Gliederung

1. Ausbildungsbetrieb und Einsatzgebiet

Das zweite Praktikumssemester im Rahmen meines Informatik-Studiums an der FH Regensburg leistete ich bei der Firma OneVision Software AG in Regensburg ab. Das Unternehmen existiert seit September 1994 und produziert Software für die Optimierung der Vorgänge in der Druckvorstufe. Dabei kommen vor allem Postscript und PDF (Portable document format[1]) zum Einsatz. OneVision beschäftigt ca. 100 Mitarbeiter und unterhielt zu Beginn meines Praktikums Aussenstellen in ...

- Hannover,
- St. Thibault-des-Vignes, Frankreich,
- Milton Keynes, Großbritannien,
- Kopenhagen, Dänemark und
- New Jersey, USA.

Die Firma gliedert sich in folgende Abteilungen:

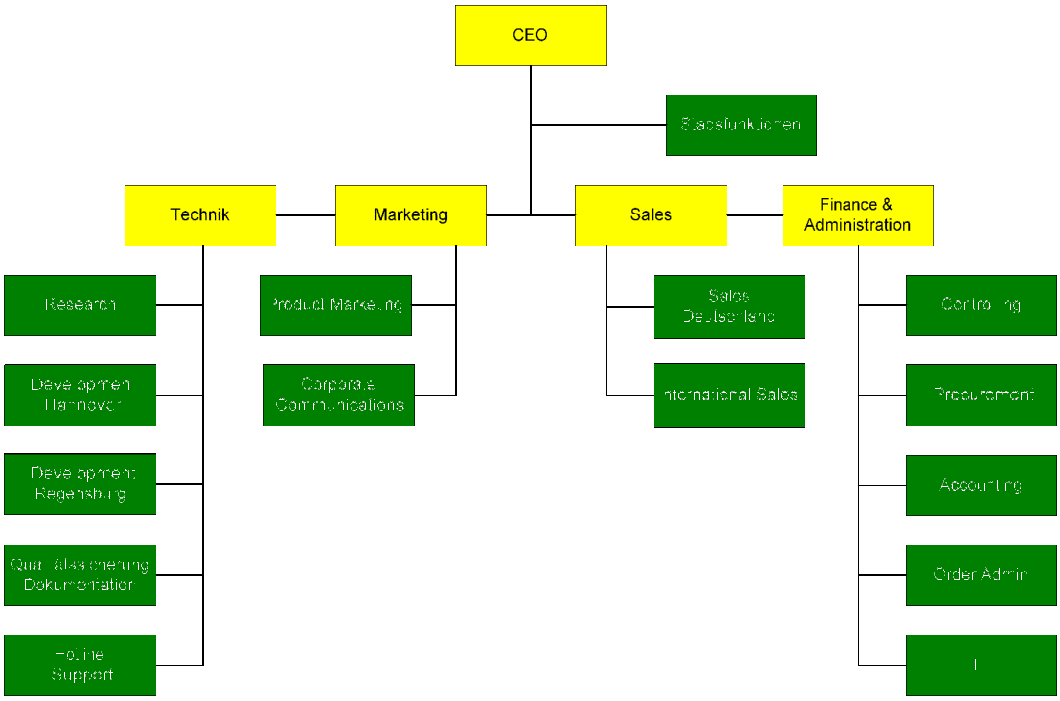

Abbildung 1: Firmenstruktur

Eingesetzt wurde ich in der IT-Abteilung, die für den reibungslosen Betrieb der Rechner und die komplette informationstechnische Infrastruktur im Unternehmen zuständig ist.

2.Eingesetzte Entwicklungsumgebung

2.1.Hardware

Während des Praktikums stand mir zum einen ein Arbeitsplatzrechner (Athlon-700, 256 MB RAM später dann ein Dual-Pentium II-400, 256 MB RAM) zum anderen ein Testfeld mit zahlreichen leistungsschwächeren Maschinen (Pentium-133 bis Pentium-300) zur Verfügung.

2.2.Software

Da die Kommunikation im Unternehmen auf Lotus Notes basiert, wurde auf den Arbeitsplatzrechnern Microsoft Windows NT bzw. 2000 mit Lotus Notes R5 installiert. Als Office-Suite kam StarOffice 6.0 zum Einsatz.

Als Betriebssysteme im Testfeld wurden SuSE Linux 7.2 und 7.3 sowie Windows 2000 benutzt. Zusätzlich waren...

- FreeS/WAN 1.95 mit X.509 Patch 0.9.8,
- openSSL 0.9.6,
- das VPN Package von Marc Müller,
- Kerio WinRoute pro 4.2.1,
- Kerio TinyFirewall 2,
- Netsaint 0.0.7,
- Apache httpd 1.3.24
- und diverse andere

... im Einsatz.

3.Projekte

Da dieser Praktikumsbericht noch während des Praktikums entsteht und die Projekte teilweise noch nicht komplett realisiert bzw. in Angriff

genommen wurden, kann im folgenden nur das erste Projekt umfassend beleuchtet werden.

3.1. Vernetzung der Standorte mit einem VPN

3.1.1. Situation vor Projektbeginn

Wie schon unter Punkt 1 erwähnt ist OneVision weltweit mit Außenstellen vertreten. In den Filialen ist -genau wie in Regensburg- ein LAN (local area network[2]) vorhanden um die Arbeitsplatzrechner und Server miteinander zu verbinden. Über einen Linux-Gatewayrechner wird das LAN an das Internet angebunden. Dabei kommen DSL (digital subscriber line[3]) und Standleitungen zum Einsatz. Ein transparenter Übergriff von einem Arbeitsplatzrechner in einem LAN auf einen Rechner im anderen LAN ist dabei nicht möglich. Das hat Schwierigkeiten in der Kommunikation im Unternehmen zur Folge: Administrationsaufgaben werden über den Umweg von SSH (secure shell[4]) -Zugriffen auf die jeweiligen Gateways durchgeführt, das Intranet wird per CD versendet und manuell eingespielt, etc.

Ziel ist es einen transparenten Übergang zwischen den Netzen und damit ein sog. VPN (virtual private network[5]) zu schaffen. Darauf setzen dann Dienste wie HTTP (hypertext transfer protocol[6]) für das Intranet, CVS (concurrent versioning system[7]) für die Codeentwicklung, SMB (server message block[8]) für die Authentifizierung am Windows-Netzwerk, VoIP (voice over internet protocol[9]) für Telefonie,... auf. Die Verbindung über das Internet wird dabei verschlüsselt. In die Lösung integriert werden sollen die Außendienstmitarbeiter, die mit ihren Laptops Präsentationen bei den Kunden vorführen oder per Wählverbindung Kontakt mit dem VPN aufbauen wollen.

3.1.2. Grundlagen VPN und IPSec

OneVision benötigt Site-to-Site und Site-to-Host – Verbindungen. Dabei werden die Daten im ersten Fall nur zwischen den Gateways, die die lokalen Netze mit dem Internet verbinden verschlüsselt. Ein Abhören

innerhalb den beiden LANs ist theoretisch möglich, aber als Gefahrenquelle zu vernachlässigen. Vorteilhaft bei dieser Lösung ist, dass auf den Arbeitsstationen keine spezielle Software laufen muss, für den Anwender ändert sich praktisch nichts. Im zweiten Fall wird zwischen einem Gateway und dem Arbeitsrechner, einem Laptop direkt verschlüsselt. Dadurch übernimmt der Laptop Aufbau und Kryptographie des Tunnels, was mit höherer Rechnerlast und dem Installieren spezieller Software bezahlt werden muss. Die Verbindung zum VPN kann hierbei über die eingebauten Kommunikationsschnittstellen des Laptops wie LAN-Anschluß oder Modem erfolgen.

Vom Praktikumsbetreuer Dr. Dieter Braun war die Realisierung mit IPSec (IP internet security[10]) angedacht. IPsec wird von der IETF (internet engineering task force[11]) entwickelt und verwaltet. Mit IPSec steht ein allgemein verbindlicher, herstellerübergreifender Standard zur Verfügung, der den Datenaustausch zwischen unterschiedlichen Security Gateways im Rahmen einer VPN-Lösung regelt. Dabei muss IPSec folgende Aufgaben leisten:

- Authentifikation der Gesprächspartner,
- Sicherstellen der Integrität der Information,
- Verschlüsselung der Information,
- Massnahmen gegen sog. Replay-Angriffe und
- Schlüssel-Management.

Die bereits existierenden Gateways, die momentan hauptsächlich als Firewalls genutzt werden, nutzen SuSE Linux mit Kernel 2.4.x als Betriebssystem. Das unter der GPL (GNU public license[12]) stehende Projekt FreeS/WAN (free and secure wide area network[13]) von John Gilmore ist die bevorzugte IPSec Implementierung für Linux.

3.1.3.Einordnung von IPSec in das ISO/OSI-Schichtenmodell

Während andere Verschlüsslungsprotokolle wie L2TP (layer 2 tunneling protocol[14]), PAP (password authentification protocol[15]) oder CHAP

(challenge handshake authentification protocol[16]) bereits auf Layer 2 des ISO/OSI[17]-Schichtenmodells aufsetzen, nutzt IPSec die Vermittlungsschicht auf Layer 3. Hier läuft ein Grossteil des IPSec Codes. Lediglich die Administrationstools und der Schlüsselaustausch läuft in der Anwendungsschicht. Damit werden alle Anwendungen, die auf dem TCP[18]/IP-Stack ab Layer 3 aufsetzen auf Wunsch verschlüsselt. Dazu wird das eigentliche IP-Paket verschlüsselt und in ein neues Paket „eingepackt“. Somit bleiben die im ursprünglichen Paket enthaltenen IP Adressen, Portnummern und Kommunikationsinhalte geheim. Auch nicht routbare IPs können auf diese Art und Weise durch das Internet transportiert werden: die Internet-Router sehen nur die (öffentlichen) Source- und Destination-IPs der Gateways. Diese Eigenschaften gelten nur für IPSec im sog. Tunnelmodus. Die andere mögliche Spielart, der Transportmodus soll hier nicht näher betrachtet werden, da sie zur Realisierung eines VPN nicht beitragen kann.

3.1.4.„Verpacken“ der Daten mit ESP

Weiterhin soll hier nicht näher auf das AH- (authentication header[19]) Protokoll eingegangen werden. Obwohl Bestandteil von IPSec, chiffriert es die Nutzdaten nicht, sondern stellt nur sicher, dass die empfangenen Daten auch vom richtigen Sender kommen. ESP (Encapsulated security payload[20]) hingegen führt dazu zusätzlich Verschlüsslungsalgorithmen durch: Datenauthentizität und Datenintegrität werden sichergestellt. Der IPSec Standard sieht einige mögliche Algorithmen vor (DES_CBC[21] – data encryption standard-cypher block chaining, IDEA[22] – international data encryption algorithm, Blowfish, CAST_128[23] und 3DES[24] – triple data encryption standard). Das OneVision VPN wird mit 3DES-Kodierung realisiert. Der Sender schickt die Daten an sein VPN-Gateway. Dieses verschlüsselt das ankommende IP-Paket und verpackt es in ein neues Paket. Das Resultat ist in der folgenden Abbildung zu sehen. Unverschlüsselte Daten sind gelb bzw. hell, verschlüsselte grün bzw. dunkel dargestellt:

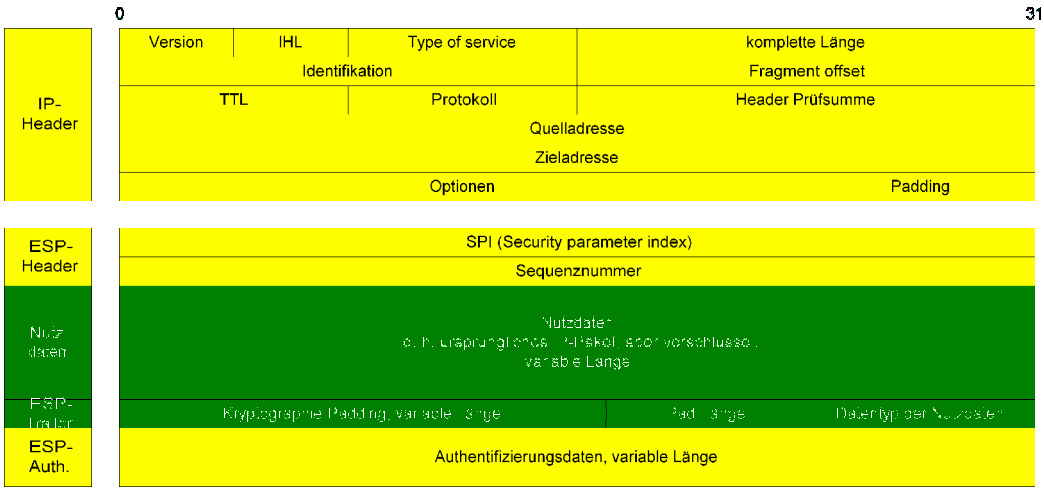

Abbildung 2: Aufbau eines ESP-Pakets

Kommt ein ESP Paket beim Empfänger an, so wird eine Authentifikation durchgeführt. Kann die unveränderte Herkunft des Pakets nicht bestätigt werden, so wird es verworfen. Durch diese Vorgehensweise wird nicht unnötig Rechenzeit für das Dekodieren des Pakets in Anspruch genommen und ein DoS (denial of service[25]) – Angriff durch Unmengen an gefälschten ESP-Pakten vereitelt. Ist hingegen die Herkunft des Pakets in Ordnung, wird es entschlüsselt und im TCP/IP-Stack hochgereicht.

3.1.5. Schlüsselmanagement mit IKE

Dreh- und Angelpunkt einer Authentifizierung, wie sie bei IPSec passiert ist das Schlüsselmanagement. Die Kryptographiealgorithmen können noch so sicher sein und sind doch wertlos, wenn den falschen Kommunikationspartnern vertraut wird. FreeS/WAN unterstützt zwei Arten der Schlüsselverteilung: Manuell oder automatisch. Da die manuelle Verteilung schnell unübersichtlich wird, ist ihr eine automatische Verteilung klar vorzuziehen. Das verwendete Verfahren heisst IKE (internet key exchange[26]). IKE muss die Kommunikationspartner authentifizieren, eine sog. SA (security association[27]) erzeugen und bei Bedarf Schlüssel erzeugen und regenerieren. IKE basiert auf dem ISAKMP[28]/Oakley-Protokoll (internet security association and key management protocol, Oakley ist die konkrete Ausgestaltung benannt nach seinem Entwickler). ISAKMP schreibt zwei Phasen vor: In der ersten (main mode) wird eine ISAKMP-SA erzeugt, die den ISAKMP-Datenverkehr kodiert, in der zweiten (quick mode) folgt die IPSec-SA,

welche für die Verschlüsslung der Nutzdaten zuständig ist. Der main mode wird nur einmal, beim Verbindungsaufbau durchlaufen. Der quick mode hingegen kann öfters durchgeführt werden. Je öfter, desto höher ist die Sicherheit falls das VPN trotz aller Sicherheitsmassnahmen doch kompromittiert wird. Der Erwähnung wert ist zu guter letzt noch die Tatsache, dass FreeS/WAN mit einer Untermenge von IKE arbeitet. Der Schlüsselmanagement-Deamon ist vom Funktionsumfang keine vollständige Implementierung von ISAKMP, jedoch reichen die Fähigkeiten für das Aufbauen eines VPNs aus.

3.1.6. Testumgebung

Ein Einspielen der Software auf die Gateways per SSH wäre vermutlich möglich, ist aber wegen der Gefahr einer Fehlkonfiguration nicht empfehlenswert. In diesem Fall müsste die Maschine von Hand neugestartet und der Fehler lokal an der jeweiligen Maschine korrigiert werden. Deshalb werden die zu erwartenden Szenarios vorher in einem speziellen Testfeld ausgibig getestet.

Der Test an nur einem Rechner unter Zuhilfenahme von user-mode-linux, welches virtuelle Linux-Maschinen auf einem Rechner bereitstellt, erwies sich wegen hoher Komplexität und Inkompatibilitäten zu SuSE Linux 7.x als schwierig. Da das Entwickeln eines SuSE root filesystems wohl zu lange gedauert hätte, entschied man sich für den Test mit real existierenden Rechnern durchzuführen.

Dazu wurde mit fünf Computern ein vereinfachtes Abbild der echten Rechnerstruktur gebildet, wie auf der folgenden Abbildung 3 zu erkennen ist. Dabei wurden die IP-Adressen teilweise verfälscht, um keine seniblen Daten zu verbreiten.

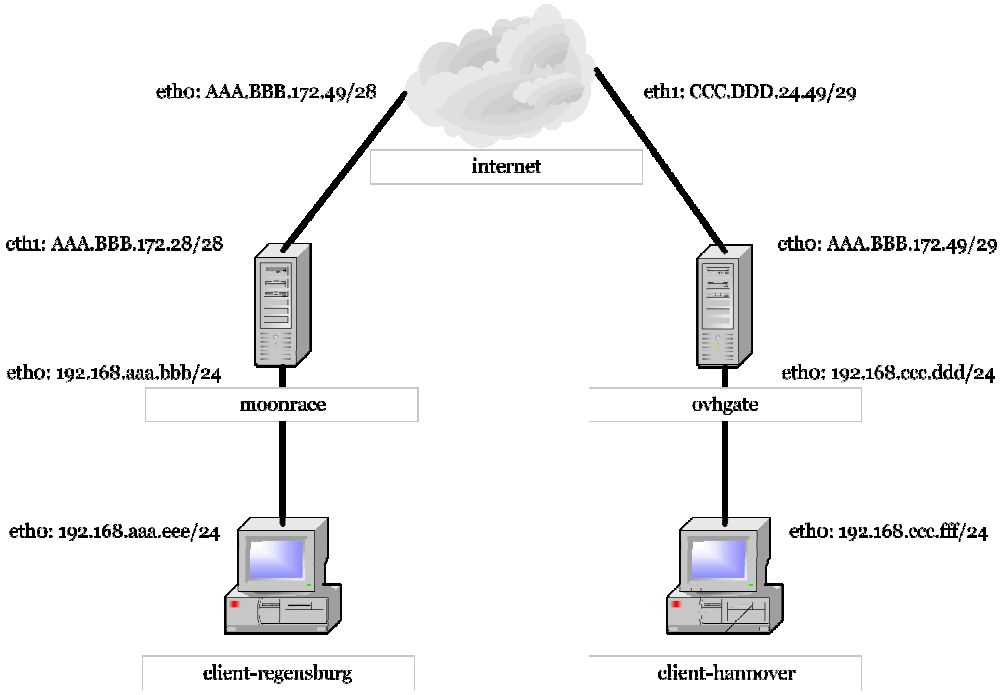

Abbildung 3: Grundkonstellation des Testfelds

Zwei Rechner stellen die Gateways moonrace in Regensburg und ovhgate in Hannover dar. Dahinter liegt jeweils ein Rechner, der das lokale Netz in Regensburg und Hannover simuliert (client-regensburg und client-hannover). Das Routing zwischen den beiden Netzen wird über einen weiteren Rechner (internet) realisiert. Private Adressen werden per SNAT (Source network adress translation[29]) auf den Gateways durch öffentliche IPs maskiert. Dieser Vorgang wird in /etc/rc.d/netfilter zusammen mit den Firewall-Regeln konfiguriert. Erreicht werden soll ein direktes Anpingen von client-hannover von client-regensburg aus, was ohne VPN nicht möglich ist: IPs aus dem privaten Addressräumen 192.168.xxx.yyy werden im Internet nicht geroutet.

FreeS/WAN besteht aus dem Linux-Kernelpatch KLIPS[30], dem ISAKMP-Schlüsselmanagement Pluto und diversen Administrationswerkzeugen. Die Software wurde installiert und die Konfigurationsdatei angepasst. Darüberhinaus wurde die Firewall-Konfiguration geändert: Für das neue „trustednet“ (192.168.96.0/20) wurden die bisher vorhandenen NAT[31]-Regeln außer Betrieb gesetzt, wobei für konventionelle IP-Verbindungen nach außen weiterhin NAT eingesetzt wird. Um den Aufbau des Tunnels zu ermöglichen, wird UDP[32]-Port 500 und das Protokoll 50 (ESP) freigeschaltet.

Zur Authentifizierung wurden zunächst asymmetrische RSA[33]-Schlüssel mit 2048 bit Länge benutzt, deren öffentlicher Teil in die Konfigurationsdateien der FreeS/WAN-Installationen eingetragen wurde. Der private Schlüssel eines Rechers verblieb auf ihm und war durch Einschränkung der Unix-Dateirechte zu sichern.

Mit dem Netzwerksniffer tcpdump auf dem Internetrechner konnte der Tunnelaufbau beobachtet werden: Es werden insgesamt neun Datenpakete ausgetauscht bis der Tunnel steht. Die ersten sechs (main mode) erzeugen eine ISAKMP-SA, die nächsten drei (quick mode) eine IPSec-SA. Im main mode wird ausgehandelt, welche Verschlüsslungs- und Hashalgorithmen, sowie welche Authentifizierungsmethode verwendet werden. Diese gelten nur für den Verbindungsaufbau. Nun ist sichergestellt, dass man sich mit dem richtigen Partner unterhält. Im quick mode werden dieselben Parameter erneut ausgehandelt, jedoch für die spätere Verschlüsslung der Nutzdaten. Eine weitere Analyse von ISAKMP würde hier zu weit führen, ist aber in den RFCs (requests for comments[34]) 2407, 2408 und 2409 detailliert ausgeführt. Nach erfolgreichem quick mode sind die verschlüsselten ESP-Pakete zu beobachten.

Zum Testen der Verbindungsgeschwindigkeit und -zuverlässigkeit wurden diverse Client-/Serverprogramme wie der Apache httpd, lynx, proftpd, SMB- und NFS[35]-tools auf den Rechnern installiert, die die lokalen Netzwerke darstellen. In der folgenden Tabelle 1 sind einige Messwerte zu sehen:

Transferart	Zugriffsart	Paketgröße	Zeit	Durchsatz
FTP	lesend	1500 Bytes	2' 30''	5,09 Mb/s
FTP	schreibend	1500 Bytes	2' 30''	5,09 Mb/s
NFS	lesend	8192 Bytes	scheitert	scheitert
NFS	schreibend	8192 Bytes	2' 33''	4,99 Mb/s
NFS	lesend	1024 Bytes	11'53''	1,07 Mb/s
NFS	schreibend	1024 Bytes	11'32''	1,10 Mb/s

Tabelle 1: Performance-Werte beim Datentransfer

Als Obergrenze wurde eine Geschwindigkeit von ca. 5 Mbit/s festgestellt, die einerseits wohl an der mangelnden Ausstattung der Testrechner lag, zum anderen aber auch im Produktionsbetrieb vollständig ausgereicht hätte. Interessant war die Abhängigkeit von der verwendeten Paketgröße. NFS mit 8 kB großen Paketen (die Standard-Einstellung) führte zu derart starker Fragmentierung der IP-Pakete, dass ein Transfer misslang. Grund für dieses Verhalten ist der zusätzliche Overhead von ca. 60 % der bei der Chiffrierung und Kapselung entsteht. Ein Mitsniffen auf dem Internetrechner zeigte erwartungsgemäß weder verwendete Protokolle, Inhalt der Kommunikation noch Passwörter o. ä.

3.1.7. Erweiterung um Authentifizierung mit Zertifikaten

Um auch Windows-Rechner (z. B. Laptops mit Wählleitung ins Internet) ohne Gateway mit dem VPN zu verbinden wurde Software aus dem Windows Ressource Kit und ein VPN Package von Marc Müller benutzt. Die IPSec Implementierung von Windows 2000 erfordert, dass die Schlüssel in Zertifikate eingebettet und von einem zentralen „Zertifikatsspeicher“ verwaltet werden. Zertifikate werden von genau einer zentralen Zertifizierungsstelle (der certification authority, kurz CA[36]) ausgestellt und binden individuelle Informationen wie Land, Organisation, Rechnernamen und Gültigkeitsdauer an den Schlüssel. Eine digitale Signatur der CA bestätigt die Echtheit des Zertifikats.

Auf einem Linux-Rechner, der speziell für diesen Zweck bereitgestellt wurde, wurde mit openSSL (secure socket layer[37]) eine CA und Zertifikate für die Linux-Gateways und Windows-Rechner erzeugt. Auf den VPN-Gateways wurden die RSA-Schlüssel durch Zertifikate ersetzt.

Einige weitere Methoden der Schlüsselverteilung, die zwar im Projekt nicht eingesetzt, aber durchaus mein Interesse geweckt haben sollen hier nicht unerwähnt bleiben: Von den Entwicklern von FreeS/WAN favorisiert ist die umfangreiche Verteilung der öffentlichen Schlüssel durch DNS (domain name service)-Server. DNS ist seit langem ein wesentliches Standbein des Internets und bietet sich deshalb für diese

Aufgabe geradezu an. Ein zusätzlicher Eintrag für die Domain liefert hierbei auf Anfrage den public-key zurück. Dieses Verfahren, auch opportunistic encryption genannt ist zwar noch in der Testphase, klingt aber sehr zukunftsweisend, vor allem in grösseren Umgebungen. Zu beachten sind allerdings noch einige Sicherheitsaspekte rund um DNS an sich.

Eine weitere interessante Möglichkeit für große Produktionsumgebungen ist auch die Verteilung von Zertifikaten per LDAP. Damit lässt sich der Vorgang hervorragend in einen Verzeichnisdienst integrieren. Mehr dazu im Punkt 3.2.2.

3.1.4. Übernahme ins Produktionssystem

Nachdem man im Testfeld genügend Erfahrung im Umgang mit FreeS/WAN und den anderen notwendigen Programmen gesammelt hatte wurde die Lösung ins Produktionssystem übernommen. Nun konnten die Entwickler in Hannover, die über ein Windows-Gateway und eine DSL Leitung verfügten, sowie die anderen Filialen mit Linux-Gateways ans VPN angeschlossen werden.

Für jede Anwendung mussten auf den Firewalls (unter Linux iptables, unter Windows die Personal Firewall Tinysoft Tiny Firewall 2 bzw. Tinysoft WinRoute) die entsprechenden Ports freigeschaltet werden. Dadurch wurde sichergestellt, dass z. B. auch im Falle eines Verlusts eines Laptops das Netzwerk nicht völlig kompromittiert wird. Zusätzlich würde in diesem Fall das Zertifikat sofort gesperrt werden, ein Verbindungsaufbau mit diesem Rechner würde nicht gelingen.

Auch die CA unterliegt strengen Sicherheitsanforderungen: um die Datensicherheit zu gewährleisten wurde ein Software-RAID (redundant array of inexpensive disks[38]) mit Spiegelung der Festplatten eingerichtet. Eine Firewall mit extrem strengen Regeln (Zugriff nur von einem bestimmten Rechner im LAN auf dem SSH-Port) und die Tatsache, dass der Rechner nur für Verwaltungsaufgaben rund um die Zertifikate eingeschaltet wird sollen unberechtigte Zugriffe verhindern.

Einer der ersten Dienste, die über das VPN geführt wurden war die Kontrolle der regelmässigen Backups mit der kommerziellen Software ARCserve in den Außenstellen. Als äußerst praktisch stellte sich auch die Möglichkeit heraus mit VNC (virtual network computing[39]), einem Fernwartungstool, von Regensburg aus direkt auf Arbeitsplatzrechner im VPN zugreifen zu können und den Anwendern behilflich zu sein. Weitere Anwendungen, wie z. B. VoIP für den Internet-Telefonverkehr sind angedacht und werden nach einer Wirtschaftlichkeitsüberprüfung implementiert.

3.2.Migration der verschiedenen Windows-Domänen nach Active Directory

3.2.1.Anforderungskatalog

In den Standorten sind derzeit jeweils voneinander unabhängige Windows-Domänen mit eigenen PDC (primary domain controllern[40]) eingerichtet. Über diese Domänen wird die Benutzer-, Computer und Rechtenverwaltung erledigt. In einem VPN bietet sich natürlich die zentrale Benutzerverwaltung für alle OneVision Mitarbeiter weltweit an. Jedes Objekt (Benutzer, Rechner, ...) soll dabei nur einmal vorhanden sein, damit der Benutzer ohne Probleme seinen Standort im Unternehmen wechseln kann. Das Verwaltungssystem soll hierarchische Strukturen, also beispielsweise Abteilungen und Filialen nachbilden können. Sub-Administratoren sollen dann bestimmte Aufgaben in ihrem Bereich erledigen, wobei höherrangige Stellen sie überschreiben könne. Passwort-Änderungen soll der Benutzer selbst vornehmen können. Dabei soll das Passwort für seinen Windows-, den UNIX-Account und den Lotus-Notes Account gelten (sog. Single sign-on).

Im Rahmen des Projekts soll geprüft werden, ob die genannten Anforderungen zuverlässig realisiert werden können. Die gewählte Lösung soll in einer Testumgebung evaluiert werden. Abschliessend soll ein Implementationsplan mit detaillierter Beschreibung der erforderlichen Schritte und zu erwartender Änderungen erstellt werden.

3.2.2.Entwickeln einer Lösung

Als einfachste Lösung wäre es möglich, eine Vertrauensstellung zwischen den einzelnen PDCs aufzubauen. Dabei müssten nur Konfigurationsarbeiten an den PDCs vorgenommen werden. Nachteilig ist hierbei aber die Tatsache, dass sich Microsoft bereits vom Modell der Domänencontroller verabschiedet hat. Eine Zukunftssicherheit kann also nicht gewährleistet werden. Da Microsoft zudem den Support für Windows NT 4.0 Server (mit dem die PDCs derzeit ausgerüstet sind) eingestellt hat, ist die Idee sinnvoll nach Möglichkeit offene Standards zu benutzen, um nicht mehr von einer bestimmten Firma abhängig zu sein.

Windows 2000 bietet die Möglichkeit einen hierarchisches Verzeichnisdienst zu erstellen, das active directory[41], kurz AD. Als Datengrundlage dient hierbei eine LDAP-Datenbank. LDAP, das lightweight directory access protocol[42] ist für diverse Betriebssysteme frei verfügbar und befriedigt daher die Anforderung möglichst Betriebssystem-unabhängig und kostengünstig zu sein. Darüber hinaus verfügen viele Programme, darunter auch Lotus Notes über Schnittstellen zu LDAP und auch die Anmeldung an UNIX-Rechnern per LDAP stellt dank geeigneter Authentifizierungsmodule kein Problem dar.

Momentan erscheint die Migration zu einzelnen active directory – Domains, die gegenseitig in einer sog. Trustbeziehung stehen im Anbetracht des Umstellungsaufwands am sinnvollsten. Eventuell ist es möglich, die Windows Server mit Linux Servern und dem ebenfalls freien Software-Paket SAMBA zu ersetzen.

Da dieses interessante, aber sicher umfangreiche Projekt beim Schreiben dieses Berichts noch in der Planungsphase war, kann nicht viel mehr darüber berichtet werden. Im Rahmen einer Tätigkeit als Werksstudent kann ich unter Umständen die weitere Entwicklung beobachten und voran treiben.

3.3.Serverüberwachung

3.3.1.Anforderung an die Lösung

Als letztes Projekt lohnt es sich noch die Überwachung der Server anzusprechen. Vor allem die Entwicklungs- und Qualitätssicherungsabteilung sind auf einwandfreien Betrieb und Erreichbarkeit einiger wichtiger Server und Netzwerkdienste angewiesen. Um Probleme schneller erkennen zu können wurde eine kontinuierliche Kontrolle der Server mit automatischer Benachrichtigung bei Ausfällen gewünscht. Bei der Implementierung fiel die Wahl auf NetSaint, einem Netzwerkmonitor, der umfangreiche Kofigurations- und Informationsmöglichkeiten bietet. Dabei stellt NetSaint nur die Schnittstelle zwischen den eigentlichen Testprogrammen (sog. Plug-ins) und den Informationswegen (Webseiten für das Intranet, E-Mail und SMS-Benachrichtigung, Eintrag in Datenbank, ...) dar. Dabei lassen sich ...

- Abhängigkeiten zwischen Rechnern und Diensten (um zwischen ausgefallenen und „nur“ nicht erreichbaren Rechnern unterscheiden zu können),
- Eskalationsstufen bei der Benachrichtigung (um nur Personen zu informieren, die die Möglichkeit zur Problembeseitigung haben),
- geplante Ausfälle (sog. scheduled downtimes, um während Wartungsarbeiten die Überwachung einzuschränken und unnötige Benachrichtigungen zu verhindern) und
- Event-handler (um teilweise Probleme automatisch zu beseitigen)

definieren. Dadurch scheint NetSaint eine umfassende Monitoring-Lösung zu sein, die im Unternehmen mitwachsen wird.

3.3.2.Einrichten der Überwachung

Zunächst wurde NetSaint im Testfeld eingerichtet. Neben dem NetSaint Binary und den Konfigurationsdateien wurde der Apache httpd als Webserver installiert um die NetSaint-Oberfläche anzuzeigen. Mit .htaccess-Dateien wurde die Authentifizierung am Webserver konfiguriert. NetSaint ermöglicht eine feine Einschränkung des Informations- und Kontrollangebots über die Web-Oberfläche, je nach zugewiesenen

Benutzerrechten. Nachdem die zu überwachenden Server und Dienste festgelegt wurden, konnte NetSaint bereits im Produktionssystem installiert werden. Auf der inneren Firewall konnte es sowohl Rechner im internen LAN, der DMZ[43], dem VPN und dem Internet kontrollieren. Als Benachrichtigungsmethode wurde während der Bürozeiten E-Mail an die IT-Abteilung, ausserhalb das Verschicken von SMS[44] an den Leiter der IT-Abteilung unter Zuhilfenahme von YAPS (Yet another pager software[45]) gewählt.

4.Persönliche Meinung

Das Thema Netzwerksicherheit wird in Zukunft wohl noch weiter an Bedeutung zunehmen. Deshalb ist es wichtig, nicht nur ein theoretisches Wissen über die verwendeten Techniken zu sammeln, sondern auch die Praxis in einem professionellen Unternehmen kennenzulernen. Das Praktikum bei OneVision erfüllte diesen Zweck hervorragend. Meine UNIX- und Linux-Kenntnisse wurden stark erweitert, zudem hoffe ich, dass v. a. das VPN dem Unternehmen in der Zukunft helfen wird viele Aufgaben schneller und eleganter zu erledigen.

Interessant waren auch die internen Mitarbeiterschulungen, in denen ich Einblick in die Programmiersprache PERL[46] gewinnen konnte. Im Rahmen einer eigenen Schulung konnte ich meine Erkenntnisse über das Einrichten und Betreiben sowie die theoretischen Grundlagen eines VPN den anderen Mitglieder der IT-Abteilung vermitteln.

5.Abkürzungsverzeichnis

Im Bericht wurden folgende Abkürzungen verwendet. Die Zahlen in Klammern geben die hochgestellte Zahl im Text an.

- 3DES – triple data encryption standard (24)
  Verschlüsslungsalgorithmus. Gilt als sehr sicher.
- AD – active directory (41)
  hierarchischer Verzeichnisdienst von Microsoft

- AH – authentication header (19)
  Unterprotokoll von IPSec. Sichert nur die Authentizität der Kommunikationspartner, nicht jedoch die Korrektheit des Inhalts.
- CA – certificate authority (36)
  zentrale Stelle, die Zertifikate signiert und verwaltet
- CAST128 (23)
  Verschlüsslungsalgorithmus
- CHAP – challenge handshake authentification protocol (16)
  Protokoll zur gesicherten Übertragung im Internet. Bevorzugt in reinen Windows-Netzwerken eingesetzt. Unsicher.
- CVS – concurrent versioning system (7)
  Codeverwaltungssystem für Softwareentwickler
- DES_CBC – data encryption standard-cypher block chaining (21)
  Verschlüsslungsalgorithmus. Lässt sich mit absehbarem Rechenaufwand aushebeln.
- DMZ – demilitarisierte Zone (43)
  spezieller Bereich im LAN, der vom Internet durch eine äussere, vom inneren LAN durch eine innere Firewall abgeschirmt ist
- DoS – denial of service (25)
  Art des Angriffs auf einen Rechner, bei dem er mit sehr viel Traffic oder der übermässigen Anforderung von Rechenleistung lahmgelegt wird.
- DSL – digital subscriber line (3)
  Verbindungsart mit hierzulande üblicherweise 768 kBit/s Downstream und 128 kBit/s Upstream Bandbreite über Kupfer-Telefonkabel.
- ESP – encapsulated security payload (20)
  Unterprotokoll von IPSec für die Kapselung der Nutzdaten. Sichert Authentizität der Gesprächspartner und den unveränderten Inhalt der verschlüsselten Kommunikation,
- FreeS/WAN – free and secure wide area network
  Programmpaket zur Erstellung von VPNs mit IPSec

- FTP – file transfer protocol
  Allgemein gebräuchliches Verfahren für den Dateiaustausch
- GPL – GNU public license (12)
  Lizenzvertrag, der u. a. Offenlegung der Quelltexte fordert.
- HTTP – hypertext transfer protocol (6)
  Grundlage aller Seiten im World Wide Web
- IETF – internet engineering task force (11)
  Organisation, die Internet Standards entwickelt
- IKE – internet key exchange (26)
  Protokoll zum Schlüsselaustausch über das Internet
- IPSec – internet protocol secure (10)
  Protokoll zur gesicherten Übertragung im Internet. Bestandteil von IPv6, aber auch mit IPv4 einsetzbar.
- ISAKMP – internet security association and key management protocol (28)
  Protokoll zum Schlüsselaustausch über das Internet
- ISO/OSI - international standards organisation / open systems interconnections (17)
  geschichteter Aufbau des Netzwerkssystems in TCP/IP-Netzwerken
- KLIPS – kernel IP security (30)
  Kernelmodul, welches die Ver- und Entschlüsslung des Tunnels besorgt.
- LAN – local area network (2)
  ein lokales Netzwerk mit Arbeitsplatzrechnern und Servern
- LDAP – lightweight directory access protocol (42)
  Datenhaltungsmodell, mit der Möglichkeit Hierarchien zu modellieren
- L2TP – layer 2 tunneling protocol (14)
  Protokoll zur gesicherten Übertragung im Internet. Bevorzugt in reinen Windows-Netzwerken eingesetzt.
- NAT – network adress translation
  ändern der IP Adressen von IP-Paketen, um private Adressen zu

maskieren und mehreren Rechnern den Zugang zum Internet zu ermöglichen

- NFS – network file system (35)
  unter UNIX gebräuchliches Verfahren für den Dateiaustausch über ein Netzwerk
- PAP – password authentification protocol (15)
  Protokoll zur gesicherten Übertragung im Internet. Bevorzugt in reinen Windows-Netzwerken eingesetzt. Unsicher.
- PDC – primary domain controller (40)
  zentrale Stelle in einer Windows-Domäne, die alle Ressourcen verwaltet
- PDF – portable document format (1)
  vektorbasiertes Dokumentenaustauschformat
- PERL – practical extraction and reporting language (46)
  vielseitig verwendbare Programmiersprache
- RAID – redundant array of inexpensive disks (38)
  hier: Festplattenverbund, der die Daten ausfallsicher bereithält
- RFC – request for comment (34)
  Dokument, dass einen Internet Standard vorschlägt
- RSA - Rivest, Shamir, Adleman (33)
  nach den Entwicklern benannter, weitverbreiteter Verschlüsslungsalgorithmus
- SA – security association (26)
  logische Verbindung zwischen den Tunnelenden, die nach einem erfolgreichen Handshake erstellt wird.
- SMB – server message block (8)
  Protokoll für Benutzermanagement, Dateiaustausch und Ressourcenfreigabe von Microsoft
- SMS – short message service (44)
  Verfahren zur Übermittlung von Kurzmitteilungen an Mobiltelefone
- SNAT – source NAT (29)
  Änderung der Quelladresse der IP-Pakete während des NAT-Vorgangs

- SSH – secure shell (4)
  dem Telnet ähnliche, aber verschlüsselte Form der remote-Bedienung eines Rechners
- SSL – secure socket layer (37)
  Verschlüsslungsart, verbreitet bei gesicherter Übertragung von Webseiten
- TCP/IP – transmission control protocol / internet protocol (18)
  Übertragungsstandard im Internet, mit „Empfangsbestätigung“
- UDP – user datagram protocol (32)
  relativ einfacher Übertragungsstandard im Internet
- VoIP – voice over IP (9)
  Führen von Telefongesprächen u. ä. über das Internet
- VPN – virtual private netzwork (5)
  ein gesicherter Tunnel über ein nicht vertrauenswürdiges Netzwerk, dass mehrere LANs verbindet.
- VNC – virtual network computing (39)
  Möglichkeit Rechner mit grafischer Benutzeroberfläche remote zu bedienen
- YAPS – yet another pager software (45)
  Programm zur Übermittlung von SMS von einem Linux Rechner aus

6.Literaturverzeichnis

Bei der Erstellung dieses Berichts und im Laufe des Praktikums wurden folgende Informationsquellen benutzt.

6.1.Print-Medien

- unbekannter Author - Virtuelle private Netzwerke (VPN): Eine Übersicht
  Redmond: Microsoft Press, 1999

- Bachfeld, Daniel - Sicheres Netz im Netz
  Hannover: Heise Verlag, 2001
  aus c't 17/2001, Seite 164ff.
- Banning, Jens - LDAP unter Linux
  München: Addison-Wesley, 2001
  ISBN: 3-8273-1813-0
- Dr. Borkner-Delcarlo, Olaf - Das Samba Buch
  2. Auflage, Nürnberg: SuSE, 2000
  ISBN: 3-934678-22-X
- Eckstein, Robert, Collier-Brown, David und Kelly, Peter
  Using Samba
  Cambridge: O'Reilly & Associates, 2000
  ISBN: 1-56592-449-5
- Gärtner, Olivier und Ünal, Berkant – Mit sicherem Tunnel durchs Internet
  Diplomarbeit an der Züricher Hochschule Winterthur, 1999
- Lendecke, Volker - Zentrale Anbindung – Linux PDC mit Samba und OpenLDAP
  Hannover: Heise Verlag, 2002
  aus iX 4/2002, Seite 148ff.
- Michela, Franco und Palme, Markus - Active Directory
  Microsoft Press, 2000
  ISBN: 3-86-063-488-7
- Siever, Ellen - Linux in a Nutshell
  Übersetzung und deutsche Bearbeitung Matthias Kalle Dalheimer
  2. Auflage, Köln: O'Reilly Verlag, 1999
  ISBN: 3-89721-116-5
- Dr. Steffen, Andreas - Eigener Schlüsseldienst
  Hannover: Heise Verlag, 2002
  aus c't 5/2002, Seite 220ff.

6.2.Online-Medien

- diverse Autoren - diverse RFCs über IPsec und die begleitenden Protokolle
  siehe Verweise auf
  http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/rfc.html
- diverse Autoren - FreeS/WAN User mailinglist
  diverse Beiträge
  http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/mail.html
- unbekannter Autor - FreeS/WAN Documentation
  Version für FreeS/WAN 1.95 vom 3. Mai 2002
  http://www.freeswan.org/freeswan_trees/freeswan-1.95/doc/index.html
- unbekannter Autor - Installation and Configuration Guide
  Version für X.509 FreeS/WAN Patch 0.9.9 vom 10. April 2002
  http://www.strongsec.com/freeswan/install.htm
- unbekannter Autor - Linux Bridge+Firewall Mini-HOWTO
  Version 1.2.0 vom 9. April 2002
  http://www.linuxdoc.org/HOWTO/mini/Bridge+Firewall-1.html
- Carlson, Nate - Installing FreeS/WAN and X.509 Patches
  Version vom 7. Juni 2002
  http://www.natecarlson.com/include/showpage.php?cat=linux&page=ipsec-x509
- Galstad, Ethan - NetSaint Documentation
  Version vom 16. Januar 2002
  http://netsaint.org/download/contrib/docs/netsaint-0.0.7.pdf
- Müller, Marcus - Windows 2000 / Windows XP - Freeswan VPN
  Version 2.1.4 vom 30. April 2002
  http://vpn.ebootis.de/
- Russel, Rusty - Linux 2.4 NAT HOWTO
  Revision 1.15 vom 27. Juli 2001
  http://netfilter.samba.org/unreliable-guides/NAT-HOWTO/index.html

- Universität Hamburg, DFN-PCA - Das OpenSSL Handbuch
  Version 2.03 vom 18. April 2000
  ftp://ftp.cert.dfn.de/pub/pca/docs/DFN-PCA/handbuch/ossl095-hb.pdf