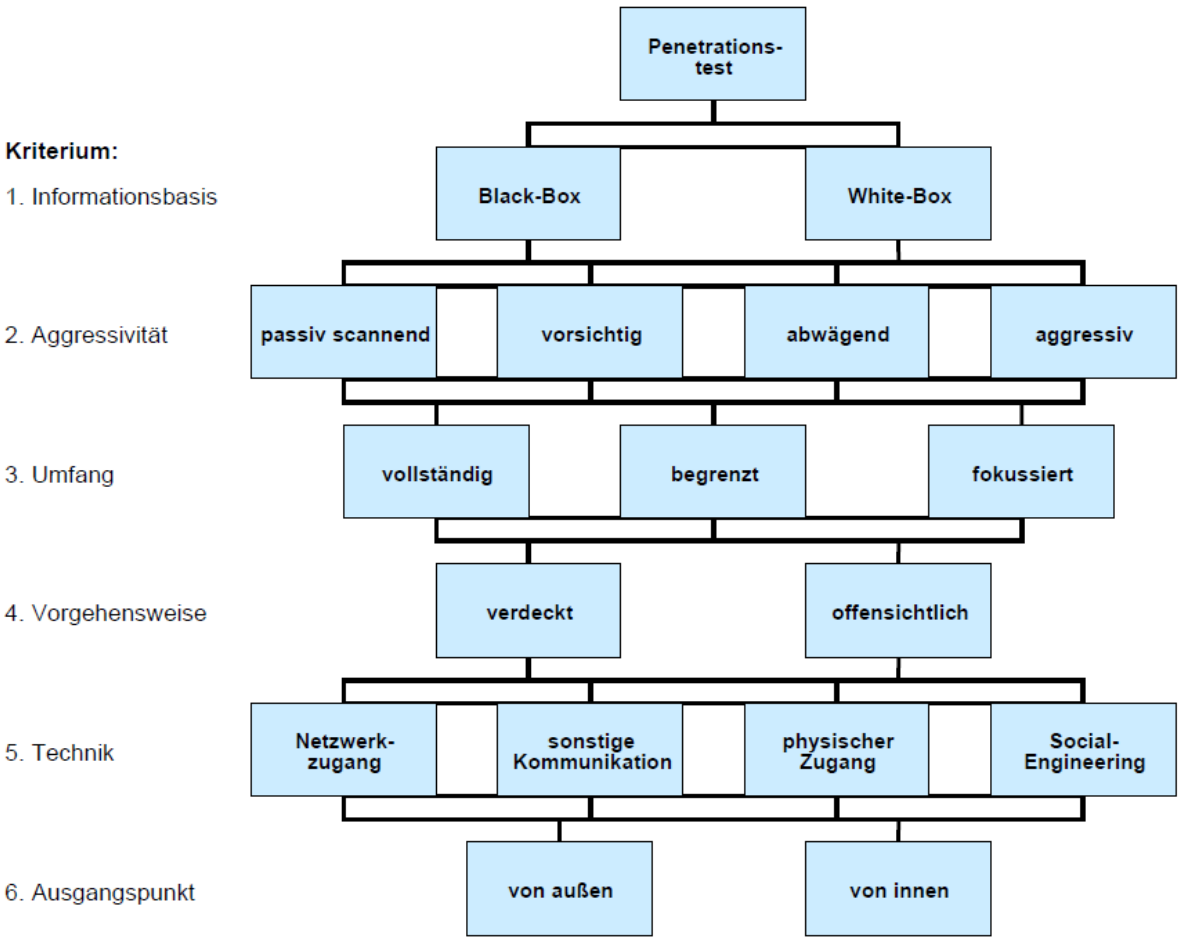
Im Folgenden werden die sechs Kriterien und die möglichen Werte erläutert:

1. INFORMATIONSBASIS:

Von welchem Wissensstand über das anzugreifende Netz bzw. Objekt geht der Penetrationstester aus? Hier unterscheidet man grundlegend zwischen sog. Black-Box-Testing ohne jegliches Insiderwissen und dem White-Box-Testing mit Insiderwissen:

- Ein **Black-Box-Test** „simuliert“ realistisch einen Angriff eines typischen Internet-Hackers. Der Hacker muss die benötigten Informationen in öffentlich zugänglichen Datenbanken recherchieren oder von außen als Unternehmensfremder erfragen.

- Bei einem **White-Box-Test** wird ein Angriff eines (Ex-) Mitarbeiters oder eines externen Dienstleisters mit bestimmten Detailkenntnissen simuliert. Der Umfang der Kenntnisse kann dabei von nur geringen Kenntnissen, wie sie z. B. ein Mitarbeiter besitzt, der nur kurze Zeit im Unternehmen beschäftigt war, bis hin zu tief gehenden Systemkenntnissen, wie sie z. B. ein externer IT-Dienstleister durch die Installation von sicherheitsrelevanten Systemen erlangt.



2. AGGRESSIVITÄT:

Wie aggressiv geht der Penetrationstester beim Testen vor? Um eine hinreichend feine Unterscheidung zu ermöglichen, werden in dieser Studie **vier Aggressivitätsstufen** unterschieden:

- Bei der niedrigsten Aggressivitätsstufe werden die Testobjekte nur passiv untersucht, d. h. gefundene mögliche Schwachstellen werden nicht ausgenutzt.
- In der zweiten Aggressivitätsstufe – vorsichtig – werden gefundene Schwachstellen nur dann ausgenutzt, wenn nach bestem Wissen eine Beeinträchtigung des untersuchten Systems ausgeschlossen werden kann, z. B. die Benutzung von bekannten Default- Passwörtern oder das Ausprobieren von Verzeichniszugriffen bei einem Web-Server.
- In der nächsten Stufe – abwägend – wird auch versucht, Schwachstellen auszunutzen, die unter Umständen zu Systembeeinträchtigungen führen könnten. Darunter fallen z.B. das automatische Durchprobieren von Passwörtern und das Ausnutzen von bekannten Buffer-Overflows bei genau identifizierten Zielsystemen. Allerdings wird vorher abgewägt, wie wahrscheinlich ein Erfolg ist und wie stark die Konsequenzen wären.
- In der höchsten Aggressivitätsstufe – aggressiv – wird versucht, alle potentiellen Schwachstellen auszunutzen, z. B. werden Buffer-Overflows auch bei nicht eindeutig identifizierten Zielsystemen eingesetzt oder Sicherungssysteme werden durch gezielte Überlastung (Denial of Service, DoS-Attacken) deaktiviert. Dem Auftragnehmer muss bewusst sein, dass neben den zu testenden Systemen auch benachbarte Systeme oder Netzkomponenten bei diesen Tests ausfallen können.

3. UMFANG:

Welche Systeme sollen getestet werden?
Bei einem erstmaligen Penetrationstest ist grundsätzlich eine vollständige Überprüfung empfehlenswert, damit keine Sicherheitslücken auf den nicht-geprüften Systemen übersehen werden.
Der Aufwand für einen Penetrationstest hängt üblicherweise direkt vom Umfang der zu untersuchenden Systeme ab. Zwar können identische und nahezu identische Systeme teilweise automatisch in einem Arbeitsschritt untersucht werden, sobald aber eine abweichende Konfiguration gefunden wird, muss jedes System individuell behandelt werden:

- Ist vereinbart, dass nur ein bestimmtes Teilnetz, System oder ein bestimmter Dienst geprüft werden soll, so wird der Penetrationstest in dieser Studie als fokussiert bezeichnet. Dieser Umfang bietet sich z. B. nach einer Änderung oder Erweiterung der Systemlandschaft an. Der Test kann dann aber naturgemäß auch nur Aussagen über das getestete System und keine allgemeinen Hinweise zur IT-Sicherheit liefern.

- Bei einem begrenzten Penetrationstest wird eine begrenzte Anzahl von Systemen oder Diensten untersucht. So können beispielsweise alle Systeme in der DMZ geprüft werden oder auch Systeme, die einen funktionalen Verbund bilden.

- Der vollständige Test prüft alle erreichbaren Systeme. Dabei ist zu beachten, dass auch bei einem vollständigen Test u.U. bestimmte Systeme, z.B. ausgelagerte und extern gehostete dennoch nicht geprüft werden dürfen (siehe 5.1).

4. VORGEHENSWEISE:

Wie „sichtbar“ geht das Team beim Testen vor?
Sollen neben den primären Sicherheitssystemen auch sekundäre wie beispielsweise ein IDS oder organisatorische und personelle Strukturen wie Eskalationsprozeduren geprüft werden, so muss die Vorgehensweise bei der Durchführung des Penetrationstests entsprechend angepasst werden:

- Zur Prüfung von sekundären Sicherheits-Systemen und der vorhandenen Eskalationsprozeduren sollten – zumindest am Anfang – **verdeckte** Penetrationstests durchgeführt werden, d.h., dass in der Erkundungsphase nur solche Methoden zum Einsatz kommen, die nicht direkt als Angriffsversuche erkannt werden können.

- Falls die verdeckte Vorgehensweise keine Reaktionen ausgelöst hat oder ein White-Box-Test mit Einbeziehung der Systemverantwortlichen durchgeführt wird, so können auch **offensichtliche** Methoden wie z. B. umfangreiche Port-Scans mit direktem Connect angewendet werden. Bei einem offensichtlichen White-Box-Test können auch Mitarbeiter des Auftraggebers mit in das Team integriert werden, was besonders bei hochkritischen Systemen aufgrund der schnelleren Reaktionsmöglichkeiten auf unvorhergesehene Probleme ratsam ist.

5. TECHNIK:

Welche Techniken werden beim Testen eingesetzt?
Beim klassischen Penetrationstest werden die Systeme nur über das Netzwerk angegriffen. Ergänzend können die Systeme auch mittels sonstigen physischen Angriffen und Social-Engineering-Techniken attackiert werden:

- Der Penetrationstest über das Netzwerk entspricht dem normalen Vorgehen und simuliert einen typischen Hackerangriff. Die meisten IT-Netzwerke verwenden zur Zeit das TCP/IP Protokoll, so dass man auch von IP-basierten Penetrationstests spricht.

- Neben TCP/IP Netzwerken existieren weitere Kommunikationsnetze, die ebenfalls für Angriffe genutzt werden können. Dazu zählen neben Telefon- bzw. Fax-Netzen auch drahtlose Netze für mobile Kommunikation, z. B. auf Basis von IEEE 802.11(b) und zukünftig wohl auch BlueTooth Verbindungen.

- Mittlerweile sind Sicherheitssysteme wie Firewalls etc. weitverbreitet und die Konfigurationen dieser Systeme meist auf einem hohen Sicherheitsniveau, sodass ein Angriff unter Überwindung dieser Systeme nicht mehr oder nur mit sehr hohem Aufwand möglich ist.

- Oftmals ist es dann einfacher und schneller, die „gewünschten“ bzw. „gesuchten“ Daten durch Umgehung dieser Systeme durch einen direkten physischen Zugriff zu erlangen. Hierzu zählt z. B. der direkte Datenzugriff an einer nichtpasswortgeschützten Arbeitsstation nach Erlangung von unberechtigtem Zugang in die Gebäude und/oder Serverräume.

- Das **schwächste Glied** in der Kette der Sicherungssysteme ist oftmals der Mensch.

- Daher sind **Social-Engineering-Techniken**, die unzureichende Sicherheitskenntnisse oder ein mangelndes Sicherheitsbewusstsein ausnutzen, häufig erfolgreich. Diese Tests bieten sich beispielsweise nach Einführung einer allgemeinen Sicherheitsleitlinie an, um den Grad der Umsetzung bzw. die Akzeptanz zu evaluieren. Falsche Annahmen über die vermeintliche Wirksamkeit der Richtlinien führen häufig zu Sicherheitsrisiken, die bei korrekter Einschätzung durch zusätzliche Maßnahmen abgefangen werden könnten.

6. AUSGANGSPUNKT:

Von wo aus wird der Penetrationstest durchgeführt?
Der Ausgangspunkt des Penetrationstests, d. h. der Punkt, an dem der Penetrationstester seinen Rechner ans Netz anschließt bzw. von dem seine Angriffsversuche ausgehen, kann außerhalb oder innerhalb des Netzwerkes oder der Gebäude des Auftraggebers liegen:

- Die meisten Hackerangriffe erfolgen über die Netzwerkanbindung an das Internet. Daher kann ein Penetrationstest von außen die potenziellen Risiken eines solchen Angriffs erfassen und bewerten. Typischerweise werden hierbei die Firewall und Systeme in der DMZ sowie RAS-Verbindungen untersucht.

- Bei einem **Penetrationstest** von innen müssen üblicherweise keine Firewalls bzw. Eingangskontrollen überwunden werden, um Zugang zu den internen Netzen zu erhalten. Daher kann mit einem Test von innen bewertet werden, was z. B. bei einem Fehler in der Firewall-Konfiguration oder bei einem erfolgreichen Angriff auf die Firewall passieren könnte bzw. welche Zugriffsmöglichkeiten Personen mit Zugang um Internen Netzwerk erlangen könnten.

HABEN SIE NOCH FRAGEN?
Internet: www.t-systems.de/security
oder schreiben Sie eine E-Mail an
security-info@t-systems.at

EXPERTENKONTAKT
T-Systems Austria GesmH
Thomas Masicek
Head of Security Management
thomas.masicek@t-systems.at

HERAUSGEBER
T-Systems Austria GesmbH
Rennweg 97-99
1030 Wien