eXpurgate 3.0

E-Mail-Sicherheit der nächsten Generation

eleven

E-MAIL-SICHERHEIT MADE IN GERMANY

E-Mail-Sicherheit Made in Germany

Herausforderung E-Mail-Sicherheit

Die E-Mail ist heute das wichtigste geschäftliche Kommunikationsmittel – und gleichzeitig eine der größten Gefahren für die IT-Infrastrukturen von Unternehmen. Der Hauptschuldige: **Spam!**

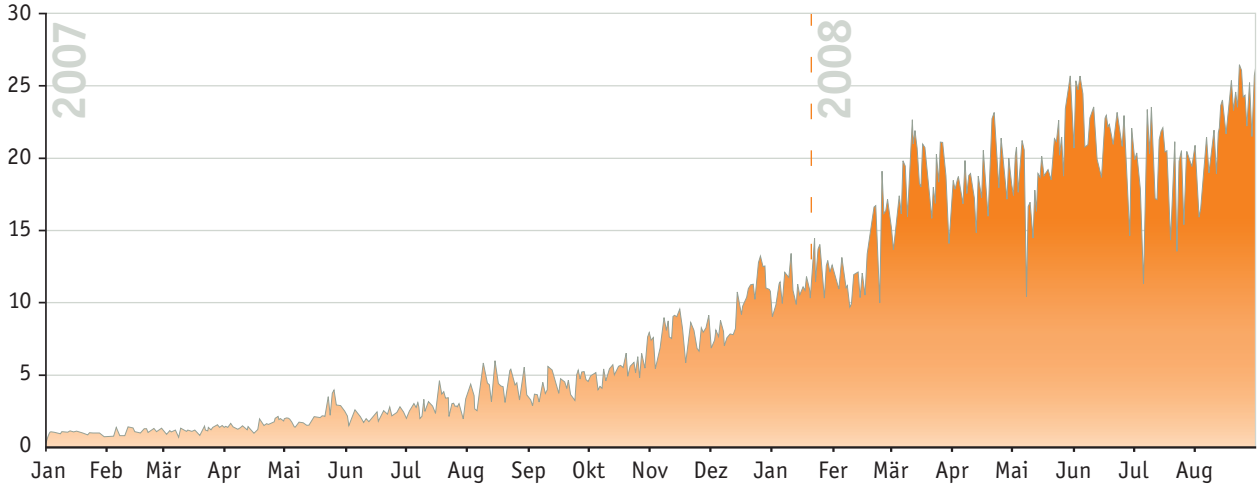
Die Gefahren

- Dauerhaft steigende Systembelastung durch das Spam-Wachstum
- Verlust geschäftsrelevanter E-Mails (False Positives) durch fehlerhafte Spam-Filter
- Überlastung der E-Mail-Infrastruktur durch Spam-Wellen oder gezielte Denial-of-Service-Attacken (DoS)

Schutz durch integrierte E-Mail-Sicherheit

- Leistungsfähige Anti-Spam-Lösung mit höchster Spam-Erkennungsrate und Ausschluss von False Positives
- E-Mail-Firewall zur Sicherstellung legitimer E-Mail-Kommunikation in jeder Situation
- Zuverlässiger Schutz vor Viren und anderer Malware – inklusive Früherkennung neuer Virenausbrüche

Spam-Aufkommen Januar 2007 – August 2008



E-Mail-Sicherheit Made in Germany

eleven ist der führende deutsche Anbieter integrierter E-Mail-Sicherheitslösungen für Unternehmen, ISPs und öffentliche Einrichtungen jeder Größe. eleven bietet ausgelagerte Managed Services sowie Inhouse-Software-Lösungen. Jeden Tag prüft eleven mehr als eine Milliarde E-Mails. Weltweit setzen über 30.000 Unternehmen die E-Mail-Sicherheitslösungen „Made in Germany“ ein.

Unter den Kunden von eleven befinden sich führende Internet Service Provider (ISP) und Telekommunikationsdienstleister wie T-Online, O2, Vodafone, Freenet und Lycos Europe, namhafte Großunternehmen, darunter Mazda, Air Berlin, DATEV, Tobit Software AG und die Landesbank Berlin, sowie führende Bildungseinrichtungen wie die Freie Universität Berlin.

Die Technologie: eXpurgate

Mittelpunkt der eXpurgate Technologie ist der „Bulkcheck“. Ein eigens entwickelter Kontrollsummen-Algorithmus reduziert jede E-Mail auf einen Code von nur wenigen Bytes, der in der eXpurgate Datenbank mit denen anderer E-Mails verglichen wird. Wird der gleiche oder ein ausreichend ähnlicher Code häufig genug gefunden, besteht die hohe Wahrscheinlichkeit, dass es sich um Spam handelt. Mit Hilfe weiterer Prüfverfahren können unerwünschte (Spam) zuverlässig von erwünschten Massen-E-Mails (z. B. Newsletter) unterschieden werden. Durch das Massen-E-Mail-Kriterium wird sicher verhindert, dass individuelle Nachrichten fälschlich als Spam aussortiert werden (Zero False Positives). eXpurgate erkennt nicht nur Spam, sondern kategorisiert zuverlässig jede eingehende E-Mail, z. B. als clean, bulk oder Spam. Derzeit klassifiziert eXpurgate nach 16 unterschiedlichen Kategorien.

eleven
E-MAIL-SICHERHEIT MADE IN GERMANY

E-Mail-Sicherheit der nächsten Generation: eXpurgate 3.0

Mit der Version 3.0 der bewährten E-Mail-Sicherheitslösung eXpurgate stellt eleven E-Mail-Sicherheit der nächsten Generation vor. eleven hat eXpurgate 3.0 völlig neu entwickelt, um Unternehmen auch in Zukunft zuverlässig vor allen Gefahren der E-Mail-Kommunikation zu schützen.

eXpurgate 3.0 stellt die geschäftsrelevante E-Mail-Kommunikation zu jedem Zeitpunkt sicher. eXpurgate 3.0 bietet optimale integrierte E-Mail-Sicherheit, entlastet Ihre E-Mail-Infrastruktur und spart Kosten: keine zusätzliche Hardware, kein Wartungsaufwand!

eXpurgate 3.0 auf einen Blick

- **Höchste Spam-Erkennungsrate > 99 %**
- **Niedrigste False-Positive-Rate: Zero False Positives bei geschäftsrelevanten E-Mails**
- **Sicherstellung geschäftsrelevanter E-Mail-Kommunikation zu jedem Zeitpunkt**
- **Erhebliche Entlastung der E-Mail-Infrastruktur**
- **Integrierte E-Mail-Sicherheit für Unternehmen jeder Größe**
- **Kein Wartungsaufwand nach der Installation nötig**

eXpurgate 3.0 – Was ist neu?

1. Performance-Steigerung um über 1.000 Prozent

Mit eXpurgate 3.0 bietet eleven die mit Abstand leistungsstärkste E-Mail-Sicherheitslösung auf dem Markt. Mit einem durchschnittlichen E-Mail-Durchsatz von über 1.000 E-Mails pro Sekunde bewältigt eXpurgate 3.0 auch riesige Spam-Wellen mühelos, ohne dass zusätzliche Hardware nötig ist. Damit ist eXpurgate 3.0 auch für ISPs mit bis zu mehreren Millionen E-Mail-Accounts optimal geeignet.

2. eXpurgate 3.0 ist integrierte E-Mail-Sicherheit

Mit der Version 3.0 wird aus einem Spam-Filter und E-Mail-Kategorisierungsdienst eine integrierte Sicherheitslösung für Unternehmen. eXpurgate 3.0 schützt nicht nur vor Spam, Viren und andere Malware, sondern stellt die geschäftliche E-Mail-Kommunikation von Unternehmen zu jedem Zeitpunkt sicher. eXpurgate 3.0 ist der Komplettschutz für die E-Mail-Kommunikation.

3. Mit eXpurgate 3.0 fit für die Zukunft

Die Bedrohungen der E-Mail-Infrastruktur von Unternehmen wachsen von Jahr zu Jahr – und mit ihnen die Anforderungen an die E-Mail-Sicherheit. eXpurgate 3.0 ist optimal auf zukünftige Gefahren und Anforderungen vorbereitet und kann jederzeit um neue Funktionen erweitert werden.

Weitere neue Features

- Erhöhte Ressourcenschonung durch deutlich reduzierten Speicherbedarf
- Unterstützung von BATV zum Schutz vor Spam-Rückläufern (Backscatter)
- Unterstützung des aktuellsten AV-Engines von Avira AntiVir

E-Mail-Sicherheit Made in Germany

eXpurgate als Managed Service

Mit eXpurgate.ASP bietet eleven integrierte E-Mail-Sicherheit für Unternehmen, die zuverlässig vor Spam und anderer Malware schützt und die geschäftliche E-Mail-Kommunikation in jeder Situation sicherstellt. Als Managed Service entlastet eXpurgate die E-Mail-Infrastruktur von Unternehmen, schont Ressourcen und erfordert dauerhaft keine zusätzliche Hardware.

Funktionsweise

eXpurgate.ASP arbeitet für den Kunden als vorgeschalteter E-Mail-Server. Alle eingehenden E-Mails werden zunächst auf eleven-Server geleitet und dort geprüft. Die Zustellung „sauberer" E-Mails erfolgt verzögerungsfrei. Für die Einrichtung von eXpurgate.ASP ist lediglich die Änderung des MX Record im DNS-Eintrag erforderlich.

Was ist neu?

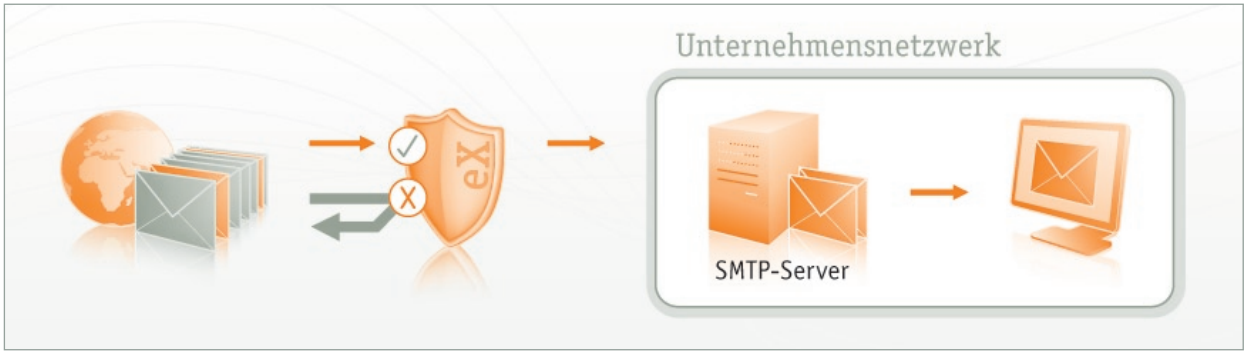
- Verbesserte und nutzerfreundlichere Konfiguration per Web-Interface
- Detailliertere und nutzerfreundlichere Reporting- und Berichtsfunktionen
- Domain-Routing (bei mehreren Domains Zustellung an unterschiedliche Empfänger möglich)

Vorteile von eXpurgate als Managed Service

- Zuverlässiger Schutz vor Spam: Spam-Erkennungsrate > 99%
- False-Positive-Rate < 0,00001% (< 1 : 10 Millionen)
- Keine Systembelastung durch hohes Spam-Volumen
- Keine Gefährdung der IT-Infrastruktur, da Gefahren schon vor Eintritt in das Netzwerk abgewehrt werden können
- Kein Wartungsaufwand
- Keine zusätzliche Hardware nötig
- Individuelle und bequeme Konfiguration per Web-Interface bis auf Nutzerebene

Spam einfach abprallen lassen: Der eXpurgate Reject-Modus

Der Reject-Modus ermöglicht es Unternehmen, Spam-E-Mails zu identifizieren und zurückzuweisen, bevor sie in das Unternehmensnetzwerk eindringen. Dabei geschieht die Prüfung bereits während des bestehenden SMTP-Dialogs, der den E-Mail-Verkehr zwischen den E-Mail-Servern regelt. Wird eine E-Mail als Spam klassifiziert, so wird über eine permanente SMTP-Fehlermeldung der Einlieferungsversuch negativ quittiert. Da eXpurgate verfahrensbedingt Fehlsortierungen individueller E-Mails ausschließt, ist sichergestellt, dass keine geschäftsrelevanten E-Mails abgewiesen werden.



eXpurgate Virenschutz

Als Teil seines integrierten E-Mail-Sicherheitspakets bietet eXpurgate.ASP zusätzlich zum zuverlässigen Spam-Schutz eine umfassende Anti-Virus-Lösung, die aus drei Komponenten besteht, deren Kombination die optimale Identifizierung bekannter und neuer Viren ermöglicht:

- **eXpurgate Virus-Outbreak-Detection (Virenfrüherkennung)**
- **codebasierter Virenschutz**
- **signaturbasierte Anti-Virus-Software AntiVir**

eXpurgate Virus-Outbreak-Detection

Die eXpurgate Virus-Outbreak-Detection ist eine einzigartige Virenfrüherkennung, die neuartige Virenwellen bereits unmittelbar nach ihrem ersten Auftreten und damit in der Regel mehrere Stunden vor signaturbasierten Virenscannern identifiziert. Damit schließt eleven die Sicherheitslücke herkömmlicher Anti-Virus-Lösungen und bildet eine wesentliche Ergänzung der Virenschutzmaßnahmen von Unternehmen.

Weitere Optionen von eXpurgate.ASP

Outbound-Schutz mit Mail-Relay-Funktion

Die Mail-Relay-Funktion ergänzt das integrierte E-Mail-Sicherheitsangebot von eleven um den Schutz des ausgehenden E-Mail-Verkehrs. Die Mail-Relay-Funktion stellt sicher, dass Unternehmen nicht als Spam- und Malware-Versender missbraucht werden. Dabei wird der gesamte ausgehende E-Mail-Verkehr über die Server von eleven geleitet und dort auf Spam, Viren und unerwünschte Dateianhänge überprüft.

eXpurgate Quarantäne

Die Quarantäne-Funktion von eXpurgate ermöglicht es, als Spam kategorisierte Nachrichten bei eleven zwischenzuspeichern. Jeder Anwender bekommt nach einem individuell einstellbaren Zeitraum eine Liste der so vorgehaltenen E-Mails und kann nun mit einem Mausklick entscheiden, welche dieser E-Mails dennoch zugestellt werden sollen.

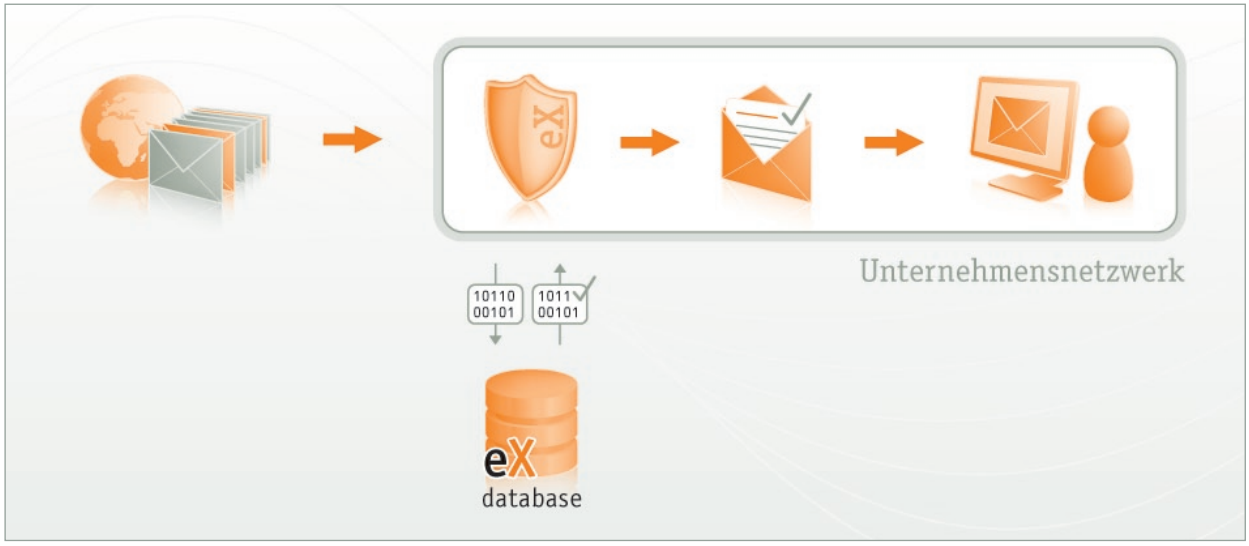
Gesicherte Kommunikation mit TLS

Die TLS-Option bietet insbesondere Anwendern aus sicherheitsrelevanten Branchen wie dem Finanz- oder Gesundheitssektor die Verschlüsselung des gesamten Kommunikationsweges mittels Transport Layer Security (TLS) und damit eine gesicherte Datenübertragung mit ausgewählten Kommunikationspartnern. Darüber hinaus ermöglicht die TLS-Option ein vollständiges Zertifikatsmanagement durch das die Authentizität der Kommunikationspartner und die Echtheit der E-Mail sichergestellt werden kann.

E-Mail-Sicherheit Made in Germany

eXpurgate als Inhouse-Lösung

Unternehmen, die ihre E-Mail-Services eigenständig betreiben wollen, bietet eleven integrierte E-Mail-Sicherheit als Inhouse-Variante. eXpurgate.Inhouse stellt die geschäftsrelevante E-Mail-Kommunikation in jeder Situation sicher und schützt zuverlässig vor Spam, Viren und anderer Malware. eXpurgate.Inhouse ist extrem ressourcenschonend und erfordert keinerlei Wartungsaufwand. Die Lösung kombiniert höchste E-Mail-Sicherheit mit minimaler Systembelastung.



Funktionsweise

eXpurgate.Inhouse wird als Plug-In in die existierende E-Mail-Server-Software des Kunden integriert. Dazu bietet eXpurgate.Inhouse zahlreiche Schnittstellen, unter anderem für SpamAssassin und Sendmail Milter. Die Inhouse-Lösung ist für alle gängigen Plattformen geeignet, darunter Windows, alle gebräuchlichen Linux-Distributionen und Solaris 9+. Mit der Version 3.0 unterstützt eXpurgate auch sämtliche 64-Bit-Systeme.

Die Prüfung und Kategorisierung der eingehenden E-Mails wird bei eleven durchgeführt, aber auf dem Server des Kunden bearbeitet. So werden lediglich kurze Kontrollsummen über eine verschlüsselte Vebindung (SSL) in der zentralen eXpurgate Datenbank überprüft. Hier wird der Bulkcheck durchgeführt, der im Zentrum des eXpurgate Prüfverfahrens steht. Aufgrund des Prüfverfahrens geschieht die Zustellung in der Regel ohne merkliche Verzögerung.

Vorteile von eXpurgate.Inhouse

- Zuverlässiger Schutz vor Spam: Spam-Erkennungsrate > 99%
- False-Positive-Rate < 0,00001% (< 1 : 10 Millionen)
- Minimale Systembelastung
- Kein Wartungsaufwand
- Einfach in die bestehende E-Mail-Infrastruktur integrierbar
- Keine zusätzliche Hardware nötig

Was ist neu?

- Unterstützung aller 64-Bit-Systeme
- Kompatibel mit allen gängigen Linux-Distributionen
- Flexible und einfache Konfiguration bis auf Nutzerebene

E-Mail-Firewall enSurance

Die E-Mail-Firewall enSurance komplettiert das E-Mail-Sicherheitsangebot von eleven und sichert die E-Mail-Kommunikation in Zeiten extremer Belastung, zum Beispiel bei Denial-of-Service-Attacken oder Spam-Wellen. enSurance verhindert die Überlastung der E-Mail-Infrastruktur und stellt die geschäftsrelevante E-Mail-Kommunikation in jeder Situation sicher. Gemeinsam mit dem Spam-Schutz und der Anti-Virus-Lösung von eXpurgate bietet enSurance Unternehmen jeder Größe umfassende integrierte E-Mail-Sicherheit.

Funktionsweise

enSurance nutzt ein eigenes, vollständig dynamisches Verfahren, das mit Hilfe einer Frequent-Partner-Liste die vorwiegenden und relevanten Kommunikationspartner ermittelt. In Zeiten besonders hoher Belastung werden diese bevorzugt behandelt, während eher nachrangige E-Mails temporär abgewiesen werden und ihre Zustellung auf einen späteren Zeitpunkt verschoben wird. Wichtige E-Mails werden dadurch weiterhin ohne Zeitverzögerung zugestellt. enSurance ist vollständig skalierbar und arbeitet plattformübergreifend. Eine enSurance Plattform unterstützt und schützt hierbei bis zu 20 parallele eXpurgate Installationen (E-Mail-Server) gleichzeitig.

Normalsituation

enSurance Mailbomb Protection

enSurance schützt zuverlässig vor Mailbomb-Attacken. Mailbombings sind die bekannteste Form von Denial-of-Service-Attacken. Dabei wird eine große Anzahl E-Mails an eine bestimmte Person oder von einem einzelnen Absender an ein E-Mail-System versandt, um einzelne E-Mail-Accounts oder ganze E-Mail-Server gezielt zu überlasten. Die enSurance Mailbomb Protection schützt zuverlässig und individuell vor Mailbombings, indem sie dem Kunden ermöglicht, die Anzahl der E-Mails, die für einen bestimmten Empfänger oder von einem bestimmten Absender pro Zeitintervall angenommen werden, individuell zu konfigurieren.

Lastsituation

enSurance Mailloop Protection

enSurance schützt Unternehmen sicher vor so genannten Mailloops, die entstehen, wenn beispielsweise Mitarbeiter automatische Weiterleitungen ihrer privaten E-Mails auf den Firmen-Account oder umgekehrt einrichten. Kommt es hierbei nun beispielsweise zu vollen Postfächern in Kombination mit Abwesenheitsnotizen, kann das E-Mail-Aufkommen innerhalb kürzester Zeit regelrecht explodieren. Die enSurance Mailloop Protection erkennt solche Schleifen und ermöglicht es, den E-Mail-Verkehr zwischen einem Sender und einem Mitarbeiter-Account zu reglementieren und damit den Mailloop auszubremsen.

mit eXpurgate 3.0

E-Mail-Sicherheit Made in Germany

eXpurgate in der Praxis

Zahlen und Fakten

Spam-Erkennungsrate:	False-Positive-Rate:	Durchsatz geprüfter E-Mails	Wartungsaufwand:
über	unter	über	genau
99	**0,00001**	**1000**	**0,0**
Prozent	Prozent	E-Mails/Sek.	Std./Woche

Technische Spezifikationen

Lösung:	eXpurgate.ASP	eXpurgate.Inhouse
Unterstützte Betriebssysteme	unabhängig	**Windows** (ab NT), **Linux:** direkte Unterstützung von Debian 3, 4, Fedora 8, 9, Redhat Enterprise Linux 2 und höher, generisch (glibc2.2+), **Solaris** 9+
Unterstützte Protokolle	SMTP	SMTP, SpamAssassin, Sendmail Milter
Hardware-Anforderungen (Minimum)	entfällt	**Windows** i368 (32bit) **Linux** i386 (32bit) oder **amd**64/x86-64 (64bit), **Solaris** i386 (32bit) oder **sparc** (32bit und 64bit)
SMTP-Server erforderlich	ja	ja, inhouse beim Kunden

Kostenloser Test

Testen Sie eXpurgate als Managed Service

30 Tage lang - kostenlos!

Bequem auf www.eleven.de

oder kontaktieren Sie unser Vertriebsteam:

E-Mail vertrieb@eleven.de

eleven – Gesellschaft zur Entwicklung und Vermarktung von Netzwerktechnologien mbH
Hardenbergplatz 2 | 10623 Berlin
fon: +49 30/56 00 52 - 0 | fax: +49 30/56 00 52 - 299
e-mail: info@eleven.de | web: www.eleven.de

Stand: September 2008