



Hinweise zur Nutzung des Mail-Servers mail.x-dot.de

Inhaltsverzeichnis

I. Zugangsdaten für den Mailserver	1
II. Angebotene Dienste	1
III. Zugriffsschutz und Zugangsdaten	2
1. Versand von Emails nur nach erfolgreicher Authentifizierung (Anmeldung) am Mailserver möglich	2
2. Versand und Empfang über verschlüsselte Verbindungen (SSL/TLS)	3
IV. Konfigurationsbeispiele	4
1. Microsoft Outlook 2002	4
2. Thunderbird 2.0	7
3. Mozilla 1.3 / Thunderbird / Netscape 7	9
V. Email Konfiguration über Web Interface (M@ilAdmin)	11
VI. Emails abrufen/ansetzen über Web Interface (Webmail)	11
VII. Spam- und Virenschutz	13
1. Die Schutzmechanismen im Detail	13
2. Kennzeichnung der Emails bei Befund	15
3. generelle Kennzeichnung der Emails durch den Server	15
4. Filtern von unerwünschten Emails (Beispiel Outlook 2002)	16

I. Zugangsdaten für den Mailserver

Servername: mail.x-dot.de
Benutzername POP3 (Empfang): wird zugeteilt; Standard: wie Emailadresse nur ohne „@“
Passwort POP3: wird zugeteilt

II. Angebotene Dienste

POP3 (Port 110), POP3 via SSL (Port 995)

SMTP (Port 25), SMTP TLS (Port 25), SMTP (Submission Port 587)

IMAP, IMAP via SSL (Port 993)

Für einen sicheren und verschlüsselten Empfang/Versand von Emails ist es zu empfehlen, POP3 via SSL (Empfang) und SMTP TLS (Versand) in Ihrem Mailprogramm zu nutzen. Ggf. müssen Sie in Ihren Antivirenprogrammen dabei die Prüfung von ausgehenden Emails abschalten, da diese bei Verschlüsselung die ausgehenden Emails nicht prüfen können.

Die Nutzung von IMAP auf dem Mailserver ist zwar möglich, es wird jedoch empfohlen, POP3/SMTP als Protokoll zu verwenden. Eine dauerhafte Speicherung der Emails auf dem Mailserver bei IMAP ist nicht vorgesehen. Emails werden nach max. 60 Tagen vom Server gelöscht.



III. Zugriffsschutz und Zugangsdaten

Der Mailserver verfügt über mehrere Sicherheitsfunktionen, die Ihren E-maildomains einen zusätzlichen Schutz gegenüber Missbrauch und Spam bieten. Leider sind daher auch einige spezielle Einstellungen für die Nutzung des Systems notwendig:

1. Versand von Emails nur nach erfolgreicher Authentifizierung(Anmeldung) am Mailserver möglich

Um zu vermeiden, dass Ihre Domains von Spammern missbraucht werden, kann über den Mailserver nur noch nach erfolgreicher Anmeldung eine Email verschickt werden. Dies ist normalerweise bei vielen Mailservern sonst nicht der Fall. Aus diesem Grund müssen Sie sich auch für den Versand von Emails gegenüber dem Mailserver authentifizieren.

Wir bieten für den Versand von Emails zwei verschiedene Optionen an, empfehlen aber die SMTP-Authentifizierung.

a) SMTP Authentifizierung

Bei der SMTP-Authentifizierung muss sich der Mailclient (z.B. Outlook) beim Versand von Emails mit einem Passwort und einem Benutzernamen bei unserem Mailserver anmelden. Dieses Verfahren sollte als Standard genutzt werden und wird von (fast) allen Mailclients unterstützt.

Bitte geben Sie folgende Daten für SMTP-Authentifizierung in Ihrem Mailprogramm ein:

Benutzername: wie POP3 Benutzername + „@email“ am Ende
Passwort: wie POP3 Passwort

Exemplarisch für die Emailadresse: max.mustermann@dom.de

Benutzername POP3: max.mustermann@dom.de

Benutzername SMTP: max.mustermann@dom.de@email

Achtung: Versand ist nur für die entsprechende Absender-Email möglich, zu der die Zugangsdaten gehören!

b) POP3 vor SMTP (POPAUTH)

Bei POPAUTH wird zuerst das Postfach, über das eine Email verschickt werden soll mit POP3 abgefragt und danach erst eine Email verschickt. Bei jedem Abrufen mit POP3, wird die IP-Adresse des abrufenden Systems für 10 Minuten für SMTP freigeschaltet.

Achtung: Bei Wählverbindungen (ISDN; DSL) ändert sich bei jeder Einwahl die IP-Adresse. Ein Versand ist nach erfolgreichem Abrufen mit beliebigen Absender-Emails möglich.



2. Versand und Empfang über verschlüsselte Verbindungen (SSL/TLS)

Der Mailserver bietet zusätzlich Optionen für den verschlüsselten Empfang (POP3, IMAP) und Versand (SMTP, IMAP) von Emails. Damit können Sie zuverlässig Ihre Emails von und zu unserem Server übertragen, ohne dass jemand Ihre Daten einsehen kann. Unser Server versucht Ihre Emails auch – wenn möglich – verschlüsselt an das Zielsystem weiterzuleiten.

Achtung: Ein sicherer Schutz ist nur durch zusätzliches Verschlüsseln der Emails mit S/MIME oder besser noch PGP (www.pgp.com, www.gnupg.org) möglich! Mit SSL/TLS wird nur der Übertragungsweg – soweit möglich – verschlüsselt.

a) SSL verschlüsselter Empfang

Um den Empfang von Emails zu verschlüsseln, aktivieren Sie bitte die entsprechenden Optionen in Ihrem Mailclient (z.B. Outlook):

POP3 via SSL: Port 995

IMAP via SSL: Port 993

b) SSL verschlüsselter Versand

Um den Versand von Emails zu verschlüsseln, aktivieren Sie bitte die entsprechenden Optionen in Ihrem Mailclient (z.B. Outlook):

SMTP TLS: Port 25 oder den Port 587

IMAP via SSL: Port 993



IV. Konfigurationsbeispiele

Folgend nun einige Beispiele, wie die Änderungen bei den verschiedenen Mailclients einzustellen sind:

Alle Beispiele für die exemplarische Email „max.mustermann@dom.de“

1. Microsoft Outlook 2002

Die benötigten Einstellungen für Outlook finden Sie im Menü unter „Extras“, „Email Konten“. Dort dann „Vorhandene E-Mail-Konten anzeigen oder bearbeiten“ auswählen. Dann wählen Sie bitte das Email-Konto aus und klicken auf „Ändern“. Sie sollten dann die folgende Maske sehen (erscheint auch bei Einrichtung eines neuen Kontos):

Bitte geben Sie in die oben abgebildeten Felder die entsprechenden Daten ein.

Klicken Sie danach bitte auf „Weitere Einstellungen“. Dann erscheint eine weitere Eingabemaske mit vier verschiedenen Reitern. Die für die Änderung entscheidenden Reiter sind „Postausgangsserver“ und „Erweitert“.

Bitte füllen Sie die Masken mit Ihren Daten entsprechend den folgenden Masken aus:



Internet-E-Mail-Einstellungen

Allgemein Postausgangsserver Verbindung Erweitert

Der Postausgangsserver (SMTP) erfordert Authentifizierung

Gleiche Einstellungen wie für Posteingangsserver verwenden

Anmelden mit

Benutzername: max.mustermann@dom.de@email

Kennwort: *****

Kennwort speichern

Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)

Vor dem Senden bei Posteingangsserver anmelden

OK

Einstellung für SMTP-Authentifizierung

Internet-E-Mail-Einstellungen

Allgemein Postausgangsserver Verbindung Erweitert

Der Postausgangsserver (SMTP) erfordert Authentifizierung

Gleiche Einstellungen wie für Posteingangsserver verwenden

Anmelden mit

Benutzername: max.mustermann@dom.de@email

Kennwort: *****

Kennwort speichern

Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)

Vor dem Senden bei Posteingangsserver anmelden

OK Abbrechen

Einstellung für POP vor SMTP (POPAUTH)



Internet-E-Mail-Einstellungen

Allgemein | Postausgangsserver | Verbindung | Erweitert

Serveranschlussnummern

Posteingangsserver (POP3): 110 Standard verwenden

Dieser Server verwendet eine sichere Verbindung (SSL)

Postausgangsserver (SMTP): 25

Dieser Server verwendet eine sichere Verbindung (SSL)

Servertimeout

Kurz ————— Lang 1 Minute

Übermittlung

Kopie aller Nachrichten auf dem Server belassen

Vom Server nach 10 Tagen entfernen

Entfernen, wenn aus "Gelöschte Objekte" entfernt

OK

Hier können Sie dann statt Port 25 auch den Submission Port 587 einstellen. Allerdings müssen Sie dann die SMTP-Authentifizierung nutzen. Mit POP vor SMTP ist dies nicht möglich. Siehe vorhergehende Seite.

Einstellung für unverschlüsselten Empfang/Versand.

Internet-E-Mail-Einstellungen

Allgemein | Postausgangsserver | Verbindung | Erweitert

Serveranschlussnummern

Posteingangsserver (POP3): 995 Standard verwenden

Dieser Server verwendet eine sichere Verbindung (SSL)

Postausgangsserver (SMTP): 25

Dieser Server verwendet eine sichere Verbindung (SSL)

Servertimeout

Kurz ————— Lang 1 Minute

Übermittlung

Kopie aller Nachrichten auf dem Server belassen

Vom Server nach 10 Tagen entfernen

Entfernen, wenn aus "Gelöschte Objekte" entfernt

OK Abbrechen

Einstellung für Empfang/Versand mit SSL/TLS Verschlüsselung.



2. Thunderbird 2.0

Im Mozilla Thunderbird finden Sie die benötigten Einstellungen im Menü unter „Extras“, dann „Konten“. Wählen Sie danach die Kategorie „Server-Einstellungen“:

Konten

Max Mustermann Emailkonto

- Server-Einstellungen
- Kopien & Ordner
- Verfassen & Adressieren
- Speicherplatz
- Junk-Filter
- Empfangsbestätigungen
- S/MIME-Sicherheit
- Lokale Ordner
 - Speicherplatz
 - Junk-Filter
- Postausgang-Server (SMTP)

Server-Einstellungen

Server-Typ: POP

Server: Port: Standard: 110

Benutzername:

Sicherheit und Authentifizierung

Verschlüsselte Verbindung verwenden:

Nie TLS, wenn möglich TLS SSL

Sichere Authentifizierung verwenden

Server-Einstellungen

Beim Starten auf neue Nachrichten prüfen

Alle Minuten auf neue Nachrichten prüfen

Neue Nachrichten automatisch herunterladen

Nur die Kopfzeilen herunterladen

Nachrichten auf dem Server belassen

Lösche Nachrichten vom Server nach Tagen

Nachrichten vom Server löschen, wenn sie vom Posteingang gelöscht werden

Papierkorb beim Verlassen leeren

Erweitert...

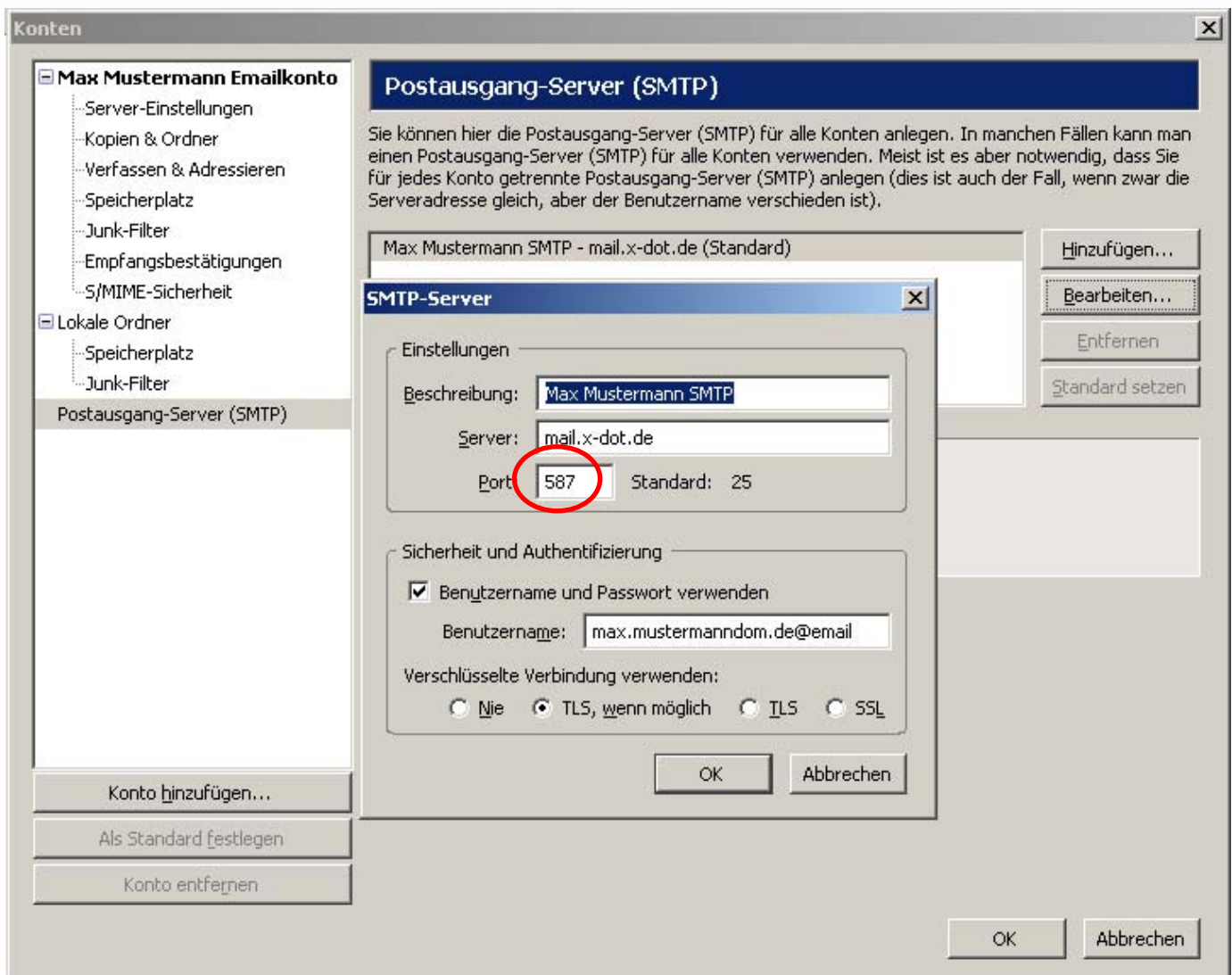
Lokales Verzeichnis:

Verzeichnis wählen...

OK Abbrechen

Einstellung für unverschlüsselten Empfang.

Mit dem Mozilla Thunderbird Mailclient ist es nicht möglich, ohne SMTP Authentifizierung Emails zu verschicken. Es muss daher unter „Benutzername für Mail-Server“ immer der entsprechende Benutzername eingetragen sein. Das Passwort wird dann beim ersten Sendeversuch abgefragt und gespeichert.



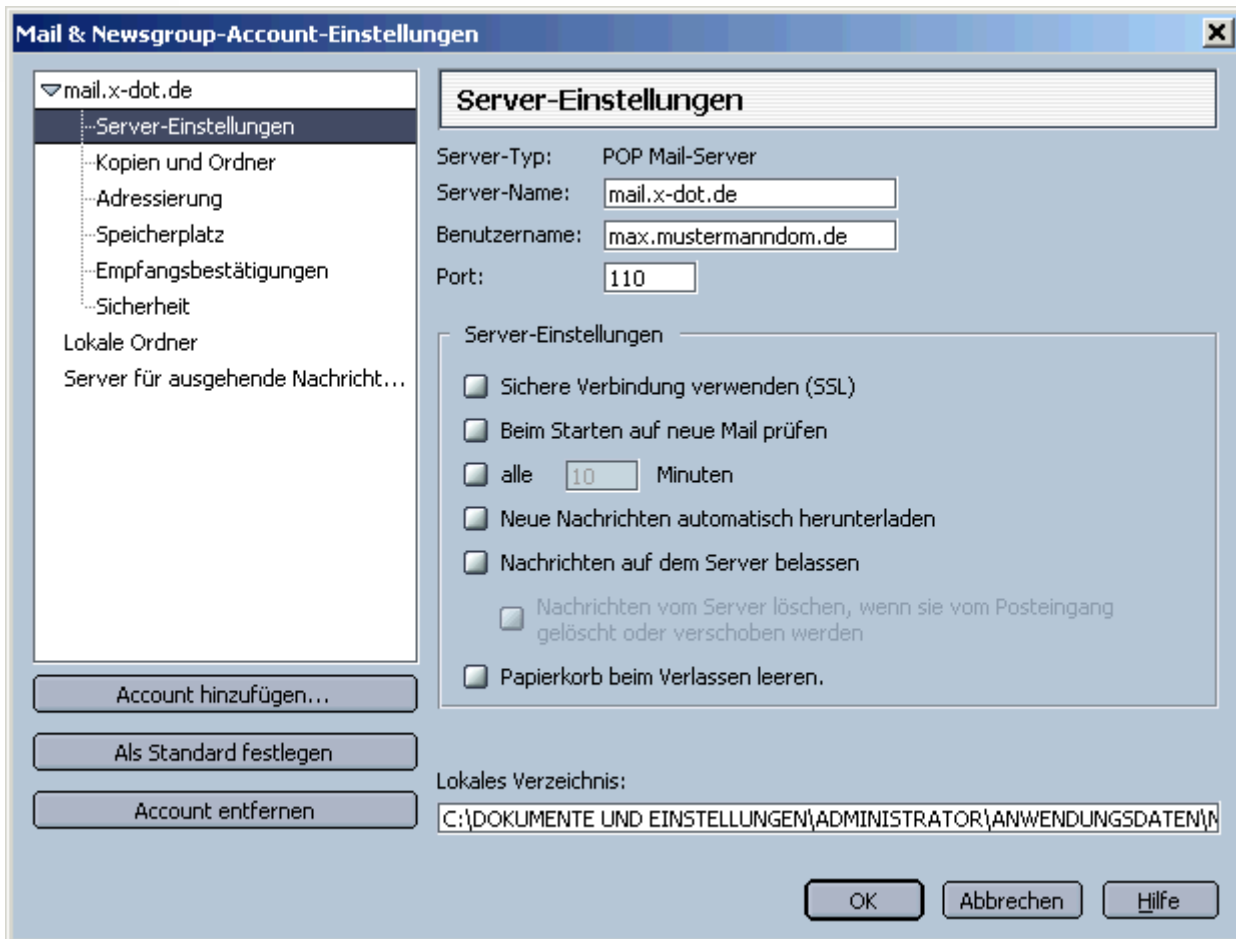
Einstellung für verschlüsselten Versand.

Die Einstellungen sind im Prinzip identisch wie für den unverschlüsselten Versand, es muss nur die Option „TLS, wenn möglich:“ ausgewählt werden. In dem Bild ist auch schon auf den sogenannten Submission Port 587 umgestellt worden, der Port 25 funktioniert aber auch.



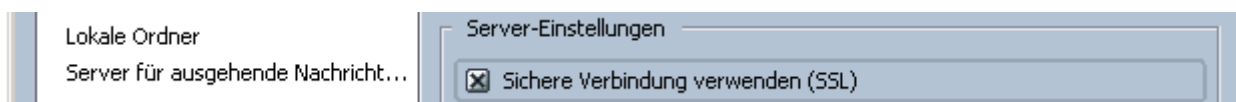
3. Mozilla 1.3 / Thunderbird / Netscape 7

Unter Mozilla / Netscape 7 finden Sie die benötigten Einstellungen im Mailclient im Menü unter „Bearbeiten“, dann „Mail & Newsgroup-Account-Einstellungen“.



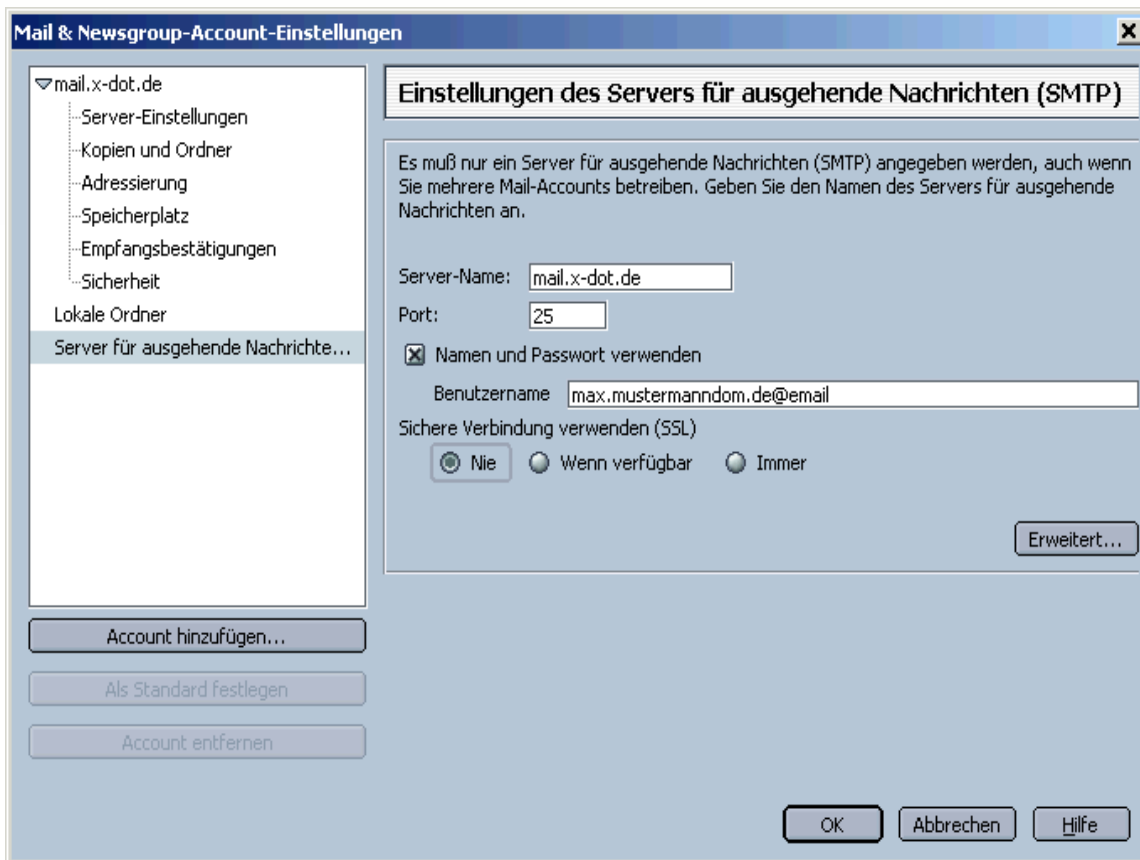
Einstellungen für unverschlüsselten Empfang.

Wenn Sie die Emails verschlüsselt per POP3 Abrufen wollen, so müssen Sie lediglich auf der obigen Maske unter „Server-Einstellungen“ ein Häkchen bei „Sichere Verbindung verwenden (SSL) setzen“.



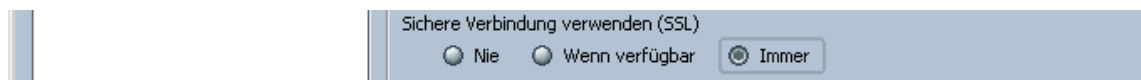
Zusätzliche Einstellungen für verschlüsselten Empfang.

Für den Versand von Emails mit SMTP-Authentifizierung wählen Sie die Maske „Server für ausgehende Nachrichten...“:



Einstellung für unverschlüsselten Versand.

Mit dem Mozilla /Netscape 7 Mailclient ist es nicht möglich, ohne SMTP Authentifizierung Emails zu verschicken. Es muss daher unter „Benutzername für Mail-Server“ immer der entsprechende Benutzername eingetragen sein. Das Passwort wird dann beim ersten Sendeversuch abgefragt und gespeichert.



Einstellung für verschlüsselten Versand.

Die Einstellungen sind im Prinzip identisch wie für den unverschlüsselten Versand, es muss nur die Option „Sichere Verbindung verwenden (SSL)“ auf „Immer“ gestellt werden. Alternativ können Sie auch die Einstellung „Wenn verfügbar“ nehmen.

Achtung: POPAUTH (POP3 vor SMTP) ist mit Mozilla / Netscape 7 nicht möglich.

V. Email Konfiguration über Web Interface (M@ilAdmin)

Sie haben die Möglichkeit für jede Ihrer Domains über eine Internetseite (M@ilAdmin) die Emailkonfiguration einzurichten.

Öffnen Sie dazu einfach die Internetseite <https://mail.x-dot.de/mailadmin> (SSL verschlüsselt) und geben dann auf der folgenden Anmeldemaske die Ihnen mitgeteilten Zugangsdaten für den M@ilAdmin ein.

Die Konfiguration wird für jede registrierte Domain getrennt durchgeführt.

Folgende Optionen stehen Ihnen im M@ilAdmin zur Verfügung:

- Emailkonten löschen/ändern/erstellen
- Weiterleitungen konfigurieren (Email, Fax)
- Weiterleitungen für unbekannte Aliase konfigurieren (Sammelkonto/CatchAll) wird aufgrund des hohen SPAM Aufkommens aber nicht empfohlen
- Autoresponder konfigurieren
- SMS Benachrichtigungen konfigurieren
- Passwörter ändern
- Übersichten über Konten
- Statusinformationen (Anzahl eingerichteter Emailkonten, maximale Anzahl Emailkonten)

VI. Emails abrufen/ansetzen über Web Interface (Webmail)

Sie haben die Möglichkeit, von jedem Ort der Welt ohne weitere Installationen jederzeit Ihre neuen Emails zu lesen und auch neue Emails zu schreiben.

Öffnen Sie einfach die Internetseite <https://mail.x-dot.de/webmail> (SSL verschlüsselt) und geben dann auf der folgenden Anmeldemaske die Zugangsdaten ein, die Sie auch für den Empfang über POP3 in Ihrem Mailclient (z.B. Outlook) eingeben. Der Login ist jeweils für eine einzelne Emailadresse.

Achtung: Sie können parallel mit Webmail und Ihrem lokalen Emailprogramm arbeiten. Beachten Sie dabei nur, dass alle Emails, die Sie an einer Stelle (lokal oder Webmail) löschen natürlich nicht mehr auf der anderen Stelle sichtbar sind. Das gleiche gilt, wenn Sie zusätzliche Ordner unter Webmail anlegen. Die in diese Ordner verschobenen Emails können Sie nicht mehr lokal mit POP3 abrufen, ein Zugriff darauf ist dann nur noch mit IMAP möglich.

Bevor Sie über Webmail Emails verschicken, müssen Sie unter „Einstellungen“ – „Persönliche Angaben“ Ihre Absenderangaben eingeben. Geben Sie dazu wie im folgenden Beispiel Ihre entsprechenden Daten in die Felder „Vollständigen Namen...“ und „Von...“ ein.

Der vollständige Name sollte nicht zu lang sein und um Probleme mit alten Emailclients zu vermeiden auch keine Umlaute oder Sonderzeichen wie z.B. „.“ enthalten.

Eine Signatur für ausgehende Emails können Sie ganz unten auf der Seite im Feld „Ihre Signatur“ zusätzlich auch eingeben.



Einstellungen für Webmail

Einstellungen bearbeiten

Persönliche Angaben

<< S/MIME-Einstellungen | E-Mail

Ihre Standardidentität:

Standardidentität

Wählen Sie die Identität, die Sie ändern möchten:

Standardidentität

Ausgewählte Identität löschen

Bezeichnung der Identität

Standardidentität

Ihr vollständiger Name:

Max Mustermann

Ihre Von: Adresse:

max.mustermann@dom.de

Ihre E-Mail-Adresse für das Feld "Antwort an." (optional)

Ihre Alias-Adressen: (optional, jede Adresse in einer eigenen Zeile eintragen)

Adressen, die an diese Identität gebunden sind: (optional, jede Adresse in einer eigenen Zeile eintragen)

Einstellungsmaske Webmail unter <https://mail.x-dot.de/webmail>



VII. Spam- und Virenschutz

Der Mailserver verfügt über weitreichende Anti-Spam und Anti-Virus Schutzmechanismen. Sämtliche Emails, die von dem Mailsystem verarbeitet werden, durchlaufen verschiedene Prüfungssysteme. Somit wird ein zusätzlicher Schutz gegen ungewollte Viren, gefährliche Dateien und unerwünschte Spam Nachrichten geboten.

1. Die Schutzmechanismen im Detail

Folgende Schutzmechanismen werden auf dem Server angewendet:

- a) HTML-Email Überprüfung „IFRAME“
HTML-Emails mit gefährlichen „IFRAME“ Objekten im Quelltext werden in einfache Text-Emails konvertiert, um diese schadlos zu machen
- b) HTML-Email Überprüfung „CODEBASE“
HTML-Emails mit gefährlichen „CODEBASE“ Objekten im Quelltext werden in einfache Text-Emails konvertiert, um diese schadlos zu machen.
- c) Texterkennungsfilter inkl. Selbstlernender Bayes-Filter (Spamassassin)
Emails werden anhand diverser Verfahren gescannt und inhaltlich überprüft
- d) „Rule-based Rankings“ (Spamassassin)
Anhand eines komplexen Regelwerkes, werden Punktzahlen für Emails vergeben, die den Grad der Spamwahrscheinlichkeit für die einzelnen zutreffenden Regeln kennzeichnen.
- e) RBL Blacklist-Server abfragen
Verschiedene Blacklist-Server, auf denen Emailserver eingetragen sind, die Spam versenden, werden abgefragt. Emails, die über dort eingetragene Server verschickt werden, werden von unserem Server nicht angenommen.
- f) Virus Überprüfung
Überprüfung aller Emails inkl. Attachments auf Viren. Virendatenbank wird mehrmals täglich aktualisiert. Virulente Attachments werden gelöscht und durch Text-Attachments mit entsprechender Warnung ausgetauscht. Viren innerhalb der Email werden ebenfalls durch eine entsprechende Text-Meldung ausgetauscht.
- g) Dateinamen Überprüfung
Es wird eine Überprüfung der Dateinamen von Attachments durchgeführt. Gefährliche Attachments werden dabei sofort gelöscht und der Absender und der Empfänger der Email über das Löschen informiert.



Dateien mit folgendem Typ werden gelöscht, da diese in den meisten Fällen für Angriffe genutzt werden:

Endung	Beschreibung
.reg	Windows Registry
.chm	Kompilierte Windows Hilfe
.cnf	SpeedDial
.hta	Microsoft HTML Archiv
.ins	Microsoft Internet Einstellungen
.jse?	Microsoft JavaScript
.lnk	Eudora *.lnk Sicherheitsloch Angriff
.ma[dfgmqrstvw]	Microsoft Access Verknüpfung
.pif	MS-DOS Programm Verknüpfung
.scf	Microsoft Explorer Kommando
.sct	Microsoft Windows Script Komponente
.shb	Dokumenten Verknüpfung
.shs	Shell Scrap Objekt
.vb[es]	Microsoft Visual Basic
.ws[cfh]	Microsoft Windows Scripting Host
.xnk	Microsoft Exchange Verknüpfung
.com	Windows/DOS ausführbare Datei
.scr	Bildschirmschoner (meistens inkl. Virus!)
.bat	Batch Script
.cmd	Batch Script
.cpl	Systemsteuerungs-Komponente
.mhtml	Eudora meta-refresh Angriff
{[a-zA-H0-9-]{25,}}	Dateinamen mit CLID's (Verschleierung der wahren Dateieindung)
s{10,}	Dateinamen mit vielen Leerzeichen (Verschleierung)
Dateiname.doc.exe	Verschleierung des wahren Dateityps



2. Kennzeichnung der Emails bei Befund

Sämtliche Emails, die von dem Server überprüft wurden werden gekennzeichnet, um auf dem Mail-Client des Users entsprechende Regeln für die Filterung vorzusehen und ein evtl. erneutes scannen von einem weiteren System zu vermeiden.

Folgende Kennzeichnungen werden durchgeführt:

a) Besondere Kennzeichnung bei Spam-/Virus- oder HTML-Gefahrbefund

Bei der Erkennung der obigen Typen werden die Betreffzeilen der Emails umgeschrieben um ein einfaches Filtern zu ermöglichen. Es werden dabei die folgenden Begriffe an den Anfang der Betreffzeile gesetzt:

Typ	Markierung Betreffzeile
Spam Emails	*****SPAM*****
Emails mit Virus (der gelöscht wurde)	*****VIRUS*****
Emails mit gefährlichen Attachment laut Dateinamenüberprüfung	*****ATTACHMENT*****
Emails mit gefährlichem HTML-Code	*****DANGEROUS CONTENT*****

3. generelle Kennzeichnung der Emails durch den Server

Zusätzlich zu dem Umschreiben der Betreffzeile bei Befund, wird jede Email, die durch den Server verarbeitet wurde mit weiteren Informationen versehen. Diese Informationen befinden sich nicht sichtbar in den Headern jeder Email und werden bei Ansicht der Email normalerweise nicht angezeigt, lassen sich aber für eine Filterung nutzen.

Folgende Header-Informationen werden der Email hinzugefügt:

a) X-xdot-MailScanner-Information: Please contact x-dot GmbH for more information

→ Allgemeine Informationsmeldung

b) X-xdot-MailScanner: Found to be clean

→ Meldung des Virenschanners über das Ergebnis der Überprüfung

c) X-xdot-MailScanner-SpamCheck: spam, SpamAssassin (Wertung=7.265, benötigt 5, FORGED_MUA_OUTLOOK 1.58, FORGED_OUTLOOK_HTML 1.10, FORGED_OUTLOOK_TAGS 1.10, HTML_70_80 0.10, HTML_FONTCOLOR_BLUE 0.10, HTML_FONTCOLOR_RED 0.10, HTML_FONT_BIG 0.10, HTML_MESSAGE 0.00, MIME_BASE64_LATIN 1.10, MIME_BASE64_TEXT 1.10, MIME_HTML_ONLY 0.10, MSGID_FROM_MTA_HEADER 0.76, TO_ADDRESS_EQ_REAL 0.01)

→ Meldung des Ergebnisses der Spamassassin Überprüfung inkl. der angewendeten Regeln und des Spam-Scores (Spam Wahrscheinlichkeit). Details zu den Regeln (in Englisch) sind zu finden unter <http://www.spamassassin.org/tests.html>

d) X-xdot-MailScanner-SpamScore: ssssss

→ Ausgabe des Spam-Scores für die Filterung durch ein Emailprogramm.

Hinweis: Ab einem Spam-Score von 5 Punkten wird zusätzlich die Betreffzeile (s.o.) umgeschrieben und der Begriff „*****SPAM*****“ hinzugefügt.

Die Ausgabe des Scores an dieser Stelle in den Headern – wobei jedes „s“ für einen Punkt steht – ermöglicht eine genauere Einstellung, ab welcher Wahrscheinlichkeit eine Email durch einen Filter verschoben/gelöscht werden soll.

Die Filterung anhand der Betreffzeile würde immer ab einem Ergebnis von 5 Punkten zutreffen!

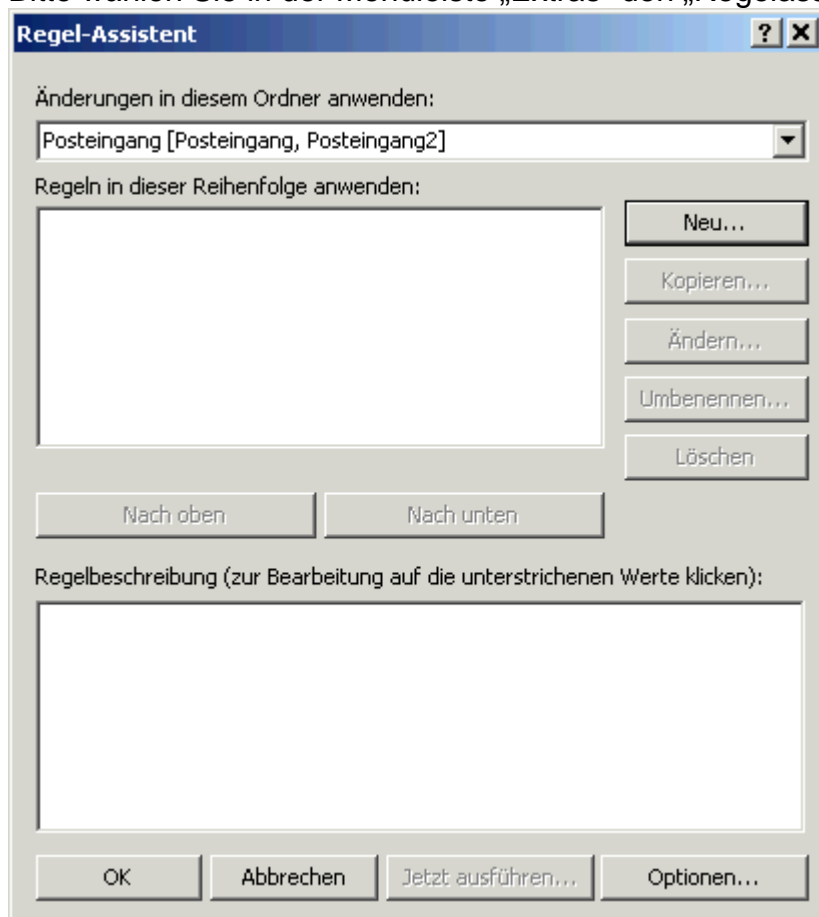
4. Filtern von unerwünschten Emails (Beispiel Outlook 2002)

Durch die Markierung der Emails vom Server ist es leicht möglich, die ungewollten Emails im Email-Client zu filtern und damit sofort zu löschen/verschieben.

Folgend nun ein Beispiel für die Filterung der Emails anhand der zusätzlichen Header-Information „X-xdot-MailsScanner-SpamScore“:

a) Microsoft Outlook 2002

Bitte wählen Sie in der Menüleiste „Extras“ den „Regelassistent“.



Klicken Sie dann bitte auf „Neu...“.

Jetzt können Sie mit dem Assistenten eine Regel erstellen, die folgendermaßen aufgebaut ist, um z.B. alle Emails aus dem Posteingang automatisch anhand der Kopfzeileninformation in den Papierkorb zu verschieben:



„Nach Erhalt einer Nachricht
mit X-xdot-MailScanner-SpamScore: ssssss in der Nachrichtenkopfeile
diese in den Ordner Gelöschte Objekte verschieben.

Das Ergebnis sollte etwa folgendermaßen aussehen, wobei natürlich die Ordner entsprechend Ihrer
Konfiguration gewählt werden müssen:



Sie können bei dieser Regel anhand der Anzahl der „s“, nach der Sie Filtern, entscheiden, wie empfindlich der Filter reagieren soll.

Beispiel:

Suche nach „X-xdot-MailScanner-SpamScore: sss“ ist sehr empfindlich, da ab einem Score von 3 die Email gefiltert wird, wobei Suche nach „X-xdot-MailScanner-SpamScore: sssssssssssssssssssss“ relativ wenig Emails filtern wird.

Um den neuen Filter zu aktivieren klicken Sie bitte auf „Fertig stellen“.