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

Stand: 2018-11

Inhaltsverzeichnis

1. Zugangsdaten für den Mailserver

Servername:	mail.x-dot.de
Benutzername (Empfang):	wie Emailadresse nur ohne „@“
Benutzername (Versand):	wie Emailadresse nur ohne „@“ + „@email“ am Ende
Passwort:	wird Ihnen gesondert zugeteilt, im M@ailAdmin änderbar
Exemplarisch für die Emailadresse:	max.mustermann@domain.de
Benutzername Empfang:	max.mustermanndomain.de
Benutzername Versand:	max.mustermanndomain.de@email

2. Angebotene Dienste

Für einen sicheren Empfang/Versand von Emails sind immer die verschlüsselten Verbindungen zu nutzen (SSL, TLS). Ggf. müssen Sie in Ihren Antivirenprogrammen dabei die Prüfung von ausgehenden Emails abschalten, da diese bei Verschlüsselung die ausgehenden Emails nicht prüfen können.

EMAIL VERSAND

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

EMAIL EMPFANG

IMAP via SSL (Port 993)
IMAP (Port 143)

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

EMAIL WEBMAIL

Empfang und Versand von Email-Nachrichten direkt über einen Webbrowser.
https://mail.x-dot.de/webmail/

3. Zugriffsschutz und Zugangsdaten

Um zu vermeiden, dass Ihre Domains von Spammern missbraucht werden, kann über den Mailserver nur nach erfolgreicher Anmeldung eine E-Mail verschickt werden. Aus diesem Grund müssen Sie sich für den Versand von Emails gegenüber dem Mailserver authentifizieren (SMTP-Authentifizierung).

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

Der Mailserver bietet 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 verschlüsselt an das Zielsystem weiterzuleiten.

Achtung: Ein sicherer Schutz ist nur durch zusätzliches Verschlüsseln der Emails oder Anhänge mit S/MIME, PGP, verschlüsselte ZIP-Files mit Passwortschutz o.ä. möglich. Mit SSL/TLS wird nur der Übertragungsweg verschlüsselt.

5. Email Konfiguration über Web Interface im Kundenportal

Sie haben die Möglichkeit für jede Ihrer Domains über das Kundenportal die Emailkonten einzurichten, zu ändern, usw.

Öffnen Sie dazu einfach die Internetseite https://kundenportal.xdot.de/Login und geben dann auf der folgenden Anmeldemaske die Ihnen mitgeteilten Zugangsdaten für den das Kundenportal ein.

Die Konfiguration wird für jede registrierte Domain getrennt durchgeführt.

Folgende Optionen stehen Ihnen u.a. im Kundenportal 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)

6. Emails abrufen/ansehen 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/ und geben dann auf der folgenden Anmeldemaske die Zugangsdaten ein, die Sie auch für den Empfang in Ihrem Mailclient (z.B. Outlook) eingeben. Der Login ist jeweils für eine einzelne Emailadresse.

Hinweis

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.(E-Mail)

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.

7. 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.

7.1 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 (Spam Assassin)
Emails werden anhand diverser Verfahren gescannt und inhaltlich überprüft

d) „Rule-based Rankings“ (Spam Assassin)
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-hA-H0-9-]{25,}\}	Dateinamen mit CLID´s (Verschleierung der wahren Dateiendung)
s{10,}	Dateinamen mit vielen Leerzeichen (Verschleierung)
Dateiname.doc.exe	Verschleierung des wahren Dateityps
mehrere Punkte im Anhang .xxx.xy.d.txt	Unzulässig

7.2 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*****

b) 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 Virenscanners 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: sssssss

→ 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 E-Mail durch einen Filter verschoben/gelöscht werden soll.

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