Kapitel 9

VPN-Sicherheitspolitik und weitere Sicherheitsmaßnahmen

Ein VPN ist kein Produkt, das »von der Stange« gekauft werden kann und dann automatisch Sicherheit gewährleistet. Unterschiedliche Aspekte müssen berücksichtigt werden, damit mit Hilfe eines VPN das gewünschte Sicherheitsmaß erreicht werden kann. Das VPN muss

- auf einer VPN-Sicherheitspolitik aufbauen,
- in das IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

In diesem Kapitel wird exemplarisch beschrieben, wie eine VPN-Sicherheitspolitik auszusehen hat und welche Sicherheitsmaßnahmen für den Betrieb eines VPN zusätzlich benötigt werden. Jedoch können Sicherheitsmaßnahmen für eine korrekte Installation oder Administration nicht berücksichtigt werden, weil sie vom jeweils eingesetzten Produkt abhängen. Auch die Einbettung der VPN-Sicherheitspolitik in ein IT-Sicherheitskonzept wird nicht dargestellt, da sie organisationsspezifisch ist /BSI99/.

9.1 VPN-Sicherheitspolitik

Eine VPN-Sicherheitspolitik ist die Voraussetzung für den sicheren Betrieb eines VPN. Ein VPN macht nicht automatisch sicher, sondern mit einem VPN kann die Kommunikation über unsichere Netze sicher gemacht werden. Die Installation eines VPN ohne vorausgehendes Sicherheitskonzept kann zu einem falschen Sicherheitsgefühl führen. Oft wird irrtümlicher weise davon ausgegangen, dass mit der Installation eines VPN alles gesichert sei. Dieser Irrtum wiegt noch schwerer, wenn keine genaue Kenntnis über die vorhandene Netzwerktopologie vorhanden ist. Denn bei Unkenntnis der Netzwerktopologie kann man nicht davon ausgehen, dass nicht doch mehr als eine Verbindung zum Internet oder zu anderen unsicheren Netzen existiert, über die dann die Daten ungesichert übertragen werden.

Die VPN-Sicherheitspolitik orientiert sich am Schutzbedarf der eingesetzten IT-Systeme und muss Teil einer vorhandenen organisationsweiten Sicherheitspolitik sein. Die Festlegung der VPN-Sicherheitspolitik kann auch bestehende Richtlinien und Vorschriften der allgemeinen Sicherheitspolitik betreffen, die dementsprechend mit berücksichtigt werden müssen.

Die VPN-Sicherheitspolitik definiert Sicherheitsziele, die durch den Einsatz eines VPN erfüllt werden sollen, und stellt die zu schützenden Ressourcen dar. Die Kommunikationsanforderungen werden darin festgelegt. Die VPN-Sicherheitspolitik ist wie eine organisationsweite Sicherheitspolitik auf die jeweilige Organisation und den Bereich abgestimmt, zum Beispiel Medizin, Banken, Versicherungen, Energieversorgungs-Unternehmen, Betriebs- oder Personalrat usw. /Pohl97a und Pohl97b/.

9.1.1 Sicherheitsziele

Im ersten Schritt müssen die Sicherheitsziele definiert werden, die mit dem Einsatz eines VPN erreicht werden sollen. Als Richtwerte können folgende Punkte betrachtet werden:

- Vertraulichkeit,
- Authentikation (implizit – über die Verschlüsselung – oder explizit),
- Zugangskontrolle (für Datenpakete oder Benutzer),
- Rechteverwaltung (für Kommunikationsprotokolle und -dienste),
- Beweissicherung und
- Protokollauswertung.

9.2 Zusätzliche Sicherheitsmaßnahmen

Das eigentliche VPN-Produkt besteht aus Soft- und Hardware. Neben dieser technischen Seite müssen weitere Aspekte beachtet werden, damit der sichere Betrieb des VPN garantiert werden kann. Die im folgenden Abschnitt aufgeführten Sicherheitsmaßnahmen gelten auch allgemein für den Einsatz von IT-Systemen und sind in den meisten Organisationen vorhanden. Andere Maßnahmen müssen speziell für den sicheren Betrieb eines VPN umgesetzt werden.

Die zusätzlichen Sicherheitsmaßnahmen gliedern sich in die folgenden Unterpunkte:

- Infrastruktur
- Organisation
- Personal
- Festlegungen für den Notfall

9.2.1 Infrastruktur

Die folgenden infrastrukturellen Sicherheitsmaßnahmen tragen dazu bei, die Sicherheit des VPN-Betriebs zu erhöhen:

Zugangsgesicherter Raum

Sämtliche Komponenten des VPN sollten in abgeschlossenen und zugangsgesicherten Räumen aufgestellt werden, um zu verhindern, dass unberechtigte Personen die technischen Sicherheitsmechanismen manipulieren oder ausschalten.

Unterbrechungsfreie Stromversorgung (USV)

Eine USV sollte installiert werden, um kurzzeitige Stromausfälle zu überbrücken oder die Stromversorgung wenigstens so lange aufrecht zu erhalten, dass ein geordnetes Herunterfahren angeschlossener Rechnersysteme möglich ist. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben. Dauert ein Stromausfall länger, so bleibt bei einer Überbrückungszeit von ca. 10 bis 15 Minuten noch eine Reserve von etwa 5 Minuten, um das angeschlossene VPN geordnet herunterfahren zu können. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die ein automatisches Herunterfahren (Shut-down) nach einer vorher definierten Zeit einleiten können. Das Intervall wird dem Zeitbedarf zum Herunterfahren des VPN und der Kapazität der USV entsprechend festgelegt. Alternativ zu einer lokalen USV kann die Stromversorgung unterbrechungsfrei aus einer vorhandenen Quelle bezogen werden, beispielsweise durch den Anschluss an eine zentrale USV.

Geschützte Leitungsführung

Die Zuleitungen (zu schützendes und unsicheres Netz) sollen so eingerichtet werden, dass sie nicht außerhalb des zugangsgeschützten Raums überbrückt werden können.

Dokumentation

Durch eine gute Dokumentation und die eindeutige Kennzeichnung aller Leitungen des VPN kann einer fehlerhaften Verkabelung vorgebeugt werden, die zu einer Überbrückung des VPN führen könnte. Die Dokumentation ist ebenfalls für die Wartung sowie gegebenenfalls für eine erfolgreiche Fehlersuche und Instandsetzung erforderlich. Die Qualität dieser Dokumentation ist abhängig von ihrer Vollständigkeit, Aktualität und Lesbarkeit.

Zentrales Netzwerkmanagement-System

Durch Kopplung des VPN an ein vorhandenes Netzwerkmanagement-System können von diesem bestimmte Informationen über das VPN abgefragt werden oder werden vom VPN an das Netzwerkmanagement-System gemeldet. Dazu gehören Statusmeldungen und Alarme, die durch das Auftreten sicherheitskritscher Ereig-

nisse ausgelöst werden. Da Netzwerkmanagement-Systeme in der Regel lange Betriebszeiten erfüllen, häufig rund um die Uhr, erhöht die Kopplung des VPN an das Netzwerkmanagement-System die Verfügbarkeit des gesamten IT-Systems.

9.2.2 Organisation

Für den sicheren Betrieb eines VPN müssen auch einige organisatorische Sicherheitsmaßnahmen berücksichtigt werden. Diese Maßnahmen betreffen die allgemeine Organisation, die technische Realisierung, das Sicherheitsmanagement und die Benutzer.

Technische Realisierung

Externe Zugänge

Klare Richtlinien, die allen Benutzern bekannt sind, müssen genau festlegen, dass keine externen Zugänge unter Umgehung des VPN eingerichtet werden dürfen.

Sichere Anordnung weiterer Komponenten im Bereich des VPN:

Neben der Installation und dem Betrieb des VPN müssen auch weitere Komponenten, die der Kommunikation zwischen zu schützendem und unsicherem Netz dienen, sicher angeordnet werden. Dazu gehören zum Beispiel Firewall-Systeme.

Sicherheitsmanagement

Festlegung der Verantwortlichkeiten für das VPN

Die Verantwortlichkeiten für das VPN müssen klar geregelt und aufgeteilt sein. Für den VPN-Einsatz müssen die Fachverantwortung und die Betriebsverantwortung festgelegt werden. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben für das VPN. Die Fachverantwortung liegt in der Regel beim IT-Sicherheitsmanagement, das ein VPN-Sicherheitskonzept auf Grundlage der definierten VPN-Sicherheitspolitik erstellt. Die Betriebsverantwortung hingegen umfasst den sicheren Betrieb und die Überwachung des VPN. Diese Aufgabe wird vom Security Administrator ausgeführt, der unter anderem für die korrekte Einrichtung von weiteren Benutzerkonten für das Security Management verantwortlich ist.

Zugriffsrechte für das Security Management

Der Fachverantwortliche (IT-Sicherheitsmanagement) legt im VPN-Sicherheitskonzept die Zugriffsrechte von Benutzern für das Security Management fest. Die Zugriffsrechte regeln, in welcher Funktion ein Administrator das Security Management nutzen darf. Der Betriebsverantwortliche (Security Administrator) richtet die Funktionen ein, denen ein Administrator zugeordnet wird. Solche Funktionen sind zum Beispiel Operator, Auditor (Revisor), Editor (Datenerfasser) usw. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie für die Wahrneh-

mung der spezifischen Aufgaben notwendig ist (»Need-to-know-Prinzip«). Der jeweils Verantwortliche veranlasst und dokumentiert die Veränderung von Zugriffsrechten. Aus der Dokumentation muss hervorgehen,

- welche Funktion unter Beachtung der Funktionstrennung mit welchen Zugriffsrechten ausgestattet wird,
- welcher Administrator welche Funktion wahrnimmt,
- welche Zugriffsrechte ein Administrator erhält und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Konflikte können beispielsweise daraus resultieren, dass ein Administrator unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom VPN die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.

Der Security Administrator aktiviert sinnvoll einsetzbare Protokollfunktionen zur Beweissicherung, falls das Sicherheitsmanagement es zulässt. Dazu gehört die Protokollierung von erfolgreichen und erfolglosen An- und Abmeldevorgängen, unerlaubten Zugriffsversuchen und von Fehlermeldungen des Systems.

Im Vertretungsfall muss der Security Administrator kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist, bevor er die erforderlichen Zugriffsrechte einrichtet.

Kontrolle der Protokolldaten

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten auch ausgewertet werden. Deshalb müssen die Protokolldaten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Wenn es technisch nicht möglich ist, die Rolle eines unabhängigen Revisors für Protokolldaten einzurichten, kann die Auswertung auch durch den Administrator erfolgen. In diesem Fall sind die Tätigkeiten des Administrators jedoch nur schwer zu kontrollieren. Das Ergebnis der Auswertung sollte dann dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Die regelmäßige Kontrolle und anschließende Löschung der Protokolldaten verhindert darüber hinaus ein übermäßiges Anwachsen der Protokolldaten. Da Protokolldaten in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (vgl. §§ 14 Abs. 4 und 31 BDSG).

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit? (Hinweis auf Manipulationsversuche)

- Häufen sich fehlerhafte Anmeldeversuche? (Hinweis auf den Versuch, Passworte zu erraten)
- Häufen sich unzulässige Zugriffsversuche? (Hinweis auf Manipulationsversuche)
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden? (Hinweis auf eventuell gelöschte Protokollsätze)
- Ist der Umfang der protokollierten Daten zu groß? (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Login oder Logout stattgefunden hat? (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (zum Beispiel mehrfache fehlerhafte Login-Versuche) hervorheben.

Informationsbeschaffung über Sicherheitslücken des VPN

Wenn durch Veröffentlichungen neue Sicherheitslücken bekannt werden, müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen oder zusätzliche Sicherheitshardware beziehungsweise -software eingesetzt werden, um diese Lücken zu schließen.

Deshalb ist es sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren. Informationsquellen sind:

- Hersteller bzw. Vertreiber von VPNs. Sie informieren registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Versionen des VPN oder Patches zur Behebung der Sicherheitslücken zur Verfügung. Dieser Service kann zum Beispiel in einem Wartungsvertrag geregelt werden.
- Computer Emergency Response Teams (CERT)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- hersteller- und systemspezifische sowie sicherheitsspezifische Newsgroups im Internet
- IT-Fachzeitschriften

Reaktion auf Verletzungen der Sicherheitspolitik

Reaktionen auf Verletzungen der Sicherheitspolitik sollten vorab festgelegt werden, damit im Bedarfsfall schnell und wirksam gehandelt werden kann.

Art und Herkunft der Verletzung müssen untersucht und angemessene schadensbehebende oder -mindernde Maßnahmen ergriffen werden. Falls erforderlich, müssen zusätzlich schadensvorbeugende Konsequenzen gezogen werden. Welche

Aktionen durchgeführt werden müssen, hängt sowohl von der Art der Sicherheitsverletzung als auch von ihrem Verursacher ab.

Es muss vorab geklärt sein, wer dafür verantwortlich ist, Informationen über bekannte Sicherheitslücken einzuholen oder Informationen über aufgetretene Sicherheitslücken an andere Organisationen weiterzugeben. Auch muss dafür Sorge getragen werden, dass eventuell mitbetroffene Stellen schnellstens informiert werden.

Verpflichtung des Security Administrators zur Datensicherung

Da die Datensicherung eine wichtige Sicherheitsmaßnahme ist, sollte der zuständige Security Administrator zur Einhaltung des Datensicherungskonzepts beziehungsweise eines minimalen Datensicherungskonzepts für das VPN verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

Benutzer

Keine Weitergabe von Security Token und Passworten

Werden für die Authentisierung gegenüber dem *VPN* Security Token verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung entscheidend von der sicheren Benutzung der Security Token abhängig. Dazu gehört auch, dass die Passworte geheimgehalten und die Security Token nicht weitergegeben werden. Den Benutzern muss bewusst sein, dass sie für ihre Passworte und Security Token verantwortlich sind. Sie können auch dafür verantwortlich gemacht werden, wenn Fremde damit Schaden anrichten.

Betreuung und Beratung der Benutzer, die über das VPN kommunizieren

Der Einsatz eines VPN erfordert eine Schulung der Benutzer, die sie in die Lage versetzt, das eingesetzte VPN sachgerecht zu nutzen. Über die Schulung hinaus muss den Benutzern eine Betreuung und Beratung für im laufenden Betrieb eventuell auftretende Probleme zur Verfügung stehen. Probleme können aus unterschiedlichen Gründen entstehen, unter anderem wegen Unzulänglichkeiten der Benutzer, die eventuell eine andere Art und Weise der Nutzung von Diensten über das VPN erlernen müssen.

In größeren Organisationen kann es deshalb sinnvoll sein, eine zentrale Stelle mit der Betreuung der Benutzer, die über das VPN kommunizieren, zu beauftragen, und diese allen Benutzern bekannt zu geben.

Allgemeine Sicherheitsmaßnahmen

Regelung für Wartungs- und Reparaturarbeiten am VPN

Die ordnungsgemäße Durchführung von Wartungsarbeiten ist eine besonders wichtige vorbeugende Maßnahme, um das VPN vor Störungen zu bewahren. Die

Wartungsarbeiten sollten von vertrauenswürdigem Personal oder externen Firmen durchgeführt werden.

Wenn Wartungs- und Reparaturarbeiten durch externes Personal durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: Während der Arbeiten sollte eine fachkundige Kraft die Arbeiten so weit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit nichtautorisierte Handlungen, beispielsweise die Einrichtung unerlaubter Zugriffsrechte aus dem unsicheren Netz, durchgeführt werden.

Vor und nach Wartungs- und Reparaturarbeiten sind folgende Maßnahmen einzuplanen:

- Die Arbeiten müssen den betroffenen Benutzern angekündigt werden.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen beziehungsweise zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind – je nach »Eindringtiefe« des Wartungspersonals – Passwortänderungen erforderlich.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, eventuell Name des Wartungstechnikers).

Rechtzeitige Beteiligung des Personal- / Betriebsrats

Die Protokollierung ist eine Maßnahme, die geeignet ist, eine Verhaltens- oder Leistungsüberwachung von Benutzern zu ermöglichen, und bedarf somit der Mitbestimmung der Personalvertretung. Grundlage sind die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrats kann eine Zeitverzögerung bei der Einführung eines VPN verhindern.

9.2.3 Personal

Personelle Sicherheitsmaßnahmen können das Sicherheitsmanagement und die Benutzer betreffen.

Sicherheitsmanagement

Profil des Security Administrators

Der Security Administrator muss grundlegende Kenntnisse im Bereich IT-Sicherheit und speziell über VPNs besitzen und diese Kenntnisse kontinuierlich aktualisieren und erweitern. Die Teilnahme an Schulungen über die Konfiguration und sichere Verwaltung des VPN, die vom jeweiligen Hersteller oder seinem Vertriebspartner angeboten werden, ist zu empfehlen. Der Security Administrator muss in der Lage sein, Fehlermeldungen und Alarme richtig einzuschätzen, um geeignete

Gegenmaßnahmen ergreifen zu können. Bei Eingriffen von externem Personal ins VPN muss der Administrator die durchgeführten Arbeiten nachvollziehen können.

Auswahl eines vertrauenswürdigen Administrators und Vertreters

Den Administratoren des VPN und ihren Vertretern muss großes Vertrauen entgegengebracht werden, da sie sehr weitgehende Befugnisse haben. Administrator und Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie zu verändern und Berechtigungen zu vergeben, so dass durch einen Missbrauch der Befugnisse erheblicher Schaden entstehen könnte.

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt und regelmäßig darüber belehrt werden, dass es seine Befugnisse nur für die erforderlichen Administrationsaufgaben verwenden darf.

Vertretungsregelungen

Vertretungsregelungen haben den Sinn, in vorhersehbaren (Urlaub, Dienstreise) und auch in unvorhersehbaren Fällen (Krankheit, Unfall, Kündigung) des Personalausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Dazu muss *vor* Eintritt eines solchen Falls geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist beim VPN von besonderer Bedeutung, weil dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter im Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Der Verfahrens- oder Projektstand muss hinreichend dokumentiert sein.
- Der Vertreter muss geschult werden. Der Ausfall von Personen, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, bedeutet eine gravierende Gefährdung des Normalbetriebes. In diesem Fall ist die Schulung eines Vertreters von besonders großer Bedeutung.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für eine Person einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte im Vertretungsfall eingesetzt werden können.

Geregelte Verfahrensweise beim Ausscheiden von Benutzern

Scheidet ein Benutzer aus, so ist zu beachten, dass sämtliche für ihn eingerichteten Berechtigungen im VPN widerrufen beziehungsweise gelöscht werden müssen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen.

Benutzer

Aufklärung der Benutzer über die Protokollierung von VPN-Daten

Die Benutzer müssen darüber aufgeklärt werden, dass ihre Verbindungen über das VPN protokolliert werden können. Gleichzeitig sollte der Grund der Protokollierung erklärt werden, damit er von den Benutzern verstanden und akzeptiert wird. Eine Aufklärung der Benutzer hat auch einen Warneffekt, der vor einem potentiellen Missbrauch schützen kann.

Sensibilisierung der Benutzer für mögliche Gefahren bei der Kommunikation über das Internet

Benutzer müssen darauf hingewiesen werden, welche Gefahren durch die Kommunikation über das Internet entstehen können. Durch Aufklärung und Sensibilisierung der Benutzer kann verhindert werden, dass das VPN, beispielsweise aus Bequemlichkeit, umgangen wird und dadurch eine ungeschützte Verbindung über das Internet mit all ihren Gefahren entsteht.

Schulung zum Thema Sicherheit

Die überwiegende Zahl von Schäden entsteht durch Nachlässigkeit. Um dem entgegenzuwirken, muss jeder einzelne Benutzer zum sorgfältigen Umgang mit der Informationstechnologie motiviert werden. Zusätzlich sind Verhaltensregeln zu vermitteln, die ein Verständnis für die Sicherheitsmaßnahmen wecken. Die Schulung zu Sicherheitsmaßnahmen soll insbesondere folgende Themen umfassen:

- *Sensibilisierung für IT-Sicherheit:* Jeder Benutzer ist auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten der Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, eventuell auch durch praktische Hinweise in der Hauspost oder ähnliches.
- *Benutzerbezogene IT-Sicherheitsmaßnahmen:* Dieses Thema soll die Sicherheitsmaßnahmen vermitteln, die in einem VPN-Sicherheitskonzept erarbeitet wurden und von den einzelnen Benutzern umgesetzt werden müssen. Dieser Teil der Schulung ist von großer Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach entsprechender Schulung und Motivation effektiv umgesetzt werden können.
- *Vorbeugung gegen Social Engineering:* Die Benutzer sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, sollten ebenso bekannt gegeben werden wie die Methoden, sich dagegen zu schützen. Da Social Engineering oft mit der Vorspiegelung einer falschen Iden-

tität einhergeht, sollten Benutzer regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

9.2.4 Notfall

Festlegung von Verfügbarkeitsanforderungen

Verfügbarkeitsanforderungen an das VPN und die Dienste, die darüber zur Verfügung gestellt werden, müssen festgelegt werden. Bei Ausfall des VPN ermöglicht ein Übersichtsplan über die Verfügbarkeitsanforderungen eine schnelle Aussage, ab wann ein Notfall vorliegt. Dies bildet die Grundlage für eine Untersuchung und Einrichtung von Backup-Möglichkeiten.

Backup-Möglichkeiten

Sind die Verfügbarkeitsanforderungen an bestimmte Dienste besonders hoch, müssen Backup-Möglichkeiten geschaffen werden, die diesen Anforderungen genügen.