

Mail Whitepaper

Kunde/Projekt: 2024
TIC The Internet Company AG, Rotkreuz

Version/Datum: 1.3
29-July-2006

Neuste Version Online:
www.tic.ch/de/support/manuals/mail-whitepaper.pdf

Autor/Autoren: Aldo Britschgi
aldo.britschgi@tic.ch

1 Inhaltsverzeichnis

1	Inhaltsverzeichnis	2
2	Einleitung – Wozu dieses Dokument?	3
2.1	Zuverlässige Email-Kommunikation mit TIC	3
3	Spam und Virus	4
3.1	Spam-Bekämpfung ist Sache des Anwenders	4
3.2	Definition Spam	4
3.3	Notwendige Massnahmen für Anwender und IT-Verantwortliche	4
3.3.1	Firewall	4
3.3.2	Antivirusprogramm	5
3.3.3	Kunden mit firmeneigenen Mailserver.....	5
3.4	Die bessere Alternative – Hosted Exchange	6
3.5	Hosted Exchange ist ein «Managed Service»	7
3.5.1	Managed Services.....	8
3.5.2	Weitere Informationen zu Hosted Exchange	9
4	Blacklists: SORBS, SpamCop, etc.....	10
4.1	Wie kommt mein Server auf eine «Blacklist»?	10
4.1.1	Typische Blacklist-Betreiber sind:	10
4.1.2	Gründe, warum man auf eine Blacklist kommt:	10
4.2	Wer ist für die Störungs-Behebung verantwortlich?.....	10
4.3	Warum kommt ein TIC-Server auf eine Blacklist?	11
4.3.1	Massnahmen von TIC The Internet Company AG:	11
5	Relaying	12
5.1	Mailserver-Missbrauch.....	12
5.2	Empfohlene Massnahmen gegen «Relaying»	12
5.3	Kunden ohne eigenen Mailserver	13
5.4	POP, IMAP, SMTP Server Einstellungen.....	13
6	Mail Backup Queue (SMTP Queue)	14
6.1	Email Zwischenspeicherung für Firmen-Mailserver	14
6.2	So erhalten Sie Mail Backup.....	14
6.3	Produkteübersicht Mail Backup	14
7	Über TIC The Internet Company AG	16
7.1	www.tic.ch	16

2 Einleitung – Wozu dieses Dokument?

2.1 Zuverlässige Email-Kommunikation mit TIC

Längst hat sich Email zu einem der wichtigsten Kommunikationsmittel etabliert. Laut Statistiken verschiedener renommierter Forschungsinstitute nimmt die Email-Kommunikation einen wichtigeren Stellenwert als Telefax, Telefon und Briefpost zusammen ein. Die Vorteile überzeugen: Rasche und einfache Kommunikation rund um die Uhr und rund um die Welt.

Leider ist Email aber auch sehr «verletzlich», sofern nicht bestimmte Richtlinien eingehalten werden. Sobald bestimmte Parameter nicht stimmen, bestimmte Regeln nicht beachtet werden oder eine Detail-einstellung übersehen wird, steigt die Wahrscheinlichkeit, dass Emails die Empfänger nicht erreichen oder sonstiger Missbrauch mit dem Email-System betrieben wird, vielleicht ohne dass man dies selbst bemerkt. Die Folgen sind meist signifikant.

TIC The Internet Company AG ist ein langjähriger erfahrener Internet Service Provider und kennt sich in der Email-Kommunikation als auch jeglichen Sicherheitsaspekten bestens aus. Dieses Dokument erläutert aktuelle Probleme in der Email-Kommunikation und natürlich deren Lösungen.

Dieses Whitepaper gibt den Kunden von TIC The Internet Company wichtige Hinweise für die Email-Kommunikation, Spam & Antispam, Virus & Antivirus und die Einstellungen von Email-Servern oder Mail-Programmen. **Zudem wird die Marktrichtung «Managed Services» und «Hosted Exchange» als auch Email-Bewirtschaftung unterwegs (Mobile Mail & Mobile Office) aufgezeigt.**



TIC The Internet Company AG
support@tic.ch

www.tic.ch/support

3 Spam und Virus

3.1 Spam-Bekämpfung ist Sache des Anwenders

Spam ist nichts anderes als eine unerwünschte Email-Zustellung an gültige oder ungültige Email-Adressen. Nicht selten sind dies Dutzende, Hunderte oder gar Tausende unerwünschte Emails an eine einzige Email-Adresse und dies täglich – selbst Zustellungen an ungültige Adressen in Millionenfacher Ausführung belasten das System spürbar. Wer auf eine bestimmte Email-Adresse noch kein Spam in diesem Ausmass erhalten hat, sollte sich nicht zu früh freuen, es ist nur eine Frage der Zeit. Oft enthalten Spam-Emails auch Computerviren oder der Spam wurde durch einen Virus erzeugt.

Spam ist eine Tatsache und der Internet Service Provider (ISP) kann nichts dafür. Die Spam- und Viren-bekämpfung liegt zudem in der Verantwortung des Endanwenders bzw. beim Informatik-Verantwortlichen einer Unternehmung. Es sind unbedingt Massnahmen zur Spam-Bekämpfung erforderlich, ansonsten funktioniert das Email-System nicht richtig. Der Internet Service Provider verfügt meist über die Erfahrung und das Wissen, um den Endanwender bei der Spam- und Virenbekämpfung kostenpflichtig zu unterstützen.

3.2 Definition Spam

- Frei übersetzt: Sülze. Müll und Wurfungen in elektronischer Form (Email), oft kommerzieller Art, die gewöhnlich an viele nicht daran interessierte Empfänger gesendet werden. Ein Wort, das unerwünschte elektronische Nachrichten bezeichnet. Einige Email-Programme enthalten Spam-Filter, die den Eingang unerwünschter Nachrichten verhindern sollen.

Quelle: Uni Bielefeld, www.ub.uni-bielefeld.de/library/search/dictionary/reg-s.htm

3.3 Notwendige Massnahmen für Anwender und IT-Verantwortliche

3.3.1 Firewall

- **Jeder Internetzugang muss über eine Firewall geschützt sein.** Empfohlen wird eine Managed Firewall, wo der Internetprovider die regelmässigen Aktualisierungen (Updates) der Firewall übernimmt. So ist der Endkunde gut gegen Angriffe aus dem Internet geschützt.
- Einzelplatz-Computer müssen ebenfalls über eine **Firewall** geschützt sein, z.B. durch eine Software-Firewall (Windows Firewall, etc.) oder über die Firewall-Funktion des Internetzugang-Routers.
- **Eine Firewall dient primär der Zugangssicherheit (Access Security)** und sollte verhindern, dass unerwünschte Angriffe auf den Computer stattfinden. Eine Firewall schützt NICHT primär vor Spam und Viren. Ebenfalls ist die Verwendung von Firewalls für VPN-Verbindungen (Virtual Private Network) problematisch.

- Von TIC The Internet Company AG empfohlene Firewall-Lösung:
WatchGuard Security bzw. Managed TIC Security: www.watchguard.com

TIC The Internet Company AG übernimmt vollständige Firewall-Installationen.
Weitere Informationen: www.tic.ch/de/itservices/viasecurity.php

3.3.2 Antivirusprogramm

- **Jeder Computer muss zwingend über ein permanent aktualisiertes Antivirenprogramm verfügen.** Es ist absolut fahrlässig und nicht akzeptabel, wenn ein Computer über einen Internetzugang verfügt und kein aktuelles Antivirenprogramm installiert hat.
- Von TIC The Internet Company AG empfohlene Antivirus-Lösung für Server, Notebooks und Arbeitsplatz-Computer:
McAfee Antivirus-Software von McAfee Inc.: www.mcafee.com

Antivirus-Software kann bei TIC The Internet Company bezogen werden. Ebenfalls übernimmt TIC The Internet Company fachmännische Vor-Ort Installationen für Server, Notebooks und Arbeitsplatz-Computer.
Weitere Informationen: www.tic.ch/de/itservices/antispam.php

3.3.3 Kunden mit firmeneigenen Mailserver

Für Kunden mit einem firmeneigenen Mailserver, z.B. Microsoft Exchange, gibt es eine ganze Menge zu beachten:

- **Grundsätzlich sollte nur ein Mailserver der neusten Software-Generation mit aktuellen Servicepacks und Patches verwendet werden.** Ältere Mailserver- und Betriebssystemversionen sind im Unterhalt aufwändiger und verfügen nicht über die Sicherheitsvorteile jeglicher Art wie die neusten Software-Generation.
- Ein Mailserver muss zwingend über eine **permanent aktualisierte Firewall** geschützt sein.
- **Ein Mailserver muss zwingend «Relaying-Funktionen» unterbunden haben, ansonsten können aussenstehende (trotz Firewall) den firmeneigenen Mailserver missbrauchen und Spam generieren.** Dies führt dazu, dass die Zuleitung zum Server «verstopft» wird (Anmerkung: Auch eine 100 Mbit/s-Leitung kann nach Inbetriebnahme eines ungeschützten Mailserver innert Stunden «verstopft» sein und somit Schäden generieren).
- **Ein Mailserver muss zwingend mittels Antispam-Massnahmen geschützt sein.** Antispam-Installationen auf dem Server sind sehr aufwändig und anfällig im Unterhalt, es werden externe Antispam-Lösungen empfohlen. Vorteile: Spam und Viren werden im Provider-Backbone-Netzwerk bereits vor Erreichen des eigentlichen Zielmailservers zurückgehalten. Zudem verfügt der Internet Service Provider über ausgeklügeltere Mechanismen als auf einem Kunden-Mailserver zur Verfügung gestellt werden können.

TIC The Internet Company AG kann Ihren Mailserver vollumfänglich unterhalten und permanent die notwendigen Aktualisierungen vornehmen als auch einen bestehenden Server auf Sicherheitsmängel prüfen. Sollten Sie eine ältere Server-Version als Exchange 2003 verwenden, so ist eine Aktualisierung dringend empfohlen.

Weitere Informationen: www.tic.ch/de/itservices/securitychecks.php

3.4 Die bessere Alternative – Hosted Exchange

Bisher benutzten Firmen, vor allem KMUs, einen eigenen Mailserver, z.B. Microsoft Exchange Server für die effiziente Email-Kommunikation.



Hosted Exchange
Ihre Managed Email-Plattform: Mobile Office und Mobile Mail mit Hosted Exchange. Die einfache, schnelle und sichere Kommunikation, firmenintern und extern, ist ein entscheidender Faktor für Ihren Erfolg.

- Ihre eigene **Exchange 2003 Umgebung** auf Knopfdruck
- Volle Funktionalität von Exchange 2003 & Outlook 2003
- 99,99% Verfügbarkeit der Mailplattform
- Top Security, Spam & Virenschutz
- **Zugriff immer und von überall**
- **Managed Services mit Hosted Exchange (PDF)**
- **Publikation in ICT-Kommunikation (PDF)**

«Vergessen Sie den eigenen Mailserver - nutzen Sie Hosted Exchange und überlassen Sie Antispam, Antivirus und sämtliche Sicherheitsmassnahmen den Profis.»

Mit Hosted Exchange ändert sich das signifikant und Unternehmen senken ihre IT-Kosten entscheidend bei gleichzeitig stark erweitertem Anwendungsportfolio. Ein MSP (Managed Service Provider wie TIC The Internet Company AG) betreibt eine Hosted Exchange Serverumgebung in einem

Hochleistungs-Datacenter und bietet so für eine Vielzahl von Unternehmen mit eigenen Email-Domains die komplette Email-Verwaltung an.

- Das Komplettangebot umfasst **modernste und komfortablen Antivirus und Antispam-Lösungen.**
- **Ein weiterer Hauptvorteil liegt in der Mobilität,** da Hosted Exchange Infrastrukturen nahtlos in die Benutzung von mobilen Endgeräten (PDA, Personal Digital Assistant) wie Qtek-Geräte, Smartphones und IPaqs konzeptioniert sind.
- **Über eine bequeme Adminstrationsoberfläche verwalten IT-Verantwortliche Mailboxen, Email-Adressen, Speicherplatz und aktivierte Optionen.**
- Der Dienstleistungsanbieter wird mit einem monatlichen Entgelt entschädigt und stellt dafür den Betrieb rund um die Uhr sicher.
- Für den Kunden entstehen **keine Einmalinvestitionen** mehr für den Aufbau und Betrieb eigener Mailserver.

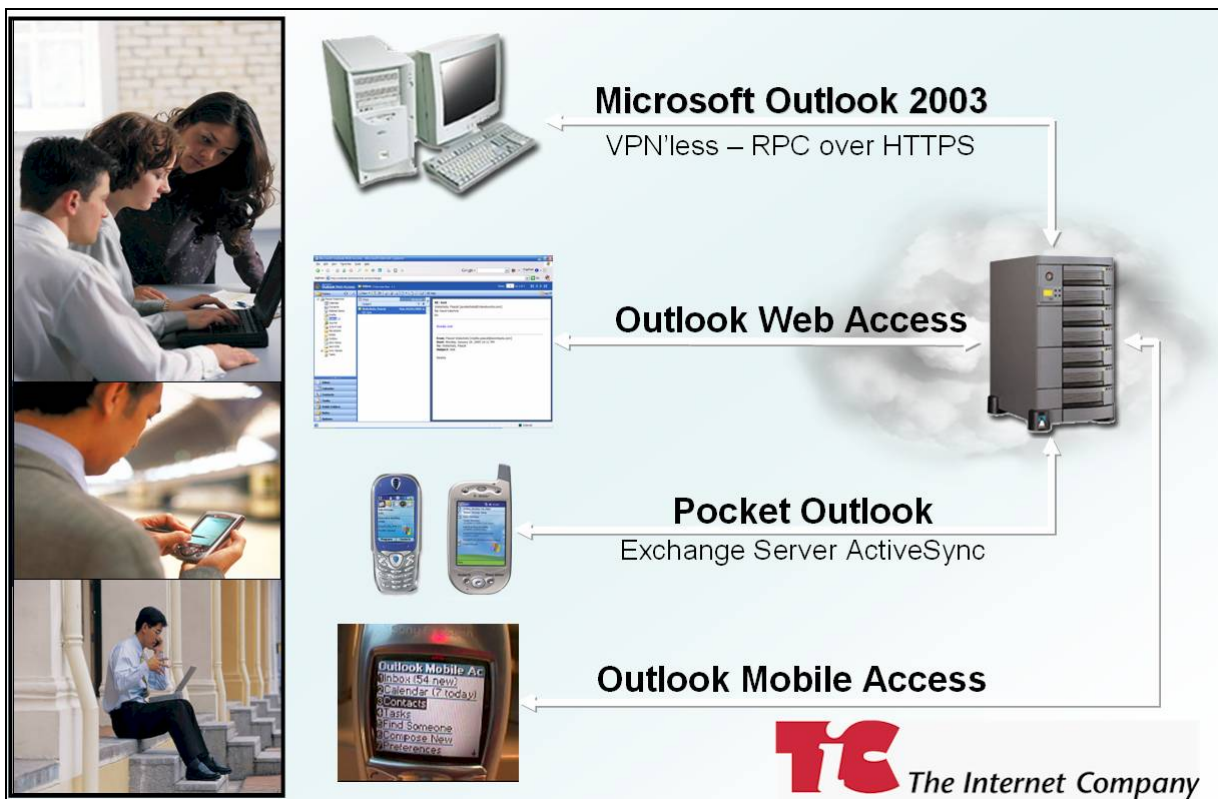


Bild: Hosted Exchange bildet das eigentliche Rückgrat für die integrierte Mobilkommunikation von Unternehmen.

3.5 Hosted Exchange ist ein «Managed Service»

Mit Hosted Exchange erreichen Firmen grenzenlose Mobilität in ihrer Kommunikation und dank dem Managed Services Gedanken ein Maximum an Stabilität sowie Zuverlässigkeit.

TIC The Internet Company AG verfügt mit dem «Virtual Office» Ansatz traditionell über einen klaren Leistungsvorsprung. Zudem zählt die angebotene Hosted Exchange Plattform nach unabhängigen Aussagen zu den besten und sichersten in der Schweiz. Überall und immer auf alle persönlichen Organisations-Daten Zugriff haben, Emails verschicken, Termine planen und Aufgaben koordinieren ist nun auf einfachste Weise möglich.



Bild: Qtek S200 – Mobiltelefon und Mobilcomputer in einem Gerät: Ideal in Kombination mit Hosted Exchange von TIC The Internet Company AG.

3.5.1 Managed Services

Der neuzeitliche Begriff «Managed Services» dürfte die ICT-Zukunft massgebend beeinflussen – seitens IT-Verantwortlichen als auch seitens IT-Lösungsanbieter.

Managed Services ist ein Mix zwischen Outsourcing und ASP (Application Service Providing). Anbieter sind in der Regel so genannte MSPs, was wiederum für «Managed Service Provider» steht.

Normalerweise sind dies Internet Serviceanbieter oder Hostingfirmen, welche an Kunden vollständig betriebene Dienstleistungen in ihren Datacentern zur Verfügung stellen.

Klassisches Outsourcing basiert gewöhnlich auf der Form, dass ein Technologieunternehmen einen bedeutenden Anteil eines Geschäftes einschliesslich der Angestellten in den eigenen Personalstamm über-

nimmt. Aber bei den Managed Services beschränkt sich die Leistungsbereitstellung auf die technische Infrastruktur, welche natürlich rund um die Uhr vom MSP professionell unterhalten und betrieben wird.

«Hosted Exchange» ist ein typisches Beispiel für Managed Services und entwickelt sich immer mehr als «Change Enabler» in Unternehmen. Weitere Beispiele sind «Managed Security» (Sicherheitslösungen), «Managed Server» (vollständiger Betrieb beliebiger Serversysteme) usw.

3.5.2 Weitere Informationen zu Hosted Exchange

www.tic.ch/exchange

Mit Hosted Exchange verfügen KMUs über eine umfassende Kommunikationsplattform mit integrierter mobiler Bewirtschaftung.

4 Blacklists: SORBS, SpamCop, etc.

4.1 Wie kommt mein Server auf eine «Blacklist»?

Es gibt im Internet Betreiber von so genannten «Blacklists», welche den Mailverkehr im Internet nach bestimmten Attributen überprüfen. Sobald eines dieser Attribute zutrifft, kommt eine IP-Adresse oder ein IP-Range (also der Mailserver) auf eine schwarze Liste (Blacklist).

Die Folgen sind fatal: Alle Ziel-Mailserver, welche auf eine solche Blackliste zugreifen, akzeptieren keine Emails mehr von diesem spezifischen Absender-Server auf der Blacklist. Die meisten Ziel-Mailserver benutzen Blacklists, ansonsten könnten die ständigen Email-Fluten nicht mehr bewältigt werden.

4.1.1 Typische Blacklist-Betreiber sind:

- SORBS: Spam and Open-Relay Blocking System, www.nl.sorbs.net
- SpamCop: www.spamcop.net

4.1.2 Gründe, warum man auf eine Blacklist kommt:

Die Gründe sind vielfältig und können jederzeit ändern, teilweise sogar täglich. Hauptgründe sind jedoch:

- Versand von Emails mit Spam-Verdächtigem Inhalt (es muss aber nicht zwingend Spam sein, das kann das System aber gerade aufgrund vieler Sprachen nicht immer genau erkennen), z.B. Versand eines Newsletter oder sonstigen Emails an mehrere Empfänger.
- Offenes Relay – der Mailserver ist nicht genügend gegen Spam geschützt (sehr häufige Ursache bei firmeneigenen Mailservern und/oder älteren Mailservern).
- Ein Virus auf einem Computer bzw. Server, welcher Spam generiert (oft ist dies dem PC-Besitzer nicht bewusst. Als einziges Symptom nimmt er eine langsame Internet-Verbindung wahr).
- Änderung der Blacklist-Regeln von Blacklist-Providern, z.B. neue DNS-Einstellungen (Domain Name Server).
- Fehler im System (Eine regelmässige Ursache aufgrund der anspruchsvollen Problematik von Spam- und Virenbekämpfung).

4.2 Wer ist für die Störungs-Behebung verantwortlich?

TIC The Internet Company AG hat keinen Einfluss auf die Blacklists. Es ist alleinige Sache des betroffenen Mailserver-Betreibers, Anwender des Computers oder Servers, Gegenmassnahmen zu ergreifen (meist Behebung der Sicherheitslücke) und den Normal-Zustand beizuführen.

- Das Customer Care Support Team von TIC The Internet Company AG wird regelmässig speziell auf Email- und Spam-Problematiken trainiert und ist immer auf dem neusten Wissensstand, wie

erläutert ändern sich die Rahmenbedingungen dauernd. **Sämtliche Unterstützung zur Bereinigung von Sicherheitslücken und dem Entfernen von Blacklists werden durch TIC The Internet Company AG kostenpflichtig vorgenommen.**

- Noch was: Das Entfernen von der Blacklist ist zeitraubend und mühsam, unterhalb von 12 bis 24 Stunden geht meist nichts und es muss alles online umgesetzt werden – Telefonnummern von Blacklist-Providern gibt es keine und auf Emails wird nicht geantwortet.

TIC The Internet Company AG empfiehlt unbedingt, präventive Sicherheitsmassnahmen gemäss diesem Whitepaper auszuführen oder besser gleich auf Hosted Exchange zu wechseln, da ist nämlich der Provider verantwortlich und der Endkunde profitiert erst noch von einer ganzen Menge Zusatzleistungen (wie Mobile-Mail, integrierte Antivirenfunktionen, etc.).

4.3 Warum kommt ein TIC-Server auf eine Blacklist?

Wenn ein TIC-Kunde, typischerweise ein Mail-Kunde, einen Virus auf seinem Computer hat und ins Internet verbindet, Massenmails über den TIC-Mailserver versendet oder sogar Spam generiert (bewusst oder unbewusste Spam-Generierung), dann kommt der TIC-Mailserver auf die Blacklist. Die Folge: Andere TIC-Kunden sind im Email-Versand ebenfalls eingeschränkt.

4.3.1 Massnahmen von TIC The Internet Company AG:

- Selbstverständlich verfügt TIC über entsprechende präventive Einrichtungen: Im Hintergrund sind mehrere physikalische Maschinen vorhanden, es kommt also nur eine Maschine bzw. IP-Adresse auf die Blacklist und es ist nicht die gesamte TIC-Kundschaft betroffen.
- Sämtliche störungsverursachenden Kunden von TIC werden über ein automatisches System aus Sicherheitsgründen umgehend abgeschaltet, egal ob es sich um einen ADSL- oder Standleitungskunden handelt.

TIC The Internet Company AG unternimmt alles Mögliche, um die Einschränkungen für Kunden möglichst gering zu halten.

Dennoch, die bessere Alternative: Kunden mit Hosted Exchange, also eigenem virtuellem Mailserver, sind von diesen Einschränkungen nicht betroffen.

5 Relaying

5.1 Mailserver-Missbrauch

Unter Relaying versteht man, dass ein Mailserver einen anderen Mailserver zum Versenden von Emails beansprucht. Typischerweise benutzt ein Mailserver über die Internetverbindung von TIC den TIC-Mailserver als Ausgangsserver und missbraucht somit einen andere Mailserver, in diesem Fall den TIC-Mailserver.

Relaying kommt aber auch vor, wenn ein Kunden-Mailserver durch einen «Spammer» für den Spamversand missbraucht wird. Die Folge sind meist eine überlastete Internetverbindung und der Mailserver landet auf einer Blacklist, die betroffene Firma kann Emails kaum noch versenden.

Relaying-Konfigurationen über TIC-Mailserver sind nach geltenden Internet- und Antispam-Richtlinien als auch gegenwärtigen Sicherheitsanforderungen nicht weiter zulässig. Kunden mit eigenen Mailserver, welche einen TIC-Mailserver als Postausgangsserver verwenden, müssen diese Einstellungen zwingend ändern.

5.2 Empfohlene Massnahmen gegen «Relaying»

Wer einen TIC-Mailserver für den Postausgang verwendet, muss aus erläuterten Sicherheitsgründen zum Wohl der gesamte TIC-Kundschaft und gemäss Internet-Standards Massnahmen ergreifen:

- **Umkonfiguration des firmeneigenen Mailserver, dass dieser direkt über DNS-Auflösung (Domain Name System) Mails versendet.**

Das hat weiter den Vorteil, dass Mails vom Absender-Server direkt und ohne weitere Verzögerungen zum Ziel-Server gelangen (weniger aktive Komponenten und höhere Zuverlässigkeit).

- **Berücksichtigung der Sicherheitsmassnahmen gemäss diesem Whitepaper-Dokument.**
- **Alternative: Wechsel auf Hosted Exchange, welche alle gegenwärtigen und zukünftigen Sicherheitsvorteile beinhaltet.**

«Einen eigenen Mailserver zu betreiben erfordert ein hohes Mass an Fachwissen und vor allem permanente Betreuung sowie Anpassungen an sich ständig ändernde Gegebenheiten.»

*«Die Alternative: Hosted Exchange – **Alle Vorteile eines eigenen Inhouse-Mailserver**, günstigere Kosten und maximale Zuverlässigkeit.»*

5.3 Kunden ohne eigenen Mailserver

Kunden ohne eigenen Mailserver können weiterhin folgende Mailserver verwenden:

Email	
Posteingangsserver (POP3/IMAP Server)	pop.switzerland.net - oder - mail.tic.ch (nur wenn im zugestellten Datenblatt so angegeben) Wichtiger Hinweis: pop.vianetworks.ch wird per 30. Juni 2006 eingestellt. Bitte nehmen Sie zwingend die Migration von pop.vianetworks.ch auf pop.switzerland.net vor.
Postausgangsserver (SMTP Server)	smtp.switzerland.net - oder - smtp.tic.ch (nur wenn im zugestellten Datenblatt so angegeben) Mailversand bei eigenen Mailservern, z.B. eigener Microsoft Exchange Server: Verwenden Sie zwingend «DNS-Auflösung» zum Versand von Emails von einem dedizierten Kundenmailserver. Für «Mail-Relay» Services kontaktieren Sie bitte das TIC Verkaufsteam. Wichtiger Hinweis: mail.vianetworks.ch wird per 30. Juni 2006 eingestellt. Bitte nehmen Sie zwingend die Migration von mail.vianetworks.ch auf smtp.switzerland.net vor.

Die neusten Informationen sind verfügbar: www.tic.ch/support

5.4 POP, IMAP, SMTP Server Einstellungen

Die Server-Angaben sind auf der Homepage von TIC The Internet Company AG online verfügbar:

www.tic.ch – Support – Technische Infos (Subrubrik «Konfigurationen»)

Server Konfigurationen: www.tic.ch/de/support/konfigurationen.php

6 Mail Backup Queue (SMTP Queue)

6.1 Email Zwischenspeicherung für Firmen-Mailserver

Sie betreiben einen eigenen Mailserver und möchten zusätzlich eine SMTP Backup-Queue (Mail-Hosting), **um Überlastungen und Serverstörung zu überbrücken?** TIC The Internet Company AG bietet Ihnen die Mail Backup Queue einfach und kostengünstig an. Die Aufschaltung ist erst noch innert wenigen Minuten möglich. So profitieren Sie von maximaler Email-Erreichbarkeit und Stabilität.

6.2 So erhalten Sie Mail Backup

1. Mitteilung der Domain, welche für Mail Backup Queue aufgeschaltet werden soll (z.B. firma.ch)
2. TIC konfiguriert die Mail Backup Queue auf der TIC Provider Infrastruktur
3. Erfassung eines weiteren MX-Records auf Ihrem DNS (TIC übernimmt dies für Sie oder gibt Ihnen genaue Informationen)
4. Fertig – Mail Backup ist aktiviert und Sie profitieren von maximaler Email Zuverlässigkeit

Hinweis: Ergänzen Sie Ihren Mailserver mit der leistungsfähigen Antispam- und Antivirus Lösung von TIC. Jetzt kostenlos während 30 Tagen unverbindlich testen... www.tic.ch/de/itservices/antispam.php

6.3 Produkteübersicht Mail Backup

Artikel	Artikel-Bezeichnung und Artikel Detailbeschreibung	Preis exkl.	Preistyp
300034	Mail Backup Queue – Einrichtung Konfiguration der Mail Backup Queue für die erste Domain auf der Mail Backup Infrastruktur - Konfigurationen auf Mail-Infrastruktur - Zweiter MX-Record: mailbackup.switzerland.net (Kunde erhält Information zur Erstellung des MX-Records falls DNS nicht bei TIC The Internet Company AG gehosted ist). - 1 Domain: ###	180.00	Stück
300036	Mail Backup Zusatzdomain – Einrichtung Erfassung 1 weitere Domain für Mail Backup Queue - 1 Domain: ###	70.00	Stück
300033	Mail Backup Queue – Monatsabo Speicherung von ankommenden Emails auf einem Backup Queue Mailserver von TIC The Internet Company AG, falls der primäre Ziel-Mailserver nicht erreichbar ist. Der Backup Queue Server versucht Emails in verschiedenen Intervallen während 120 Stunden an den primären Mailserver zuzustellen, bevor diese an den Absender retourniert werden. - Nachrichtengrösse max. 30 MB	28.00	Monat

	<ul style="list-style-type: none"> - Sessiongrösse max. 300 MB - Messages per Connection max. 20 - Speicherplatz max. 1'000 MB (1 GB) - 1 Domain: ### 		
NEU	<p>Mail Backup Queue Speicher – Monatsabo</p> <p>Zusätzliche Speicherkapazität pro Backup-Domain, als Ergänzung zum regulären «Mail Backup Abonnement».</p> <ul style="list-style-type: none"> - Speicherplatz max. 10'000 MB (10 GB) - 1 Domain: ### 	36.00	Monat

7 Über TIC The Internet Company AG

7.1 www.tic.ch

TIC The Internet Company AG ist ein international ausgerichteter Full Service Internet- und IT-Provider für professionelle LAN- und WAN-Lösungen anspruchsvoller Geschäftskunden mit Sitz in der Zentralschweiz. Das unabhängige Gigabit IP-Netzwerk mit mehrfach redundanten Anbindungen sowie hochstehenden Datacentern erfüllt höchste Qualitätsansprüche für nationale und internationale Kunden in den Bereichen IP-VPNs, MPLS, Mobile Office, Mobile Mail, Hosted Exchange, VoIP Internet-Telefonie, Managed ICT Services und Internet-Zugang.

Das paneuropäische Tätigkeitsgebiet erstreckt sich flächendeckend über die ganze Schweiz und umfasst mit zahlreichen Partnerschaften Europa, Nordamerika und China.

Innovative IT Lösungen, vom Infrastruktur-Betrieb mit Managed Solutions bis hin zu kompletten Outsourcing-Dienstleistungen, reduzieren bei Kunden die Kosten bei gleichzeitig gesteigerter Sicherheit und Produktivität. Das umfangreiche Managed Security Portfolio und die umfassenden 7x24 Customer Care Support Dienstleistungen ergänzen die moderne Dienstleistungspalette von TIC The Internet Company AG.

TIC The Internet Company AG ist ein Unternehmen von Solution24 AG, Rotkreuz/Zug, entstanden aus VIA NET.WORKS (Schweiz) AG und TIC.

International Business: Full Service Internet- and IT-Provider – We Connect the World

