RedDot Solutions AG

Projektdokumentation

Planung und Installation eines WLAN

Ausbildungsbetrieb:	**RedDot Solutions AG** **Industriestrasse 11** **26121 Oldenburg**
Ausbilder:	**Arne Koblitz**
Auszubildender:	**Rolf Hechtenberg** **Brookweg 183** **26127 Oldenburg** *** 29.12.1968 in Gelnhausen**
Ausbildungsberuf:	**Fachinformatiker** **Systemintegration**

Inhaltsverzeichnis

1. Projektbeschreibung

1.1. Projektumfeld

Die RedDot Solutions AG in Oldenburg stellt Content-Management-Software zur Verwaltung von Internet-Seiten her. Sie ist mit den Produkten RedDot CMS und RedDot XCMS weltweit Marktführer und beschäftigt zur Zeit 140 Mitarbeiter.

Die Zentrale in Oldenburg ist über eine 4 MBit-Leitung an das Internet angeschlossen. Die Geschäftstellen in Deutschland (Köln, München und Berlin) sowie USA, Australien, England, Italien und Polen sind über VPN-Zugang an dem LAN der Hauptgeschäftstelle Oldenburg angebunden. USA, Australien und England besitzen eigene Domänen.

1.2. Kundengespräch mit dem Systemadministrator

Im Gespräch mit dem Systemadministrator Herrn Koblitz ergab sich, das alle Sales-Mitarbeiter in ihren Büros auf Notebooks arbeiten und über Ethernet-Kabel mit dem Intranet verbunden sind. Mit diesen Notebooks werden Präsentationen für Kunden direkt vor Ort durchgeführt. Regelmäßig finden Treffen der Geschäftsführung mit den Sales-Mitarbeitern aus allen deutschen Niederlassungen im Konferenzraum der Zentrale in Oldenburg statt. Es ist jedesmal aufwendig die Notebooks an das Intranet anzuschließen.

1.3. Problemstellung und Erteilung des Auftrages

Da mittlerweile alle Notebooks der Sales-Mitarbeiter über integrierte WLAN-Netzwerkkarten verfügen, bietet es sich an, im Konferenzraum den drahtlosen Zugang zum Intranet zu ermöglichen. Weiterhin soll in allen Räumen der Zentrale Oldenburg drahtloser Zugang möglich sein, ohne das vorhandene Ethernet abzulösen. Die Administration des WLANs soll ohne Mehraufwand möglich sein. Für diese Anforderungen soll eine kostengünstige und leicht administrierbare Lösung gefunden werden. An der bereits vorhandenen Architektur soll so wenig wie möglich geändert werden. Der Neukauf von Hard- und Software soll auf das notwendigste beschränkt sein. Ganz besonderer Schwerpunkt liegt auf der Sicherheit des WLANs gegen unbefugten Zugriff. Die bereits vorhandene Sicherheits-Architektur soll mit berücksichtigt werden.

Meine Aufgabe ist es ein Sicherheitskonzept für das WLAN zu erarbeiten und dieses umzusetzen.

2. Projektplanung

2.1. Ist-Analyse

Das Intranet der RedDot Solutions AG besteht aus etwa 80 Servern, 180 Workstations und 40 Notebooks. Eingesetzt wird Microsoft Windows 2000 Professional, Windows 2000 Server, Windows 2003 Server, Windows XP Professional und Linux.

Die Zentrale in Oldenburg ist über eine 4 MBit-Leitung an das Internet angeschlossen. Als Firewall dient ein Windows 2003 Server mit ISA 2004 und 3 Zonen: Extern, DMZ und Intern. In der DMZ stehen unter anderem der Web-Server mit der URL www.reddot.de sowie News-, FTP- und Demo-Server. Das Intranet mit Domänencontrollern, File- und Produktivservern sowie den Arbeitsplatzrechnern ist in der internen Zone. Die externe Zone ist direkt mit dem Cisco-Router des Providers verbunden.

Auf der Messe Cebit 2005 war die Firma RedDot Solutions AG mit 2 Messeständen vertreten. Diese Messestände waren mit je einem WLAN ausgestattet. Jetzt stehen diese Access-Points für das Projekt WLAN zur Verfügung.

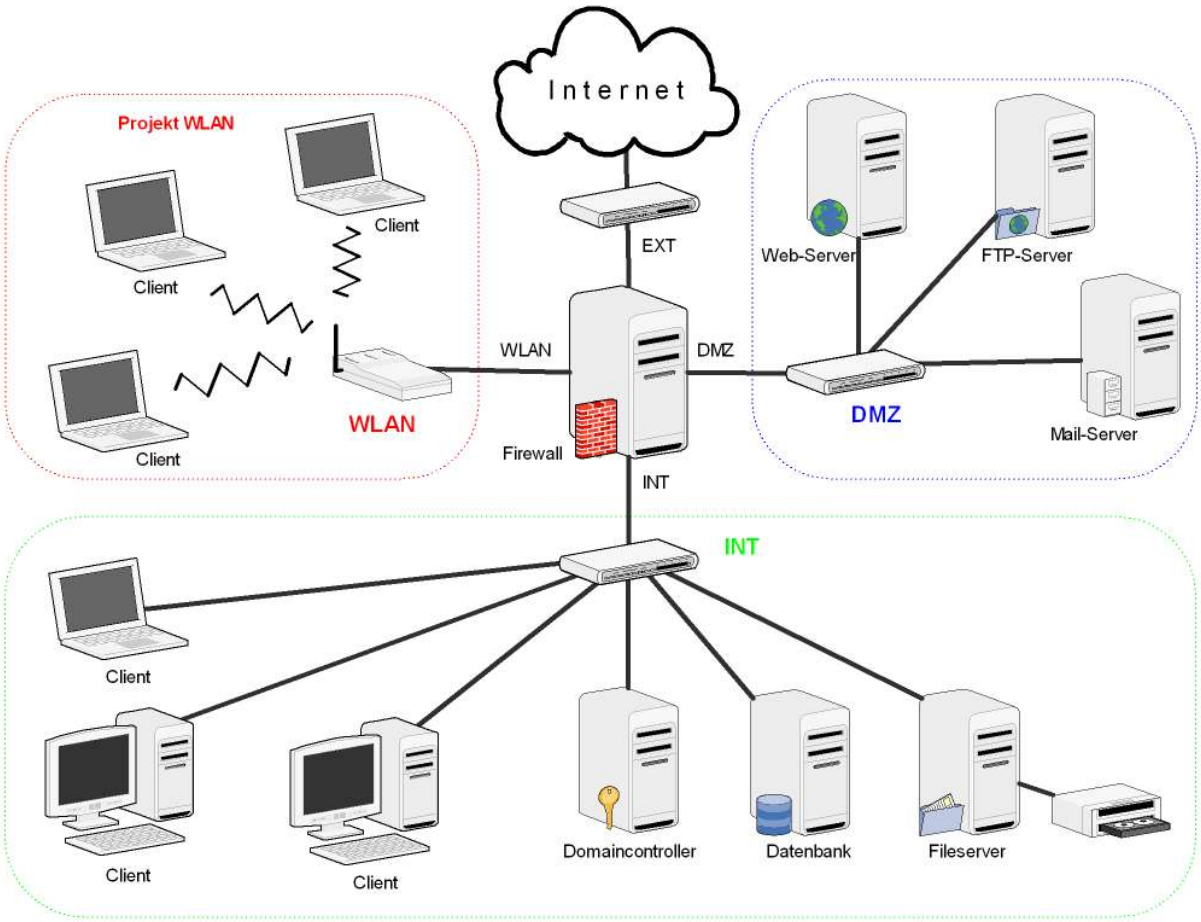


Abb. 1, Schematischer Netzplan der RedDot Solutions AG mit dem Projekt WLAN

2.2. Risiko-Analyse

Die von einem WLAN gesendeten Daten können von jedem empfangen werden, der sich innerhalb dessen Reichweite befindet. Die Sendeleistung der Access-Points ist durch den Standard 802.11g festgelegt und beträgt 100 mW. Die mögliche Reichweite ist etwa 100m innnerhalb und etwa 300m außerhalb von Gebäuden. Mit speziellen Antennen kann sie noch weiter vergrößert werden. Dadurch ergeben sich bei dem Betrieb eines WLAN für die Firma RedDot Solutions AG in der Hauptsache folgende Sicherheitsbedrohungen:

Abhören übertragener Daten
Bei nicht vorhandener oder nur unzureichender Verschlüsselung können vertrauliche Daten in die Hände von nicht autorisierten Personen gelangen. Erfahrene Personen mit böswilliger Absicht haben dadurch die Möglichkeit Informationen über weitere vorhandene IT-Systeme und Benutzer zu sammeln. Diese können sie für einen Angriff auf IT-Systeme oder Daten verwenden, die sonst nicht anfällig wären.

Zugriff auf das interne Netzwerk über den Access-Point
Falls der Access-Point direkt an das Intranet angeschlossen ist und per DHCP IP-Adressen aus dem Intranet-Bereich vergibt, genügt alleine das Überwinden eines Access-Points um vollen Zugang zu erhalten. Dies ist dann ein idealer Ausgangspunkt für weitere Aktionen.

Angriff auf mit dem WLAN verbundene Client-Rechner
Eine weitere Möglichkeit in das Intranet einzudringen besteht darin sich Zugang auf ein ungesichertes Notebook zu verschaffen das über WLAN mit dem Intranet verbunden ist. Ein Angreifer hätte dann die Möglichkeit über das installieren eines Trojaners permanenten Zugang zu erhalten.

2.3. Recherche zu möglichen Sicherheitstechnologien

Es bestehen mehrere Möglichkeiten ein WLAN abzusichern. Sie unterscheiden sich in Aufwand und erzielter Sicherheitsstufe:

MAC-Filter
Jede Netzwerkkarte verfügt über eine einmalige Hardware-Adresse, die MAC (Media Access Control Adress). In vielen Access-Points ist ein MAC-Adressen-Filter eingebaut, mit dem sich der Zugriff auf eine definierte Anzahl von MACs beschränken läßt. Durch abhören des Datenverkehrs läßt sich leicht eine gültige MAC herausfinden. Diese wird dann anstelle der eigenen MAC benutzt und dadurch der Filter ausgehebelt.

WEP
Der WLAN Standard 802.11, mit dem die Daten übertragen werden, besitzt die Sicherheitstechnologie WEP (Wired Equivalent Privacy), die Vertraulichkeit, Integrität und Authentifizierung ermöglichen soll. Diese verschlüsselt jedes Datenpaket nach dem RC4-Algorithmus mit einer konstanten Schlüssellänge von entweder 40 Bit oder 104 Bit und einem Initialisierungsvektor (IV) von 24 Bit. Dieser IV erhöht sich mit jedem verschlüsselten Datenpaket um 1 und wiederholt sich dadurch nach 16.777.216 Datenpaketen. Mit einer genügenden Anzahl von mitgeschnittenen Paketen und deren IV kann z. B. das Programm “Aircrack“ auf den WEP-Schlüssel schließen. Je nach Länge des verwendeten Schlüssels braucht man 100.000-250.000 IVs (bei 64-Bit-Schlüsseln) oder 500.000-1.000.000 IVs (bei 128-Bit-Schlüsseln). WEP ist deshalb kompromitiert und scheidet als Sicherheitstechnologie aus.

WPA
Der Nachfolger von WEP ist WPA (Wi-Fi Protected Access) und ermöglicht eine größere Sicherheit als sein Vorgänger. WPA ist eine Zwischenlösung bis zur Einführung des neuen Sicherheitsstandards 802.11i und enthält einige Teile aus diesem. Es bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren. Die erhöhte Sicherheit gegenüber WEP besteht darin, dass der Schlüssel nur bei der Initialisierung verwendet wird und anschließend ein Session-Key zum Einsatz kommt. Die Schlüsselverwaltung geschieht entweder über einen zentralen Server oder es wird ein Pre-Shared-Key eingesetzt, bei dem sich alle Nutzer eines Netzes mit gleichem Kennwort anmelden. Es dürfen nur lange und schwer zu erratende Passwörter eingesetzt werden. Zu kurze und leicht zu erratende Passwörter ermöglichen einen Brute-Force- oder einen Wörterbuch-Angriff. Dies ist aber keine Sicherheitslücke des WPA-Standard. Seit November 2004 existiert das Programm "WPA Cracker", um eventuell vorhandene schwache Passwörter auszunutzen.

RADIUS
Das Client-Server Protokoll RADIUS (Remote Authentication Dial-In User Service) wurde zur Authentifizierung von Benutzern bei Einwahlverbindungen entwickelt. Es gilt als der Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN oder WLAN. Der RADIUS-Server übernimmt hierbei die Verwaltung der Zugangsdaten von Client-Geräten und Benutzern. Außerdem stellt er Möglichkeiten zur gebührenpflichtigen Abrechnung der Einzelverbindungen bereit.

VPN mit IPsec
Ein VPN (Virtuelles Privates Netzwerk) ist ein Tunnel durch ein öffentliches Netzwerk. IPsec (IP-Security) ist eine Erweiterung des Internetprotokolls. In dem kommenden Internet-Protokoll IPv6 ist IPsec fester Bestandteil. Es stellt eine Sicherheitsarchitektur mit Zertifikaten für die Kommunikation über IP-Netzwerke zur Verfügung und bietet die folgenden Sicherheitsdienste an:

- Authentifikation der Kommunikationspartner
- Integrität der Informationen
- Verschlüsselung der Informationen
- Massnahmen gegen Replay-Angriffe
- Schlüssel Management

Zur Erfüllung dieser Forderungen verwendet IPsec das AH- (Authentication Header), ESP- (Encapsulating Security Payload) und das IKE (Internet Key Exchange) Protokoll.

VPN mit IPSec wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zum Einsatz bei WLANs besonders empfohlen.

2.4. Ergebnis der Recherche zu Sicherheitstechnologien

Hauptsächlich unterscheiden sich die anwendbaren Sicherheitstechnologien darin, daß neben dem Benutzer auch die beteiligten Rechner authentifiziert werden können. Dies geschieht durch Einbeziehen einer dritten Partei denen die beiden kommunizierenden Parteien vertrauen (Zertifikate und Public Key Infrastruktur, PKI).

2.5. Sicherheitskonzept auf Basis VPN mit IPsec

Die Firma RedDot Solutions AG verfügt bereits über einen VPN-Zugang. Aus diesem Grund entscheide ich mich für VPN mit IPsec. Die notwendigen Software-Komponenten stehen in der Firewall ISA 2004 und im Betriebssystem Windows XP Professional der Notebooks bereits zur Verfügung.

Der Zugang über WLAN zum Intranet erfolgt dann in diesen Schritten:

- **Anmeldung beim Access-Point**
  Der Access-Point erhält ein 256 Bit WPA Passwort. Das WPA-Passwort wird mit einem Passwort-Generator erstellt und besteht aus zufälligen Folgen von Zahlen und Buchstaben. Dies macht Wörterbuch-Attacken erfolglos.

- **Zuweisung einer IP-Adresse mit DHCP**
  Das WLAN wird als unsichere Zone behandelt und bekommt einen anderen IP-Adress-Bereich als das Intranet. Es ist durch die Firewall gesichert.

- **Einwahl mit VPN**
  Die Firewall erlaubt den Zugang vom WLAN zum Intranet nur über VPN. Der notwendige Pre-Shared-Key für IPsec wird ebenfalls mit dem Passwort-Generator erstellt.

Die Notebooks der Sales-Mitarbeiter werden durch die Firewall des Windows XP SP2 ebenfalls gesichert. Jeder Mitarbeiter, der sich über das WLAN einwählen möchte, bekommt zusammen mit dem Pre-Shared-Key besondere Hinweise zum Umgang mit der eigenen Firewall.

Die Vertraulichkeit der Daten bei der Übertragung im WLAN beruht jetzt nicht mehr auf dem Standard 802.11 sondern auf IPsec. Auch wenn sich herausstellt das WPA kompromitiert werden kann, bleibt die Vertraulichkeit erhalten.

Zusammengefaßt erfolgt die Absicherung des WLANs in folgenden Stufen:

Anmeldung
- Stufe 1 256 Bit WPA-Key für Zugang zum Access-Point
- Stufe 2 Pre-Shared-Key (=Zertifikat) für die Authentifizierung bei IPsec des VPN
- Stufe 3 Benutzername und Passwort des Domänen-Account

Netz und Firewall
- Stufe 4 Trennung durch eigenen IP-Kreis vom Intranet
- Stufe 5 Zugang nur per VPN über Firewall möglich
- Stufe 6 Client-Notebooks mit Firewall gesichert

2.6. Sollkonzept / Pflichtenheft

Auf Basis dieses Sicherheitskonzeptes ergeben sich für mich folgende Aufgaben:

Hardware
- optimale Aufstellplätze für Access-Points bestimmen, installieren und anschließen
- Ausleuchtung der Büroräume um Empfangsqualität sicherzustellen
- weitere Netzwerkkarte für die WLAN-Zone in den Firewall-Rechner einbauen

Software
- Access-Points konfigurieren
- WLAN-Zone in ISA 2004 einrichten
- Firewall-Regeln für WLAN-Zone definieren
- VPN-Dienste in ISA 2004 konfigurieren
- WPA-Passwort und Pre-Shared-Key mit Passwort-Generator erstellen
- VPN-Verbindung zum Testen auf einem Notebook einrichten
- Firewall des Notebooks konfigurieren

Test
- Funktionstest durchführen

Dokumentation
- Sicherheitshinweise für alle Benutzer des WLAN
- Anleitung zur Einrichtung von WLAN und VPN
- Kundendokumentation
- Betriebsdokumentation

2.7. Projektablaufplan / Terminplan

Für dieses Projekt sind 35 Arbeitsstunden vorgesehen. Da keine weiteren Komponenten eingekauft werden, entfallen Warte- und Lieferzeiten.

2.8. Kosten-Nutzen-Analyse

Aufgrund der bereits vorhandenen Hard- und Software sind weitere Anschaffungen nicht notwendig. Für meine Arbeitszeit als Umschüler berechne ich 15,- € pro Stunde. Dies ergibt folgende Kalkulation:

Kosten des WLAN			
Access-Point	2x	70,00 €	140,00 €
Netzwerk-Kabel	2x	5,00 €	10,00 €
Netzwerk-Karte	1x	20,00 €	20,00 €
Switch	1x	30,00 €	30,00 €
Arbeitszeit	35x	15,00 €/h	525,00 €
Einmalige Gesamt-Kosten			**725,00 €**

Allgemein entfällt die Vorbereitung des Konferenzraumes mit Aufstellen von Switches und deren Verkabelung für den Zugang der Notebooks in das Intranet. Ebenso erübrigt sich das Abbauen nach den Konferenzen. Die regelmäßig eingesparte Arbeitszeit beträgt pro Konferenz etwa eine halbe Stunde. Es finden regelmäßig alle 2 Wochen Konferenzen statt. Weiterhin wird der Konferenzraum für Meetings und Präsentationen der Produktmanager und der Marketingabteilung genutzt. Insgesamt ergeben sich daher etwa 35 Konferenzen und Meetings im Jahr.

Nutzen des WLAN			
Auf/Abbau je Konferenz: 30 min	35x	15,00 €/h	262,50 €
Jährliche Einsparung			**262,50 €**

Der rein finanzielle Vergleich der Kosten und der Einsparungen durch dieses Projekt erlaubt keine umfassende Aussage zum Nutzen. Die besonderen Vorteile durch den Einsatz des WLAN wie Komfortabilität und Zufriedenheit der Mitarbeiter sowie vereinfachte Geschäftsabläufe lassen sich nur bedingt in Zahlen fassen. Diese Vorteile sind der Geschäftsführung bewußt und waren der Grund ein WLAN zu installieren. Dadurch erübrigt sich eine weitere Gewichtung des erreichbaren Nutzen.

2.9. Vorstellung des Gesamtkonzeptes

Beim nächsten Treffen mit Herrn Koblitz präsentierte ich das Pflichtenheft mit dem Sicherheitskonzept. Herr Koblitz ist mit der erreichten Sicherheitstufe und den geringen Kosten sehr zufrieden und erteilt mir den Auftrag zur Umsetzung.

3. Projektdurchführung

3.1. Installation der Access Points

Die Zentrale in Oldenburg hat Büroräume in 2 Stockwerken, im Obergeschoß und im Dachgeschoß. Der Serverraum im Dachgeschoß befindet sich über dem Konferenzraum im Obergeschoß, deshalb wird der erste Access-Point hier installiert. Der zweite Access-Point wird entlang dem Flur 20m gegenüber dem ersten Access-Point installiert. Sein Netzanschluß wird in den Serverraum gepatched. Zusammen mit dem ersten Access-Point ist er über einen Switch an die Firewall angeschlossen. Durch ihre Roaming-Fähigkeit ist ein einfacher Übergang zwischen den beiden Funkzellen möglich.

3.2. Messung und Auswertung mit Ekahau Site Survey 2.1

Die Ausbreitung von Funkwellen in Gebäuden wird durch Wände, Decken, Türen und Büro-Inventar gedämpft. Ebenfalls besteht die Möglichkeit einer Störung durch benachbarte WLANs. Eine Funkausleuchtung zeigt grafisch die Empfangsqualität in den betreffenden Räumen an. Dabei werden nach der Installation der Access-Points in den gesammten Räumlichkeiten Messungen durchgeführt. Eventuell schon vorhandene WLANs und ihre Kanäle werden erkannt und die am besten verfügbaren Kanäle bestimmt. Ich habe hierfür die Demo-Version von Ekahau Site Survey 2.1 eingesetzt.

3.3. Hard- und Software-Konfiguration

3.3.1. Konfiguration der Access-Points

Die Access-Points werden über ein Browser-Menu konfiguriert. Zuerst wird das Standard-Passwort durch ein eigenes ersetzt. Beide bekommen eine feste IP, die gleiche SSID und den gleichen WPA-Key. Dann wird DHCP und der zu vergebende IP-Bereich eingestellt.

3.3.2. Weitere Netzwerkkarte und Firewall-Regeln für ISA 2004

Der Firewall-Rechner wird um eine Netzwerkkarte erweitert. Dies geschieht außerhalb der Bürozeiten damit der laufende Betrieb nicht gestört wird. Der neuen Netzwerkkarte wird im ISA 2004 die Zone WLAN mit einem eigenen Adress-Bereich zugewiesen.

3.3.3. Ergänzen der VPN-Dienste des ISA 2004

Der ISA 2004 ist bereits für die Anbindung der Geschäftstellen über VPN an das Intranet eingerichtet. Jeder VPN-Client bekommt über DHCP eine IP-Adresse aus dem IP-Kreis des Intranet zugewiesen. In den Sicherheiteinstellungen von IPsec wird der Pre-Shared-Key hinzugefügt.

3.3.4. Einrichten der Notebooks

Auf den Notebooks wird die VPN-Verbindung „VPN RedDot“ hinzugefügt und mit der IP der Firewall und dem Pre-Shared-Key konfiguriert. Die Windows-Firewall des Service-Pack 2 wird eingeschaltet.

3.4. Testlauf

Nachdem alle Komponenten installiert und fertig konfiguriert waren, wurde ein erfolgreicher Testlauf durchgeführt.

4. Projektabschluss

4.1. Übergabe des WLAN

Nach Abschluß aller Arbeiten wurde das WLAN an Herrn Koblitz übergeben. Er überzeugte sich von der ordnungsgemäßen Funktion und ließ sich die Einrichtung einer VPN-Verbindung auf einem Notebook vorführen.

4.2. Vergleich von Soll- und Ist-Zustand

Alle Vorgaben des Pflichtenheftes sind erfüllt:

- Das WLAN wurde auf der vorhandenen Sicherheitsarchitektur aufgebaut.
- Es war keine weitere Hard- oder Software notwendig.
- Die erreichte Sicherheitsstufe ist sehr hoch.

4.3. Anfertigung der Betriebs- und Kundendokumentation

Die Betriebs- und Kundendokumentation habe ich nach Vorgaben von Herrn Koblitz angefertigt. Er hat mit dem Einsatz von Screenshots sehr gute Erfahrungen gemacht und mich deshalb gebeten die Anleitung zum Einrichten der VPN-Verbindung für die Sales-Mitarbeiter als Abfolge der Menüs und ihrer Eingaben darzustellen. Dies vermeidet viele Rückfragen.

4.4. Änderungen gegenüber dem Projektantrag

Ursprünglich hatte ich eine kurze Gegenüberstellung von Einstufigen und Mehrstufigen Sicherheitstechnologien geplant. Jetzt schien es mir jedoch sinnvoller die Ergebnisse der Recherche zu den Sicherheitstechnologien zusammenzufassen und dabei auf ihre Unterschiede einzugehen.

4.4. Fazit

Wärend der Projektdurchführung stellte sich heraus, daß ich den Zeitaufwand für einige Punkte ganz anders eingeschätzt habe.

Die Recherche nach Informationen über Sicherheit im WLAN, VPN und IPsec brachte eine überwältigende Fülle an Material zusammen. Z.B. ist es für einige Computer-Interessierte zu einem Sport geworden mit ihrem Notebook und einem GPS-Empfänger durch die Umgebung zu fahren und dabei Karten von gefundenen WLANs anzulegen. Diese „Wardriver“ haben Spass daran die Besitzer, vor allem Firmen, auf mangelhaft gesicherte WLANs hinzuweisen – ohne diese Lücken zum Schaden auszunutzen. Besonders interessant und ausführlich fand ich auch die Erklärungen und Sicherheitshinweise der National Security Agency (NSA) zu IPsec. Insgesamt habe ich mir doppelt soviel Zeit für die Recherche genommen als vorher geplant.

Das Ausleuchten mit Ekahau Site Survey ging wesentlich schneller voran als vorher von mir vermutet. Ich benötigte nur etwa die Hälfte der veranschlagten Zeit.

Im Endeffekt haben sich diese zeitlichen Verschiebungen wieder aufgehoben und hatten daher keine Auswirkung auf den festgelegten Abgabetermin.

Ich wäre gerne noch auf den Bereich Elektrosmog und eventuelle Strahlenbelastung durch WLANs am Arbeitsplatz eingegangen – leider war dafür im Rahmen dieses Projektes keine Zeit mehr übrig.

Das Projekt hat mir sehr viel Spass gemacht.

I. Anhang

I.I Testergebnisse von Ekahau Site Survey 2.1

Bild 1, Gesamtansicht Obergeschoß

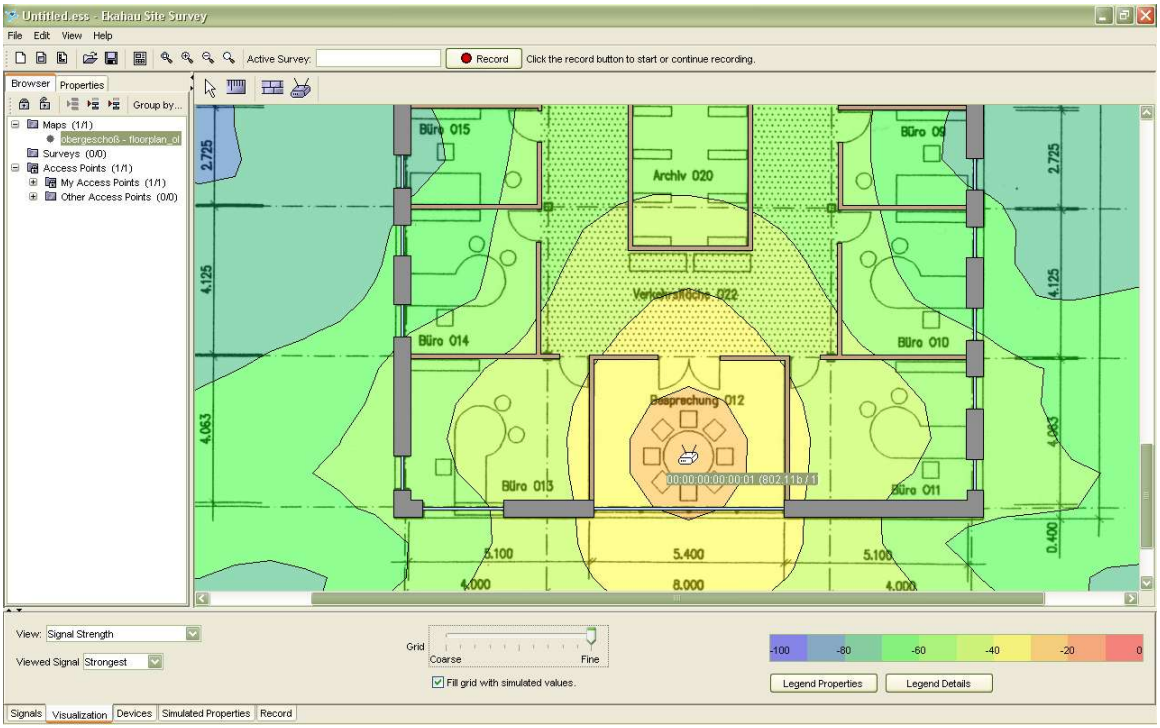


Bild 2, Detailansicht Obergeschoß

I.II. Konfiguration der Access-Points

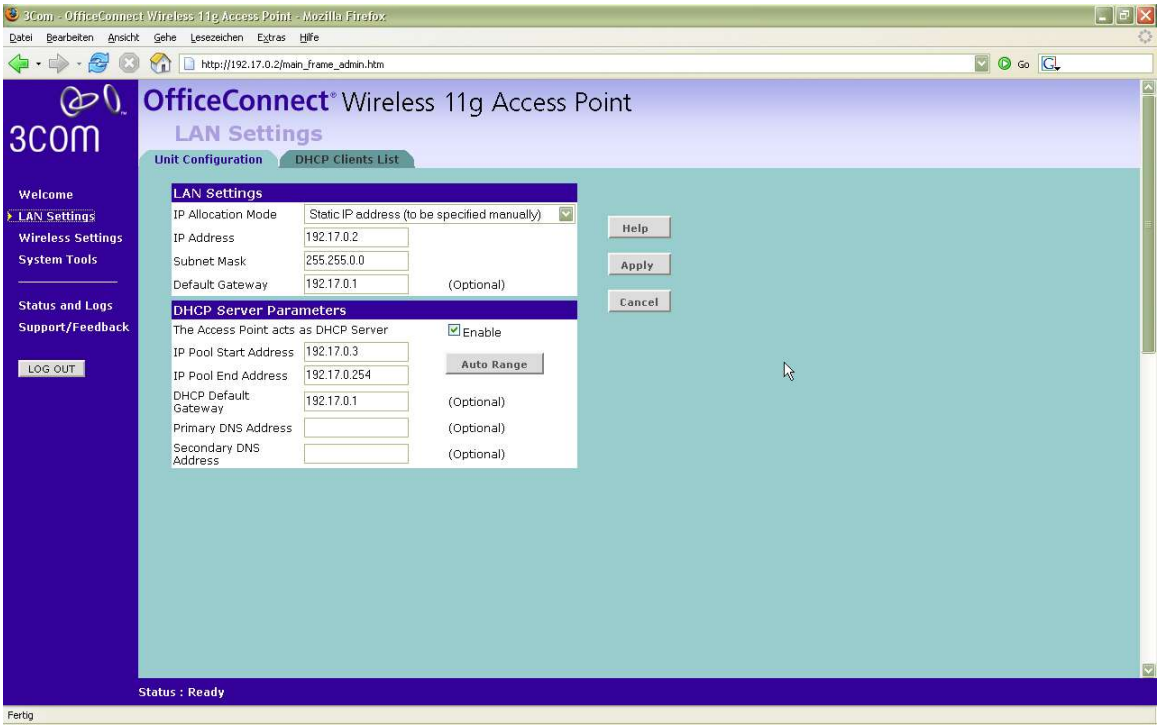


Bild 3, LAN und DHCP Einstellungen

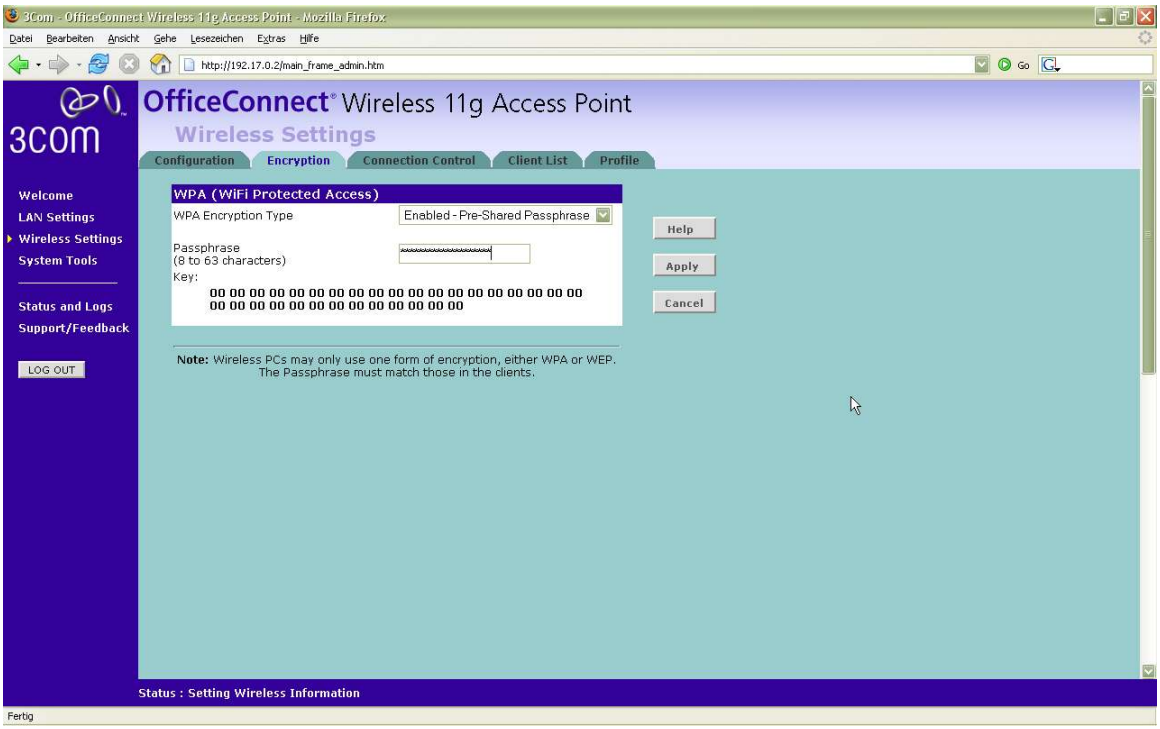


Bild 4, WPA Passwort

I.III. Konfiguration des ISA 2004

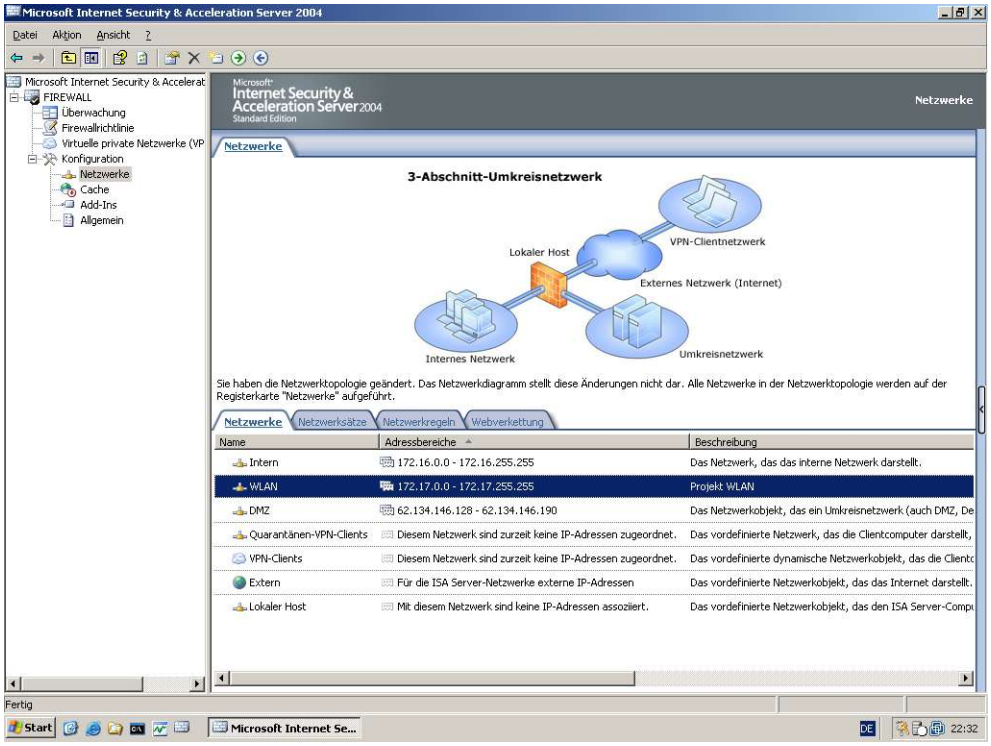


Bild 5, Neue Zone WLAN

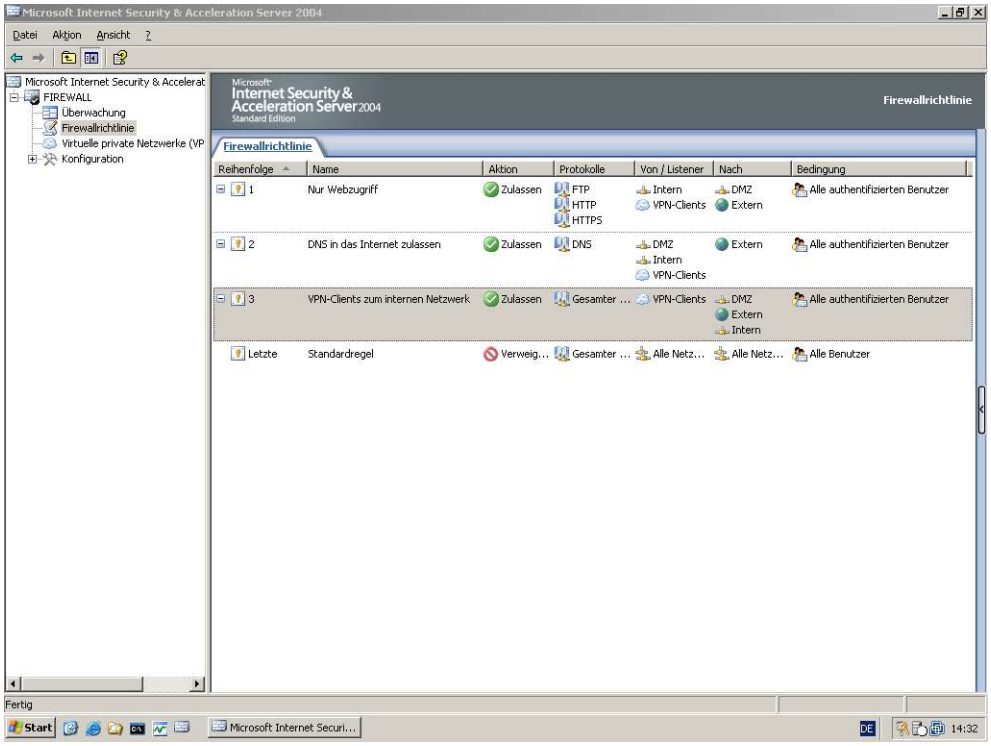


Bild 6, Firewallregeln

I.V. Passwortgenerator

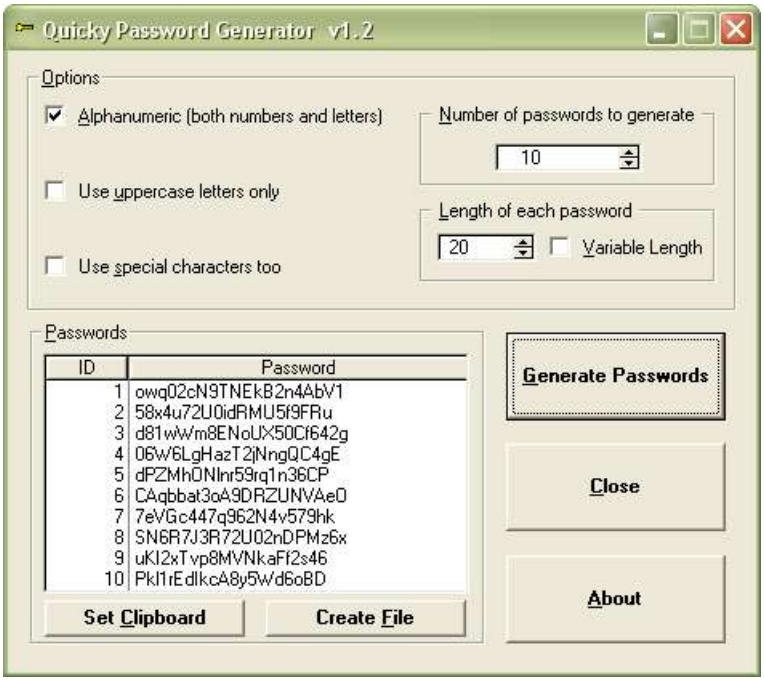


Bild 7, Passwörter bestehend aus Zahlen und Buchstaben

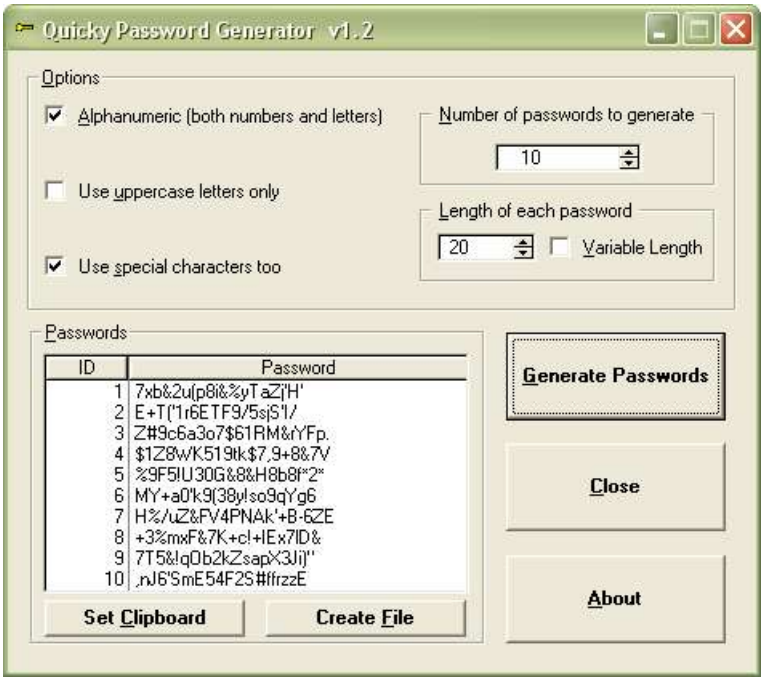


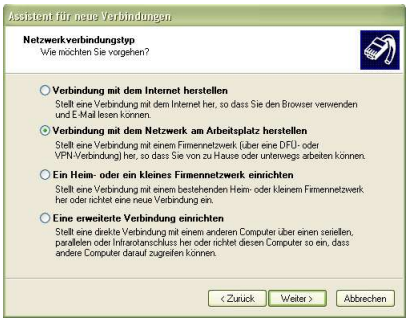
Bild 8, Passwörter bestehend aus Zahlen, Buchstaben und Sonderzeichen

I.VI. Kundendokumentation: Einrichtung des VPN der Notebooks

Anleitung zur Einrichtung des WLAN-Zugang über VPN

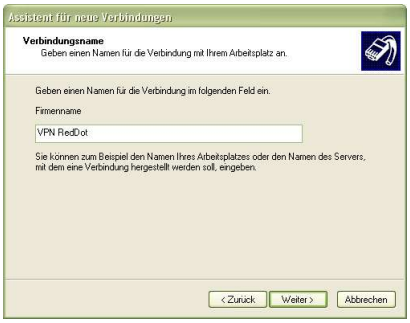
1. Neue Verbindung erstellen

2. Auswahl des Assistent

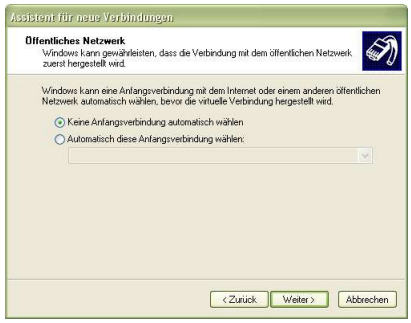


3. Netzwerk am Arbeitsplatz

4. Art der Verbindung ist VPN



5. Namen vergeben



6. Keine Anfangsverbindung

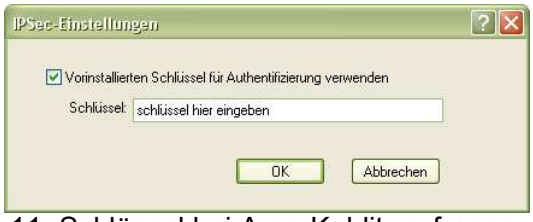
7. IP des VPN-Server

8. VPN ist fertig eingerichtet

I.VI. Kundendokumentation: Einrichtung des VPN der Notebooks (Fortsetzung)

9. Eigenschaften anklicken

10. IPsec-Einstellungen klicken



11. Schlüssel bei Arne Koblitz erfragen.

12. Windows Firewall aktivieren !

I.VII. Quellenverzeichnis

- 3Com: Wireless Solutions
  http://www.3com.com/en_US/jump_page/abg_wireless.html
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheit im WLAN
  http://www.bsi.de/literat/doc/wlan/index.htm
- Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutzhandbuch
  http://www.bsi.de/gshb/deutsch/download/index.htm
- Chaos Computer Club
  http://www.ccc.de/
- Chaos Computer Club: IPsec
  http://www.chscene.ch/ccc/ds/80/013.htm
- Ekahau Site Survey 2.1
  http://www.ekahau.com/products/sitesurvey/
- Ekahau Site Survey 2.1 Planner
  http://www.ekahau.com/products/sitesurvey/modules.html
- Elektronik Kompendium: Remote Access Service
  http://www.elektronik-kompendium.de/sites/net/0907081.htm
- FreeBSD: VPN mit IPsec
  http://www.freebsd.org/doc/de_DE.ISO8859-1/books/handbook/ipsec.html
- Heise-Verlag: WLAN Hacking en passant
  http://www.heise.de/security/artikel/print/38099
- Intel: Thema Sicherheit
  http://www.intel.com/cd/business/enterprise/emea/deu/bss/infrastructure/security/index.htm
- Inform IT: Wireless Security
  http://www.informit.com/guides/content.asp?g=security&seqNum=61
- Inform IT: IPsec
  http://www.informit.com/guides/content.asp?g=security&SeqNum=24&rl=1
- Microsoft: Sicherheitsprobleme in WLANs
  http://www.microsoft.com/germany/sicherheit/guidance/modules/secmod168.mspx
- Microsoft Sicherheits Portal
  http://www.microsoft.com/germany/sicherheit/default.mspx
- Microsoft: Schützen von Netzwerken mit IPsec
  http://www.microsoft.com/germany/sicherheit/newsletter/artikel/ipsec.mspx
- Microsoft: Planungshandbuch zur WLAN Absicherung
  http://www.microsoft.com/germany/sicherheit/guidance/modules/secmod168.mspx
- Microsoft: ISA 2004 Sicherheitshandbuch
  http://www.microsoft.com/germany/sicherheit/guidance/modules/isa/hardeningguide.mspx
- Microsoft: Konfiguration eines VPN unter Windows 2003 Server
  http://support.microsoft.com/default.aspx?scid=kb;de;323441
- msisafaq.de: ISA 2004
  http://www.msisafaq.de/Anleitungen/2004/index.htm
- National Security Agency: Microsoft Windows IPsec Guide
  http://www.nsa.gov/snac/os/win2k/w2k_ipsec.pdf
- National Security Agency: Securing Microsoft Windows XP
  http://www.nsa.gov/snac/downloads_all.cfm?MenuID=scg10.3.1
- OpenSwan
  http://www.openswan.org/
- The Honeynet Projekt
  http://www.honeynet.org/

I.VII. Quellenverzeichnis (Fortsetzung)

- The Hacktivist
  http://www.thehacktivist.com/hacktivism.php
- Universität Oldenburg: Rechnernetze
  http://einstein.informatik.uni-oldenburg.de/rechnernetze/inhalt.htm
- VMWare: GSX Server
  http://www.vmware.com/products/server/gsx_features.html
- Wikipedia: Hacker
  http://de.wikipedia.org/wiki/Hacker
- Wikipedia: IPsec
  http://de.wikipedia.org/wiki/Ipsec
- Wikipedia: VPN
  http://de.wikipedia.org/wiki/VPN
- Wikipedia: WarDriving
  http://de.wikipedia.org/wiki/WarDriving

- AirSnort
  http://airsnort.shmoo.com/
- Airopeek
  http://www.wildpackets.com/products/airopeek_nx
- Black Alchemy: fakeAP
  http://www.blackalchemy.to/project/fakeap/
- Kismet
  http://www.kismetwireless.net/
- Netstumbler
  http://www.netstumbler.com/
- Wellenreiter
  http://www.wellenreiter.net/

I.VIII. Genehmigter Projektantrag

Für die Büroräume der RedDot Solutions AG in der Industriestrasse 11 soll ein WLAN errichtet werden, um drahtlosen Anschluss an das Internet (WWW) zur Verfügung zu stellen. Ganz besonderer Schwerpunkt liegt auf der Sicherheit gegen unbefugten Zugriff.

Derzeitiger Zustand
Die Zentrale in Oldenburg ist über eine 4 MBit-Leitung an das Internet angeschlossen. Als Firewall dient ein Windows 2003 Server mit ISA 2004 und 3 Zonen: Extern, DMZ und Intern. In der DMZ stehen unter anderem der Web-Server mit der URL www.reddot.de sowie News-, FTP- und Demo-Server. Das Intranet mit Domänencontrollern, File- und Produktivservern sowie den Arbeitsplatzrechnern ist in der internen Zone. Die weiteren Bürostandorte in Deutschland: Köln, München und Berlin sind per VPN an das Intranet angeschlossen. Alle Sales-Mitarbeiter arbeiten in ihren Büros auf Notebooks, die über Ethernet-Kabel mit dem Intranet verbunden sind. Sie setzen die MS Office Suite 2003 für Schreibarbeiten und zur Kommunikation ein und demonstrieren die Firmenprodukte RedDot CMS und RedDot XCMS bei Kunden vor Ort unter VMWare.

Regelmäßig finden Treffen der Geschäftsführung mit den Sales-Mitarbeitern aus allen Niederlassungen im Konferenzraum in Oldenburg statt.

Zielsetzung
Das WLAN soll bei Meetings im Konferenzraum in Oldenburg den drahtlosen Zugang zum Intranet ermöglichen. Weiterhin soll in allen Räumen der Zentrale Oldenburg drahtloser Zugang möglich sein, ohne das vorhandene Ethernet abzulösen. Die Administration des WLAN soll ohne Mehr-Aufwand erfolgen.

Notwendige Schritte
Aufbauend auf der vorhandenden Sicherheits-Architektur wird das WLAN in die Firewall integriert und die weitere Zone WLAN in der ISA 2004 Firewall eingerichtet. Aus Sicherheitsgründen wird IPSec über VPN eingesetzt und der Zugang nur tagsüber zu den Bürozeiten erlaubt sein. Um gleichmässig guten Zugang in allen Räumen sicherzustellen, wird zur optimalen Platzierung der Access-Points Ekahau Site Survey eingesetzt.

Wirtschaftlicher Aspekt
Die Projektvorgaben sind es, eine kostengünstige und leicht zu administrierende Lösung zu finden. An der bereits vorhandenen Architektur soll so wenig wie möglich geändert werden. Der Neukauf von Hard- und Software soll auf das notwendigste beschränkt sein.

Meine Aufgaben in diesem Projekt
- Planung des WLAN mit Sicherheitskonzept
- Informationssammlung (Internet, Kataloge, Case Studies...)
- Ermittlung des Hard- und Softwarebedarf
- Vergleich der Hard- und Software und Kaufentscheidung
- Wareneingangskontrolle
- Installation und Einrichtung der WLAN Hard- und Software
- Übergabe und Einweisung
- Dokumentation des Projektes

I.VIII. Genehmigter Projektantrag (Fortsetzung)

Projektablauf

1.	**Projektbeschreibung**	**(2,0h)**
1.1.	Projektumfeld	(0,5h)
1.2.	Kundengespräch mit dem Systemadministrator	(1,0h)
1.3.	Problemstellung und Erteilung des Auftrages	(0,5h)
2.	**Projektplanung**	**(8,0h)**
2.1.	Ist-Analyse	(0,5h)
2.2.	Recherche zu möglichen Sicherheitstechnologien	(3,0h)
2.2.1	Einstufige Sicherheitstechnologien	
2.2.2	Mehrstufige Sicherheitstechnologien	
2.3.	Sollkonzept / Pflichtenheft	(0,5h)
2.3.1	Auswahl von IPSec über VPN und Begründung	
2.4	Projektablaufplan / Terminplan	(2,0h)
2.5.	Kosten-Nutzen-Analyse	(1,0h)
2.6.	Vorstellung des Gesamtkonzeptes	(1,0h)
3.	**Projektdurchführung**	**(15,0h)**
3.1.	Installation der Access Points	(2,0h)
3.2.	Hard- und Software-Konfiguration	(3,0h)
3.2.1.	ISA 2004	
3.2.2.	Access-Points	
3.2.3.	Notebooks	
3.3.	Testlauf	(2,0h)
3.4.	Messung und Auswertung mit Ekahau Site Survey 2.1	(8,0h)
4.	**Projektabschluss**	**(10,0h)**
4.1.	Übergabe des WLAN	(0,5h)
4.2.	Vergleich von Soll- und Ist-Zustand	(0,5h)
4.3.	Anfertigung der Betriebs- und Kundendokumentation	(8,0h)
4.4.	Fazit	(1,0h)
		ges. (35,0h)

I.	**Anhang**
I.I.	Projektablaufplan
I.II.	Konfiguration des WLAN
I.III.	Testergebnisse von Ekahau Site Survey 2.1
I.IV.	Glossar
I.V.	Quellenverzeichnis

I.VIIII. Bestätigung der Ausbildungsfirma und Eidesstattliche Erklärung

Prüfungsteil A

Prüfling (private Anschrift):

Rolf Hechtenberg
Brookweg 183
26127 Oldenburg

Ausbildungsbetrieb:

RedDot Solutions AG
Industriestrasse 11
26122 Oldenburg

Bestätigung über durchgeführte Projektarbeit

Ausbildungsberuf:	Fachinformatiker / Systemintegration
Projektbezeichnung:	Planung und Installation eines WLAN
Projektbeginn:	21.03.2005
Projektfertigstellung:	25.03.2005
Zeitaufwand in Std.:	35

Bestätigung der Ausbildungsfirma:

Wir bestätigen, dass der/die Auszubildende das oben bezeichnete Projekt einschließlich der Dokumentation im Zeitraum vom 21.03.2005 bis 25.03.2005 selbständig ausgeführt hat.

Projektverantwortliche(r) in der Firma:

_____

Vorname Name Telefon Unterschrift

Ausbildungsverantwortliche(r) in der Firma:

_____

Vorname Name Telefon Unterschrift

Eidesstattliche Erklärung:

Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbständig erstellt habe.

Oldenburg, _____, Unterschrift des Prüflings:_____