F A C H H O C H S C H U L E W E D E L

S E M I N A R A R B E I T

in der Fachrichtung
Wirtschaftsingenieurwesen
SoSe 2017

Seminar: Informatik - Technik

Thema:

Anonymität im Netz - VPN (Virtual Private Network)

Eingereicht von:	Michael Constantin Cremer (Matrikelnr.: Wing100535) Beim Gesundbrunnen Nr. 5 20537 Hamburg E-Mail: wing100535@fh-wedel.de
Erarbeitet im:	8. Semester
Abgegeben am:	22.06.2017
Betreuer:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 143 22880 Wedel Tel. (0 41 03) 8048 - 24

Inhaltsverzeichnis

1. Anonymität im Netz - Einleitung

1.1 Erkenntnisinteresse

Im September 2007 veröffentlichte die Zeitschrift „*Profil*“ unter dem provokanten Titel www.anonymitaet.ade einen Artikel, der sich eingehend mit der Problematik der unbedachten Selbstveröffentlichung in Social Networks und der damit verbundenen Freigabe persönlicher Daten beschäftigte (vgl. Fink et al. 2007: 110ff). Damals waren beim Social Network „Facebook“ etwa 50 Millionen User registriert. Trotz der Gefahren bezüglich der eigenen Privatsphäre, registrierten sich seitdem immer mehr Internetuser in Online-Netzwerken. Heute, zehn Jahre später, zählt Facebook bereits 1,94 Milliarden Mitglieder und ist damit das erfolgreichste Social Network weltweit.

Internet-Experten alarmieren zunehmend über diese sehr freizügige Bekanntgabe der eigenen Person im Internet. Vor allem in Online-Netzwerken verzichten die Nutzer durch das Erstellen eines eigenen Profils und durch das Hochladen von Fotos und Videos immer mehr auf die Wahrung ihrer Anonymität und Privatsphäre. Diesbezüglich schreibt der ORF am 27.2 2009 unter dem Titel „In der Netzwerkfalle“: „ Eine 16-jährige verliert ihren Job, weil sie auf Facebook den Büroalltag als „langweilig“ bezeichnet hat, ein Politiker kommt wegen kompromittierender Facebook-Fotos in Bedrängnis; Ehepartner erfahren via Facebook von der Scheidung: Rund um den immer populärer werdenden Social-Networking-Giganten häufen sich derzeit die Schauermeldungen. Facebook ist endgültig zum Mainstream geworden – und mit ihm eine neue Art des Cyber-Exhibitionismus, die unvorsichtige User Kopf und Kragen kosten.“

Dass der Internetnutzer generell im Netz seine Spuren hinterlässt, indem er Online-Käufe tätigt, Suchanfragen stellt oder sich einfach nur durch das Netz klickt, stellt an sich schon ein ernst zu nehmendes Problem dar. Jeder virtuelle Schritt wird von den Betreibern der besuchten Seiten gespeichert und bei Bedarf beispielsweise für kommerzielle Zwecke genutzt. Jedoch scheint sich in Fachkreisen seit dem Boom der Social Networks im Internet berechtigterweise die Frage einer möglichen Verschiebung der Bedeutung der Begriffe Anonymität beziehungsweise Privatsphäre zu formulieren.

1.2 Forschungsstand

Für den deutschsprachigen Raum konnten zwei Studien gefunden werden, die sich unter anderem mit dem Social Network Facebook beschäftigen. So fokussiert sich die Studie des Fraunhofer Instituts mit dem Titel *Privatsphärenschutz* in Soziale-Netzwerke-Plattformen auf die technischen Aspekte, die zum Schutz der Privatsphäre von Seiten der untersuchten Social Networks geboten werden. In Bezug auf Facebook zeigen die Ergebnisse, dass Facebook die umfangreichsten Zugriffkontrollen für seine Mitglieder bietet und dass bis auf einige Ausnahmen alle Daten nach Außen geschützt sind (vgl. Studie des Fraunhofer Instituts 2008: 80)

Einen anderen Zugang hat die Arbeit von Fuchs (2009), der sich auf das Wissen der Facebook-Mitglieder über die Verwendung ihrer Daten konzentriert hat. Die Untersuchung hat gezeigt, dass nur etwa ein Drittel der befragten Facebook-Nutzer sehr gut bis gut über die Verwendung ihrer Daten informiert waren (vgl. Fuchs 2009:80).

Darüberhinaus existieren bereits diverse Arbeiten, die sich allgemein mit dem Thema *Social Networks* beschäftigen und deren Erkenntnisse in die vorliegende Arbeit eingeflossen sind.

2. Zentrale Begriffe

2.1 Anonymität

Im Hinblick auf die Geschichte der Philosophie ist „Anonymität“ kein unpopulärer Begriff. Es stammt aus dem Altgriechischen bzw. Spätlateinischen und heißt in anderen Worten: „Ungenannt, ohne Namen oder namenlos“.
Es werden also jegliche Personen als „anonym“ bezeichnet, die Ihren Namen nicht bekanntgeben.
Um „Anonymität“ im Alltag nutzen zu können, sind mindestens zwei „Parteien“ notwendig, schließlich eine Partei, die ihre eigene Identität nicht ausgibt und eine andere Partei, der gegenüber diese Identität geheim gehalten wird.
Demnach ist es nicht korrekt, nur nicht zu wissen, dass eine Person existiert, sondern es ist auch zwingend zu wissen, dass eine Person existiert, ohne die Kenntnis zu haben, welche Identität sich hinter dieser Person verbirgt.

2.1.1 Definition

Kurz und prägnant definiert die Brockhaus-Enzyklopädie (2006: 100) den Begriff Anonymität als „*Unbekanntsein des Namens, Namenlosigkeit, Nichtbekanntsein, Nichtgenanntsein*.“

Eine umfangreichere Definition ist in Wikipedia, der Online-Enzyklopädie, zu finden: „*Anonymität (von altgriechisch ἀνώνυμος anónymos ‚ohne Namen‘) ist die Geheimhaltung der Identität einer Person, einer Gruppe, einer Institution oder einer agierenden Struktur auch können sich zum Beispiel Computersysteme anonym oder offen erkennbar an einem anderen System anmelden beziehungsweise einloggen.“*

Ausführlicher beschäftigt sich Denninger (2003: 41) mit dem Begriff Anonymität. Er geht von dem Wort an-onymus aus, welches für „der Namen-lose“ steht, und gleichzusetzen ist mit der „Un-Bekannte“, also „einer (oder etwas), der (das) zwar einen Namen hat, den man aber nicht kennt.“
Er unterscheidet schließlich weit in *historische, institutionelle und gewillkürte* Anonymität. (vgl. Denninger 2003: 44).

2.1.2 Historische Entwicklung von Anonymität

Eine mögliche Erklärung, warum sich bisher so wenige Autoren mit einer exakten Begriffsdefinition beschäftigt haben, ist, dass der Begriff *Anonymität* kein etablierter philosophischer Begriff ist und in der philosophischen und juridischen Begriffsgeschichte erst seit etwa hundert Jahren eine nennenswerte Rolle spielt (vgl. Rössler 2003: 28). Verwendet wurde der Begriff davor nur für den namenlosen, anonymen Schriftsteller oder Künstler in Zusammenhang mit literarischen oder künstlerischen Erzeugnissen. Solche Formen anonymer Sozialbeziehungen, die die Menschen heutzutage in modernen Großstädten täglich leben, gab es in vormodernen Zeiten nicht. In einer mittelalterlichen Stadt konnte jeder Bürger, auch wenn sein Name nicht bekannt war, aufgrund seiner Kleidung zumindest einem eindeutigen Status zugeordnet werden (vgl. Rost 2003: 64). Anonymität, also die Namenlosigkeit oder die Unbekanntheit eines Menschen, war lange Zeit eher negativ behaftet und wurde ausschließlich in einem pejorativen Sinn verwendet (vgl. Rössler 2003: 28).

2.2 Privatsphäre

Das Recht auf Privatsphäre ist wie das Recht auf Anonymität essentiell für persönliche Freiheit und Autonomie. Ohne persönliche Freiheit könnte man keine autonome Person sein, die die Art und Weise des Lebens, welches sie führen will, selbst bestimmt, sofern dies mit der Freiheit von anderen verträglich ist (vgl. Pauer-Studer 2003: 20). Privatsphäre ist der Raum, in dem sich eine Person zurückziehen kann und vor den Blicken der Öffentlichkeit geschützt ist.

Privatsphäre ist der zweite der beiden zentralen Begriffe dieser Arbeit. Bei der Durchsicht der Fachliteratur hat sich gezeigt, dass neben dem Begriff *Privatsphäre* oft der Terminus *Privatheit* verwendet wird, der vor allem in Zusammenhang mit gesetzlichen Bestimmungen und rechtlichen Belangen des Datenschutzes genannt wird. Der Begriff *Privatheit* ist im alltäglichen deutschen Sprachgebrauch jedoch eher unüblich und wird entsprechend selten verwendet; die Begriffe *Privatsphäre*, *Intimsphäre* oder *Privatangelegenheit* sind dagegen gebräuchlicher (vgl. Sanhüter 2004: 23). Da keine Literaturhinweise gefunden werden konnten, die einen Unterschied zwischen Privatsphäre und Privatheit belegen, werden die beiden Begriff in der vorliegenden Arbeit synonym verwendet.

2.2.1 Definition

Als erstes kann *Westins* Konzept (1967) genannt werden, dass auf vier Stadien von Privatsphäre basiert (vgl. Westin 1967 zit. nach Margulis 2003: 412): Erstens ist Privatsphäre nur dann gegeben, wenn eine Person von anderen nicht überwacht wird (*Einsamkeit*), zweitens muss jeder Mensch das Recht haben, mit bestimmten Personen, beispielweise mit der Familie oder mit Freunden, eine innige Beziehung haben zu können (*Intimität*), drittens muss jeder die Möglichkeit haben, sich ohne eine Identifikationspflicht auf öffentlichen Plätzen bewegen zu können (*Anonymität*) und viertens ist die Kontrolle persönlicher Informationen ein wesentlicher Aspekt für das Privatheitskonzept (*Reserviertheit*).

2.2.2 Historische Entwicklung von Privatsphäre

Die Entstehung der Privatsphäre lässt sich bis in die Antike zurückverfolgen. Schon bei den Griechen und Römern wurde zwischen einer öffentlichen und einer privaten Sphäre unterschieden. Das private Haus war das Gegenstück zum politisch-öffentlichen Marktplatz (vgl. Schaar 2007: 15). Der Begriff der Privatheit lässt sich aus dem Lateinischen ableiten. So bezeichnete der Begriff *privatus* den Bürger, der sich nicht politisch betätigte. Der Ausdruck *privat* wird erstmal im 16. Jahrhundert verwendet und stand für Sachverhalte oder Personen, die für sich und unabhängig sind (vgl. Schaar 2007: 16). Seit dem Mittelalter ist das Konzept der Privatsphäre einem ständigen Wandel unterworfen. Damals waren der Ort der Arbeit und
16
der Familie räumlich meist nicht getrennt, alles spielte sich in den gleichen Räumlichkeiten des Hauses ab (vgl. Sanhüter 2004: 27). Dieses Privatheitskonzept ließ sich auch auf die ganze Dorfgemeinschaft umlegen, denn jeder einzelne war für die Gemeinschaft transparent. Eine Trennung von Privatem und Öffentlichem war nur zwischen dem Staat und der Gesellschaft gegeben.

Der Begriff *Privatsphäre*, wie wir ihn heute verwenden, hat sich erst parallel mit der Aufklärung entwickelt, die die Stellung des Bürgertums neu formulierte (vgl. Sanhüter 2004: 27).
Jede Person rückte mehr in den Vordergrund und damit verbunden auch die Interessen jedes einzelnen. Die Privatsphäre spielte von nun an eine wesentliche Rolle in der bürgerlichen Gesellschaft und hatte folgende Funktion: *„In einer von individuellen Entscheidungen geprägten Gesellschaft muss die Privatsphäre gegen Einblicke Dritter geschützte werden, damit das individuelle öffentliche Handeln überhaupt möglich ist“* (Schaar 2007: 16).

2.3 Anonymität und Privatsphäre im Internetzeitalter

Der Wunsch nach Mobilität, ständiger Erreichbarkeit und der Möglichkeit, allerorts auf seine Daten zugreifen zu können, hat für den Menschen zur Folge, dass er ein Stück seiner Anonymität und Privatsphäre aufgeben muss. Haben die vorigen Generationen noch für ein Recht auf diese Grundpfeiler des autonomen, freien Lebens gekämpft, so scheint die sogenannte Informationsgesellschaft freiwillig auf diese Rechte zu verzichten. Speziell die Technologie des Internets hält für den unwissenden Internetnutzer viele mögliche Gefahren für seine Anonymität und Privatsphäre bereit. Jeder Einstieg in das Netz hinterlässt Spuren und Daten, die gespeichert und beispielsweise für kommerzielle Zwecke weiterverwendet werden.
Treffend zitiert *Siegetsleitner* (2001: 17) das *Privacy Rights Clearinghouse5*: *„The information superhighway can bring many benefits to our daily lives. Unfortunately, it may create many new threats to our personal privacy as well. Unless you know the privacy ‘rules of the road’, your online activity may lead to significant privacy problems.”*

3. Internet und Internetnutzung

3.1 Zum Begriff „Internet“

Das Internet beschreibt sich als weltweit umspannendes Netz, welches autonome Computernetzwerke, durch einer gemeinsamen Sprache (TCIP/IP-Protokolle), kommunizieren lässt. (vgl. Sanhüter 2004: 34).

Was einst allein zur Datenübertragung von zimmergroßen Computern geschaffen wurde, hat heute das Potenzial gewaltigen Fortschritt zu bewirken und furchtbaren Schaden anzurichten.
Das Internet umfasst ein endlos vielfältiges Betätigungsfeld der menschlichen Kreativität und befindet sich gleichzeitig in einem konstanten Veränderungsprozess, der mit jeder Sekunde größer und komplexer wird.

Bevor die Geburtsstunde des Internets begann, wurde im Jahr 1958 in den USA eine Gruppe names „ARPA“ (Advanced Research Projects Agency) gegründet.
Die „ARPA“ diente größtenteils als *„Investor und Inkubator für wissenschaftliche Projekte bei Universitäten und Forschungseinrichtungen, deren Ergebnisse bei einer eventuellen Eignung dem US-Militär zu überlassen waren. Alternativ konnten die Ergebnisse bei Nichteignung privatwirtschaftlich von den entsprechenden Universitäten beziehungsweise Forschungseinrichtungen genutzt werden.“*
Bereits im Jahr 1969 fing die Vernetzung der ARPA-Forschungseinrichtungen an, zudem waren ab 1971 schon mehr als 30 verschieden Computerzentren landesweit verknüpft.
Seit der Entwicklung der „TCP/IP“ (1977) als Kommunikationsmittel von verschiedenen Computernetzwerken, machte sich das Internet bekannt als das „Netz der Netze“.

3.2 Anonym im Internet

Alle Internet-„Bürger“ werden zukünftig zunehmend Schwierigkeiten haben, anonym zu bleiben. Vor dem Zeitalter der Computer reichte es zumeist schon aus, nicht aufzufallen oder so zu handeln, wie alle anderen, um unter dem Radar zu bleiben.
Doch in der Welt der Computer sind mittlerweile zahlreiche Methoden entstanden, um die „User“ zu identifizieren:

- IP-Adressen. Alle Geräte, die mit dem Internet verbunden sind, können anhand ihrer IP-Adresse identifiziert werden. Diese Adresse wird vom Provider hergestellt, sodass das Konto und der Standort des verwendeten Systems durch eine IP-Adresse ermittelt werden kann.
- Browsercookies. Webserver, die Dienste anbieten, hinterlassen auf ihrem System „Cookies“ mit identifizierenden Informationen, wenn man auf den Dienst zugreift.
- Systemprofile. Informationen über Ihr System, z.B. den verwendeten Browser, das Betriebssystem, die installierten Schriftarten, Plug-Ins und jegliche Software können dazu gebracht werden, ein Profil ihres Systems zu erstellen.

3.3 Das Web 2.0

Im Jahr 2008 in einer Folge des Video-Podcasts „Elektrischen Reporters“ berichtet der amerikanische Medienprofessor Clay Shirky: *„The assumption that things can be linked, that they can be found easily wherever they are, that they can be accessed easily, and that they can be shared easily, these are all metaphors that are moving from the (...) electronic layer up into the social layer. They are just expectations now that people have of their lifes with one another. People are rebuilding their social lifes around those kinds of assumptions.”*
Das Internet ist in den letzten Jahren rasant mit unserer Gesellschaft zusammengewachsen. Das neue Netz sorgt nicht nur für Information, sondern auch für Menschen, welche sowohl untereinander als auch miteinander verknüpft sind und sich füreinander auffindbar machen. Demnach stehen technische Innovationen nicht allein in der Kritik, hier geht es auch ausschließlich um soziale Prozesse. Somit stellt sich auch die Frage, wie der Mensch das Internet in den Alltag einbindet.
Der Zusatz „2.0“ bezieht sich auf den starken Wandel des Internets und sollte das Gefühl von Veränderungen aufbringen. Im Oktober 2004 organisierte der amerikanische Verleger Tim O’Reilly die erste „Web 2.0 Conference“, die sich an „leading figures and companies driving innovation in the Internet economy“ wandte.
Auf dem ersten Blick scheint das Web 2.0 ein großer Hoffnungsträger zu sein. Das Ziel war die Zusammenarbeit zwischen Menschen oder die Bekanntgebung an Inhalten zu verbessern.
Zudem gibt es diverse Namen für das neue Web: „Web 2.0, das lebendige Web, das Hypernet, das Mitmach-Web, das Schreib-Lese-Web.“
Das Web 2.0 orientierte sich bei der Entwicklung an verschiedene große Bereich:

- Websites können durch kostenlosen Inhalt kostengünstig gefüllt werden.
- Sowohl für den aktiven wie auch den passiven Internetnutzer entsteht ein Mehrwert, denn der aktive Nutzer kann sich und seine Gedanken einem großen Rezipientenkreis präsentieren und für den passiven ist es von Interesse zu erfahren, was andere denken und schreiben.
- Das Image eines Medienprodukts kann durch die Möglichkeit von Bewertungen und Ratings verbessert werden.
- User Generated Plattformen sind gefüllt mit persönlichen Angaben und Informationen und sind daher für die Marktforschung und Werbewirtschaft von großem Interesse geworden.

3.3.1 Das Web als Service-Plalttform

Aufgrund vieler Funktionen des Internets, sowie die Verwaltung von alltäglichen Aufgaben, können beispielsweise Termine online koordiniert werden oder Text- und Bildbearbeitung über Online-Programme durchgeführt werden. Dadurch erschafft sich der Internetuser bestimmte Vorteile:

- Programme müssen nicht mehr auf lokalen Rechner installiert und gepflegt werden.
- Sämtliche Dienste können unabhängig von einem Betriebssystem genutzt werden.
- Persönliche Daten, wie Termine, Fotos, Texte oder Lesezeichen sind jederzeit und überall verfügbar.
- Eine kooperative und kollaborative Arbeitsweise wird somit möglich.

3.4 Internet – Revolution für sich

Datiert sind Hunderte Millionen von Menschen, die in einer virtuellen Welt digitale Inhalte produzieren und konsumieren, wo Gesetze kaum an Anspruch finden. Gesehen wird das Ganze als neue Perspektive der freien Meinungsäußerung und des Informationsaustauschs.
Es bietet ein breites Spektrum an Informationen, welches uns nicht nur an Dingen verknüpft, wie unser Job, unsere Beziehung oder auch unsere Traumreisen. Zum Anderen ermöglicht es auch Menschen „Onlinebetrug, Mobbing, Aufrufe zu Hass und Gewalt oder Terror-Chatrooms“ auszuüben.
Das Internet spiegelt eine unregulierte Onlinewelt dar.
Nichtsdestotrotz wird es weiterwachsen und zukünftig gewisse Aspekte unseres Lebens im Alltag ändern: Unsere Identität, unsere Beziehungen und unsere Sicherheit.
Bis jetzt habe es noch nie in der Geschichte der Menschheit eine solche Auswirkung einer Revolution gegeben, die es weltweit an Einfluss geschafft hat.

4. Ein Blick in die Zukunft

4.1 Vernetzung der Welt

In den nächsten Zehn jahren zählt man mehr virtuelle als physische Mitbewohner auf der Erde. Grund dafür ist das Erschaffen mehrerer Online-Identitäten, womit die Menschen sich zu aktiven Gemeinschaften mit ihren gemeinsamen Interessen zusammenschließen.
Diese Netzwerke führen zu einer gewaltigen Ansammlung von Datenmengen. Man redet von einer Datenrevolution, die uns enorme Fortschritte vorbereitet aber auch die Kontrolle über unsere privaten Daten in der virtuellen Welt raubt.
Obwohl unsere Online-Identitäten heute zwar einen gewissen Einfluss auf unser Leben haben, spielen sie weiterhin eher eine zweitrangige Rolle.
Jedoch lassen sich unsere Online-Identitäten Jahr für Jahr mehr durch unsere virtuellen Aktivitäten und Beziehungen identifizieren.
Hinzu kommt noch, dass wir unsere Information heutzutage zunehmend in „Clouds“ speichern. (In anderen Worten auch als *Cloud Computing Software* bezeichnet. Die Speicherung von Dokumenten

und anderen Inhalten „in der Wolke“ bedeutet, dass Daten nicht mehr auf dem eigenen Rechner abgelegt werden, sondern auf einem entfernten Server, auf den andere Netzwerke Zugriff haben.)

4.2 Vertrauen ihrer Nutzer gewinnen

In diesem Abschnitt wird die Frage näher erläutet, was die Vernetzung für Bürger in der Zukunft bedeutet und welche Folgen sie für Gesellschaften haben wird.

Die Technologieunternehmen sind durch diese Umstellung zunehmend mit zwei Dingen beschäftigt:

- Privatsphäre und
- Datenschutz ihrer Kunde

Dadurch ist die Technologie besonders fokusiert nach möglichen Lösungen für die Datensicherung, zum Beispiel durch doppelte Identitfizierung. Hier müssen Sie zwei der folgenden drei Dinge vorlegen: etwas, das Sie wissen (Passwort), etwas, das Sie haben (zum Beispiel ein Gerät), oder etwas, was Sie sind (Fingerabdruck). Die Idee der Informatiker ist die kodierung so zu gestalten, dass sie nur von einem Nutzer gelesen und verwendet werden können, der über den nötigen Schlüssel verfügt.
Einigen Staaten könnte es zu gefährlich werden, Tausende anonyme oder verborgene Personen zu haben. Sie werden wissen wollen, wer hinter jedem Nutzer-konto steckt und werden eine staatliche Verifizierung anforden, um auch in der virtuellen Welt Kontrolle ausüben zu können.
Man kann sich vorstellen, dass alle Online-Aktivitäten – Facebook, Twitter, Skype, Google+, Netflix – sich zu Einem Profil erstellen lassen. Wir stehen vor einem Wandel von einer Identität, die später riesige Auswirkungen für Bürger, Staaten und Unternehmen haben wird.

5. VPN – Virtual Private Networking

5.1 Einleitung

Von den Unternehmen und deren Mitarbeiter wird in der heutigen Zeit immer mehr Flexibilität erwartet. Es werden nach Außendienstler gesucht. Die Erfüllung der Aufgabe von Außendienstlern ist jedoch nur effizient, wenn sich diese von unterwegs schnell und kostengünstig an das Firmennetzwerk anbinden können. Gefordert wird dabei eine gut funktionierende interne Kommunikation. Briefe und Faxe sind mittlerweile traditionelle Verfahren zum Datenaustausch, die zu zeitaufwendig und verwaltungsintensic sind. Sie werden den neuen Anforderungen nicht mehr mithalten können.

Seitdem der erste graphische Browser Mosaic 1993 entwickelt wurde, stiegen die Benutzer- und Anbieterzahlen im Internet gigantisch an.

Zudem entwickelte sich ein erhöhtes Sicherheitsbedürfnis für die vernetzte Informationsverarbeitung. Es wuchs der Wunsch nach kontrollierten Netzbereichen, die ausschließlich nach Vorstellungen des nutzenden Unternehmens zugänglich sind und in der Regel nur durch Unternehmenszugehörige selbst genutzt werden können.

5.1.1 Problemstellung

Ein „Virtual Private Network“ ist eine Methode zur Vernetzung von Standorten und erfüllt das erhöhte Sicherheitsbedürfnis. Es nutzt das Internet als Kommunikationsinfrastruktur. In der Praxis kommen auch weitere Kommunikationsplattformen zum Einsatz.

Da ein VPN über das Internet kommuniziert, stellt sich die Frage, ob es sich hier um ein sicheres Netzwerk handelt.

5.2 Was ist ein VPN ?

Der Begriff VPN läßt viel Spielraum für Interpretationen. Daher existiert für diese Bezeichnung mehrere Definitionen.

„Ein VPN ist eine Kommunikationsumgebung bei der Verbindungen unter Kommunikationspartnern nur dann erlaubt sind, wenn diese zu einer bestimmten Gruppe gehören. Ein VPN wird unter Nutzung einer allgemeinen zugänglichen Kommunikationsinfrastruktur aufgebaut, die ihre Dienste nicht nur einer exklusiven Benutzergruppe zur Verfügung stellt“ (Ferguson, Huston, „Whats is a VPN?“, in „ The Internet Protocol Journal“, Volume 1, Number 1).

Die Filialen eines Unternehmens wurde noch zu Beginn der 90er Jahre üblicherweise über Weitverkehrsstrecken verbunden, die entweder permanent oder nach Bedarf aufgebaut wurden. Dem Unternehmen standen diese Leitungen exklusiv zur Verfügung.

Ein VPN ermöglicht Verbindungen zwischen Unternehmensstandorten, bei denen lediglich der Weg der Daten in der Kommunikationsplattform hinterlegt ist. Das heißt, dass erst, wenn eine Datenübertragung ansteht, erforderliche Bandbreiten zugewiesen werden.

5.2.1 Begriffserklärung

Hinter der Abkürzung VPN verbirgt sich Virtual Private Network, ein virtuelles privates Netzwerk. Die Bezeichnung „virtual“ ist durch die Architektur begründet. Es handelt sich nicht um ein physisch separates Netz, sondern um eine übergeordnete Struktur, die sich quasi auf das öffentliche Netz aufsetzt.

Durch die Nutzung des Internets als Übertragungsmedium besteht die Gefahr, dass Dritte die übertragenen Daten mitlesen oder sogar verändern können. Um dies zu verhindern und bei einem VPN dem „P“ nämlich „privat“, gerecht zu werden, sind bestimmte Sicherheitsmaßnahmen eine Voraussetzung. Weiteres dazu folgt an anderer Stelle in dieser Arbeit.

„Network“ steht in diesem Zusammenhang für eine Gruppe von Computern, die über diverse Protokolle miteinander kommunizieren.

5.3 Aufbau eines VPN (Tunnelverfahren)

Tunneling ist ein Konzept, mit dem beliebige Datenpakete über ein Transitnetz sicher weitergeleitet werden können. Solch ein Tunnel wird, mit dem Internet als Übertragungsmedium zwischen dem Client und Server aufgebaut. Dieser bewirkt, dass die transportierten Datenpakete den Tunnel nicht verlassen können und fremde Datenpakete nicht in den Tunnel eindringen können.

Die Privatsphäre der Kommunikation bleibt gewahrt indem die virtuellen Verbindungen zwischen den Unternehmensstandorten innerhalb einer geschlossen Benutzergruppe als Closed User Group (CUG)

verwaltet werden. Die Gesamtheit aller IP-Tunnel für eine solche geschlossen Benutzergruppe stellt ein virtuelles privates Netz für diese Gruppe dar.

5.3.1 Layer-2-Tunnelprotokolle

Das Grundprinzip aller Tunnel-Protokolle ist das Verpacken der Anwendungspakete in die Datenpakete des Transportsprotokolls. Das Originalpaket wird als Nutzlast bzw „Payload“ eines anderen Protokolls verschickt. Dafür wird dem Originalpaket ein zusätzlicher Protokollkopf vorangestellt. Zum Versenden wird dieses Paket durch einen Router in einen PPP-Rahmen verpackt. Es fungiert nun praktisch wie ein Container und kann über jedes IP-Netz transportiert werden, da sein Inhalt für die Übertragungssysteme nicht von Bedeutung ist. Im Zielrechner wird der Header bzw. Tunnel- Header entfernt und das Originalpaket ist wiederhergestellt. Diesen Vorgan bezeichnet man als Decapsulation.

Hier ist kurz der General Routing Encapsulation (GRE) Tunnel zu erwähnen. 1994 wurde mit dem GRE-Protokoll eine erste Standardisierung für Tunnel-Verfahren vorgenommen. Nach diesem Standard sind andere Tunneling-Protokolle, wie z.B. PPTP, aufgebaut worden.
Ein GRE-Paket wird in drei Abschnitten unterschieden. In den GRE-Header (Protokollkopf), in den eigentlichen Netzwerk-Prokollkopf und in die Nutzlast. Nahezu jedes beliebe Paket aus höheren Protokollschichten kann als Nutzlast eingesetzt werden.

Im GRE-Header werden Informationen über die verwendeten Tunnel- und Verschlüsserlungsalgorithmen hinterlegt. Im Netzwerk- Protokollkopf wird hingegen das Tunnelziel gespeichert.

5.3.2 Point-to-Point-Tunnelprotokolle

Das Point-to-Point-Tunneling Protcol findet häufig Anwendung, da es in den Microsoft Betriebssystemen Windows NT, Windows 98 und Windows 95 implementiert worden ist. PPTP stellt eine Erweiterung des bereits erwähnten Point-to-Point-Protokolls (PPP) dar. Erzielt wird dies, indem PPP mit einem GRE-Header gekapselt und mit einem zusätzlichen Tunnel-IP-Header versehen wird. Durch die Einbindung des GRE-Headers bietet PPTP auch die Möglichkeit, andere Protokolle zu verwenden, wie z.B. IPX oder NETBUI. Ohne den GRE-Header ist PPTP an das Internet-Protokoll gebunden..

Ein Vorteil von PPTP ist die starke Authentifizierung sowie Verschlüsselung der übertragenen Nutzdaten. Die Verschlüsselung endet nicht wie bei einer Standard PPP-Verbindung beim Einwahlpunkt des International Service Providers, sondern erstreckt sich bis zum PPTP-Server.

Bevor eine PPP-Verbindung zwischen dem Anfangs- und Endpunkt des Tunnels aufgebaut werden kann, muss eine virtuelle TCP-Verbindung aufgebaut werden. Diese Verbindung fungiert als Kontrollverbindung des Tunnels.

Des Weiteren ist für ein PPTP-Tunnelaufbau eine Anforderung vom Endgerät erforderlich. Bei einer Verbindung kann lediglich nur ein Tunnel aufgebaut werden, der eine Kontrollverbindung besitzt.

PPTP ermöglicht einen Außendienstmitarbeiter über ein öffentliches Netz den Zugriff in das firmeneigene Intranet. Einerseits kann diese Verbindung über eine nuterinitiierte dynamischen Dial-In kann der Nutzer neben dem Zugangsserver des Unternehmens noch beliebig viele andere Adressen im Internet ansteuern.

5.3.3 IPSec

IPSec ist gemäß IETF ein Sicherheitsstandard, mit dem herstellerübergreifend ein sicherer geschützter Datenaustausch mittels des IP-Protokolls ermöglicht werden kann. Der Normenrahmen von IPSec definiert die Vorgehensweise für die Datenintegrität, die Vertraulichkeit der Inhalte sowie die Verwaltung der kryptografischen Schlüssel.

Mit IPSec ist es möglich, Integrität, Authentizität und Vertraulichkeit bei einer Datenübertragung in einem offenen Netz durchzusetzen. Integrität erhält man, indem die Daten (IP-Pakete) vor Verfälschung während des Transports gesichert werden. In dem Datenpaket wird eine verschlüsselte Prüfsumme aufgenommen, die der Empfänger im Nachhinein verifizieren kann. Authentizität garantiert die Echtheit der IP-Pakete. Druch die Integritätsbedingung wird dies bereits erfüllt. Vertraulichkeit bedeutet, dass kein unerlaubter Dritter die Möglichkeit bekommt, Daten während der Übermittlung zu lesen. Dies wiederum erreicht man durch die Verschlüsselung der Datenpakete mittels kryptographischen Verfahren.

IPSec wird durch zwei weitere Standards ergänzt, welche schlussendlich ein IPSec-Protokoll implementieren. Nämlich einerseits das Simple Key management für Internet Protocol (SKIP) und andererseit das Internet Security Association and Key Management (ISAKMP)

Da IPSec weder die Kommunikationsprotokolle noch die Anwendungsprogramme beeinflusst, wird eine Zusammenarbeit über verschiedene IP-Netze nicht beeinträchtigt. Momentan arbeitet IPSec auf Ipv4, soll aber fester Bestandteil von Ipv6 werden.

Ein zentraler Bestandteil von IPSec ist die Security Association (SA). Bevor zwei Kommunikationspartner mit IPSec abgesicherte Daten austauschen können, müssen einige Sicherheitsvereinbarungen getroffen werden. Darunter zählen z.B. Verschlüsselungsverfahren für die Nutzlast oder die Spezifizierung der zeitlichen Gültigkeit aller Schlüssel. Eine SA-Verbindung ist stets unidirektional. Das heißt, es muss, nachdem eine Verbindung vom Sender zum Empfänger ausgerichtet worden ist, eine weitere SA für den Rücktransport eingerichtet werden.

5.3.4 Transport und Tunnelmodus

Zwei unterschiedliche Arbeits-Modi sind zum Transport der nach IPSec modifizierten IP-Pakete einsetzbar, der Transport-Modus und der Tunnel-Modus. Sie unterscheiden sich beide im Wesentlichen durch den Aufbau der Paketergänzungen und durch ihre Einsatzmöglichkeiten.

IPSec verschlüsselt im Transportmodus nur den Datenteil des zu transportierenden IP-Paketes. Dabei bleibt der Original-IP-Kopf erhalten und ein zusätzlicher IPSec-Kopf wird hinzugefügt. Der Vorteil ist, dass jedem Paket nur wenige Bytes hinzugefügt werden. Ein Nachteil jedoch ist die Möglichkeit für Angreifer, den Datenverkehr im VPN zu analysieren, da die IP-Köpfe nicht modifiziert werden. Da die Daten aber verschlüsselt sind, ist nur feststellbar, welche Stationen wieviel Daten austauschen. Daten werden häufig in privaten Netzen im Transportmodus verschickt.

Im Tunnelmodus hingegen wird das komplette IP-Paket verschlüsselt. Das verschlüsselte Paket wird mit einem neuen IP-Kopf und einem IPSec-Kopf versehen. Verglichen zum Transportmodus ist das IP-Paket hier durch die Modifizierung wesentlich größer geworden. Dagegen ist diese Methode noch sicherer, da Angreifer hier weder die Daten, noch den Datenweg sehen können. Durch die bessere Sicherheit im Tunnelmodus wird dieser Betriebsmodus häufig für die öffentlichen Netze genutzt.

5.3.5 Der AH- Header und der ESP-Header

Wie bereits erwähnt, enthält ein IP-Paket Informationen über die IP-Adresse des Absenders und des Zieles sowie Informationen über die Nutzlast (Payload), die transportiert wird. Um eine Authentifizierung und Verschlüsselung zu erreichen, definiert IPSec zwei weitere Protokollköpfe für IP-Pakete, den Authentification Header (AH) und den Encapsulation Security Payload (ESP).

Der AH-Header kann im Transport- sowie auch im Tunnel-Modus eingesetzt werden. Je nachdem , welche Grad der Absicherung eines IP-Paketes erreicht werden soll, kann der Authentification Header eigenständig oder zusammen mit dem ESP-Header genutzt werden.

Im Gegensatz zum AH-Header ist ein ESP-Header in der Lage, sowohl eine Verschlüsselung als auch eine Authentifizierung zu leisten. Der Encapsulation Security Payload Header Beinhaltet einen Verweis auf den Schlüssel, mit dem die nachfolgenden Daten verschlüsselt werden.

5.4 Ausprägungen eines VPN-Netzes

5.4.1 End-to-End

Bei einer End-to-End Kommunikation, auch Extranet-VPN genannt, wickeln zwei oder mehrere Computer ihre komplette Datenkommunikation verschlüsselt ab. Jeder Computer muss über die öffentlichen Schlüssel aller potentiellen Kommunkationspartner verfügen. Zusätzlich muss jede an der verschlüsselten Kommunikation beteiligte Arbeitsstation mit entsprechender VPN-Software ausgestattet sein. Zugangskontrollmechanismen regeln den beschränkten Zugriff der unterschiedlichen Arbeitsstationen.

Ein Extranet-VPN öffnet das private Netz, wie z.B. das Intranet, auch für externe Personen oder Unternehmen. Diese haben dann Zugriff auf Ressourcen im Untenehmensnetzwerk.

5.4.2 Site-to-Site

Die Site-to-Site Kommunikation wird ebenso als Intranet-VPN bezeichnet, da es als Erweiterung interner LANs angesehen werden kann. Hier tauschen zwei Firmenstandorte ihre Daten über das Internet aus. Am Aufbau eines Intranet-VPNs sind zwei VPN-Gateways/ Firewall-Systeme beteiligt. Nur auf dem Weg zwischen den beiden VPN-Gateways erfolgt eine Verschlüsselung der Daten. Der Weg durch das lokale Netz vom Gateway zum Endgerät bleibt unverschlüsselt. Dadurch benötigen die Endgeräte keine zusätzliche VPN-Clientsoftware.

Da die Gateways auf der Seite des Internets eine öffentliche IP-Adresse haben, können die Standorte für die Endgeräte durchaus private IP-Adressen verwenden.

Aufgaben der Gateways sind also, empfangene IP-Pakete für den Transport über das Internet zu verschlüsseln, in ein neues IP-Paket einzuüacken und zum Partner Gateway zu schicken, das den beschriebenen Vorgang wieder rückgängig macht.

5.4.3 End-to-Site

Bei der End-to-Site Kommunikation handelt sich um eine Mischform der beiden bereits erläuterten Kommunikationsarten. Diese Lösung, welche auch als Remote-Access-Lösung bezeichnet wird, ist besonders für einen Außendienstmitarbeiter interessant, der sich an irgendeinem Ort in der Welt über einen lokalen ISP in sein Firmennetzwerk einwählen möchte.

Die Telefongebühren für die Einwahl ihrer Remote User zu einem Remote Access Server (RAS) können sehr hoch ausfallen, insbesondere wenn dabei über Staatsgrenzen hinweg telefoniert wird. Bei der End-to-Site Kommunikation fallen jeweils nur die Kosten für den lokalen Zugang zum Internet an.

Der Tunnel existiert hier zwischen dem Notebook und dem Gateway. Im Regelfall muss der Rechner des Außendienstmitarbeiters eine IP-Adresse haben, die im Internet auch weitergeleitet werden kann. Zusätzlich ist eine VPN-Software auf dem Notebook erforderlich, da das Internet-Protokoll selbst erst ab Version Ipv6 eine Verschlüsselungsmöglichkeit besitzt.

5.5 VPN und Firewall

5.5.1 VPN Gateway außerhalb der Firewall

Wenn das VPN-Gateway außerhalb der Firewall liegt, dann ist die Abwicklung des gesamten Datenverkehrs über das Internet recht problemlos, da erst das Gateway alle IP-Pakete verschlüsselt.

Bei dieser Architektur bildet die Proxy-Firewall alle internen IP-Adressen des Intranets auf eine öffentliche IP-Adress ab. Wenn nun die gesamten IP-Pakete über das Internet verschlüsselt transportiert werden sollen, ist dies in dieser Anordnung relativ problemlos möglich. Sollen jedoch nur einzelne TCP-Applikationen verschlüsselt werden, so ist beim VPN eine Selektion auf Destination-Port-Ebene notwendig. Allgemein ist die Absicherung einzelner TCP/IP-Anwendungen oder nur bestimmer Rechner in diesem Falle schwer durchführbar.

5.5.2 VPN Gateway innerhalb der Firewall

Im Falle eines VPN-Gateways innerhalb der Firewall nimmt die Proxy-Firewall ihre traditionellen Funktionen wahr und macht die Selektion der VPN-Funktionen für bestimmte IP-Pakete möglich. Da die Datenpakete bereits verschlüsselt und für eine VPN-Verbindung „verpackt“ zur Proxy-Firewall kommen, ist von den früheren Anwendungen nichts mehr sichtbar. Aus diesem Grund muss an der Firewall ein Kanal konfiguriert werden, durch den nur Paketfilterung aber keine Proxy-Funktion stattfindet. Dadruch ist eine zweite öffentlichte IP-Adresse erforderlich, über die alle VPN-verschlüsselten Daten geroutet werden.

6.0 Zusammenfassung und Fazit

VPN werden als kostengünstige Alternative Standleitungen vermarktet. Allgemein gilt jedoch, dass ein Kostenvergleich der Anfangskosten und der laufenden Betriebskosten zu herkömmlichen Diensten unausweichlich ist. Des Weiteren ist eine sorgfältige Produktauswahl und gutes Testen obligatorisch.

Besonders für Außendienstmitarbeiter ist VPN eine lohnende Technologie, da durch die geringen Telefonkosten bei einer End-to-Site-Lösung ein Virtual-Private Network auf jeden Fall rentabel ist.

Trotz der vielen Vorteile von VPN muss erwähnt werden, dass die Technologie momentan noch nicht ausgereift ist. Selbst die im Namen integrierte „Privacy“ ist nur mit hohem Aufwand an Rechenleistung und Bandbreite erreichbar. Mit der Entwicklung Ipv6 wird jedoch ein großer Schritt Richtung „einfacher Sicherheit“ gegangen. Vieles wird in Ipv6 integriert und einfach bedienbar sein, wofür heutzutage noch großer Administrieraufwand nötig ist.

Das Interesse der Firmen ist groß. Das kurbelt die Popularität und Entwicklung der VPNs an und macht VPNs zu keiner Eintagsfliege, sonder zu einem vielversprechenden Netzwerk der Zukunft.

In meinen Augen ist ein VPN sehr erfolgsversprechend und wird in den nächsten Jahren noch viele Ve

Quellen und Literaturverzeichnis

Alby, Tom (2007). *Web 2.0. Konzepte, Anwendungen, Technologien*. München u.a.: Carl Hanser Verlag

Dax, Patrick (2009). *Facebooks Kleingedrucktes verärgert Nutzer*. In: futurezone.ORF.at vom 17. 2. 2009. URL: http://futurezone.orf.at/stories/1502679/ [25. 5. 2009

D. Bachfeld: *Sicheres Netz im Netz*, CT Heft 17, S.164-169.

http://www.netplanet.org/geschichte/arpa.shtml

Fuchs, Christian (2009). *Social Networking Sites and the Surveillance Society*. A critical Case Study of the Usage of StudiVz, Facebook and MySpace by Students in Salzburg in the Context of Electronic Surveillance. Salzburg/Wien: Forschungsgruppe Unified Theory of Information

Prof. Dr. Roman Beck (2009), *Interview mit Peter Tauber zum Thema „Anonymität im Internet: Menschenrecht oder Schutz für Kriminelle?“.*

http://wirtschaftslexikon.gabler.de/Definition/internet.html