

## Mail Security

Bis zu 95 Prozent aller Mails sind heute Spam: Viren und Trojaner gefährden Ihre IT-Systeme. Manuell kann der Flut unerwünschter und gefährlicher Mailinhalte heute niemand mehr Einhalt gebieten. Sichern Sie ihre Mailsysteme und arbeiten Sie ungestört ohne Ausfälle mithilfe von **Mail Security!**

Vermeiden Sie (Spam) ...

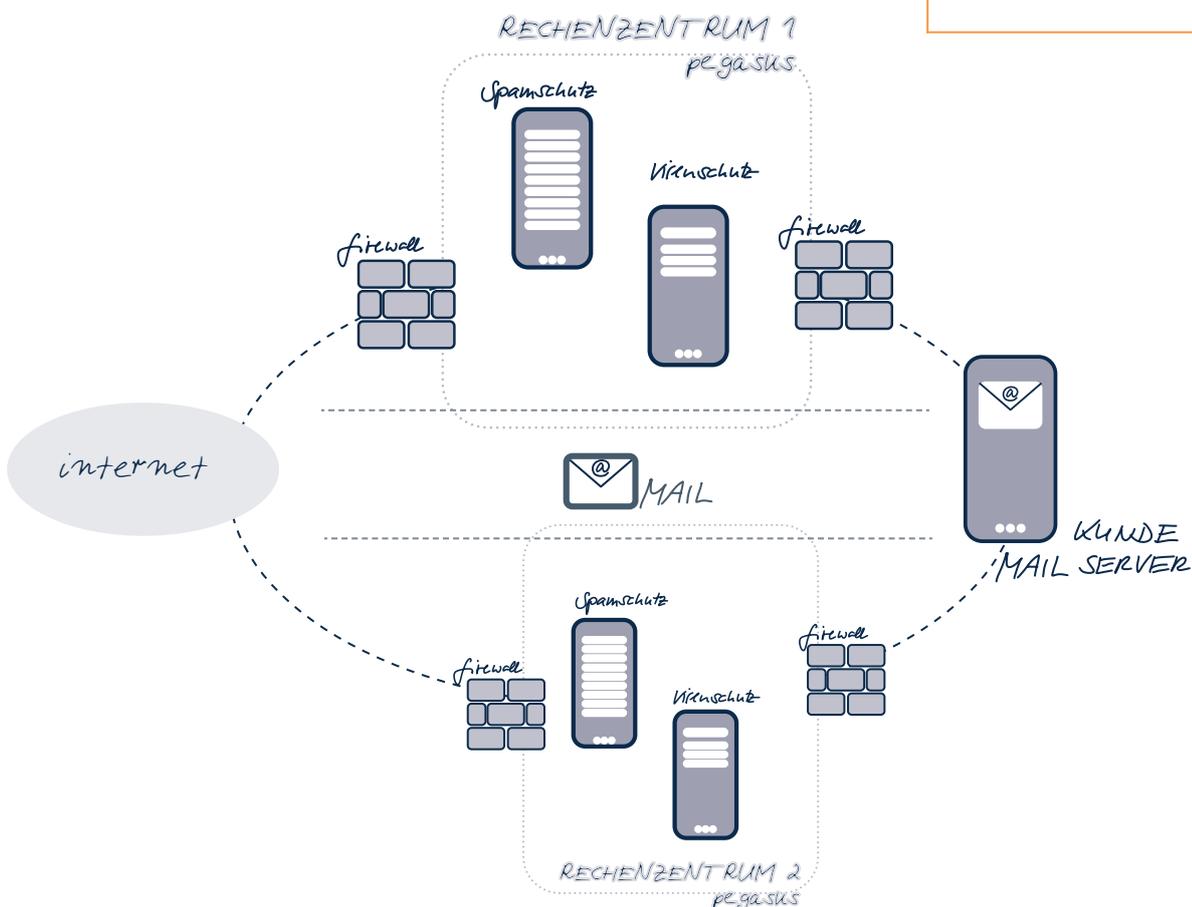
- unnötigen und unerwünschten Netzwerktraffic
- zusätzliche Arbeitszeit für das Personal
- den Verlust von Produktivität und Arbeitszeit
- Gefährdung durch Viren und Trojaner.
- die Beanspruchung großer Mengen an Speicherplatz und Rechenleistung.

Steigern Sie die Produktivität Ihrer Mailsysteme durch **Mail Security!**

## Lösung/Produkt

**Mail Security Service** basiert auf verschiedenen Techniken, um Spam-E-Mails und Viren mit hoher Sicherheit zu erkennen und zu markieren. Die eingehenden E-Mails müssen nur durch eine kleine Änderung im DNS (MX-Record) über unsere Server umgeleitet werden. Dabei wird eine Spambewertung vorgenommen und die E-Mails anschließend weiter zu Ihrem bisherigen Mailserver übertragen.

## MAIL SECURITY



pegasus IT ist zertifiziert nach DIN ISO/IEC 27001 im Bereich *Innovative Rechenzentrumsdienstleistungen und IT-Lösungen* und nach DIN ISO/IEC 9001 im Bereich des *Qualitätsmanagements*.



## Content Security

### Nutzen und Vorteile

- wartungsfrei
- ausfallsicher
- einfache und völlig transparente Anwendung
- keine Anschaffungskosten für Hard- oder Software
- keine Kosten für Administration und Updates
- kalkulierbare Kostenstruktur der Leistungen
- individuelle Black- und Whitelisten
- schnelle Reaktionszeit
- mehrstufige Virenprüfung mit aktuellen Virensignaturen.

## Leistungsbeschreibung

Die Komplexität und die Menge der von Spammern und Hackern versendeten E-Mails nehmen ständig zu. Dies, zusammen mit dem spezifischen Targeting von Unternehmen durch Mail-Bombing, DoS, Backscatter und andere Bedrohungen, erfordert ständig wachsende Ressourcen, um diesen Bedrohungen entgegenzuwirken. Die perimeterorientierte E-Mail-Sicherheitslösung des *Central Net Points (CNP)* hat die Fähigkeit, unerwünschten Verkehr, einschließlich Viren, Spam und Phishing, unabhängig von deren Inhalt, am IP- und E-Mail-Envelope-Level zu blocken. Dies setzt Bandbreite und Ressourcen für die Inhaltsanalyse der verbleibenden E-Mails durch Antivirus- und Anti-Spamfilter frei.

### Mail Security

<b>Lizenzierung</b>	<b>Per E-Mail-Adresse</b> Mailverteiler / und mailaktivierte öffentliche Ordner zählen ebenfalls als Mailadresse
<b>Internes Load Balancing</b>	Ja
<b>Betrieb in zwei getrennten Rechenzentren</b>	Ja
<b>Mailprotokolle</b>	<ul style="list-style-type: none"> <li>◉ SMTP / SMTPS optional mit LDAP-Anbindung</li> <li>◉ Webaccess</li> </ul>
<b>Antivirus</b>	ClamAV und eigene
<b>Anti-Spam-Engines</b>	11 Ebenen unter anderem inklusive: <ul style="list-style-type: none"> <li>◉ RPD™ (Recurrent Pattern Detection)</li> <li>◉ RBL (Realtime Black List)</li> <li>◉ ZDS™ (Zombie Detection System )</li> </ul>
<b>Verschlüsselungsverfahren</b>	<ul style="list-style-type: none"> <li>◉ PFS</li> <li>◉ TLS</li> <li>◉ not Heartbleed vulnerable</li> <li>◉ no weak ciphers</li> <li>◉ KEIN SSLv3</li> </ul>
<b>Statistik- und Auswertungsportal</b>	Ja
<b>Mailserverkompatibilität</b>	<ul style="list-style-type: none"> <li>◉ MS Exchange</li> <li>◉ Lotus Notes</li> <li>◉ GroupWise</li> <li>◉ Standard SMTP-Server</li> </ul> <i>Betreibt der Kunde keinen eigenen Mailserver, so ist ein Mailserver in Verbindung mit einem Internethostingpaket zusätzlich zu buchen.</i>
<b>Anbindung E-Mail-Archivierung</b>	CNP Mail Archive Standard SMTP-Archiv

## Features

verfügbar als:

- on premise IT**
- managed IT**
- cloud IT** ✓