



## Lassen Sie Ihren Email-Verkehr von Profis steuern!

antispameurope bietet umfassende, integrierte **Managed E-Mail Security Services**. Das Angebot erstreckt sich von Premium-Spam- und Virenschutz und E-Mail-Signierung über E-Mail-Continuity bis hin zur E-Mail-Archivierung.

Warum antispameurope Managed Services?

- Keine Software, keine Hardware, somit kein Wartungsbedarf
- Zentrales Management der Systeme durch IT-Security-Experten von antispameurope
- 24-Stunden-Überwachung, proaktives Incident-Management
- Voller 24/7/365 E-Mail und Telefonsupport
- Betrieb in redundanten, mehrfach gesicherten Rechenzentren in Deutschland
- Gesicherter Datenaustausch zwischen Kundennetzwerk und antispameurope

NUR GUTE NACHRICHTEN

NIE WIEDER  
SPAM!



## Spamfilter Service

Spamfiltersoftware auf dem Arbeitsplatz-PC oder auf dem Mailserver und übliche Spamfilter-Appliances haben alle das gleiche Problem: Sie werden In-House installiert. Schädliche Mails kommen dadurch bis in das Unternehmen und belasten unnötig die Internet-Anbindung und Infrastruktur. Zudem müssen diese Einrichtungen sorgfältig administriert werden, um den gewünschten Schutz zu bieten. Das verursacht erheblichen Aufwand. Bei nicht sachgerechter Administration kann der eigentlich beabsichtigte Schutz sogar ins Gegenteil verkehrt werden und Schaden durch Sicherheitslöcher oder verloren gegangene E-Mails entstehen.

Der Managed Spamfilter Service von antispameurope bietet klare Vorteile. Die Server, von antispameurope in redundanten gesicherten Rechenzentren betrieben, werden als Schutzwall im Internet noch vor der

Infrastruktur der Kunden installiert. Spam, Viren, Phishing-Mails und andere Malware wird sicher abgefangen, noch bevor sie die Unternehmens-IT überhaupt erreichen.

Zusätzlich enthält der Service einen individuell einstellbaren Contentfilter, der die detaillierte Festlegung und Einhaltung unternehmenseigener IT-Richtlinien für den E-Mail-Verkehr ermöglicht. Dadurch lassen sich gezielt Attachements aus eingehenden E-Mails herausfiltern. Je nach Definition durch den Administrator können bestimmte Dateiarnten zugelassen oder geblockt werden. E-Mails mit unerwünschten Anhängen werden entweder komplett geblockt und der Absender benachrichtigt, oder die nicht zulässigen Attachements werden entfernt und der Empfänger wird in der E-Mail darüber informiert. Der Administrator hat die Möglichkeit, die geblockten oder gefilterten Mails nachträglich zuzustellen.

Mit einer garantierten Erkennungsrate von 99,9% bei weniger als 0,0004% Falsch-Positiven ist antispameurope führend im Markt. Im statistischen Mittel werden sogar mehr als 99,99% Erkennungsleistung bei weniger als 0,0001% Falsch-Positiven erzielt. Auch Viren und Trojaner werden von zwei unabhängigen Filtern sicher erkannt garantiert werden 99,99% Erkennung.

## E-Mail Archivierung

Die Bedeutung von E-Mail Archivierung geht längst über die Entlastung der Mailserver hinaus. In Deutschland schreibt zum Beispiel die GDPdU seit 2002 die revisions-sichere Archivierung geschäfts-relevanter E-Mails zwingend vor. Die technisch eigentlich nötigen Systeme sind jedoch für den Mittelstand unerschwinglich. Der E-Mail-Archivierungs-service von antispameurope macht Compliance bezahlbar.

Rechtskonforme E-Mail-Archivierung erfordert nachweislich unveränderte und unveränderbare Speicherung über lange Zeit sechs, zehn oder sogar 30 Jahre. Viele Unternehmen archivieren E-Mails auf Papier, im Mailserver, in persönlichen Ordnern der Mitarbeiter oder über Backups. Dies dient zwar der Sicherung der Daten gegen Verlust die geforderte Revisions-sicherheit ist aber nicht gegeben. Denn die meisten Mailserver erlauben die Veränderung von E-Mails ohne Spuren schon mit dem Eintreffen auf dem Mailserver des Unternehmens ist es deshalb mit der Revisions-sicherheit vorbei.

Auch die geforderten langen Aufbewahrungs-fristen werden zum Problem. Scheinbar günstige Systeme sind meist gar nicht in Lage, Daten über die geforderte Zeit vorzuhalten. Die in größeren Unternehmen eingesetzten Archivierungs-systeme sind dagegen kaum zu bezahlen.

Der antispameurope E-Mail-Archivierungs-service speichert 100% Ihrer ein- und ausgehenden E-Mails jeweils so, wie sie Ihr Unternehmen erreichen bzw. verlassen. Die Archivierung interner E-Mails ist optional möglich. Die Daten werden außerhalb Ihrer IT in gesicherten Rechenzentren auf redundanten Systemen abgelegt. Der Service erfüllt die Compliance-Anforderungen z.B. nach GDPdU.

Archivierte E-Mails lassen sich über das Webinterface oder das Outlook-Plugin suchen und auf Knopfdruck erneut zustellen.

## E-Mail Verschlüsselung

Der antispameurope E-Mail Verschlüsselungs-service signiert und verschlüsselt ausgehende E-Mails und entschlüsselt eingehende E-Mails vollautomatisch und transparent ohne Benutzereingriffe. E-Mails werden damit zuverlässig gegen Ausspähung und Verfälschung geschützt.

Bisher ist es für Unternehmen teuer, kompliziert und aufwändig, ausgehende Geschäftsmails per Zertifikat gegen Ausspähung und Verfälschung zu schützen. Vor allem die Installation und Anwendung der Zertifikate ist umständlich, Signaturen müssen einzeln beantragt, freigeschaltet und für jeden Benutzer installiert werden. Das hochkomplexe Zertifikats-Management für E-Mail-Signaturen kostet Unternehmen viel Zeit und Geld. Die Lösung: Der vollautomatische E-Mail-Verschlüsselungs-Service von antispameurope. Der Service verschlüsselt ausgehende E-Mails im E-Mail-Gateway von antispameurope mit dem öffentlichen Schlüssel des E-Mail-Empfängers. Ob ausgehende E-Mails verschlüsselt werden sollen und wie im Falle fehlender Schlüssel verfahren wird, können die Kunden dabei in einer Policy festlegen. Die zur Verschlüsselung notwendigen öffentlichen Schlüssel des Empfängers werden automatisch aus signierten E-Mails extrahiert und gespeichert. Eingehende verschlüsselte E-Mails wiederum werden vom Gateway automatisch entschlüsselt. Diese Entschlüsselung wird im Header der E-Mail angezeigt. Alle ausgehenden E-Mails können zudem vollautomatisch signiert werden. Auch das wird in der Policy über das Webinterface im antispameurope Control Panel festgelegt.

Der Verschlüsselungs-Service übernimmt das komplette Zertifikats-Management für die Kunden. Verschlüsselung, Entschlüsselung und Signierung erfolgen vollautomatisch und transparent ohne weitere Benutzer-Eingriffe. Ein- und ausgehende E-Mails werden damit nicht nur gegen Ausspähung sondern auch zuverlässig gegen Verfälschung geschützt.

Jeder Nutzer erhält eine eigene Signatur ohne jeglichen Aufwand wie z.B. zusätzliche Installationen oder Wartung für den Benutzer und damit zu minimalen internen Kosten. Der Verschlüsselungs-Service kann mit allen gängigen E-Mail-Servern und -Clients genutzt werden. Einzige Voraussetzung ist die Verwendung des Spamfilter Service mit Mail-Relay.

## Webfilter Service

Versteckte Downloads von Viren und Trojanern, Phishing, unerwünschte oder so-gar kriminelle Inhalte - die Liste der möglichen Risiken beim unbedarften Surfen im Web ist lang. Gefährdung der Systemsicherheit, Datenverluste, Rufschaden oder Schadenersatzforderungen und dadurch finanzielle Verluste sind die Folgen. Schutz bietet der antispameurope Webfilter Service. Er blockiert zuverlässig den Zugang zu unerwünschten und gefährlichen Inhalten.

Der antispameurope Webfilter steht als Managed Service nicht nur den am Standort fest vernetzten Mitarbeitern zur Verfügung sondern auch Personengruppen, die mit mobilen Geräten im Außendienst arbeiten. Gefährliche Inhalte werden automatisch geblockt: Neben den Webseiten, deren Inhalte in über 15 Themenbereichen mit bis zu 18 Unterpunkten kategorisiert zugeordnet werden, wird der Datenverkehr auch auf verbotene Downloads und Viren geprüft.

Der Aufwand für Konfigurationen ist minimal, da über das zentrale Control Panel alle Einstellungen für alle Benutzer an allen Standorten durch Policies vorgegeben werden.

Die umfassende Vorkonfiguration ermöglicht Ihnen die reibungslose Einführung des Web-filter Services: Fertig erstellte Policies werden als Vorlage bereitgestellt. Über den zentralen Zugangspunkt des Control Panels können Administratoren Änderungen an der Standardrichtlinie für alle Benutzer vornehmen. Unterschiedliche Anforderungen verschiedener Benutzergruppen werden über zusätzlich konfigurierbare Policy-Gruppen abgebildet, wobei nur die jeweils notwendigen Themenbereiche angepasst werden müssen und alle anderen Berechtigungen vererbt werden.

Benutzer können bei gegebener Sperrung von Webseiten eine Freischaltung anfordern, die umgehend an den Verantwortlichen gemeldet wird. Anhand der Filterung aller ausstehenden, genehmigten und abgelehnten Anforderungen entsteht eine übersichtliche Liste, die mit einem Klick abgearbeitet werden kann. Eine benutzerfreundliche Rückmeldung über den Status der Anfrage wird automatisch verschickt. Freigaben einer Webseite können individuell dem anfordernden Benutzer, einer Policy-Gruppe oder pauschal allen Surfenden zugewiesen werden.

Zusätzlich zu den im Laufe der Zeit entstehenden Whitelists kann der Administrator eine grundsätzlich geltende Whitelist für bestimmte Webadressen importieren, ohne die Richtlinien für die übrigen Themenbereiche derselben Kategorie anzutasten. Alternativ können Filtereinstellungen grundsätzlich alle Kategorien bis auf explizite Ausnahmen verbieten (Explicit Whitelisting). Die nächste Ausbaustufe erlaubt zusätzlich die temporäre Freigabe von Webseiten (z.B. Surfen in der Mittagspause).

*Haben wir Ihr Interesse geweckt? Mehr Informationen erhalten Sie unter dem Kontakt oben rechts.*