Höhere Technische Bundeslehranstalt Wien Ottakring
Informationstechnologie und Elektronik

Netzwerktechnik

Netzwerksicherheit

Autoren:

Lorenz Leutgeb
lorenz.leutgeb@gmail.com

Moritz Wanzenböck
moritz9422@gmail.com

Betreuer:

FOL Ing. Dipl.–Päd. Michael Rausch

Wien, am 11. Mai 2011

Zusammenfassung

In diesem Paper wollen wir Sie in die Grundlagen der Netzwerksicherheit einführen und häufige Sicherheitslücken erläutern. Dabei hat ein guter Überblick Priorität, um eine Ausgangsbasis zur weiteren Recherche zu bieten.

Abstract

In this Paper, we want to introduce you to the basics of network security and point out common vulnerabilities. A good overview was priorized, to provide a base for research.

Inhaltsverzeichnis

1 Physical Layer

Physikalische Sicherheit ist das Um und Auf der Sicherungsmaßnahmen, wer nicht hier beginnt, hat schon verloren. Durch physikalischen Zugriff kann ein Angreifer praktisch alle höherliegenden Sicherungsmaßnahmen umgehen.

Schon bei der Planung des Netzwerkes sollte man auf die Absicherung der physikalischen Schicht bedacht sein. Dies beginnt schon bei den Zugangskontrollen zu den Gebäuden und endet bei dem Zugang zum Serverraum. Etwas Paranoia ist hier nicht übertrieben, denn auch wenn es sehr unwahrscheinlich erscheinen mag, es ist durchaus nicht auszuschließen, dass ein Angreifer als ganz normaler Besucher beim Vordereingang hereinspaziert und sich eine ungesicherte physikalische Schicht zu Nutze macht.

Diese Problem wird bei drahtlosen Netzwerken nur noch verstärkt, da man hier keine Kabel zur Verfügung hat, welche man absichern kann. Hier muss man sich mit Verschlüsselung und ähnlichen Maßnahmen so gut wie möglich schützen. Da dieses Thema eine sehr große Relevanz hat, ist ihm Abschnitt 2.3 auf Seite 6 gewidmet.

1.1 Planung

Die Sicherung muss schon in der Planungsphase begonnen werden. In dieser Phase sollte beschlossen werden, wo und wie die Verkabelung zu erfolgen hat. Dabei gilt die Faustregel: so wenig wie möglich, soviel wie notwendig. Ein Netzwerkzugang auf der Gästetoilette wird, auch unter dem Gesichtspunkt des „modernen“ Eindrucks der Firma, nur ein unnötiges Sicherheitsrisiko darstellen.

1.2 Der Serverraum

Dem Serverraum sollte hierbei eine besondere Bedeutung zukommen, ist er doch das Herz eines jeden Netzwerkes. Eine oberste Regel sollte es sein, so wenig Leuten wie möglich Zugang zu gewähren, denn, je weniger Personen ihn betreten, desto geringer ist die Chance eines missbehandelten Servers. [5]

1.3 Sicherungsmaßnahmen

Ein großer Gewinn an Sicherheit kann durch Zugangskontrollen, seien es Portiers oder Schlüsselkarten, erzielt werden. Weiters kann man sich prinzipiell durch den Einsatz von VPNs schützen. Genauere Informationen gibt es in Abschnitt 5.3 auf Seite 12.

Doch so ambitioniert die Sicherungsmaßnahmen auch sein mögen, es gilt immer den Faktor Mensch mit einzubeziehen. Leichtsinniger Umgang mit Passwörtern oder vergessene Handys mit sensiblen Firmendaten wird man zwar nie vollkommen ausrotten können, trotzdem kann man bei den Beteiligten ein Bewusstsein für eben jene Dinge wecken und so zumindest das Risiko minimieren.

2 Data Link Layer

2.1 Schwachstellen und deren Absicherung

2.1.1 ARP Spoofing

Funktionsweise Mithilfe des *Address Resolution Protocol* (ARP) werden IP-Adressen in MAC Adressen übersetzt. Jedes Gerät im Netzwerk kann ein Paket broadcasten, indem die gesuchte IP-Adresse

vermerkt wird (sog. *ARP Request*). Der Teilnehmer, auf die IP-Adresse passt, teilt diese nun dem Sender mit (sog. *ARP Reply*).

Ein Angreifer kann einem Gerät einen ARP Reply senden, welcher dann aufgrund fehlender Sicherheitsmechansimen als korrekt interpretiert und im *ARP-Cache* zwischengespeichert wird. [5, S. 99 u. 215] Ersetzt der Angreifer so beispielsweise die MAC Adresse des Gateways durch seine eigene, empfängt er alle Daten des Opfers, die an das Gateway gesendet werden sollen.

Anschließend an eine ARP Spoofing Attacke folgt oft eine Erweiterung des Verfahrens zu einer Man-In-The-Middle Attacke, indem das Gateway ebenfalls attackiert wird und alle Daten zwischen den Kommunikationspartnern weitergeleitet werden. So kann der Angreifer die Kommunikation zwischen Gateway und Opfer mitlesen und nach belieben verändern.

Gegenmaßnahmen Die Attacke basiert auf der Tatsache, das ARP keine Sicherheitsmaßnahmen vorsieht, um falsche Antworten auszuschließen. Außerdem fußt die Attacke auf dem Verhalten mancher Betriebssysteme, welche selbst richtige Einträge im ARP- Table durch falsche ersetzen. Abhilfe kann durch externe Tools geschaffen werden, die beispielsweise Replies ignorieren, falls bereits ein Record vorhanden ist. [5, S. 253]

Anmerkungen Diese Attacke wurde erfolgreich mit dem Tool `arpsoof` aus der `dsniff` Collection an einem Computer mit Microsoft Windows XP SP2 getestet.

2.1.2 MAC Flooding

Funktionsweise Das sogenannte *MAC Flooding* nutzt Schwachstellen in der Vermittlungseinheit eines Netzwerkes aus. Im speziellen ist diese Attacke auf Switches ausgerichtet.

Switches mappen über den sogenannten *Content Adressable Memory Table* (CAM Table) angeschlossene Geräte über ihre MAC Adresse auf einen bestimmten Port des Geräts. So kann im regulären Betrieb eine Vermittlung von Frames erfolgen, was das Sniffen von Frames, die für Geräte, welche an einem anderen Port des Switches angeschlossen sind, verhindert. Da ein Switch die Zustellung der Daten zu priorisieren hat, fällt er in den *Failopen*-Modus zurück, falls er keine neuen Geräte in sein speichertechnisch begrenztes Mapping aufnehmen kann. In diesem Modus werden alle Frames an alle Ports des Switches gesendet und der Angreifer kann alle Daten mitlesen. [5, S. 215]

Gegenmaßnahmen Moderne Switches sind solchen Angriffen gewappnet. Es lässt sich häufig ein Maximum an Einträgen im CAM Table pro Port festlegen, oder eine Sperre konfigurieren, welche verhindert, dass neue Einträge gesetzt werden, falls in gewisser Zeit eine abnorm große Menge an Geräten an einem Port verzeichnet wird.

Anmerkungen Diese Attacke wurde erfolgreich mit dem Tool `macof` aus der `dsniff` Collection an einem 3Com 330 Switch getestet.

2.2 VLANs

Um eine Strukturierung des Netzwerks in Broadcastdomains auch im Data Link Layer zu ermöglichen, wurde das Verfahren mit *Virtual Local Area Networks* (VLANs) vom *Institute of Electrical and Electronics Engineers* (IEEE) im Standard 802.1Q definiert. In einer Erweiterung des Ethernet Frames kann so eine Identifikationsummer hinterlegt werden. Weiters besteht die Möglichkeit bei neueren

Switches, einzelne Ports eigenen VLANs zuzuordnen. Diese neue Ebene der Netzwerkstruktur birgt natürlich Sicherheitsrisiken, sobald man damit sicherheitsrelevante Zonen unterteilt.

2.3 WLAN-Sicherheit

Bei der Verwendung von kabellosen Netzkomponenten entstehen neue Sicherheitsrisiken, daher möchten wir dieses Thema gesondert behandeln.

2.3.1 Einleitung

Die immer beliebter werdende Technik der drahtlosen Netzwerkinfrastruktur, insbesondere die unter IEEE 802.11 zusammengefassten Normen, bringen eine neue Arten von Sicherheitsproblemen und -risiken. Bei klassischer Infrastruktur wird ein Großteil der Sicherung über den physikalischen Zugriff auf das Übertragungsmedium erreicht, zum Beispiel über eine Zugangskontrolle zum Gebäude.

Diese Mechanismen sind bei drahtloser Kommunikation nur teilweise bis gar nicht wirksam, da elektromagnetische Wellen nicht an Gebäudegrenzen halt machen. Daher mussten und wurden neue Sicherungsmaßnahmen entwickelt, welche sich praktisch ausschließlich auf Layer 2 abspielen.

2.3.2 Authentifizierung & Verschlüsselung

In normalen LANs war es nicht üblich seine Daten zu veschlüsseln, im WLAN ist dies aber absolut notwendig. Die ersten Versionen des 802.11 Standards sahen ein Protokoll vor, welches äquivalente Sicherheit wie ein klassisches LAN bieten sollte, hierzu wurde das *Wired Equivalent Privacy-Protokoll* (WEP) entwickelt. Schon kurz nachdem der Standard veröffentlicht wurde, erschienen einige Publikation über Fehler im Protokoll, die zu Angriffen ausgenutzt werden konnten. [2] Daher wurde inzwischen ein neues Protokoll *Wi-Fi Protected Access (WPA)* und sein Nachfolger WPA2 entwickelt.

WEP Bei WEP wird eine einfache bitweise Verknüpfung mit einem pseudozufälligen Bitstrom aus dem *Rivest Cipher 4*-Algorithmus (RC4-Algorithmus) angewandt. Die Pseudozufallszahlen werden mit Hilfe eines *Initialisierungsvektors* (IV) und einem geteilten Schlüssel, der allen Stationen bekannt sein muss, errechnet. Für jeden Frame der gesendet wird, wird ein neuer IV berechnet und am Anfang des Frames mitgeschickt.

Hier liegen auch die Nachteile von WEP, da bereits ein Teil des Schlüssels bekannt ist. Bereits 2003 war es möglich bei ausreichend Netzwerkverkehr den geteilten Schlüssel innerhalb von 15 Minuten zu berechnen. Außerdem sieht WEP keine Benutzer-Identifikation oder - Authentifizierung vor und kämpft natürlich mit dem Problem aller *Pre-Shared-Key*-Verfahren: *Brute-Force*-Attacken oder die unbedachte Weitergabe von Passwörtern kann das Protokoll nicht verhindern.

WPA WPA wurde ursprünglich entwickelt, um eine Alternative zum unsicheren WEP-Standard zu bieten. Daher wurde von der WiFi-Alliance eine Teilmenge des damals in Arbeit befindlichen 802.11i-Standards genommen, und daraus ein neues Verfahren zu entwickeln: WPA. In WPA wird an Stelle des 40bit langen, einheitlichen Schlüssels aus WEP, ein 128bit langer Per-Paket-Schlüssel. Außerdem wird der geteilte Schlüssel mit Hilfe einer Kombinationsfunktion mit dem IV verbunden, im Gegensatz zu WEP, wo der Schlüssel einfach an den IV angehängt wird. Um Replay-Attacken zu verhindern wird eine fortlaufende Nummer im Paket mitgesendet. Zusätzlich wurden durch WPA eine weitere Art der Authentifizierung ergänzt, um auch Benutzer authentifizieren zu können.

Allerdings wird durch WPA nicht das Problem des geteilten Schlüssels gelöst, zumindest nicht im Consumer-Modus. Außerdem führt eine Schwachstelle im Verschlüsselungsalgorithmus dazu, dass mehrere kurze Nachrichten, wie zum Beispiel ARP-Antworten entschlüsselt werden, und der Schlüsselstrom des Pakets bis zu 7 mal wiederverwendet werden kann, um zum Beispiel gefälschte DNS-Antworten zu versenden. [1]

WPA2 Wie seine Vorgänger ist auch WPA2 nicht gegen Passwortattacken immun, allerdings setzt er nicht mehr auf den inzwischen als unsicher geltenden RC4-Verschlüsselungsalgorithmus sondern auf den weltweit anerkannten *Advanced Encryption Standard* (AES). WPA2 setzt den gesamten IEEE 802.11i-Standard um, wie bei seinem direkten Vorgänger ist eine Client-Authentifizierung per RADUIS-Server möglich.

3 Network Layer

3.1 IP

Das *Internet Protocol* (IP) ist das verbindende Glied zwischen entfernten Rechnern. Seine Adressierung ermöglicht Routing und ist somit unentbehrlich für große Netzwerke. Daher kommt ihm auch hinsichtlich der Netzwerksicherheit eine besondere Bedeutung zu. Auch wenn das Protokoll selbst eher selten Ziel von Attacken wird, gibt es eine Reihe von Gegenmaßnahmen um sich gegen Angriffe zu wehren, um Sicherheitsprobleme in anderen Schichten zu eliminieren.

3.1.1 IP-Spoofing

Bei dieser Attacke wird die Absender-Adresse des IP-Pakets gefälscht, um sich zum Beispiel Zugriff auf, per IP-Adress-Filter geschützte, Funktionen und Ressourcen eines Netzwerkgerätes zu verschaffen. [5, S. 110] Ein häufiges Beispiel sind Firmennetzwerke, in denen bestimmte Ressourcen innerhalb des firmeninternen Netzes auch ohne Authentifizierung nutzbar sind.

Allerdings ist diese Art der Attacke nur bedingt zu gebrauchen, da die Kommunikation nur einseitig erfolgen kann, denn wenn ein Antwortpaket geschickt wird, verwendet natürlich dieses Paket die gefälschte IP-Adresse als Zieladdresse, so dass es nahezu unmöglich ist das dieses Paket beim Angreifer ankommt. Eine weitere Absicherung stellen die Sequenznummern von TCP dar, welche neben einer Kommunikation in richtiger Reihenfolge auch eine Absicherung gegen IP-Spoofing darstellen, kann ein Angreifer doch nicht einfach in eine laufende Kommunikation eingreifen.

3.2 IPsec

Die *Internet Protocol Security* (IPSec) Suite besteht aus verschiedensten Komponenten und definiert Funktionen zum Tunneln von Datenströmen, aufbauend auf IP. [5, S. 158 ff.]

Authentifizierte Pakete IPSec gewährleistet, dass Pakete tatsächlich von der angegebenen Quelladresse gesendet wurden.

Integrität der Nutzdaten Durch *Hash Based Message Authentication Code* (HMAC) kann gewährleistet werden, dass die empfangengen – getunnelten – Nutzdaten fehlerfrei sind.

Replay Protection Mechanismen wie *Anti Replay Service* (ARS) schützen mithilfe von Sequenznummern vor dem erneuten Senden eines mit IPSec geschützten Pakets.

3.2.1 Tunnel-Modi

IPSec unterscheidet zwei Varianten der Übertragung [5, S. 159]:

Transport Mode Ist für die Host-to-Host Kommunikation konzipiert. Verschlüsselt wird nur der Payload des IP Protkolls, nicht aber der IP Header. So können die Pakete ohne Einschränkungen alle Router und NATs passieren.

Tunnel Mode Um Pakete mehrerer Rechner eines Netzwerkes verschlüsselt durch ein anderes zu tunneln, wird das komplette IP Paket verschlüsselt und in ein neues verpackt. Der Empfänger kann dann das ursprüngliche Paket wieder entpacken und in das private Netzwerk weiterleiten.

3.3 ICMP

Das *Internet Control Message Protocol* (ICMP) wird genutzt um Fehlermeldungen und andere Mitteilungen über das Internet zu übertragen. Der bekannteste Teil dieses Protokolls ist der Echo-Service, weithin auch als `ping` bekannt. Desweiteren lässt sich mit Hilfe von ICMP der Weg eines Paketes durch das Netzwerk verfolgen. Doch genau in dieser Nutzung von ICMP liegt auch das Problem des Ausspionierens der Netzwerktopologie, weswegen viele Unternehmen häufig die ICMP-Funktionen ihrer Router ausschalten.

```
10: telekabel.asn-wien.ac.at (193.170.115.130)
11: no reply
12: no reply
13: 193.170.162.12 (193.170.162.12)
```

Abbildung 1: Deaktiviertes ICMP

4 Transport Layer

4.1 TCP

Das wohl am häufigsten eingesetzte Protokoll des Transport Layers ist das *Transmission Control Protocol* (TCP). Es ermöglicht eine verbindungsorientierte und sichere Datenübertragung.

4.1.1 Spoofing

Ein Angreifer muss bei diesem Verfahren *Destination* - sowie *Source Port Number*, aber auch *Sequence Number* und *Acknowledgement Number* kennen. Letztere beide können nur bei alten Implementierungen erraten werden, daher werden sie üblicherweise durch sniffen des Datenstroms in Erfahrung gebracht. Aufbauend auf einer Spoofing Attacke kann dann ein Hijack ausgeführt werden. [5, S. 134]

4.1.2 Hijack

Ziel eines Hijackings ist es, eine TCP-Verbindung zu übernehmen. Dies lässt sich über eine Desynchronisation der Verbindung, mit darauffolgendem ACK-Storm erreichen. Im Idealfall bemerkt keiner der Verbindugnspartner den Eingriff und Authentifizierungsmechanismen wie *S/Key* können überbrückt werden. [5, S. 134]

4.1.3 Reset

Durch ein gesetztes *RST-Flag* in einem gespooften Paket kann die Kommunikation umgeleitet werden. Hier gilt es wieder die nötige *Sequence Number* herauszufinden. Lösungsansatz der *Internet Engineering Task Force* (IETF) ist es, nur die exakte Sequence Number zu akzeptieren (anstatt einer üblichen

Schwankung von mehreren Window Sizes) und der Lösungsvorschlag des *OpenBSD*-Projekts sieht zufällig verwendete Portnummern vor, welche praktisch unmöglich fälschbar sind. [5, S. 134]

4.1.4 SYN-Flood

Der Angreifer sendet andauernd Verbindungsversuche an den Server, dessen Rückfragen unbeantwortet bleiben. Diese, mitten im Handshake hängenden Verbindungen, werden als "halb-offen" bezeichnet. So wird der Server schnell überlastet, da natürlich alle Verbindungen zwischen gespeichert werden müssen. [5, S. 134]

4.2 UDP

Pendant des TCP stellt das *User Datagram Protocol* (UDP) dar. Verwendet wird es zur verbindungslosen und "unsicheren" Kommunikation. Vorteile bringen aber die kleinen Header und die somit höhere Geschwindigkeit durch weniger Overhead.

Da in UDP keine Sicherheitsmechanismen vorgesehen sind, ist es ein Leichtes, Pakete zu spoofen, oder bestehende Verbindungen zu hijacken. [5, S. 124 ff.]

4.3 Firewalls

Firewalls gehören zu den *Zugangsschutzssystemen*, das heißt, dass sie den Datenfluss zwischen zwei Endpunkten überwachen und bei Bedarf unterbrechen. Dies gilt für eingehende und ausgehende Verbindungen. Zusätzlich könnnen sie die Hardware im lokalen Netzwerk vor *Denial-Of-Service* Attacken (DoS Attacken) schützen.

4.3.1 Paketfilter Firewalls

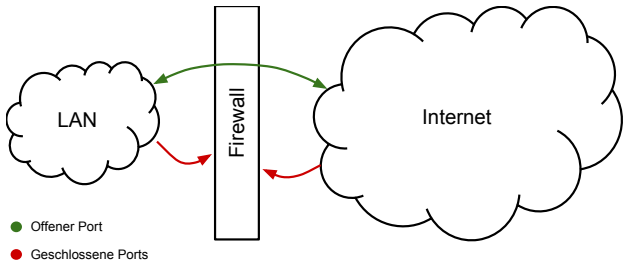

Abbildung 2: Paketfilter Firewall

Paketorientierte Firewalls sind oft zwischen einem Router und dem Internet angebracht. Sie filtern Pakete, adressiert an bestimmte Ports oder IP-Adressen. [5, S. 169]

Wurde eine Firewall wie in Tabelle 1 konfiguriert, ermöglicht sie den Zugriff auf Rechner via Port 80 und 22, verhindert aber allen sonstigen Verkehr. Dies würde zum Beispiel das Surfen im *World Wide Web* und die Nutzung von *Secure Shell* ermöglichen. Welche Dienste für die Verwendung freigeschaltet werden, bestimmt allein der Administrator.

type	source	destination
allow	192.168.1.*:*	*.*.*.*:80
allow	192.168.1.*:*	*.*.*.*:22
deny	all	all

Tabelle 1: Konfigurationsbeispiel einer Paketfilter Firewall

4.3.2 Personal Firewalls

Eine weitere Gattung der Firewall ist die *Personal Firewall*, eine Software, die lokal installiert wird und bestimmt, welche Verbindungen vom Host selbst initiiert beziehungsweise entgegengenommen werden dürfen. [5, S. 170]

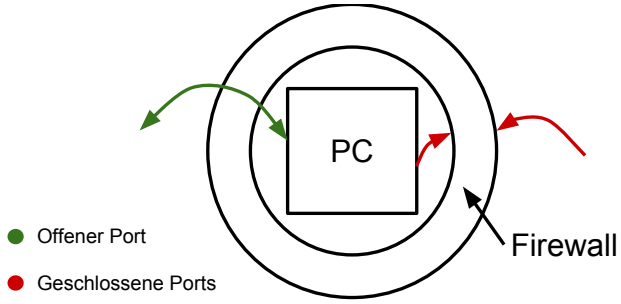

Abbildung 3: Personal Firewall

5 Application Layer

5.1 Proxy-Server

Proxy-Server (vom Engl. *proxy representative* = *Stellvertreter*) sind Stellvertreter, die zwischen Client und Server angesiedelt sind und so transparent die Verbindungen vermitteln können. Die meisten Proxy-Server werden als Cache oder Filter benutzt, häufig für eines oder mehrere der folgenen Protokolle: HTTP, SMTP und FTP.

Neben einigen anderen Funktionen können Proxys auch zu Sicherheitszwecken herangezogen werden. Außer der Filter-Funktion, welche zum Beispiel Dateien nach Viren scannen kann, kann ein Proxy-Server auch zum Zweck der Zugangskontrolle verwendet werden.

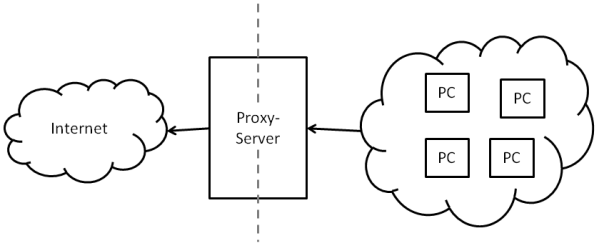

Abbildung 4: Schema Proxy-Server

5.1.1 SOCKS

Das *SOCKS* (Sockets) Protokoll definiert eine allgemeine Schnittstelle für Clients um alle möglichen Verbindungen über einen Proxy-Server zu leiten. Es unterstützt mehrere Arten der Nutzer-Authentifizierung und Autorisierung, zum Beispiel über Username und Passwort.

Anfrage			Antwort	
Version	Anzahl	Methoden	Version	Methode
1	2	134 ; 135	1	134

Tabelle 2: SOCKS-Anfrage und Antwort

Zuerst sendet der Client eine Anfrage an den Proxy-Server, in welcher er seine gewünschten Authentifizierungs-Methoden bekannt gibt, woraufhin der Server die von ihm priorisierte Methode zurücksendet. Wenn keine passende gefunden wurde, kann er die Verbindung auch abweisen. Ist die Authentifizierung erfolgt, muss der Client in einem weiteren Paket *Destination Port* und *Destination Address* bekanntgeben. Bestätigt der Server dies, kann der Proxy vom Client genutzt werden. [3]

5.2 DNS

Das *Domain Name System* (DNS) ist ein hierachisches Namensystem, das hauptsächlich dazu dient, Hostnamen in IP-Adressen aufzulösen. Es ist eines der am intensivsten genutzten Systeme des Internets. Da sich Menschen wesentlich leichter Namen statt Zahlen merken, wird DNS beinahe immer in Anwendungen eingesetzt, die eine Benutzerinteraktion möglich machen. Dies macht DNS natürlich attraktiv für Angreifer.

DNS ist aus Nutzersicht ein einfaches *Request-Response*-Verfahren, und genau dies macht es so gefährlich, es gibt nämlich keine Absicherung, die sicherstellt, dass die zurückgelieferte IP-Adresse tatsächlich stimmt. So ist bei den meisten Nutzern der DNS-Server ihres lokalen Internet-Providers für die echte Auflösung der Namen zuständig, welche diese Tatsache manchmal für ihre eigenen Zwecke missbrauchen und damit auch noch Sicherheitslücken öffnen. [4]

5.2.1 DNS Spoofing

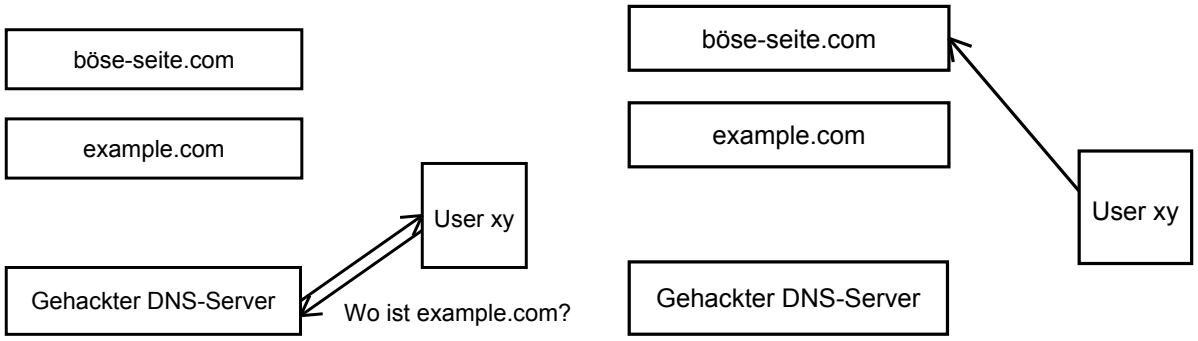

Abbildung 5: DNS Spoofing

Als DNS Spoofing wird das fälschen von DNS-Antworten bezeichnet, bei denen sich der Angreifer als

DNS-Server ausgibt und so dem Client statt der echten die IP-Adresse des Angreifer-Servers ausliefert. Dies kann zum Beispiel durch gehackte DNS-Server erfolgen, über eine manipulierte `hosts`-Datei oder durch *Cache-poisoning*, bei dem – ähnlich dem ARP Spoofing – früher eine Anfrage eines großen DNS-Resolvers zu beantworten als der befragte Server.

5.2.2 DNSSEC

DNS Security Extensions (DNSSEC) ist eine Weiterentwicklung des DNS-Protokolls. Es dient dazu, einem Client Sicherheit im Sinne einer vertrauenswürdigen Antwort zu geben. Durch asymmetrische Verschlüsselung kann eine Validierbarkeit der DNS-Antwort gewährleistet werden. Derzeit sind viele normale DNS-Clients nicht in der Lage diese, für DNS-Verhältnisse, relativ komplizierte Überprüfung durchzuführen. Häufig werden diese nur von den mächtigeren DNS-Resolvern eigener Namensserver durchgeführt.

5.3 VPN

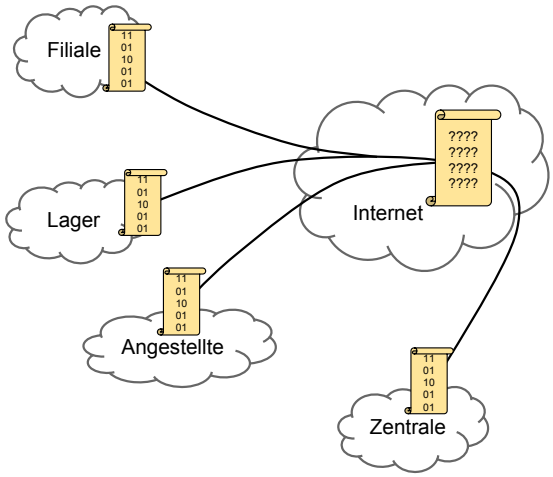

Abbildung 6: VPN Szenario

Virtual Private Networks (VPNs) sind virtuelle Netzwerke, deren Datenverkehr verschlüsselt über physikalische Netzwerke transportiert wird. So kann innerhalb von öffentlichen, womöglich unsicheren Netzwerken, Information übertragen werden. Man hört oft, dass VPNs, andere Protokolle *tunneln*. Dies bedeutet, dass die Daten eines Protokolls in die Nutzdaten eines anderen gekapselt werden. Dies geschieht im Falle von VPN zusätzlich verschlüsselt. Auf diese Art und Weise wird über den Application Layer des physikalischen Netzwerks der Data Link Layer des virtuellen Netzwerks gestülpt, und alle Protokolle des virtuellen Netzes werden durch die des physikalischen getunnelt. [5, S. 153]

5.3.1 VPN-Konfigurationen

Site-to-Site Wohl am bekanntesten ist beispielsweise die Verbindung einer Außenstelle mit einer Zentrale über VPN. Mittel zum Aufbau eines Netzweres zwischen Staaten sind schwer aufzubringen. Stattdessen kann ein Internetzugang genutzt werden, über welchen das interne Netzwerk getunnelt wird.

Remote-Access Dieses Verfahren, auch *Virtual Private Dial-up Network* (VPDN) genannt, ist eine flexiblere Version eines Site-to-Site VPNs. Das interne Netzwerk ist in der Zentrale mit dem Internet verbunden und Mitarbeiter aus aller Welt können sich vie VPN Clients auf deren Endgeräten einloggen.

5.3.2 Verschlüsselung

Häufig werden die Nutzdaten in VPNs mit Hilfe des *Data Encryption Standard* (DES) beziehungsweise dessen Erweiterung *Triple-DES* verschlüsselt. Um die Performance und somit den Datendurchsatz des virtuellen Netzwerkes zu verbessern, wird oftmals auch auf synchrone Schlüssel zurückgegriffen. Ist dies der Fall, müssen Schlüssel mit kurzer Verfallszeit verwendet werden, was schnell zu erheblichem

Verwaltungsoverhead führt. Ratsam ist dies daher nur in kleineren, überschaubaren Netzwerken. Für die Distribution der Schlüssel wurden eigens Systeme wie *Internet Key Exchange* (IKE) entwickelt. [5, S. 155]

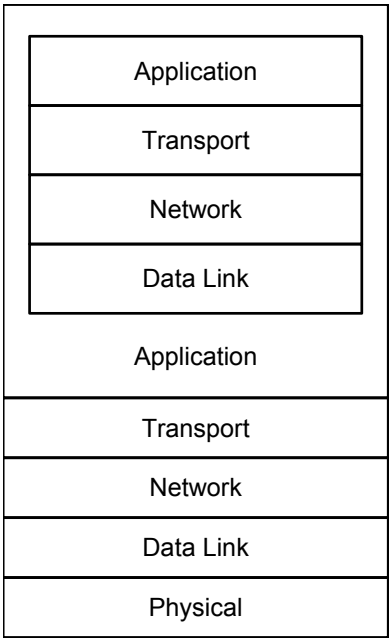

Abbildung 7: Encapsulation

6 Schlussbemerkung

Heutzutage werden Netzwerke – speziell computergestützte – immer wichtiger. Es ist nicht übertrieben, zu sagen, dass sie unersetzliche Voraussetzungen der modernen Gesellschaft und Wirtschaft sind. In diesem Sinne, sollten wir unsere Informationen vor neugierigen Augen schützen, sogar während sie in globalen Netzwerken über Kontinente übertragen werden. Seitdem Computernetzwerke ihren Aufschwung erleben, versuchen Wissenschaftler verlässliche Lösungen zu entwickeln. Da jedoch niemand unfehlbar ist, stieg die Zahl der Sicherheitslücken ebenso.

Dies wird sich auch in Zukunft nicht ändern, deshalb ist bei keiner Netzwerkbetreuung der Aspekt der Sicherheit zu vernachlässigen. Es ist zu empfehlen, sich immer auf dem Stand der Dinge bezüglich Sicherheit zu halten.

Literatur

[1] Beck, Martin ; Tews, Erik: *Practical attacks against WEP and WPA*. 2008. – URL `http://dl.aircrack-ng.org/breakingwepandwpa.pdf`. – Zugriffsdatum: 10.03.2011

[2] Khan, Jahanzeb ; Khwaja, Anis: *Building Secure Networks with 802.11*. Indianapolis : Wiley Publishing, Inc., 2003. – ISBN 9780471237150

[3] Leech, M. ; Ganis, M. ; Lee, Y. ; Kuris, R. ; Koblas, D. ; Jones, L.: *RFC 1928*. 1996

[4] Singel, Ryan: *ISPs' Error Page Ads Let Hackers Hijack Entire Web*. 2008. – URL `http://www.wired.com/threatlevel/2008/04/isps-error-page/`. – Zugriffsdatum: 06.04.2011

[5] Wendzel, Steffen ; Plötner, Johannes: *Netzwerk-Sicherheit*. 1. Galileo Press, 2005. – ISBN 3898425711

Abbildungsverzeichnis

Tabellenverzeichnis