7 Systemtest und Dokumentation vorbereiten

Bevor mit der Installation begonnen wird, wird die Dokumentation der in den vorherigen Kapiteln beschriebenen Schritte vorgenommen. Zusätzlich sind die Anforderungen an den Internetserver in Form von Testfällen zu dokumentieren, d. h., wie die Erfüllung der Anforderungen getestet wird.

Nebst der Dokumentation der Testfälle werden die Testresultate ebenfalls dokumentiert, um Probleme nachvollziehbar zu machen. Damit wird vermieden, dass durch Installation oder Änderungen am Internetserver andere Funktionen nicht mehr verfügbar sind. Anhand der Testdokumentation ist es so immer möglich, auf den letzten funktionierenden Stand des Systems zurückzugehen.

7.1 Technische Tests am Internetserver

Zu den technischen Tests am Internetserver gehören vor allem die Überprüfung der generellen Erreichbarkeit des Internetservers und die Berechtigungen auf Netzwerkebene innerhalb des Subnetzes und vom Internet her.

Folgendes sollte überprüft werden:

- Routing: Kann die IP-Adresse des Internetservers von den notwendigen Zugangspunkten aus erreicht werden (Intranet/LAN, DMZ, Internet, andere Netzwerke innerhalb des Unternehmens)? Erfolgt der Zugang über die korrekten Routen (mithilfe von tracert/traceroute überprüfen)? Ebenfalls überprüft werden muss, ob der Server von Netzen erreichbar ist, von welchem er nicht erreichbar sein sollte. Dieser Test soll zusätzlich auch umgekehrt erfolgen: Welche Netze kann der Internetserver erreichen (ein von einem Angreifer kompromittierter Internet-Server im internen Netzwerk kann dadurch Schaden auf anderen Systemen anrichten)?
- Umgebung: Stromversorgung (Test unterbruchfreie Stromversorgung), Belüftung und Klimatisierung (Test der Temperatur; auch nach ein paar Tagen ununterbrochenen Betriebs), Zugang zu Kabeln und Server (für Reparaturen, Austausch); dies besonders wenn der Server andernorts «housed» und nicht in eigenen Räumlichkeiten betrieben wird.
- Burn-in Test: Hardware über mehrere Tage laufen lassen, um Funktionsstörungen zu beobachten die sich evtl. erst nach einer gewissen Betriebsdauer einstellen.

7.2 Applikatorische Tests am Internetserver

Die applikatorischen Tests umfassen die Überprüfung der Funktionen der einzelnen installierten Applikationen. Beim Internetserver ist dies:

- **Webserver (Port 80 und 443, evtl. andere Ports je nach Konfiguration; Administrations-Interface z. B. auf Port 8080 falls vorhanden):** Werden die richtigen Seiten angezeigt? Bei Konfiguration von mehreren Domains: Werden alle richtig angezeigt? Spezielle Konfigurationen testen (individuelle Error-Messages). Zusätzlich sollen die Zugriffe von nicht authentisierten Benutzern getestet werden: Auf welche Verzeichnisse haben die Benutzer Zugriff? Bei verschlüsselten Verbindungen die Zugänglichkeit und Gültigkeit der Zertifikate überprüfen. Möglicherweise wurde konfiguriert, dass nur verschlüsselte Verbindungen möglich sind: Testen der Umleitung bei Verbindung mit nicht-verschlüsselter Verbindung. Wird diese auf die verschlüsselte Verbindung umgeleitet (redirect von port 80 zu 443)? Das Management-Interface auf einem anderen Port (z. B. 8080, 8081 etc.) sollte nicht von extern (Internet) zugänglich sein. Dies soll ebenfalls getestet

werden. Der Webserver ist generell sehr detailliert zu testen (insbesondere Sicherheitstests), ganz besonders wenn eine Datenbank mit vertraulichen Daten mit dem Webserver verbunden ist. Weitere wichtige Informationen zu diesem Thema liefern verschiedene Webseiten, darunter: http://www.webappsec.org und http://www.osstmm.org

- **Mailserver (port 25 SMTP, 110 POP3, 143 IMAP etc.)**: Dieser soll ebenfalls ausführlich getestet werden:
  - Können E-Mails von aussen her versendet werden? (Spam-Relaying vom Internet aus, E-Mail versenden ohne Authentifikation, E-Mail senden mit falschem Absender)
  - Werden E-Mails von verschiedenen externen (und internen) Absendern akzeptiert? Werden Spams blockiert, und werden berechtigte E-Mails als Spam blockiert? Können E-Mails auch vom Internet aus abgefragt werden (POP3, IMAP), bzw. soll dies nicht möglich sein? Sind verschlüsselte Verbindungen konfiguriert und sollen diese auch von extern erreichbar sein?
- **FTP-Server (port 20, 21):** Ist dieser von extern erreichbar und welche Benutzer können einloggen? Ist anonymer Zugriff (anonymous) möglich? Wenn ja, welche Verzeichnisse sind sichtbar? Können auch grössere Dateien übermittelt werden, oder unterbricht die Verbindung? Wie viele Sessions/Sitzungen können gleichzeitig geöffnet werden (wichtig bei starkem Verkehr auf dem FTP-Server, wenn viele Benutzer gleichzeitig Downloads machen möchten)? Welche Benutzer dürfen schreiben, welche nur lesen? Welche Verzeichnisse sind sichtbar?
- **DNS-Server (udp/tcp port 53):** Werden von extern auch interne Domains aufgelöst (und somit interne Adressen nach aussen preisgegeben), bzw. werden externe Anfragen beantwortet (oft ist der DNS-Server nur für internen Gebrauch, d. h. Anfragen von aussen sollen nicht möglich sein)? Erlaubt der DNS-Server gar einen zone-transfer von extern (dies sollte nur für den secondary DNS server möglich sein)? Ist die Konfiguration des DNS-Servers geschützt (v. a. bei Web-GUI zur Konfiguration) oder besteht für Angreifer die Möglichkeit Einträge zu ändern?

7.3 Sicherheitstests rund um den Internetserver

Die Sicherheitstests rund um den Internetserver umfassen einerseits die oben genannten Tests und sollen vor allem die Anforderungen an Verfügbarkeit, Vertraulichkeit und Integrität sicherstellen.

- Verfügbarkeit: Wie verhält sich der Internetserver unter Last? Ist der Internetserver immer verfügbar? (Dieser Test lässt sich einfach von einem benachbarten System automatisieren, um die ständige Erreichbarkeit des Internetservers dauernd zu überwachen.)
- Vertraulichkeit: Sind die schützenswerten Daten entsprechend sicher und können nur berechtigte Benutzer darauf zugreifen? Welche Daten über Mitarbeiter, Kunden oder das Unternehmen sind sichtbar?
- Integrität: Ist das Zertifikat des Webservers aktuell (Ablaufdatum), und entspricht es der Domain der WWW-Adresse? Sind die DNS-Einträge korrekt und können diese nicht verändert werden?

Neben diesen generellen Hinweisen finden sich im Internet detaillierte Anleitungen für die Absicherung der verschiedenen Internet-Server-Dienste. Die Sicherheit des Internetservers kann auch mit automatisierten Werkzeugen getestet werden. Die bekanntesten sind:

- Nmap (www.insecure.org): Portscanner zur Überprüfung der Dienste auf einem Server
- Nessus (Unix), NeWT (Windows) (www.nessus.org): Vulnerability Scanner, der die Schwachstellen von einer Vielzahl von Diensten aufspürt und testet; sehr empfehlenswertes Werkzeug

- Ethereal (www.ethereal.org): Sniffer, um Daten und Verbindungen im lokalen Netzwerk zu überprüfen
- Nikto (www.cirt.net), N-Stealth (www.nstalker.com): Webserver-Scanner, die speziell Webserver überprüfen
- Microsoft Baseline Security Analyzer (MBSA, www.microsoft.com): nur für Windows-Systeme
- IIS Lockdown Tool (www.microsoft.com): schliesst nicht benötigte Dienste und Lücken im Internet Information Server

7.4 Lasttest

Das Verhalten des Internetservers unter Last ist oft nicht einfach zu testen, da das Benutzerverhalten sehr schwierig vorauszusagen ist. Dennoch gibt es verschiedene Tools, um solche Tests durchzuführen und mehrere Benutzeranfragen zu simulieren.

Die beste Möglichkeit für einen Lasttest auf dem Internetserver ist die Benutzung durch echte User. Ein solcher Test kann während der Pilotphase durchgeführt werden, wenn immer mehr Benutzer für den Internetserver zugelassen werden. Während dieser Phase werden die Logs und Auslastungsprotokolle genau beobachtet, um bei Problemen sofort eingreifen zu können.

Microsoft bietet für den IIS das «Web Capacity Analysis Tool» an, um Benutzersitzungen zu simulieren. Daneben gibt es auch das «Web Application Stress Tool». Es gibt des weiteren viele Stresstest-Tools im Internet. Die meisten davon sind jedoch kostenpflichtig, können aber als Testversion oft 30 Tage lang ausprobiert werden.

7.5 Dokumentation des Internetservers

Die Dokumentation der Installationsparameter (Auswahl Hardware, Software, Versionen, Speicher- und Lagerorte der SW und HW) sowie des Installationsvorgehens ist ebenso wichtig wie die Beschreibung der Tätigkeiten im täglichen Betrieb des Servers. Wenn nötig, wird auch eine Dokumentation für die Benutzer des Systems erstellt bzw. bei den entsprechenden Applikationsverantwortlichen in Auftrag gegeben.

Eine vollständige und aktuelle Dokumentation erleichtert die Installation und Pflege eines Internetservers ungemein und ist daher als zwingend zu erachten.

Detailliertere Angaben zur Dokumentation eines Servers sind im Modul 127 «Server betreiben» behandelt.

7.5.1 Installationsdokumentation

Die Installationsdokumentation umfasst die gesamte Hardware, die zur Installation benötigten wurde sowie die Software, die installiert wurde. Es lohnt sich auch, die Original-Lieferscheine bzw. Garantie-Vereinbarungen zentral aufzubewahren (zusammen mit der Installationsdoku), um bei Beschaffung von Ersatzteilen die benötigten Dokumente zusammen zu haben.

Serienummern von Hard- und Software werden idealerweise ebenfalls in die Installationsdokumentation aufgenommen, um diese immer im Zugriff zu haben (elektronisch).

Die Installationsdokumentation beschreibt Schritt für Schritt die notwendigen Installationspunkte und Anfangs-Konfigurationen und idealerweise Möglichkeiten, um die Installa-

tion jeweils zu testen (Funktionstest). Sehr geeignet sind dabei «screenshots», um das Vorgehen bildhaft zu dokumentieren.

7.5.2 Betriebsdokumentation

Die Betriebsdokumentation umfasst die Informationen für den Administrator eines Systems, die für den täglichen Betrieb benötigt werden. In der Betriebsdokumentation wird auch das Notfallkonzept beschrieben, damit die Informationen zentral (und nicht auf verschiedene Dokumente verteilt) verfügbar sind.

Konfigurationen, Konfigurationsdateien und für den Betrieb notwendige Einstellungen werden dokumentiert. Befehle und Hilfsprogramme, um den Server zu warten (Back-ups, Funktionstests, sog. «morning checks» um den Betrieb des Servers regelmässig zu überprüfen) werden ebenfalls beschrieben.

7.5.3 Benutzerdokumentation

Die Benutzerdokumentation umfasst im Wesentlichen die Handbücher für die einzelnen Applikationen und idealerweise auch das Vorgehen bei Problemen (Hotline, Kontaktmöglichkeiten).

Ebenfalls in der Benutzerdokumentation enthalten sind allfällige Konfigurationen von Client-Software, die der Benutzer vornehmen muss, um mit dem Internetserver zu kommunizieren/arbeiten.

Repetitionsfragen

13	Welche Art von Tests sollen vor der Abnahme des Internetservers geplant werden?
18	Nenne Sie die verschiedenen Arten von Dokumentationen für einen Internetserver?