# Aufgabenstellung

Wir (Alexander Halbarth, Onur Tuncel und ich) hatten die Aufgabe, ein Security-Konzept zu entwerfen und anschließend eine Cisco ASA-5510 zu konfigurieren, um diese Security-Richtlinien auch umzusetzen.

# Das Security-Konzept

Am Anfang haben wir uns in einem eigenen Dokument die wichtigsten Richtlinien hinsichtlich Security überlegt.

Dieses Dokument beinhaltet:

* Einteilung der gesamten User in Untergruppierungen, die jeweils unterschiedliche Rechte haben
* Passwort-Policies
* Definition von Empfehlungen der VLAN-Planung
* Anregungen von uns an die Teams, welche Services benutzt werden könnten, um die bestmögliche Sicherheit zu garantieren
* Überwachungsempfehlung an die anderen Teams

## Usergruppen

Um die bestmögliche Nutzung des Netzes zu gewährleisten, haben wir uns überlegt, die User innerhalb der Firewalls in einzelne „Gruppen“ einzuteilen, die allesamt unterschiedliche Rechte haben.

Folgende Gruppen haben wir definiert:

* Standarduser
* Netzwerkadministratoren
* Applikationsadministratoren
* Gäste

## Standarduser

Die Gruppe der Standarduser ist eine generische Gruppe, die folgende Berechtigungen aufweist:

1. Zugang zum Internet, mit eventueller Möglichkeit, nach der erfolgreichen Implementierung einige Domains, die als schädlich bekannt sind, per DNS-Einträgen nicht verfügbar zu machen
2. Zugang zum firmeneigenen Intranet zur Verwaltung von firmeninternen Prozessen
3. Möglichkeit, E-Mails per SMTP bzw. POP3 zu verschicken bzw. zu empfangen
4. Fileservice-Zugriffe (z.B. SFTP), die natürlich abgesichert sein sollen
5. Loginmöglichkeit im Active Directory® nach Zuweisung eines geeigneten Accounts

## Netzwerkadministratoren

Netzwerkadministratoren sind (wie der Name schon sagt) hauptsächlich für die Administration des Netzwerks (sprich: der Konfiguration der Hardware) verantwortlich.

Diese Gruppe hat grundsätzlich dieselben Berechtigungen wie die Gruppe der „Standarduser“.

Sie haben zusätzlich allerdings die Berechtigung, via SSH-Verbindungen die Netzwerkgeräte zu konfigurieren.

Auf diesen Netzwerkgeräten würden wir auch eine lokale Datenbank empfehlen, mit der sich die Netzwerkadministratoren zusätzlich auf den Geräten (Routern, Switches) authentifizieren müssen – dies ist allerdings nicht verpflichtend umzusetzen.

## Applikationsadministratoren

Applikationsadministratoren sind für die Applikationen sowie die Administration der ganzen Server innerhalb des Netzwerks verantwortlich.   
Beispiele: Fileverwaltung auf einem Server, E-Mail-Server-Verwaltung

Grundsätzlich hat auch diese Gruppe dieselben Berechtigungen wie die Gruppe der „Standarduser“.

Zusätzlich bekommen sie die Freigabe für SSH, Microsoft RDP und VNC. Mit diesen Protokollen können sämtliche Server im Netzwerk administriert werden.

Für die Administration vom Active Directory® bekommen sie selbstverständlich auch dort nach erfolgreicher Authentifizierung Admin-Rechte.

## Gäste

Die Gruppe der „Gäste“ ist die einzige der vier existierenden Gruppen, die nicht von der Gruppe „User“ die Rollen übernimmt. Diese Gruppe ist für firmenexterne Gäste vorgesehen, deren Vertrauenswürdigkeit nicht gewährleistet werden kann.

Sie haben Zugriff auf das Intranet, auf das Internet gewähren wir nur sehr begrenzt Zugriff. Wir haben einige Domains definiert, die wir als „vertrauenswürdig“ betrachten und auch freigeben, da von diesen Domains im Regelfall keine Viren ausgehen. Alle anderen Domains werden per DNS-Locking gesperrt und sind für die normalen User nicht zugreifbar. In späterer Entwicklung ist auch eine IP-Adresssperre angedacht, diese werden wir aber aufgrund der nicht verfügbaren Ressourcen noch nicht umsetzen.

Folgende Domains sind von uns vorerst als „vertrauenswürdig“ definiert:

|  |  |  |
| --- | --- | --- |
| http://www.wikipedia.org/ | http://www.amazon.de/ | http://www.youtube.com/ |
| http://www.google.com/ | http://www.google.at/ | http://www.google.de/ |
| http://www.facebook.com/ | http://www.xing.com/ | http://www.ebay.com/ |
| http://www.ebay.de/ | http://www.orf.at/ | http://www.twitter.com/ |

Diese Liste wird schrittweise im Betrieb erweitert.

## Passwort-Richtlinien

Um die bestmögliche Sicherheit zu gewährleisten, haben wir für sämtliche Passwörter Richtlinien definiert, die eingehalten werden müssen.

Folgende Richtlinien gelten für Passwörter:

* Jedes Passwort muss mindestens einen Großbuchstaben enthalten
* Jedes Passwort muss mindestens einen Kleinbuchstaben enthalten
* Jedes Passwort muss mindestens eine Zahl enthalten
* Jedes Passwort muss mindestens eine Länge von 8 Zeichen haben

## Vorschlag für VLANs

Als Vorschlag für die Gruppe, die die VLANs erstellt und verwaltet, haben wir eine Liste mit VLANs ausgearbeitet, die die User in eben diese Gruppen einteilt.

Daher wären die VLANs von unserer Seite:

* Server (jeder Server ist hierbei in einem eigenen VLAN)
* Netzwerkadministratoren
* Applikationsadministratoren
* Standarduser
* Gäste

## Empfehlungen für benutzte Services

Genauso wie mit den VLANs haben wir eine Liste mit Services ausgearbeitet, die hinsichtlich der Sicherheit sinnvoll wären. Weil wir allerdings nicht die Aufgabe haben, diese Services zu implementieren, ist diese Liste auch nur ein Vorschlag.

Folgende Services bzw. softwaretechnische Richtlinien sind von unserer Seite aus empfohlen:

* Jegliche Kommunikation, die normalerweise über Telnet funktioniert, soll über abgesicherte bzw. verschlüsselte Verbindungen realisiert werden (z.B. SSH)
* Dateiübertragungen sind auch immer verschlüsselt zu realisieren, d.h. statt FTP sollte SFTP verwendet werden.
* Telefone dürfen auch TFTP verwenden, wenn keine andere Möglichkeit besteht
* Mailkommunikation sollte auch immer verschlüsselt erfolgen
* Zur Sicherheit darf in den lokalen Netzen kein OSPF verwendet werden – auch Routing updates dürfen nicht ins lokale Netzwerk kommen, um es nicht unnötig zu belasten
* Nach Möglichkeit sollte auch die Kommunikation zwischen den Routern verschlüsselt werden
* Für den Zugriff zum Internet sollte auch eine ACL verwendet werden, um unvorteilhafte Domains zu sperren

## Überwachungsempfehlung

Auf Anfrage des Teams, das die Überwachung betreut, haben wir eine Liste ausgearbeitet, was (von unserer Seite) überwacht werden soll.

Wir haben folgende Aktionen zur Überwachung veranlasst:

* Sämtliche Auslastungen von Netzwerkkomponenten, um stets eine Übersicht zu behalten
* Verdächtiger Traffic innerhalb des Netzwerks
  + Unverhältnismäßig viele pings, DHCP- oder DNS-Aufrufe
  + http-requests, um den Internet-Traffic zu überwachen
* Wenn interfaces an Netzwerkgeräten ausgeschaltet werden
* Sämtliche Adminuser-Aktivitäten
* Beim Herunterfahren von Servern, bzw. wenn die Interfaces geändert werden

# Konfiguration der Cisco ASA

Nachdem wir einen Teil der ersten Einheit mit der Beschaffung der Cisco ASA verbracht haben, haben wir mithilfe von den benötigten Werkzeugen (Serial-Adapter sowie zwei Patchkabel) begonnen, die ASA zu konfigurieren.

Wir mussten (und müssen) auf das genaue IP-Adresskonzept warten, da wir ohne IP-Adressen keine Security implementieren können. Wir haben uns wohl eine Grundkonfiguration überlegt (diese ist beigelegt), konnten diese allerdings nicht praktisch im Projekt umsetzen. Wir werden uns jetzt auf die Konfiguration in einem Testsystem innerhalb des Cisco Packet Tracers® fokussieren, sodass die Sicherheitsrichtlinien wenigstens in der Theorie umgesetzt sind.