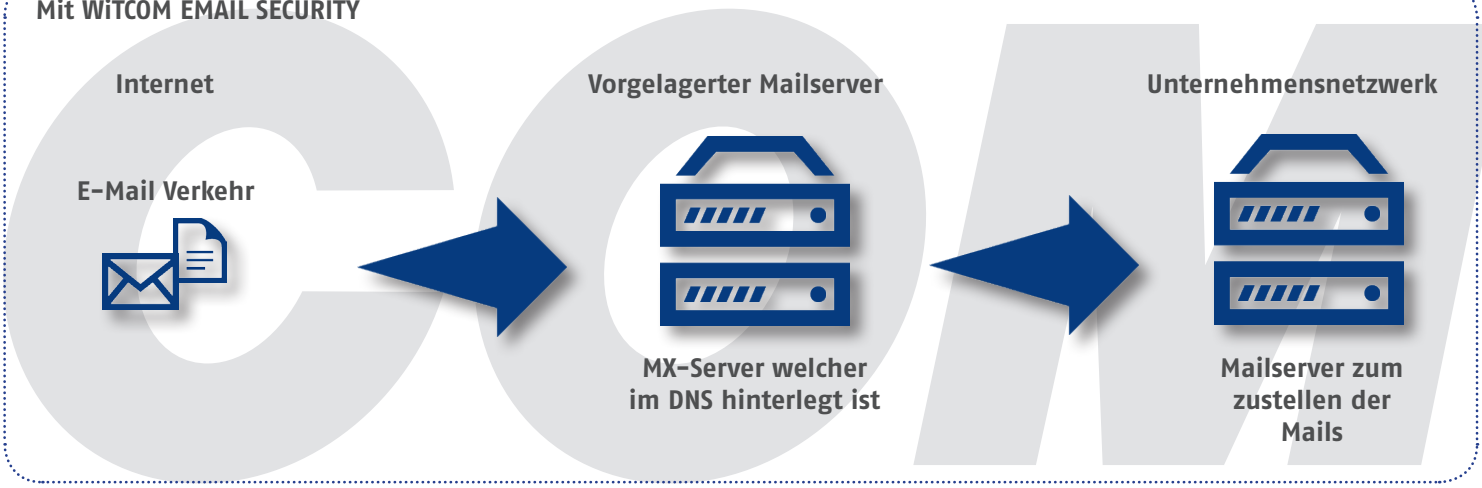
WiTCOM
direkt, persönlich.

WiTCOM EMAIL SECURITY: ERSTE SCHRITTE!

Der Ablauf im Detail.

Ohne WiTCOM EMAIL SECURITY

Mit WiTCOM EMAIL SECURITY



ToDo – Welche Änderungen müssen vorgenommen werden?

Um **WiTCOM EMAIL SECURITY** nutzen zu können, muss der E-Mail Verkehr über vorgelagerte E-Mail Server geleitet werden. Hierzu wird im **DNS** (Domain Name System), bei Ihrem jeweiligen Dienstleister, in der **Domain Zone** der zu schützenden Domain, der **MX-Record** Eintrag (Mail Exchanger) angepasst. Es sollten dabei alle vier MX-Records mit gleich hoher Priorität hinterlegt sein. Parallel dazu werden die an WiTCOM mitgeteilten **MX Server** des Kunden zum zustellen der kategorisierten & markierten Mails auf den vorgelagerten Mailserver hinterlegt.

MX-Record Einträge welche Sie an Ihren Dienstleister weiterleiten:

mxa.expurgate.net mxb.expurgate.net mxa.expurgate.de mxb.expurgate.de mxtls.expurgate.net*

*) Nur bei der Option TLS Verschlüsselung benötigt.

Stand: 09.2016

WiTCOM
direkt, persönlich.

WiTCOM EMAIL SECURITY: ERSTE SCHRITTE!

Best Practise Empfehlung der Filterregeln:

Die hier aufgeführten Filterregeln sind Empfehlungen, wie E-Mails nach dem markieren weiterverarbeitet werden können. Entsprechende Änderungen teilen Sie dem WiTCOM NOC mit. Für ein ablehnen bestimmter E-Mails, bedarf es einer gesonderten schriftlichen Anweisung.

Kategorie	Standardeinstellung (default)	Empfehlung
Clean	zustellen	zustellen
Spam	markieren & zustellen	ablehnen
Bulk	zustellen	default
Bulk.Advertising	behandeln wie Spam	default
Bulk.Porn	behandeln wie Spam	default
Clean.Empty	behandeln wie Spam	default
Clean.Almost-empty	behandeln wie Clean	default
Clean.Empty-body	behandeln wie Clean	default
Clean.Bounce	behandeln wie Clean	default
Clean.Whitelist	behandeln wie Clean	default
Suspect	behandeln wie Clean	default
Dangerous	zustellen	default
Dangerous.Virus	markieren & zustellen	ablehnen
Dangerous.Attachement	markieren & behandeln wie Dangerous	default
Dangerous.Code	behandeln wie Dangerous	default
Dangerous.Iframe	behandeln wie Dangerous	default
Dangerous.Virus-Outbreak	markieren & behandeln wie Dangerous	ablehnen

Zur weiteren Verarbeitung werden den kategorisierten E-Mails entsprechende Header hinzugefügt. Diese Header sind:

- X-purgate-ID mit einer eindeutigen ID (X-purgate-ID: expurgator-69e11b/1472919286-000019B6-B17D0A3C/0/0)
- X-purgate-type mit der entsprechenden E-Mail Kategorie (X-purgate-type: clean)
- X-purgate-size mit der jeweiligen Größe der E-Mail in Byte (X-purgate-size: 10347)
- X-purgate-Ad & X-purgate mit einer Zeichenfolge welche auf die Verwendung des Services hinweisen

Fragen oder Änderungen zu Ihren WiTCOM EMAIL SECURITY Einstellungen? Kontaktieren Sie uns:
08000-948266 (08000-WiTCOM) - technik@witcom.de

INTERNETZUGÄNGE | STANDORTVERNETZUNG | DATACENTER | TELEFONIE

Stand: 09.2016