THORSTEN JANTZEN
INFORMATIONS- / KOMMUNIKATIONS-TECHNIK
Güldenkamp 64 • 38108 Braunschweig
tel: 0531 / 233 56-47 • fax: - 49 • mobil : 0160 / 44 95 379 • web: www.jantzen.de • email: info@jantzen.de

Hinweise zur Nutzung der E-Mail Services

Der E-Mailserver bietet einige Einstellmöglichkeiten bezüglich Behandlung eingehender E-Mails. Um das stark vermehrte Aufkommen unerwünschter E-Mails (SPAM) zu minimieren, wurden einige Maßnahmen ergriffen, die sie kennen sollten, um bei Problemen zu verstehen, woran es liegen könnte und welche Einstellungen zur Verfügung stehen.

Hierzu muss ein wenig verstanden werden, wie E-Mails bei Eintreffen verarbeitet werden:

Begriffe:
Wenn ein fremder Rechner (ab jetzt sending host genannt) E-Mails abliefern möchte, so meldet er sich zuerst mit seinem eigenen Namen beim empfangenden Rechner (receiving host) an und sagt, von welcher E-Mail-Adresse (sender address) er E-Mails für welche Empfängeradresse (receiver address) hat; hierbei können mehrere Empfänger zugleich genannt werden.

dns-lookup:
Bevor der Server die E-Mail annimmt, wird kontrolliert, ob der sending host im Internet gültig registriert ist (es wird ein sogenannter reverse dns lookup durchgeführt).
Wenn dieses nicht der Fall ist, wird die E-Mail zu diesem Zeitpunkt schon abgelehnt. Dieses soll verhindern, dass E-Mails direkt von Privatrechnern angenommen werden, die sich dynamisch ins Internet einwählen und ggf. mit schadhafter Software verseucht sind und somit für SPAM-Versand missbraucht werden. Dieses bedeutet, das ihre E-Mail-Partner unbedingt die E-Mails über deren E-Mail-Provider verschicken müssen, was normalerweise immer der Fall sein sollte.

blacklisting:
Des Weiteren wird überprüft, ob die sender address auch gültig ist. Wenn nicht, wird die E-Mail ebenfalls abgelehnt. Ergänzend wird in einer sogenannten blacklist nachgesehen, ob der sending host als SPAM-Versender bekannt ist. Wenn ja wird der Empfang abgelehnt.
Diese blacklists unterliegen ständigen Erneuerungen und können zeitweise einen sending host ablehnen, der schon bereinigt wurde oder durch Falscheintrag dort gelandet ist. Dieses Verhalten korrigiert sich somit nach kurzer Zeit meist von selbst.

Prüfung auf existierendes Postfach:
Eine weitere Kontrolle vor Annahme der E-Mail besteht darin, zu prüfen, ob die Empfängeradresse existiert. Wenn weder ein Postfach noch eine Weiterleitung mit passender Adresse besteht, wird der Empfang abgelehnt. Ausnahme: der catchall-Eintrag, siehe unter Weiterleitung.

Überprüfung der eingehenden E-Mail:
Wenn die Prüfungen bis hierhin erfolgreich waren, übergibt nun der sending host den Inhalt der E-Mail an den Mailserver. Zu diesem Zeitpunkt wäre es noch möglich, die gesamte E-Mail abzulehnen, indem der Empfang nicht bestätigt wird.
Dieses hat den Vorteil, dass, wenn es sich um unerwünschte E-Mails handelt, sie nicht übernommen und abgespeichert werden müssen., was auch bedeuten würde, dass der Empfänger sie im seinem Postfach vorfindet. Ziel dieses Verfahrens ist es zu, SPAM-Versendern den Erfolg der Zustellung zu unterbinden sowie ungewollte E-Mails nicht im Postfach des Empfängers abzulegen.

Nun kann aber die Einstufung dessen, was unter unerwünschter E-Mail zu verstehen ist, recht unterschiedlich sein und der E-Mail-Provider darf und will dem Kunden die Entscheidung nicht abnehmen. Er kann nur technische Hilfsmittel zur Verfügung stellen, die der Kunde selbst zur Nutzung aktiviert.

Der Mailserver akzeptiert eingehende E-Mails, auch wenn für mehrere Empfänger bestimmt, immer nur als Datenstrom für eine domain (alle Adressen mit @ihredomain.de), um kundenbasierte Einstellungen zu berücksichtigen.

Einstellungen:

Dadurch kann jeder Kunde für seine domain konfigurieren, wie bei der Annahme der Mails verfahren werden soll:

Dazu bitte auf der Webseite http://www.jantzen.de im Bereich „Service“ unter „Emailservices“ die „Domainverwaltung“ auswählen.

Nach dem Login können unter dem Menüpunkt „DomainMenü“ folgende Punkte gewählt werden:

Stufenschema:
Es steht ein vierstufiges Schema zur Verfügung:
Stufe 0 = nur eintragen einer neuen Kopfzeile „X-Spam-Score:“
Stufe 1 = auf Viren scannen und Warnung in Betreff eintragen
Stufe 2 = abweisen von E-Mails, in denen ein Virus erkannt wurde
Stufe 3 = abweisen von E-Mails, in denen ein Virus erkannt wurde oder Spamscore überschritten.

Erläuterung:
Spamscore beschreibt einen Wert, der die Wahrscheinlichkeit angibt, ob es sich um eine E-Mail mit unerwünschtem Inhalt handeln könnte.

Jede E-Mail wird durch einen SPAM-Filter geschickt und der ermittelte Wert in einer zusätzlichen Kopfzeile eingetragen. Diese Kopfzeile lautet X-Spam-Score: und wird sichtbar, wenn im E-Mail-Programm die Option zum Anzeigen aller Kopfzeilen aktiviert wird.

Ab Stufe 1 aufwärts wird jede E-Mail von einem simplen Virenscanner untersucht und bei Befall wird die Betreffzeile der E-Mail mit einem Warnhinweis versehen.

Wenn Stufe 2 eingestellt ist, werden E-Mails mit identifiziertem Virus bei Empfang abgewiesen.

Ab der Stufe 3 werden E-Mails, deren Spamscore einen vorgegeben Wert überschreitet, ebenfalls abgewiesen. Dieser Wert ist pro Kundendomain einstellbar und betrifft dann **alle** E-Mail-Adressen dieser domain, d.h. sie sollten klären, ob sie diese Vorgabe machen dürfen und ggf. Einverständnis einholen bzw. die Nutzer davon in Kenntnis setzen.

spam_score_deny:
Es wird ein freies Produkt eingesetzt (http://spamassassin.apache.org/), um SPAM-Mails zu erkennen. Dieses vergibt Punkte nach Kriterien um eine Wahrscheinlichkeit zu erhalten, ob es sich um SPAM handelt oder nicht. Ab einem Wert von 12.0 ist eine recht hohe Sicherheit gegeben, dass SPAM erkannt wurde. Dieses ist auch der Wert, der als Vorgabe für das Abweisen von E-Mails gemäß Stufe 3 empfohlen wird. Da das Programm eine Nachkommastelle vergibt, wird hier mit dem Faktor 10 eingestellt, also ist ein Wert von 120 einzutragen.

Spamerkennung trainieren:
Das Produkt spamassassin kann für seine Erkennung trainiert werden.
Wenn explizit gewünscht, kann für den Kunden ein individuelles Training konfiguriert werden. Dazu muss dann jede zugestellte ungewollte E-Mail in einen speziellen Unterordner is_SPAM verschoben werden, damit spamassassin diese in seine Datenbank aufnehmen kann. Wichtig ist hierfür auch, wiederholt gewollte E-Mails als „nicht-SPAM“ anzulernen, die falsch erkannt wurden, damit sich die Erkennungsqualität erhöht.
Die Standardeinstellung ist, einen vorgegebenen systemweiten Filter zu verwenden. Wenn sie dieses umstellen möchten, so wenden sie sich bitte direkt an mich für weiteres Vorgehen und Informationen.

Postfachbezogene Einstellungen:

Unabhängig davon, ob kundenspezifisch E-Mails abgewiesen werden, wird für jede E-Mail, die angenommen wird, ein spamscore-Wert ermittelt. Jeder Nutzer eines Postfaches hat drei Parameter, um festzulegen, wie damit verfahren werden soll. Der Nutzer kann einen persönlichen Grenzwert festlegen, ab dem er eine E-Mail als SPAM markiert haben möchte, dieser Wert wird spam-score-mark genannt. Sinnvolle Vorgabe ist ein Wert von 50.

Ist die Funktion „spam-move" aktiviert, so wird jede E-Mail, dessen Wert den persönlich eingestellten Grenzwert überschreitet, in einen eigenen Unterordner des Posteinganges gelegt, der die Bezeichnung SPAM trägt.

Unabhängig von „spam-move" gibt es den Schalter „spam-mark":
Ist dieser gesetzt, so wird bei jeder E-Mail, die den Grenzwert überschritten hat, die Betreffzeile verändert, indem der Text *SPAM* gefolgt von der Zahl des ermittelten spamscores gefolgt vom Originaltitel der E-Mail gesetzt wird.
Dieses sieht dann in etwa folgendermaßen aus:

SPAM 28.8(++++++++++++++++++++++++++++)* Make Your Dreams Become Your Reality

(Hierbei ist der Wert hinter *SPAM" der vom System ermittelte Wahrscheinlichkeitswert/spamscore. Die Pluszeichen sind als eine Art Aussteuer-Balken gedacht)

Letzteres ist sinnvoll, wenn der Postfachnutzer das POP3-Protokoll (Einstellung im E-Mail-Programm) zum Abholen von E-Mails einsetzt, da er hiermit den Unterordner SPAM nicht erhält.

Alternativ kann per Webmail-Login auf den SPAM-Ordner zugegriffen werden, um diese E-Mails zu sichten, löschen und ggf. in den Posteingang zurückzuschieben.

Weiterleitungen:
Es besteht die Möglichkeit, dem Mailserver Weiterleitungen vorzugeben.

Hierfür werden mindestens zwei Werte benötigt:
Der localpart ist der Teil der E-Mail-Adresse, für den die Weiterleitung erfolgen soll.
Wichtig: Es ist nur der Teil der Adresse **vor** dem @-Zeichen einzutragen.

Unter Zieladresse ist das Weiterleitungsziel einzutragen, hier immer eine vollständige E-Mail-Adresse angeben inklusive @domain, da auch Adressen außerhalb der eigenen Domain verwendet werden können.
Es besteht auch die Möglichkeit, an mehrere Ziele gleichzeitig weiterzuleiten.

Beispiel:

localpart	*Weiterleitungsziel*
vorstand	user1@ihredomain.de, user2@ihredomain.de, privatadresse@anderedomain.de

Somit würde alle E-Mails an vorstand@ihredomain.de an zwei Adressen der gleichen und eine Adresse außerhalb ihrer domain weitergeleitet werden.

***Vorsicht**:* Es ist zu beachten, dass eine Weiterleitung Vorrang vor dem persönlichen Postfach hat. Wenn also eine Weiterleitung eingerichtet ist, so wird die E-Mail nur an die Zieladresse zugestellt und nicht ins Postfach gelegt. Wenn gewünscht wird, dass sowohl an die Weiterleitungsadresse als auch ins Postfach zugestellt werden soll (also quasi eine Kopie), so muss die Postfach-E-Mail-adresse zusätzlich als Weiterleitungsziel eingetragen werden.

Catchall-Weiterleitung:
Für manche Kunden ist es wichtig, alle E-Mails zu sichten, selbst wenn der E-Mail-Partner diese falsch adressiert hat. Wie oben beschrieben, ist das Standardverhalten des Mailservers die Ablehnung von E-Mails für eine nichtexistierende Adresse.

Hierfür kann in der Weiterleitungstabelle unter localpart ein * eingetragen werden, Beispiel:

localpart	*Weiterleitungsziel*
*	info@ihredomain.de

Bitte beachten: Wenn ein Postfach deaktiviert wurde und keine Weiterleitung für die Adresse eingetragen ist, so wird die E-Mail in diesem Falle trotzdem angenommen und an den catchall-Empfänger zugestellt. Ohne catchall-Eintrag wird die E-Mail abgewiesen.

Aliased domains:
Das System sieht für Kunden, die mehrere domains registriert haben, die Möglichkeit vor, diese exakt gleich bzgl. E-Mail-Empfang wie eine bestehende domain zu behandeln. Hierfür kann auf Wunsch einen sogenannter alias eingerichtet werden. Somit müssen nicht alle Postfächer und Weiterleitungen doppelt gepflegt werden.

Verschlüsselung:
Die Mailserver kann die E-Mails verschlüsselt zustellen und entgegennehmen. Dieses ist im E-Mail-Programm entsprechend einzustellen. Es wird dringend empfohlen ausschließlich die verschlüsselte Übertragung zu verwenden. Wenn aus gegebenem Grund ein unverschlüsseltes Protokoll verwendet wird, so stellen sie zumindest sicher, das Login-Passwort nicht im Klartext zu übertragen, indem im E-Mail-Programm „verschlüsseltes Passwort“ eingestellt wird. Die zu verwendenden Ports sind auf der Parameter-Übersichtsseite angegeben.
Es besteht weiterhin die Möglichkeit, als Servernamen für Posteingang als auch Postausgang ihre eigene domain zu verwenden nach dem Muster mail.ihredomain.tld, jedoch ist hiervon bei Verwendung von Verschlüsselung abzuraten, da die meisten E-Mail-Programme dann auf nicht übereinstimmende Servernamen des übertragenen Zertifikates hinweisen und sich diese Warnung nicht bei allen Programmen abstellen lässt. Es wird empfohlen, die Servernamen wie auf der Parameter-Übersichtsseite angegeben zu verwenden.

Autokonfiguration:
Für Anwender des freien E-Mail Programms Thunderbird (https://www.mozilla.org/de/thunderbird/) wurde die Möglichkeit einer Autokonfiguration eingerichtet.
Somit ist es möglich, im Einrichtungsassistenten nur noch die eigene E-Mail-Adresse und Passwort einzugeben und Thunderbird wird automatisch alle benötigten Parameter für eine sichere Konfiguration einstellen.

Login-Sperre:
Auf den Server ist ein Angrifferkennungssystem installiert, um die Gefahr des wiederholten Ausspähens und Missbrauchs der Postfächer zu minimieren. Wenn eine definierte Anzahl von ungültigen Login-Versuchen für ein Postfach erkannt wird, so wird der Rechner für eine feste Zeitspanne gesperrt. In diesem Falle sollte etwas über 2 Stunden warten, bevor sie es mit den korrekten Login-Daten erneut versuchen.

Parameterübersicht E-Mail-Konfiguration

Parameter Posteingang	*Wert / Option*	*Empfehlung / Anmerkung*
Unterstützte Protokolle E-Mail-Empfang/Servertyp	POP3 IMAP	IMAP ist zu bevorzugen, da hiermit auch Zugriff auf Unterordner (z.B. Gesendet/SPAM)
Servername Posteingang	mail.tjmx.de	mail.ihredomain.tld ebenfalls möglich, aber bei Verschlüsselung problematisch
Verbindungssicherheit	SSL/STARTTLS/keine	SSL dringend empfohlen
Port	IMAP: 993 oder 143 POP3: 995 oder 110	993 bei SSL, 143 bei STARTTLS / keine 995 bei SSL, 110 bei STARTTLS / keine
Authentifizierungsmethode	Verschlüsseltes Passwort oder Passwort normal	Verschlüsseltes Passwort empfohlen
Benutzername Posteingang	vollständige E-Mail-Adresse	name@ihredomain.tld
Passwort für Posteingang	Wie vorgegeben	Im Webinterface einstell- und änderbar
Parameter Postausgang	*Wert / Option*	*Empfehlung / Anmerkung*
Servername Postausgang	mail.tjmx.de	mail.ihredomain.tld ebenfalls möglich, aber bei Verschlüsselung problematisch
Verbindungssicherheit	STARTTLS / keine	STARTTLS empfohlen
Port	25 oder 587	
Authentifizierungsmethode	Verschlüsseltes Passwort oder Passwort normal	Verschlüsseltes Passwort empfohlen
Benutzername Postausgang	vollständige E-Mail-Adresse	*Gleiche Adresse wie unter Posteingang*
Passwort für Postausgang	Wie vorgegeben	*Gleiches Passwort wie unter Posteingang*

Bitte beachten:
Wenn Sie ein *neues Postfach* einrichten, wird die Verzeichnisstruktur auf dem Server automatisch bei Eintreffen der ersten E-Mail angelegt. Senden Sie also zuerst eine Test E-Mail an das neue Postfach, sonst gibt es eine Fehlermeldung durch das E-Mail-Programm oder Webmail.

Domainweite Einstellungen:
use_spamfilter = Wert entsprechend Stufenschema
spam_score_deny = Grenzwert für Ablehnung E-Mails nach Stufe 3
spam_score_mark = Vorgabewert für neu angelegte Postfächer
spam_mark = Vorgabewert für neu angelegte Postfächer
spam_move = Vorgabewert für neu angelegte Postfächer

Stufenschema:
Stufe 0 = nur eintragen der Kopfzeile X-Spam-Score:
Stufe 1 = auf Viren scannen und Warnung in Betreff eintragen
Stufe 2 = abweisen von E-Mails, in denen ein Virus erkannt wurde
Stufe 3 = abweisen von E-Mails, in denen ein Virus erkannt wurde oder Spamscore überschritten.

Postfachbezogenen Einstellungen:
spam_score_mark = Grenzwert für Markieren / Verschieben von E-Mails
spam_mark = Erweitert Betreffzeile bei Überschreiten des Grenzwertes
spam_move = Verschiebt E-Mail in Ordner SPAM bei Grenzwertüberschreitung
deliver_mailbox = wenn nicht gesetzt, wird keine E-Mail in das Postfach gelegt