**Aufgaben Blockwoche vom 05.05.2014 - 08.05.2014**

**Betriebssysteme:** 2 x Windows Server 2008 R2 Standard  
 1 x Ubuntu Server  
 1 x Windows 7 Client

**Allgemeine Anforderungen:**

Alle Konfigurationen müssen dokumentiert werden.  
Ein kompletter Netzwerkplan muss in der Dokumentation enthalten sein.  
Nach einem Stromausfall muss das Netz wieder vollständig von selbst funktionieren!  
Stammzertifikate der Domäne werden von einer zentralen Stelle zur Verfügung zertifiziert.

**Netzwerk und Firewall Anforderungen:**

Ihre Firma hat zwei getrennte Netze für Client-Rechner. Im Netz "Produktion" sind die Rechner der Produktionsstätten. Im Netz "Verwaltung" sind alle anderen Client-Rechner (Sekretariat, Buchhaltung, Führungskräfte, Planer, Zeichner)  
Server die nicht direkt aus dem Internet erreichbar sein sollen sich in einem eigenen Netz befinden.  
Alle aus dem Internet erreichbaren Server sollen sich in einem eigenen Netz (DMZ) befinden.  
Die Firewall wird zweistufig aufgebaut. Eine Firewall (Perimeter) sichert die DMZ gegen das Internet ab. Diese Firewall übernimmt auch das NAT für die internen Netze. Eine zweite Firewall sichert die DMZ gegen die restlichen Netze ab. Auf dieser Firewall erfolgt kein NAT. Auf den Firewalls sollen nur die notwendigsten Dienste erlaubt werden!!!  
Rechner der Verwaltung haben vollen Internetzugriff (http und https)  
Rechner der Produktion haben nur Zugriff auf die internen Internetseiten. Zugriffversuche nach extern sollen auf eine Website verweisen auf der die Mitarbeiter auf die Sperre des Internetzugriffs hingewiesen werden sollen. Ihnen steht das Subnetz 192.168.1.0/24 zur Verfügung. Dieses Netz muss auf Subnetze aufgeteilt werden. Dabei ist zu beachten:  
Im Produktionsnetz sind min. 60 IP-Adressen für Hosts vorzusehen  
Im Verwaltungsnetz sind min. 50 IP-Adressen für Hosts vorzusehen  
Im Servernetz sind min. 20 IP-Adressen für Hosts vorzusehen  
In der DMZ sind min. 10 IP-Adressen für Hosts vorzusehen  
Jedes Netz soll möglichst klein gehalten werden um eventuell noch freie IPs für zukünftige Netze zu haben. Der Default-Gateway hat immer die 1. Host-IP im jeweiligen Subnetz

**Serverdienste:**

Active Directory  
Microsoft Exchange  
DHCP-Server  
Fileserver  
Webserver

**Details Active Directory:**

Active Directory übernimmt die Benutzerverwaltung  
Benutzer der Verwaltung sollen sich an allen Rechnern anmelden können. Benutzer der Produktion nur an den Produktionsrechnern.  
Wenn sich Benutzer an Verwaltungs-Rechnern anmelden sollen ihre eigenen Dokumente auf eine Freigabe am Server umgeleitet werden auf die nur sie und Administratoren Zugriff haben.  
Die Homepage ihrer Firma soll als Startseite im Internet-Explorer festgelegt werden.

**Details Webserver:**

Die öffentliche Website ihrer Firma wird ein CMS in ASP.NET sein. Sie soll als www.gruppe2.at erreichbar sein. Da es bis zum umsetzen dieses CMS noch etwas dauern wird erstellen sie eine Seite die Besucher auf diesen Umstand hinweist.  
Des Weiteren wird ihren Kunden eine Website zur Auftragsverwaltung zur Verfügung gestellt. Diese Seite soll als "kunden.gruppe2.at" erreichbar sein. Zur Sicherheit wird der Zugriff auf diese Seite SSL verschlüsselt. Stellen sie auch hier eine Infoseite zur Verfügung dass dieser Dienst bald erreichbar sein wird. Die Kundenseite wird auf einem Apache Webserver installiert.  
Damit OWA nicht direkt aus dem Internet erreichbar ist, soll einer ihrer Webserver in der DMZ als Reverse-Proxy für OWA dienen.  
Nach dem installieren des Stammzertifikates ihrer Firma sollen alle SSL-Seiten ohne Fehlermeldung aus dem Internet erreichbar sein.

**Details Microsoft Exchange**

Als Groupware-Lösung kommt Microsoft Exchange zum Einsatz.  
Es gibt zwei Besprechungsräume in der Firma. Diese sollen über Exchange gebucht werden können. Dabei sollen doppelte Belegungen verhindert werden.

**Details DHCP-Server**

Alle Clients der Firma sollen ihre IP-Adresse per DHCP beziehen.  
Die Lease-Time soll auf eine Stunde gesetzt werden um rascher auf Netz-Änderungen reagieren zu können.  
Clients sollen aber immer die gleiche Adresse zugewiesen bekommen um Rechner, die Probleme verursachen, leichter feststellen zu können.

**Details File-Server**

Es soll ein Bereich geben auf den alle Firmenmitarbeiter Lese-Zugriff haben. Aber nur Mitglieder der Gruppe "Dokumentenadmins" dürfen Änderungen an Dokumenten vornehmen. Der Speicherplatz dieser Freigabe darf 150 MB nicht übersteigen.  
Es soll einen Bereich geben auf den nur das Sekretariat und die Führungskräfte der Firma Zugriff haben. Der Speicherplatz soll nicht begrenzt werden doch soll die Gruppe der Führungskräfte per Mail darauf hingewiesen werden sobald mehr als 200 MB Speicherplatz belegt sind.  
Es soll einen Bereich geben in den die Zeichner ihre Pläne für die Produktion ablegen können. Die Produktion darf diese Pläne aber nicht verändern können. Hier sollen maximal 120 MB Speicherplatz belegt werden können. Wenn aber mehr als 80 % belegt sind sollen die Zeichner darüber informiert werden. Weiteres soll das Speichern unerwünschter Dokumente wie Bilder, Musik, .... verhindert werden.   
Für jeden Benutzer der Verwaltung soll ein Bereich existieren in dem seine eigenen Dokumente gespeichert werden. Diese sollen ihm auf jedem Rechner der Verwaltung zur Verfügung stehen - nicht aber wenn er sich an einem Rechner der Produktion anmeldet!! Der Speicherplatz soll hier auf 80 MB beschränkt werden. Der Benutzer wird bei 75% und 90% per Mail gewarnt. Der Administrator bei 95% per Mail informiert. Weiteres wird dies in den Logfiles eingetragen.  
Alle Daten am Fileserver sollen regelmäßig gesichert werden. Dabei sollen jeden Tag nur die Änderungen gesichert werden und am Wochenende die gesamten Daten.

**Details Druck-Server**

Gedruckt soll über einen zentralen Druckserver werden.  
Wenn es sich bei dem Drucker um einen Farbdrucker handelt soll dieser auch als Schwarz/Weis Drucker zur Verfügung gestellt werden. Rechner im Produktionsnetz bekommen als Standard den Schwarz/Weis Drucker zur Verfügung gestellt werden. Rechner im Produktionsnetz bekommen als Standard den Schwarz/Weis Drucker installiert und den Farbdrucker als zusätzlichen Drucker. Im Verwaltungsnetz ist es umgekehrt.  
Druckaufträge des Sekretariats sollen allen anderen Druckaufträgen vorgezogen werden.  
Ein zentraler PDF-Drucker soll allen Benutzern des Verwaltungsnetztes zur Verfügung stehen.  
Gedruckte PDFs sollen in den Eignen Dateien der Benutzer im Ordner "PDFs" abgelegt werden.

Ende der Aufgaben

Nun werden die Aufgaben bearbeitet!

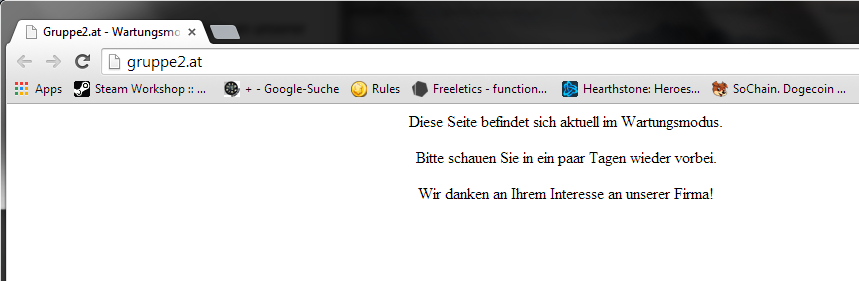
**Active Directory**

Wie wir AD installieren haben wir schon in anderen Blockwochen gelernt daher verweisen wir hier auf das vorherige Blockwochenprotokoll.

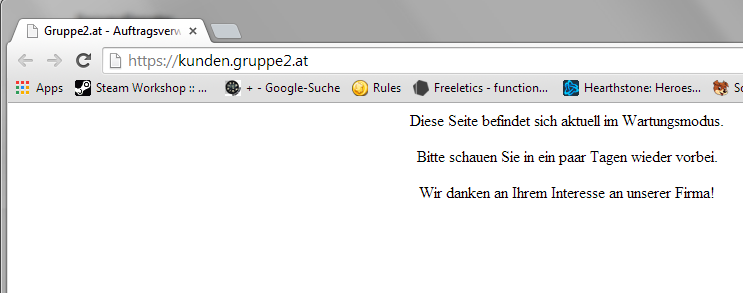
**Webserver**

Zu installieren: IIS

Es ist eine Wartungsseite zu erstellen da es für die Erstellung des CMS noch einige Zeit dauern wird.  
Dies ist nötig, dass die Kunden Information haben was mit der Homepage los ist und wie lange sie sich noch im Wartungsmodus befindet (In unserem Beispiel haben wir keine Zeit angegeben.).

Wartungsseite:   


Nun ist es noch unsere Aufgabe eine Auftragsverwaltungsseite für unsere Kunden zu erstellen welche durch SSL verschlüsselt wird. (https://..)



**Firewall**

Wir setzen eine Ubuntu-Firewall in unserem Netzwerk auf. Dazu installiert man entweder Ubuntu (mit grafischer Oberfläche) oder Ubuntu-Server (ohne grafischer Oberfläche).   
  
Sobald man dies installiert hat kann man, sofern man root Rechte hat, die Firewall konfigurieren. Es wird empfohlen zuerst einmal den Speicherort der Konfiguration zu überprüfen/testen. Im normalfall liegt diese unter /etc/iptables/rules.v4 [für TCP/IPv4] oder /etc/iptables/rules.v6 [für TCP/IPv6]. Da die Firewall-Einstellungen ohne korrekte Sicherung nach jedem reboot gelöscht wird sollte man diese mit dem Befehl „iptables-save > /etc/iptables/rules.v4“ speichern.

Um eine rule zu erstellen benötigt man den Befehl

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

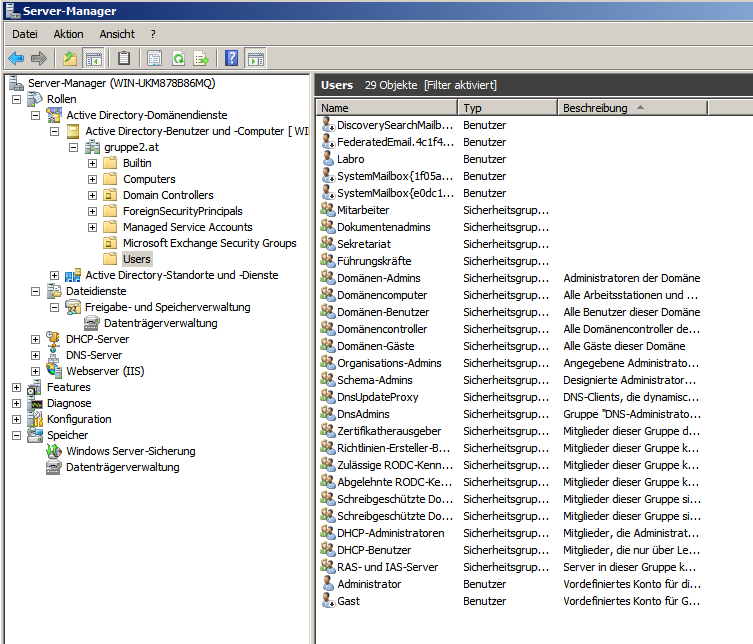
Bei –A fügt man die entsprechende Chain ein (FORWARD; INPUT; OUTPUT). Je nachdem in welche Chain man die Rule einträgt bedeutet sie etwas anderes. FORWARD bedeutet das es weitergeleitet wird, sprich erlaubt wird. INPUT bedeutet das die Verbindung eingehen kann, allerdings nicht wieder raus. OUTPUT ist das Gegenteil von INPUT.

-p steht für Protocoll. Es gibt UDP und TCP. Um asoziieren zu können welcher Port auf welchem Protocoll läuft schlägt man am besten den entsprechenden Port im Internet nach.

--dport steht für den eigentlichen Port. Z.B. um auf HTTP zugreifen zu können muss man den Port 80 öffnen da dieser dafür zuständig ist.

[Source für Ports: http://de.wikipedia.org/wiki/Liste\_der\_standardisierten\_Ports]

Fileserver (mit AD gemanaged)



Hier haben wir verschiedene Gruppen wie „Führungskräfte“ erstellt in welcher dann unser Benutzer „Labro“ hinzugefügt wird und alle Rechte die der Gruppe „Führungsrechte“ vergeben wurden besitzt.

Nun mussten wir nur noch Ordnerstrukturen erstellen und diese für die jeweiligen Gruppen freigeben. Dies hat alles ohne Probleme funktioniert.