Kapitel 11

Evaluierung und Zertifizierung von VPNs

Vor der Anschaffung eines VPN stellt sich Kunden und Benutzern die Frage, welche Sicherheitskriterien es wirklich erfüllt.

Mit dem Mittel der Evaluation kann überprüft werden, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen. Ziel der Evaluierung ist, dem Anwender des Sicherheitssystems das Vertrauen zu geben, dass das VPN-System ordnungsgemäß und wunschgemäß arbeitet.

Ein Kunde oder Benutzer kann die Evaluation eines VPN selbst durchführen oder von einem Spezialisten durchführen lassen. Eine Evaluation selbst durchzuführen, scheitert oft an der fehlenden Fachkenntnis oder dem damit verbundenen enormen Aufwand.

Die Alternative besteht darin, die Evaluation durch eine kompetente und unabhängige Stelle durchführen zu lassen. Ein von Experten aufgrund einer durchgeführten Evaluation vergebenes Zertifikat bietet Kunden und Benutzern einen Maßstab bei der Bewertung unterschiedlicher VPNs. Die Evaluation erfolgt dabei nach definierten Kriterien.

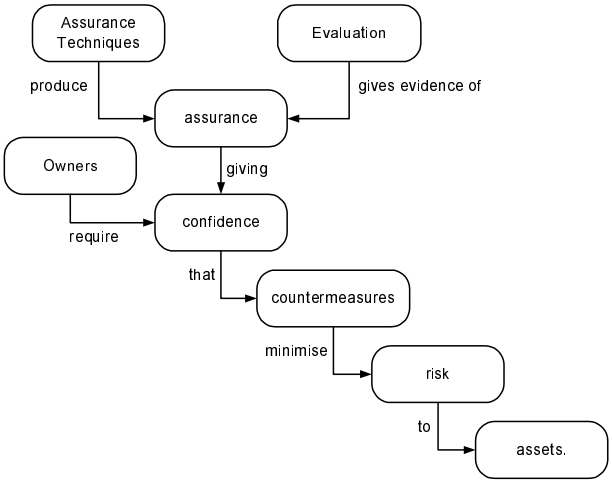

Abb. 11.1: Evaluierung und Zertifizierung

Zur Durchführung der Evaluierung und Zertifizierung von VPNs gibt es verschiedene Möglichkeiten. In den folgenden Abschnitten wird exemplarisch das bekannteste Zertifizierungsverfahren dargestellt, die Zertifizierung nach ITSEC. Zugleich wird die in der Praxis erreichbare »Tiefe« der Bewertung der beiden Verfahren beschrieben.

11.1 ITSEC-Zertifizierung

Die ITSEC (Information Technologie Security Evaluation Criteria) wurden von Frankreich, der Bundesrepublik Deutschland, den Niederlanden und Großbritannien auf der Grundlage von existierenden nationalen IT-Sicherheitskriterien [CESG3, DTIEC, SCSSI, ZSIEC, TCSEC] erarbeitet. Für eine Harmonisierung der unterschiedlichen Kriterien sprach die Forderung der Industrie, die in den verschiedenen Ländern verschiedene Sicherheitskriterien vorfand, und zum anderen der Vorteil, den sich die Beteiligten davon versprachen, die in den unterschiedlichen Ländern gesammelten Erfahrungen gemeinsam gewinnbringend zu nutzen.

Die erarbeiteten Kriterien stellen die Grundlage für eine Zertifizierung durch die nationalen Zertifizierungsstellen dar, die nach diesen Kriterien erstellte Zertifikate gegenseitig anerkennen.

Eine Zertifizierung kann sowohl vom Hersteller als auch vom Vertreiber eines VPN beantragt und durchgeführt werden. Der Vorteil einer vom Hersteller beantragten Zertifizierung liegt darin, dass die notwendigen Unterlagen bereits vorhanden sind und nicht erst erstellt werden müssen. Der mit dem Zertifizierungsprozess verbundene Aufwand ist allerdings sehr hoch. Die Zertifizierung durch einen Vertreiber lohnt nur bei einer niedrigen Evaluationsstufe, da dem Vertreiber die entsprechenden Sourcen (zum Beispiel für die Software) nicht zur Verfügung stehen.

Im folgenden wird exemplarisch dargestellt, welche Unterlagen vom Hersteller beziehungsweise Entwickler bereitzustellen sind und welche Tests durchgeführt werden müssen, um eine Zertifizierung nach Stufe E3 zu erreichen.

Neben dem Hersteller beziehungsweise Entwickler und der Zertifizierungsstelle ist eine akkreditierte Prüfstelle an der Evaluierung beteiligt. Die Prüfstelle (Prüflabor) führt die erforderlichen technischen Prüfungen im Auftrag des Herstellers unter Aufsicht der Zertifizierungsstelle durch und erstellt die jeweiligen Prüfberichte. Abschließend wird von der Zertifizierungsstelle ein Zertifizierungsreport mit allen Ergebnissen erstellt und veröffentlicht. Ergebnisse im Zertifizierungsreport sind beispielsweise die Beschreibung der Bedrohungen, denen das VPN entgegenwirkt, die Liste der implementierten Sicherheitsmechanismen, Angaben zur genauen technischen und organisatorischen Einsatzumgebung des VPN und Restrisiken unter bestimmten Voraussetzungen.

Die Evaluation erfolgt unter den Aspekten Korrektheit und Wirksamkeit. Bei der Bewertung der Korrektheit wird untersucht, ob die sicherheitsspezifischen Funktionen und Mechanismen korrekt implementiert wurden. Bei der Bewertung der Wirksamkeit wird beurteilt, ob die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des VPN die vorgegebenen Ziele tatsächlich erreichen. Zusätzlich wird die Fähigkeit der Sicherheitsmechanismen bewertet, Widerstand gegen einen direkten Angriff zu leisten (Stärke der Sicherheitsmechanismen).

Die für die Bewertung der Korrektheit erforderlichen Unterlagen, die der Hersteller beziehungsweise Vertreiber zur Verfügung stellen muss, sind:

- die informelle Beschreibung der Architektur des VPN
- die informelle Beschreibung des Feinentwurfs des VPN
- die Testdokumentation
- die Bibliothek der Testprogramme und -werkzeuge, die für den Test des VPN benutzt wurden
- Der Quellcode beziehungsweise die Hardware-Konstruktionszeichnungen für alle sicherheitspezifischen und sicherheitsrelevanten Komponenten
- die informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode beziehungsweise Hardware-Konstruktionszeichnungen und Feinentwurf darstellt
- die Konfigurationsliste, die eindeutig die Version des VPN identifiziert
- die Informationen über das Konfigurationskontrollsystem
- die Informationen über das Abnahmeverfahren
- die Informationen über die Sicherheit der Entwicklungsumgebung
- die Beschreibung aller benutzten Implementierungssprachen
- die Benutzerdokumentation
- die Systemverwalter-Dokumentation
- die Auslieferungs- und Konfigurationsdokumentation
- die Anlauf- und Betriebsdokumentation

Folgende Unterlagen des VPN müssen unter dem Aspekt der Wirksamkeit zur Verfügung gestellt werden:

- die Analyse der Eignung der Sicherheitsmechanismen
- die Analyse des Zusammenwirkens der Sicherheitsmechanismen
- die Analyse der Stärke der Sicherheitsmechanismen des VPN
- die Liste der bekannten Schwachstellen in der Konstruktion
- die Analyse der Benutzerfreundlichkeit
- die Liste der bekannten Schwachstellen bei der operationellen Nutzung des VPN

Sicherheitsvorgaben

In den Sicherheitsvorgaben werden die Sicherheitseigenschaften des VPN beschrieben. Dabei handelt es sich um Kriterien, die die Sicherheitsmaßnahmen auf drei Ebenen betrachten:

- Sicherheitsziele: Weshalb wird die Funktionalität gebraucht?
- sicherheitsspezifische Funktionen: Welche Funktionalität wird zum Erreichen der Sicherheitsziele zur Verfügung gestellt?
- Sicherheitsmechanismen: Wie wird die Funktionalität zur Verfügung gestellt?

Die Sicherheitsvorgaben müssen die folgenden Punkte enthalten:

- eine Produktbeschreibung (welche Dienste sind implementiert, was für ein Security Management steht zur Verfügung usw.)
- die Art des Produkteinsatzes
- die vorgesehene Einsatzumgebung (technisch und administrativ)
- die Definition der Sicherheitsziele
- die angenommenen Bedrohungen, denen das VPN entgegenwirkt
- die zur Verfügung gestellten sicherheitsspezifischen Funktionen
- die Sicherheitsmechanismen
- eine Beschreibung der Zweckmäßigkeit der Sicherheitsmechanismen

Das Prüflabor prüft, ob für jede mögliche Bedrohung mindestens eine sicherheitsspezifische Funktion existiert, die ihr entgegenwirkt. Die Sicherheitsmechanismen, die die entsprechenden Funktionen zur Verfügung stellen, werden auf ihre Zweckmäßigkeit überprüft.

Architekturentwurf

Im Architekturentwurf wird die grundsätzliche Struktur des VPNs mit allen seinen externen Schnittstellen beschrieben. Hier findet eine Aufteilung des VPN-Systems in sicherheitsspezifische und nicht-sicherheitsspezifische Komponenten statt. Sicherheitsspezifische Komponenten sind Komponenten, die direkt sicherheitsspezifische Funktionen ausführen oder daran beteiligt sind. Die Trennung von sicherheitsspezifischen und nicht-sicherheitsspezifischen Komponenten wird beschrieben und die Wirksamkeit dieser Trennung wird überprüft.

Feinentwurf

Der Feinentwurf des VPN enthält die Spezifikation aller Komponenten und ihrer Schnittstellen. Alle sicherheitsspezifischen Funktionen müssen beschrieben und auf die Komponenten abgebildet werden. Alle Sicherheitsmechanismen müssen definiert und spezifiziert werden. Im Feinentwurf muss nachgewiesen werden, dass die angegebenen Sicherheitsmechanismen nicht in irgendeiner Form umgangen werden können.

Tests

Alle Sicherheitsmechanismen müssen dem Quellcode zugeordnet werden, das heißt, es muss beschrieben werden, welcher Sicherheitsmechanismus wo und wie implementiert ist. Jeder einzelne Sicherheitsmechanismus muss durch Tests nachgewiesen werden. Dazu muss der Hersteller neben dem Quellcode des VPN die Testpläne, Testziele, Testverfahren, Testergebnisse und die Bibliotheken aller verwendeten Testprogramme und -werkzeuge in einer Testdokumentation festhalten.

Das Prüflabor überprüft anhand des Quellcodes und der Testdokumentation, ob alle sicherheitsspezifischen Funktionen betrachtet und alle Sicherheitsmechanismen getestet wurden. Dazu wird der Quellcode auf eventuell vorhandene Möglichkeiten zur Umgehung von Sicherheitsmechanismen analysiert und die Tests werden wiederholt. Zusätzlich werden Penetrationstests und Tests zur Fehlersuche durchgeführt.

Entwicklungsumgebung

Die Entwicklungsumgebung umfasst das Konfigurationskontrollsystem, das Abnahmeverfahren, die Konfigurationsliste, die Beschreibung aller benutzten Implementierungssprachen und die Sicherheit der Entwicklungsumgebung.

Mit dem Konfigurationskontrollsystem, dem Abnahmeverfahren und der Konfigurationsliste stellt der Hersteller sicher, dass das VPN mit der zur Verfügung gestellten Dokumentation übereinstimmt, dass nur autorisierte Änderungen daran möglich sind sowie dass das VPN vollständig und die angegebene Version eindeutig ist.

Das Prüflabor prüft den Einsatz des Konfigurationskontrollsystems und das Abnahmeverfahren beim Hersteller.

Die Programmiersprachen, die für die Implementierung benutzt werden, müssen mit allen verwendeten Optionen eindeutig angegeben werden. Dies dient zu einer eventuell notwendigen Rekonstruktion der VPN-Software.

Der Hersteller muss mit Informationen über die Sicherheit seiner Entwicklungsumgebung beschreiben, wie die Schutzmaßnahmen bezüglich der Integrität des VPN und die Vertraulichkeit der zugehörigen Dokumente realisiert werden. Alle dazu notwendigen Sicherheitsmaßnahmen müssen beschrieben werden. Die Maßnahmen werden eingeteilt in

- materielle Sicherheitsmaßnahmen, wie zugangsgeschützte Räume für die Entwicklungsrechner des VPN, USV und ähnliches,
- organisatorische Sicherheitsmaßnahmen, beispielsweise restriktive Rechteverwaltung für die Entwicklungsrechner des VPN und Regelungen für den Modemgebrauch, und
- personelle Sicherheitsmaßnahmen, wie zum Beispiel Sicherheitsüberprüfungen der VPN-Entwickler und Mitarbeiter.

Das Prüflabor prüft die Anwendung und Einhaltung der angegebenen Verfahren beziehungsweise Vorschriften. Zusätzlich wird nach eventuell vorhandenen Fehlern in den angewendeten Verfahren gesucht.

Betriebsdokumentation

Die Betriebsdokumentation des VPN unterteilt sich in Benutzerdokumentation und Systemverwalterdokumentation.

Die Benutzerdokumentation muss strukturiert aufgebaut und in sich konsistent sein. Sie muss Richtlinien für ihre sichere Anwendung enthalten und beschreiben, wie der Benutzer das VPN auf sichere Art und Weise bedient.

Die Systemverwalterdokumentation muss ebenfalls strukturiert aufgebaut und in sich konsistent sein. Sie muss beschreiben, wie das Produkt installiert, konfiguriert und sicher verwaltet wird. Die Beschreibung der Sicherheitsparameter, der möglichen sicherheitsrelevanten Ereignisse, der Verfahren für die Sicherheitsadministration, der Sicherheitseigenschaften und deren Zusammenwirken müssen in der Systemverwalterdokumentation enthalten sein.

Betriebsumgebung

Die Betriebsumgebung kann unter zwei Aspekten betrachtet werden:

- Auslieferung und Konfiguration
- Anlauf und Betrieb

Die Informationen zum angewendeten Verfahren der Auslieferung und Konfiguration müssen beschreiben, wie der Hersteller die Sicherheit des VPN aufrechterhält, beispielsweise durch Prüfsummen der Software, Siegel usw. Sind unterschiedliche Konfigurationen möglich, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit beschrieben werden.

Das Prüflabor hat die korrekte Anwendung des Auslieferungsverfahrens für das VPN zu überprüfen und nach Fehlern zu suchen.

Der Hersteller muss beschreiben, wie die Prozeduren für den Anlauf und Betrieb realisiert sind und auf welche Weise sie die Sicherheit aufrecht erhalten. Dazu müssen die sicherheitsspezifischen Funktionen beschrieben werden, die eventuell während des Anlaufs, des Betriebs oder der Wartung ausgeschaltet oder modifiziert werden können. Beispiele von Protokollaufzeichnungen beziehungsweise Ergebnisse von Diagnoseprozeduren, die während des Anlaufs und des Betriebs erstellt werden, müssen vorgelegt werden. Das Prüflabor prüft die Protokollaufzeichnungen beziehungsweise die Ergebnisse von Diagnoseprozeduren und sucht nach Fehlern in den Prozeduren.

Wirksamkeit

Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des VPN. Bei dieser Analyse werden alle Wege gesucht, die es einem Angreifer erlauben würden, die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Dabei werden alle zur Verfügung stehenden Informationen, das heißt auch der Quellcode, verwendet.

Analyse der Eignung der Funktionalität

Bei der Analyse der Eignung der Funktionalität wird geprüft, ob es Bedrohungen gibt, denen nicht eine oder mehrere sicherheitsspezifische Funktionen des VPN angemessen entgegenwirken.

Analyse des Zusammenwirkens der Funktionalität

Mit der Analyse des Zusammenwirkens wird gezeigt, dass die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des VPN so zusammenwirken, dass sie sich gegenseitig unterstützen und ein wirksames Ganzes bilden. Des Weiteren wird gezeigt, dass keine sicherheitsspezifische Funktion und kein sicherheitsspezifischer Sicherheitsmechanismus existiert, die oder der in Konflikt mit anderen sicherheitsspezifischen Funktionen oder Sicherheitsmechanismen geraten oder ihnen entgegenwirken kann.

Analyse der Stärke der Sicherheitsmechanismen

Diese Analyse bewertet die Fähigkeit der Sicherheitsmechanismen, direkten Angriffen zu widerstehen, die auf Mängel in den ihnen zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften zurückzuführen sind. Dabei wird auch der Aufwand an Betriebsmitteln betrachtet, den ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen. Analysen über die Algorithmen, Prinzipien und Eigenschaften, die diesen Sicherheitsmechanismen zugrunde liegen, müssen erstellt oder es muss auf solche Analysen verwiesen werden. Die Analyse erfolgt hinsichtlich der Einstufung der Mindeststärke und unter Verwendung aller zur Verfügung stehenden Informationen, einschließlich des Quellcodes des VPN.

Das Prüflabor überprüft unter Verwendung aller zur Verfügung stehenden Informationen einschließlich des Quellcodes, ob die Sicherheitsmechanismen die beanspruchte Mindeststärke gewährleisten. Zusätzlich werden aktive und aggressive Penetrationstests zur Bestätigung der Mindeststärke durchgeführt.

Analyse der Benutzerfreundlichkeit

Ob sicherheitsspezifische Funktionen oder Mechanismen durch menschliche oder andere Fehler ausgeschaltet oder unbrauchbar gemacht wurden, muss einfach festzustellen und zu erkennen sein, damit Endbenutzer oder Administratoren

nicht von einem sicheren Zustand ausgehen, obwohl das VPN möglicherweise in einer Weise konfiguriert oder benutzt wird, die unsicher ist. Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des VPN – einschließlich des Betriebs nach Bedien- und Betriebsfehlern – und ihre Konsequenzen für die Aufrechterhaltung eines sicheren Betriebs beschreiben.

Das Prüflabor hat Analysen der Benutzerfreundlichkeit unter Verwendung aller zur Verfügung stehenden Informationen einschließlich des Quellcodes nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es muss jede Konfigurations- und Installationsprozedur nachvollziehen, um zu überprüfen, ob das VPN sicher konfiguriert und benutzt werden kann.

11.2 Wirksamkeit von VPN-Sicherheitsmechanismen

Im Folgenden werden die Wirksamkeitsaspekte von VPN-Sicherheitsmechanismen untersucht.

Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des VPN-Systems. Bei dieser Analyse werden alle Wege gesucht, die es einem Angreifer erlauben würden, die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Dabei werden alle zur Verfügung stehenden Informationen, auch der Quellcode, verwendet.

Stärke der Sicherheitsmechanismen, die im VPN-System realisiert sind:

Selbst wenn ein Sicherheitsmechanismus nicht umgangen, außer Kraft gesetzt oder in andere Weise korrumpiert werden kann, kann es dennoch möglich sein, ihn aufgrund von Mängeln in den zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften durch einen direkten Angriff zu überwinden. Für diesen Aspekt der Wirksamkeit muss die Fähigkeit der Sicherheitsmechanismen bewertet werden, solchen direkten Angriffen zu widerstehen. Der Aspekt der Wirksamkeit unterscheidet sich von anderen Aspekten dahingehend, dass er den Aufwand an Betriebsmitteln betrachtet, die ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen.

Wirksamkeit von Sicherheitssystemen:

Für die Beurteilung von Sicherheitssystemen ist es ein wichtiges Kriterium, ob die Sicherheitssysteme, die zum Beispiel ein VPN-System bietet, auch tatsächlich geeignet sind, den realen Angriffen entgegenzuwirken.

Im Folgenden wird dargestellt, wie die Wirksamkeit von Sicherheitssystemen generell beurteilt werden kann /ITSEM94/.

In der ersten Grafik werden die Werte einer Organisation, die es vor einem Angriff zu schützen gilt, durch einen Geldsack dargestellt. Die Angriffe, denen ein System ausgesetzt ist, werden durch Nägel repräsentiert, deren Länge proportional zur Größe der Fachkenntnisse, der Gelegenheiten und Ressourcen ist, über die der Angreifer verfügt.

Die Sicherheitsmechanismen, die eingesetzt werden, sind durch eine Wand dargestellt. Die Dicke dieser Wand ist proportional zur Stärke des Sicherheitsmechanismus. Je länger also der Nagel ist, desto schwerwiegender ist die Bedrohung. Je dicker die Wand, desto größer die Fähigkeit der Sicherheitsmechanismen, diese Bedrohung der Werte einer Organisation abzuwehren.

Sicherheitsmechanismen sind dann sicher, wenn die Werte vollständig von einer Wand umgeben sind und die Dicke der Wand auch an ihrer schwächsten Stelle mindestens gleich der Länge des größten Nagels ist.

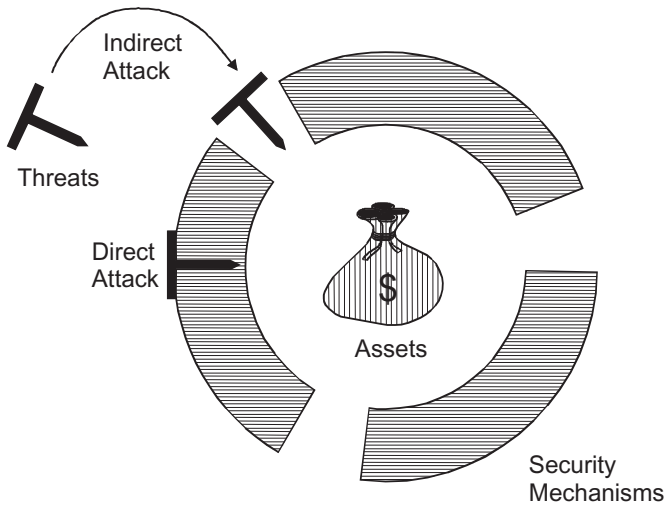

Abb. 11.2: Wirksamkeit

Es kann aber auch der Fall auftreten, dass die gewählten Sicherheitsdienste zur Abwehr der Bedrohung nicht ausreichen, obwohl ihre Sicherheitsmechanismen eigentlich stark genug sind.

Beispiel für »Indirect Attack«:

Ein Angreifer hat die Möglichkeit, zum Beispiel über das eingesetzte Betriebssystem die Rechteverwaltung des VPN-Systems zu verändern.

Grundsätzlich kann die Stärke der Sicherheitsmechanismen von Sicherheitssystemen unterschiedlich bewertet werden. Hierbei wird die Bewertung niedrig, mittel und hoch verwendet.

Eine wichtige Größe für die Bewertung von Sicherheitsmechanismen ist die Mindeststärke des Sicherheitsmechanismus (SoMmin), die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.

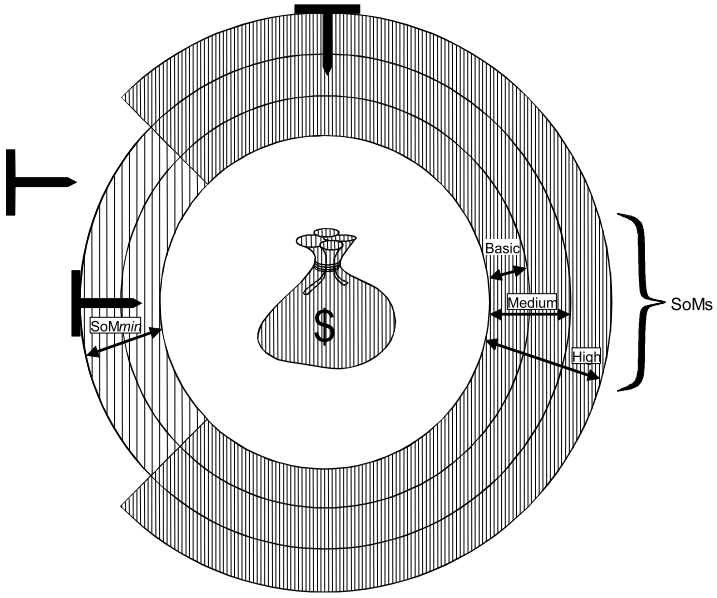

Abb. 11.3: Mindeststärke

Die nun folgenden Bilder sollen verdeutlichen, wie Schwachstellen im VPN-System einzuschätzen sind, wie sie eingeordnet und schließlich wie sie behoben werden können.

Bild (a) zeigt eine erfolgreiche Überwindung der Sicherheitsmechanismen. Die Breite der Wall entspricht nicht der erforderlichen Mindeststärke des Sicherheitsmechanismus und kann daher vom Angreifer überwunden werden.

In Abbildung (b) ist ersichtlich, dass durch die eingesetzten Mechanismen, also Algorithmen, Prinzipien und Eigenschaften, die erforderliche Mindeststärke der Sicherheitsmechanismen gewährleistet ist und der Angriff daher erfolgreich abgewehrt werden kann.

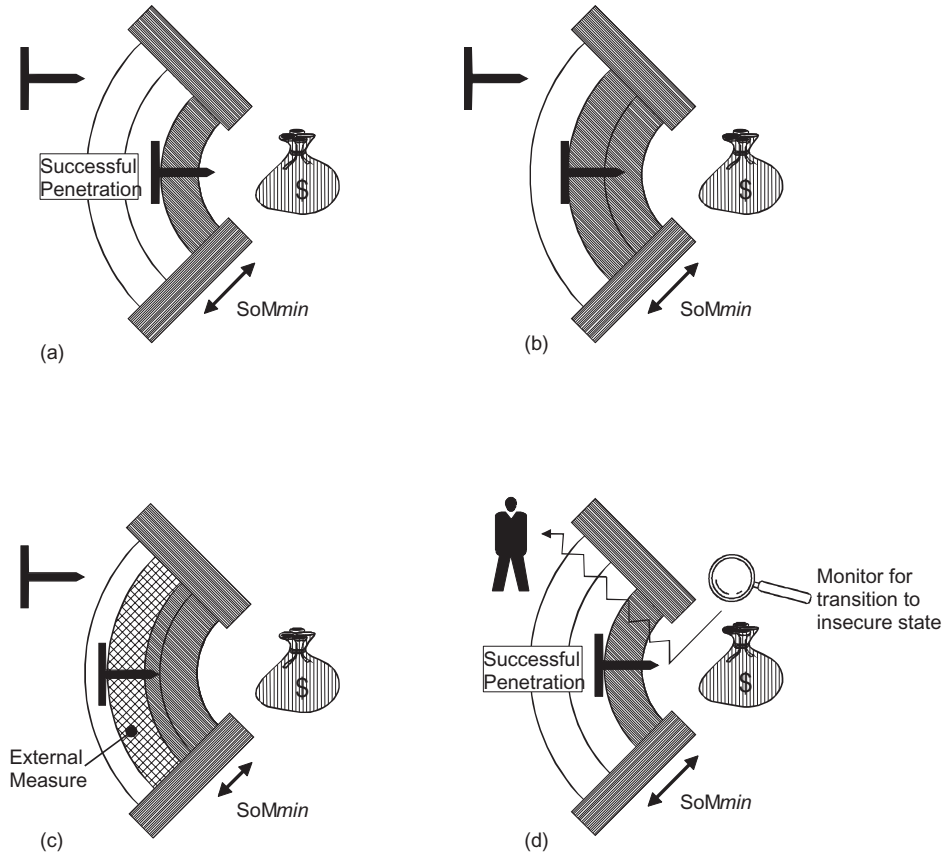

Abb. 11.4: Schwachstellen

Bild (c) stellt dar, wie durch externe Maßnahmen die Wirksamkeit des Sicherheitsmechanismus noch erhöht werden kann, mit dem Ziel, den Angriff abzuwehren.

Im Bild (d) ist dargestellt, dass zwar ein erfolgreicher Angriff nicht verhindert werden konnte, es jedoch möglich ist, den Angriff zu verfolgen, und dass so Maßnahmen eingeleitet werden können, um den Schaden – die Verwundbarkeit – zu reduzieren.

Mechanismenstärke und Evaluationsstufen

Dieser Abschnitt gibt die Mechanismenstärke und die Evaluationsstufen wieder, wie sie in den ITSEC-Kriterien definiert sind.

Mechanismenstärke	Beschreibung
niedrig	Es muss erkennbar sein, dass der Mechanismus Schutz gegen zufälliges Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.
mittel	Es muss erkennbar sein, dass der Mechanismus Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.
hoch	Es muss erkennbar sein, dass der Mechanismus nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

Tabelle 11.1: Unterscheidung der Mechanismenstärke in den Stufen niedrig, mittel und hoch.

Evaluationsstufe	Beschreibung
E0	Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.
E1	Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.
E2	Zusätzlich zu den Anforderungen für die Stufe E1 muss hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muss bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.
E3	Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode beziehungsweise die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muss bewertet werden.
E4	Zusätzlich zu den Anforderungen für die Stufe E3 muss ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.
E5	Zusätzlich zu den Anforderungen für die Stufe E4 muss ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode beziehungsweise den Hardware-Konstruktionszeichnungen bestehen.
E6	Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrunde liegenden formalen Sicherheitsmodell ist.

Tabelle 11.2: Unterscheidung der Evaluationsstufen