Kapitel 10

VPN: Eine Investition für die Zukunft

In diesem Kapitel werden die Kosten eines VPN-Systems aus unterschiedlichen Blickwinkeln betrachtet. Da ein VPN-System eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

10.1 Total Cost of Ownership

Im Folgenden soll beschrieben und abgeschätzt werden, wie groß der Aufwand ist, ein VPN anzuschaffen und zu betreiben.

Bei den Aufwendungen für ein VPN können drei Phasen unterschieden werden:

- Beschaffungsphase
- Installationsphase
- Aufrechterhaltung des Betriebs

Die Aufwendungen, die in diesem Abschnitt benannt werden, sind reale Aufwendungen, die unabhängig vom jeweiligen Zeitpunkt erbracht werden müssen. Aufwand wird auf Tage gerundet, wobei davon ausgegangen wird, dass sechs Stunden Aufwand einen Arbeitstag ausmachen.

Bei den angegebenen Aufwendungen wird davon ausgegangen, dass ein VPN 20 Organisationseinheiten und 300 Mobil- und Telearbeitsplätze miteinander verbindet.

Die Personalkosten werden mit EUR 750,- pro Tag veranschlagt. Falls die angegebenen Leistungen von Fachfirmen durchgeführt werden, muss sicherlich mit einem höheren Kostenbetrag gerechnet werden.

10.1.1 Beschaffungsphase eines VPN

In der Beschaffungsphase muss von der Organisation eine Sicherheitspolitik festgelegt werden, die als Grundlage für den Betrieb des VPN dient. Hier ist besonders wichtig, den Schutzbedarf des zu schützenden Netzes zu analysieren, damit eine richtige Sicherheitsanforderung festgelegt werden kann.

Sind die Randbedingungen der Sicherheitspolitik der Organisation definiert, dann kann die Produktauswahl eines VPN beginnen, zum Beispiel durch Einholen von Angeboten, Testinstallationen, Referenzbewertung etc. Dabei muss im Vorfeld festgelegt werden, nach welchen Kriterien ein Produkt bewertet werden soll.

Wichtig in dieser Phase ist, dass auch infrastrukturelle, personelle und organisatorische Sicherheitsmaßnahmen vorbereitet werden, damit die nächste Phase eingeleitet werden kann.

Aufwand für die Beschaffungsphase

Falls die Organisation noch keine generelle Sicherheitspolitik erarbeitet hat und diese im Rahmen der VPN-Beschaffung erstellt werden muss, ist der dafür erforderliche Aufwand in der Beschaffungsphase zu berücksichtigen. Die Erstellung einer Sicherheitspolitik kann je nach Größe der Organisation, je nach Anwendungsform und je nach Schutzbedarf zwischen zwei Wochen und zwei Monaten in Anspruch nehmen.

Für die Auswahl eines VPN-Produkts ist der Aufwand abhängig vom Auswahlverfahren sehr unterschiedlich, je nachdem, ob beispielsweise nur mit Hilfe von Prospekten ausgewählt wird oder Testinstallationen mehrerer VPNs mit Aufbau eines Testsystems stattfinden sollen. Der Aufwand liegt in der Regel zwischen zwei Wochen und drei Monaten.

Die Definition und Vorbereitung der infrastrukturellen, personellen und organisatorischen Sicherheitsmaßnahmen kann zwischen einer Woche und vier Wochen beanspruchen.

Die Anschaffungskosten für ein VPN-System (für 20 Organisationseinheiten und 300 Mobil- und Telearbeitsplätze) liegen zwischen 60 000 EUR und 150 000 EUR (20 VPN-Gateways und 300 VPN-Software-Clients), abhängig von seiner Leistungsfähigkeit und vom Maß an Sicherheit und Vertrauenswürdigkeit, das es erbringen kann.

Installationsphase eines VPN

In der Installationsphase gliedern sich die Aufwendungen für ein VPN in mehrere Teilbereiche.

- *Installation des VPN:* Diese Phase umfasst alle infrastrukturellen Sicherheitsmaßnahmen, die zum sicheren Betrieb eines VPN notwendig sind (siehe Kapitel 9 *Ein VPN ist mehr als ein Produkt*).
- *Inbetriebnahme des VPN:* In dieser Phase ist es sinnvoll, entsprechend den Vorgaben der Sicherheitspolitik Benutzerprofile für bestimmte Mitarbeitergruppen zu definieren, damit die Eingaben des Regelwerks später mit Hilfe dieser

Benutzerprofile schneller erfolgen können. Nach Formulierung der Profile werden die Benutzer, die über das VPN kommunizieren dürfen, mit ihren Rechten in das Sicherheitsmanagement eingetragen.

- *Sonstige Sicherheitsmaßnahmen:* In der Installationsphase ist es wichtig, dass weitere Sicherheitsmaßnahmen wie zum Beispiel die Schulung der Benutzer durchgeführt werden, damit diese den richtigen Umgang mit dem VPN lernen und dadurch unnötige Schwierigkeiten beim Betrieb vermieden werden. Hierzu gehört auch die Erarbeitung von Organisationsanweisungen usw. (siehe Kapitel 9 *Ein VPN ist mehr als ein Produkt*).

Die folgenden Tabellen sollen zeigen, welche zeitlichen und finanziellen Aufwendungen für die Beschaffungs- und Installationsphase einzuplanen sind.

Beschaffungsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Sicherheitspolitik	zwei Wochen bis zwei Monate	EUR 7 500	EUR 30 000
Auswahl eines Produktes	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000
weitere Sicherheitsmaßnahmen	eine bis vier Wochen	EUR 3 800	EUR 15 000
Produktkosten		EUR 60 000	EUR 150 000

Tabelle 10.1: Aufwand und Kosten in der Beschaffungsphase

Installationsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Installation des VPN	2 bis 5 Tage	EUR 1 500	EUR 3 800
Inbetriebnahme des VPN	3 bis 10 Tage	EUR 2 300	EUR 7 500
Sonstige Sicherheitsmaßnahmen	3 Wochen bis 3 Monate	EUR 11 300	EUR 45 000

Tabelle 10.2: Aufwand und Kosten in der Installationsphase

Anschaffungskosten	minimale Kosten	maximale Kosten
Summe	EUR 93 900	EUR 296 300

Tabelle 10.3: Gesamtkosten in der Beschaffungs- und Installationsphase

10.1.2 Aufrechterhaltung des Betriebs eines VPN

Die Aufwendungen für die Aufrechterhaltung des Betriebs eines VPN können unter verschiedenen Gesichtspunkten betrachtet werden.

Rechteverwaltung

Ein VPN ist prinzipiell so aufgebaut, dass es nach Eintrag sämtlicher Rechte vollkommen selbständig und ohne aktive Eingriffe eines Administrators betrieben werden kann.

Aus unterschiedlichen Gründen kann jedoch ein personeller Eingriff notwendig werden, unter anderem zur Einrichtung neuer Mitarbeiter oder Organisationseinheiten beziehungsweise zur Änderung der Rechte schon eingetragener Mitarbeiter oder Organisationseinheiten. Je nach Anzahl der definierten Benutzerprofile und der erforderlichen Änderungen ergibt sich ein sehr unterschiedlicher personeller Aufwand für diese Aufgaben.

Rechenbeispiel: Für die Eintragung eines neuen Mitarbeiters oder für die Änderung der Rechte eines schon eingetragenen Mitarbeiters benötigt der Administrator im Schnitt 10 Minuten. Die Veränderung der Mitarbeiterzahl in einer Organisation, die über das VPN kommunizieren darf, wird in unserem Beispiel mit 5 % im Monat veranschlagt.

Das bedeutet bei 300 (Mobil- und Tele-)Mitarbeitern, die potentiell über das VPN kommunizieren dürfen, dass 15 Veränderungen im Monat stattfinden. Für die Rechteverwaltung ist somit ein Zeitaufwand von 150 Minuten im Monat, also ca. 3 Stunden im Monat beziehungsweise 6 Tagen im Jahr notwendig.

Analyse der Logbuchdaten

Für die Analyse der Logbuchdaten, die vom VPN generiert werden, ist ein Aufwand für den Administrator einzukalkulieren. Auch hier kann der personelle Aufwand sehr unterschiedlich ausfallen. Bei VPNs, die eine automatische Vorauswertung durchführen, ist der Zeitaufwand weitaus geringer als bei VPNs, bei denen der Administrator die Logbuchdaten vollständig selbst auswerten muss.

Rechenbeispiel: Für die Analyse der Logbuchdaten wird 1 Stunde pro Woche veranschlagt. Dies bedeutet einen Aufwand von 1/2 Tag im Monat beziehungsweise 6 Tagen im Jahr.

Einrichtung von Updates

Da die TCP/IP-Technologie einer starken Dynamik und permanenten Veränderung unterworfen ist, muss davon ausgegangen werden, dass im Abstand von drei bis sechs Monaten ein Update des VPN durchgeführt werden muss, um den neuen

Anforderungen gerecht zu werden. Diese Updates erfordern ebenfalls einen bestimmten Zeitaufwand, da sie getestet werden müssen, um einen weiterhin sicheren Betrieb des VPN garantieren zu können.

Rechenbeispiel: Für diese Arbeit müssen pro Update 2 Tage vorgesehen werden, das bedeutet im Schnitt 6 Tage im Jahr.

Genereller administrativer Aufwand für das VPN

Für den sicheren Betrieb des VPN müssen Backups des aktuellen Regelwerks und der Logbuchdaten, regelmäßige Löschungen der Protokolldaten im Sicherheitsmanagement etc. durchgeführt werden.

Rechenbeispiel: Für diese generellen Arbeiten muss ein Aufwand von 1 Stunde pro Woche, das heißt von 1/2 Tag im Monat beziehungsweise 6 Tagen im Jahr, berücksichtigt werden.

Auswertung der Logbuchdaten im Sicherheitsmanagement

Da das Sicherheitsmanagement eines VPN sehr sicherheitskritisch ist, muss ein Revisor in regelmäßigen Abständen alle Aktionen der Administratoren des Management Systems mit Hilfe der Logbuchdaten des Sicherheitsmanagements überprüfen.

Rechenbeispiel: Für diese Arbeit sollen 3 Stunden im Monat berücksichtigt werden, das heißt 6 Tage im Jahr.

Sicherer Betrieb eines VPN

Damit mit Hilfe eines VPN ein effektiver Schutz für die Kommunikation durch das unsichere Netz gewährleistet werden kann, müssen die folgenden Bedingungen erfüllt sein:

- Das VPN-Konzept muss in das IT-Sicherheitskonzept der Organisation eingebunden werden.
- Der Betrieb des VPN muss auf eine umfassende Sicherheitspolitik aufbauen.
- Das VPN muss korrekt installiert sein.
- Das VPN muss korrekt administriert werden.

Aus diesem Grund ist eine regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen notwendig. Hierbei soll festgestellt werden, ob die unterschiedlichen Maßnahmen ordnungsgemäß eingehalten werden.

Diese Überprüfung muss alle Sicherheitsmaßnahmen einschließen, die zum sicheren Betrieb des VPN beitragen.

- Technische Sicherheitsmaßnahmen:
  - Durch regelmäßige Tests sollte überprüft werden, ob die in der Sicherheitspolitik festgelegten Regeln korrekt umgesetzt worden sind.
  - Mit einem Penetrationstest sollte überprüft werden, ob das VPN-System sicher konfiguriert ist.
- Infrastrukturelle Sicherheitsmaßnahmen:
  - In regelmäßigen Abständen sollte überprüft werden, ob die infrastrukturellen Sicherheitsmaßnahmen (zugangsgesicherter Raum, geschützte Leitungsführung, Dokumentation und Kennzeichnung der Verkabelung des VPN usw.) eingehalten werden.
- Organisatorische Sicherheitsmaßnahmen:
  - In zyklischen Abständen muss überprüft werden, ob neue ungesicherte Verbindungen nach außen geschaffen wurden.
  - Die Logbuchdaten müssen regelmäßig überprüft werden, ob beispielsweise Angriffsversuche stattgefunden haben.
- Personelle Sicherheitsmaßnahmen:
  - In regelmäßigen Abständen sollten Aktionen eingeleitet werden, die das Sicherheitsbewusstsein erhöhen, zum Beispiel Rundschreiben, Schulungen, Informationsveranstaltungen

Durchzuführende Maßnahmen	Aufwand
Technische Sicherheitsmaßnahmen	2 Tage pro Jahr
Infrastrukturelle Sicherheitsmaßnahmen	2 Tage pro Jahr
Organisatorische Sicherheitsmaßnahmen	2 Tage pro Jahr
Personelle Sicherheitsmaßnahmen	6 Tage pro Jahr
Summe	12 Tage pro Jahr

Tabelle 10.4: Aufwendungen für den sicheren Betrieb eines VPN

Durchzuführende Maßnahmen	Aufwand
Rechteverwaltung	6 Tage pro Jahr
Analyse der Logbuchdaten	6 Tage pro Jahr
Einrichtung neuer Dienste	6 Tage pro Jahr
Genereller administrativer Aufwand	6 Tage pro Jahr
Auswertung der Logbuchdaten im Sicherheitsmanagement	6 Tage pro Jahr
Weitere Maßnahmen für den sicheren Betrieb eines VPN	12 Tage im Jahr
Summe	42 Tage pro Jahr

Tabelle 10.5: Aufwendungen für die Aufrechterhaltung des Betriebs eines VPN

Für die Aufrechterhaltung des Betriebs eines VPN, über das 300 Mobil- und Telearbeiter sowie 20 Organisationseinheiten unter den beschriebenen Annahmen kommunizieren dürfen, ergibt sich ein Kostenaufwand von ca. EUR 31 500 im Jahr.

10.1.3 Zusammenfassung aller Kosten im Sinne der Total Cost of Ownership

Aufwendungen für ein VPN sind zum einen die Anschaffungskosten, die zwischen EUR 93 900 und EUR 296 300 liegen können, und zum anderen die Kosten für die Aufrechterhaltung des Betriebs, die in unserem Rechenbeispiel mit EUR 31 500 im Jahr veranschlagt werden.

Diese Zahlen hängen sehr stark von der Struktur und der Größe der Organisation ab. Außerdem müssen die folgenden Aspekte berücksichtigt werden:

- Typ des verwendeten VPN
- Qualität des VPN-Konzepts
- Möglichkeit eines automatischen Updates von zentraler Stelle
- funktionierendes Redundanz-Konzept
- Anzahl der Benutzer, die über das VPN kommunizieren dürfen
- Veränderung der Kommunikationsprofile
- Qualifikation der Administratoren des Sicherheitsmanagements
- Betriebszeiten
- Veränderungen der Benutzer
- Veränderung der Netzstruktur
- Tiefe der Auswertung der Logbuchdaten
- verwendetes Authentikationsverfahren

Bei der Auswahl eines VPN-Systems ist neben der gewünschten Sicherheit auch die Möglichkeit des einfachen und kostengünstigen Managements der einzelnen VPN-Komponenten ein wichtiges Kriterium, damit das System im Sinne der Total Cost of Ownership wirtschaftlich betrieben werden kann.

10.2 Kosten-Nutzen-Betrachtung im Hinblick auf die Sicherheit

Am Beispiel einer Bank mit 100 Filialen soll eine Kosten-Nutzen-Betrachtung eines VPN-Systems durchgeführt werden. Dabei wird angenommen, dass ohne den Einsatz eines VPN-Systems die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr hoch ist.

Profit der Bank im letzten Jahr

- Profit: EUR 25 000 000

Kosten eines VPN-Systems

- Anschaffungskosten: EUR 250 000 (1 % des Profits)
- Betriebskosten: EUR 35 000/Jahr

Beschreibung eines möglichen Angriffs

Die Bank wird von einem professionellen Kriminellen über das Internet angegriffen. Dieser liest während einer Übertragung zwischen der Zentrale und einer Filiale der Bank die Namen und Kontostände der 500 wichtigsten Kunden mit. Diese Daten werden dann via Internet veröffentlicht, Fernsehen und Presse berichten und die Bank erleidet dadurch einen enormen Imageverlust.

Möglicher Schaden durch diesen Angriff

Durch den enormen Imageverlust wechseln sehr viele Kunden zu einer anderen vertrauenswürdigeren Bank. Der dadurch entstehende Schaden für die angegriffene Bank wird folgendermaßen angenommen:

- sofort: EUR 12.500.000 (50 % des Gewinns)
- mittelfristig: EUR 2.500.000/Jahr

Zusammenfassung

Unter der Voraussetzung, dass der Schaden mit Hilfe eines VPN-Systems vollständig verhindert worden wäre, hätte sich die Investition in ein VPN-System gelohnt. Mit der Investition von 1 % des Gewinns kann der Bank ein Schaden erspart werden, der sich auf ein Vielfaches der Investition beläuft (in diesem Beispiel das 50fache).

Mit Bekanntwerden des Angriffs werden auch »Trittbrettfahrer« animiert, den Angriff nachzuahmen. Dadurch steigt das Risiko, erneut Opfer zu werden, und zu den Aufwendungen zur Behebung des Schadens kommen die Aufwendungen für die Anschaffung eines geeigneten VPN-Systems, um weiteren Angriffen vorzubeugen.

10.3 Wahrscheinlichkeit eines bestimmten Profits

Die folgende Abbildung stellt dar, wie die Höhe des Investments in Sicherheitsmechanismen vom eigenen Schutzbedarf und der Wahrscheinlichkeit, einen bestimmten Profit erreichen zu können, abhängig ist.

Die Abbildung zeigt, dass in Bereichen mit hohem Schutzbedarf (zum Beispiel in Finanzinstituten) höhere Investitionen in Sicherheitsmaßnahmen notwendig sind, um die gleiche Chance auf einen bestimmten Gewinn zu bewahren.

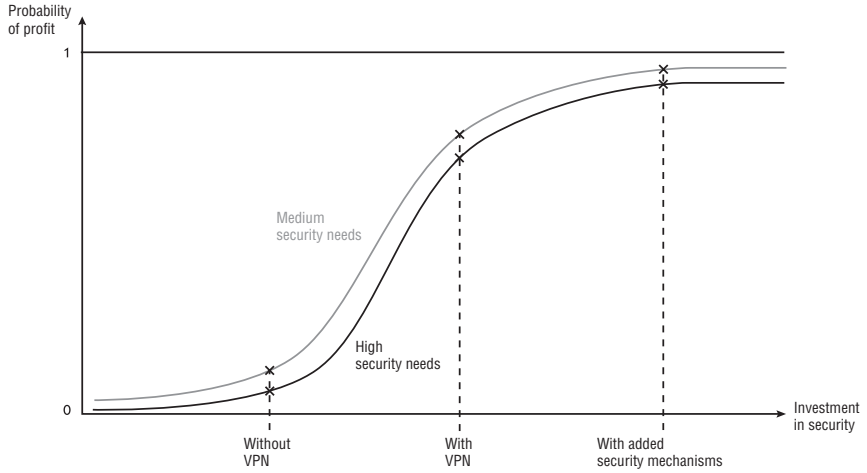

Abb. 10.1: Investment in Sicherheitsmechanismen und Wahrscheinlichkeit eines bestimmten Profits

Mit den Investitionen in Sicherheitsmechanismen steigt auch die Wahrscheinlichkeit, einen bestimmten Profit zu erreichen. Das heißt, die Anschaffung von Sicherheitssystemen wie VPN, Firewall-System, Intrusion Detection und Viren-Scanner ist ein Investment in die Absicherung des Gewinns. Die Wahrscheinlichkeit auf einen bestimmten Gewinn wird um so höher, je höher die Ausgaben für Sicherheitsmechanismen sind. Der Gewinn kann durch diese Maßnahmen allein aber nie hundertprozentig sicher sein, da immer ein Restrisiko bestehen bleibt.

Die Wahrscheinlichkeit der Gewinnerzielung hängt auch vom Schutzbedarf und damit von der Eintrittswahrscheinlichkeit eines Angriffs ab. Bei höherer Eintrittswahrscheinlichkeit steigt auch der Schutzbedarf vor einem Angriff.

Ist der Schutzbedarf sehr hoch, ist die Wahrscheinlichkeit auf einen Profit geringer als bei niedrigem Schutzbedarf. Bei Verzicht auf Sicherheitsmechanismen ist dieser Unterschied viel größer als bei hohem Einsatz von Sicherheitsmechanismen, da die Eintrittswahrscheinlichkeit eines Angriffs bei niedrigem Schutzbedarf kleiner ist.

Letztlich ist die Unternehmensleitung für die Sicherheit in einem Unternehmen verantwortlich und muss über das richtige Kosten-Nutzen Verhältnis entscheiden. Die Unternehmensleitung ist gut beraten, wenn sie einen gewissen Prozentsatz des Gewinns als Gewinnversicherung für die IT-Sicherheit ausgibt. Dieser Prozentsatz wird bei Unternehmen, deren Image als vertrauenswürdiges Unternehmen die Basis ihres Erfolgs darstellt (beispielsweise bei Banken und Versicherungen), höher liegen als bei Unternehmen wie Speditionen und Brauereien, bei denen die IT-Sicherheit in bezug auf das Image eine untergeordnete Rolle spielt.

10.4 Kosten-Nutzen-Betrachtung im Hinblick auf die Kommunikation

Mit der Hilfe von Virtual Private Networks können Kosten im IT-Bereich massiv gesenkt werden.

Im Folgenden werden zwei mögliche Lösungen zum Aufbau einer vertrauenswürdigen Kommunikationsinfrastruktur zwischen mehreren Niederlassungen und der Zentrale eines Unternehmens verglichen.

Bedingungen

- Die Zentrale des Unternehmens ist in Frankfurt. Niederlassungen befinden sich in Aachen, Berlin, Hamburg und München.
- Die Übertragungsrate zwischen der Zentrale und den Niederlassung soll 2 Mbit/s betragen.
- Beim Datenvolumen wird davon ausgegangen, dass im Schnitt nicht mehr als 30 Gigabyte im Monat übertragen werden. Das macht bei einer Auslastung von 100 % mehr als 5 Stunden Übertragungszeit pro Tag aus.

Lösung 1

Zwischen der Zentrale und den Niederlassungen werden »Leased Links« mit 2 Mbit/s genutzt, um eine IP-Kommunikation zu realisieren. Die notwendigen Router hat das Unternehmen bereits gekauft.

Eine zusätzliche Sicherheit wird nicht eingesetzt, da die Wahrscheinlichkeit eines Schadens bei Leased Links als gering anzusetzen ist.

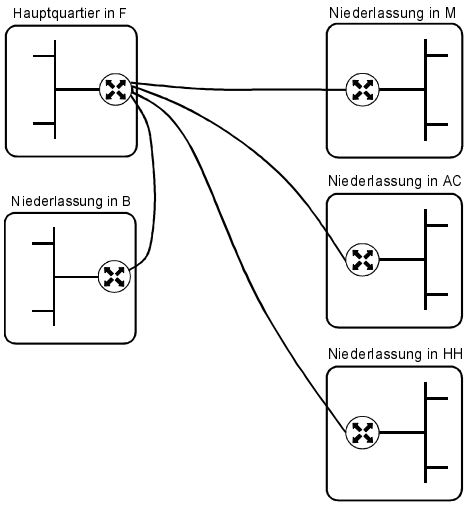

Abb. 10.2: Kommunikation eines Unternehmens über »Leased Links«

Kosten dieser Lösung (in EUR)

	Miete/Monat	Kosten/Monat für Datenvolumen	Einmalige Kosten für Installation	Einmalige Investitionskosten umgerechnet in Kosten/Monat über 5 Jahre
Frankfurt/ Aachen	ca. 2 750,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ Hamburg	ca. 3 400,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ Berlin	ca. 3 500,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ München	ca. 3 150,–	0	ca. 2 100,–	ca. 35,–
Summe	ca. 12 800,–	0		ca. 140,–

Die Kosten pro Monat betragen in diesem Beispiel 12 940,– EUR.

Lösung 2

Die Zentrale und die Niederlassungen werden mit Hilfe von »T-InterConnect«-Anschlüssen mit 1,92 Mbit/s an das Internet angeschlossen. Die notwendigen Router hat das Unternehmen bereits gekauft.

Zusätzlich wird in jede Niederlassung ein VPN-Gateway installiert, damit eine vertrauenswürdige Kommunikation gewährleistet werden kann.

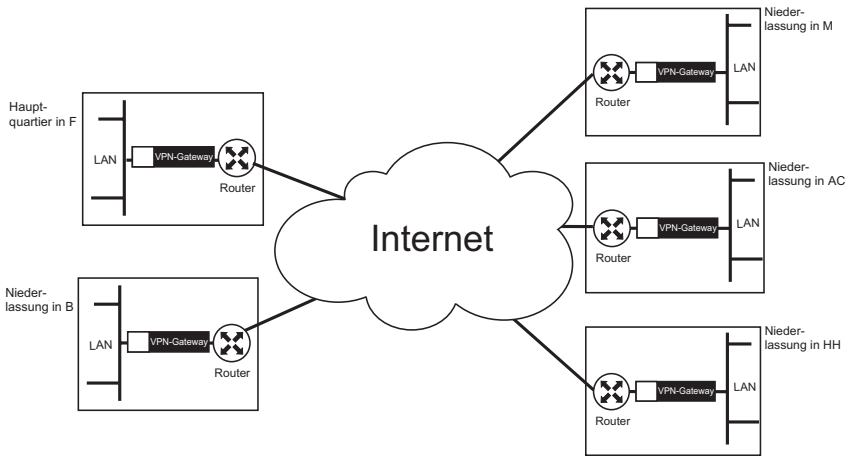

Abb. 10.3: VPN-gesicherte Kommunikation eines Unternehmens über das Internet

Kosten dieser Lösung (in EUR)

	Miete/ Monat	Kosten/ Monat für Datenvolumen	Einmalige Kosten für VPN-Gateways	Einmalige Kosten für Installation der VPN-Gateways	Einmalige Kosten für Installation der Anschlüsse	Einmalige Investitionskosten umgerechnet in Kosten/Monat über 5 Jahre
Frankfurt	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Aachen	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Hamburg	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Berlin	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
München	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Summe	ca. 4 500,-	ca. 4 250,-				ca. 650,-

Die Kosten pro Monat betragen in diesem Beispiel ca. 9 400,- EUR

Vergleich der beiden Lösungen

- Die erste Lösung kostet im Monat ca. 3 500,- EUR mehr und bietet einen höheren garantierten Datendurchsatz.
- Die zweite Lösung ist flexibler in ihrer Verwendung, da sie auf einer weltweit verbreiteten Infrastruktur basiert und bietet eine höhere Sicherheit.
- Soll mit Niederlassungen im Ausland kommuniziert werden, vergrößert sich die Kostendifferenz zwischen den beiden Lösungen wesentlich.
- Die Sicherheit der ersten Lösung beruht lediglich auf der Annahme, dass die Leased Links nicht abgehört werden.
- Die Sicherheit der zweiten Lösung wird vom Unternehmen eigenverantwortlich und seinem Schutzbedarf entsprechend realisiert.

10.5 Kosten-Nutzen-Betrachtung im Hinblick auf die Nicht-Realisierung von Kommunikation

Verzichtet ein Anwender aufgrund von Sicherheitsbedenken darauf, das Internet als geschäftliches Kommunikationsmittel zu nutzen, so kann er das darin liegende – oftmals erhebliche – Rationalisierungspotenzial nicht ausschöpfen. Auf längere Sicht droht dadurch ein Verlust geschäftlicher Handlungsmöglichkeiten.

Aus diesem Grund kann die Investition in IT-Sicherheitskomponenten, sofern sie geringer ist als die dadurch mögliche Wertschöpfung, zu einer Steigerung der Effizienz beitragen, die letztlich auch die Wachstumschancen des Unternehmens verbessern kann.