IT-Sicherheit auf dem Prüfstand

Penetrationstest

datenschutz nord GRUPPE

Risiken erkennen und Sicherheitslücken schließen

Zunehmende Angriffe aus dem Internet haben in den letzten Jahren das Thema IT-Sicherheit für Unternehmen unverzichtbar gemacht. Dennoch führen unzureichend administrierte Server, veraltete Softwareversionen oder Programmierfehler zu erfolgreichen Angriffen insbesondere auf Mail- und Web-Server. Schützen Sie Ihr Unternehmen vor wirtschaftlichen Schäden und Imageverlust und optimieren Sie Ihre IT-Sicherheit – wir helfen Ihnen dabei!

Wie sicher Computersysteme wirklich sind, lässt sich am effektivsten durch gezielte Penetrationstests erkennen, die wir für Sie durchführen und die Antworten auf u.a. folgende Fragen geben:

- Können externe Angreifer die Firewall umgehen?
- Können Externe aufgrund veralteter Softwareversionen die Kontrolle über Mail- oder Web-Server übernehmen?
- Können sich Unbefugte über einen Exploit Zugriff auf sensible Daten verschaffen?
- Können Kundendaten auf der Webapplikation mittels SQL-Injection oder Cross-Site-Scripting ausgelesen werden?

In einem Bericht stellen wir Ihnen nicht nur die Ergebnisse über vorhandene Schwachstellen in Netzwerken, Serversystemen und Anwendungen zusammen, sondern geben Ihnen Handlungsempfehlungen und zeigen Lösungswege auf.

Penetrationstest in drei Stufen

Der Penetrationstest erfolgt dreistufig: In einem ersten Schritt werden die extern verfügbaren Dienste auf dem Zielsystem mit einem Portscan ermittelt. Dazu werden Verbindungen zu dem Zielsystem aufgebaut, Anfragen gesendet und die Antworten ausgewertet. Um Intrusion Detection/Prevention Systeme (IDS/IPS) gegebenenfalls zu umgehen, können alle Tests sequentiell durchgeführt werden.

In einem zweiten Schritt werden die ermittelten Dienste als Grundlage für einen passiven Schwachstellenscan genutzt. Ein passiver Schwachstellenscan zeigt mögliche Gefährdungen des Zielsystems auf, wobei jedoch eventuell vorhandene Schwachstellen nicht aktiv überprüft und ausgenutzt werden. Es werden keine Tests ausgeführt, die die Erreichbarkeit der Zielsysteme beeinträchtigen! Sofern es sich um eine Web-Applikation handelt, werden zusätzlich die Funktionen der Web-Applikation auf mögliche Schwachstellen getestet. Getestet werden u.a. sämtliche Angriffe der OWASP-Top-10.

In einem dritten Schritt werden die Ergebnisse des Port- sowie des Schwachstellenscans validiert und um manuelle Tests erweitert.

Der Penetrationstest kann sowohl als Blackbox- als auch als Whitebox-Test durchgeführt werden: Während bei einem Blackbox-Test keine Details über die Zielsysteme bekannt sind, werden für einen Whitebox-Test umfangreiche Informationen über die eingesetzten Netzwerke, Serversysteme und Anwendungen durch den Auftraggeber bereitgestellt.

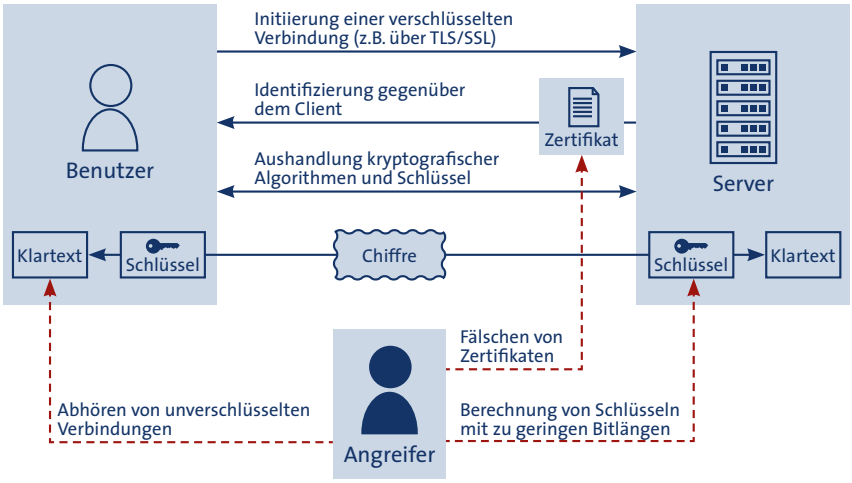
Darüber hinaus wird zwischen internen und externen Penetrationstests unterschieden: Bei externen Tests werden die per Internet erreichbaren Systeme untersucht, bei internen Tests erfolgen die Scans aus dem Intranet des Auftraggebers heraus.

Umfang der Tests

Ermittlung verfügbarer Ports und Dienste
Serversysteme, beispielsweise Web- oder Mailserver, bieten Ports und Dienste zur Nutzung an. Es wird in diesem Zusammenhang geprüft, welche Ports verfügbar sind und ob Dienste veraltet oder falsch konfiguriert sind.

Auswertung von Fehlermeldungen
Gibt ein System Standardfehlermeldungen aus, so werden dadurch in der Regel Informationen über die Infrastruktur oder über eingesetzte Programmversionen offen gelegt. Während des Penetrationstests wird daher detailliert nach Fehlermeldungen gesucht.

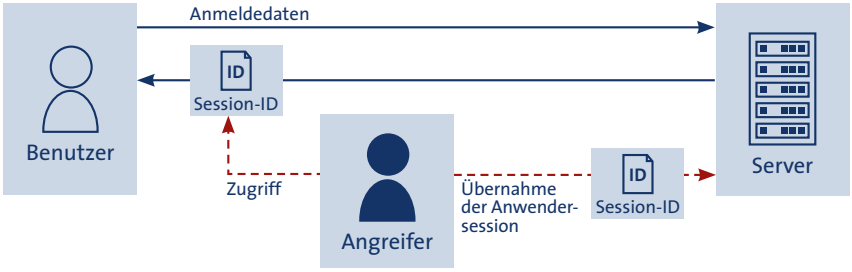
Überprüfung der Verschlüsselung
Vertrauliche Daten wie z.B. Anmelde- oder Bankinfomationen sollten grundsätzlich verschlüsselt übertragen werden, um zu verhindern, dass Angreifer den Datenstrom abhören. Es wird daher geprüft, ob alle sensiblen Daten verschlüsselt übertragen und ob ausschließlich aktuelle und sichere Verschlüsselungsverfahren eingesetzt werden.



Überprüfung der Registrierung und Authentisierung
Bei zahlreichen Webseiten besteht die Möglichkeit, sich registrieren zu lassen und mit Hilfe einer Benutzerkennung spezielle Dienste zu nutzen. Im Rahmen des Penetrationstests wird daher die Art und Qualität der Registrierung und Authentisierung geprüft.

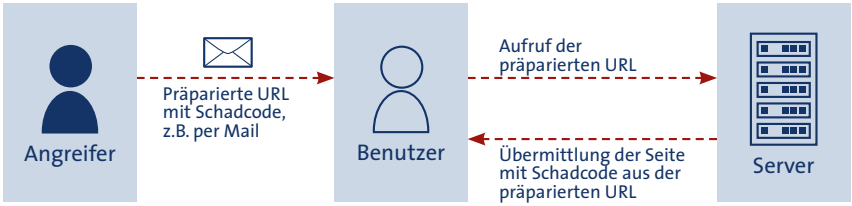
Ausweitung der Zugriffsrechte
Über Zugriffsrechte und deren Verwaltung wird sichergestellt, dass der Anwender nur Daten lesen und Funktionen ausführen kann, für die er berechtigt ist. Im Rahmen einer horizontalen Rechteausweitung wird geprüft, ob auf Daten eines anderen Benutzers zugegriffen werden kann. Ebenso wird vertikal versucht, Zugriff auf administrative Funktionen und Ressourcen zu erhalten. Über Path Traversal Angriffe wird der Zugriff auf Dateien und Verzeichnisse getestet, die nicht zur Veröffentlichung durch den Webserver vorgesehen sind.

Manipulation des Session-Managements
Das http-Protokoll ist ein zustandsloses Protokoll, d.h. der Zugriff auf den Webserver ist unabhängig von vorherigen Zugriffen des gleichen Anwenders. Interaktive Webanwendungen müssen daher eine Session-ID verwenden, um den Anwender über mehrere Zugriffe hinweg identifizieren zu können. Bei der Überprüfung des Session-Managements wird versucht, durch Manipulation der Verbindungsdaten (URL, Verbindungsparameter, SessionID) die Daten einer bestehenden Session zu verwenden und diese zu übernehmen.



Cross-Site-Scripting (XSS)

Beim Cross-Site-Scripting manipuliert der Angreifer eine Webseite und fügt neue Inhalte hinzu, die dann von einem anderen Benutzer gelesen werden. Wenn es sich bei dem eingefügten Inhalt um einen Programmcode, z.B. JavaScript, handelt, wird dieses Programm auf dem System des Benutzers ausgeführt. Beim Cross-Site-Scripting wird zwischen Angriffen unterschieden, die vom Benutzer selbst durch präparierte Links in einer Mail initiiert werden (reflected XSS) und Angriffen, die persistent im Webauftritt gespeichert sind und von jedem Besucher einer Webseite ausgeführt werden (stored XSS). Im Rahmen des Penetrationstestes werden beide Angriffstechniken getestet.



Injection

Injection ist ein Sammelbegriff für das Ausnutzen einer Sicherheitslücke, bei der Schadcode an eine Webapplikation übermittelt wird, welcher anschließend durch fehlerhafte Weiterverarbeitung oder unzureichende Überprüfung von Metazeichen durch den Webserver ausgeführt wird. Während bei einer SQL-Injection versucht wird, Datenbankbefehle einzuschleusen, wird bei einer OS-Injection die Webapplikation dazu genutzt, Betriebssystembefehle mit den Rechten des Webservers auszuführen. Bei einer Header-Injection wird der Responseheader manipuliert, um beispielsweise den Benutzer auf eine Phishingseite umzuleiten.
Die Anfälligkeit für Injections wird durch eine automatische und manuelle Eingabe von entsprechenden Zeichenketten z.B. im Anmeldefenster oder in Suchmasken überprüft.

datenschutz nord Gruppe

Zu der datenschutz nord Gruppe gehören die **DSN Holding GmbH,** deren Tochterunternehmen **datenschutz nord GmbH,** die **datenschutz süd GmbH,** die **datenschutz cert GmbH,** die international tätige **FIRST PRIVACY GmbH** sowie die **PRIVACY Central GmbH.**

Die datenschutz nord Gruppe ist einer der bundesweit führenden Dienstleister im Bereich Datenschutz. Bei mehr als 500 Unternehmen sind wir als externer betrieblicher Datenschutzbeauftragter tätig. Darüber hinaus beraten unsere IT-Sicherheitsexperten – lizenzierte ISO/IEC 27001- bzw. IT-Grundschutz-Auditoren – in allen Bereichen der Informationssicherheit.

Außerdem betreiben wir die **datenschutz nord Akademie,** das Datenschutz-Managementsystem **privacy port** und den News-Blog **www.datenschutz-notizen.de**.

Beratung & Konzeption	Schulungen, E-Learning, Datenschutz-Managementsystem	Auditierung & Zertifizierung

DATENSCHUTZ & IT-SICHERHEIT

BERLIN • BREMEN • HAMBURG • KÖLN • WÜRZBURG

02/dsn

datenschutz nord GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: +49 (0) 421 69 66 32-0

office@datenschutz-nord.de
www.datenschutz-nord-gruppe.de

datenschutz süd GmbH

Hauptsitz Würzburg
Wörthstraße 15
97082 Würzburg
Tel.: +49 (0) 931 30 49 76-0

office@datenschutz-sued.de
www.datenschutz-nord-gruppe.de

Weitere Niederlassungen der datenschutz nord Gruppe siehe **www.datenschutz-nord-gruppe.de/standorte**

datenschutz nord

datenschutz süd