Netzwerkpolicy

des

Campus Brigittenau

(03/2010)

Kontakt
Referat für Netzwerktechnik
Tel.: +43 (0)1 33109 10 8010
E-Mail: network@campusbrigittenau.at

Geltungsbereich der Networkpolicy:

Die Networkpolicy des Referats für Netzwerktechnik Campus Brigittenau findet Geltung sobald ein netzwerkfähiges Gerät an das Netzwerk des Campus Brigittenau angeschlossen ist.

1.) Voraussetzungen und Vorbereitung

Software:

Jedes Betriebssystem, das über einen IPv4 Stack verfügt(IPv6 ist derzeit in Vorbereitung), ist verwendbar. Beispiele: Windows 2k, XP, 2k3, Vista, Windows 7, Linux 2.x, aktuelle Versionen von MacOS, BeOS, FreeBSD sowie verschiedene Linux-Live-CD (alles erfolgreich getestet). Wenn die Konfiguration im Einklang mit der Policy ist, darf eine beliebige Anzahl beliebiger Betriebssysteme benutzt werden.

Hardware:

Eine Netzwerkkarte mit 10/100BaseT (10/100/1000Mbit/s RJ-45 Anschluss), die vom benutzten Betriebssystem unterstützt wird und ein twisted-pair cat5 (cat5e, cat6) Kabel sind notwendig.

Netzwerkkarteneinkauf kann mit einem Administrator besprochen werden. Netzwerkkabel (5m) gibt es im Computerreferatsbüro zu kaufen.

Obwohl es in jedem Zimmer 2 Buchsen gibt, ist nur eine aktiv, meistens die linke (beschriftet). Ausnahmen: Zweibettzimmer. Man kann die aktive daran erkennen, ob bei der Netzwerkkarte die LED "Link" leuchtet wenn man sie mit der richtigen Buchse verbindet.

Wie geht's weiter?

Damit man Zugriff auf das Netzwerk/Internet erhält, muss der Computer im Computerreferatsbüro registriert werden, wobei Zimmernummer, Vor- und Nachname und Emailadresse sowie MAC-Adresse des Computers mitzuteilen sind.

Ohne Registrierung ist der Zugriff auf das LAN beschränkt und man kommt nicht ins Internet. Jeder Zimmerwechsel und Netzwerkkartenwechsel ist unverzüglich zu melden.

Für die einfache Benutzung des Internets ist ein Instandhaltungsbetrag von EUR 5 an die Heimvertretung zu bezahlen. Nähere Informationen in den FAQ (http://www.panorama.sth.ac.at).

2.) Dienste

Den Benutzern werden zur Verfügung gestellt:

- 1 IP Adresse aus dem lokalen IP-Pool pro Computer
- 1 DNS Eintrag ("Hostname") für das lokale Netz pro Computer
- Bei Bedarf ein IMAP/SMTP Account (Email) auf unserem Mailserver (vorname.nachname@campusbrigittenau.at)

Allgemein wird zur Verfügung gestellt:

- Standard Sicherheit im Netzwerk (Firewall, Blacklist)
- Öffentliches Verzeichnis (SMB, HTTP) mit aktuellen Patches, Bug fixes, Antivirenprogrammen, Free- und Shareware und Linux-Distributionen.
- Mailserver (IMAP, POP3, SMTP, SSL)
- Portal mit Forum, Wiki, etc., das über wichtige Ereignisse informiert (http://www.campusbrigittenau.at)
- IRC Forumschat
- VoIP (http://voip.campusbrigittenau.at)

Bitte beachten:

- Wenn man im Zimmer mehrere Rechner an das Netzwerk anschließen will, stehen 3 Möglichkeiten zur Verfügung: Router (auch wireless) oder eigener HUB/SWITCH. Diese sind erlaubt, dürfen jedoch den ordentlichen Netzwerkbetrieb nicht stören. Eine Installation/Konfiguration muss mit einem Netzwerkadministrator besprochen werden.

Die folgenden Einstellungen dürfen von den vorgegebenen nicht abweichen:

- DHCP (IP automatisch beziehen) muss aktiviert sein.
- Andere Einstellungen müssen mit einem Netzwerkadministrator besprochen werden!

3.) Verhalten vom Benutzer

Jede Benutzer ist für sämtliche Aktivität an seinem Netzwerkanschluss selbst verantwortlich.

*Die Benutzer dürfen **KEINE** von den folgenden Diensten (Server) betreiben, weil diese den ordentlichen Netzwerkbetrieb behindern:*

- DHCP
- BOOTP/RARP
- DNS
- Proxy (e.g. squid, winproxy, wingate) nur zum lokalen Gebrauch!!!, sprich sicher konfiguriert.

- Dienste für Fernwartung/-zugriff wie z.B. ssh, VNC müssen mit einem Passwort geschützt und verschlüsselt sein, d. h. kein einloggen ohne Passwort bzw. keine Accounts ohne Passwort und SSL-Verbindung.

Die Benutzer müssen folgende Dienste für anonymen Schreibzugriff aus Sicherheitsgründen strikt begrenzen (oder wenn nicht unbedingt notwendig ganz unterbinden):

- FTP
- SMB
- NFS

Die Benutzer dürfen folgende Dienste grundsätzlich ohne Einschränkungen zur Verfügung stellen:

- HTTP/HTTPS
- POP3/IMAP4
- SMTP. Sollte SPAM-Filtering unterstützen, Relaying verweigern und unbedingt ordentlich konfiguriert sein.
- Spiele (Quake, StarCraft, …)
- Messenger-Dienste (Skype, ICQ, MSN,…)

Vom Benutzer ist unbedingt zu beachten:

- Wenn ein Dienst verwendet werden soll, der nicht aufgelistet ist muss man sich an die Netzwerkadministratoren wenden (admins@campusbrigittenau.at)
- Wenn ein Dienst betrieben wird, muss darauf geachtet werden, dass die benutzte Software den aktuellen Sicherheitsstandards folgend konfiguriert ist und die aktuellen Bug fixes/Patches installiert sind.
- Es ist verboten, eine TCP/IP Verbindung mit dem Modem aufzunehmen, es sei denn, es ist ein privates Netzwerk, das nicht am Intranet angeschlossen ist, und

Sicherheitsvorkehrungen getroffen wurden. Im Zweifelsfall an einen Netzwerkadministrator wenden!

- Durchführung von illegalen Tätigkeiten (z.B. Warez-Server) gilt als Verstoß gegen die Policy. Es ist untersagt jegliche Art von Peer to Peer Diensten zu betreiben, die zum Zweck des illegalen Datenaustausches dienen.
- Benutzer dürfen eigene SMB-Workgroups und Domänen einrichten. Die Domänen ADMIN, ADMINS und OFFICE sind für das Computerreferat reserviert und dürfen nicht verwendet werden.
- Programme, die keine Server darstellen (keine Dienste zur Verfügung stellen), dürfen grundsätzlich ohne weitere Begrenzung ausgeführt werden, wenn sie sonst gegen keine Anordnungen der Policy verstoßen.
- Benutzer müssen ihre(n) Rechner regelmäßig auf Viren überprüfen. Aktuelle Software und Virendatenbanken werden von den Administratoren zum Download zur Verfügung gestellt. Ebenfalls müssen regelmäßig Betriebssystem-Updates (alle wichtigen Updates und Security Patches) durchgeführt werden.
- Benutzer dürfen Firewalls und Portscanschutz verwenden, sofern sie damit den ordentlichen Netzwerkbetrieb nicht stören und keinen Schaden bei anderen Benutzern verursachen. Sofern man einen Portscanschutz (z.B. Firewall) benutzt, wird man von der globalen Sicherheit ausgeschlossen und darf nicht mit Hilfe von Administratoren rechnen, falls Sicherheitsprobleme auftreten.
- Benutzer dürfen keine Portscans und ähnliche Tätigkeiten ausführen.
- Benutzer dürfen keine defekten Netzwerkkomponenten verwenden. Benutzer dürfen die Leitungen (sowohl interne als auch die für die Internetverbindung) nicht unangemessen belasten, auch wenn sie nur erlaubte Tätigkeiten ausführen.
- Beim Auftreten von Sicherheitslücken sind umgehend das Computerreferat und der Eigentümer zu informieren. Weiters ist es verboten Daten zu beschädigen, kopieren oder zu verteilen.
- Auf das österreichische Recht wird ausdrüchlich hingewiesen; Benutzer die gegen dem österreichischen Recht vestoßen werden umgehend gesperrt. Bei Anfrage von Behörden ist der Referat verpflichtet die Daten von Benutzer die rechtswindig handlen weiterzuleiten.
- Bei zu hohem Traffic (4GB Upload/24h; 8GB Upload/72h) wird der Benutzer für 72h gesperrt. Ausnahmen müssen vor dem Upload mit den Administratoren besprochen werden.

4.) Konsequenzen bei Verstößen gegen die Netzwerkpolicy

Ein Verstoß gegen die Netzwerkpolicy kann zur Kündigung des Heimplatzes führen. Weiters behält sich die Netzwerkadministration vor eine Strafgebühr in Höhe von 50 EUR einzuheben. Desweiteren sind folgende Konsequenzen zu beachten:

Sind im folgenden Abschnitt Verstöße aufgelistet, die bisher in der Policy nicht explizit aufgelistet sind so gelten diese ab hier als Verstoß! Ebenso gelten alle nicht aufgelisteten Aktivitäten im Netzwerk, die einen Ausfall oder eine Beschränkung der zur Verfügung stehenden Dienste in Folge haben, als Verstoß.

Legende:
Fall (1): Einmalig, kurzfristiger Verstoß
Fall (2): Einmalig, längerfristiger (min 1h) Verstoß
Fall (3): Mehrmaliger Verstoß

[*]**Account-Sharing**
(1) 50€, offizielle Verwarnung (beide Zimmer)
(3) Heimplatzverweis (beide Zimmer)

[*]**IP/Mac-Spoofing von Servern**
(1) 50€, offizielle Verwarnung
(2) Heimplatzverweis

[*]**IP/Mac-Spoofing von Mitbewohnern**
(1) Verwarnung
(2) 50€, offizielle Verwarnung
(3) Heimplatzverweis

[*]**DoS-Attack**
(1) Heimplatzverweis

[*]**Switch-Cache-Poisoning**
(1) 50€, offizielle Verwarnung
(2) Heimplatzverweis

[*]**Flooding**
(1) Rechner-Check durch das Computerreferat
(2) Rechner-Check durch das Computerreferat
(3) 50€, offizielle Verwarnung (bei erneutem Auftreten dauerhafte Port-Sperre)

[*]**Server-Attack**
(1) 50€, offizielle Verwarnung
(2) Heimplatzverweis

[*]**Verbotene Dienste ((dns/)dhcp, Bootp/rarp, anonymous-proxy)**
(1)50€, offizielle Verwarnung
(2) Heimplatzverweis

[*]**Ungesicherte Dienste (ssh, smtp, telnet, rlogin, vnc...)**
(1) Offizielle Verwarnung
(2) 50€ Strafe
(3) dauerhafte Portsperre

[*]**SPAM-Versand**
(1) Rechner-Check durch das Computerreferat
(2) 50€ Strafe, Offizielle Verwarnung, Erneuter Rechner-Check durch das Computerreferat
(3) Heimplatzverweis

Nicht aufgelistete Verstöße können von den Administratoren angemessen behandelt werden!

Der Benutzer hat das Recht gegen die jeweilge Sanktion bei der Heimvertretung Einspruch zu erheben.

5.) Verhalten von Administratoren

- Administratoren dürfen offizielle Portscans und Scans auf Sicherheitslücken durchführen um die Sicherheit des Netzwerks und der angeschlossenen Geräte zu überprüfen. Administratoren dürfen bei Verletzungen der Policy dem Benutzer den Zugang auf Port-Ebene sperren (bei schwerwiegenden Fällen auch ohne Benachrichtigung).

- Administratoren dürfen mit Absprache der Heimvertretung und entsprechender Begründung Internet-Seiten sperren.

- Administratoren dürfen auf anonymer Ebene die Netzwerkpakete überwachen und Statistiken sammeln.

- Administratoren dürfen auf anonymer Ebene die Netzwerkhardware überwachen, Statistiken sammeln und gegebenenfalls Portmapping erstellen.