LSI-Info T#03

# PENETRATIONSTEST

## EIN ÜBERBLICK

*Version 1.0 vom: 29.05.2020*


### Management Summary

Ein Penetrationstest ist ein bewährtes Vorgehen, um das Potential eines Angriffs auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung zu ermitteln. Dabei werden die einzelnen IT-Services (Webanwendung, Fileserver, Mailserver, etc.) und die zugrunde liegenden IT-Systeme (Betriebssystem, Datenbank, etc.) auf Schwachstellen überprüft. Ziel ist es, die Erfolgsaussichten möglicher Angriffe einzuschätzen und daraus notwendige zusätzliche Sicherheitsmaßnahmen abzuleiten. Ein Penetrationstest kann auch für die Überprüfung der Wirksamkeit bereits umgesetzter Sicherheitsmaßnahmen verwendet werden.


*Im folgenden Text wird aufgrund der einfacheren Lesbarkeit das generische Maskulinum verwendet. Dieses soll alle Geschlechter einschließen.*

## Zielsetzung

Zielsetzungen eines Penetrationstests ist die Identifizierung von möglichen Schwachstellen, in den meisten Fällen der IT-Technik, in Form von:

- Sicherheitslücken in Software
- Offenen Ports
- Veraltete Softwareversionen
- Unzureichenden Zugriffsbeschränkungen
- Fehlerhafte Konfiguration

Zusammenfassend dient ein solcher Test der Beurteilung der Verwundbarkeit der Informationstechnik und daraus ableitend der Möglichkeit zur Erhöhung der Sicherheit auf technischer und konzeptioneller Ebene.

Als Abgrenzung muss berücksichtigt werden, dass ein Penetrationstest nicht zwingend alle Schwachstellen aufdeckt. Es können immer noch unbekannte Sicherheitslücken („Zero-Day-Exploit“) existieren oder bekannte Sicherheitslücken nicht entdeckt werden.

## Ansätze

Üblicherweise werden bei Penetrationstests Blackbox-, Whitebox- und Graybox-Tests unterschieden.

### Blackbox-Test

Bei einem Blackbox-Test stehen den Prüfern lediglich öffentlich zu ermittelnden Informationen des potentiellen Opfers zur Verfügung. Damit wird der Angriff eines typischen externen Täters simuliert. Der Prüfer hat nur unvollständige Kenntnisse über das IT-System seines Opfers.

### Whitebox-Test

Hier verfügen die Prüfer über umfangreiche interne Informationen der IT-Infrastruktur. Dazu gehören unter anderem Informationen über IP-Adressen und Netzaufbau, die Versionen, Art und ggf. Quellcode der eingesetzten Soft- und Hardware und Konfigurationen von Firewalls. Dies hat den Vorteil, dass die Tester ohne zeitaufwändige Informationsbeschaffung gezielter nach Schwachstellen in der tatsächlichen Infrastruktur suchen können und keine kritischen Systeme übersehen werden.  Die notwendigen Informationen werden beim Test von der beauftragenden Institution bereitgestellt.

Graybox-Test

Ein Graybox-Test ist eine Mischform aus Black- und Whitebox-Tests. Bei diesem verfügt der Prüfer über öffentlich ermittelbare Informationen über die Struktur des Testobjekts und teilweise auch über interne Informationen, z.B. aus bereitgestellten Dokumentationen.

## Prüfumfang

Übliche Prüfobjekte für einen Penetrationstest sind:

- Aktive Netzkomponenten (Router, Switches)
- Sicherheitskomponenten (Firewalls, Intrusion Detection Systeme, Virenscanner etc.)
- Physikalische oder virtuelle Server (Datenbankserver, Webserver, Fileserver, Speichersysteme etc.)
- Webanwendungen (Internetauftritt, Foren, Vorgangsbearbeitung, Apps)
- Hypervisor (Virtualisierungstechnologien)
- Mail- und Messaging Systeme
- Telekommunikationskomponenten (VoIP-Telefone, Multifunktionsgeräte)
- Cloud-Systeme
- Clients (Desktop-Computer, Laptops, Tablets, Smart devices wie z. B. Smartphones)
- Funknetze (WLAN, Bluetooth, NFC)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)
- SCADA-Systeme

Bei der Durchführung eines Penetrationstests werden vorrangig Schnittstellen untersucht, über die potenzielle Angreifer in die Prüfobjekte eindringen könnten. Abhängig von der Testtiefe können verschiedene Stellen analysiert werden. Mindestens sollten jedoch folgende Punkte geprüft werden:

- Aktualität des Patch-Standes und der eingesetzten Software-Versionen
- Authentisierung bei Programmzugriffen (z.B. Passwörter, Gruppenrechte)
- offene Ports
- Schnittstellen zu anderen Systemen oder Netzen
- Regelwerke (z.B. Firewalls, Nutzerrechte)

- Webanwendungen
  Eine gute Orientierungshilfe ist es für Webpentests, die OWASP (Open Web Application Security Project) Top 10 zu prüfen. Dies sind die aktuell zehn kritischsten Sicherheitsrisiken für Web-Anwendungen

- Eine Sonderform des Webpenetrationstests, welches das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Webcheck bezeichnet, dient der Überprüfung des Sicherheitsstands für eine, im Internet erreichbare, Webanwendung (Webseite, Blog, Online-Shop, Mobile-Apps). Diese erfolgt zu einem großen Teil mittels automatisierter Methoden über das Internet.

  Folgende Punkte stellen den empfohlenen Umfang dar, der bei einem Webcheck überprüft werden sollte:

  - Einsatz von Transportverschlüsselung (https)
  - Validierung von Benutzereingaben (z.B. in Kontaktformulare, Kommentarfunktionen gegen Cross-Site-Scripting)
  - Absicherung des Session-Handlings
  - Umsetzung der Zugriffskontrolle (z.B. interne Bereiche, geschützte Dateien und Verzeichnisse)
  - Behandlung von Fehlern (z.B. Informationsabfluss durch Fehlermeldungen)
  - Ausführung von Datenbank-Abfragen (z.B. gegen SQL-Injections)
  - Möglichkeiten zum Datei-Upload (z.B. präparierte Dateien mit Schadcode)
  - Validierung von „versteckten“ Parametern (z.B. in Cookies oder POST-Requests)
  - Aktualität von Softwareversionen (z. B. MySQL, PHP, Javascript, Angular)

- Gefährdungen / Nebenwirkungen können auch bei einem Penetrationstest auftreten und sollten bei der Planung berücksichtigt werden.

- Durch einen Penetrationstests kann es zu:
  - Systemgefährdungen,
  - Netzbelastungen,
  - Ausfällen und
  - Datenverlust

  kommen. Deshalb sollten Umfang, Intensität, tolerierbare und nicht tolerierbare Auswirkungen vorab genau vertraglich geregelt werden.

- Sollten im Outsourcing betriebene Systeme (z.B. ein externer Hosting-Provider) überprüft werden, muss der Vertrag mit diesem Dienstleister eine s.g. „Permission to attack“ enthalten, bzw. diese muss separat gegeben werden. Dies ist allerdings auch bei internen Tests ratsam.

- Bei Penetrationstests von Cloud-Umgebungen besteht aufgrund der möglicherweise mit anderen Kunden geteilten Ressourcen das Risiko, dass der Prüfer auf Daten anderer Kunden Zugriff erlangt. Dies muss auf jeden Fall vermieden werden.
  Größere Provider von Cloudangeboten wie Microsoft (https://docs.microsoft.com/de-de/azure/security/azure-security-pen-testing) Google (https://cloud.google.com/security/overview/) und Amazon bzw. AWS (https://aws.amazon.com/de/security/penetration-testing/) gestatten bei Einhaltung der Richtlinien und Nutzungsbedingungen bestimmte Penetrationstests mit definiertem Umfang. Da sich die Nutzungsbedingungen aber jederzeit ändern können, sollte die Rechtslage vor jedem Test erneut geprüft werden.

- Ein Penetrationstest sollte in unkritischen Zeitfenstern mit ausreichend Puffer durchgeführt werden. Damit wird die Beeinträchtigung des regulären Betriebs auf ein Minimum reduziert. Der Nachteil dieses Vorgehens ist allerdings, dass die fehlende Last im Netz und auf den Systemen das Ergebnis verzerren kann. Dasselbe gilt für die Durchführung auf Nicht-Live-Systemen (z.B. Test- oder Staging-Systemen). Außerdem ist es ratsam, die potentiell betroffenen Personen vor einem Penetrationstest zu informieren.

- Anforderungen an den Prüfer

- Penetrationstests sind komplex und erfordern fachlich qualifizierte Prüfer. Diese sollten unabhängig sein und nicht beim Entwurf, Aufbau oder dem laufenden Betrieb der zu testenden Systeme beteiligt gewesen sein. So soll einerseits einem möglicherweise auftretenden Interessenkonflikt schon vorab entgegengewirkt werden und andererseits eine mögliche Betriebsblindheit des Prüfers vermieden werden.

- Der Prüfer muss den Testablauf, die verwendeten Techniken und die Ergebnisse detailliert dokumentieren. Diese Dokumentation stellt die Grundlage für weitere Maßnahmen dar.

- Die Durchführung eines Penetrationstests kann in unterschiedlicher Intensität erfolgen. Grundsätzlich können drei Stufen unterschieden werden.

- Sicherheitsaudit

  In der einfachsten Form wird ein technisches Sicherheitsaudit z.B. nach BSI-Leitfaden durchgeführt. Bei diesem werden potentielle Schwachstellen aufgrund der Versionen der verwendeten IT-Anwendungen, der Härtungsmaßnahmen und der Konfigurationen geschlossen. Die Untersuchung der IT-Systeme geschieht dabei vor Ort durch den Prüfer und den zuständigen Administrator.

- Nicht invasiver Schwachstellenscan

  Zusätzlich zum Sicherheitsaudit ist ein nicht invasiver Schwachstellenscan die nächsthöhere Stufe einer Prüfung. Dabei werden das zu untersuchende Netz und die zu untersuchenden Systeme mit einem Schwachstellenscanner des Prüfers auf Sicherheitslücken gescannt. Die eingesetzte Software scannt nach Schwachstellen, die als Common Vulnerabilities and Exposures (CVE) bekannt gemacht wurden. Die gefundenen Sicherheitslücken werden durch den Schwachstellenscanner nicht ausgenutzt. Das Ergebnis sind die potentiellen Sicherheitslücken, die ein Angreifer theoretisch nutzen könnte. Der Nachteil dieser Methode ist das Risiko, viele falsche Meldungen (sogenannte "False Positives" - also nicht tatsächlich vorhandene Sicherheitslücken) zu erhalten. Der Test auf Schwachstellen erfolgt primär anhand der Versionen der eingesetzten Betriebssysteme und Anwendungen. Patch-Maßnahmen können hier aber schon Sicherheitslücken geschlossen haben.
  Diese Art von Scan kann auch durch die eigene IT-Abteilung in regelmäßigen Abständen durchgeführt werden, um z.B. die Wirksamkeit von Maßnahmen oder den aktuellen Sicherheitsstand der Systeme zu prüfen. Dieses Vorgehen wird auch in einigen ISMS gefordert.

- Invasiver Schwachstellenscan

  Eine weitere Erhöhung der Penetrationsstufe führt zu einem invasiven Schwachstellenscan. Mit diesem Ansatz wird versucht, die gefundenen Schwachstellen mittels so genannter Exploits auszunutzen. Exploits dienen dazu, bekannte Schwachstellen in Anwendungen oder in der Kombination von verketteten Anwendungen auszunutzen. Durch diesen Ansatz wird bewiesen, dass ein IT-System tatsächlich unter Nutzung dieser Sicherheitslücke erfolgreich angegriffen werden kann. Außerdem lassen sich damit unter Umständen weitere Sicherheitslücken finden – beispielsweise mit einer Erweiterung der Benutzerrechte oder einer Abschaltung von Sicherheitsmaßnahmen. Der Nachteil ist, dass beim Einsatz von Exploits die IT-Systeme stark beeinträchtigt werden können. Es könnte zu Datenverlust oder Ausfällen kommen.

- Einstufung der Schwachstellen

  Die Einstufung der im Zuge eines Penetrationstests gefundenen Schwachstellen hängt vom Schutzbedarf der verarbeiteten Daten sowie der Kritikalität der Verfügbarkeit des Systems ab. Abhängig davon, ob das IT-System offene oder geschützte Daten verarbeitet und ob der Betrieb auch ohne dieses System aufrecht erhalten werden kann, muss eine Schwachstelle unterschiedlich eingestuft werden. Bei der Einstufung der gefundenen Schwachstellen sollte darüber hinaus die Wahrscheinlichkeit der Ausnutzung dieser Schwachstelle unter Berücksichtigung der Fähigkeiten und der Mittel der Angreifer Berücksichtigung finden.

- Tools und Anbieter

  Neben vielen kommerziellen Lösungen existieren auch diverse frei verfügbare Open Source Tools, z.B. ein Scanner speziell für die OWASP TOP 10. Die Open Source-Varianten stellen für IT-Verantwortliche eine kostengünstige Möglichkeit dar, sich einen ersten Überblick über die IT-Infrastruktur zu verschaffen.

  Auf dem Markt lässt sich eine Anzahl an kleineren und größeren Anbietern finden, die Penetrationstests anbieten. Diese führen in der Regel einmalig Penetrationstests durch. Es existieren aber auch Unternehmen, die Verträge mit längeren Laufzeiten anbieten und dabei in regelmäßigen Abständen Tests durchführen.

  Sowohl bei den Tools als auch den Anbietern ist es aufgrund der Kritikalität der durchgeführten Arbeiten extrem wichtig, auf die Zuverlässigkeit zu achten.

Quellen


- BSI – Ein Praxis-Leitfaden für IS-Penetrationstests (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=10)
- BSI – Ein Praxis-Leitfaden für IS-Webchecks (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Webcheck.pdf?__blob=publicationFile&v=4)
- OWASP Top 10 (https://www.owasp.org/images/9/90/OWASP_Top_10-2017_de_V1.0.pdf)
- Stanford University, Microsoft - Measuring and Troubleshooting Large Operational Multipath Networks with Gray Box Testing (https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr2015-netsonar.pdf)
- iX, Juni.2019


## KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.