»Das Internet? Gibt's den Unsinn immer noch?«

Homer J. Simpson

4 Netzwerksicherheit herstellen

In diesem Kapitel betrachten wir die Sicherheit der Netzwerke im SAP-Umfeld. Diese entsprechen den Netzwerken, die für die gesamten Unternehmensbereiche zum Einsatz kommen, denn in der Regel gibt es keine abweichende Netzwerkarchitektur für die SAP-Lösungen. Nach einer Einführung in die wichtigsten Begriffe und Architekturgrundlagen werfen wir einen Blick auf die Netzwerkprotokolle, die im SAP-Umfeld stark genutzt werden. Wir geben Ihnen Hinweise, wie Sie diese Netzwerke und Komponenten härten können. Abschließend geben wir noch einen Ausblick, wie die Zukunft der Netzwerke in Gestalt der Software Defined Networks aussehen wird.

4.1 Netzwerk, Switches, Router und Firewalls

In diesem Abschnitt erklären wir Ihnen zunächst wichtige Begriffe im Zusammenhang mit den Netzwerken anhand des ISO/OSI-Referenzmodells.

4.1.1 Das ISO/OSI-Referenzmodell

Um die Elemente, die in Unternehmen ein komplettes SAP-Netz bilden, besser zu verstehen, ist es oft hilfreich, diese in einen normierten Zusammenhang zu stellen. Bei allen Diskussionen um das Wie, Wo und Was in einem Unternehmensnetzwerk hat es sich als hilfreich erwiesen, hier auf das Netzwerkmodell der Standardisierungsgremien ISO bzw. OSI zurückzugreifen, Diese haben die gesamte Netzwerkkommunikation in einzelne Ebenen isoliert und den Ebenen jeweils einen definierten Funktionsumfang zugewiesen. So kann man auch in komplexen Netzwerken den Verkehr jeweils in diese

funktionalen Ebenen (Layer) unterteilen und die Diskussion gezielt auf einzelne Segmente führen. Denn auch die Funktionen von Ethernet-Adaptern, Clients, Switches, Routern und Firewall lassen sich hervorragend semantisch und syntaktisch im Rahmen dieser Norm beziehungsweise dieses Modells erklären.

Ohne es hier im Detail vorzustellen (das würde den Rahmen dieses Buches sprengen) werden wir in den Kapiteln über SAP-Netzwerke immer wieder auf das ISO/OSI-Referenzmodell zurückgreifen. Deshalb wollen wir die wichtigsten Funktionsmerkmale kurz erläutern und in den SAP-Netzwerkkontext stellen

Netzwerkreferenzmodell

In dem ISO/OSI-Referenzmodell wird beschrieben, wie ein Datenpaket von einer Anwendung selbst (die nicht im OSI-Referenzmodell beschrieben wird) über die Anwendungsschnittstelle (Ebene 7) bis hinunter auf die Bit-Ebene (Ebene 1) und dann letztlich auf das Übertragungsmedium (z. B. Kupferkabel) kommt. Abbildung 4.1 zeigt die verschiedenen Ebenen im Überblick. Wie die Anwendung ist auch das potenzielle Kupferkabel nicht in ISO definiert, wohl aber die Methode, wie das Bit auf das Medium kommt.

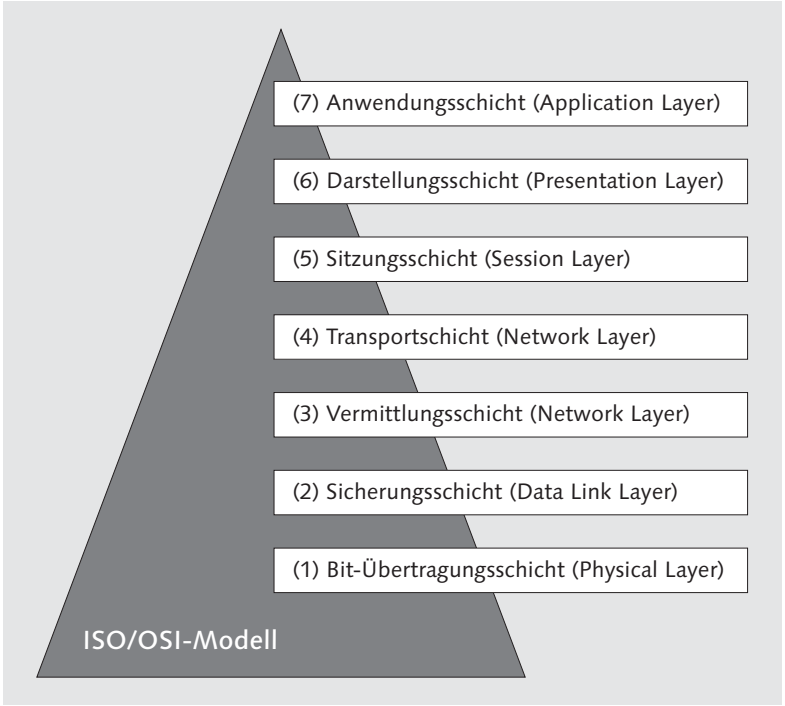

Abbildung 4.1 Das Sieben-Schichten-Modell nach ISO/OSI

Ebene 1: Netzwerkebene (Physical Layer)

Für die Betrachtung der *Netzwerke* sind vor allem die Ebenen 1 (Bit-Ebene, physische Ebene) bis 4 (Transportschicht) relevant. Diese bilden die Elemente ab, die als akademische Norm das abbilden, was man in Unternehmen und in der IT gemeinhin als Netzwerke versteht.

Die physikalische Ebene der Übertragung

Die erste Ebene ist die der bitweisen Übertragung, der Netzwerktopologie und der Infrastruktur (im englischen Original auch als *Physical Layer* bezeichnet). Die dabei verwendeten Verfahren bezeichnet man als übertragungstechnische Verfahren. Geräte und Netzkomponenten, die der Bit-Übertragungsschicht zugeordnet werden, sind z. B. die Antenne und der Verstärker, Stecker und Buchse für das Netzwerkkabel, der Repeater, der Hub oder der Switch. Hier gibt es keine technische Verknüpfung zu spezifischen SAP-Protokollen.

Ebene 2: Sicherungsschicht (Data Link Layer)

Die zweite Ebene, die auf Deutsch etwas unbeholfen mit *Sicherungsschicht* übersetzt ist, wird im Englischen als *Data Link Layer* funktional deutlicher bezeichnet. In der Nomenklatur ist schon zu erkennen, dass es darum geht, die Verbindung und Sicherstellung der fehlerfreien Datenübertragung zwischen zwei Netzwerkpunkten zu gewährleisten. Nach der amerikanischen Normungsbehörde IEEE ist Ebene 2 in zwei Unterebenen (*sub layers*) unterteilt: LLC (*Logical Link Control*, Ebene 2b) und MAC (*Media Access Control*, Ebene 2a).

Die Verbindung der physischen Kommunikation

Die Hardware, die dieser Schicht zugeordnet ist, sind Bridges, Switches und Multiport-Bridges. Das Ethernet-Protokoll beschreibt sowohl Ebene 1 als auch Ebene 2, wobei auf dieser als Zugriffskontrolle CSMA/CD zum Einsatz kommt. Letztlich sind in Ebene 2 die Elemente definiert, die für ein Netzwerk das definieren, was man gemeinhin als »Topologie« bezeichnet. Im Bereich des Ethernets sind es vor allem die Idee der Leitungen aus Ebene 1, in die sich die Netzwerkeinheiten einklinken und über die sie sich an das Netzwerk anschließen. Diese Leitungen können so miteinander kommunizieren und sich gegenseitig auf bestehende Kollisionen und Störungen hin überprüfen (CSMA/CD). So verbundene Leitungen bilden einen Strang, an dem die einzelnen Netzwerkelemente (Taps) hängen. Auch hier gibt es noch keine Verbindung zu einem SAP-Protokoll, in der SAP-Netzwerkarchitektur ist dies eine Ebene, die den Herstellern vorbehalten ist.

Ebene 3: Vermittlungsschicht (Network Layer)

Die Ebene 3 ist die Vermittlungsschicht, der *Network Layer*. Es ist die Schicht, die im Router adressiert ist. Hier erfolgt das Handling der Adressen, die Identifikation der Weiterleitung zu anderen Netzwerksegmenten etc. Das »IP« im Interchange Protocol von TCP/IP findet hier statt. Die zugehörige Hardware auf dieser Schicht sind Router und Layer-3-Switches.

Ein Netzwerk bilden

Auch hier gibt es noch keine direkte Verknüpfung mit einem SAP-Protokoll, da hier noch die klassische Netzwerkadressierung, Wegsuche und Transportfindung (Routing) stattfinden.

Ebene 4: Transportschicht (Transport Layer)

Die Ebene 4 ist die Anwendungsebene, auf der die SAP-Protokolle aufsetzen. Sie wird als *Transportschicht* bezeichnet (engl. *Transport Layer*; auch *Ende-zu-Ende-Kontrolle* oder *Transport-Kontrolle*), die den »Payload« (Nutzdaten) weiterleitet. Aufgabe der Transportschicht ist die Segmentierung des Datenstroms. Sie stellt auch für die höheren Ebenen eine definierte Schnittstelle dar, auf die diese einheitlich zugreifen können.

Daten transportieren

Ein Datensegment ist dabei eine Dateneinheit (Data Unit) die zur Datenkapselung auf der vierten Schicht (Transportschicht) verwendet wird. Es besteht aus Protokoll-Elementen, die Schicht-4-Steuerungsinformationen enthalten. Als Adressierung wird dem Datensegment eine Schicht-4-Adresse vergeben, also ein Port. Das Datensegment selbst wird in der Schicht 3 in ein Datenpaket gekapselt. Hier setzen die Netzwerkprotokolle der SAP auf. Um von verschiedenen Plattformen unabhängig zu sein, hat SAP für alle Netzwerkverbindungen die Zwischenschicht *Network Interface* (NI) entwickelt. Diese wird von SAProutern und allen SAP-Programmen, sowie von den Software Development Kits für CPI-C und Remote Function Call (RFC) genutzt.

Somit setzt auch das DIAG-Protokoll von SAP auf die Transportschichten auf. Aus Sicht des Angreifers sind dies die Schichten, die bei einer Attacke adressiert werden. Dies sind vor allem die Protokolle selbst sowie der Router-Verkehr.

Ebene 5: Sitzungsschicht (Session Layer)

Auf der Ebene 5 (Sitzungsschicht oder *Session Layer*) wird die Prozess-Kommunikation definiert. Dies ist nicht nur die technische Kommunikation, die auf den Schichten 1–3 stattfindet, sondern definiert den Session Context, den Zusammenhang und die Abfolge der Kommunikation.

Session-Kontext und RPC/RFC

Der Unix *Remote Procedure Call* (RPC) und somit auch das SAP-Derivat *Remote Function Call* (RFC) sind hier zu finden. SAP hat eine Abfolge definiert und die Ebene 5 definiert die Synchronisations- und Wiederaufsetzpunkte hierzu.

Ebene 6: Darstellungsschicht (Presentation Layer)

Die Darstellungsschicht (*Presentation Layer*; setzt die systemabhängige Darstellung der Daten in eine unabhängige Form um und ermöglicht somit den syntaktisch korrekten Datenaustausch zwischen unterschiedlichen Systemen. Das heißt, dass hier die Funktionen des SAP GUI durch das DIAG-Protokoll umgesetzt werden.

DIAG und SNC

Ebenso findet hier nominell die SNC-Verschlüsselung statt, da SNC ja letztlich die Anwendungsdaten verschlüsselt, aber natürlich nicht die darunter liegenden Schichten des Protokolls. Die Darstellungsschicht gewährleistet, dass Daten, die von der Anwendungsschicht eines Systems gesendet werden, von der Anwendungsschicht eines anderen Systems gelesen werden können.

Ebene 7: Anwendungsschicht (Application Layer)

SAP-GUI-Schnittstelle

Die Ebene 7 ist die technische Schnittstelle des Netzwerks zur Anwendungsebene und wird oft von Programmierern als *Application Programming Interface* (API) wahrgenommen. Es handelt sich um die Schnittstelle des Anwendungsprogramms. Ebene 7 beschreibt also nicht die Anwendung selbst, sondern definiert die Art und Weise, wie Programme mit den Netzwerkkomponenten kommunizieren können. In aktuellen Programmiersprachen wird eine solche Schnittstelle in der Regel als API bezeichnet. In der SAP-Welt stellt etwa das Protokoll *Dynamic Information and Action Gateway* (DIAG) die Schnittstelle zu Ebene 7 des Modells dar.

Gesamtsicht auf das ISO/OSI-Modell

Wichtig ist es aus sicherheitstechnischer Sicht, das Netzwerk als Abfolge von Funktionen wahrzunehmen: Es gibt das Netzwerk selbst mit seinen technischen Elementen wie Repeatern etc. und es gibt den Zugang zu den Netzwerken wie Netzwerkadapter und Switches. Dann folgen die »intelligenten« Funktionen des Netzwerks wie Router und darüber liegen die session-bezogenen Layer wie RFC-Protokoll, RFC-Gateway und die Anwendungsschnittstellen. Verschlüsselung ist eine Form des Darstellungsschicht, das SAP GUI eine Form des Presentation Layers.

4.1.2 Verschlüsselung der Netzwerkverbindungen mit SNC

Mit den *Secure Network Communications*, den SNC-Verbindungen, hat SAP eine eigene Verschlüsselungsebene geschaffen. In den letzten Jahren wird speziell die Verschlüsselung von Verbindungen zwischen kommunizierenden Komponenten in SAP-Landschaften bei Audits immer wieder gefordert. Bei vielen Kunden war sie bisher noch nicht im Einsatz.

Verschlüsselung mit SNC

Im Standardfall, z. B. bei einer Kommunikation zwischen einem Benutzer mit SAP GUI und dem SAP NetWeaver Application Server erfolgt die Kommunikation unverschlüsselt im Klartext bzw. zwar komprimiert, aber trotzdem ungesichert. Das bedeutet, dass bei einem Mitschnitt der Verbindung, einem *Sniff*, die Daten (inkl. Passwort und weiteren Anmeldedaten) unverschlüsselt zu sehen sind. Abhilfe schafft hier eine auf kryptografischen Grundlagen vorgenommene Verschlüsselung. SAP hat hierfür das SNC-Protokoll geschaffen.

SNC sichert die Datenkommunikationspfade zwischen verschiedenen Client- und Serverkomponenten des SAP-Systems. Es gibt bekannte kryptografische Algorithmen, die von den unterstützten Sicherheitsprodukten implementiert wurden; mit SNC können Sie diese Algorithmen auf Ihre Daten im Netzwerkverkehr anwenden, um die Sicherheit zu erhöhen. Die gesamte Kommunikation zwischen zwei mit SNC geschützten Komponenten wird gesichert (z. B. zwischen dem SAP GUI und dem Anwendungsserver). Sie können so zusätzliche Sicherheitsfunktionen von Drittanbietern verwenden (z. B. Smartcards).

Voraussetzung für die Nutzung aller Verschlüsselungsfunktionen, aber auch aller weitergehenden Funktionen im Bereich Sicherheitszertifikate und digitaler Signierung ist die Installation der SAP Cryptographic Library. Dies ist ein Produkt, das Kunden auch für SNC-Verbindungen zwischen Systemkomponenten zur Verfügung steht. Weitere Informationen über Verschlüsselung im SAP-Bereich, dem SNC-Protokoll und der Implementierung dieser Technolgien erhalten Sie im SAP Help Portal unter der Rubrik SAP Cryptographic Library.

4.1.3 Firewall in der SAP-Umgebung (ISO/OSI)

Eine klassische Firewall, die immer wieder als zentrales Element in jedem Sicherheitskonzept aufgeführt ist, ist keiner Ebene des ISO/OSI-Modells direkt zugeordnet. Sie ist eher komplementär zur Architektur von Netzwerk und Anwendungskommunikation.

Firewall und SAP-Systeme

Eine Firewall ist eine Software, die sich in das Netzwerk einklinkt und dieses von dem Rechnernetz (*Topologie*), das sich jeweils vor der Firewall befindet, segregiert damit jedes angeschlossene Netzwerksegment eine eigene Sicherheitsebene, eine *Policy* bilden kann. So werden logische Ebenen gebildet, sogenannte *Tiers*, die voneinander getrennt sind. Die Firewall stellt dabei beim Übergang von einem Netzwerksegment zu einem anderen die Einhaltung des in der Firewall hinterlegten Regelwerks sicher. Ein klassisches Beispiel sind die Regeln, welcher Client auf Systeme hinter der Firewall zugreifen darf. Wichtig ist, dass Sie die verschiedenen Richtungen der Kommunikation einzeln betrachten. So überprüft die Firewall z. B., ob ein SAP GUI von einem bestimmten Rechner auf ein SAP-System zugreifen darf, stellt aber auch sicher, das umgekehrt der Server nicht beliebige Verbindungen öffnen kann, sondern dem Client nur auf der gerade geöffneten Leitung antwortet. Dies sind die grundlegenden Anwendungen der Firewall, die man den Ebenen 1 bis 4 des ISO/OSI-Modells zuordnen kann.

Darüber hinaus beschränken sich moderne Firewalls nicht nur auf die physikalische Kontrolle von Verbindungen, sondern erweitern die Funktionen um die intelligente Analyse des Datenverkehrs. Sie setzen dann auf den Ebenen 4 bis 7 des ISO/OSI-Modells auf und beziehen damit auch Komponenten aus der Anwendungskontrolle mit in die Sicherheitsbetrachtung ein.

Paketfilter

Die einfache Filterung von Datenpaketen anhand der Netzwerkadressen ist die Grundfunktion aller Firewalls (in einem TCP/IP-Netz ist damit die Filterung des Ports und der IP-Adresse des Quell- und Zielsystems gemeint). Filterung bezeichnet hier sowohl das positive als auch das negative Routing, also den Zugang (*Access*) oder die Ablehnung (*Deny*) einer Route.

Stateful Inspection

Diese zustandsgesteuerte Filterung ist eine erweiterte Form der Paketfilterung. Damit gelingt es, den Zugriff auf eine etablierte Verbindung genauer zu beschränken und so das interne Netz besser vor ungewollten Zugriffen von außen zu schützen. Bei dieser Betrachtung eines Paketes bzw. einer Kommunikation wird auch der Kommunikationszustand (Ebene 5 ISO/OSI, der Session Layer) mit berücksichtigt.

Firewall und Kontext

Hier wird kontrolliert, ob eine etablierte Verbindung auch keine Seitenkommunikation aufbaut, um etwa aus einer Session auf eine andere zu verzweigen. In SAP-Systemen kann solch eine Stateful Inspection sich z. B. als Verbindungsabbruch manifestieren, wenn Inhalte (z. B. Content Header) sich während der Kommunikation von Client zu Server verändern. SAP Web Services können in diese Kategorie fallen.

Proxyfilter

Ein Proxyfilter stellt stellvertretend für den anfragenden Client die Verbindung mit dem Zielsystem her und leitet die Antwort des Zielsystems an den ursprünglichen Client weiter. Da er die Kommunikation selbst führt, kann er sie nicht nur einsehen, sondern auch beliebig beeinflussen. Während in großen Netzen die Proxy-Funktion oft von dedizierten Servern übernommen wird, kann dies in Einzelsituationen auch von spezialisierten Firewalls übernommen werden.

SAP Web Dispatcher

Der SAP Web Dispatcher übernimmt einige dieser Funktionen, wenn im SAP-Bereich Webanwendungen angesprochen werden. Eine Sonderform ist der *Reverse Proxy*, dessen Aufgaben im SAP-Bereich von dem inzwischen bei den meisten Kunden in Vergessenheit geratenen SAP Business Connector übernommen werden konnten.

Content-Filter

Dieser Inhaltsfilter ist eine Form des Proxyfilters, der die Nutzdaten einer Verbindung auswertet und z. B. dafür gedacht ist, auf beliebigen Inhalt der Kommunikation zu filtern.

SAP Web Dispatcher als Content Filter

Auch diese Funktionen können nicht nur von einer Firewall übernommen werden, sondern auch von einem SAP Web Dispatcher. Gerade bei SAP-NetWeaver-AS-Java-Servern wird diese Funktion benutzt, um gewisse bekannte und gefährliche Kommandos von außen aus dem Verkehr heraus zu filtern. Auch das Sperren von unerwünschten Webseiten anhand von Schlüsselwörtern und Ähnliches fallen darunter. Auch können in Bezug auf SAP-Traffic mit Firewalls der neuesten Generation verhaltenstechnische und semantische Analysen des Datenstroms ausgeführt werden, wie z. B.: Darf ein HR-Nutzer CRM-Daten herunterladen? Solche Fälle können dann erkannt und geblockt werden.

4.2 SAP-Landschaft analysieren

Wenn die Sicherheitsbedürfnisse einer SAP-Landschaft betrachtet werden, ist es wichtig, sich über die grundlegenden Komponenten zu verständigen. In den 1980er Jahren, als es im SAP-Umfeld noch kein umfängliches Internet gab (von den Anfängen als DARPA-Netzwerk der amerikanischen Verteidigungsministerien einmal abgesehen), waren auch das Ethernet und die damit verbundenen Protokolle nicht wie im heutigen Ausmaß vorhanden. Die SAP-Ingenieure mussten sich Teile ihres Netzwerkprotokolls selbst realisieren und haben deshalb eigene Teilkomponenten erstellt.

Diese Elemente, die sich auch oft nicht eindeutig im ISO/OSI-Modell wiederfinden, sollen hier als Grundlage für die Sicherheitsbetrachtungen aufgezählt werden.

Die Implementierung der Netzwerkkomponenten der 3-Tier-SAP-Architektur auf einem TCP/IP Stack war geprägt von den Anforderungen der Portierung der Kommunikation der alten IBM-Welt mit ihren Terminals. Viele Artefakte im SAP-GUI-Protokoll resultieren daraus.

Deshalb müssen die Angriffe auf diese Protokolle auch sehr SAP-spezifisch sein. Hier versagen oft die standardisierten Netzwerk-Hacker-

Werkzeuge der Internet-Ära und müssen durch Programmierer mit profunden SAP-Protokoll-Kenntnissen selbst erschaffen werden. Das ist mit Sicherheit eines der Hauptgründe, warum es in der Vergangenheit wenig ausgewiesene Hacker für die SAP-Netzwerke gibt. Das hat sich aber gerade in den letzten Jahren stark geändert.

Multi-Tier-Architektur im SAP-Umfeld

Schon im Bereich der Mainframe-Kommunikation war es immer das Credo der SAP-Entwickler, sich nie auf spezifische Hardwareprotokolle einzulassen. Deshalb wurde zur Integration der Siemens BS/2000- und IBM/370-Architektur die jeweilige Ebene immer abstrahiert angesprochen. Diese Weitsicht zahlte sich aus, als man mit SAP R/3 in die Unix-Welt migrierte. Die eigene abstrakte Architektur passte hervorragend zu den Client-Server-Strukturen. Und mit den drei Komponenten Präsentationsebene (SAP GUI), Anwendungsserver (SAP NetWeaver AS ABAP und RFC) und Datenbankabstraktion hatte man die notwendigen Elemente für die herstellerunabhängigen Implementierungen beisammen. Auf diese drei Ebenen gehen wir im Folgenden genauer ein.

4.2.1 Tier 1: SAP-GUI-Client

Der Hauptzugang zu SAP-Systemen basiert in allen Systemen auf dem SAP GUI. Dieser Zugang basiert auf einem *Rich-Client-Konzept*, das ein proprietäres Netzwerkprotokoll verwendet. Das Konzept, das das SAP GUI verwirklicht, kommt ursprünglich aus der Terminal-Steuerung; dort wurden pro Bildwechsel 24 × 80 Zeichen übermittelt und der Server (damals: Mainframe) leitete daraus die notwendigen nächsten Schritte (basierend auf den Benutzereingaben) ab. Auf dieser Basis wurde in SAP R/3 dann eine client-/server-basierte Dialogsteuerung entwickelt. Durch die damals schon praktizierte Herstellerunabhängigkeit der verwendeten Protokolle war die SAP-Dialogsteuerung in allen Netzwerkvarianten ablauffähig.

Das Protokoll, das in der alten Welt benutzt wurde, war die SNA-Architektur der 3270-Terminals. Für die Unix-Welt von SAP R/3 wurde die Dialogsteuerung auf dem TCP-IP-Stack realisiert beziehungsweise wurde die DIAG-Struktur der übermittelten Pakete darauf angelegt. Deshalb liegt die Zuordnung des DIAG-Protokolls auch auf Ebene 6 des ISO/OSI-Modells (des Presentation Layers) und nicht auf Ebene 3 oder 4 (Network bzw. Transport Layer).

SAP-GUI-Hack

Aus Sicht eines Angreifers ist das SAP GUI sehr interessant. Zum einen bietet die auf dem Client liegende SAPINI-Datei einen hohen Informationswert, denn dort sind SAP-Systeme mit Adressen und Zielrouten hinterlegt. Zum anderen kann man sicher sein, das die Strecke vom Client zum SAP-System für diesen Desktop freigeschaltet ist.

SAP GUI Hack zur Übernahme der IP-Adresse **[zB]**

Wenn man Zugang zu einer Workstation oder einem Desktop hat, auf dem SAP GUI installiert ist, möchte man von hier aus mit seinen eigenen Hacker-Werkzeugen wie Nmap oder Metasploit weiter arbeiten. Da aber selbst einfach geschützte Arbeitsplätze in Unternehmen es nicht erlauben, Software zu verändern oder installieren, muss man hier einen Trick verwenden. Ich benutze dafür oft meinen Laptop mit einer Kali-Linux-Distribution. Hiermit versuche ich, die MAC-Adresse des PCs oder Laptops, den ich übernehmen will, zu ermitteln. Das geht meistens in der DOS-Kommandozeile mit dem Windows-Befehl `ipconfig /all`. Dieser zeigt mir für den Ethernet-Adapter die MAC-Adresse an. Diese gebe ich dann in Kali-Linux ein (»MAC Spoofing«). Dann stecke ich den Netzwerkstecker vom Desktop in den Laptop um. Ich bin jetzt zwar mit meiner neuen Maschine nicht angemeldet, habe aber auf der Netzwerkebene vollen Zugriff auf die Infrastruktur. Viele werden sagen, dass dies ein simpler Hack ist, aber trotzdem gehört er zum Standard-Repertoire und verdient es, hier erwähnt zu werden.

Eine klassische Gegenmaßnahme liegt im Betrieb des Netzwerks. In vielen Unternehmen wird bei dem für die Sicherheit zuständigen Netzwerkadministrator eine Warnung ausgelöst, wenn an Arbeitsplätzen Netzwerkkabel ausgesteckt und wieder eingesteckt werden. Darüber können solche Versuche identifiziert werden. Bei sicherheitsbewussten Unternehmen wird dann auch gleich jener berühmte breitschultrige Herr im schlecht sitzenden dunklen Anzug (mit der Beule in der Brusttasche) losgeschickt, um nachzusehen, was dort passiert.

4.2.2 Tier 1: Zugang aus dem Internet und Übergang ins Intranet

Dieses Netzwerksegment ist der Übergang vom Benutzer im anonymen Internet zum authentifizierten Intranet-Benutzer und kennzeichnet auch die Grenze zum Unternehmensnetzwerk. Traditionell nennt man eine solche Zone auch *Demilitarisierte Zone* (DMZ), abhängig von der jeweiligen Architektur. Wichtig ist, das hier, meist durch eine Firewall geschützt, der Prozess oder der Benutzer sich in

irgendeiner Form anmelden muss, sei es durch ein Ticket, einen VPN-Zugang oder ein simples Log-in. Aus Sicht eines SAP-Netzwerks ist Tier 1 eine weit außen liegende Grenze, denn in klassischen Unternehmensnetzwerken liegen die Anwendersysteme im Tier 2 und erst die SAP-Systeme selbst in Tier 3.

Das DIAG-Protokoll

Für die Kommunikation zwischen SAP GUI und dem Anwendungsserver wurde das *Dynamic Information and Action Gateway Protocol* (kurz DIAG) entwickelt. Es ist ein proprietäres Protokoll, dessen Spezifikation nicht veröffentlicht wurde – einige Details sind jedoch inzwischen bekannt geworden. DIAG übertragt binäre Daten, die im Standard komprimiert sind, es findet jedoch ohne die zusätzliche Verschlüsselung per SNC keine Absicherung des Datenverkehrs gegen Sniffing statt.

SAP-GUI-Netzwerkverkehr dekodieren

Die Art der Datenkompression ist inzwischen bekannt und es existieren bereits Add-ons für bekannte Netzwerkdiagnose-Tools, wie z. B. Wireshark, die den DIAG-Datenverkehr dekomprimieren und so die Rohdaten lesbar machen. Ein Angreifer, der die Workstation kompromittiert hat, auf der das SAP GUI läuft, kann sogar die Kompression einfach ausschalten; der Benutzer merkt dies zwar, da ein Pop-up-Fenster im SAP GUI ihn warnt – ein findiger Angreifer könnte dies allerdings umgehen (ein Ansatz hierzu ist den Autoren bekannt). Zudem ist fraglich, ob es sich für einen Hacker lohnt, den zusätzlichen Aufwand der Dekompression des Datenverkehrs zu vermeiden, wo dies doch recht einfach möglich ist. Dazu muss einfach die Windows-Umgebungsvariable `TDW_NOCOMPRESS` auf den Wert `1` gesetzt werden. Ob dies auf einem mutmaßlich gehackten Windows-Rechner der Fall ist, können Sie einfach über die erweiterten Systemeinstellungen prüfen:

1. Öffnen Sie die Systemsteuerung über das Startmenü.
2. Klicken Sie auf System und dann auf Erweiterte Systemeinstellungen.
3. Im Pop-up-Fenster wählen Sie den Reiter Erweitert und klicken dann auf Umgebungsvariablen.
4. Sollte die Variable gesetzt sein, erhalten Sie folgendes Bild (siehe Abbildung 4.2):

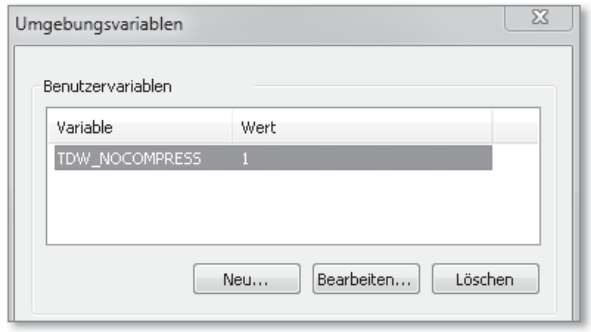

Abbildung 4.2 Umgebungsvariable zur Deaktivierung der DIAG-Kompression

Analyse eines Netzwerk-Mitschnitts

Trotzdem kennt damit ein Angreifer noch nicht die Protokollinterna und ist nicht in der Lage, eine SAP-GUI-Sitzung vollständig in verständliche Kommandos und Antworten zu übersetzen. Um an Benutzername/Passwort-Kombinationen zu gelangen oder kritische Daten zu extrahieren, ist dies jedoch auch nicht unbedingt notwendig! Ist dem Angreifer der Benutzername bekannt, so findet er das Passwort im Klartext in direkter »Nähe«. In Abbildung 4.3 ist ein Mitschnitt des Netzwerkverkehrs eines SAP-GUI-Log-ins als Benutzer `ddic` zu sehen. Das Passwort `abcd1234` ist nur einige Bytes nach dem Benutzernamen sichtbar (siehe Markierungen auf der rechten Seite).

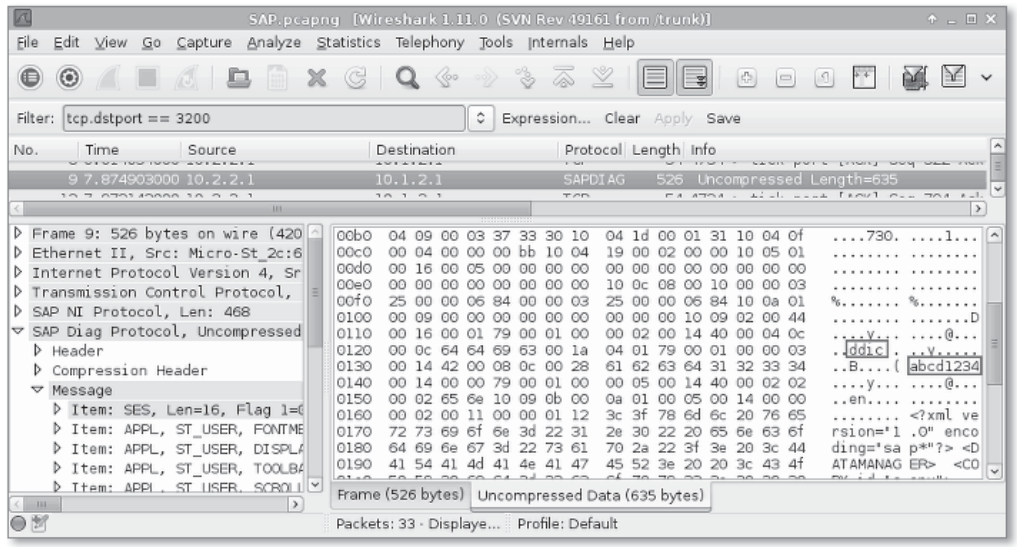

Abbildung 4.3 Benutzername und Passwort im Klartext

Das DIAG-Protokoll ist also im Standard – komprimiert oder nicht – ungeschützt! Ein Angreifer kann ohne tiefgreifendes, technisches Wissen Log-in-Daten Ihrer Benutzer aus mitgeschnittenem Netzwerkverkehr extrahieren. Doch es gibt Abhilfe. Sie können auch ohne eine Sign-on-Infrastruktur in SAP NetWeaver den Netzwerkverkehr zwischen SAP GUI bzw. dem BEx Analyzer und dem AS ABAP verschlüsseln.

SNC Client Encryption

Mithilfe von SNC Client Encryption können Sie die Kommunikation zwischen dem Client und einem AS ABAP per Secure Network Communications (SNC) verschlüsseln und die Daten vor neugierigen Blicken und Manipulationen absichern. Da der komplette Verkehr geschützt ist, können Hacker weder Log-in-Daten mitzulesen, noch geschäftliche Vorgänge ausspionieren oder in sie eingreifen. Als einzige technische, nicht in jedem Falle bereits vorhandene Voraussetzung ist ein *Microsoft Active Directory Server* zu nennen.

Eine verschlüsselte SAP-GUI-Sitzung, wie sie in Abbildung 4.4 zu sehen ist, läuft dann folgendermaßen ab:

1. Der Anwender meldet sich an einer Windows-Domäne an und startet eine SAP-GUI-Verbindung zu einem AS-ABAP-System, das SNC Client Encryption verwendet.
2. Die SNC-Client-Encryption-Komponente fordert ein Service-Ticket vom Microsoft Active Directory Server an.
3. Der Microsoft Active Directory Server gibt das Ticket an die SNC-Client-Encryption-Komponente zurück.
4. Der Benutzer wird vom SAP GUI zur Eingabe seiner Log-in-Daten aufgefordert.
5. Alle Kommunikation mit dem AS-ABAP-System findet nun verschlüsselt statt.

Das genaue Vorgehen zur Einrichtung von SNC Client Encryption kann je nach Release-Stand der beteiligten Systeme variieren – bitte rufen Sie daher immer die zur Version ihres AS-ABAP-Systems gehörige SAP-Dokumentation auf; dort gibt es ein eigenes Kapitel »SNC Client Encryption für Kennwortanmeldung verwenden«, in dem auch weiterführende Hinweise verlinkt sind.

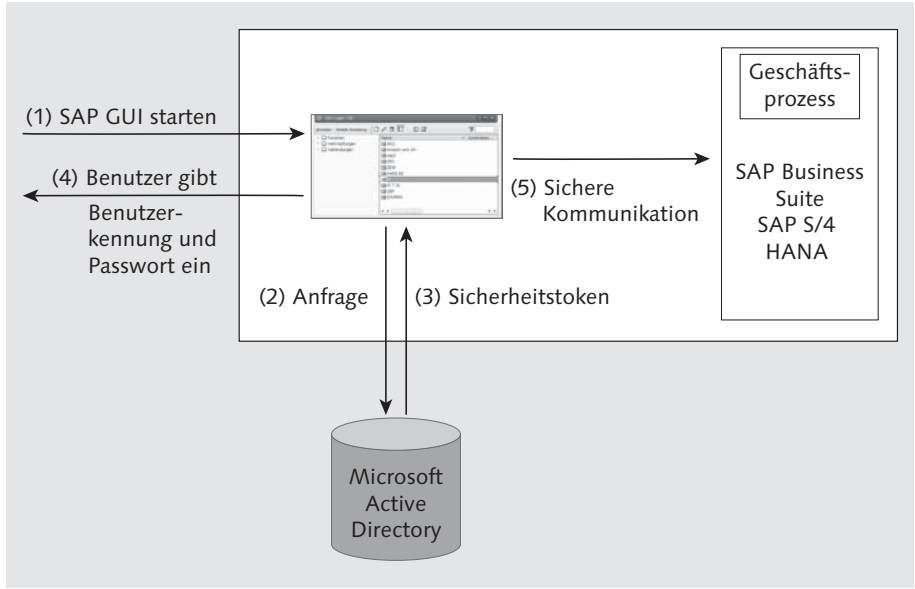

Abbildung 4.4 Ablauf einer SAP-GUI-Sitzung mit Client Encryption (Quelle: SAP)

4.2.3 Tier 2: Übergang von Intranet zur SAP-Tier

Der Übergang von Tier 1 (der DMZ) nach Tier 2 funktioniert in der Regel wieder durch eine Firewall, die das DMZ-Intranet gegen das interne Netzwerk, manchmal auch Campusnetzwerk genannt, abgrenzt. In Tier 2 liegen oft die Mitarbeiter-Systeme, auf denen dann auch der SAP Rich Client (SAP GUI) läuft. Aber auch externe Programme und nicht unternehmenskritische Anwendungen können hier laufen. Aus dieser Ebene 2 werden dann die Verbindungen zu den SAP-Systemen im inneren Tier 3 aufgebaut.

RFC-Protokoll

Remote Function Call (RFC) ist ein proprietäres SAP-Protokoll. Der RFC-Gateway ist die funktionale Verbindung der Endpunkte der Kommunikation mit einer äußeren Komponente. Es gibt in einem Standard-SAP-System zehntausende solche Funktionsaufrufe, von denen in der Regel nur ein kleiner Teil wirklich von außen aufgerufen wird. In vielen Fällen sprechen SAP-Server mit anderen SAP-Servern auf der Basis von ABAP-Anwendungen miteinander und benutzen das RFC-Protokoll zwischen AS-ABAP-Stacks. Ein System, der *RFC Client*, initiiert die Kommunikation und der Server nimmt diese Kommunikation auf. Abbildung 4.5 zeigt einen Überblick dieser unterschiedlichen Verbindungen.

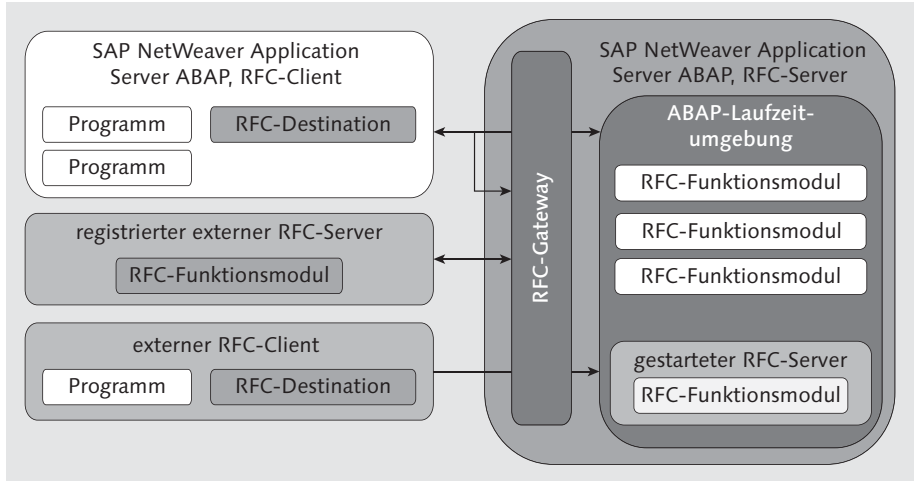

Abbildung 4.5 Überblick über das RFC-Protokoll (Quelle: SAP)

Aber auch externe Anwendungssysteme können diese Kommunikation initiieren. Es gibt Implementierungen der SAP-Kommunikationsbibliothek als SAP-Konnektoren in Java und als .NET-Implementierung für Microsoft-Umgebungen.

RFC-Verbindungen und Verschlüsselung

RFC-Verbindungen können sich auch der Verschlüsselungsfunktionen der SNC-Bibliotheken bedienen, ähnlich wie es das SAP GUI und das DIAG-Protokoll auch machen (siehe Abbildung 4.6). Diese Kommunikation wird dann in den entsprechenden Basis-Transaktionen STRUST, SM59 und RZ11 konfiguriert. Für die Clients gibt es ebenfalls entsprechende Bibliotheken, die alle auf der SAP Cryptolib basieren und diese implementieren.

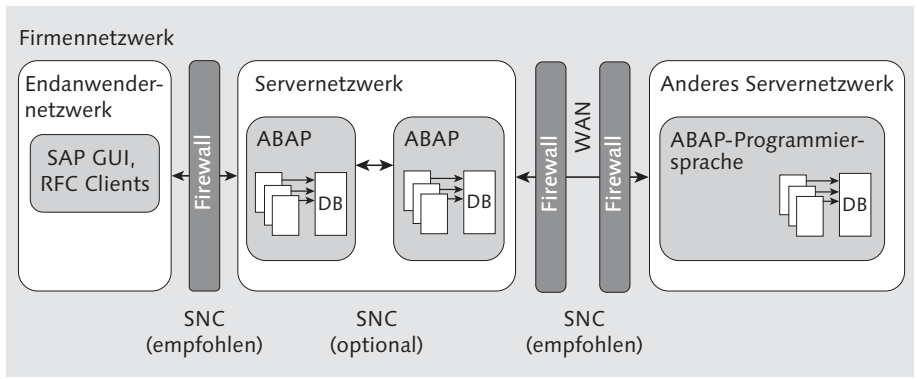

Abbildung 4.6 RFC mit SNC-Verschlüsselung (Quelle: SAP)

4.2.4 Tier 3: Die SAP-Systeme

Bis zur Einführung von SAP HANA hatte SAP zu Datenbanken eine ähnliche Haltung wie zu den Netzwerken. SAP wollte weitestgehend unabhängig von Datenbanken sein und implementierte nur eine Schnittstelle zu den Datenbanken hin und nannte diese *Open SQL*. Es war letztlich eine klassische Implementierung einer Datenbankschnittstelle, wie man sie auch im Bereich ODBC kennt, einem Protokoll, das letztlich von und zu Datenbanken redet.

ODBC und DBCON

Dieses Protokoll heißt DBCON und ist in der gleichnamigen Tabelle implementiert. Auf dieser Schnittstelle werden ausführbare SQL-Befehle gesendet und das SAP-System (in der Regel der laufende ABAP-Serverdienst) erhält die Antwort in Form von einer mehr oder weniger komplexen Tabelle als Datenbereich zurück. Dieses *Result Set* ist die rohe Datenbasis, die das ABAP-Programm weiter bearbeitet.

Die Kommunikation zwischen SAP-System und Datenbank wurde bis vor ein paar Jahren kaum als Sicherheitsproblem gesehen. Man betrachtete die Server als sicher (da diese ja bereits in den Netzwerksegmenten standen, die durch eine oder mehrere Firewalls geschützt waren). Zudem waren die Datenbankserver von einem ehemaligen Marktführer wie Oracle ja auch noch einmal besonders geschützt. SAP allerdings kommunizierte in der Regel über Verbindungen vom Anwendungs- zum Datenbankserver, die keinen oder nur sehr rudimentären Schutz auf den Verbindungen hatte. Bis vor einigen Jahren (und in vielen Systemen heute noch existierenden Produktivversionen) war die Oracle-Verbindung komplett ungeschützt. Ein Angreifer konnte (und kann) auch heute noch diese passwortlose Verbindung jederzeit übernehmen.

4.3 Virtuelle Netzwerke und Software-Defined Networks

Der Begriff der *Software-Defined Networks* (SDN) ist schon seit vielen Jahren im Umlauf, aber seinen Weg aus dem Elfenbeinturm der Wissenschaft in die Welt der industriell genutzten Netzwerke begann 2008. So wie die In-Memory-Datenbanktechnologie SAP HANA aus Stanford-Forschungen heraus entstand, wurde auch das Software-Defined Networking hier weiterentwickelt.

Stanford und Open Network Foundation

Da die Stanford-Universität in Palo Alto liegt, also im Herzen des Silicon Valley und in direkter Nähe zu Google, Facebook, SAP und Oracle, wurde die Idee entsprechend gut aufgenommen. Aus dem zuerst einmal in akademischen Kreisen bekannten Modell wurde 2001 die Open Networking Foundation gegründet, die das Modell als Open-Source-Modell weiter benutzt.

Die Hauptidee ist es, nur noch die Layer 1 und 2 (und eventuell 3) von entsprechenden Switches vornehmen zu lassen und die Switches direkt mit einem rein auf Software basierenden Controller kommunizieren lassen, der die anderen Funktionen (Ebene 3 bis 7) eines Netzwerks implementiert in reiner Software übernimmt. Bisher lag ja die überwiegende Funktion in dedizierter Hardware, von Netzwerkadaptern über Switches und Router bis hin zu den entsprechenden Adaptern in den Zielservern. Nun sollte dies alles von einer eigenen (Software-)Appliance vorgenommen werden.

Nur die Switches bleiben bestehen

Switches mit mehreren Dutzend Anschlüssen gibt es heute als sogenannte »Commodity«, also als Massen-Billigware vor allem aus China. Dort werden die Switches mit integrierten Schaltungen hergestellt, so dass ein 48-Port-Switch für ein paar hundert Euro zu bekommen ist. Dieser Switch brauchte nur ein Interface nach der Norm der in Stanford initiierten *Open Network Foundation*, und man kann den Rest des Netzwerks über entsprechende Frameworks abbilden.

Der Ansatz mit den billigen Switches und Softwareframeworks sollte neue Möglichkeiten bringen. Netzwerke sollten direkt programmierbar werden und zentral durch einen reinen softwarebasierten Ansatz zu managen sein. Damit sollten Sie den Netzwerkverkehr optimal organisieren, lenken und verwalten können. Dadurch wären auch Anforderungen aus neuen Diensten wie Videostreams, cloud-basierenden Diensten oder die Separierung von Kundenetzen in großen Datacentern direkt möglich.

Separierung von Kontrollfluss und Datenfluss

Der Datenfluss in einem Netzwerk wird in eine *Control Plane* aufgesplittet, in der das ganze Routing stattfindet. Hier wird ein Netzwerk-Request von und nach einem Ziel geleitet. Auf der *Data Plane* läuft der assoziierte Datenverkehr. Sieht man sich heute einen beliebigen Backbone eines großen Providers an, so sind dort 30–50 % der Auslastung auf Streaming Video Services wie YouTube und Amazon zurückzuführen. Die immer größere Menge an Video-Konferenzen

kommt hinzu. Solch ein Verkehr würde davon profitieren, wenn er separat als Stream und nicht paketorientiert weitergeleitet wird.

Gerade große Datacenter haben begonnen, in ihren Rechenzentren SDN-Netzwerke zu schaffen und produktiv einzusetzen. Zwar gibt es noch keine Standards, aber die Möglichkeiten, die sich die Betreiber hier selbst schaffen, sind den Aufwand nach eigenem Bekunden wert. Gerade in den Bereichen Kundensegmentierung (Multi-Tenant) und content-basiertem Routing (Streaming, Packeting) sind die Vorteile sehr hoch.

Auch der Bereich Security wächst deutlich. Wo es protokollunabhängige Ebenen gibt, die nur für die Kontrolle zuständig sind und wo es Datenebenen gibt, die die kompletten Datenströme steuern, ist es möglich, ganz neue Sicherheitskontrollen einzubauen. Die *Security-Information- und Event-Management-Systeme* (SIEM, siehe Abschnitt 1.2.7, »Bestimmung der technischen Auswirkungen eines Angriffs«) mit ihren Datenmustern lassen sich hier in Echtzeit auf die Datenströme anwenden. So können auch kontrolltechnisch komplett neue Anwendungen entstehen.

Die neue Architektur der Software Defined Networks wird die Implementierung von Netzwerken in den Datacentern grundlegend verändern. Und mit der Architektur wird auch die Sicherheit in Netzwerken komplett neu definiert. In jeder der neuen Komponenten dieser Architektur steckt auch ein starker Sicherheitsaspekt, der nicht mehr an eine Protokoll-Implementierung wie bei ISO/OSI gekoppelt ist, sondern sich ausschließlich über Software und deren Schnittstellen definiert. Dieser Ansatz hat heute schon neue Sicherheitssysteme erzeugt, die in den noch wenigen proprietären Implementierungen in ausgewählten Datacentern zu sehen ist. Die flächendeckende Einführung und Adaptierung dieser Technologie wird aber in den nächsten Jahren zu einer radikalen Änderung auch in der Sicherheit der Netzwerke führen. In Abbildung 4.7 wird solch eine Architektur gezeigt.

Control Plane

Die grundlegende Idee ist es, dass eine *Control Plane* die eigentlichen Datenströme kontrolliert und bewegt. Die Control Plane hat ein *Northbound Interface*, das die Anwendungen kontrolliert, die auf diese Control Plane einwirken.

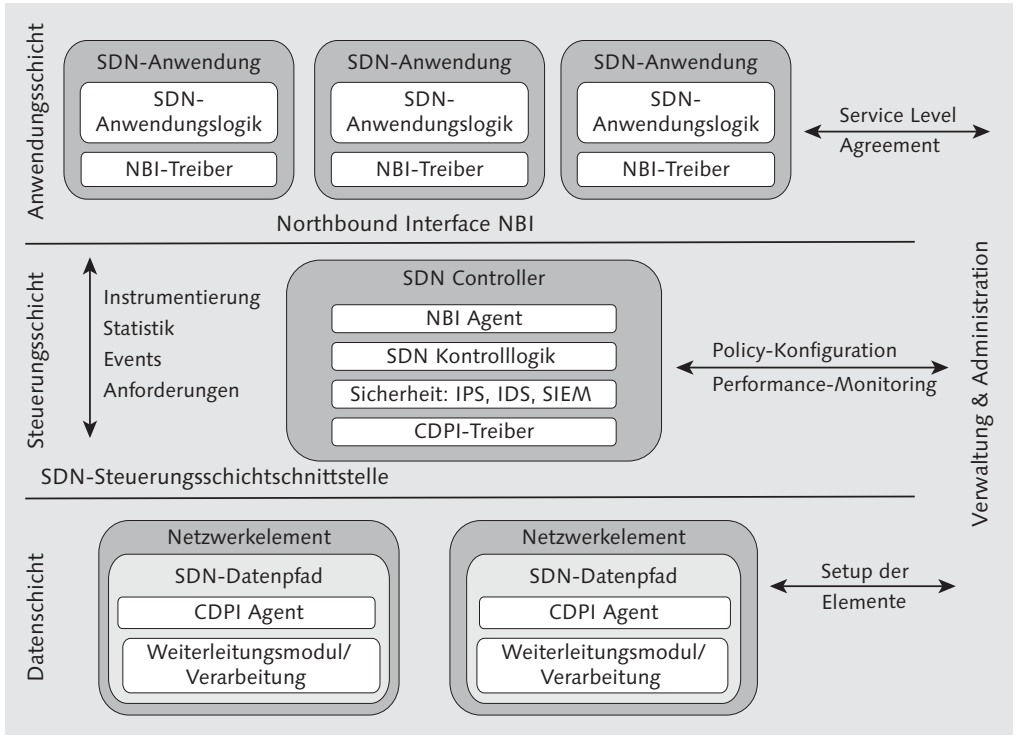

Abbildung 4.7 SDN-Architektur: Überblick der Open Networking Foundation

Application Plane

Die Anwendungen selbst bestimmen das Verhalten des Netzwerks und haben die Intelligenz und die Attribute zur Steuerung. Die Ausführung dieser Logik wird dann aber der Control Plane übergeben. Die klassischen Funktionen wie Session Handling, intelligentes Routing und Datenanalyse sind in den Anwendungen und nicht mehr Funktionen des Netzwerks.

CDPI

Ebenso verhält es sich mit dem *Control to Data Plane Interface* (CDPI). Das CDPI übergibt die Steuerungen (von der Control Plane an die *Data Plane)* an die Schicht, die die Daten enthält und die Destinationen, von denen und an die die Daten bewegt werden sollen. Somit sind Netzwerksteuerung, Netzwerklogik und Daten vollkommen entkoppelt. Dadurch ist eine wesentlich höhere Flexibilität möglich als in herkömmlichen Netzwerkmodellen nach ISO/OSI. Die Segmentierung und Paketorientierung der Netzwerke sowie die Fokussierung auf Endpunkt-Kommunikation fällt hier komplett weg.

Data Plane

Aus Sicht der Endpunkte entsteht durch die Control Plane, die Daten von A nach B bewegt, ein Datenpfad. Hier können auch große Datenmengen wie Videostreams bewegt werden, ohne diese stark zu segmentieren, oder es können Datenmengen gezielt geroutet werden, wie es in einem Multimandanten-Rechenzentrum nötig ist.

Forwarding Engine

Letztlich muss das SDN in letzter Konsequenz wieder Switches bedienen, die die Umsetzung auf die »letzte Meile«, die Netzwerktopologie der ISO/OSI-Ebenen 1 und 2 bringt. In großen Datacentern werden diese SDN-Segmente aber auch direkt gekoppelt, gerade bei hohen Datenmengen. Die neue Generation von Netzwerken jenseits der 10-Gbit-Datenmengen, die Backbone-Netze mit 100 Gbit, benötigen neue Methoden, solch hohe Datenmengen zu bewegen.

4.3.1 Die Idee einer neuen offenen Netzwerkarchitektur

Die offene SDN-Architektur erregte natürlich das Missfallen aller Hersteller, die bisher teure Appliances verkauft haben. Dies betrifft alle Switch-Hersteller wie IBM und andere, aber vor allem die großen Netzwerkausrüster wie Cisco, CheckPoint Juniper und viele andere. Natürlich sahen sie eine Vision von billigen Switch-Appliances aus China und offener, kostenloser Software als nicht zielführend an. Aber auch die Hersteller konnten nicht ignorieren, das herkömmliche Netzwerkarchitekturen an ihre Leistungsgrenzen kommen, und konnten die vom großen Data-Center-Markt schon antizipierte Architektur nicht mehr zurücknehmen.

Open Network Foundation

So umarmte man, was man nicht mehr bekämpfen konnte und wurde Mitglied in der Open Networking Foundation, um fortan die Entwicklung so zu lenken, dass kommerzielle Interessen und Portierungen weiterhin berücksichtigt werden. Es gibt mittlerweile SDN-Lösungen von allen großen Anbietern, die aber eher eine proprietäre Tendenz haben. Die SDN-Frameworks im Umfeld der Standford-Initiative sind langsam verblichen, vor allem, weil keines der Frameworks so hochskalierbar und belastbar ist, wie es vor allem von großen Datacenter gefordert wird. Die Datacenter wiederum haben, als größte Kunden der Netzwerkausrüster, funktionierende eigene Implementierungen, die sie aber gerne gegen kommerzielle Implementierungen austauschen würden, um nicht weiterhin selbst entwickeln zu müssen.

SDN im Datacenter heute

SDN ist weiterhin im Fluss: Große Kunden und Datacenter können und werden unter dem Innovationsdruck hier weiter entwickeln. Man erwartet in den nächsten fünf Jahren auch den flächendecken-

den Durchbruch dieser Technologien. Dann wird SDN das Networking, wie wir es heute kennen, komplett verwandelt haben.

4.3.2 Sicherheit im Software-Defined Network

SDN bietet komplett neue Ansatzmöglichkeiten, Sicherheit im Rechenzentrum zu implementieren. Ist es bisher softwaretechnisch ein mühseliges Unterfangen, die Pakete der ISO/OSI-Ebenen 1 bis 4 zu sammeln, auszuwerten und in einen Kontext wie SAP zu stellen, fällt all dies weg. Bei Netzwerkgeschwindigkeiten von 10 bis 100 Gbit/s würden auch herkömmliche Ansätze nicht mehr funktionieren.

Im Zusammenspiel von Application Plane, Control Plane und Data Plane lassen sich Datenströme gezielt analysieren. Es muss nicht künstlich ein Kontext hergestellt werden (was den Echtzeit-Ansatz nicht realisierbar macht), sondern der Datenfluss kann ebenso wie ein Stream betrachtet und analysiert werden. Mustererkennung und Reaktion auf die Muster kann direkt in der Application Plane implementiert werden. Durch die Einwirkung der Control Plane auf die Data Plane kann dann direkt eine Aktion (wie z. B. der Abbruch) ausgeführt werden und es muss nicht umständlich eine weitere Network Appliance angesteuert werden.

Angriffe auf SDN

Aber auch das Hacking auf diese Infrastrukturen wird sich in demselben Maße entwickeln und als Sicherheitsberater werden wir uns dann damit beschäftigen, wo die Angriffsvektoren auf die Data und Control Planes entstehen und wie man diese bekämpft.

Zukunft von SDN

SDN wird heute schon von großen Datacentern als proprietäre Lösung eingesetzt und hat das Potenzial bewiesen, das es in einem solchen Umfeld haben kann. Es wird noch einige Jahre dauern, bis diese Technologie in den klassischen IT der Unternehmen ankommt, vermutlich mit dem nächsten Generationenwechsel der Appliances wie Firewalls, Load Balancern und Switches. Und diese Technologie steckt auch schon in allen virtualisierten Netzwerkumgebungen wie NSX von VMware, die bereits zeigen, wie Security auf einem solchen Layer funktioniert.