Stefan Gora

Security Audits

Kontrolle und Auditierung getroffener Sicherheitsmaßnahmen sind wichtige Bestandteile eines erfolgreichen Sicherheitsmanagements. Um eine Aussage über das erreichte Maß an Sicherheit treffen zu können, werden Audits und Sicherheitsanalysen durchgeführt. Hierdurch kann festgestellt werden, welche Maßnahmen nicht ausreichend wirksam sind oder welche Maßnahmen fehlen.

1 Begriffsdefinitionen und Audit-Typen

Um einen „gemeinsamen Nenner" und einheitlichen Sprachgebrauch zu schaffen, werden vorab zentrale Begriffe definiert.

1.1 Audit

Ein Audit (lateinisch für „Anhörung") ist die Durchführung eines Soll-Ist-Vergleichs zu einem bestimmten Zeitpunkt, wobei der Soll-Zustand möglichst genau festgelegt sein sollte. Audits gibt es in vielen Bereichen; in diesem Beitrag werden ausschließlich Security Audits, d. h. Audits mit dem Fokus IT-Sicherheit oder Informationssicherheit, betrachtet.

Bei diesen wird der Soll-Zustand mehr oder weniger formal festgelegt durch

- implizite Definitionen, z. B. „Systeme sollen sicher sein"[1] oder „unbefugter Zugriff nicht möglich" und
- explizite Definitionen, z. B. standardisierte Vorgaben (bspw. nach IT-Grundschutz) oder abgeleitete Bedingungen (z. B. spezifische Anpassungen nach ISO 2700x).

Stefan Gora

ist er Security Consultant bei der Secorvo Security Consulting GmbH. Seine Beratungsschwerpunkte liegen in den Bereichen Information Security Management, IT-Sicherheitsaudits, Sicherheit von Webapplikationen, Penetrationstests und Forensik

Primäres Ziel eines Audits ist neben den Ergebnissen des Soll-Ist-Vergleichs eine Bewertung der Angemessenheit der bereits getroffenen Maßnahmen im Prüfungsumfeld sowie die Festlegung weiterer Maßnahmen zur Annäherung an den Soll-Zustand.

Ein Audit beinhaltet insbesondere auch die Dokumentation des Vorgehens und der Ergebnisse. Nur wenn lückenlos der Nachweis erbracht werden kann, wie die Auditoren zu den Ergebnissen und Bewertungen kommen, sind diese ausreichend aussagekräftig. An die Darstellung werden daher hohe Anforderungen gestellt, das Ergebnis muss zumindest nachvollziehbar oder – wie im Bereich IT-Grundschutz – sogar reproduzierbar sein.

1.2 Penetrationstest

Ein Penetrationstest ist eine Unterform von Audits, durch welchen das Vorhandensein und die Wirksamkeit von Sicherheitsmaßnahmen durch Überwindungsversuche geprüft werden.

Diese Untersuchungen sind in der Regel rein technischer Natur, d. h. organisatorische Sicherheitsmaßnahmen stehen nicht im Fokus der Untersuchungen. Neben automatisierten Schwachstellen-Scans und einer manuellen Verifikation der Ergebnisse sollten sie weitere manuelle Untersuchungen unter Einsatz von Kreativität und Erfahrung beinhalten. Hierzu können so genannte Exploits[2], welche ggf. angepasst oder selbst entwickelt werden müssen, und spezifische Angriffstools, beispielsweise für inside-out-Angriffe[3], verwendet werden. In vielen Fällen reicht aber auch schon ein Browser aus, um z. B. Schwachstellen in Webapplikationen festzustellen.

In jedem Fall sollten geeignete Vorsichtsmaßnahmen (siehe unten) für mögliche Störfälle ergriffen werden. Selbst wenn manche Angriffs-Tools nicht auf „scharf" geschaltet sind, kann eine Störung nicht vollständig ausgeschlossen werden.

1.3 Black-Box-Analyse

Eine Black-Box-Analyse ist eine Unterform von Audits, wobei diese ohne Kenntnis von Sicherheitsmaßnahmen, Systemdetails, Infrastrukturen, Personen und Rollen durchgeführt wird. Sie wird also aus Sicht eines externen oder internen Angreifers konzipiert, wobei aufgrund der hohen Integration von IT-Systemen mit Partnern, Dienstleistern etc. die Unterscheidung zwischen intern und extern immer schwieriger wird. Ein interner Angreifer kann beispielsweise jeder sein, der über eine Netzverbindung verfügt, aber auch ein eigener Mitarbeiter, der in der Lage ist, Angriffstools auf seinem System zu installieren oder bereits vorhandene Werkzeuge nutzt.

Black-Box-Analysen sind in der Regel technisch und zeigen organisatorische oder architektonische Mängel nur implizit auf (z. B. unzureichendes Patch-Management oder einstufige Firewall-Konzeptionen).

Die Begriffe „Black-Box-Analyse" und „Penetrationstest" werden fälschlicherweise oft synonym verwendet. In man-

1 In der Regel ist damit „so sicher wie möglich" und ein Abgleich gegen „best practice" gemeint.

2 Ein Exploit ist Software zur gezielten Ausnutzung einer Schwachstelle.

3 Inside-Out Angriffe sind eine Sonderform von Angriffen, bei denen versucht wird, durch Schwachstellen, beispielsweise in Browser oder Mail-Client, oder bei fehlendem Bewusstsein der Mitarbeiter Verbindungen aus lokalen Netzen heraus in Richtung Angreifer im Internet aufzubauen.

chen Fällen werden aber vorab Informationen für Penetrationstests zur Verfügung gestellt, es handelt sich in diesem Fall dann per Definition nicht um eine Black-Box-Analyse. Dieser Fall wird als „Grey-Box-Analyse" bezeichnet; die Begriffe werden in der Praxis aber oft nicht unterschieden.

1.4 Grey-Box-Analyse

Im Unterschied zu einem „echten" Angreifer, beispielsweise aus dem Internet, unterliegen Anbieter im Bereich der Sicherheitsanalysen in der Regel einem Termin- und Budget-Druck. Das Projekt soll in absehbarer Zeit durchgeführt werden und auch die zur Verfügung stehenden personellen und monetären Ressourcen sind beschränkt. Daher bietet es sich in vielen Fällen an, bestimmte Informationen zur Verfügung zu stellen. Man spricht dann von Grey-Box-Analysen.
Eine Informationsbeschaffung zu den Netzen eines Unternehmens und den zur Verfügung gestellten Internet-Diensten kann in der Regel ohne Unterstützung in wenigen Minuten durchgeführt werden.

Anders sieht es aus, wenn beispielsweise gezielt Schwachstellen in eingesetzter Software wie dem Internet Browser überprüft werden sollen. Anstatt zu versuchen, über einen präparierten Webserver die Anfälligkeit auf sämtliche Schwachstellen aller potenziell einsetzbaren Browser zu prüfen, kann einige Zeit gespart werden, wenn die Untersuchung auf den eingesetzten Browsertyp (Internet Explorer, Firefox, Mozilla, Opera etc.) eingeschränkt wird.

Es sollten allerdings nur solche Informationen geliefert werden, die – mit ausreichendem zeitlichen Vorlauf – auch ohne Hilfestellung beschafft werden könnten.

1.5 White-Box-Analyse

Im Rahmen einer White-Box-Analyse haben der Auditor und das Auditor-Team (vgl. Abschnitt Maßnahmen zur Qualitätssteigerung) Zugang zu Informationen über Konzepte, Sicherheitsmaßnahmen, Architekturen und Rollen. Beispielsweise werden die Systemverantwortlichen oder – insbesondere bei ausgelagerten Dienstleistungen – die Betreiber in Form von Interviews und konkreten Konfigurationsprüfungen mit einbezogen. Eine White-Box-Analyse erfordert daher in der Regel auch einen höheren Zeitbedarf seitens des Auftraggebers bzw. der Betreiber. Die Prüfungsbereiche sind vielfältig und sollten vorab im Detail festgelegt werden. Beispielsweise können

- Architekturen und Konzepte,
- Konfigurationen,
- Organisatorische Maßnahmen,
- Regelungen und Arbeitsanweisungen oder die
- Angemessenheit von Maßnahmen

untersucht werden.

Bei bestimmten Fragestellungen kann ein White-Box-Ansatz aber auch effizienter Antworten liefern als eine Black-Box-Analyse. Ein Beispiel: Um zu bestimmen, ob Angriffsversuche durch Brute-Force-Angriffe[4] auf Passwörter erfolgreich sind, können im Rahmen einer Black-Box-Analyse entsprechende Angriffe auf Benutzerkonten durchgeführt werden. Derartige Angriffsversuche können durchaus mehrere Wochen Zeit erfordern. Alternativ kann man im Rahmen einer White-Box-Analyse mit den Verantwortlichen die verwendete Passwortregelung diskutieren. Die Geschwindigkeit, mit welcher sich derartige Angriffe durchführen lassen, kann durch praktische Tests in wenigen Minuten bestimmt werden. Hierdurch kann dann einfach und mit wenig Zeitaufwand berechnet werden, ob in absehbarer Zeit derartige Angriffsversuche erfolgsversprechend sind.

2 Vorgehensweise bei Audits

2.1 Referenzdokumente

Mit der Vorgehensweise bei Sicherheitsanalysen und Penetrationstests beschäftigen sich unter anderem das OSSTMM (Open Source Security Testing Methodology Manual) [1], die BSI-Studie „Durchführungskonzept von Penetrationstests" aus dem Jahr 2003 [2] und die NIST Special Publication 800-115 „Technical Guide to Information Security Testing and Assessment" [11].

OSSTMM wird oft als Vorgehensmodell im Bereich der Sicherheitsanalysen referenziert. Liest man es im Detail, kommen jedoch Unwägbarkeiten zum Vorschein. Beispielsweise ist der Detaillierungsgrad einzelner Prüfgebiete sehr unterschiedlich, und die optisch ansprechende „security map" wirkt willkürlich zusammengestellt. Das OSSTMM bietet aber einen guten Einstieg in die Systematik von Sicherheitsanalysen und kann auch als „Fundgrube" zur Erstellung von eigenen Checklisten verwendet werden.

Die BSI-Studie bietet ebenfalls einen guten Einstieg, wirkt aber an manchen Stellen recht theoretisch und komplizierter als erforderlich. Beispielsweise werden bei dem vorgeschlagenen Ablauf Kriterien wie „Informationsbasis", „Aggressivität" und „Umfang" unterschieden. Während eine Unterscheidung nach „Informationsbasis", d. h. ob man Informationen seitens des Auftraggebers erhält, sinnvoll erscheint (Black-Box vs. White-Box, siehe oben), muss bezweifelt werden, ob eine Unterscheidung in „vorsichtig", „abwägend" und „aggressiv" zielführend ist. Bei der Durchführung von Angriffen sollten diese so „echt" wie möglich angesetzt werden – schließlich wird ein potenzieller Angreifer hier auch keine Rücksicht nehmen.[5]

Lediglich bei einer Verkettungsmöglichkeit von Schwachstellen sind Einschränkungen denkbar. Kann beispielsweise ein System in einer DMZ übernommen werden, sollten potenziell weiterführende Angriffe vor deren Ausführung abgestimmt sein.

Die NIST Special Publication ist eine sehr hilfreiche und praktisch-konkrete Handreichung zur Durchführung von Information Security Audits. Alle wesentlichen Risiken einer Netzwerkinfrastruktur werden betrachtet und eine systematische Vorgehensweise für deren Analyse vorgeschlagen. Abgerundet wird das instruktive Dokument durch eine aktuelle Liste frei verfügbarer Tools und Informationsquellen über bekannte Schwächen.

2.2 Vorbereitung und Durchführung

Die folgenden acht wesentlichen Schritte werden bei der Planung und Durchführung von Audits empfohlen.

▸ **Schritt 1:** *Was soll auditiert werden?*
Auch wenn die Fragestellung einfach anmutet, ist eine eindeutige Definition und Abgrenzung des Untersuchungsgegenstands oft gar nicht so einfach. Beispiels-

4 Systematisches Durchprobieren aller Passwortkombinationen.

5 Selbstverständlich wird man auf Produktivsysteme mit sehr hohen Verfügbarkeitsanforderungen Rücksicht nehmen und ggf. auf Testumgebungen ausweichen; dennoch sollte ein Audit niemals gerade kritische Systeme aussparen.

weise spielen Firewall-Infrastrukturen und eingesetzte Betriebssysteme durchaus auch für die Sicherheit einer komplexen Applikation eine wichtige Rolle, werden oft aber nicht vom „Application Owner" (Anwendungsverantwortlichen) betrieben. Daher sollte im Detail der Gegenstand und auch der Umfang der Analysen bzw. im Umkehrschluss die Abgrenzung, was nicht untersucht werden soll, festgelegt werden.

▸ **Schritt 2:** *Was sind die konkreten Ziele des Audits?*

Die Ziele des Audits sollten zu Beginn dokumentiert und noch einmal kritisch hinterfragt werden. Soll die eigene IT oder ein Dienstleister überprüft werden? Geht es um eine Statusbestimmung und den Vergleich mit anderen Unternehmen und Institutionen? Wer ist der Initiator des Audits und welcher Zielgruppe sollen die Ergebnisse präsentiert werden? Allein aufgrund der vorgesehenen Zielgruppe, beispielsweise IT-Leiter/ Sicherheitsverantwortliche, Projektleiter/Fachverantwortliche oder Geschäftsführung/Vorstand ergeben sich gegebenenfalls unterschiedliche Schwerpunkte.

▸ **Schritt 3:** *Wie soll auditiert werden?*

Soll eine reine Black-Box-Analyse durchgeführt werden, oder ist eine Kombination Black-Box/White-Box sinnvoll? Eine Black-Box-Analyse hat nur Aussagekraft zum Zeitpunkt der Überprüfung; über Sicherheits-Prozesse wie die Aktualisierung von Systemen, Monitoring und Alerting können keine oder nur in geringem Umfang Aussagen getroffen werden. Auf der anderen Seite erhält man mit einer Black-Box-Analyse zügig und mit überschaubarem Aufwand einen ersten Eindruck über das erreichte Sicherheitsniveau.

▸ **Schritt 4:** *Definition der Prüftiefe*

Der Umfang einer Analyse hängt maßgeblich von der Prüftiefe ab. Ein einfacher Scan auch von mehreren Dutzend Servergruppen kann inklusive Auswertung in wenigen Tagen durchgeführt werden. Aufwand entsteht dabei hauptsächlich bei der Auswertung und Verifikation der Schwachstellen – und hängt damit von der Anzahl und Komplexität der festgestellten Schwachstellen ab.

Eine individuelle Analyse auch nur einer einzigen Anwendung kann dagegen, in Abhängigkeit von den gewählten Angreifermodellen und dem Umfang der gewählten Angriffsszenarien, leicht einen Aufwand von Wochen erfordern.

Im Rahmen der Prüftiefendefinition sollten auch der „Härtegrad" von technischen Angriffen sowie das Verfahren bei Feststellung erheblicher Schwachstellen festgelegt werden. Sollen beispielsweise über identifizierte Schwachstellen weitere Systeme angegriffen werden, oder wird die zeitnahe Benachrichtigung der Verantwortlichen bevorzugt, so dass die Schwachstellen mit möglichst wenig Zeitverzug behoben werden können?

Es hat sich in der Praxis als hilfreich erwiesen, Grenzen von Audits festzulegen. So sind z. B. in bestimmten Kontexten Angriffsmöglichkeiten per Social Engineering eine sehr ernst zu nehmende Gefährdung; allerdings muss im Einzelfall oft nicht der Nachweis erbracht werden, dass solche Angriffe durchführbar wären – abgesehen davon, dass derartige Angriff auch zu Unruhe in der Belegschaft führen können.

▸ **Schritt 5:** *Wann soll auditiert werden?*

Die Abstimmung geeigneter Zeiträume ist in Anbetracht gestiegener Verfügbarkeitsanforderungen und oftmals weltweitem Schichtbetrieb sehr wichtig und häufig nicht einfach. Konnten früher noch eindeutige Produktivzeiten von Nicht-Produktivzeiten unterschieden werden, so stellt sich heute oft die Herausforderung, Zeitfenster mit möglichst wenig störenden potenziellen Auswirkungen zu definieren. Besonders beachtet werden sollte die Störung weiterer Prozesse wie nächtlich durchgeführte Backup-Jobs oder automatische Batch-Verarbeitungsaufgaben.

In bestimmten Fällen, wie beispielsweise einem War-Dialing[6], muss auch die Störung von Mitarbeitern in Kauf genommen werden. Zur effektiven Projektdurchführung sollte dies vorab klar als Störung benannt und die Durchführung explizit frei geben werden.

Zusätzlich sollte man hinterfragen, ob besondere Aufgaben, wie beispielsweise Migrationen, Jahresabschluss oder sonstige größere Umstellungen, in Zielkonflikt mit dem Projekt stehen.

▸ **Schritt 6:** *Erstellung des Auditplans*

In diesem sehr wichtigen Schritt sollten mindestens die folgenden Punkte festgelegt werden:

- Details zur Vorgehensweise
- (Teil-) Aufgaben, Parallelisierung von Aufgaben, Aufgabenverteilung intern/ extern/ggf. Dienstleister
- Liste der Prüfungspunkte
- Terminplan

Zusätzlich sollten hier auch entsprechende Vorsichtsmaßnahmen zur Vermeidung/Verminderung von Störungen diskutiert werden, z. B.:

- Notfall-/Bereitschaftsnummern, Meldewege
- Backup-/Restore-Möglichkeiten
- Laufende Überwachung von automatisierten Tests

▸ **Schritt 7:** *Durchführung des Audits*

Wie Audits konkret durchgeführt werden, wird im Detail in den folgenden Abschnitten dargestellt. Die folgenden vorbereitenden Schritte sollten mindestens durchgeführt werden:

Vorbereitung seitens des Auditor-Teams:

- Checklisten
- Software/Tool-Sammlungen
- Netzzugang, Angriffssysteme, Analysesysteme etc.
- Prüfung der rechtlichen Rahmenbedingungen

Vorbereitung seitens des Auftraggebers:

- Benennung von geeigneten Ansprechpartnern
- Bereitstellung der Infrastruktur für Analysen, z. B. Netzzugang für interne Prüfungen, ggf. Clientsysteme für Untersuchungen mit Mitarbeiterberechtigungsstufe etc.
- Besprechungszimmer, Projekt-Arbeitsplätze

▸ **Schritt 8:** *Auswertung der Audit-Ergebnisse*

Die Auswertung sollte eine Vergleichbarkeit von Ergebnissen und ggf. sogar ein Benchmarking ermöglichen. Die folgenden Auswerteschritte werden für das Auditor-Team empfohlen:

- Konsolidierung und Bewertung der Feststellungen
- Abstimmung der Feststellungen („findings") mit den Interviewpartnern und Verantwortlichen, Verifikation

Die Betreiber der auditierten Systeme sollten mindestens prüfen, ob

- Angriffe anhand von Aufzeichnungen, wie z. B. Logfiles, erkannt wurden;
- die Angriffe als solche im Regelbetrieb identifiziert würden;
- geeignete Maßnahmen zur Reaktion auf Angriffe und Vorfälle definiert sind;
- die durch das Auditor-Team festgestellten Findings (Black-Box und White-

6 Automatische Prüfung von Nummern-Kreisen zur Feststellung ggf. nicht autorisierter ISDN- und Modemverbindungen.

Box) den Tatsachen entsprechen; sowie ob

- weitere Schwachstellen oder Anforderungen im Prüfungsbereich existieren, welche vom Auditor-Team ggf. noch nicht betrachtet wurden.

▸ **Schritt 9:** *Ergebnisdokumentation*

Zur Darstellung der Ergebnisse wird die Verwendung geeigneter Vorlagen empfohlen.

Da die Audit-Ergebnisse in der Regel vertraulich sind, sollten sie nur verschlüsselt und nur an autorisierte Personen übermittelt werden. Bei der Speicherung und Archivierung sollten ebenfalls angemessene Schutzmechanismen (z. B. Berechtigungskonzepte, Verschlüsselung) getroffen werden.

Wichtig ist in allen Projektphasen eine reproduzierbare Protokollierung der einzelnen Arbeitsschritte. Dies dient einerseits zum Verständnis und als Nachweis, wie einzelne Angriffe durchgeführt wurden. Andererseits können die Informationen auch für die Hersteller von Hard- und Softwarekomponenten zur Behebung festgestellter Schwachstellen von Relevanz sein.

▸ **Schritt 10:** *Ableitung von Maßnahmen und Folgeaktivitäten*

Bei der Ableitung von Maßnahmen sollten die vorhandenen und auch bereits geplanten Sicherheitsmaßnahmen berücksichtigt werden. Die mit den Verantwortlichen abgestimmten Maßnahmen sollten priorisiert und durch eine Kostenschätzung ergänzt werden. Als Maßnahmen können auch Nachprüfungen oder regelmäßig wiederkehrende Prüfungen definiert werden. Werden Audits durch externe Dienstleister durchgeführt, so sollten diese turnusmäßig, beispielsweise jährlich, getauscht werden. Dies bietet dem Auftragsgeber zum einen Vergleichsmöglichkeiten zwischen den Anbietern; zum anderen wird das Risiko einer möglichen „Betriebsblindheit" des Auditor-Teams („same procedure as every year") vermindert.

Generell wird durch ein in regelmäßigen Abständen durchzuführendes IT-Sicherheitsaudit

- die Einhaltung der getroffenen Sicherheitsmaßnahmen (technisch und organisatorisch) überprüft;
- festgestellt, ob sich wesentliche Änderungen in der IT-Infrastruktur ergeben haben, die bislang nicht sicherheitstechnisch berücksichtigt wurden, und
- beurteilt, ob die getroffenen Sicherheitsmaßnahmen weiterhin dem aktuellen Stand der Technik entsprechen.

Das Ergebnis des IT-Sicherheitsaudits kann auf der einen Seite als Testat für das realisierte Sicherheitsniveau betrachtet werden und dient auf der anderen Seite dazu, konkrete Maßnahmen zur Verbesserung der IT-Sicherheit zu identifizieren.

2.3 Black-Box-Analyse

Die meisten Audits haben die Überprüfung auf bekannte und aktuelle Schwachstellen zum Ziel. Die Identifikation bislang unbekannter „neuer" Schwachstellen ist in der Regel keine Zielsetzung. Dennoch findet man hin und wieder „nebenbei" neue Schwachstellen oder alte Schwachstellen in neuen Gewändern[7].

Im Rahmen einer Black-Box-Analyse werden die folgenden spezifischen Teilschritte durchgeführt:

▸ **Informationsbeschaffung**

Bei Angriffen über das Internet reicht in der Regel alleine der Firmenname aus, um über entsprechende Abfragen über Standard-Internetdienste wie DNS und Internetdaten¬banken wie RIPE die Ziel-Netzbereiche in Erfahrung zu bringen.

Zusätzlich können über die Webseiten des Unternehmens bzw. der Behörde oder über Suchmaschinen oft zahlreiche weitere Informationen in Erfahrung gebracht werden.

▸ **Portscans**

Die Kommunikation der verschiedenen Anwendungen wie E-Mail oder WWW erfolgt über Internet-Protokolle, wie SMTP und HTTP, welche oft definierte Standardverbindungen („Ports") verwenden. Um Dienste und Systeme angreifen zu können, muss eine Kommunikation mit diesen Ports möglich sein. Fast immer gilt: „Wo kein Dienst (Port) zur Verfügung gestellt wird, ist kein Angriff möglich"[8].

Um festzustellen, welche Dienste und Versionen der Dienste auf welchen Ports betrieben werden („Fingerprinting"[9]), können mit so genannten Portscannern[10] in kurzer Zeit durch Kommunikationsversuche geöffnete Ports festgestellt werden. Die Vorgehensweise dabei ist vergleichbar mit einem systematischen Durchrütteln aller Haustüren in einer Straße, um festzustellen, welche Türen nicht verschlossen sind.

Heute gehören (automatisierte) Portscans zum „Grundrauschen" im Internet. Vor Jahren noch konnte ein Portscan als Vorstufe zu einem Angriff gewertet werden; heute dürfte das Fehlen von Portscans am Internet-Zugangsrouter oder Firewall-Systemen eher auf eine gestörte Verbindung hinweisen. Es sollte also beachtet werden, dass sich im Verlauf der Zeit durchaus die Einstufung bestimmter Angriffsszenarien ändern kann.

▪ Security Scans („Sicherheits-Scans")

Security Scans bezeichnen die Durchführung von Schwachstellenanalysen mit automatisierten Tools und Programmen. Sie können heutzutage auch von weniger erfahrenden Anwendern und insbesondere auch von den so genannten „Skript-Kiddies" durchgeführt werden.

Eine Verschärfung der Bedrohungslage ist zum einen durch eine gesteigerte Komplexität der Angriffe einerseits und die einfache Benutzbarkeit von Angriffstools andererseits gegeben.

Ein Beispiel für Angriffstools ist der Security-Scanner Nessus. Nessus wurde ursprünglich als OpenSource-Projekt entwickelt und ist seit 2008 ein kommerzielles Produkt. Eigenschaften von Nessus sind zum einen die automatisierte Prüfung von inzwischen über 20.000 bekannten Schwachstellen; zum anderen stellt Nessus auch Schnittstellen zur Integration eigener Überprüfungen mit Hilfe einer Skriptsprache bereit. Die Bedienung erfolgt einfach per Mausklick; weiter gehende Kenntnisse über die Techniken der Angriffe und Schwachstellen sind nicht erforderlich. Es gibt eine ganze Reihe von weiteren spezifischeren Tools zur Durchführung von Überprüfungen und Ausnutzung von Schwachstellen.[11]

Generell ist bei allen Analysen eine systematische Vorgehensweise sehr wichtig. So sollten beispielsweise Systeme nicht ausschließlich über das Internet geprüft werden. Zusätzlich sollten Zugangswege vom LAN in Richtung DMZ und Internet

7 Zahlreiche festgestellte Schwachstellen sind eine Wiederholung von bereits vor Jahren festgestellten Fehlern. Ursache sind oft fehlerhafte Prozesse in der Softwareentwicklung.

8 Es gibt wenige bekannte Ausnahmen. Beispielsweise gelangen in manchen Fällen Angriffe auf nur passiv lauschende Intrusion-Detection-Systeme.

9 Zusätzlich können in vielen Fällen auch die Versionen der eingesetzten Betriebssysteme und weiterer Software-Module in Erfahrung gebracht werden.

10 Bekannte Scanner sind Nmap und Superscan.

11 Eine Übersicht der interessantesten Tools findet sich unter http://www.sectools.org/.

(ausgehende Verbindungen) und insbesondere Verbindungsmöglichkeiten von der DMZ in Richtung weiterer DMZs bzw. des LAN geprüft werden. Weitere Untersuchungen sollten innerhalb der jeweiligen DMZs erfolgen. Auf diese Weise wird geprüft, welche Möglichkeiten ein Angreifer bei Übernahme eines oder mehrerer DMZ-Systeme hätte und ob weitere Sicherheitsbrüche durch die Verkettung von Schwachstellen möglich wären. In der folgernden Abbildung sind diese und weitere Überprüfungen intern und per Remote Access, ggf. auch VPN, eingezeichnet.

Die Durchführung von manuellen Überprüfungen wird unbedingt empfohlen, auch wenn hierfür teilweise ein recht hoher Aufwand betrieben werden muss. Die Aufwände für automatisierte Prüfungen skalieren hierzu im Vergleich in der Regel recht gut, d. h. der Arbeitsaufwand um z. B. 60 Systeme automatisiert zu überprüfen, ist nicht doppelt so hoch wie der für 30 Systeme erforderliche; anders sieht es aus, wenn festgestellte Schwachstellen verifiziert und weitere Schwachstellen recherchiert und untersucht werden sollen.

Eine manuelle Verifikation ist außerdem erforderlich, da die automatisierten Programme produktabhängig mal mehr und mal weniger „false positives" liefern – „Fehlalarme", also Schwachstellen, die tatsächlich nicht vorhanden sind.

Nachdem Dienste, Versionen und Module in Erfahrung gebracht wurden, wird zusätzlich empfohlen, weitere Angriffsmöglichkeiten bei einschlägigen Internetdatenbanken zu recherchieren.[12]

Die identifizierten Schwachstellen sollten nach ihrem Schweregrad[13], z. B. niedrig, mittel, hoch, aufgeführt werden, wobei der Bewertung durch automatisierte Scanner nicht immer gefolgt werden kann.

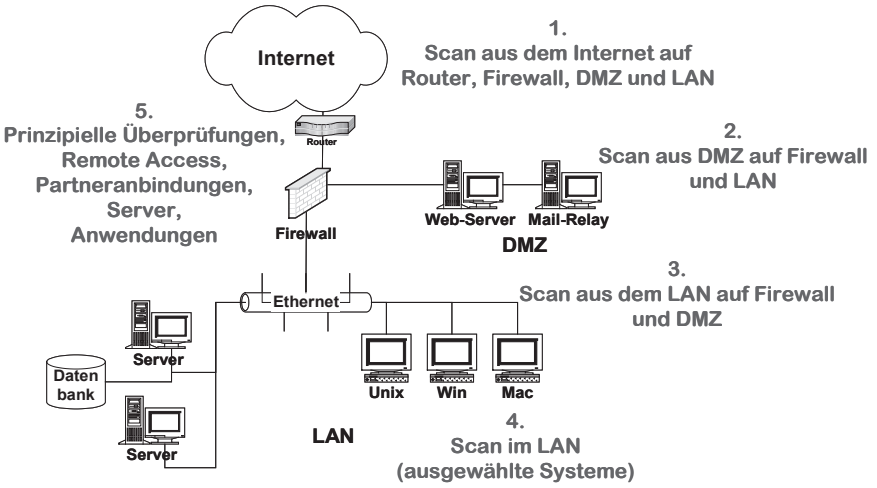
Ein Kritikpunkt rein automatisierter Prüfungen ist, dass durch die Scan-Programme oft nur eine Aussage in Form von „Das System könnte übernommen werden" getroffen wird. Zur aussagekräftigen Bewertung ist zum einen eine technische Betrachtung der Schwachstelle erforderlich (Wie funktioniert sie? Ist sie eine theoretische Angriffsmöglichkeit, oder kann eigener Code ausgeführt werden?) und zum anderen die Recherche, Erstellung oder Anpassung von Angriffscode per Skript oder Exploit[14]. Erst dann kann eine fundierte Aussage darüber getroffen werden, ob das System wirklich übernommen werden kann. Diese Untersuchungen können einigen Aufwand erfordern.

Für eine ganze Reihe von Angriffsszenarien existieren keine oder nur mit größeren Anpassungen benutzbare Tools. So sollte bei Individualsoftware eine Untersuchungen der Protokolle, Benutzerverwaltung, Rollen, Authentifizierung etc. durchgeführt werden. Zur Steigerung der Effektivität bietet es sich an, für gleichartige Aufgaben Skripte zu erstellen und einzusetzen.

In vielen Fällen ist Kreativität gefragt: „Womit rechnet die Applikation nicht?", oder besser „Womit haben die Entwickler nicht gerechnet?". Beispielsweise findet man es immer noch häufig, dass Authentisierungsdaten in einem Link übergeben werden – und somit einfach durch Durchprobieren unter Berücksichtigung der Syntax zu fremden Benutzerkonten führen. Ebenso entsprechen eingesetzte Verschlüsselungsverfahren oft nicht dem Stand der Technik.

Eine Aufzählung sämtlicher Untersuchungsmöglichkeiten würde den Rahmen dieses Beitrags sprengen, daher zusammenfassend der Tipp: „Rechnen Sie mit dem Unmöglichen" und versuchen Sie, sich bestmöglich in einen raffinierten Angreifer zu versetzen.

Abbildung 1 | Schema Sicherheits-Scans und manuelle Überprüfung



2.4 Grey-Box-Analyse

Die Durchführung von Grey-Box-Analysen entspricht im Wesentlichen der von Black-Box-Analysen. In vielen Fällen können im direkten Vergleich zu einem reinen Black-Box-Ansatz bei Vorlage bestimmter Informationen Analysen zielführender und effizienter durchgeführt werden. Es sollte hierbei nur beachtet werden, dass der Nachweis erbracht werden kann (erfordert eine saubere und umfassende Dokumentation), dass das Auditor-Team die Informationen auch selbst hätte beschaffen können.

2.5 White-Box-Analyse

Ziele einer White-Box-Analyse sind in der Regel die Überprüfung der Sicherheitsarchitekturen und –infrastrukturen, das Aufdecken von Schwachstellen mit technischem oder organisatorischen Bezug, sowie die Feststellung von Maßnahmen zur Behebung der Schwachstellen bzw. eine Verminderung der potenziell schädlichen Auswirkungen.

Im Gegensatz zu einer Black-Box-Analyse erfordert eine White-Box-Analyse die Beteiligung der Verantwortlichen und Betreiber der auditierten Umgebung, wobei diese dem Auditor-Team umfassende Informationen zur Verfügung stellen. Bereits vorhandene interne Kenntnisse über Optimierungsmöglichkeiten werden berücksichtigt und ggf. weitere Informationsquellen genutzt, wie beispielsweise

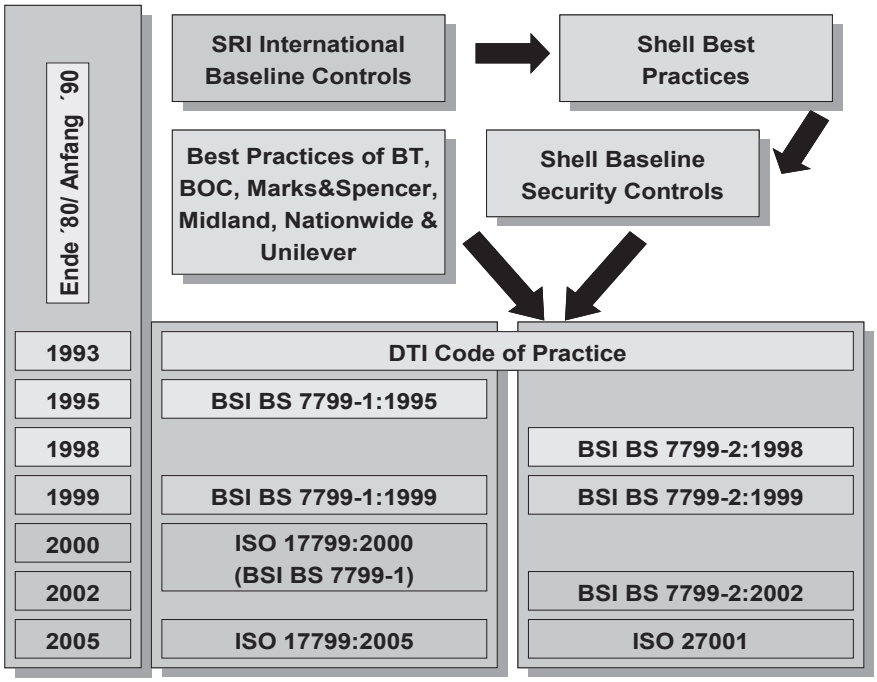
- technische Betriebshandbücher und Konzepte
- Organigramme und Organisationsabläufe

12 Wie beispielsweise cve.mitre.org, xforce.iss.net oder auch Exploits, z. B. bei www.securiteam.com.

13 Kriterien hierfür können sein, ob ein System oder Dienst nachhaltig gestört, außer Funktion gesetzt oder sogar übernommen werden kann.

14 Inzwischen gibt es benutzerfreundliche Exploit-Frameworks, wie Metasploit oder das kommerzielle Produkt Core Impact, die auch automatisiert Schwachstellen und Exploits ausnutzen können.

Abbildung 2 | Historische Entwicklung BS 7799/ISO 17799/ISO 27001 [6, 7]



- Prozessdokumentationen (z. B. ITIL-Framework, Schnittstellenmatrizen Technik und Geschäftsprozesse)
- Service Level Agreements
- Audit- und Revisionsberichte
- Dokumentations-Anwendungen (Dokumenten-Management, Help Desk Fälle/Tickets)
- Datenbanken (Asset-Datenbanken, Incident-Datenbanken etc.)

Da eine White-Box-Analyse – auch hinsichtlich des erforderlichen Aufwands – schwieriger abzugrenzen ist als eine Black-Box-Analyse, sollten in der Vorbereitungsphase ausreichende Informationen über den Prüfungsgegenstand und die Prüfungsfelder vorliegen. Folgendes sollte genau definiert werden:

- Prüfungsfelder und Prüfungsgegenstand
- Prüftiefe, ggf. Stichprobenverfahren und Abgrenzungen
- Prüftechniken (Interviews, Konfigurationsprüfungen, Dokumentensichtung etc.)
- Prüfplan (Vorgehensweise, Ansprechpartner, Termine)

Ebenso sollte festgelegt werden, wie mit den Feststellungen umgegangen wird und in welcher Form die Ergebnisse dargestellt werden sollen.

3 Audits auf Basis von Standards

Für den Aufbau eines IT-Sicherheitsmanagements, einer IT-Sicherheitsorganisation und die Erstellung eines IT-Sicherheitskonzepts gibt es eine Reihe von Standards, die als Orientierung herangezogen werden können. Diese Standards können auch für Audits eingesetzt werden.

Als Ergebnis eines auf Standards basierenden Audits erhält man einerseits die Aussage, wie „compliant" – also standardkonform – ein Unternehmen oder eine Behörde aufgestellt ist, und zum anderen, welche Maßnahmen noch getroffen werden müssen, um die Anforderungen des für den Untersuchungsbereich gewählten Standards zu erfüllen („Gap-Analyse").

In den Bereichen IT-Sicherheit und Informationssicherheit werden vor allem BS 7799/ISO 17799/ISO 27001 [8-10] und das IT-Grundschutzhandbuch des BSI für Audits verwendet. Weitere Standards, wie z. B. ISO 20000, ITIL und SAS-70, spielen in der Praxis auch eine Rolle, werden hier aber nicht weiter vertieft.

3.1 Audits auf Basis ISO 17799/BS 7799/ISO 27001

Der internationale Standard ISO 17799 entstand aus dem British Standard BS 7799-1 und stellt eine umfassende Sammlung von „Best Practices" zum Thema Management von Informationssicherheit dar. Er eignet sich daher sehr gut für Audits mit dem Fokus Sicherheitsorganisation und Sicherheitsmanagement.

ISO 27001 ist der internationale Nachfolger von BS 7799-2 und beschreibt den Aufbau eines Information Security Management System (ISMS) [6, 7]. Im Gegensatz zu ISO 17799 und BS 7799-1 ist eine Zertifizierung möglich. Auch dieser Standard eignet sich für Audits, wobei der Schwerpunkt hierbei nicht auf der Umsetzung bestimmter Maßnahmen, sondern in der Etablierung von Prozessen liegt.

Prinzipiell können folgende Ansätze gewählt werden:

- Wenn als Schwerpunkt ein Information Security Management System, also Prozesse zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit geprüft werden sollen, wird man BS 7799-2 oder ISO 27001 als Grundlage wählen. Schwerpunkt hier ist die Betrachtung von Prozessen und Vorgehensweisen wie dem PDCA-Modell (plan do check act). Eine Zertifizierung ist möglich.
- Wenn der Schwerpunkt die Überprüfung von organisatorischen Maßnahmen ist, eignen sich BS 7799-1 und ISO 17799/27002[15] sehr gut. Sinnvolle „Best Practice"-Ansätze sind in Form von Managementgebieten („clauses"), Maßnahmenkategorien („main security categories") und auch in Einzelmaßnahmen („baseline controls") dargestellt. Diese können recht gut abgeprüft werden; eine Zertifizierung ist nicht möglich.

In beiden Fällen ist es sinnvoll, mit standardisierten Checklisten zu arbeiten, Auswertungen können beispielsweise durch die Verwendung von Excel oder dedizierten Tools vereinfacht werden.

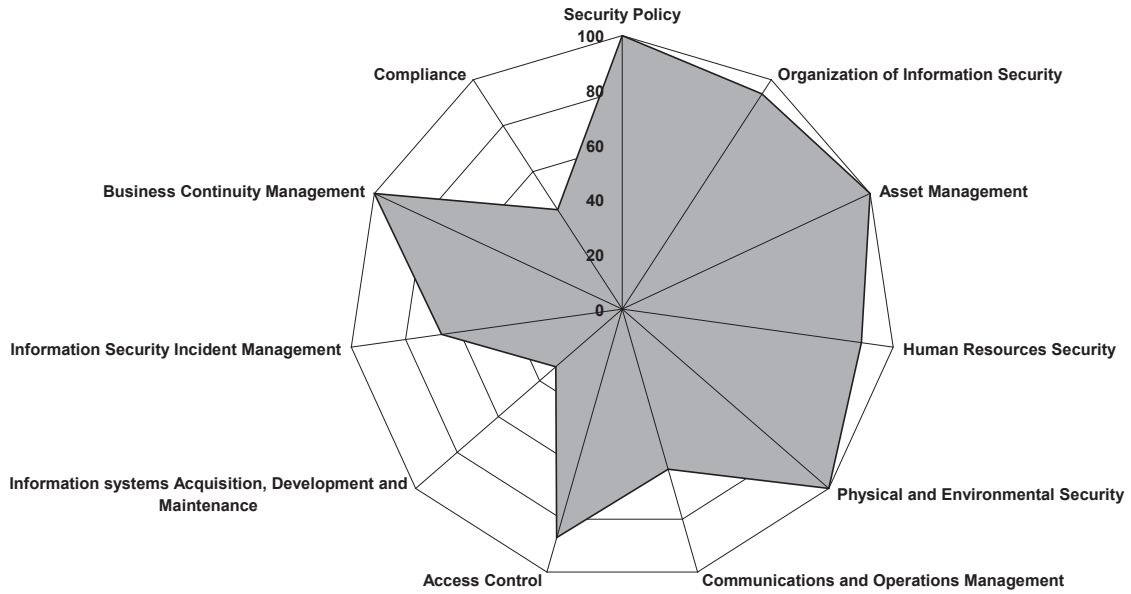
Da in vielen Fällen ein Audit durchgeführt wird, um einen ersten Überblick zu erhalten oder auch um Tendenzen beispielsweise von Jahr zu Jahr erkennen zu können, ist eine Auswertelogik mit komplexem Bewertungsschema der jeweiligen Einzelfragen meist nicht zielführend.

Zur Vereinfachung können beispielsweise die in ISO 17799 /27002 definierten Einzelmaßnahmen gleich bewertet werden.[16] Eine Anpassung und Entwicklung

15 ISO 27002 ist der Nachfolger von ISO 17799 und wurde 2007 veröffentlicht.

16 Werden beispielsweise in einer Maßnahmenkategorie sieben Einzelmaßnahmen abgeprüft, von

Abbildung 3 | Ergebnisdarstellung nach Erfüllungsgrad



eines individuellen Bewertungsschemas ist für Unternehmen und Behörden möglich, es sollte aber hierbei beachtet werden, dass eine fortlaufende Anpassung an ggf. sich ändernde Anforderungen einigen Aufwand erzeugen kann.

In der folgenden Grafik ist zusammenfassend die Ergebnisse eines Audits auf Basis von ISO 17799:2005 aufgetragen. Für das jeweilige Management Gebiet ist der Erfüllungsgrad angegeben.

Man erkennt durch diese Darstellung recht einfach die Gesamtabdeckung und Bereiche mit niedrigem Erfüllungsgrad. Ein Soll-Zustand, z. B. Abdeckung von mindestens 80 % in allen Management-Gebieten, könnte definiert werden und auch eine zeitliche Darstellung, welche beispielsweise einen Vergleich zum Vorjahr ermöglicht, könnte durch Nutzung verschiedener Farben vorgenommen werden.

Durch Compliance-Audits, beispielsweise wie oben dargestellt auf Basis von ISO 17799, kann in der Regel nur ein Erfüllungsgrad bezüglich den Vorgaben des Standards bestimmt werden. Es wird nicht überprüft, ob die Umsetzung von Maßnahmen angemessen ist. Dies wäre nur möglich, wenn das Unternehmen oder die Behörde auf Basis von allgemeinen Standards durch Anpassung an das erforderliche Sicherheitsniveau eigene Standards definiert hätte. Dies ist in der Praxis selten der Fall. Das Auditor-Team sollte daher in der Lage sein, mit Augenmaß auch die Angemessenheit von Maßnahmen abzuschätzen.

Bei einer Auditierung, beispielsweise auf Basis von ISO 27001, wird abgefragt, welche Prozesse definiert sind. Es wird aber nicht hinterfragt, ob die Prozesse als solche auch sinnvoll sind und wirkungsvoll ineinander greifen.

3.2 Audits auf Basis von IT-Grundschutz

Das IT-Grundschutzhandbuch des BSI bietet wertvolle Unterstützung bei der Erstellung von Sicherheitskonzepten. Im Vergleich zu anderen Standards ist es recht umfangreich (> 3.000 Seiten) und bietet umfassende und konkrete Maßnahmenbeschreibungen. Die wesentlichen Vorgehensweisen zur Erstellung eines Sicherheitskonzepts und der Aufbau von ISMS sind in den BSI-Standards 100-x beschrieben [3, 4].

Die IT-Grundschutz-Kataloge [5], bestehend aus den so genannten Baustein-, Gefährdungs- und Maßnahmen-Katalogen, stellen umfangreich technische und organisatorische Informationen zusammen. Sie können daher sehr gut auch als Prüfkatalog oder Prüfplan verwendet werden. IT-Grundschutz eignet sich als Grundlage zur Prüfung des IT-Sicherheitsmanagement (ISO 27001), der Sicherheitsorganisation sowie organisatorischer und technischer Maßnahmen. Eine Zertifizierung nach IT-Grundschutz ist möglich.

Audits auf Basis von IT-Grundschutz sind in der Regel reine White-Box-Analysen, welche in Form von Interviews, Fragebögen und technischen (Konfigurations-) Prüfungen durchgeführt werden. Zusätzlich bietet das IT-Grundschutzhandbuch auch Inhalte, welche für Checklisten oder eine Prüfung von Dokumentationen einsetzbar sind.

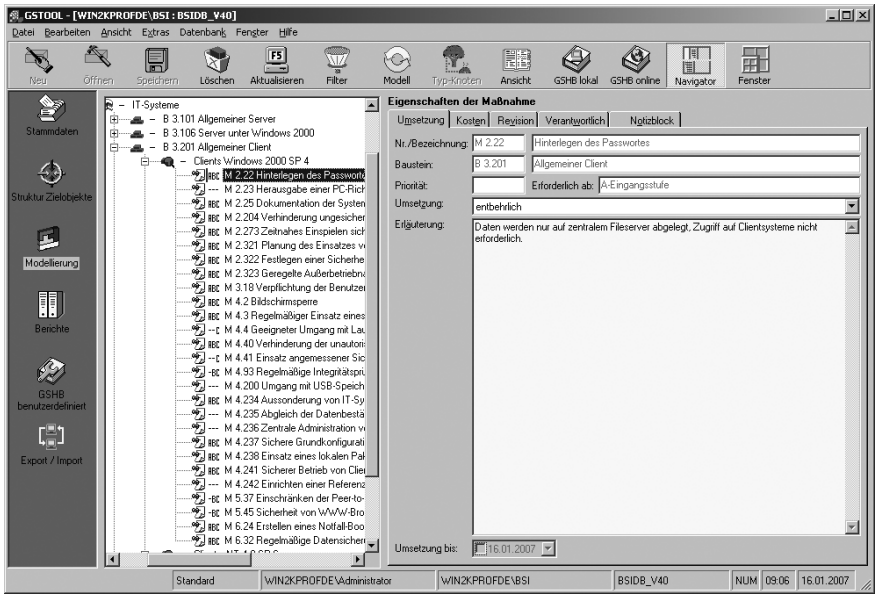
Die wesentliche Fragestellung vor der Durchführung eines Audits ist die Klärung der Zielsetzung. Soll das Audit als „Self-Assessment" zur Beurteilung des gebotenen Sicherheitsniveaus bzw. Abdeckung des Erfüllungsgrads der Maßnahmen durchgeführt werden, oder wird eine Zertifizierung nach IT-Grundschutz angestrebt?

Das Prüfschema, die Vorgehensweise und Zertifizierungsstufen – Auditor-Testat Einstiegsstufe, Auditor-Testat Aufbaustufe und ISO 27001-Zertifikat auf Basis von IT-Grundschutz – sind auf den Webseiten des BSI beschrieben, ebenso erfolgreich abgeschlossene Zertifizierungen. Die Erstellung von Auditor-Testaten und die Zertifizierung muss durch einen vom BSI lizenzierten Auditor erfolgen.

Die zweite wichtige Fragestellung bei Audits auf Basis von IT-Grundschutz ist die Definition und Abgrenzung des Un-

welchen vier vollständig umgesetzt sind und die restlichen drei nicht, so ergibt sich ein Erfüllungsgrad von 4/7 = 57 %. Eine gewisse Verfälschung ist gegeben, da Maßnahmen unterschiedlich wichtig sind und auch die Anzahl von Einzelmaßnahmen pro Maßnahmenkategorie variiert.

Abbildung 4 | Einsatz des GS-Tools bei Audits auf Basis von IT-Grundschutz



tersuchungsgegenstandes. Soll ein vollständiger „IT-Verbund“[17] überprüft werden, oder soll das Grundschutzhandbuch exemplarisch für bestimmte Aufgabenstellungen, z. B. Infrastrukturkomponenten oder Systeme, eingesetzt werden?

Zur Unterstützung der Erstellung von Sicherheitskonzepten auf Basis von IT-Grundschutz wurde im Auftrag des BSI ein Grundschutz-Tool entwickelt. Dieses bietet wie auch die Tools weiterer Anbieter die Möglichkeit, Strukturobjekte, Bausteinzuordnungen und insbesondere den Umsetzungsgrad von Maßnahmen zu erfassen. Es kann daher auch sehr gut bei der Durchführung von Audits und der Erstellung von Berichten eingesetzt werden:

Auch die Erstellung von Berichten wird durch das Tool vereinfacht, z. B. um Maßnahmen aufzuführen, welche für das Erreichen einer bestimmten Zertifizierungsstufe noch erforderlich wären.

Die BSI-Standards und das IT-Grundschutzhandbuch bieten eine sehr gute Grundlage zur Durchführung von Audits. Durch die Darstellung definierter und systematischer Vorgehensweisen und Maßnahmen ist ein eindeutiger Soll-Zustand vorgegeben, gegen welchen geprüft werden kann. Durch den Einsatz von Tools können Audits recht effizient durchgeführt werden.

Der Umfang von Audits hängt stark vom definierten IT-Verbund ab; eine vollständige Analyse komplexer IT-Verbünde erfordert hohe Aufwände.

Da nur Grundschutz-Niveau, also ein „normaler“ (BSI-Definition) Schutzbedarf abgedeckt ist, gibt es keine detaillierten Vorgaben zur Prüfung von Maßnahmen für hohen oder sehr hohen Schutzbedarf. Die Prüfung komplexer Infrastrukturen und Architekturen stehen ebenso nicht im Fokus wie ein Abgleich mit spezifischen Sicherheitsanforderungen (Hardening-Profile, Best-Practice Ansätze). Es wird empfohlen, falls derartige Bereiche zum Untersuchungsgegenstand gehören, keine „reine“ Grundschutz-Auditierung durchzuführen.

4 Praxishinweise

Die folgenden Schritte haben sich bei der Durchführung von Audits in der Praxis bewährt („**V**iersprung **d**es **e**rfolgreichen **A**udits“):

- **V**orbereitung
- **D**urchführung
- **E**rgebnisdokumentation
- **A**bleitung Maßnahmen

Im Folgenden sind noch einzelne Anmerkungen zu weiteren wichtigen Punkten zusammengestellt.

4.1 Organisation

Die Aufwände zur Vorbereitung und Abstimmung von Ergebnissen und Maßnahmen sollten nicht unterschätzt werden. Je gründlicher ein Audit vorbereitet wurde, desto weniger Probleme werden bei der Durchführung auftreten.

Auch der Ressourcenbedarf bei Betreibern und Verantwortlichen des Untersuchungsgegenstands wird oft unterschätzt. Durch eine vorausschauende Zeitplanung lassen sich in der Regel Stresssituationen vermeiden und die Durchführung optimieren.

4.2 Dokumentation

Ein sehr wichtiger Punkt ist die saubere Dokumentation von Audits. Diese kann nicht nebenbei erfolgen, sondern nimmt einen hohen Stellenwert und auch Ressourcen-Posten bei Audits ein.

Die Vorgehensweise und Ergebnisse eines Audits müssen umfassend dokumentiert werden. Nur so kann nachvollzogen werden, wie das Auditor-Team zu seinen Bewertungen kommt und in welchen Bereichen ein hohes Kosten-Nutzen-Verhältnis für Maßnahmen gegeben ist.

Die Darstellung sollte immer an der vorgesehenen Zielgruppe und deren Bedürfnissen ausgerichtet werden.

4.3 Personal

Für Audits sollte fachlich qualifiziertes Personal eingesetzt werden. Die folgenden Lizenzierungen können – neben der nachzuweisenden Erfahrung – einen Hinweis auf die Qualifikaiton der Auditoren geben:

- BSI-lizenzierter IT-Grundschutz Auditor
- ISO 27001 Auditor auf Basis von IT-Grundschutz
- BS 7799 Lead Auditor
- CISA
- CISM
- T.I.S.P.

4.4 Maßnahmen zur Qualitätssteigerung

Um eine hohe Audit-Qualität zu erzielen, sollten von Beginn an Mindestanforde-

17 Die Definition des zu prüfenden IT-Verbunds kann vom Auftraggeber des Audits vorgenommen werden, wobei für die Testate und die Zertifizierung bestimmte Eigenschaften, wie eine sinnvolle Abgrenzung und Mindestgröße, erforderlich sind. Der IT-Verbund kann das gesamte Unternehmensnetzwerk, ein relevanter Teilbereich, aber auch ein Fachverfahren sein. Das BSI unterstützt vorab Fragestellungen zur Zertifizierungsmöglichkeit eines spezifizierten IT-Verbunds.

rungen an die Qualitätssicherung und weitere Maßnahmen zur Steigerung der formalen und inhaltlichen Qualität definiert werden. Es wird empfohlen

- inhaltliche Diskussionen mit mehreren erfahrenden Teilnehmern sowohl beim Auditor-Team als auch bei Mitarbeitern des Untersuchungsgegenstands vorzusehen,
- wichtige Zwischenschritte als Meilenstein im Projektplan zu definieren und für die Dokumente Peer-Review Prozesse vorzusehen, sowohl innerhalb des Auditor-Teams (Qualitätssicherung) als auch zwischen Auditor-Team und Kunde (Verständlichkeit, Randbedingungen, Stileigenschaften der Darstellung abgestimmt auf Unternehmenskultur[18]),
- Regelungen zur Versionierung von Berichten, Arbeitsdokumenten und weiteren Datenträgern zu treffen,
- in jedem Arbeitsschritt die Reproduzierbarkeit der Ergebnisse zu hinterfragen (Würde ein anderes Auditor-Team zu vergleichbaren Ergebnissen kommen?) und
- bei der Definition die Maßnahmen die Wirtschaftlichkeit und Wirksamkeit kritisch zu prüfen.

4.5 Datenschutz und rechtliche Rahmenbedingungen

Bei der Durchführung von Audits können auch Mitarbeiter in ihren Persönlichkeitsrechten betroffen sein. Es wird empfohlen, bereits in der Planungsphase des Audits die Mitbestimmungsrechte von Betriebsrat bzw. Personalrat zu beachten und diese bei den Audits mit einzubeziehen.

Weitere rechtliche Rahmenbedingungen sollten – ggf. in vertraglicher Form – durch einen Juristen geregelt werden.

5 Ausblick

Je genauer die Vorgaben zu Vorgehensmodell, Prüfungs-Plan und Audit-Bericht, desto präziser werden die Einzelergebnisse sein. Man sollte also vorab die Zielsetzung eines geplanten Audits genau festlegen, um geeignete Ergebnisse zu erzielen. Eine hohe Ergebnisqualität erfordert eine systematische Vorgehensweise.

18 Im Rahmen eines Audits werden Tatsachen festgestellt, die möglichst neutral dargestellt werden müssen. Wie die Ergebnisse präsentiert werden, sollte aber abgestimmt werden. In den meisten Fällen werden es Vorstände und Geschäftsführer begrüßen, wenn Sachverhalte exakt so dargestellt werden, wie sie sind. Auf Beschönigungen sollte verzichtet werden.

Literatur

[1] Institute For Security And Open Methodologies: *Open-Source Security Testing Methodology Manual*, http://www.isecom.org/osstmm/

[2] BSI: *Durchführungskonzept von Penetrationstests*, Studie, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf

[3] BSI: *Managementsysteme für Informationssicherheit (ISMS)*, BSI-Standard 100-1, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/literat/bsi_standard/standard_1001.pdf

[4] BSI: *IT-Grundschutz-Vorgehensweise*, BSI-Standard 100-2, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/literat/bsi_standard/standard_1002.pdf

[5] BSI: *IT-Grundschutz-Kataloge*. November 2007, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/gshb/deutsch/index.htm

[6] Völker, Jörg: *BS 7799 – Von "Best Practice" zum Standard*, White Paper Secorvo, http://www.secorvo.de/whitepapers/secorvo-wp10.pdf

[7] Völker, Jörg: *BS 7799 – Von „Best Practice" zum Standard*. DuD 2/2004, S. 102-108.

[8] ISO/IEC 17799:2000, International Organization for Standardization, http://www.iso.org/

[9] ISO/IEC 17799:2005, International Organization for Standardization, http://www.iso.org/

[10] ISO 27001:2005, International Organization for Standardization, http://www.iso.org/

[11] National Institute of Standards and Technology: Technical Guide to Information Security Testing and Assessment http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[12] ISO 27002:2007, International Organization for Standardization, http://www.iso.org/