



Das Lübecksche Maildreieck

**... eine Variante zur
kostenlosen Sicherung des
Mailverkehr in kleinen und
mittelständischen Unternehmen
(KMU)**

**- Basierend auf frei
verfügbaren Ressourcen -**

Einleitung

Grundsätzliches

...Es ist in der Regel mit einigem technischen und finanziellen Aufwand verbunden, eine sinnvolle und wirtschaftliche Lösung zur Sicherung des Mailein- und Ausgangs zu gewährleisten.

Aus der Praxis, konnte ich jedoch entnehmen, wie bedeutsam dieses Thema für kleine und mittelständische Unternehmen ist. Ergo musste ich einen Lösungsansatz konzipieren der praktikabel und sehr kostengünstig ist.

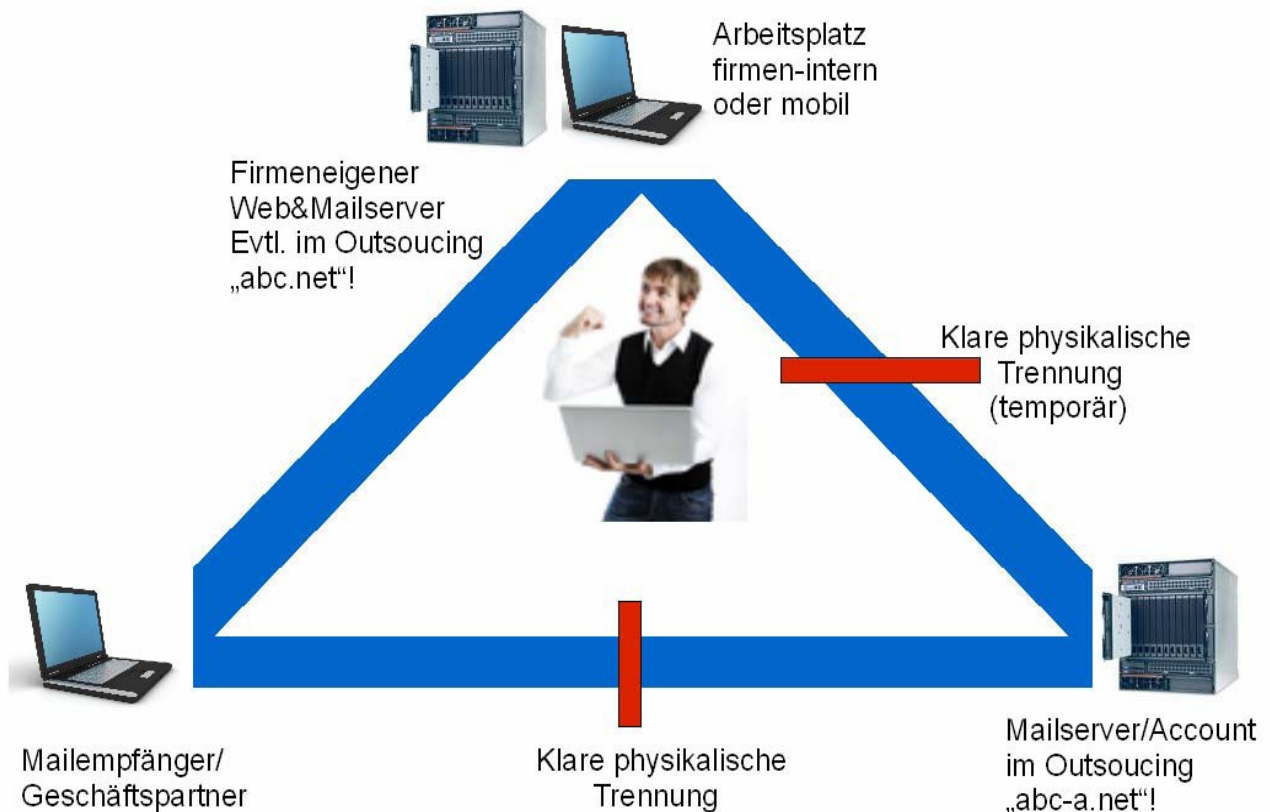
Die Idee besteht darin, durch die Nutzung vorhandener Ressourcen und frei verfügbarer Mittel, ein Verfahren zu etablieren, dass die Ansprüche einer adequaten Sicherung der Firmen-Mail Kommunikation Rechnung trägt, eine Art High Uselibility System (HUS).

Es sollte des weiterem mit geringem technischen Aufwand realisierbar sein und eine sehr hohe Verfügbarkeitsrate aufweisen.

Daher entstand die Idee des "Lübeckschen Mail-Dreieck"

Grundtenor:

1. **Nach einem Crash muss meine Mail- Kommunikation schnell restaurierbar sein.**
2. **Die hohe Verantwortung sollte auf mehrere Ressourcen verteilt werden.**
3. **Die Verfügbarkeits-Rate sollte nahezu verdoppelt werden**



Wirkungsweise

Das Prinzip der doppelten Datenführung

Datenbestand: Sever „abc.net“ = Datenbestand Server „abc-a.net“

(Spätestens am Ende des Arbeitstages)

Die Idee musste in die Richtung gehen, die Verantwortung für die Verfügbarkeit der Mail-Kommunikation zu splitten, auf mehrere „Schultern“ zu verteilen. Es lag nahe, einen „Standby Account“, hier abc-a.net genannt, zu etablieren. Dieser „Standby Account“ fungiert ähnlich des hinreichend bekannten Standby Server Modell, mit dem Unterschied, dass er in meinem Modell immer out- gesourcet ist.

Es werden defacto 2 von einander unabhängige Accounts auf 2 physikalisch von einander unabhängigen Servern betrieben.

Wie schon erwähnt, kann abc-a.net auch inhouse stehen. Ich persönlich bin kein Freund der inhouse Lösung. Lassen Sie mich die Begründung auf eine kurze Formel reduzieren.

Inhouse = zwei Server in einem Gebäude, beide Server sind der selbem latenten Gefahr ausgesetzt.

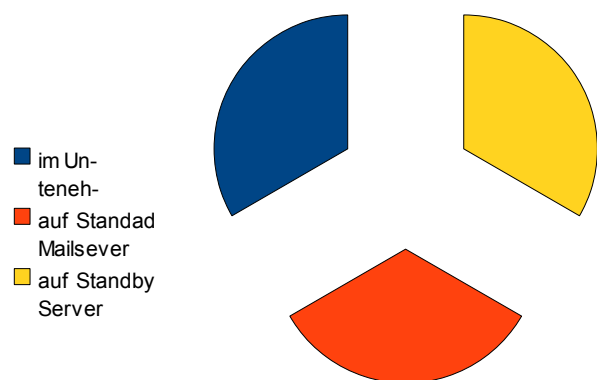
Das bedeutet:

Im Ernstfall (Einbruch, Brand, einem viralem bzw. kriminell motiviertem Angriff, sind die Datenbestände beider Server 1:1 in Gefahr.

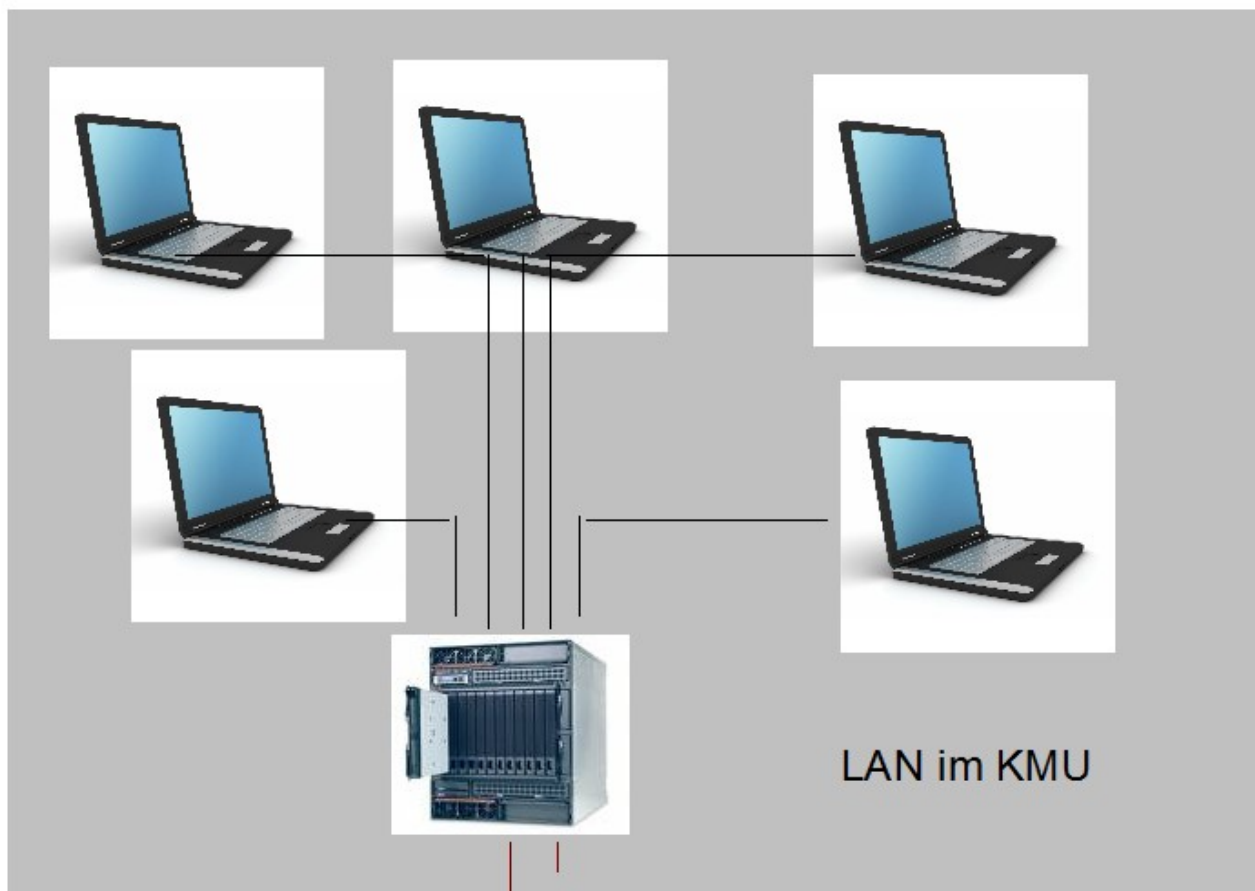
Beim Modell des „Lübeckischen Maildreieck“ liegt eine Spiegelung des gesamten Verkehr auf einem Server bei einem Host Ihres Vertrauens. Die Gefahr eines Totalverlust Ihrer Mailkommunikation wird auf 50% reduziert.

Berücksichtigen wir Ihre inhouse Backup, die im besten Fall noch außerhalb Ihres Firmengebäudes lagern, reden wir über eine Gefahr von 33%.
Mailverkehr auf Cilenten im LAN
Mailverkehr auf Server im LAN
Mailverkehr im Outsourcing.

Abb 10



Genug der Theorie: Ich habe mal ein Netzwerk eines KMU, wie es 100.000fach in Deutschland existiert dargestellt, ich nenne es mal „LAN X1“. Ich denke, hier kann ich das Prinzip des „Lübeckischen Maildreieck“ gut verdeutlichen.



Kommerzieller
Web/Mail Server



Kostenloser
Mailclient

„LAN X1“

INHOUSE Backup
extern gelargert

Client/POP

Client/POP

Client/POP

Client/POP

Client/POP

z.B. Router
im KMU + Firewall

WWW / POP3 / SMTP Server

Standad
Mailserver

Standaby
Mailserver

Das vorangegangene Organigramm soll eine von vielen Möglichkeiten der Implementierung im KMU verdeutlichen. Alle Endpoints/Clients haben Anbindung an beide Mailserver bzw. -Accounts.

Wenn nun eine relevante Mail das KMU erreicht, ist der Mitarbeiter per Dienst-anweisung instruiert, diese an den Standby-Mailaccount bzw. Server weiter zu leiten. Das bedeutet, jede eingegangene Mail, existiert nach der Prüfung auf Relevanz durch den Mitarbeiter doppelt. (sh. Formel) Das selbe Procedere geschieht beim Senden einer Mail. Der Mitarbeiter wird angewiesen, ausgehende Mails zusätzlich an den Standby Server/Account zu übermitteln. So wird Step by Step eine onDemand Spiegelung des Mailverkehrs erzeugt.

Implementierung:

... Jede eingehende und ausgehende eMail des KMU wird an einen zweiten, autonomen Mailclient/-Server (Standby Server/Client) übermittelt.

Der Zugang zum Standby Server/Client ist ausschließlich einem ausgewählten Personenkreis (Inhaber + Administrator) zugänglich und wird engmaschig überwacht.

Der Administrator trägt die volle Verantwortung für den Standby Server/ Clienten und erstellt intervallmäßig ein optisches Backup/ Mirror, welches

außerhalb des Firmengebäudes gelagert wird.

Es erfolgt eine engmaschige Mailvirus Überwachung aller implementierten Schnittstellen.

Der Admin stellt die höchst mögliche Verfügbarkeit beider Server/Accounts sicher.

Das Ziel:

abc.net = abc-a.net = Backup auf optischem Datenträger (an einem intervallmäßig definierten Zeitpunkt)

Was meint der Begriff intervallmäßig?

Es ist notwendig, den „Datenstand“ der Formel hin und wieder einer Prüfung zu unterziehen. Dies ist Aufgabe des Inhabers des KMU bzw. einer vom Inhaber benannten Person (Admin). Diese Prüfung kann zum Beispiel durch Abgleich der Volumina beider Clients erfolgen, sollte an einem Zeitpunkt festgemacht werden.

$$Tx = V abc = V abc-a$$

...zu einem Zeitpunkt im Arbeits-Alltag (Tx) wird manuell geprüft, ob die Volumina des Datenbestandes von abc.net (V abc) und abc-a.net (V abc-a) identisch sind.

Es ist nun von der Beschaffenheit des KMU abhängig, in welchem Intervall Tx (Zeitpunkt der Synchronität beider Server) eintritt. Ich empfehle es spätestens am Tagesende.

Gestatten Sie mir in diesem Context, einige wenige Sätze zum Thema Spam.

Grundsätzliches muss die Frage geklärt sein **Erlaube ich die private Nutzung von www und Mailclients im KMU oder nicht?**

Hier würde ich differenzieren, die Reservierung einer Fahrkarte für eine Dienstreise oder die schnelle Mail „Ich

mach Überstunden“, ist rechtlich anders zubewerten als z.B. die Eröffnung eines privaten eBay Kontos eines Mitarbeiters.

Ein grundsätzliches Recht auf privates Surfen im KMU besteht nicht.

Jetzt stellt sich die Frage : Sicher ich private Mails mit?

NEIN = Wenn ich die private Nutzung erlaube, darf ich private Inhalte, Cookies etc. nicht zur Kenntnis nehmen oder gar sichern.

Das bedeutet natürlich rein von der Infrastruktur einen erheblichen Mehraufwand.

Daher würde ich die private Nutzung von Firmen- Mailclients ganz eng definieren.

Warum der Aufwand?

An Hand dreier willkürlich/realitätsnaher Problemfälle, möchte ich kurz das Wirkungsprinzip des „Lübeckschen Mail-Dreiecks“ darlegen. In jedem der drei Szenarien haben wir einen Mailserver „abc.net“ und den Backup-Mailserver „abc-a.net“.

Abc.net und abc-a.net gehören 2 von einander physikalisch unabhängigen Hostern an. Grundlage ist unser „LAN X1“ :

Das Szenario "A"

Das Unternehmen ABC sendet täglich ca. 50 geschäftliche Mail (Angebote, Kalkulationen etc. über den firmeneigenen Account angebot@abc.net bzw. info@abc.net (im LAN X1). Es nutzt den Mail Clienten Outlook:

Eines schönen Freitag Nachmittag, hat

der Conficker über die Lücke MS08-067 in Ihrem System eingenistet und fühlt sich heimisch. Ihre Mailkommunikation ist faktisch tot und eventuell verloren. Die Anfrage für den 100.000 € Auftrag war auch dabei.

Ein schönes Wochenende!?

Mit diesem Mail Management Konzept Ja! Denn, als die Anfrage für den 100.000 € Auftrag einging, hat Ihre Sekretärin laut Ihrer Arbeits -anweisung, umgehend an backup@abc-a.net (auf externen Server) weiter geleitet und Sie können ihn problemlos, wenn der Admin Ihr Conficker-Problem behoben hat, per POP3 rücksichern und wie gehabt in Ihrem Posteingang verwalten.

Das Szenario „B“

Das Unternehmen ABC erhält einen Liefertermin eines Zulieferers per Mail. Der Termin wird ordnungsgemäß im Out.. festgehalten. Durch ein physikalisches Festplatten-Problem gehen alle Termindaten den Bach hinunter.

Das große Chaos?

Mit diesem Mail Management Konzept, Nein! Denn Sie haben Ihre Sekretärin instruiert, alle geschäftsrelevant eingehenden Mails an **umgehend an backup@abc-a.net weiter**

zuleiten und Sie können ihn

problemlos, wenn der die Festplatte wieder läuft bzw. Sie für 69,00 € im Fachhandel eine neue geholthaben, Ihre Eingangs-Mail per POP3 rücksichern und wie gehabt in Ihrem Posteingang verwalten.

Das Szenario „C“

Sie sind ein Einzelhändler für Angelsportbedarf. Sie betreiben einen kleinen Laden in einer Großstadt, zentrumsnah, Parkmöglichkeiten sind eher nicht vorhanden. 41% Ihres Jahresumsatzes generieren Sie aus eBay Aktivitäten bzw. aus Aktivitäten des eigenen Webshop's.

Alle Bestellung aus beiden Portalen laufen auf bestellung@abc.net zusammen.

„Whatever can go wrong, will go wrong“ (Morphy)

Das Rechenzentrum des Hosters (abc) Ihrer Domain ist tagelang nicht erreichbar.

Sie kommen nicht an Ihre Neubestellungen und als wenn das Chaos nicht ausreichend wäre, der Kunde bekommt sein per Typo3 generiertes Bestell-Formular als „unzustellbar“ in seinen Posteingang zurück. Der Kunde ist definitiv weg.

Das ganze Dilemma bemerken Sie 5 Stunden nach dem Knockout. Klar, diese 5 Stunden sind für Ihr Internetgeschäft verloren! Aber nun, da Sie das Problem erkannt haben, können Sie sehr zeitnah reagieren und vorübergehend backup@abc-a.net bei eBay als Bestelleingangs-Adresse konfigurieren.

Wenn ABC wieder läuft, drehen Sie das Prinzip des „Lübeckischen Mail-Dreieck“ ganz einfach um,

<<abc-a.net wird nun nach abc.net gespiegelt.>>

buchen in Ihrem ERP nach und der Schaden hält sich in akzeptablen Grenzen, sowohl wirtschaftlich als auch bzgl. des zusätzlichen Zeitaufwands. So gewährleisten Sie wieder die

Synchronität beider Accounts. Nachfolgend mal ein Exemple, wie eine Ausgangs-Mail aussehen sollte.

Nun gehen wir einmal davon aus, die schlimmst- mögliche Variante tritt ein und ABC ist 36 Stunden nicht verfügbar. Das ein Problem aufgetreten ist bemerken Sie nach 3 Arbeitsstunden. Sie kennen die Gründe nicht, Ihr Support des Outsourcing Partners ist nicht verfügbar.

Welche Vorteile bietet Ihnen nun das „Lübeckische Mail-Dreieck“?

- 1. Ihre komplette bzw. relevante Teile Ihrer Mail-Korrespondenz (Ein- und Ausgang) liegt/liegen gespiegelt auf abc-a.net**
- 2. abc-a.net kann mit wenigen Handgriffen, alternativ / vorübergehend zu abc.net, in Ihrem Mail-Client und ERP eingebunden Ausgang (POP) genutzt werden.**
- 3. Bei einem Totalausfall von abc.net kann abc-a.net zeitnah als Mailserver der Firma agieren.**
- 4. Es basiert auf frei verfügbaren Mitteln, da abc-a.net ein Freemail Account sein kann und verursacht daher keinerlei Kosten, es muss nicht aufwendig implementiert werden, da es prinzipiell onDemand läuft. Es ist keine zusätzliche Hard- oder Software erforderlich.**
- 5. Sie selbst können nun sofort geeignete Maßnahmen ergreifen, um Ihren Mailverkehr sicher zustellen, ohne Administrator, ohne Fremdfirma.**

Voraussetzungen und Umsetzung

Infrastruktur:

Sie benötigen Ihre eh existierenden Mail- Accounts und einen zweiten Freemail Account eines andern Host.

Investition = 0

Achten Sie beim implementieren neuer Mailschnittstellen darauf, dass eine Anbindung an abc-a.net mittels POP/BCC gewährleistet ist. Ich empfehle unter abc-a.net, die Option „Save Copy on Server“ bzw. und abc-a.net, in Kombination mit Outlook „Kopie auf Server belassen zu nutzen, diese Maßnahme gibt zusätzlich einen Rückhalt. Natürlich sollte ich in diesem Fall eine Zugriffskontrolle/ Protokollierung für abc-a.net fahren.

Das technische Knowhow entnehmen Sie bitte der Anleitung zu Ihrem Mailprogramm/Clients, da es von Anbieter zu Anbieter variieren kann. Es ist in der Regel unter den Stichpunkten „Mailclient“, „Post Operating Protocol (POP)“ und „Simple Mail Transfer Protocol (SMTP)“ zu finden.

Beim Rücksichern beachten!

1. POP des Backupclients einrichten
2. Mails rücksichern
3. rückgesicherte Mails vom Posteingang in den Postausgang verschieben**(es ist Ihre Ausgang-Korrespondenz!)**
4. POP des Backupclients durch POP des normalen Firmenclients ersetzen.

Im Allgemeinen werden Sie Ihren POP

Dienst bei dem Anbieter nutzen, bei dem auch Web-Präsenz liegt, das ist Imagetechnisch gut. Sicherlich muss nicht jeder Kunde Ihren Backup-Server kennen. Es ist auch fraglich, ob jeder Ihrer Mitarbeiter Einblick in Ihre Sicherheitsvorkehrungen haben muss.

„Informationen schaden demjenigen, der sie nicht hat“

Daher kann der BBC Versand natürlich auch 1x täglich als Sammelversand durch eine autorisierte Person erfolgen. Das ist dann nur eine Frage der Administrations Rechte auf abc-a.net. In dem Fall, kann man einfach kurz vor Feierabend, alle Ausgangs-Mails des Tages im Mail-Client markieren und an die CC Adresse (backup@abc-a.net) weiterleiten, es muss ja nicht direkt jeder mitbekommen.

Eins sei der Genauigkeit wegen an dieser Stelle erwähnt. Es wird sicherlich problematisch sein, dass originale Datum des Sendens an den Empfänger, bzw. des Erhalts der Mail zu rekapitulieren, da bei der Weiterleitung, auch Datum und Zeit der Weiterleitung an den BCC übertragen werden. Gesendete Objekte des aktuellen Tages markieren – „weiterleiten“ in der Outlook Menüzeile wählen – an backup@abc-a.net .

Noch ein paar Sätze zur Wirkungsweise & technischem Hintergrund. Ein Mailserverdienst, egal ob er in Ihrer Firma steht oder bei Ihrem Outsourcing Unternehmen, kann aus einer Vielzahl von technischen oder politisch/ terroristisch motivierten Gründen, von einer Minute auf die nächste, nicht mehr verfügbar sein.

Auf deutsch : Keine Typo3 oder HTML Oberfläche, kein POP3, kein SMTP

Sie kommen Minuten, Stunden evtl. einen Arbeitstag **nicht** an Ihre aktuelle Unternehmens-Mail Kommunikation.

Wie dem vorangegangenen Struktogramm (Abb. 1) zu entnehmen ist, können Sie nun vorübergehend, komplett auf den zweiten Anbieter ausweichen.

Wenn Ihr Tagesgeschäft sehr von Mail-Kommunikation bestimmt wird, bietet es sich zusätzlich an, an „neuralgischen“ Punkten (Firmenleitung, Auftragswesen, Rechnungswesen...) standardmäßig zwei Mailclients jeweils an einen Server anzubinden.

Somit haben Sie das Risiko eines totalen Knockout geviertelt. „Ein Fallschirm firmenintern, einer im Outsourcing.“

Bsp.
Das normale Tagesgeschäft regle ich über Outlook 2007 und zur Administration von abc-a.net nutze ich die Open-Version von Eudora 7, geht aber auch mit jeder anderen Kombination von Mailclients. Es ist dann nur relevant, welchen POP welchem Client gehört.

In unserem Fall wäre
POP von abc.net = Outlook
SMTP von abc.net = Outlook
und
POP von abc-a.net = Eudora

Ein SMTP für abc.a.net ist nicht zwingend erforderlich.

Es sei an dieser Stelle noch mal auf die allgemeinen Verhaltensregeln in Bezug auf Protokolleinstellungen und Viren – Prophylaxen hingewiesen.
An dieser Stelle seien noch ein paar Verhaltens-Vorschläge zum Umgang auf mit abc-a.net erlaubt.

1. Einen Client für abc-a.net nur **auf einem maximal zwei PC** (Chef/Admin) einrichten. Diesen Client besonders schützen z.B. gesonderte Administrationsrechte
2. Eine schriftliche Arbeitsanweisung zum Umgang mit abc-a.net an alle relevanten Mitarbeiter ausgeben. Hierbei muss der Lagerarbeiter nicht verstehen, was abc-a.net ist, er muss wissen, dass er ihn zu nutzen hat.
3. regelmäßig physikalische Backups von abc-a.net fahren und diese firmenextern lagern.
4. Viren- Prophylaxe für abc-a.net

... Ich verstehe die beschriebene Variante nicht als „Allheilmittel der Mailsicherheit“. Angesichts den großen Kostendruck im Bereich der KMU, ist sie jedoch ein geeignetes Mittel, geschäftlich relevante elektronische Post zu sichern. Ich praktiziere dieses Prinzip in KMU verschiedener Branchen erfolgreich. Die große Angst vor dem totalen Knockout, sollte hiermit genommen werden.

Es wird aber auch klar, dass ich agieren muss. IT-Sicherheit ist kein Selbstläufer.

Ich bedanke mich, für Ihre Aufmerksamkeit. Für Rückfragen stehe ich gern zur Verfügung

IMPRESSUM

Herausgeber/Redaktion/Inhalt

© 2009 Swen Lübeck

Györer Straße 2/08

99089 Erfurt

Fon : +49 361 555 93 670

Fax : +49 361 555 93 68

Mail: luebeckweb@gmx.net

<http://www.123-eintrag.de/suchmaschinen/suchmaschinen-eintrag.htm>

<http://4stats.de/de/stats?id=63983&contr=hide>