Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitseigenschaften von Standleitungstechnologien

Studie

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 200363, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Impressum

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53179 Bonn

Ersteller

T-Systems Enterprise Services GmbH
Systems Integration
Service & Solution Center Testfactory & Security
Goslarer Ufer 35
D-10589 Berlin

Kontakt	Telefon / Fax	E-Mail
Dr. Eberhard von Faber	(228) 9841-564 (228) 9841-590	Eberhard.Faber@t-systems.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Zusammenfassung

Unter dem Begriff „Standleitung“ wird im Allgemeinen eine Datenverbindung als Dienst mit einer vertraglich vereinbarten Qualität an Verfügbarkeit und Bandbreite für die Datenübertragung zwischen zwei oder mehreren Endpunkten angeboten. Dabei stellt der Provider (Diensteanbieter) einen Teil seiner Netzinfrastruktur zur Verfügung. Hierfür existiert eine Reihe von Lösungen auf unterschiedlichen technologischen Plattformen. In diesem Dokument wird eine vergleichende Sicherheitsbewertung der einzelnen Lösungen für die Schutzziele „Vertraulichkeit“ und „Integrität“ gegenüber Dritten vorgenommen.

Klassifikation der betrachteten Lösungen nach Schichtenmodell

Für die Klassifikation der technischen Lösungen bietet sich das OSI-Schichtenmodell an. Dabei wird zwischen der Bereitstellung eines physischen Mediums, einer Standard-Festverbindung (Schicht 1), eines Switched Links (Schicht 2) oder einer IP-Plattformlösung (Schicht 3) unterschieden.

Die Standleitung als die vom Kunden exklusiv genutzte physische Leitung, z. B. als Kupfer-Doppelader oder auch als LWL-Verbindung (Dark Fiber), gibt es nicht – jedenfalls nicht als Standardprodukt der großen Anbieter. Es kann jedoch vorkommen, dass Spezialösungen diese Variante realisieren. Als Alternative werden Satelliten- oder Richtfunkübertragungen angeboten. Allen diesen Lösungen entspricht die Bereitstellung eines „Dienstes“ unterhalb Schicht 1 des OSI-Schichtenmodells. Wir sprechen in diesem Zusammenhang von Schicht „0“. Hierbei liegt der größte Teil der technischen Umsetzung der Datenübertragung beim Anwender (Kunde).

Am anderen Ende der Skala befinden sich komplexe Dienste auf Schicht 3, die als IP-Plattformlösungen bezeichnet werden. Hier werden Zusatzdienste für Verschlüsselung (IPSec), Firewall, Remote-Dial-In etc. angeboten. Garantien für Verfügbarkeit, Bandbreite und Quality of Service (QoS) gehören ebenso dazu.

Verantwortungsbereich des Kunden bzw. des Providers

Allgemein kann man sagen, dass umso mehr Netztechnik und unterschiedliche Übertragungstechnologie des Providers zum Einsatz kommt, je höher der Dienst im OSI-Schichtenmodell angesiedelt ist. Es liegt auf der Hand, dass in dem Maße, in dem man Verantwortung auf den Serviceprovider überträgt, das Vertrauen in dessen Leistung und Integrität steigen muss. Dies gilt für den Serviceprovider als Vertragspartner und Unternehmung. Im internationalen Bereich wird oft auch auf die Netze von Kooperationspartnern zurückgegriffen, um Standorte, die nicht im Einzugsgebiet liegen, zu erschließen.

Sicherheitsbewertung

- Schicht „0“ und 1

  Das Risiko des Abhörens von Leitungen im WAN-Bereich ist auf Grund seines hohen technischen Aufwandes eher von geringer Bedeutung. Das Auskoppeln der Signale, das Demultiplexen oder gar die Manipulation ist nur mit speziellem Know-how und hohem technischen Aufwand möglich. Daher eignen sich Standleitungslösungen auf niedrigen Schichten („0“ und 1) ohne zusätzliche Verschlüsselung für die Übertragung von Daten mit mittlerem (normalen) Schutzbedarf. Eine Ausnahme bilden Satellitenübertragungen, die aufgrund des einfachen Zugangs zum Medium nur für niedrigen Schutzbedarf geeignet sind.

- Schicht 2 und 3

  Mit dem Einsatz von Lösungen auf höheren Schichten (2 und 3) steigt die theoretische Gefährdung durch Dritte stark an. Unter der Voraussetzung, dass sich Unberechtigte Zugang zu den Netzelementen des jeweiligen Übertragungsweges verschaffen können, sind je nach eingesetzter Lösung unterschiedliche Szenarien denkbar. Dabei ist der Zugangsrouter mit seinem LAN-Interface am meisten gefährdet. Aber auch die Netzknoten bieten eine Reihe technischer Möglichkeiten für Angriffe, wie z. B. die missbräuchliche Verwendung von Spiegelports.

  Bei IP-Plattformlösungen können zusätzlich Angriffe über das Internet durchgeführt werden, falls öffentliche IP-Adressen verwendet werden, die zusätzlich aus dem Internet erreichbar sind.

  Lösungen auf Schicht 2 oder 3 ohne zusätzliche Verschlüsselung sind für mittleren Schutzbedarf geeignet, sofern vom Provider die Grundschutzmaßnahmen für alle Netzkomponenten (in der Regel Router und Switches) auf dem gesamten Übertragungsweg lückenlos umgesetzt werden. Andernfalls können nur Daten mit niedrigem Schutzbedarf unverschlüsselt übertragen werden.

VLANs und „Sharing Access“

Im Rahmen von Diskussionen über Netzsicherheit wird häufig mit der VLAN-Technologie argumentiert. Virtuelle LANs ermöglichen es, den Datenverkehr auf Schicht 2 nach frei wählbaren Kriterien zu strukturieren, ohne dabei auf Schicht 3-Informationen zurückgreifen zu müssen. Die VLAN-Technologie beinhaltet jedoch keine Sicherheitsmechanismen.

Sharing Access ist die Bezeichnung für eine Lösung, bei der verschiedene Kunden eines Providers über dieselbe Zugangstechnik geführt werden. Hier gibt es verschiedene Lösungen.

- Aus sicherheitstechnischer Sicht nicht zu empfehlen ist, dass sich zwei kleine Unternehmen oder Behörden unter einem Dach einen ATM-Switch teilen.

- Teilen sich mehrere Unternehmen oder Behörden eine SDH-Anbindung (z. B. bei der Erschließung eines Gewerbegebietes), hängt die Sicherheit im Wesentlichen vom physischen Zugangsschutz ab. Angreifer könnten, das Know-how vorausgesetzt, Datenströme über Spiegelports doppeln oder umleiten.

Fazit

Zusammenfassend kann festgestellt werden, dass viele der vorgestellten Technologien ohne zusätzliche Maßnahmen bereits dem Schutzbedarf „normal“ genügen, wenn der Provider entsprechende Grundschutzmaßnahmen umgesetzt hat. Im Falle eines Schutzbedarfs von „hoch“ oder „sehr hoch“ sollte der Kunde immer auf Verschlüsselung zurückgreifen. Provider bieten diese Möglichkeit bei den IP-Plattformlösungen an. Hier hängt es vom Vertrauen sowohl in die Seriosität als auch in das Know-how des Providers ab, ob man den Schutz seiner sensitiven Daten dem Provider überlässt. Die Bewegung des Anbietermarktes wie Konkurse, Verkäufe und Fusionen sollten auch berücksichtigt werden.

Schließlich soll darauf hingewiesen werden, dass es dem Kunden obliegt, durch den Einsatz von Ende-zu-Ende-Verschlüsselung eine entscheidende Verbesserung der Sicherheit zu erreichen. So können z. B. besonders sensitive Client-Server-Verbindungen durch den Einsatz von Subnetzen und ggf. IPSec geschützt werden.

2 Einleitung

2.1 Inhalt

Bei der Vernetzung von Standorten greifen Behörden und Unternehmen häufig auf Angebote von Telekommunikationsdiensteanbietern (Provider, Betreiber) zurück, die alle unter dem Oberbegriff „Standleitung“ zusammengefasst werden können, aber teilweise mit unterschiedlichen Technologien realisiert werden. Ziel des vorliegenden Dokuments ist es, eine vergleichende Bewertung der Sicherheitseigenschaften dieser verschiedenen Standleitungstechnologien zu geben. Dabei soll ein Überblick über häufig eingesetzte Technologien für die Standortvernetzung gegeben werden.

Die Sicherheitsbewertung der einzelnen Lösungen wird nur für die Schutzziele „Vertraulichkeit“ und „Integrität“ vorgenommen. Das Schutzziel „Verfügbarkeit“ wird nicht berücksichtigt, da davon ausgegangen wird, dass die Provider diesen Aspekt gut beherrschen.

Die Bewertung erfolgt für den normalen (niedrigen bis mittleren) Schutzbedarf für die zu übertragenen Daten als auch für den Fall, dass mindestens eines der Schutzziele mit hohem Schutzbedarf einzustufen ist. Es wird davon ausgegangen, dass für die Bereiche Organisation, Personal und Infrastruktur die Provider ausreichende Maßnahmen umgesetzt haben. Innentäterangriffe und damit Angriffe des Providers gegen den Kunden werden insofern nicht betrachtet.

Die Einordnung der Lösungen und Produkte orientiert sich am OSI-Schichtenmodell. Vereinfacht gesagt stellt der Provider dem Kunden einen Dienst zur Verfügung, der weitestgehend der Funktionalität eines OSI-Schicht-Dienstes entspricht. Daran wird sich auch die Gliederung dieses Dokuments orientieren.

Die betrachteten Angriffsszenarien betreffen Angriffe Dritter und beschränken sich bei Lösungen bis zur Schicht 2 auf passive Angriffe, d. h. das Abhören der übertragenen Daten, und auf aktive Angriffe auf Netzknoten. Ab Schicht 3 werden auch aktive Angriffe auf Endgeräte betrachtet, da es sich dabei in der Regel um IP-Endgeräte handelt. Ein aktiver Angriff auf ein Endgerät ausgehend von einer unteren Schicht setzt das vollständige Nachbilden der MAC- und IP-Schicht und detaillierte Kenntnisse der Netztopologie voraus, was für einen Angreifer eine hohe Hürde darstellt und deshalb hier nicht betrachtet wird.

Das OSI-Modell bildet auch die Grundlage für die weitere Sicherheitsbewertung nach IT-Grundschutz des BSI.

2.2 Aufbau des Dokuments

In Kapitel *3 Bewertungskriterien* werden die Kriterien definiert, nach denen die betrachteten Lösungen bewertet werden.

In Kapitel *4 Das OSI-Schichtenmodell* wird das OSI-Schichtenmodell beschrieben, nach dem die verschiedenen Lösungen in diesem Dokument geordnet werden.

In Kapitel *5 Zusammenfassung der betrachteten Lösungen* findet man eine Übersicht über die betrachteten Lösungen und ihre Bewertung.

In Kapitel *6 Standleitungslösungen* werden diese Lösungen im Detail beschrieben und ihre Sicherheit ausführlich bewertet.

In Kapitel *7 Vergleichende Sicherheitsbewertung* erfolgt eine tabellarische Zusammenfassung der Gefährdungen der betrachteten Lösungen und die Zuordnung zum Schutzbedarf gemäß der IT-Grundschutz-Vorgehensweise des BSI (BSI-Standard 100-2).

In Kapitel *8 VLANs und „Sharing Acccess“* werden zwei aktuelle Schlagwörter aus dem Bereich Netzsicherheit in den Kontext der Studie sortiert.

3 Bewertungskriterien

3.1 Kundenleistung / Providerleistung

In dem nachfolgend dargestellten Abhängigkeitsmodell wird davon ausgegangen, dass mit zunehmender Leistungserbringung durch den Provider die Eigenleistung des Kunden sinken wird. Um sich dies zu verdeutlichen, setzt man beispielsweise den hohen technischen Aufwand, den der Kunde bei einer Dark-Fiber-Lösung selbst leisten muss, ins Verhältnis zu einer IP-Plattform, die dem Kunden gemanagte Zugangsrouter, Firewalls und weitere Dienste bereitstellt. Aus diesem Grund ergänzen sich Kundenleistung und Providerleistung immer zu 100% (siehe Tabelle 1).

Lösung	Kundenleistung	Beschreibung der Kundenmaßnahmen	Providerleistung	Beschreibung der Providermaßnahmen
	0%	Eine Kundenleistung von 0% darf als rein theoretisch betrachtet werden. Eine gewisse Einflussnahme besteht immer. Zusätzlich hat der Kunde die Möglichkeit, auf höheren Schichten Sicherheitsdienste zu realisieren.	100%	Das Angebot des Providers (aus 60%) wird zusätzlich um die Bereitstellung von Verschlüsselung erweitert.
IP-Plattformlösung mit Verschlüsselung	20%	Der Kunde benutzt lediglich das Produkt. Die genaue Beschreibung des überlassenen Dienstes ist Bestandteil des Vertrages. Der Schutz der Daten (Vertraulichkeit und Integrität) wird dem Provider überlassen.	80%	Entspricht der Stufe 100%
IP-Plattformlösung ohne Verschlüsselung	40%	Der Kunde benutzt lediglich das Produkt. Die genaue Beschreibung des überlassenen Dienstes ist Bestandteil des Vertrages. Der Einsatz von Verschlüsselung wird ggf. durch den Kunden realisiert.	60%	Bereitstellung der kompletten virtuellen LAN-Infrastruktur einschließlich Konfiguration, Management, Entstörung und Überwachung. Realisierung von Zusatzdiensten (Dial-In, Voice Gateway), die nicht typisch für Standleitungen sind. Die genaue Beschreibung der gelieferten Dienste ist Bestandteil des Vertrages.
Switches Links	60%	Bereitstellung der Gateways für den LAN/WAN Netzübergang. Einbindung dieser Gateways in das lokale Netz. Die Konfiguration der Gateways übernimmt der Provider.	40%	Bereitstellung einer zellen- oder rahmenbasierten Punkt-zu-Mehrpunkt Netzstruktur, die Redundanz und Ausfallsicherheit gewährleistet. Der Provider übernimmt Garantien für die vertraglich vereinbarte Bandbreite.
Satellitenübertragung, SFV, Leased Links	80%	Bereitstellung des LAN/WAN Netzübergangs für jeden angeschlossenen Standort. Punkt-zu- Mehrpunkt Verbindungen werden über verschiedene Punkt-zu-Punkt Verbindungen realisiert.	20%	Bereitstellung einer dienstneutralen transparenten Punkt-zu-Punkt Übertragung. Bereitstellung einer Endeinrichtung. Maßnahmen zur Aufrechterhaltung des Betriebes.

Lösung	Kunden-leistung	Beschreibung der Kundenmaßnahmen	Provider-leistung	Beschreibung der Providermaßnahmen
Dark Fiber Richtfunk	100%	Vollständige Bereitstellung aller übertragungstechnischen Einrichtungen und aller höheren Dienste.	0%	Keinerlei Aufwand und Einflussmöglichkeit.

Tabelle 1: Kunde/Provider-Verhältnis

3.2 Potenzielle Fremdeinwirkung (PF) auf den Provider

Zusätzlich wird ein Maß für die potenzielle Fremdeinwirkung auf den Provider definiert, also die grundsätzlichen Möglichkeiten eines Dritten, die Vertraulichkeit oder Integrität der übertragenen Daten im Leistungsbereich des Providers zu verletzen (siehe Tabelle 2). „Grundsätzlich“ bedeutet hier, dass die Sicherheitsmaßnahmen, die der Provider ggf. bereits ergriffen hat, um eine Fremdeinwirkung zu verhindern, *nicht* berücksichtig werden.

Nähere Angaben zu den Möglichkeiten der Fremdeinwirkung auf den Provider werden in dem entsprechenden Kapitel zur jeweiligen Lösung besprochen.

PF	Einflussnahme des Angreifers	physischer Zugriff	Signalgewinnung	Datengewinnung
0	Keine Einflussnahme auf Daten oder Datengewinnung möglich (Verschlüsselung). Ausreichender Zugangschutz zur Technik der Tunnelendpunkte ist gegeben.			
1	extrem erschwert	hoher technischer Aufwand	hoher technischer Aufwand	hoher technischer Aufwand
2	Erschwert	geringer technischer Aufwand	hoher technischer Aufwand	hoher technischer Aufwand
3	bedingt möglich	geringer technischer Aufwand	geringer technischer Aufwand	hoher technischer Aufwand
4	Möglich	Datensicherheit hängt im Wesentlichen vom physischen Zugangsschutz zur Zugangstechnik ab.	geringer technischer Aufwand	geringer technischer Aufwand

Tabelle 2: Potenzielle Fremdeinwirkung

4 Das OSI-Schichtenmodell

Das OSI-Schichtenmodell oder OSI-Referenzmodell beschreibt das Durchlaufen von sieben Schichten, in denen Funktionen und Protokolle definiert sind, denen jeweils eine bestimmte Aufgabe bei der Kommunikation zwischen zwei Systemen zugeordnet ist. Die Protokolle einer Schicht sind von den Protokollen der über- und untergeordneten Schichten weitgehend unabhängig, so dass die Verhaltensweise eines Protokolls sich wie bei einer direkten Kommunikation mit der entsprechenden Schicht auf der Gegenseite darstellt (z. B. Erzeugen und Auswerten der IP-Adressen).

Die Übergänge zwischen den Schichten sind Schnittstellen, die von den Protokollen verstanden werden müssen. In Ausnahmefällen kommt es auch vor, dass sich Protokolle über mehrere Schichten erstrecken und mehrere Aufgaben abdecken (z. B. http in der Sitzungs-, Darstellungs- und Anwendungsschicht).

Protokolle sind eine Sammlung von Regeln zur Kommunikation auf einer bestimmten Schicht des OSI-Modells. Die Endgeräte der Endsysteme und das Übertragungsmedium sind jedoch aus dem OSI-Modell ausgeklammert.

In diesem Dokument wird auch eine Schicht „0“ betrachtet, die nicht zum üblichen OSI-Schichtenmodell gehört.

Schicht „0“ – Das Übertragungsmedium

Das physische Übertragungsmedium ist kein Bestandteil der Schicht 1 des OSI-Schichtenmodells. Dafür wird im weiteren Verlauf des vorliegenden Dokumentes die Schicht „0“ eingeführt. Mit der Schicht „0“ ist beispielsweise ein Lichtwellenleiter oder die „Luftschnittstelle“ bei Funkübertragung – per Richtfunk, WLAN oder Satellit – gemeint.

Schicht 1 – Die Bitübertragungsschicht

Die Bitübertragungsschicht definiert die elektrische, mechanische und funktionale Schnittstelle zum Übertragungsmedium. Die Protokolle dieser Schicht unterscheiden sich nur nach dem eingesetzten Übertragungsmedium und -verfahren. Schicht 1-Protokolle sind beispielsweise Protokolle mit PDH- oder SDH-Technik, wie G.703/G.704 oder ein ISDN-BRI-Anschluss (I.430).

Schicht 2 – Die Sicherungsschicht

Die Sicherungsschicht sorgt für eine zuverlässige und funktionierende Verbindung zwischen Endgeräten über das Übertragungsmedium. Zur Vermeidung von Übertragungsfehlern und Datenverlust enthält diese Schicht Funktionen zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle. Auf dieser Schicht findet auch die physische Adressierung von Datenpaketen statt. Zu den Schicht 2-Protokollen gehören ATM und Frame Relay, aber auch Ethernet.

Schicht 3 – Die Vermittlungsschicht

Die Vermittlungsschicht steuert die zeitliche und logische getrennte Kommunikation zwischen den Endgeräten, unabhängig von Übertragungsmedium und -topologie. Auf dieser Schicht erfolgt erstmals die logische Adressierung der Endgeräte. Die Adressierung ist eng mit dem Routing (Wegfindung vom Sender zum Empfänger) verbunden. Die größte Bedeutung hat heutzutage IP, weswegen es hier als einziges Protokoll der Schicht 3 betrachtet wird.

Darüber hinaus werden noch die Schichten 4 – 7 im OSI-Schichtenmodell definiert. Auf diesem Niveau werden allerdings Dienste angeboten, die über eine Datenübertragung weit hinausgehen. Diese gehören nicht zum Untersuchungsgegenstand. Daher wird hier auf eine Darstellung verzichtet.

5 Zusammenfassung der betrachteten Lösungen

Die folgende Tabelle 3 fasst die unten behandelten Lösungen in einer Übersicht zusammen. In Tabelle 4 werden die Bewertungen zusammengefasst.

Details zu den Lösungen und ihren Bewertungen findet man im folgenden Kapitel 6 *Standleitungslösungen*.

5.1 Übersicht der betrachteten Lösungen

Lösung	Schicht	Medium	Netzknoten	Endgeräte	Protokoll*
Dark Fiber	0	Glasfaser	—	—	—
Satellitenübertragung	0	„Luftschnittstelle“	—	Multiplexer mit meist optischem Eingang†	—
Richtfunk	0	„Luftschnittstelle“	—	Multiplexer mit meist optischem Eingang	—
SFV, Leased Links	1	Verbindung kann über verschiedene Medien geführt werden	Add/Drop Multiplexer, Cross Connectoren	Digitale Modems (PDH), SMT (Synchrone Multiplex Terminals mit SDH Technik)	PDH-, STM-Rahmen
Switched Links	2	Verbindung kann über verschiedene Medien geführt werden	X.25 Netzknoten Frame Relay/ ATM Switches	Data Termination Equipment (DTE für X.25), Router mit ATM/FR Schnittstelle	ATM, FR, X.25
IP-Plattform-Lösung ohne Verschlüsselung	3	Verbindung kann über verschiedene Medien geführt werden	MPLS-Core Switche	CPE-Router mit entsprechender Schicht 2 Schnittstelle	MPLS
IP-Plattform-Lösung mit Verschlüsselung	3	Verbindung kann über verschiedene Medien geführt werden	MPLS-Core Switche	CPE-Router mit IPSec Funktion oder abgesetztes IPSec-Gateway	IPSec

Tabelle 3: Technologiematrix

* Hiermit ist das höchste Protokoll der OSI-Schicht gemeint, das vom Provider zur Verfügung gestellt wird.

† Die sende- und empfangstechnischen Einrichtungen, die für RiFu/Satellit benötigt werden, sind der Komponente MAU (Media Access Unit) zuzuordnen und stellen kein Endgerät für die Daten dar.

5.2 Bewertung der Lösungen

Lösung	Leistungsverteilung Kunde / Provider (in Prozent)	Potenzielle Fremdeinwirkung auf den Provider
Dark Fiber	100 / 0	1
Satellitenübertragung	80 / 20	3
Richtfunk	100 / 0	1
SFV, Leased Links	80 / 20	2
Switched Links	60 / 40	4
IP-Plattform-Lösung ohne Verschlüsselung	40 / 60	4
IP-Plattform-Lösung mit Verschlüsselung	20 / 80	1

Tabelle 4: Bewertung der Lösungen

5.3 Interpretation

Die Leistungsverteilung zwischen Kunde und Provider (Spalte 2 in Tabelle 4) ist ein Indikator für die Verteilung der Verantwortung zur Minimierung der Risiken einer Standleitungslösung mit der jeweiligen Technologie. Beispielsweise stellt der Kunde bei einer Standleitungslösung mit zugekauftem Dark Fiber und Richtfunk alle übertragungstechnischen Einrichtungen bereit und erbringt alle höheren Dienste selbst, die gesamte Verantwortung zur Minimierung der Risiken liegen daher im Zuständigkeitsbereich des Kunden.

Die potenzielle Fremdeinwirkung auf den Provider (Spalte 3 in Tabelle 4) ist ein qualitatives Maß für den Verantwortungsbereich des Providers, der grundsätzlich – aufgrund der eingesetzten Technologie – Fremdeinwirkungen Dritter ausgesetzt ist. Dieser Bereich muss durch Sicherheitsmaßnahmen geregelt werden.

Beispiel Satellitenübertragung versus Standardfestverbindungen (SFV) und Leased Links: Bei gleicher Leistungsverteilung zwischen Kunde (80%) und Provider (20%) sind bei der Satellitenübertragung als gewählter Standleitungstechnologie „mehr“ potenzielle Fremdeinwirkungen auf den Provider zu berücksichtigen (Maßwert = 3) als bei Standardfestverbindungen (SFV) oder Leased Links (Maßwert = 2) als gewählter Standleitungstechnologie.

Beispiel Switched Links versus IP-Plattformlösung ohne Verschlüsselung: Trotz eines größeren Leistungsanteils des Providers (60% statt 40%) sind in gleichem Maße (Maßwert = 4) potenzielle Fremdeinwirkungen auf den Provider zu berücksichtigen.

Beispiel IP-Plattformlösung mit Verschlüsselung: Die Verschlüsselung der Übertragung reduziert die potenzielle Fremdeinwirkung signifikant.

Die Studie enthält demnach *keine Aussagen* zur Gesamtsicherheit eines Unternehmens- oder Konzernnetzes auf der Basis von unterschiedlichen Standleitungstechnologien. Die Gesamtsicherheit wird wesentlich durch die Leistungsverteilung im Netzbereich, das Sicherheitsniveau des Kunden, das Sicherheitsniveau des Providers und die vertragliche Gestaltung bestimmt.

6 Standleitungslösungen

In diesem Abschnitt werden die oben genannten Lösungen im Detail betrachtet. Für jede Lösung wird dabei wie folgt vorgegangen:

- Verbreitung
- Beschreibung der technischen Grundlagen
- Beschreibung des Kundenzugangs (Netzabschluss)
- Beschreibung des Managements
- Sicherheitsbetrachtung
- Fazit

6.1 Übertragungsmedium auf Schicht „0“

6.1.1 Dark Fiber

6.1.1.1 Verbreitung

Dark Fiber konnte nicht als Standardprodukt für eine Standleitung identifiziert werden. Das liegt daran, dass diese Lösung nur dort angeboten werden kann, wo Ersatz- oder Reserve-LWL-Kabel von Providern auf den Strecken vorgehalten werden, die zufällig dem Verbindungswunsch eines Kunden entsprechen.

6.1.1.2 Technische Grundlagen

„Dark Fiber“ ist die Bezeichnung für eine technische Lösung, die dem Kunden das reine physische Übertragungsmedium überlässt. Diese Variante ist gewissermaßen als Schicht „0“ Lösung zu betrachten, da sie unterhalb des OSI-Modells liegt. Der Lichtwellenleiter (LWL) ist nicht durch den bereitstellenden Provider kontrollierbar und nicht mit dessen Übertragungstechnik verbunden. Daraus folgt, dass der Kunde selbst für die Bereitstellung aller nötigen Funktionen für eine Datenübertragung verantwortlich ist.

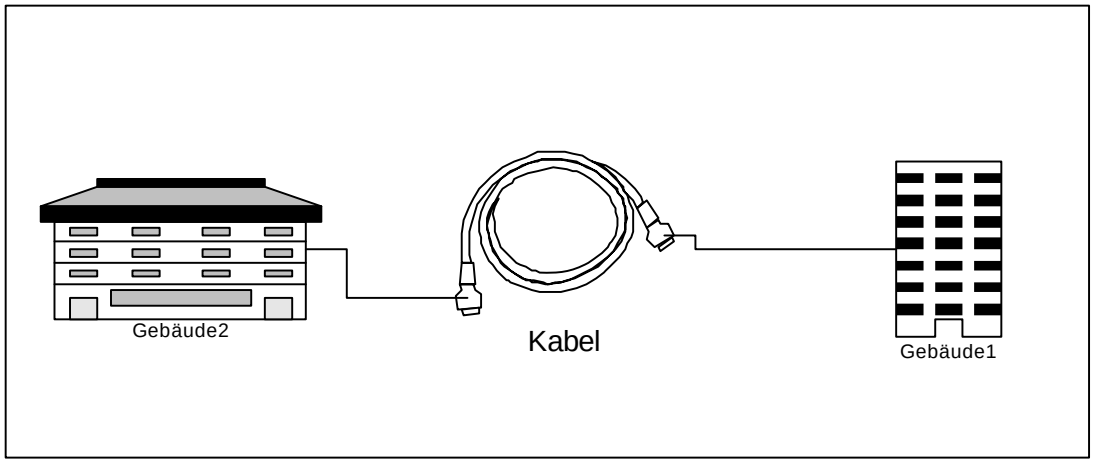

Abbildung 1: Dark Fiber

6.1.1.3 Zugang

Die Art der Zugangstechnik hängt bei diesen Lösungen natürlich vom Medium ab. Für den Einsatz von Glasfaser können Router mit entsprechenden Schnittstellenkarten eingesetzt werden. So sind für die einschlägigen Routertypen (Cisco, Juniper, …) entsprechende Baugruppen erhältlich, die Fast- oder Gigabit-Ethernet direkt über Glasfaserkabel übertragen können. Für das Management solcher Verbindungen (im Sinne der Bereitstellung der Verbindung) ergibt sich deshalb kaum ein Unterschied zum LAN des Kunden. Die Schnittstellen, an die diese Leitungen angeschlossen sind, werden wie LAN-Schnittstellen behandelt. Sie können aktiviert und deaktiviert werden, mit Accesslisten oder Policies beschränkt, geloggt und überwacht werden.

6.1.1.4 Management

Da keine Netzknoten vorhanden sind, beschränkt sich das Management auf die Zugangstechnik. Als Protokolle werden hier SSH für die Mensch-Maschine- und SNMPv3 für die Maschine-Maschine-Schnittstelle empfohlen. Durch den Einsatz von Access-Listen kann sichergestellt werden, dass nur den autorisierten Managementstationen der Administratoren Zugang gewährt wird. Der Einsatz von Accountingfunktionen mittels RADIUS oder TACACS sollte zum personalisierten Nachweis jeder einzelnen Managementhandlung verwendet werden.

Die Verantwortung für das gesamte Management obliegt dem Kunden. Die Maßnahmen, die im Grundschutzbaustein „Router-Switches“[*] aufgeführt werden, können vom Kunden in vollem Umfang angewendet werden.

[*] http://www.bsi.bund.de/gshb/deutsch/baust/b03302.htm

6.1.1.5 Sicherheitsbetrachtung

Für den Betrieb von Dark-Fiber-Strecken in der oben beschriebenen Art und Weise treffen alle sicherheitstechnischen Betrachtungen, die für Router oder Switche gelten, in vollem Umfang zu. Spezielle Maßnahmen, die der Tatsache Rechnung tragen, dass das verbindende Medium ein LWL ist, sind damit aber nicht möglich.

Physische Medien dieser Art können abgehört werden. Grundsätzlich ist es möglich, dass das Lichtsignal teilweise die Glasfaser verlässt. Dazu können folgende Verfahren angewendet werden:

- Doppelspleiße können bereits während der Bauphase, aber auch nachträglich angebracht werden.
- Biegekoppler ermöglichen das Empfangen von austretendem Licht.
- Das Anlegen eines Biegekopplers („Clip-on Device“), der zur Kommunikation zwischen Servicetechnikern eingesetzt wird, führt zur Erzeugung von Mikroverwerfungen und damit zum Auftreten von Leckwellen.

Die austretenden Signale sind trotz ihrer geringen Intensität verwertbar. Transportierbare Mess- und Signaleinrichtungen zur Gewinnung des Nutzsignals sind verfügbar.

Die von Providern auf optischen Leitern angewandten hochkomplexen Multiplexverfahren, etwa in PDH oder ATM stellen zwar eine Schwelle gegen schlecht ausgerüstete Angreifer dar, können aber von jedem professionellen Angreifer überwunden werden. Multiplexverfahren beinhalten keinen kryptographischen Schutz.

6.1.1.6 Fazit

Bewertung für Dark-Fiber Schicht „0“: Kunde/Provider-Verhältnis (KPV) = 100%/0%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 1.

Aufgrund dieser Bewertung ist der Einsatz einer Dark-Fiber-Strecke für den Schutzbedarf „normal“ bis „hoch“ geeignet. Für den Schutzbedarf „hoch“ empfiehlt sich der Einsatz von kryptographischen Verfahren auf den Zugangsroutern.

6.1.2 Satellitenübertragung

6.1.2.1 Verbreitung

Satellitenübertragung ist keine explizite Standleitungstechnologie. Sie wird vielmehr von global agierenden Providern als Ergänzung und Rückfalllösung in ihren Netzen eingesetzt. Somit können Lücken oder Ausfälle im Backbone überbrückt werden. Aber auch temporäre Verbindungen für Großveranstaltungen, bei Notfällen oder Katastrophen werden so geschaltet.

6.1.2.2 Technische Grundlagen

Die Satellitenübertragung benutzt Frequenzbereiche mit äußerst großer Übertragungskapazität (siehe Tabelle 5). Die Verbindung von der Erdfunkstelle (Hubstation) zum Satelliten wird als Uplink, die Verbindung vom Satelliten zur Bodenstation als Downlink bezeichnet.

Frequenzband (kommerziell)	Uplink	Downlink
C – Band	5.925 – 6.425 GHz	3.7 – 4.2 GHz
Ku – Band	14 – 14.5 GHz	11.7 – 12.2 GHz
S – Band	1980 – 2010 MHz	2170 – 2200 MHz
Ka – Band	27.5 – 31 GHz	17.7 – 21.2 GHz
L – Band	1610 – 1626.5 MHz	1525 – 1530 MHz

Tabelle 5: Frequenzen Satellitenübertragung

Eine Satellitenübertragung realisiert folgende Punkt-zu-Punkt-Verbindungen:

- zwischen Erdfunkstelle und Satellit,
- zwischen Satellit und Bodenstation,
- sowie zwischen zwei Satelliten.

Für eine störungsfreie Übertragung ist eine Sichtverbindung erforderlich (siehe Abbildung 2).

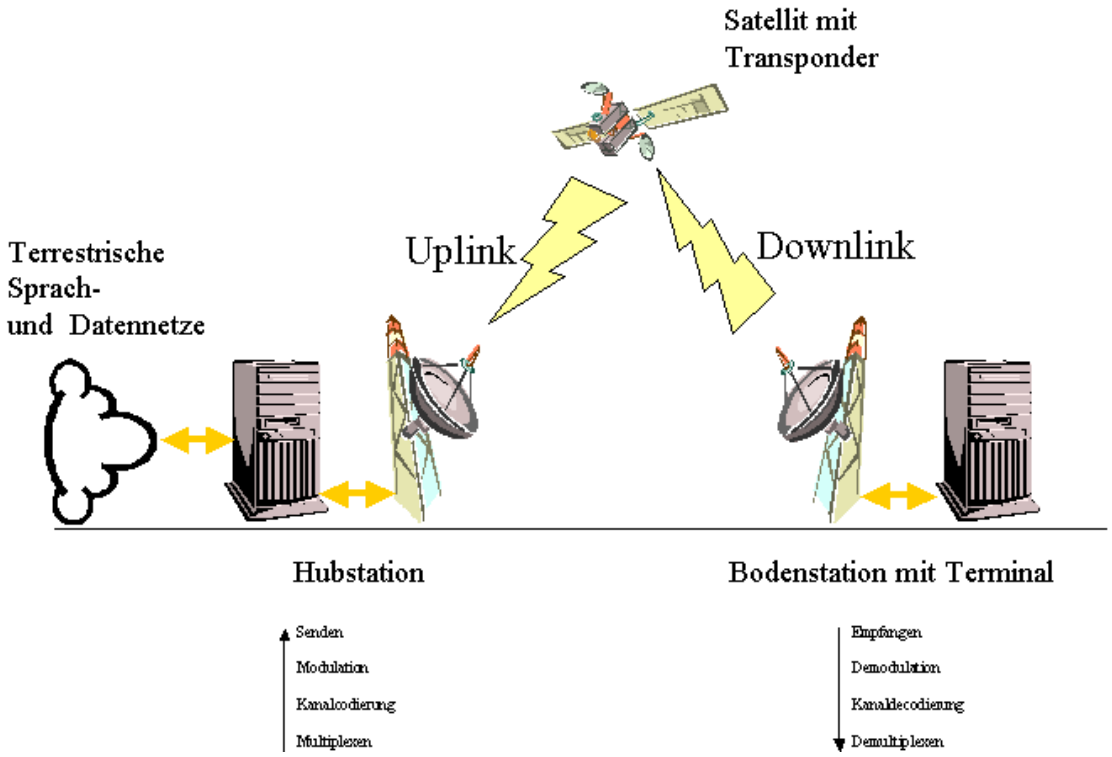

Abbildung 2: Satellitenübertragung

Die Übertragungskapazität eines Satellitensystems wird gewöhnlich durch Multiplexen mehrerer Kanäle an einer Sendestation zur Verfügung gestellt. Die zu übertragenden Daten werden danach mit einem Kanalcodierungsverfahren gegen Fehler gesichert und auf die gewünschte Trägerfrequenz für den Uplink moduliert. Der Satellit empfängt das Signal, setzt es mittels Transponder auf die Downlink-Frequenz um, verstärkt es und sendet es an die Empfangsstation, welche entsprechend das Signal demoduliert, decodiert und demultiplext.

Ein Nachteil der Satellitenübertragung besteht in den Verzögerungszeiten, die sich aus den langen Übertragungsstrecken ergeben.

6.1.2.3 Zugang

Die Bereitstellung von Richtfunk und Satellitenübertragung setzt den Betrieb von entsprechenden Sende- und Empfangseinrichtungen voraus.

6.1.2.4 Management

Das Management der Anlagen erfolgt in der Regel vor Ort über proprietäre Schnittstellen oder bei Fernzugriff über Inbandmanagement z. B. einen speziellen ATM-Kanal.

In ihrer grundsätzlichen Funktion als Medienwandler (Modem) sind die Konfigurationsmöglichkeiten der Anlagen, die den Nutzdatenstrom direkt betreffen, eher gering. Im Wesentlichen werden Parameter für das Tracking des/der Satelliten, der Funkkanäle und die möglichen Modulationsverfahren konfiguriert.

6.1.2.5 Sicherheitsbetrachtung

Kommunikation via Satellit ermöglicht eine Reihe von Angriffsszenarien. Für die in diesem Dokument behandelten Themen ist natürlich die Problematik des Abhörens relevant. Satelliten sind im Grunde Relaystationen für Funksignale. Ihr Downlink ist in der Regel weit gestreut und somit problemlos abzuhören. Der hierfür zu betreibende Aufwand für die Signalgewinnung ist gering. Allerdings müssen die Multiplexverfahren der Bitübertragungsschicht decodiert werden. Hierfür ist spezielle Hardware und entsprechendes Know-how erforderlich. Das Abhören von Satellitenkommunikationen ist nur mit geeigneten Empfangsanlagen in einem bestimmten Ausleuchtradius, dem so genannten Footprint, möglich. Eine exklusive Nutzung einer Satellitenverbindung ist für zivile Unternehmen oder Behörden eher unwahrscheinlich. Jedoch sollten Subscriber ihren Provider um Auskunft bitten, ob Satellitenverbindungen genutzt werden, da schon auf Grund der langen Signallaufzeiten bei einigen Applikationen Probleme auftreten könnten.

Hinsichtlich der Systematik „Endgerät – Netzzugang – Netzknoten – Netzzugang – Endgerät“ stellt die Bodenstation den Netzzugang und der Satellit selbst den Netzknoten dar. Wegen des problemlosen Zugangs zum Medium soll hier auf etwaige Angriffe auf Bodenstationen oder gar „Star-Wars“-Szenarien (physische Beeinträchtigung des Satelliten) nicht näher eingegangen werden.

Aus sicherheitstechnischer Sicht stellt eine Satellitenstrecke das schwächste Glied in den zur Anwendung kommenden Medien dar. Die benutzten Übertragungsverfahren auf der Bitübertragungsschicht wie das CDMA (Code Division Multiple Access) sind nach kurzer Analyse des Signals entschlüsselt. Damit ist die Signalgewinnung relativ einfach, die Datengewinnung ist aufgrund der komplexen Multiplexverfahren jedoch nur für professionelle Angreifer möglich. Die auf der Schicht 2 anwendbaren Protokolle zur Verschlüsselung werden derzeit kaum eingesetzt. Hier sind es eher die Anbieter von Pay-TV, die eine Vorreiterrolle spielen (allerdings in einem Broadcast-Szenario ohne Rückkanal). Eine weitere Möglichkeit wäre die Nutzung von ATMSec. ATMSec wird aufgrund seiner Komplexität jedoch kaum angewendet.

Für den Schutz der zu übertragenden Daten sind Maßnahmen auf vorgelagerten Einrichtungen und höheren Protokollen eher geeignet. So können bei Bedarf auf den angeschlossenen Routern kryptographische Verfahren eingeschaltet werden.

6.1.2.6 Fazit

Bewertung für Satelliten Schicht „0“: Kunde/Provider-Verhältnis (KPV) = 80%/20%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 3.

Satellitenübertragungen sind also nur für niedrigen Schutzbedarf geeignet. Für mittleren (normalen) Schutzbedarf empfiehlt es sich vorgelagerte, kryptographische Verfahren einzusetzen. Für hohen Schutzbedarf sind diese Maßnahmen bei Satellitenübertragungen obligatorisch.

6.1.3 Richtfunk

6.1.3.1 Verbreitung

Der Richtfunk als reine Standleitungstechnologie wird nur von Kunden oder Anwendern im eigenverantwortlichen Betrieb, etwa als Campuslösung eingesetzt. In Providernetzen wird diese Technologie, ähnlich wie bei Satellitenübertragungen, als Rückfalllösung, zum Lückenschluss (etwa Überbrückung der „letzten Meile“) oder als temporäre Verbindung eingesetzt.

6.1.3.2 Technische Grundlagen

Richtfunkstrecken unterteilen sich in drei Bereiche:

- Optischer Richtfunk,
- Richtfunk in regulierten Frequenzbereichen,
- Richtfunk in unregulierten Frequenzbereichen.

Die folgende Tabelle stellt die einzelnen Varianten gegenüber:

	Optischer Richtfunk	**Regulierter Richtfunk**	**Nichtregulierter Richtfunk**
Datenrate	4x2 bis 1250 Mbit/s	4x2 bis 4x155 Mbit/s	11 bis 108 Mbit/s
Reichweite	Max. 3 km	Max. 50 bis 70 km	Bis zu 10 km
Verfügbarkeit	> 99 %	> 99,9 %	> 99 %
Störsicherheit	Störungen praktisch ausgeschlossen	Sehr hoch (exklusive Frequenz)	Mittel (allg. genehmigtes ISM Frequenzband)
Abhörsicherheit	Sehr hoch[*]	hoch[†]	hoch (nur mit zusätzlicher Sicherungstechnologie[‡])

[*] Direkter Zugang zur optischen Richtfunkstrecke, Auskoppelung mit halbdurchlässigen Spiegeln erforderlich

[†] Direkter Zugang zur Richtfunkstrecke und spezielle Hardware erforderlich

	Optischer Richtfunk	Regulierter Richtfunk	Nichtregulierter Richtfunk
Frequenzen	Licht (Laser)	6/7/13/18/23/26/38 GHz	2,4/5 GHz (ISM Band)
Schnittstellen	S2M, Fast- und Gigabit-Ethernet, SDH STM-1	Ethernet 10/100BT	S2M, E1 (2,048 Mbit/s), 10/100 BT, STM-1
Genehmigung	Keine (Anmeldung aber erforderlich)	Erforderlich (Bundesnetzagentur)	Keine

Tabelle 6: Richtfunk

6.1.3.3 Zugang

Für Richtfunklösungen existiert eine Reihe von Anbietern:

Anwendung	Schnittstelle	Bandbreite	Entfernung	System
LAN-2-LAN Richtfunk	Ethernet/ FastEthernet	2-54 Mbps	5-15 km	BreezeNET B
LAN-2-LAN Richtfunk mit Telefonie	Ethernet/ FastEthernet plus 4x E1	2-54 Mbps	5-10 km	AirMux-200
Richtfunk	Fast Ethernet	34 Mbps	bis zu 50 km	Sagem Link F
LAN-2-LAN Richtfunk mit Telefonie	Ethernet/ FastEthernet plus 8x E1	116 Mbps	bis zu 40 km	FibeAir-1500PI
PDH Richtfunk	E1	16 x 2 Mbps	bis zu 50 km	Sagem Link F
PDH Richtfunk	E3	34 Mbps	bis zu 50 km	WitLink 2000
SDH Richtfunk	STM-1	155 Mbps	bis zu 30 km	FibeAir-1500P

Tabelle 7: Anbieter für Richtfunktechnik (ungewichtete Auswahl)

Aus Tabelle 7 wird das Spektrum der derzeit möglichen Lösungen ersichtlich. Für das Management wird neben proprietären Lösungen häufig auch SNMP als Schnittstelle angeboten. Bei einigen Systemen (wie z.B. BreezeNET) ist eine WEP Verschlüsselung konfigurierbar. Dies ist aber für den sicheren Transport von Daten mit hohem Schutzbedarf nicht ausreichend.

‡ Keine spezielle Hardware erforderlich (WLAN-Empfänger), daher nur mit Verschlüsselung (WPA2)

6.1.3.4 Sicherheitsbetrachtung

Richtfunk wird oft als abhörsicher bezeichnet, dem ist aber nicht so. Im nichtregulierten Richtfunk wird deshalb eine zusätzliche Verschlüsselung auf der Funkstrecke empfohlen. Abhören lassen sich Richtfunkstrecken dann, wenn man sich direkt in die Strecke zwischen oder hinter den Empfangsantennen stellt, denn der Funk wird gebündelt. Bei einer Stellung parallel zur Achse der Richtfunkstrecke ist ein sehr geringer Abstand nötig. Für das Abhören des optischen Richtfunks können Einrichtungen mit halbverspiegelten Empfangskomponenten angewendet werden. Hinzu kommt ein hoher technischer Aufwand für die Decodierung und das Demultiplexen des Signals.

6.1.3.5 Fazit

Bewertung für Richtfunk Schicht „0“: Kunde/Provider-Verhältnis (KPV) = 100%/0%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 1.

Richtfunk ist damit für normalen Schutzbedarf geeignet, für hohen Schutzbedarf empfiehlt es sich, vorgelagerte kryptographische Verfahren einzusetzen.

6.2 Lösungen auf Schicht 1

6.2.1 Verbreitung

Lösungen auf dieser Ebene werden auch als Leased Links, Leased Lines oder Standard-Festverbindungen (SFV) bezeichnet. Sie werden von jedem größeren Telekommunikationsanbieter als Standardprodukt vertrieben. Aufgrund der zunehmenden Verbreitung von IP-Plattformlösungen nimmt ihre Bedeutung jedoch ab.

6.2.2 Technische Grundlagen

Standard-Festverbindungen sind qualifizierte Anlagenteile in Form von Kabel- und/oder Funkverbindungen mit ihren übertragungstechnischen Einrichtungen. Sie stellen Punkt-zu-Punkt-Verbindungen mit einem spezifizierten Informationsdurchsatzvermögen (Bandbreite bzw. Bitrate) dar. Die Standard-Festverbindungen enthalten nur solche Funktionseinheiten, die für die dienstneutrale und transparente Punkt-zu-Punkt-Übertragung von Informationen innerhalb des Übertragungswegenetzes technisch-physisch erforderlich sind. Technisch-physisch erforderlich sind in diesem Sinne auch Funktionen und Funktionseinheiten, die zur Erkennung der Betriebsfähigkeit des Übertragungswegenetzes durch den Provider dienen und das Übertragungswegenetz vor elektrischer Fremdbeeinflussung schützen. Sie transportieren nur Nutzinformationen und abhängig von der Art des Übertragungsweges Signale zur Sicherstellung der Betriebsfähigkeit. Die Standard-Festverbindungen beginnen und enden an der jeweiligen Anschalteinrichtung (auch als Netzabschlussgerät, Datenanschalteinrichtung, CPE etc. bezeichnet) und schließen diese

ein. Standard-Festverbindungen haben an den Enden jeweils nur eine Abschlusseinrichtung und werden dem Kunden über dienstneutrale, räumlich frei zugängliche Schnittstellen übergeben. In der Regel beinhaltet der Netzabschluss die Anschalteinrichtung. Die Verbindungen zwischen der Anschalteinrichtung und den daran anzuschließenden Endeinrichtungen sind nicht mehr Bestandteil der Standard-Festverbindung.

Abbildung 3 stellt eine solche Verbindung schematisch dar.

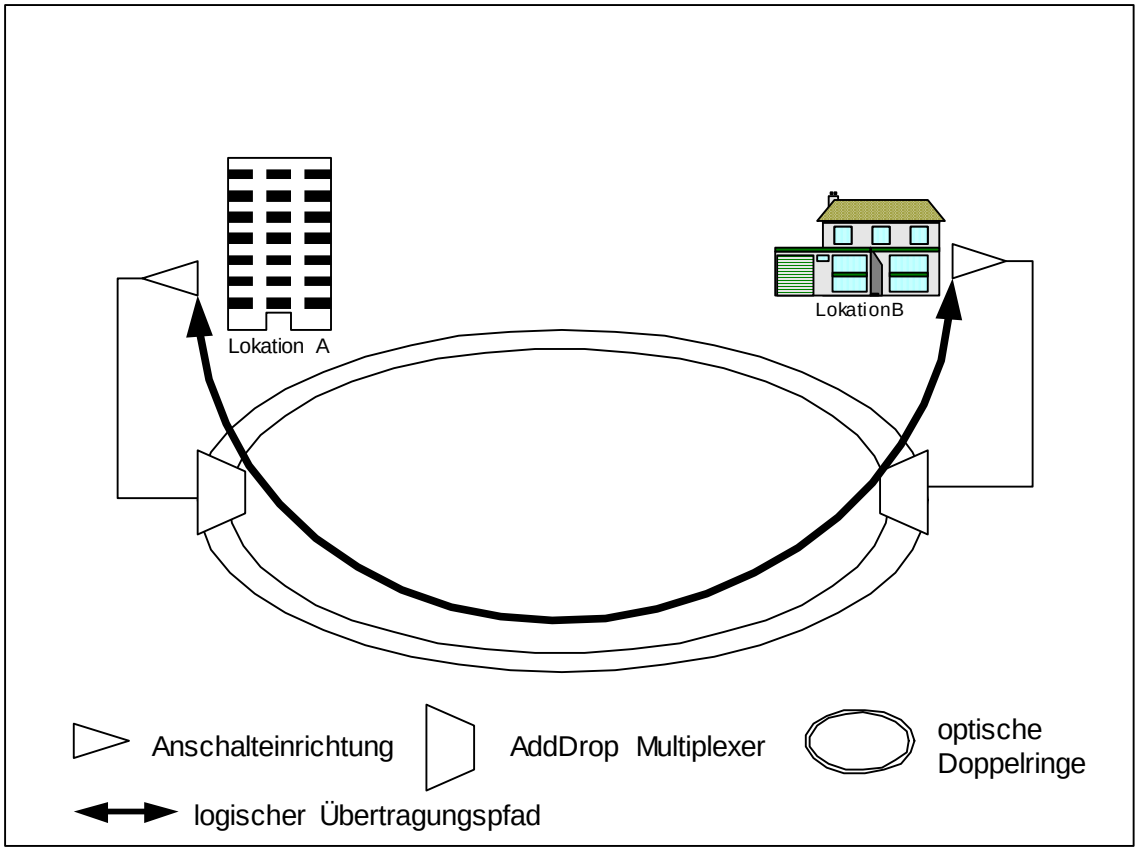

Abbildung 3: Standard-Festverbindungen

Die Verbindung beginnt und endet an den beiden Anschalteinrichtungen. Von dort aus wird die Verbindung über Glas- oder Kupferleitung zu einem Add/Drop-Multiplexer geführt und danach in den optischen Backbone des Providers eingespeist (Add), d. h. mit anderen Signalen gemultiplext. Dieses Backbone besteht typischerweise aus Glasfaserringen, die aus Redundanzgründen doppelt ausgeführt sind. In geeigneter Nähe des Zielstandortes des Kunden wird das Kundensignal durch einen Add/Drop-Multiplexer (Drop) wieder gewonnen. Typischerweise ist die Kundenschnittstelle in PDH-Technik ausgelegt. Auf dem Backbone wird das Signal durch SDH-Übertragungstechnik übertragen. Die Definitionen der Protokolle sind im Glossar enthalten.

Das Wesen der PDH- und SDH-Übertragungstechnik ist das zeitliche Ineinanderverschachteln von verschiedenen Signalströmen. Der kleinste Signalstrom der PDH-Technik

beträgt 64 Kbit/s und kann in fünf Ebenen bis 565 Mbit/s verschachtelt werden. Diese Technik wird vorwiegend im Zugangsbereich zum Backbone angewendet. Im Backbone selbst wird mit der SDH-Technik die Bandbreite von 155 Mbit/s bis hin zu 9,953 Gbit/s genutzt. Vorteil dieser Technik ist der direkte Zugriff auf jedes einzelne Signal.

In der Praxis allerdings ist der genaue physische Signalweg für den Kunden völlig transparent, d. h., es können bei Bedarf Funkstrecken oder, im internationalen Fall, Satellitenverbindungen genutzt werden. Entscheidend ist nur, dass die vertraglich vereinbarte Bandbreite je Teilsignalweg unterstützt wird.

SFV sind in der Regel für folgende Bandbreiten zu erhalten:

Bandbreite	Protokoll	Technik
64 Kbit	G.703/I.430	PDH
128 Kbit	G.703/I.430	PDH
1,984 Mbit	G.703/G.704	PDH
2,048 Mbit	G.703/G.704	PDH
34,368 Mbit	G.703/G.704	PDH
139,264 Mbit	G.703/G.704	PDH
155 Mbit	G.703/G.707 (elektrisch)	SDH
	G.957/G.707 (optisch)	

Tabelle 8: Standard-Festverbindungen

Das Protokoll G.703 nach (ITU-T) legt die elektrischen und physischen Merkmale eines PCM (Pulse Code Modulation) Interfaces fest. Wahlweise kann diese SFV auch im strukturierten Modus (G.704, G.707) betrieben werden. Für 64 Kbit/s bzw. 128 Kbit/s kann durch Konformität mit dem Standard I.430 dem Kunden ein vollwertiges Basic Rate Interface (BRI) zur Verfügung gestellt werden.

6.2.3 Zugang

Die Standard-Festverbindungen beginnen und enden an der jeweiligen Anschalteinrichtung (auch als Netzabschlussgerät, Datenanschalteinrichtung, CPE etc. bezeichnet). Ein typischer Vertreter dieser Klasse von Geräten ist das DAG 2048 als Anschalteinrichtung für 2 Mbit/s Verbindungen. Es wird LAN-seitig über seine X.21 Schnittstelle mit dem entsprechenden Interface eines Routers verbunden. Als Medienkonverter und Signalwandler konzipiert, sind seine Konfigurationsmöglichkeiten gering. Es ist wahrscheinlich, dass Manipulationsversuche eher den angeschlossenen Router (der in diesem Fall aber bereits dem Kunden gehört) betreffen werden.

6.2.4 Management

Das Management der Zugangstechnik beschränkt sich im Wesentlichen auf das Ein- oder Ausschalten des Gerätes.

Für das Management der Netzknoten werden von den führenden Herstellern wie Lucent, Alcatel oder ECI Client/Server Systeme mit graphischen Oberflächen zur Verfügung gestellt, deren hauptsächliche Aufgaben das Verschalten von Netzwerkpfaden und die Überwachung der Verfügbarkeit ist. Die verfügbaren Sicherheitsfunktionen hängen vom Hersteller und vom jeweiligen Produkt ab und sind oft nur rudimentär verfügbar. Ein einheitliches Bild kann hier aber nicht gegeben werden.

6.2.5 Sicherheitsbetrachtung

Die Endgeräte, die bei dieser Technologie eingesetzt werden (Digitale Modems (PDH), Synchrone Multiplex Terminals (SMT)), stellen im Grunde Medien- und Signalwandler dar. Ihre Manipulationsmöglichkeiten sind deshalb nur im Sinne der Beeinträchtigung der Verfügbarkeit zu sehen.

An den Netzknoten sind jedoch Manipulationen zur Verletzung der Vertraulichkeit technisch leicht zu realisieren. So können bei Add/Drop-Multiplexern und Cross-Connectoren aller namhaften Hersteller Monitorports geschaltet werden. Das bedeutet, dass der Verkehr für jede Richtung dupliziert und abgehört werden kann. Auch die Broadcast-Funktion ermöglicht die Weiterleitung eines ankommenden Signals zu mehreren Zielen.

Zugriff auf die Technik hat im Normalfall der Provider. Es kann aber nicht ausgeschlossen werden, dass eine Manipulation durch Dritte (sofern sie Zugang zur Technik haben) möglich ist. Man muss an dieser Stelle daran erinnern, dass im Zuge der Marktöffnung oft mehrere Netzbetreiber Zugang zu den Räumlichkeiten mit der Vermittlungstechnik haben. Hersteller haben im Rahmen ihrer Supportfunktion oft auch Fernzugang zu den Netzelementen und deren Steuereinrichtungen.

Eine Schwachstelle ergibt sich aus der Tatsache, dass der Zugang zur Datenanschalteinrichtung für den Provider frei zugänglich zu gestalten ist. Durch Unachtsamkeit der zugangsberechtigten Mitarbeiter des Providers oder des Kunden können Unberechtigte Zugang zu den entsprechenden Räumlichkeiten erlangen.

Die Sicherheit dieser Technik hängt im Wesentlichen von dem Zugangsschutz zur Anschalteinrichtung und der Vertrauenswürdigkeit des Providers ab. Es muss jedoch in Betracht gezogen werden, dass Manipulationen, wenn sie von Dritten erfolgen, ein sehr hohes Spezialwissen in folgenden Punkten erfordern:

- Kenntnis der Technik im Allgemeinen.
- Kenntnis der aktuellen physischen und logischen Topologie des Providernetzes.
- Eigene Ressourcen zur Signalableitung und Auswertung.

Alle oben erwähnten Protokolle haben lediglich die Sicherung der Datenübertragung zur Aufgabe. Sie enthalten keine Mechanismen zur Gewährleistung von Vertraulichkeit und Integrität. Dennoch werden an die Signal- und Datengewinnung erschwerte Anforderungen gestellt, zumal wenn dies unbemerkt geschehen soll. In diesem Fall kann das Signal nur durch induktive oder optische Auskopplung gewonnen werden, da sonst ein kurzeitiges Auftrennen der Leitung nötig ist.

Darüber hinaus sind die Abhörmöglichkeiten für Glasfaserstrecken, wie sie im Abschnitt 6.1.1.5 beschrieben wurden, anwendbar. Sofern Satellitenübertragungs- oder Richtfunkstrecken benutzt werden, sind auch die Abhörmöglichkeiten in den Abschnitten 6.1.2.5 und 6.1.3.4 zu beachten.

6.2.6 Fazit

Bewertung für Schicht 1: Kunde/Provider-Verhältnis (KPV) = 80%/20%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 2 (bei Verwendung einer abgesetzten Anschalteinrichtung).

Standard-Festverbindungen sind für Schutzbedarf „normal“ geeignet, sofern keine Satellitenübertragung auf einer Teilstrecke eingesetzt wird. Für hohen Schutzbedarf empfiehlt sich der Einsatz kryptographischer Verfahren auf den Zugangsroutern.

6.3 Lösungen auf Schicht 2

6.3.1 Verbreitung

Lösungen auf Schicht 2 ermöglichen bereits die Bereitstellung eines Netzes durch den Provider an den Kunden. Sie werden auch als „Switched Links“ bezeichnet. Dies wird dadurch möglich, dass auf dieser Schicht eine Adressierung der Pakete durchgeführt wird. Kunden, die solche Produkte nutzen, abstrahieren den Dienst durch eine „Wolke“, an der ihre verschiedenen Standorte angeschlossen sind (Siehe Abbildung 4).

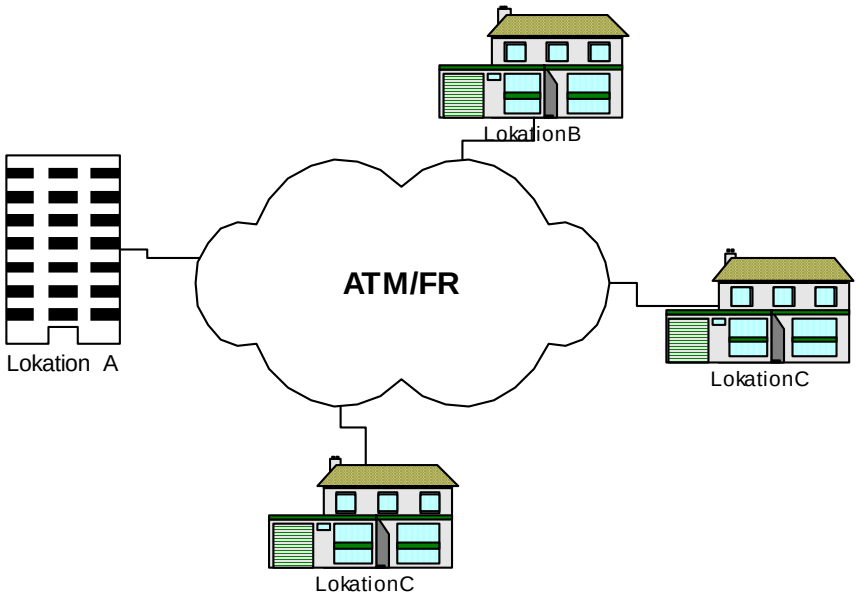

Abbildung 4: Switched Links

Diese Lösungen haben eine weite Verbreitung erfahren und spielen eine große Rolle, werden aber auch zunehmend durch die IP-Plattformlösungen abgelöst.

6.3.2 Technische Grundlagen

Die technische Plattform, auf der diese Dienste angeboten werden, sind X.25*, Frame Relay (FR) oder ATM.

Für den Einsatz von ATM als Protokoll für Mietleitungen (eigentlich muss man bereits vom Mietnetz reden) sprechen im Wesentlichen drei Gründe:

- Gute Unterstützung der SDH-Tansportschicht,
- Verbesserte Ausnutzung der Transportkapazitäten des Providernetzes durch verbesserte Granularität,
- Verbesserte Bereitstellung durch flexible Konfiguration auf der Basis der Parameter für die Wegewahl (PVC, SVC),
- Bereitstellung von QoS.

Die Wegewahl innerhalb dieser Plattformen geschieht mittels Verbindungsnummer, die je nach Technik als DLCI (Data Link Connection Identifier), PVC (Permanent Virtual Circuit) oder SVC (Switched Virtual Circuit) bezeichnet werden. Gemeinsam ist allen Plattformen,

* X.25 umfasst eigentlich die Schicht 1-3. Da aber häufig die IP-Schicht encapsuliert wird, ist eine Schicht 2 Funktionalität gegeben

dass die Netzwerkadressen des IP-Overlaynetzes auf diese Kennwerte abgebildet werden müssen. Aus diesem Grunde sind als Zugangstechnik für diese Produkte Router mit einer entsprechenden FR- oder ATM-Schnittstelle die erste Wahl.

Als typische Punkt-zu-Mehrpunkt Technologie sind in jedem Netzelement Entscheidungen zur Wegewahl zu treffen. Diese können statisch mittels PVC oder dynamisch mittels SVC getroffen werden. Virtual Circuits (in der Literatur wird auch der Begriff „Channel“ benutzt) sind Ende-zu-Ende Verbindungen zwischen zwei ATM-Endsystemen und werden in den ATM-Zellen durch einen entsprechenden Bezeichner (VCI) im Zellkopf repräsentiert. In den ATM-Vermittlungsstellen werden die virtuellen Verbindungen vermittelt, wobei der VCI entsprechend der Verbindungsdurchschaltung verändert werden kann. Da die VC-Bezeichner je Anschluss und Verbindung lokal vergeben werden, existieren in den ATM-Vermittlungsstellen (Vst.) Tabellen, welche die Zuordnung zwischen ankommenden und abgehenden VCs beinhalten. Bei PVCs (Permanent Virtual Circuits) sind sie fest eingestellt. Werden SVCs (Switched Virtual Circuits) verwendet, werden die Tabellen durch Signalisierung zwischen den beteiligten ATM-Knoten aufgebaut.

6.3.3 Zugang

Das Endgerät zur Realisierung von Switched Links sind Router oder Switches mit einem entsprechenden Interface für ATM oder Frame Relay. Diese Geräte werden in der Regel mit vom Provider gemanagt. Die beim Kunden installierte Technik, die zur Nutzung von Leistungen eingesetzt wird, kann vom Kunden gemietet, aber auch erworben sein.

6.3.4 Management

Um die Router zu managen, greifen Provider über das Backbone auf sie zu. Dies geschieht über die gleichen Schnittstellen, über die auch der Kunde seine Nutzdaten in das Backbone schickt. Hierfür wird der Begriff „Inbandmanagement“ verwendet. Um zu gewährleisten, dass auch tatsächlich nur der Provider Zugriff hat, sind an diesen Geräten entsprechende Maßnahmen zu ergreifen. So ist es nötig durch entsprechende Filtereinstellungen sicherzustellen, dass nur die autorisierten Managementstationen des Providers Zugang erhalten. Diese Filter werden als Access – Control Lists (ACL) bezeichnet. Darüber hinaus ist es nötig, die Vertraulichkeit dieses Zugangs sicherzustellen. Als Managementprotokoll sollte deshalb SSH statt Telnet verwendet werden, da hierbei eine Verschlüsselung der Kommunikation erfolgt.

Die Empfehlungen, die im IT-Grundschutz-Baustein „B 3.302 Router und Switches“ aufgeführt werden, sollten im vollen Umfang angewendet werden. All diese Maßnahmen obliegen jedoch dem Provider, der hier in die Pflicht genommen werden muss.

6.3.5 Sicherheitsbetrachtung

Aus sicherheitstechnischer Sicht liegt bei diesen Produkten folgende Situation vor (siehe Abbildung 5):

Ein Router oder Switch, meist als CPE ausgeführt, wird in einem für Kunden und Provider zugänglichem Raum aufgestellt. Die WAN-Schnittstelle dieses Gerätes ist ein ATM- oder FR-Interface, welches über eine Leased Line mit dem Providerswitch verbunden ist. Über diese Standard-Festverbindung wird auf der Schicht 1 ein PDH-Protokoll (meist E1/T1) gefahren. Die ATM-Zellen oder FR-Rahmen werden daher in einen PDH-Rahmen eingebunden. An dieser Stelle ist ein Zugriff auf die Daten nicht trivial. Dagegen sind die LAN-Schnittstellen des Routers oder Switches relativ leicht durch einen eingeschliffenen TAP (Trunk Access Point) abzuhören. Der Router/Switch selbst ist ein konfigurierbares Netzelement, welches sowohl aus dem LAN als auch aus dem WAN angegriffen werden kann. Hier sind erhöhte Sicherungsmaßnahmen für die Absicherung des Managementzugangs zu treffen.

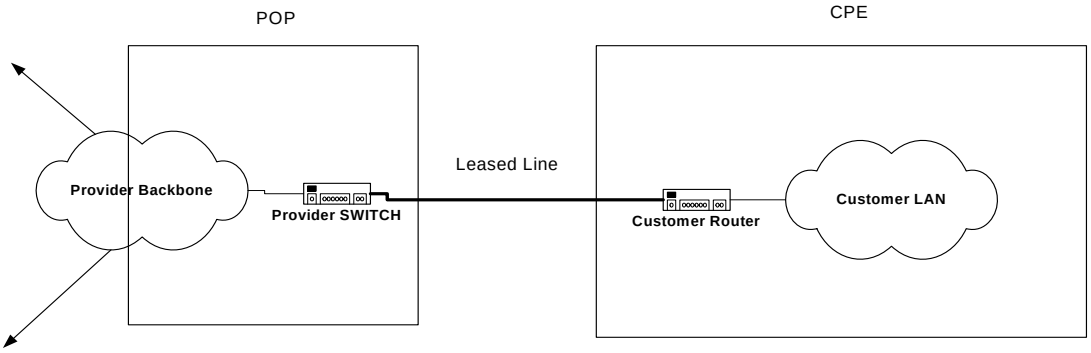

Abbildung 5: Leased Line

Durch Manipulation der Tabellen in den ATM-Vermittlungsstellen können Datenströme umgeleitet oder dupliziert werden. Die Integrität der Konfigurationsdaten und die Authentizität der ATM-Knoten bezüglich der Signalisierung ist deshalb von entscheidender Bedeutung für die Sicherheit der Kommunikation. Das Signalisierungsprotokoll selber besitzt aber weder auf der ATM-Schicht noch auf seinem Adaptionslayer* Schutzmechanismen für die Vertraulichkeit und Integrität der Signalisierungsdaten. Authentisierung der Kommunikationspartner und Schutz der Signalisierung sind standardmäßig ebenfalls nicht vorgesehen. Daraus ergeben sich Angriffsmöglichkeiten zur Verletzung der Vertraulichkeit und Manipulationsmöglichkeiten der Signalisierung. Da sich ATM-Switche nicht gegeneinander authentifizieren können, sind auch Man-in-the-Middle Angriffe möglich.

* Anpassungsschicht zu Realisierung verschiedener Dienste wie konstanter oder variabler Bitrate, verbindungsorientierter oder verbindungsloser Kommunikation

Die Gefährdung der Netzknoten ist vergleichbar mit der Situation bei Standard-Festverbindungen. Auch hier sind der Zugangschutz und die Vertrauenswürdigkeit des Providers von entscheidender Bedeutung. Allerdings ist das Gefährdungspotenzial weitaus größer, da ein Angreifer nicht nur Zugang zu den Informationsflüssen zweier Kommunikationspartner sondern zur Kommunikation eines ganzen Netzes hat. Für das Abhören von ATM-Verbindungen existieren Protokollanalysatoren mit beachtlichen Leistungsparametern. So können bei kommerziellen Geräten bis zu 3000 VCs (Kanäle) gleichzeitig analysiert werden.

In Bezug auf Authentisierung, Vertraulichkeit, Integrität und Zugangskontrolle erarbeitete das technische Komitee des ATM-Forums eine „Security Specification Version 1.0“, die seit 1999 vorliegt. Ziele waren die Verschlüsselung auf der Ebene des Zellstroms (alternative Header- und Nutzdatenverschlüsselung oder nur Nutzdatenverschlüsselung) oder auf der Ebene des virtuellen Kanals (Ende-zu-Ende-Verschlüsselung der Nutzdaten). Wegen der hohen Geschwindigkeit ist auch eine schnelle Verschlüsselung mit der Möglichkeit eines schnellen Schlüsselwechsels erforderlich. Inzwischen ist hinsichtlich ATMSec keine weitere Entwicklung zu beobachten, da der Trend eindeutig zu Internet-Technologien (TCP/IP mit IPSec) geht. Das bestätigt auch eine Änderung (bereits im Jahr 2000 von der TU München beantragt) des Forschungsvorhabens „Sicherheitsmanagement in ATM-Netzen“ in „Sicherheitsmanagement heterogener Netze“. Im Antrag der TU München wird dies u. a. mit der ähnlichen Modellstruktur von ATMSec und IPSec begründet.

In den Netzknoten können Telekommunikationsdaten z. B. mitgelesen, kopiert oder umgeleitet werden. Für den Benutzer ist bislang der gewählte Weg für die Zellen durch das ATM-Netz nicht beeinflussbar oder transparent. So ist es dem Benutzer nicht möglich, einen Weg über Vermittlungsstellen seines Vertrauens zu erzwingen oder bestimmte Vermittlungsstellen explizit auszuschließen.

Eine nähere Betrachtung von Frame Relay wird als nicht notwendig erachtet, da die Anwendung dieser Technologie, die auf dem X.25 Paketdienst aufsetzt, stark rückläufig ist.

Dennoch kann man im internationalen Bereich nie ausschließen, auch über Frame-Relay-Strecken zu kommunizieren. Grundsätzlich wird der Kunde nie genau wissen, welche Medien und Protokolle zur Übertragung seiner Daten zur Anwendung kommen. Auch für den Fall, dass Provider Aussagen hierzu machen, muss damit gerechnet werden, dass im Störungsfall Ersatzschaltungen mit anderen Technologien durchgeführt werden. Es empfiehlt sich deshalb gerade für den internationalen Verkehr immer mit Verschlüsselung zu arbeiten.

Bei der untenstehenden Bewertung ist zu beachten, dass ATM-Verbindungen bzw. ATM-Netze zusätzlich zu den oben beschriebenen Sicherheitsproblemen alle Sicherheitsprobleme der darunterliegenden Schicht 1 und Schicht „0“, die in den vorangegangenen Abschnitten betrachtet wurden, erben.

6.3.6 Fazit

Bewertung für Schicht 2: Kunde/Provider-Verhältnis (KPV) = 60%/40%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 4.

Sofern der Provider alle Maßnahmen des BSI IT-Grundschutz-Bausteins „B 3.302 Router und Switches“ für die aktiven Netzkomponenten, sowohl beim Kunden (CPE) als auch in den Vermittlungsstellen, umgesetzt hat, können Switched Links auch bei mittlerem (normalem) Schutzbedarf eingesetzt werden. Switched Links sind ansonsten nur für niedrigen Schutzbedarf geeignet. Als zusätzliche Maßnahme und für hohen Schutzbedarf bietet sich der Einsatz von Hardware-Krypto-Boxen an, die als Kunden-Equipment zum Einsatz kommen. Hiermit kann unabhängig vom Provider die notwendige Sicherheit garantiert werden.

6.4 Lösungen auf Schicht 3

6.4.1 Verbreitung

Lösungen auf Schicht 3 werden in der Regel als IP-Plattformlösungen bezeichnet. IP-Plattformlösungen finden zunehmend eine große Verbreitung und bieten auch für die Provider die größten Marktchancen. Hierbei wird eine komplette virtuelle LAN-Infrastruktur einschließlich Konfiguration, Management, Entstörung und Überwachung bereitgestellt. Die Realisierung von Zugangsdiensten (Dial-In), Voice Gateway, das Management einer DMZ und die Absicherung der Kommunikation mittels IPSec werden optional angeboten. Die genaue Beschreibung der angebotenen Dienste ist häufig Bestandteil eines Vertrages zwischen dem Provider und seinem Kunden. Da in dieser Produktgruppe die Absicherung der Kommunikation mittels IPSec als Option angeboten wird, werden Plattformlösungen mit und ohne IPSec gesondert betrachtet. Zunächst soll jedoch auf die technischen Grundlagen eingegangen werden.

6.4.2 Technische Grundlagen

IP-Plattformlösungen stellen komplette virtuelle Netzinfrastrukturen für Unternehmen oder Behörden mit verteilten Standorten über WAN-Verbindungen zur Verfügung. Hierbei befinden sich in der Regel alle beteiligten Standorte in den Subnetzen eines einheitlichen privaten IP-Adressraumes. Um diese privaten IP-Adressen über das Backbone des Providers zu routen, wird eine als VPN bekannte Technik eingesetzt. VPN (Virtual Private Network) bedeutet das Einkapseln der Datenpakete des Kunden in Datenpakete des Providers, um sie über dessen Netzinfrastruktur übertragen zu können. Im Gegensatz zu verschlüsselnden IPSec VPNs, die oft über das Internet aufgebaut werden, werden die Datenpakete bei dieser Art von VPNs in der Regel nicht verschlüsselt. Lokale Kundennetze an unterschiedlichen Standorten können auf diese Art und Weise verbunden werden. Bildlich gesprochen, wird ein Tunnel zwischen den lokalen Netzen erzeugt. Die Router,

die das Ein- bzw. Auskapseln der Datenpakete durchführen, werden als Tunnelendpunkt bezeichnet. Einkapseln bedeutet, dass dem Datenpaket des Kunden ein Protokollbestandteil vorangestellt wird, mit dessen Hilfe die Wegewahl im Providernetz erfolgen kann. Dies kann eine weitere IP-Adresse oder ein anderes geeignetes Merkmal des Protokollstacks sein.

Gegenwärtig wird als Stand der Technik das Protokoll MPLS (Multi Protocol Label Switching) verwendet. Hierbei wird wie folgt vorgegangen:

Die für die Weiterleitung eines Paketes relevanten Daten wie Zieladresse, Priorität und QoS-Klasse werden einer Forwarding Equivalence Class (FEC) zugeordnet. FEC repräsentiert eine Gruppe von Paketen, die alle nach denselben Kriterien übertragen werden. Es wird eine Referenz zwischen dieser FEC und einem kurzen Datensatz hergestellt (Binding), der allen zu einer FEC gehörenden IP-Paketen vorangestellt wird. Dieser Datensatz wird Label genannt. Die Effektivität, mit der solche Labels behandelt werden können, ist ungleich größer als das Behandeln des IP-Headers beim klassischen IP-Forwarding. Diese Pakete werden nur an den Eintrittspunkten zum Providerbackbone, dem LER (Label Edge Router), mit einem Label versehen (siehe Abbildung 6).

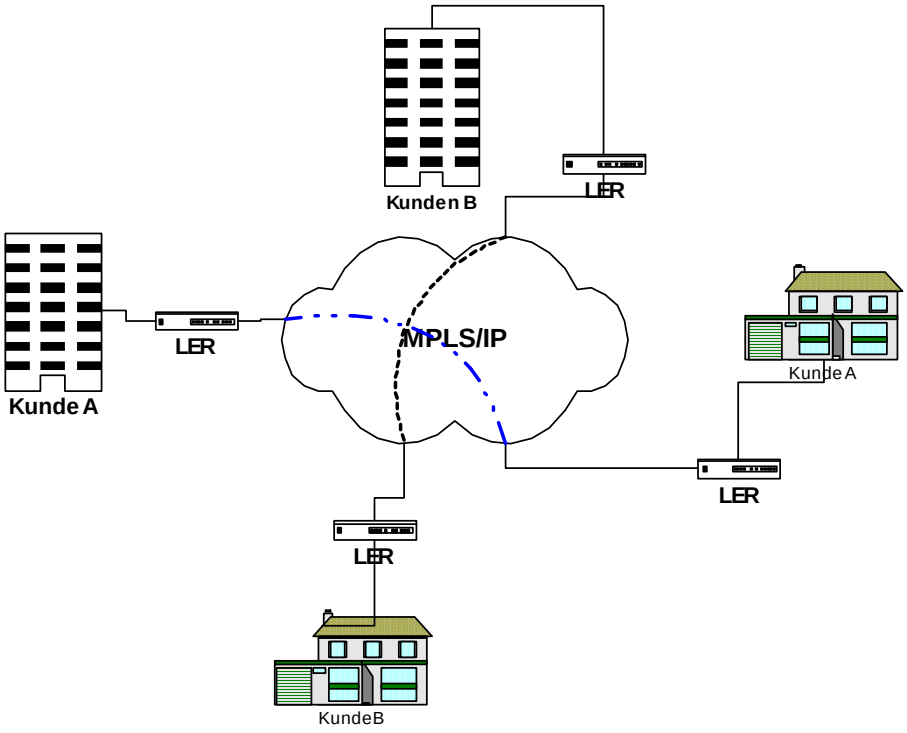

Abbildung 6: IP- Plattformlösung

Aus Sicht des OSI-Schichtenmodells ist ein Label mit einer zusätzlichen Schicht unterhalb der Netzwerk-Schicht vergleichbar, deren Zweck eine effektive Wegewahl ist. Dabei wer-

den aber im Unterschied zu einer echten Protokollschicht nicht in jedem Fall zusätzliche Oktette eingefügt, sondern, wenn möglich, Schicht 2 Protokollbestandteile verwendet. Dies betrifft die verbindungsorientiert arbeitenden Protokolle ATM und Frame Relay. Die jeweiligen Protokollbestandteile, welche bereits zur Markierung der virtuellen Verbindung benutzt wurden (VCI/VPI bei ATM, DLCI bei Frame Relay oder LCN bei X.25), übertragen nun die Labelinformation.

Die so markierten Pakete sind eindeutig einem Kunden und darüber hinaus auch einer kundenspezifischen QoS-Klasse zugeordnet. Sie sind damit eindeutig von anderen Datenströmen im Backbone zu unterscheiden. Damit stellt der Provider dem Kunden ein virtuelles privates Netz (VPN) im engeren Sinn bereit. Der Provider trennt mit Hilfe von Tags (Label) verschiedene Kundennetze auf logischer Ebene, so dass Datenströme der Kunden voneinander getrennt und abgeschottet sind. T-Systems trennt darüber hinaus MPLS-VPN physisch vom Internet. MPLS-VPN besitzt standardmäßig keine kryptografischen Mechanismen zum Schutz der Grundwerte Vertraulichkeit und Integrität (Verschlüsselung, kryptografische Prüfsummen). Solche Mechanismen können als zusätzliche Services dem VPN hinzugefügt werden.

6.4.3 Zugang

Es gelten grundsätzlich die für Lösungen auf Schicht 2 gemachten Aussagen. Auch in diesem Fall werden Router, so genannte Customer Edge (CE-) Router als Kundenequipment (CPE) und Label Edge Router (LER) in den PoPs, eingesetzt. Der Unterschied besteht nur in der Komplexität der Managementaufgaben, die an dieser Technik durchzuführen sind. So muss nicht nur die Konfigurationseinstellung zur Verbindung der verschiedenen Standorte eingegeben, sondern ggf. auch der Dial-In Zugang oder die Kryptographie konfiguriert werden. Typische Technik-Vertreter sind Cisco Catalyst 8540 oder Cisco-Router der 7000er Serie. Bei diesen Produkten wird MPLS over ATM eingesetzt.

6.4.4 Management

An dieser Stelle können alle Aussagen, die das sichere Management von Routern betreffen, uneingeschränkt wiederholt werden. Die Empfehlungen, die im IT-Grundschutz-Baustein „B 3.302 Router und Switches“ aufgeführt werden, sollten im vollen Umfang angewendet werden. All diese Maßnahmen obliegen jedoch der Verantwortung des Providers.

6.4.5 Sicherheitsbetrachtung

IP-Plattformlösungen erben die Sicherheitsprobleme der Switched Links. Wie bereits in Abschnitt 6.4.2 dargestellt, können MPLS-Labels durch ATM VCI/VPI realisiert werden. Allerdings kann nicht von einem bestimmten Schicht 2 Protokoll ausgegangen werden. Die Provider werden die Technologie einsetzen, die am kostengünstigsten die vertraglich

vereinbarten Parameter wie Verfügbarkeit und QoS realisiert und die am Ort des anzubindenden Standorts verfügbar ist. Die Betreiber von gut ausgebauten City-Netzen können hier z. B. auf Datenverbindungen zurückgreifen, die Ethernet über LWL direkt übertragen. Das Abhören von Verbindungen dieser Art ist mit dem entsprechenden Equipment zur Signalauskopplung und einem Protokollanalysator mit dem entsprechenden Interface durchaus möglich.

Als Zugangstechnik werden Router verwendet, die ggf. mit öffentlichen IP-Adressen ausgestattet werden. Die öffentlichen IP-Adressen der Router dienen dazu, Adresskollisionen mit IP-Adressen des Kunden zu vermeiden, in der Regel sind sie trotz der öffentlichen IP-Adressen aus dem Internet *nicht* erreichbar. Sofern über die IP-Plattformlösung auch der Internetzugang des Kunden realisiert wird, können die Router aber das Ziel von Angriffen aus dem Internet sein, um in das Kundennetz einzudringen. Dies stellt eine neue Qualität der Gefährdung dar.

Bei IP-Plattformlösungen mit IPSec wird vom Provider optional ein kryptographischer Schutz der Daten, die zwischen den einzelnen Standorten übertragen werden, angeboten. Die Gefährdung der Zugangsrouter ändert sich dadurch nicht. Allerdings erhöht sich deren Schutzbedarf. Wird dort der IPSec-Tunnel abgeschlossen, sind dort sicherheitssensitive Daten wie die geheimen Schlüssel konfiguriert. Sofern eine betriebliche Trennung des Netzmanagements und des Sicherheitsmanagement, wie von ITIL gefordert, gewünscht ist, empfiehlt es sich, ein dediziertes IPSec-Gateway für den Tunnelabschluss in einer DMZ aufzustellen. So kann der Netzbetrieb (durch den Provider) vom Sicherheitsmanagement (durch den Provider und/oder durch den Kunden) sauber getrennt werden, gleichzeitig ist ein höheres Schutzniveau für die kryptographischen Daten auf dem Tunnelendpunkt (IPSec-Gateway) möglich.

6.4.5.1 IP- Plattformlösung ohne Verschlüsselung

Bei der Variante ohne Verschlüsselung liegt eine Situation analog der Lösung auf Schicht 2 vor (siehe Abbildung 6). Ein MPLS-Backbone hilft einerseits dem Provider sein Netz effizienter auszulasten, kann aber auch andererseits die Datenströme des Kunden nach unterschiedlichen QoS-Anforderungen unterteilen. So können z. B. VoIP-Daten von unkritischen Datenverbindungen unterschieden und bevorzugt übertragen werden.

Fazit

Bewertung: Kunde/Provider-Verhältnis (KPV) = 40%/60%, Potenzielle Fremdeinwirkung auf den Provider (PF) = 4.

IP-Plattformlösungen ohne Verschlüsselung sind also aufgrund der von den Switched Links geerbten Sicherheitsprobleme und der hohen Komplexität der Technologie für den mittleren (normalen) Schutzbedarf geeignet, sofern der Provider alle Maßnahmen des BSI IT-Grundschutz-Bausteins „B 3.302 Router und Switches“ in allen Netzkomponenten

umgesetzt hat. Andernfalls kann nur von einer Eignung für den Schutzbedarf „niedrig“ ausgegangen werden.

6.4.5.2 IP-Plattformlösung mit Verschlüsselung

Auf der Basis von Plattformlösungen wird als Option meist das IPSec-Protokoll zur Verschlüsselung der Datenübertragung angeboten. Dadurch kann zwischen den CPE-Routern eines Kunden eine verschlüsselte Verbindung aufgebaut werden. Die Konfiguration dafür geschieht für den Kunden transparent durch das Management des Providers. Da die Wirksamkeit der Verschlüsselung in hohem Maße dabei von den verwendeten kryptographischen Verfahren abhängt, muss der Kunde ein hohes Maß an Vertrauen in die Sorgfalt, das Know-how und die Seriosität des Providers setzen. Andererseits sind spezielle Sachkenntnisse notwendig, um die Qualität der angebotenen IPSec-Konfiguration zu beurteilen.

Zunächst sind verschiedene Möglichkeiten der Authentifikation der Kommunikationspartner (Router) gegeneinander möglich. Die einfachste und zugleich schwächste Möglichkeit basiert auf einem „Preshared Key“, also einem Geheimnis, welches beide Kommunikationspartner einer Kommunikationsbeziehung gemeinsam besitzen. Besser ist die Anwendung von asymmetrischer Kryptographie auf der Basis eines Public/Private-Schlüsselpaares. Stand der Technik ist der Einsatz von X.509v3 Zertifikaten. Für diese „elektronischen Ausweise“ existieren anerkannte Verfahren der Verifikation, Verteilung sowie deren Gültigkeitsaufhebung.

Ein weiterer wichtiger Punkt ist der verwendete kryptographische Algorithmus zur Verschlüsselung der Daten. Hierbei ist neben der kryptographischen Mechanismenstärke das wesentliche Unterscheidungsmerkmal die Länge des Schlüssels (siehe hierzu auch die Maßnahme M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens* aus den IT-Grundschutz-Katalogen). Stand der Technik sind derzeit 3DES mit 168 Bit und der AES Algorithmus mit Schlüssellängen bis 256 Bit.

Dass die Datenpakte nicht nur verschlüsselt, sondern auch gegen Veränderungen geschützt sind, stellen kryptographische Prüfsummen sicher. Hier sind die aktuellen empfohlenen Verfahren SHA-2 mit 256 oder 512 Bit Länge, in der Praxis ist aber auch der weit verbreitete SHA-1 Algorithmus mit 160 Bit Schlüssellänge ausreichend. Der teilweise noch angebotene MD5-Algorithmus kann aufgrund von Schwächen jedoch nicht mehr empfohlen werden.

Die verwendeten Schlüssel sollten dynamisch erzeugt werden und sich nach festgelegten Zeiten oder nach der Übertragung bestimmter Datenmengen ändern. Für die dynamische Erzeugung der Schlüssel wird bei IPSec das Diffie-Hellman Schlüsselaustauschprotokoll eingesetzt, wofür auch Parameter, die so genannten Oakley-Gruppen, existieren. Diese werden ebenfalls mit steigender Bitlänge sicherer. Für hohen Schutzbedarf kann Gruppe 5 mit 1536 Bit oder Gruppe 14 mit 2048 Bit empfohlen werden.

Bei fachgerechter Implementierung erfolgt die Datenverbindung über einen Tunnel, in dem die Daten verschlüsselt und gegen Manipulation geschützt sind.

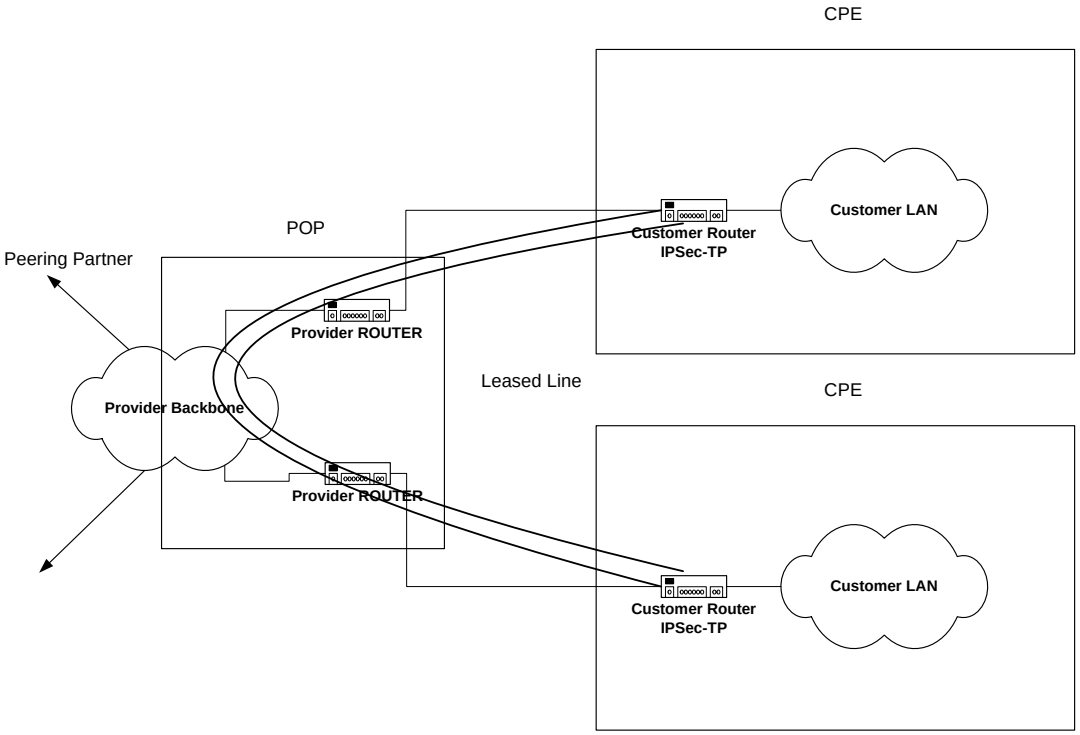

Abbildung 7: IPSec-Tunnel

Dieser IPSec-Tunnel wird an den WAN–Schnittstellen der CPE-Router terminiert (siehe Abbildung 7), so dass die WAN Verbindung geschützt ist. Ist jedoch der Zutritt zur Zugangstechnik (Router, IPSec-Gateway) nicht entsprechend gesichert, werden Angreifer ihre Manipulationen auf der unverschlüsselten LAN-Seite durchführen. Für Daten mit hohem Schutzbedarf ist deshalb nicht nur Verschlüsselung, sondern auch eine strenge Zutrittskontrolle zur Technik, wo der Tunnel terminiert wird, geboten. Aus diesem Grunde ist es besser IPSec Verbindungen nicht am CPE-Router, sondern an einem speziellen physisch geschütztem IPSec-Gateway zu terminieren. Dieses IPSec-Gateway muss sich netztechnisch in einer DMZ befinden, d. h. insbesondere hinter der LAN-Schnittstelle des CPE-Routers und durch eine externe oder integrierte Firewall vor Zugriffen über den CPE-Router geschützt.

Fazit

Bewertung: Kunde/Provider-Verhältnis (KPV) = 20%/80%, Potenzielle Fremdeinwirkung auf den Provider (PF) = < 1.

IP-Plattformlösungen mit Verschlüsselung sind für mittleren (normalen) und hohen Schutzbedarf geeignet. Bei hohem Schutzbedarf wird die Aufstellung eines dedizierten

IPSec-Gateways in einer DMZ hinter dem CPE-Router in einem zutrittsbeschränktem Bereich empfohlen.

7 Vergleichende Sicherheitsbewertung

In diesem Kapitel werden die Gefährdungen für die oben diskutierten Lösungen zusammengefasst und in Tabellenform dargestellt. Die Zuordnung zum Schutzbedarf gemäß der IT-Grundschutz-Vorgehensweise des BSI (BSI-Standard 100-2) wird ebenfalls dargestellt.

Für einen soliden Grundschutz sollte in jedem Fall der Baustein „B 3.302 Router und Switches“ aus den IT-Grundschutz-Katalogen des BSI angewendet werden. Insbesondere sind die Maßnahmen für die Installation, Konfiguration und den sicheren Betrieb dieser Komponenten umzusetzen.

Lösung	Administrative Sicherheit	Gefährdung Endgeräte	Gefährdung Netzknoten	Gefährdung des Mediums	geeignet für Schutzbedarf	Maßnahmen für Schutzbedarf „hoch“
Dark Fiber	SSH statt Telnet, SNMPv3 statt v1/2c, ACLs, personalisierte Zugänge, Accounting. (Maßnahmen des GS-BS Router und Switches anwenden)	Befinden sich unter alleiniger administrativer Kontrolle des Kunden	Keine	Abhören durch Biegekoppler, Doppelspleiße	normal (mittel)	Einsatz kryptographischer Verfahren auf IP-Ebene z. B. IPSec
Satellitenübertragung	Proprietäre Managementschnittstelle über Konsole oder ATM Inband. Spezielle Sicherheitsfunktionen sind nicht bekannt.	Hinsichtlich des leichten Zugang zum Signal irrelevant	Satellit ist für normale Angreifer nicht erreichbar	Leichtes Abhören durch breit gestreuten Kegel	niedrig	Einsatz kryptographischer Verfahren auf IP-Ebene z. B. IPSec
Richtfunk	Proprietäre Managementschnittstellen, optionale Verschlüsselung bei einigen Anbietern	Befinden sich unter alleiniger administrativer Kontrolle des Kunden	Keine	Angreifende Empfangseinrichtung muss in die Richtfunkachse	mittel	Einsatz kryptographischer Verfahren auf IP-Ebene z. B. IPSec

Lösung	Administrative Sicherheit	Gefährdung Endgeräte	Gefährdung Netzknoten	Gefährdung des Mediums	geeignet für Schutzbedarf	Maßnahmen für Schutzbedarf „hoch“
SFV, Leased Links	Variiert stark bei jedem Produkt und Hersteller, keine Kryptographie im Einsatz	Manipulation unwahrscheinlich da sie lediglich der Signalwandlung dienen	Signalvervielfältigung durch Spiegelports möglich.	Verbindung kann über verschiedene Medien geführt werden. Es müssen die Gefährdungen des schwächsten Mediums angenommen werden	mittel	Einsatz kryptographischer Verfahren auf IP-Ebene z. B. IPSec
Switched Links	SSH statt Telnet, SNMPv3 statt v1/2c, ACL’s, personalisierter Zugang, Accounting. (Maßnahmen des GS-BS Router und Switches anwenden)	Zugriff mittels Inbandmanagement auf IP-Ebene möglich. Gefahr von Datendiebstahl durch manipulierte PVC-Einträge möglich.	Datenvervielfältigung in den Netzknoten möglich	Verbindung kann über verschiedene Medien geführt werden. Es müssen die Gefährdungen des schwächsten Mediums angenommen werden	mittel (wenn die Einhaltung der Vorgaben des GS-BS Router und Switches gegeben ist, sonst: niedrig)	Anwendung von ATM Kryptoboxen, Einsatz kryptographischer Verfahren auf IP-Ebene. z. B. IPSec
IP-Plattformlösungen ohne Verschlüsselung	(Maßnahmen des GS-BS Router und Switches anwenden)	Zugriff mittels Inbandmanagement auf IP-Ebene möglich. IP Verbindungen zum Kundennetz ggf. möglich.	Datenvervielfältigung in den Netzknoten möglich.	Verbindung kann über verschiedene Medien geführt werden. Es müssen die Gefährdungen des schwächsten Mediums angenommen werden.	mittel (wenn die Einhaltung der Vorgaben des GS-BS Router und Switches gegeben ist, sonst: niedrig)	Einsatz kryptographischer Verfahren auf IP-Ebene z. B. IPSec
IP-Plattformlösungen mit Verschlüsselung	(Maßnahmen des GS-BS Router und Switches anwenden) Anwendung starker Kryptographie, Einsatz von Zertifikaten nach X.509v3	IPSec Gateway (innerhalb einer DMZ) enthält hochsensitive Daten deren Kenntnis durch Dritte die gesamte Verschlüsselung kompromittiert	Keine	Verbindung kann über verschiedene Medien geführt werden. Es müssen die Gefährdungen des schwächsten Mediums angenommen werden.	hoch Für die Zugangsrouter müssen die Vorgaben des GS-BS Router und Switches eingehalten werden.	Das IPSec-Gateway muss innerhalb einer DMZ aufgestellt werden und physisch geschützt sein.

Tabelle 9: Vergleichende Sicherheitsbewertung

8 VLANs und „Sharing Acccess“

In diesem Kapitel werden zwei aktuelle Schlagwörter aus dem Bereich Netzsicherheit in den Kontext der Studie sortiert.

Im Zusammenhang mit Netzwerksicherheit taucht der Begriff „VLAN“ häufig, aber oft unberechtigt auf. Deshalb soll an dieser Stelle eine Darstellung dieser Technologie stattfinden, um dem Klärungsbedarf genüge zu tun.

VLAN ist eine Technologie, die es ermöglicht eine Strukturierung auf Schicht 2 nach frei wählbaren Kriterien durchzuführen. Der Grund ist häufig die Aufteilung der MAC-Ebene in weitere Broadcast–Domains, ohne dass dabei auf Schicht 3 Informationen zurückgegriffen wird. Virtuelle LANs sind deshalb im Grunde nichts anderes als Verfahren zur Strukturierung des Datenverkehrs. Sie enthalten keine Mechanismen zur Sicherstellung der Vertraulichkeit. Die VLAN-Grenzen können durch Spoofing-Angriffe leicht überwunden werden. So existiert eine Reihe von Angriffen, die die VLAN-Trennung des Switches aushebeln. Beispielsweise ist es je nach Konfiguration möglich, den Anschluss eines Angreifers als Trunk auszugeben. Der Angreifer, der jetzt per Definition Mitglied in allen VLANs ist, kann nun auch den Verkehr, der nicht für sein Segment bestimmt ist, sehen und mitlesen.

Sharing Access ist die Bezeichnung für eine Lösung, bei der verschiedene Kunden eines Providers über dieselbe Zugangstechnik geführt werden. Hier können verschiedene Aspekte diskutiert werden.

In der Regel verwendet der Kunde ab Switched-Link-Lösungen CPEs, das heißt, dass der Kunde Eigentümer oder Mieter der Netzzugangstechnik ist. Es ist somit seine Entscheidung, wenn sich z. B. zwei kleine Unternehmen oder Behörden unter einem Dach einen ATM-Switch teilen. Man sollte diesen Fall ausschließen bzw. jedes Unternehmen und jede Behörde vor dieser Praxis warnen.

Etwas anderes ist die Erschließung eines Gewerbegebietes durch eine SDH-Anbindung, die von verschiedenen Unternehmen oder Behörden genutzt wird. Das jeweilige SMT (Synchrone Multiplex Terminal) wird in diesem Fall für die Einkopplung der Datenströme verschiedener Kunden ausgelegt sein. Hierbei hängt die Sicherheit im Wesentlichen vom physischen Zugangsschutz ab. Angreifer könnten, das Know-how vorausgesetzt, Datenströme über Spiegelports doppeln oder umleiten.

Zuletzt soll noch auf eine Lösung eingegangen werden, wie sie in Technologieparks oder in öffentlichen Bürogebäuden angetroffen wird, in denen ein lokaler IT-Infrastrukturdienstleister auch als Reseller für die Dienste eines Providers auftritt. Hierbei ist es durchaus üblich, den Verkehr der einzelnen dort ansässigen Firmen über verschiedene VLANs zu strukturieren. Man muss sich dies als ein gemeinsames lokales Netz vorstellen, das von verschiedenen Firmen genutzt wird. Ohne VLANs (aber leider auch mit) kann hier jeder mit jedem Daten austauschen. Hier ist die Gefahr sehr groß, dass die Firma A als Angrei-

fer gegenüber einer Firma B auftritt und deren Daten abhört, manipuliert oder fremde Daten in das Firmen-LAN einschleust. Diese Szenarien betreffen nicht nur Daten, die für die WAN-Übertragung vorgesehen sind, sondern grundsätzlich jede Form der Kommunikation zwischen den Clients und Servern einer Firma. Diese Art von IT-Infrastruktur ist für Firmen, deren Daten den Schutzbedarf „gering“ übersteigen, gänzlich ungeeignet. In diesem Fall ist eine Segmentierung des Netzes mit Hilfe von Firewalls angezeigt, so dass sich die Unternehmen gegenseitig von Zugriffen anderer Unternehmensangehöriger schützen können. Bei einzelnen Client-Server-Verbindungen mit hohem Schutzbedarf können diese auch mit einem kryptographischen Schutz (z. B. SSL/TLS oder IPSec Transport Mode) versehen werden.

Abkürzungsverzeichnis

ATM Asynchronous Transfer Modus; verbindungsorientierte Hochgeschwindigkeits-Multiplextechnik

BRI Basic Rate Interface; Bezeichnung für ISDN-Basisanschluss

BSI Bundesamt für Sicherheit in der Informationstechnik

CPE Customer Premises Equipment; Endgeräte, die in den Räumlichkeiten des Kunden installiert werden, wie Modems, Router oder Switche

DLCI Data Link Connection Identifier bei Frame Relay (D-Kanal-Protokoll, OSI-Schicht 2)

DMZ Demilitarisierte Zone; Subnetz, welches sowohl vom LAN als auch vom Internet durch Firewalls getrennt ist

FEC Forward Equivalence Class; FEC repräsentiert eine Gruppe von Paketen, die gleichartig übertragen werden.

FR Frame Relay; paketorientiertes Übertragungsprotokoll für Punkt-zu-Mehrpunkt-Verbindungen; wird zunehmend durch ATM abgelöst.

G.703 Schnittstelle nach ITU-T Standard; dient der unstrukturierten Übertragung von Daten mit 1.984 kbps

G.704 Schnittstelle nach ITU-T Standard; dient der strukturierten Übertragung verschiedener Kanäle mit Hilfe von Zeitschlitzen

G.707 Netzwerknotenschnittstelle für SDH

GS-BS Grundschutzbaustein; IT-Grundschutz-Baustein aus den IT-Grundschutz-Katalogen des → BSI

I.430 Schnittstelle nach ITU-T (→ BRI, Basic Rate Interface); zur Anschaltung von ISDN-Engeräten und -Netzen

IP Internet Protokoll; verbindungsloses Transportprotokoll auf OSI-Schicht 3

IPSec Internet Protocol Security; bietet Schicht 3 Tunneling plus Authentifizierung und Verschlüsselung von IP-Paketen

ISM Band Industrial Scientific Medicine Band; Lizenzfreies Frequenzband (u. a. im Bereich von 2,4 und 5 GHz)

ISP Internet Service Provider; Anbieter für Internet- und Intranet-Zugangsdienste

ITIL IT Infrastructure Library; Leitfaden zur Unterteilung der Funktionen und Organisation der Prozesse, die im Rahmen des serviceorientierten Betriebs einer IT-Infrastruktur eines Unternehmens entstehen

ITU International Telecommunication Union

LAN Local Area Network ; Lokale Netze über einige Hundert Meter bis Kilometer (meist innerhalb von Gebäuden oder auf einem Campus)

LCN Local Communications Network; regionales Netz

LWL Licht-Wellen-Leiter; Glasfaser zur Datenübertragung, beruht auf dem Prinzip der Totalreflexion der Lichtwellen

MAC Media Access Control; Unterschicht der OSI-Schicht 2, regelt den Zugriff auf das Übertragungsmedium

MPLS Multiprotocol Label Switching; vereint unterschiedliche Protokolle im Router, kombiniert Vorteile von Switching und Routing, ermöglicht eine hohe Skalierbarkeit

OSI Open System Interconnection (ISO Referenzmodell); 7 Schichtenmodell, beschreibt die Protokollschichten für einen Kommunikationsverbund offener und verteilter Systeme (technischer Einrichtungen zur Datenübertragung)

PCM Pulse Code Modulation; Sprachmodulationsverfahren

PDH Plesiochronous Digital Hierarchy; digitale Übertragungstechnik zwischen Netzknoten, nicht bitsynchron übertragen, bestenfalls rahmensynchron

POP Point of Presence; Einwahlknoten der Diensteanbieter, die von Teilnehmern angewählt werden können.

PVC Permanent Virtual Circuit; fest geschaltete virtuelle Verbindungen für eine dauerhafte Nutzung; Anwendung bei Frame Relay, ATM

QoS Quality of Service; bezeichnet die Bereitstellung einer definierten Dienstequalität für eine bestimmte Dienstklasse

SDH Synchronous Digital Hierarchy; digitale und transparente Multiplex-Übertragungstechnik für Glasfaserleitungen und Richtfunk.

SFV Standard-Festverbindungen

SSL Secure Socket Layer; Vorläufer von → TLS

SVC Switched Virtual Circuits; im Gegensatz zu PVC frei wählbare Verbindungen für beliebige Verbindungspartner

TAP Trunk Access Point

TLS Transport Layer Security; Sicherheitsprotokoll mit Verschlüsselungs- und Integritätsschutz der Daten ab Schicht 5

VC Virtual Channel; mehrere VCs können einen virtuellen Pfad (VP) bilden →ATM.

VCI Virtual Channel Identifier → ATM

VLAN Virtuelles LAN; unabhängig von der physischen Topologie logisch konfiguriertes LAN

VoIP Voice over IP

VPI Virtual Path Identifier → ATM

VPN Virtual Private Network; lokale Netze und Netzelemente werden derart verbunden, dass sie für den Nutzer wie ein einziges privates Netz wirken; das öffentlich zwischengeschaltete Netz ist transparent

WAN Wide Area Network; Weitverkehrsnetz mit einer Ausdehnung von mehr als 10 km; es verbindet mehrere LANs

WEP Wired Equivalent Privacy (veraltetes Verschlüsselungsprotokoll für → WLAN)

WLAN Wireless LAN; Funknetzwerke nach den Standards IEEE 802.11a, b, g

WPA2 Wi-Fi Protected Access 2; Sicherheitsstandard für → WLAN

X.21 Schnittstellendefinition vom öffentlichen geswitchten Netz zum Teilnehmer-Netzwerk

X.25 Schnittstellendefinition zwischen Endgeräten und einem digitalen paketvermittelnden Netz

Quellenverzeichnis

Grundlagen:

- „Technik der Netze“, Gerd Siegmund; Hüthig Verlag Heidelberg, 4. Auflage, 1999
- Online Ratgeber des DFN-FWL: Sicherheit in ATM-Netzen (www.dfn-cert.de/fnl/ratgeber/x381.html)
- „Antragskurzfassung“ zum Forschungsprojekt „Sicherheitsmanagement heterogener Netze“ der TU München vom Februar 2000. (www.ldv.ei.tum.de/media/files/forschung/Sicherheitsmanagement/dokumente/DFG_SPPS_Swo_Ebp_Sicherheit_Fort.pdf).
- „Völlig losgelöst?“ – Eine umfassende Analyse von Bedrohungen und Schutzmaßnahmen von Satellitenverbindungen, kes, SecuMedia-Verlag 3/2005
- IT-Grundschutz-Kataloge des BSI, Version 2005 (http://www.bsi.bund.de/gshb/index.htm)
- IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 1.0, Dezember 2005, (http://www.bsi.bund.de/literat/bsi_standard/index.htm)

Service Provider:

- Offizielle AGBs der T-Com zu den SFV Produkten: Digital 64U, Digital S01, Digital 2MS, Digital 2MU, Digital 34M, Digital 140M, Digital 155M und internationale Mietleitungen (www.telekom.de)
- Angebote Arcor zum „International Carrier Service“ (www.arcor.de)
- Angebote „Global Backbone“ der Firma Infonet (www.bt.infonet.com)

Hardware:

- Produktbeschreibung Backbone-Products der Firma Lucent (www.lucent.com/cable/)
- Cisco „Solution for Wireline Carriers“ (www.cisco.com)
- Technische Dokumentation für Juniper Broadband Access Router (www.juniper.net)