Zum Hauptmenü

Dienste

Unter den Firewalldiensten der mp-Firewall können Einstellungen zum Umgang mit eingehenden E-Mails vorgenommen werden. Weiterhin kann hier der Proxy, die DNS-Einträge und die unabhängige Stromversorgung konfiguriert werden. Hier wird auch der Wartungs- und Update-Zugang zum System eingestellt.

Laufende Dienste

Um Änderungen an den laufenden Diensten vorzunehmen melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>Laufende Dienste* aus. Der Menüpunkt *Laufende Dienste* gibt einen Überblick über die verfügbaren Dienste der mp-Firewall. Über dieses Menü können Dienste gestartet oder gestoppt werden. Weiterhin werden hier Einstellungen zu den Zugangsmethoden zur Firewall eingestellt. Es stehen folgende Dienste zur Auswahl:

Menüpunkt	**Beschreibung**
Ende	Verlassen des Menüs.
—	
Serielle Konsole	Auswahl ob und welche serielle Konsole gestartet wird. Es können die seriellen Schnittstellen ttyS0 (Com1) oder ttyS1 (Com2) ausgewählt werden.
SSH-Fernwartung	Auswahl, ob Secure Shell (SSH) auf den Ports 22 und 22222 gestartet werden soll. Wird ein Fernzugriff auf die Firewall gewünscht, so ist dieser Dienst zu aktivieren.
SSH-Passwortanmeldung	Auswahl ob die Anmeldung per SSH-Passwort auf dem Port 22 erlaubt werden soll. Ist diese Funktion deaktiviert, funktionieren nur die eingetragenen SSH-Keys. Es wird empfohlen, Passwort-Anmeldungen zu deaktivieren, wenn der SSH-Dienst von außerhalb (dem Internet) zu erreichen ist. Auf dem Port 22222 sind Passworte grundsätzlich nicht erlaubt.
DNS-Namensdienst	Auswahl ob der DNS-Namensdienst gestartet werden soll. Ist dieser Dienst aktiviert können Klienten aus dem Netzwerk die mp-Firewall als Nameserver benutzen.
DNS-TXT-Anfragen erlauben	Auswahl, ob über den DNS-Namensdienst TXT-Anfragen erlaubt werden sollen. Standardauswahl ist Nein.
NTP-Zeitserver	Auswahl ob der NTP-Zeitserver gestartet werden soll. Ist dieser Dienst aktiviert können Klienten aus dem Netzwerk die mp-Firewall als Zeitserver benutzen.
Festplatten-Temperatur-Prüfung	Auswahl, ob die Temperatur der Festplatte auf der Statusseite angezeigt werden soll. Manche Festplatten unterstützen diese Sensorik nicht. Bei fehlerhafter Anzeige auf der Statusseite, bitte diese Funktion deaktivieren.

Menüpunkt	**Beschreibung**
Festplatten-Smart-Prüfungen	Auswahl, ob das Ergebnis der Festplatte-Diagnose auf der Statusseite angezeigt werden soll. Allerdings wird diese Sensorik nicht von allen Festplatten unterstützt. Bitte deaktivieren Sie diese Funktion wenn es zu einer fehlerhaften Anzeige auf der Statusseite kommen sollte.
—	
Benutzerschnittstelle	Auswahl ob die Benutzerschnittstelle aktiviert werden soll. Die Schnittstelle ist dann für alle Klienten aus dem internen Netzwerk der Firewall zu erreichen. Über die Benutzerschnittstelle können Benutzer ihr Passwort ändern, E-Mail-Weiterleitungen einstellen, E-Mail-Filterregeln setzen und eine Abwesenheitsnotiz (z.B. bei Urlaub) einstellen.
Port der Benutzerschnittstelle	Port auf dem die Benutzerschnittstelle von den Klienten aus dem internen Netz erreicht werden kann.
Mail-Forwarding durch Benutzer	Einstellungen ob Benutzer eigene Mail-Weiterleitungen einstellen dürfen. Benutzer dürfen nur Weiterleitungen zu einem existierenden Benutzerkonto auf der mp-Firewall einstellen, welcher selber keine Weiterleitung hat. Die Weiterleitung an einen Alias-Namen oder ein Benutzerkonto mit bestehender Weiterleitung ist nicht gestattet.
Mail-Sortierung durch Benutzer	Einstellungen ob Benutzer eine Sortierung für das eigene Mail-Konto einstellen dürfen. Eine Sortierung kann nach verschieden Filtern erfolgen und erfolgt vor der Zustellung auf den jeweiligen Mail-Klienten.
Abwesenheitsnotiz durch Benutzer	Erlaubt es einem Benutzer eine Abwesenheitsnotiz zu erstellen.
—	
POP3/IMAP	Auswahl ob die POP3/IMAP-Dienste gestartet werden.
POP3/IMAP Klartext-Passworte	Auswahl ob die Dienste POP3 und IMAP eine Passwortanmeldung im Klartext erlauben sollen. Das Anschalten dieser Option bedeutet ein Sicherheitsrisiko, jedoch wird die Klartext-Anmeldung von einigen Programmen (Z.B. ältere Versionen von MS-Outlook) gefordert.
IMAP max Verb. / Ben.+IP	Anzahl der gleichzeitigen Verbindungen von einer Benutzerkennung von einer IP-Adresse. Dies dient als Schutz vor ungewollten massenhaften Spamversand.
FTP-Server	Auswahl ob der interne FTP-Server gestartet wird.
Shell-Zugang ftpupload	Auswahl, ob die Benutzerkennung zum Hochladen von Dateien auf den FTP-Server (ftpupload) einen Shellzugang zu den Verzeichnissen des FTP-Servers erhält.
IRC-Server	Auswahl ob der interne IRC-Server (Chat-Server) gestartet wird.
MySQL-Server	Auswahl ob der MySQL-Server gestartet wird.
Lokales MySQL root-Passwort setzen	Setzt das lokale MySQL root-Passwort neu.
IP-Sperren (fail2ban)	Einstellung ob externe IP-Adressen nach mehreren fehlgeschlagenen Anmeldeversuchen gesperrt werden sollen. Es wird empfohlen diesen Dienst anzuschalten, um die Gefahr von "Brute-Force"[1)] Attacken zu minimieren.
IP-Sperren-Mailadresse	E-Mail-Adresse, an die das System Informationen über gesperrte IP-Adressen versendet.
Arpwatch	Auswahl, ob Arpwatch gestartet werden soll.
—	

Menüpunkt	Beschreibung
Nagios-Agent	Auswahl, ob die Firewall von einem Nagios-System überwacht werden darf.
Warntemperatur Festplatte	Festlegung der Festplatten-Temperatur, bei dem im Nagios-System eine Warnmeldung ausgelöst wird.
Kritische Temperatur FP	Festlegung der Festplatten-Temperatur, bei dem im Nagios-System eine Meldung für einen kritischen Zustand ausgelöst wird.
TG-Pro IP für Nagios Test	IP-Adresse eines nach gelagerten TightGate-Pro Servers, welches durch ein Nagios-System mit überwacht werden kann.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Proxies und Proxy-Filter

Wenn ein Klient eine Anforderung an den Webserver sendet oder der Webserver antwortet, ist der erste Part einer solchen Antwort immer ein HTTP Request oder HTTP Response. Als ersten Teil des HTTP Request oder Response sendet der Klient oder der Server einen HTTP Header. Das Request Header Feld erlaubt dem Klienten zusätzliche Informationen über den Request an den Server mitzugeben. Mit der mp-Firewall haben Sie die Möglichkeit, den HTTP-Header Requests einzelne Informationen zu erlauben oder zu verbieten. Damit können Sie z.B. sicherstellen, dass im HTTP-Header keine Informationen über den benutzten Server oder den benutzten User-Agent übertragen werden. Solche Informationen werden von Hackern gerne zur Vorbereitung eines gezielten Angriffs genutzt.

Um Änderungen an den Proxy-Einstellungen vorzunehmen melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>Proxies* aus. Sie haben folgende Konfigurationsmöglichkeiten:

Menüpunkt	Beschreibung
Ende	Verlassen des Menüs.
—	
Squid-HTTP-Proxy	Auswahl, ob der Squid-Proxy für HTTP-Anfragen verwendet werden soll.
Squid3-HTTP-Proxy	Auswahl, ob der Squid3-Proxy für HTTP-Anfragen angewendet werden soll
Erlaubte HTTP-Ports	Auswahl der HTTP-Ports, die über den HTTP-Proxy erreichbar sein sollen.
Erlaubte HTTPS-Ports	Auswahl der HTTPS-Ports, die über den HTTP-Proxy erreichbar sein sollen.
Transparenter HTTP-Proxy	Auswahl ob ein transparenter HTTP-Proxy gestartet werden soll, der alle Anfragen die auf Port 80 an beliebige Adressen gehen auf den HTTP-Proxy umleitet. Hierfür stehen die eingeschalteten Proxys (Squid, Squid3) zur Verfügung. Dieser Dienst wird nur gestartet, wenn der HTTP-Proxy gestartet ist.
Zugriffe protokollieren	Auswahl, ob die HTTP-Proxy Zugriffe mitprotokolliert werden sollen.

Menüpunkt	**Beschreibung**
MIME-Header protokollieren	Angabe, ob der Squit-MIME-Header mit protokolliert werden soll.
HTTP-Proxy-Scanner	Auswahl, ob der Malware HTTP-Filter auf Port 3131 gestartet werden soll. Falls dieser Filter verwendet werden soll ist darauf zu achten, dass an den Klienten der Proxy-Port im Browser geändert wird.
HTTP-Jugendfilter-Proxy	Auswahl ob der Jugendschutz-Filter DansGuardian auf Port 3132 gestartet werden soll. Der Filter scannt den aktuellen Inhalt einer Website nach verschiedenen Methoden. Die Standard-Einstellungen sind geeignet für die Erfordernisse zum Betrieb in Schulen. Eine genauere Beschreibung des DansGuardian-Filters bekommen Sie im Internet unter: http://dansguardian.org/ Falls dieser Filter verwendet werden soll ist darauf zu achten, dass an den Klienten der Proxy-Port im Browser geändert wird.
HTTP-Werbefilter-Proxy	Auswahl ob der Werbefilter-Proxy auf Port 3133 gestartet werden soll. Falls dieser Filter verwendet werden soll ist darauf zu achten, dass an den Klienten der Proxy-Port im Browser geändert wird.
Auto-HTTP-Proxy-Port	Auswahl welcher Proxy-Port bei einer automatischen DHCP-Adressvergabe den Klienten übergeben werden soll. Der Standard-Proxy wird immer über Port 3128 (Squid2) angesprochen. Ist ein andere Filter-Proxy installiert und ausgewählt, so stehen auch diese zur Auswahl. Beim Squid3 ist der Proxy-Port 3138.
Auto-HTTP-Proxy-Ausnahmen	Hier können Ausnahmen definiert werden die bei der Verwendung des Auto-Proxys vom Proxy-Server ausgenommen werden. Beispiele hierfür sind lokale Server oder IP-Adressen.
Socks-Proxy	Auswahl ob der Socks-Proxy gestartet werden soll.
Erlaubte Socks-Ports	Auswahl der TCP-Ports im Internet und der DMZ, die über den Socks-Dienst zu erreichen sein sollen.
FTP-Proxy	Auswahl ob der FTP-Proxy gestartet werden soll.
Transparenter FTP-Proxy	Auswahl ob ein transparenter FTP-Proxy gestartet werden soll, der alle Anfragen, die auf Port 21 an beliebige Adressen gehen auf den FTP-Proxy umleitet. Dieser Dienst wird nur gestartet, wenn der FTP-Proxy gestartet ist.
Pound-Proxy	Auswahl ob der Pound-Load-Balancer gestartet werden soll. Achtung: Für den Load-Balancer müssen spezielle Anpassungen manuell vorgenommen werden. Wenden Sie sich bitte dazu an den Support der m-privacy GmbH.
—	
Squid-HTTP-Header filtern	Angabe, ob im Squid-Proxy die HTTP-Header gefiltert werden sollen.
Erlaubte Squid HTTP-Header	Sie können im HTTP-Header einzelne Informationen erlauben oder verbieten. Wenn Sie mit dem HTTP-Protokoll nicht vertraut sind, kann Ihnen folgender Request for Comments[2)] (RFC) über das HTTP Protokoll in der Version 1.1 weiterhelfen: http://www.ietf.org/rfc/rfc2616.txt
Squid3-HTTP-Header filtern	Hier können Sie auswählen, ob der Header gefiltert werden soll oder nicht.
Squid3-HTTP-Sende-Header	Hier können bestimmte HTTP-Header ausgewählt werden, die gesendet werden dürfen für die Anfrage.
Squid3-HTTP-Antwort-Header	Es können HTTP-Header ausgewählt werden, die für die Antwort erlaubt sind.

Menüpunkt	Beschreibung
Angezeigten User-Agent einstellen	Sie können hier eintragen welcher User-Agent bei HTTP-Header-Anfragen angezeigt werden soll, wenn der Original-Header User-Agent geblockt wird. Beispiel: Tragen Sie Mozilla 1.7.6 (Linux; 32 Bit) ein, wenn Sie einen Mozilla Browser vorspiegeln möchten.
Benutzerauthentisierung	Wenn hier ja ausgewählt wird, so müssen sich die Benutzer am Proxy authentisieren. Die Benutzer und Passwörter werden vom Benutzer *maint* in der Benutzerverwaltung angelegt, es sind die selben wie für den Mail-Zugriff.
Weitere Proxy-Klientennetze	Weitere IP-Netze, die auf den Proxy zugreifen dürfen. Diese sind in der Form a.b.c.d oder a.b.c.d./n anzugeben. Mehrere Netze müssen durch Leerzeichen getrennt werden. Bereits zugelassen sind das interne Netz inkl. weiterer interner Netze, Zusatznetz und DMZ-Netz. ACHTUNG: Beim Anlegen weitere Netze müssen ggf. die Firewall Regeln angepasst werden, aus DMZ und Zusatznetz ist ggf. der Proxy-TCP-Port zu öffnen.
Cache-Größe Festplatte MB	Festlegen des Plattenplatzes in MB, den der Proxy-Cache belegen darf. ACHTUNG: Es muss ausreichend Platz auf der Partition vorhanden sein. Falls der Proxy-Cache des Fallback-Netzwerks aktiv ist, belegt dieser zusätzlich noch einmal die selbe Menge Speicherplatz!
Cache-Größe Hauptspeicher MB	Festlegen des Hauptspeichers in MB, den der Proxy-Cache belegen darf. ACHTUNG: Falls der Proxy-Cache des Fallback-Netzwerks aktiv ist, belegt dieser zusätzlich noch einmal die selbe Menge Hauptspeicher!
Max. Objekt-Größe KB	Festlegen bis zu welcher Größe in KB Objekte auf der Festplatte gespeichert werden sollen.
Max. Objekt-Größe Speicher KB	Festlegen bis zu welcher Größe in KB Objekte im Hauptspeicher gehalten werden sollen.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

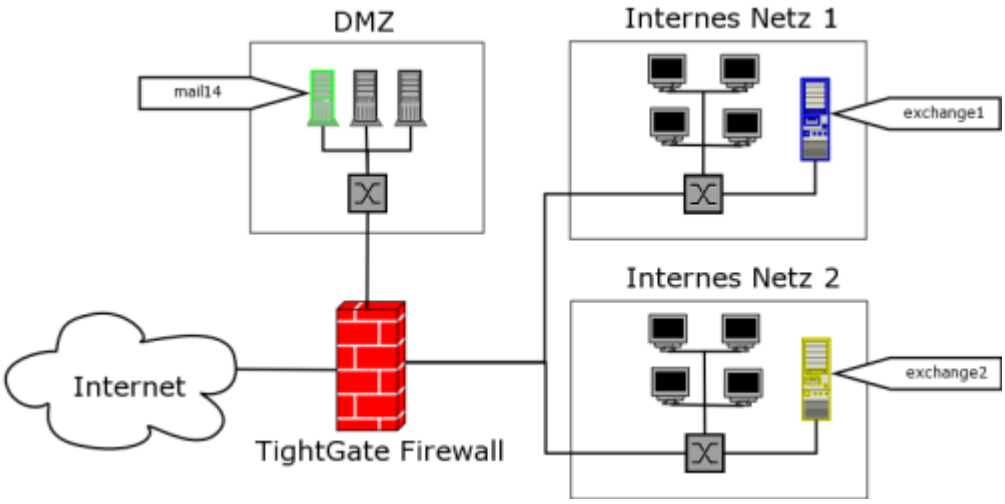
Domain Name System (DNS) Entries

Über das weltweit verfügbare Domain Name System DNS können Namen in IP-Adressen (und umgekehrt) verwandelt werden.

Beispiel: Sie haben im internen Netz verschiedenen Server. Sie haben die Möglichkeit die Server direkt über ihre IP-Adressen anzusprechen. Dies ist sehr aufwändig, da IP-Adressen aus Zahlenkolonnen bestehen und spätestens ab der dritten IP-Adresse eine Verwechslung kaum mehr vermeidbar ist. Alternativ zu den IP-Adressen können sie für jeden Server auch einen Namen vergeben. Dieser Name wird im DNS hinterlegt und einer speziellen IP-Adresse zugeordnet. Mit dieser Zuordnung können Sie nun den Server beim "Namen“ nennen. Die Umsetzung in die korrekte IP-Adresse wird vom DNS erledigt.

IP-Adresse	Servername
192.140.10.123	exchange1
192.168.53.123	mail14

IP-Adresse	Servername
192.140.8.100	exchange2



Um ein neues DNS Entry anzulegen melden Sie sich bitte als Benutzer *config* an und wählen dann bitte aus dem Menü den Punkt *Einstellungen>DNS Entries>Neu* aus.

1. Geben Sie bitte hier den Host-Namen ohne Domäne ein.
2. Geben Sie bitte im nachfolgenden Dialog die IP-Adresse des zugehörigen Servers an. Wenn Sie das Feld IP-Adresse leer lassen, wird automatisch der Name der Firewall eingetragen, so dass der neue Name als Alias verwendet wird.

Wenn sie einen bestehenden Eintrag ändern möchten, wählen Sie den zu ändernde Eintrag aus. Es öffnet sich ein Bearbeitungsdialog, der Ihnen die Möglichkeit bietet, die Einstellungen zu ändern. Bitte beachten Sie, dass der Name der Firewall automatisch eingetragen wird, also von Ihnen nicht mehr angelegt werden darf. Rechner mit dynamischen DHCP-Adressen können ebenfalls automatische eingetragen werden, siehe dazu Menü Internes Netzwerk.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Unterbrechungsfreie Stromversorgung (USV)

Eine unterbrechungsfreie Stromversorgung (USV) oder englisch uninterruptable power supply (UPS) soll bei einem Ausfall der Netzspannung die Stromversorgung sicherstellen.

Um eine neue USV anzulegen oder eine bestehende USV-Verbindung zu ändern melden Sie sich bitte als Benutzer *config* an. Wählen Sie dann bitte aus den Menüpunkt *Einstellungen>USV* aus.

Nachfolgend sehen Sie eine Übersicht des Einstellungsmenüs für den Anschluss einer USV. Dabei ist in der ersten Spalte der jeweilige Menüpunkt genannt. In der zweiten Spalte ist beschrieben, was der Menüpunkt bedeutet. In der Spalte *Master* ist jeweils dort ein Kreuz gesetzt, wo Einstellungen vorzunehmen sind, falls die USV direkt an die mp-Firewall angeschlossen ist. In der Spalte *Slave* sind entsprechend Kreuze gesetzt, wenn die mp-Firewall als Slave-System USV-Informationen von einem Master-Server erhalten soll. Folgende Einstellungsmöglichkeiten gibt es:

Menüpunkt	Beschreibung	Master	Slave
Modell	Auswahl des Modells der USV aus der vorgegeben Liste. Sollten Sie ein USV-Modell haben, welches nicht in der Liste eingetragen ist, wenden Sie sich bitte an der Support der m-privacy.	x	
Anschluss*	Anschluss der USV an der mp-Firewall	x	
Parameter	USV-spezifische Parameter	(x)	
Master	Master-Server von dem die Informationen einer USV übernommen werden. Der Master-Server ist in folgender Form anzugeben: [Name der USV]@[IP-Adresse des Master Servers]. Meist ist dies myups@a.b.c.d		x
Benutzer auf Master	Benutzername des USV-Benutzers auf dem Master-Server		x
Passwort auf Master	Benutzer-Passwort für den USV-Benutzer auf dem Master-Server		x
Slaves	IP-Adresse oder IP-Netzwerk von Rechnern, die USV-Informationen von der mp-Firewall beziehen können, wenn diese als Master-Server läuft	(x)	
Benutzer für Slaves	Benutzername für Slave-Rechner	(x)	
Passwort für Slaves	Passwort für Slave-Benutzer	(x)	
Administrations-Benutzer	Benutzernamen des USV-Administrators auf dem Master-Server	x	
Administrations-Passwort	Administrator-Passwort des USV-Administrators auf dem Master-Server	x	

Beispiel für verschiedene Anschlussmöglichkeiten einer USV:

Anschluss der USV	Anschluss
1 Serieller Port (Com1)	ttyS0
2 Serieller Port (Com2)	ttyS1
USB Port 1 oder 2	usb0 oder usb1

Hinweis : Wenn die mp-Firewall als Master für die USV läuft, so kann über die Status-Seite der mp-Firewall der aktuelle Ladezustand und weitere Informationen über die USV abgerufen werden. Mehr über die Statusseite finden Sie im Kapitel Webbasierte Dienste und Administration

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Wartungs- und Update-Zugang

Die Einstellungen für den Wartungs- und Update-Zugang sind dazu vorgesehen einen geeigneten Zugang zu Ihrem System zu konfigurieren. Hier können verschiedene Möglichkeiten des Zugangs zu Ihrem System eingestellt werden, um Fernwartungsarbeiten ausführen zu können oder einen Zugang zu schaffen, damit das System an dem automatischen Update-Verfahren teilnehmen kann. Die Einstellungen sollten nur in Absprache mit dem technischen Kundendienst vorgenommen werden.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt

Sanft Anwenden an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Hardware Sensoren

Über die Hardware Sensoren lassen sich bestimmte Zustände der eingebauten Hardware kontrollieren und auswerten. Leider liefert nicht jede Hardware diese Sensoreigenschaften. Deshalb kann es nach einem Hardwareaustausch passieren das bestimmte Sensoren nicht oder zusätzlich erkannt werden. Die über den Menüpunkt *Erkennen* erkannten Hardwaresensoren werden dann als Module im Kernel eingebunden. Diese Sensoren können mit dem Menüpunkt *Anzeigen* kontrolliert und ausgewertet werden. Falls es dennoch zu Fehlermeldungen kommen sollte, können Sie die fehlerhaften Module einfach über den Menüpunkt *Fehlerhafte Module entfernen* entfernen. Gehen Sie dabei aber vorsichtig vor.

Zum Hauptmenü

1)
Die Brute-Force-Methode bzw. Methode der rohen Gewalt beruht darauf, die auf dem Ausprobieren aller (oder zumindest eines erheblichen Teils der in Frage kommenden) Varianten beruht. Näheres dazu unter: http://de.wikipedia.org/wiki/Brute_Force

2)
RFCs sind eine durchnummerierte Serie von Dokumenten, die verschiedene tatsächliche und vorgeschlagene Gewohnheiten beschreiben, die einen Bezug zum Internet haben und von der IETF herausgegeben werden. Die Sammlung ist sowohl hinsichtlich des Themas, als auch des so genannten Status, uneinheitlich. Viele RFCs behandeln technische Festsetzungen und Übereinkommen, die Protokolle genannt werden. Protokolle sind für die Zusammenarbeit der Systeme unentbehrlich; Programme, die untereinander Daten austauschen, müssen auf einigen Übereinstimmungen hinsichtlich des Datenformates und verwandten Themen beruhen. Die m-privacy GmbH hat auf die dort dargelegten Informationen keinen direkten Einfluss, die Angabe der URL erfolgt lediglich als Hilfe für die Benutzung.