

Kurzbeschreibung



Arbeitstitel:	Abwehr von internen und externen Netzwerkattacken	
Fachgebiet:	Kommunikation	
Studenten:	Roland Beeler	mailto:roland.beeler@redit.ch
	Valentin Tanner	mailto:valentin.tanner@kbsg.ch
Dozent:	Prof. Dr. Bernhard Hämmerli	mailto:bmhaemmerli@hta.fhz.ch
Stichworte:	Sicherheit, Firewall, VPN, Attacken, Netzwerk	

Kurzfassung der Aufgabenstellung

Verschiedene Schutzmechanismen sind zu dokumentieren und zu testen. Sicherheitsmassnahmen in den untenstehenden drei Bereichen werden untersucht und in einem Testnetzwerk implementiert und überprüft.

Desktop-Firewall

Desktop-Firewalls werden bei einzelnen Rechnern im Firmennetz oder bei privaten Arbeitsstationen für die Überwachung und für den Schutz gegen externe Angriffe eingesetzt. Desktop-Firewalls kontrollieren den Datenverkehr und können den Zugriff auf Ressourcen erlauben oder verbieten.

Die Desktop-Firewalls (Norton Personal Firewall und NAI Data Security Suite) sind in der für die Diplomarbeit aufgebauten Testumgebung zu installieren und anhand eines Funktionsvergleichs auf Schwachpunkte zu analysieren. Beispielkonfigurationen sind zu erarbeiten und deren Vor- und Nachteile aufzuzeigen.

Verschlüsselung

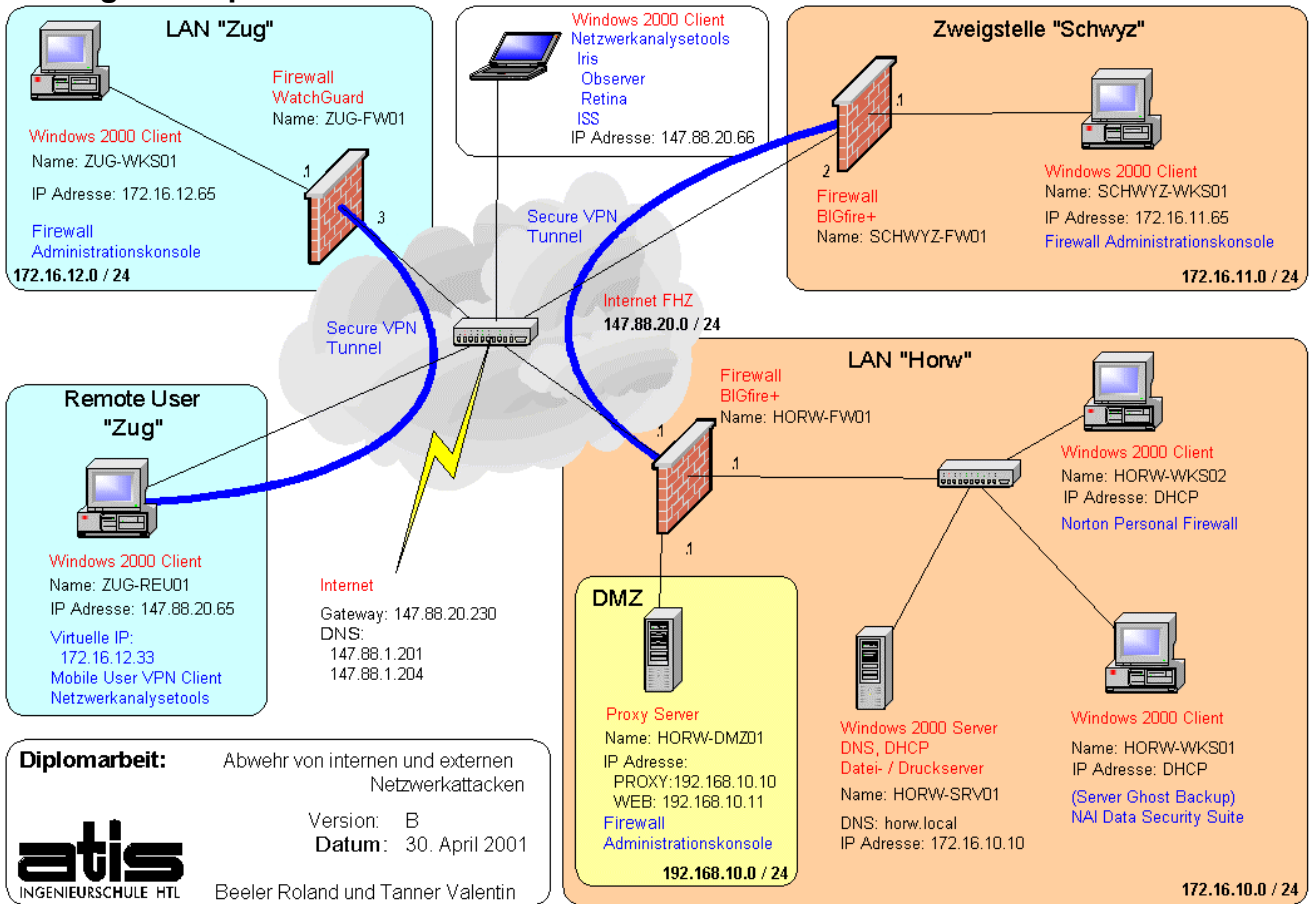
Mit Hilfe von Verschlüsselung wird eine sichere Verbindung zwischen einem Netzwerk und seinem Zweigstellennetz realisiert. In einem zweiten Aufgabenteil wird eine geschützte Verbindung zwischen einem mobilen Benutzer und seinem Netzwerk umgesetzt.

Anhand dieser beiden Verbindungen sind mögliche Keymanagementverfahren zu studieren.

Schutzkonzept

Im theoretischen Teil sind Schutzmassnahmen als Teile eines umfassenden Schutzkonzeptes zusammenstellt. Anhand von Fallbeispielen werden Schutzmassnahmen punktuell erläutert und im Testnetzwerk implementiert und bewertet.

Lösungskonzept



Desktop-Firewall

Die Theorie über Desktop-Firewalls und deren praktische Anwendung wurde überblicksartig erarbeitet. Mit den gewonnenen Erkenntnissen wurde je ein Beispiel für Firmennetzwerke und Einzelarbeitsstationen definiert. Die Fallbeispiele wurden in einer Testumgebung implementiert und mit Scannern und Mitteln aus Windows auf ihre Wirksamkeit überprüft.

Verschlüsselung

Durch das Studium von möglichen Datenverschlüsselungen und Schlüsselverwaltungssystemen wurde ein Überblick über die zur Zeit vorhandenen Algorithmen und Keymanagementverfahren gewonnen. Anhand dieses Überblickes konnte der Umfang und die Einsatzmöglichkeit der zur Verfügung stehenden Hard- und Software ermittelt und die Arbeitsbereiche im Testnetzwerk festgelegt werden.

Schutzkonzept

Durch das Studium der Theorie-Dokumente „Informationssicherheit Firewall“ von Prof. Dr. B. Hämmerli und Microsoft TechNet „Sicherheits-Planung“ wurde ein Theoriedokument zur Erstellung von Schutzkonzepten erarbeitet. Mit diesem Know-How wurden die Fallbeispiele „Schutz durch Sicherheitsrichtlinien“ sowie „Schutz durch Technologien“ erstellt. Das Fallbeispiel „Schutz durch Technologien“ wurde in der Testumgebung umgesetzt.

Konkrete Ergebnisse

Desktop-Firewall

Die Desktop-Firewalls wurden auf Arbeitsstationen installiert und so konfiguriert, dass ein Login an die Windows 2000 Domäne mit Active Directory, entgegen Aussagen von Microsoft, erfolgen konnte.

Verschlüsselung

Im Testnetzwerk wurde eine Punkt-zu-Punkt Verbindung über das öffentliche Internet erstellt, deren Daten von den Endgeräten automatisch chiffriert, bzw. dechiffriert wurden. Eine weitere Variante für mobile Teilnehmer wurde im Testnetzwerk erfolgreich umgesetzt.

Schutzkonzept

Die in der Aufgabenstellung 2.3 definierten Ziel wurden erreicht.

Projektverlauf

Vorprojekt

In der ersten Phase wurde die ganze Testumgebung eingerichtet und einer kurzen Funktionskontrolle unterzogen. Dadurch wurde gewährleistet, dass in den folgenden Phasen Schutzmechanismen implementiert und getestet werden konnten.

Die Aufgabenstellung wurde analysiert und die Ziele konkretisiert.

Desktop-Firewall

Ein Überblick über Schutzmöglichkeiten von Desktop-Systemen wurde mit einem kurzen Studium über Desktop-Firewalls geschaffen. Danach wurden die Produkte Norton Personal Firewall und NAI Data Security Suite auf Arbeitsstationen der Testumgebung installiert und konfiguriert.

Die Verwendung einer Desktop-Firewall in einem Netzwerk zeigte sich als Knacknuss, denn Sicherheit bzw. Schutz schränkt die Freiheit ein. Dieses konträre Verhalten widerspiegelte sich bei der Konfiguration der Desktop-Firewalls im Zusammenhang mit der Windows 2000 Authentifizierung im Netzwerk.

Verschlüsselung

Bei der Punkt-zu-Punkt Verbindung wurde beim Datentransfer zwischen den beiden Netzwerken ein Performanceverlust festgestellt. Eine Problemanalyse ergab, dass eine Neuaufteilung der IP- Pakete diesen Performanceverlust verursachte. Nach der Umkonfiguration des Netzwerkes konnte das Problem behoben werden, ohne die Performanceverluste bis ins letzte Detail zu analysieren.

Schutzkonzept

Das Studium von Schutzmassnahmen und Gefahren beanspruchte viel Zeit. Die Arbeit war aber nötig, um sich in die für uns neue Thematik „Schutzmassnahmen“ einzuarbeiten.

Ein Web-Server wurde mit Firewalltechnologie gegen interne und externe Attacken abgesichert. Beim Schutz des Web-Servers wurden Gegensätze bezüglich Client- und Serverschutz festgestellt.

Diese Gegensätze wurden mit verschiedenen Kompromisslösungen beseitigt.

Ein sicherer Internetzugang konnte mit Hilfe eines Applicationgateways realisiert werden.

Die implementierten Schutzfunktionen wurden durch die Netzwerksicherheitstools (ISS und Retina) gegen Angriffe geprüft.

Schlusswort

Sicherheit und Schutz stehen gegensätzlich zur Freiheit, denn: „Sicherheit muss weh tun“. Allzu oft werden durch Bequemlichkeit oder Unwissenheit Sicherheitsmassnahmen unterlassen oder zuwenig durchgesetzt. Auch das beste, luxuriöseste Produkt bietet nicht die erhoffte Sicherheit, wenn es fehlerhaft konfiguriert ist und selten gewartet wird. Im Gegenteil, es verursacht ein falsches Sicherheitsgefühl.

Die Anschaffungskosten der Hard-/Software sowie der Aufwand für die Konfiguration sollen sich in etwa die Waage halten.

Leider werden oft in der Literatur und in Standardkonfigurationen Firewalls so konfiguriert, dass vom sicheren, internen Netzwerk nach aussen in das unsichere Netzwerk alles erlaubt wird und nur von aussen nach innen gewisse Dienste gesperrt werden. Dies öffnet Programmen mit verborgenen Funktionen (Trojaner) den Kommunikationsweg von innen nach aussen.

Verschlüsselte Datenkommunikation wird in Zukunft massgebend sein, um somit das Arbeiten mit vertraulichen und aktuellen Daten von beliebigen Orten zu ermöglichen, sei es von zu Hause „privat“ oder von „öffentlichen Plätzen“ aus.

Ausblick

Das Schützen von IT- Ressourcen beinhaltet einen sehr grossen Themenbereich. In dieser Arbeit wurden gewisse Teilbereiche angeschnitten. Im weiteren könnten verschiedene Gebiete genauer analysierte werden wie:

Schlüsselmanagement für Grosssysteme mit mehreren tausend Benutzern

Schutzkonzepte für konkrete IT- Infrastrukturen

Schutztechnologien für weitere wichtige Internet Ressourcen wie Mail, Datei- Datenserver,...