spamchek
Let your spam stop here.

Schluss und aus
mit Spam und Viren.
Ein für alle Mal. 

Sex^{12} E-Mails.

Kein Mensch weiss wirklich, wie viele E-Mails eigentlich verschickt werden. Realistische Schätzungen kommen weltweit pro Jahr auf ± 6 Billiarden E-Mails (ausgeschrieben 6'000'000'000'000 oder eben 6^{12}; 1 Billiarde = 1000 Milliarden oder 1'000'000 Millionen!). Und kein Mensch weiss, wie gross der Anteil von Spam an diesen 6 Billiarden E-Mails ist. Optimisten schätzen 50 %, Pessimisten bis zu 80 %. Ob 3 oder 4,8 Billiarden Spam-Mails pro Jahr ist unerheblich – die Menge ist unvorstellbar gross. Und kommt uns alle sehr teuer zu stehen: Gemäss UN-Konferenz für Handel und Entwicklung verursacht Spam weltweit jährlich Kosten von über 17 Milliarden Franken. In der Schweiz sind es über 300 Millionen. Tendenz steigend.

Ist das bisschen Spam wirklich so schlimm?

Spam und Eisberge. Man kann es so sehen: Es ist zwar lästig, jeden Tag unzählige Spam-Mails zu löschen. Aber wirklich schlimm ist das doch nicht, oder?

So gesehen, ist Spam nicht wirklich schlimm. So gesehen, sieht man aber auch nur die Spitze des Eisbergs. Das Problem bei Spam ist jedoch der Teil, den man nicht sieht: *Spam ist nicht nur ärgerlich. Sondern auch teuer. Und gefährlich. Sehr gefährlich sogar.*

Denn Spam transportiert nicht nur lästige Werbebotschaften. Sondern auch Viren, Würmer, Trojaner, Spione und vieles mehr. Mit etwas Glück kostet es nur Zeit und Nerven, einen virenverseuchten PC zu desinfizieren. Mit etwas weniger Glück löscht das Virus sämtliche Festplatten Ihrer PCs und Server.

Die Lösung heisst Spamchek. In dieser Broschüre sprechen wir über die Gefahren des unsichtbaren Teils des Eisbergs. Und wir zeigen Ihnen, wie Spamchek das Problem löst: Ihre E-Mails landen statt auf Ihrem Mailserver bei Spamchek.  *Unsere Filter eliminieren 98,6 % des Spams und 99,99 % aller Viren.* Nur die sauberen E-Mails leiten wir an Sie weiter. So gelangen Spam und Viren gar nicht erst auf Ihren Mailserver, geschweige denn auf Ihren PC.

Ein für alle Mal sind Sie mit Spamchek Spam und Viren los. Ohne Investition, Installation oder Konfiguration. Die einzige Umstellung: Sie müssen sich höchstens daran gewöhnen, viel weniger E-Mails zu erhalten …

Günstiges Viagra ist viel teurer als Sie denken.

Alles neu und wie gehabt. Es wäre uns lieber, wenn wir Spamchek nicht hätten erfinden müssen. Denn E-Mail ist eine wunderbare Erfindung und hat innert weniger Jahre unseren Alltag komplett verändert. Bis auf eines: Nach wie vor verstopft Werbung unsere Briefkästen; früher wurde sie auf Papier gedruckt, heute besteht sie aus digitalen Nullen und Einsen, die per E-Mail verschickt werden.

Top 10 der Spam-Nationen

1. USA
2. Südkorea
3. China (mit Hongkong)
4. Frankreich
5. Spanien
6. Kanada
7. Japan
8. Brasilien
9. Grossbritannien
10. Deutschland

(Quelle: Spamchek, 2004)

Spam ist gratis, aber nicht kostenlos. Der grösste Vorteil von E-Mail ist auch der grösste Nachteil: Die elektronische Post ist gratis. Deshalb wird Spam auch nicht einzeln verschickt. Sondern in Millionenauflagen. Genau das macht die nervige Werbung für günstige Potenzmittel denn auch so horrend teuer: Wegen der Milliarden von Spammails erreichen Netze, Server und Speicher immer schneller ihre Kapazitätsgrenzen. Laufend muss die IT-Infrastruktur ausgebaut und aufgerüstet werden, damit das Internet nicht zusammenbricht. Das kostet enorme Summen. Die Rechnung bezahlen direkt und indirekt alle Empfänger von Spam. Also auch Sie.

Spam killt Ihre Rendite. Vielleicht merken Sie es nicht. Doch Spam und Viren kosten Ihr Unternehmen viel Geld:

- *Erstens sinkt Ihre Produktivität.* Ihre Mitarbeiter brauchen zwar nur wenige Minuten pro Tag, um Spam zu löschen. Doch Minuten addieren sich zu Stunden und Stunden zu Tagen. Das geht ins Geld.
- *Zweitens verlieren Sie Umsatz.* Erfahrungsgemäss wird nicht nur Spam gelöscht, sondern aus Versehen auch saubere Mails – zum Beispiel Bestellungen oder Offertanfragen.
- *Drittens kostet Ihre IT immer mehr.* Immer häufiger müssen Sicherheitssysteme aktualisiert oder ergänzt werden, um das immer grössere E-Mail-Volumen (das zu 50–80 % aus Spam besteht) zu verarbeiten. Das bedeutet entweder teure Überstunden. Oder teures zusätzliches Personal.
- *Viertens legen Viren Ihren Betrieb lahm.* Trotz aller Vorsicht fängt auch in Ihrem Unternehmen ab und zu ein PC einen Virus ein – und infiziert im Nu weitere PCs und Server. Für die Reparatur müssen Sie die Systeme herunterfahren – und schon steht Ihr Unternehmen still.
- *Fünftens werden Sie zu unnötigen Investitionen gezwungen.* Das immer grössere E-Mail-Volumen erfordert grosse Investitionen in leistungsfähigere Hard- und Software. Die wären aber nicht nötig, da 50–80 % aller Mails Spam sind.

Sechstens, siebtens … – Spam verursacht Ihrem Unternehmen noch ganz andere Kosten. Aber wir wollen Ihnen hier nicht die Laune verderben.

Schlimmer als Nitro und Glyzerin:  Spammer und Hacker.

Der Spass wird ernst: Früher waren Hacker Teenager, die der Welt beweisen wollten, dass sie cleverer sind als die Erwachsenen. Ihre «Spässe» verursachten wenig Schaden und viel Schadenfreude. Das Grinsen dürfte den meisten spätestens im Frühjahr 2004 vergangen sein. Damals legte ein 17-jähriger Deutscher mit dem Wurm «Sasser» das Internet praktisch im Alleingang lahm. Obwohl er keine Daten vernichtete, sondern «nur» Hunderte Millionen von PCs nonstop abstürzen und neustarten liess, verursachte «Sasser» Schäden in Millionenhöhe. Fazit:  Die Hacker von heute sind keine übereifrigen Teenager mehr. Sondern Psychopathen. Oder Kriminelle. Oder beides.

Eine gefährliche Allianz. Spammer wollen mit Ihnen ins Geschäft kommen, Hacker in Ihren Computer. Bislang hatten Spammer und Hacker nur wenig füreinander übrig. Doch jetzt arbeiten sie Hand in Hand. Das ist sehr beunruhigend. Denn erstens sind Hacker nicht die schlechtesten Programmierer. Zweitens kann man mit Spam immer noch sehr reich werden (der im April 2005 zu neun Jahren Gefängnis verurteilte Jeremy Jaynes brachte es immerhin auf einen monatlichen Nettogewinn von rund 700'000 Dollar).
Im Auftrag der Spammer programmieren die Hacker Trojanische Pferde, die aus PCs «Zombies» machen. Es ist übrigens gut möglich, dass auch Ihr PC schon längst ein «Zombie» ist. Davon würden Sie nämlich nichts merken. Bis der Spammer ferngesteuert die Kontrolle über Ihren PC übernimmt.

Phishing for your money. «Phishing» ist die Abkürzung von Password Fishing und der neuste Trend der Internet-Kriminalität. Das Vorgehen ist einfach.  Zum Beispiel: Sie erhalten eine E-Mail von Ihrer Bank mit der Aufforderung, einen Link anzuklicken, um wichtige Informationen zu ergänzen. Der Link in der E-Mail führt auf eine täuschend echte, falsche Phishing-Website, wo Passwort, Kontonummern usw. abgefragt werden. Neuerdings muss nicht einmal mehr ein Link im E-Mail angeklickt werden – wenn Sie die E-Mail öffnen, installiert sich unbemerkt ein Skript. Wenn Sie das nächste Mal die URL Ihrer Bank eingeben, sorgt dieses Skript dafür, dass Sie auf einer Phishing-Site landen. So gelangen Passwort und Kontoinformationen in die falschen Hände. Besonders tückisch an diesem Vorgehen: Eine E-Mail von Ihrer Bank öffnen Sie, weil Sie ihr vertrauen – und schon ist das Unheil geschehen. Solche Phishing-Mails erkennt und stoppt Spamchek. Und sorgt so dafür, dass Sie Ihrer Bank weiterhin vertrauen können.

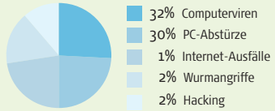
Wollen Sie mehr wissen? Öffnen Sie die Aufklappseite, und Sie erfahren ein paar ganz realistische Horrorszenarien – und was Sie dagegen unternehmen können.

Zahnlose Papiertiger:
Im Januar 2004 traten in den USA strenge Anti-Spam-Vorschriften in Kraft («CAN-Spam-Gesetz»). Seither ist das Spam-Volumen in den USA um weitere 10 % angestiegen.

Ein Wurm kann Sie Ihren guten Ruf kosten. Oder Ihre Firma.

Von Würmern, Viren und Trojanischen Pferden. Hacker sind enorm kreativ. Für jedes geschlossene Schlupfloch finden sie zwei neue Wege in fremde Computer. Und was sie dort anrichten, beweist leider ebenfalls viel Talent – das Spektrum reicht von hämischen, aber harmlosen Grüssen an den Benutzer bis zur komplett gelöschten Festplatte. Tägliche Backups halten den Schaden eines solchen Daten-GAUs in Grenzen. Scheinbar harmlosere Hackereien können indes wesentlich schlimmere Folgen haben.

Die häufigsten Ursachen für Störungen im Geschäftsalltag von KMU:



Über 30 % der KMU konnte mindestens einmal wegen Viren das Geschäft nicht wie üblich betreiben.
(Quelle: Computerworld)

«Zombies» in drei Phasen. Von «Zombies» war schon kurz die Rede. Sie verdienen aber, etwas ausführlicher behandelt zu werden. Erstens, weil sie durch Spam verbreitet werden. Und zweitens, weil sie wiederum Spam verbreiten.

Phase 1: Mit dem Absender einer bekannten, vertrauenswürdigen  Firma (zum Beispiel Symantec, Hersteller des «Norton Anti Virus») versenden Spammer eine E-Mail mit Anhang (zum Beispiel die aktuellen Virendefinitionen). Tatsächlich aber installiert sich beim Öffnen des Anhangs unbemerkt ein Programm, ein so genanntes Trojanisches Pferd. Dieses macht den Computer zum Zombie, auch «Bot» (wie Roboter) genannt. Der Benutzer des PCs merkt davon nichts.

Phase 2: Nach einer Wartezeit von mehreren Tagen bis mehreren Monaten verschickt der Spammer noch einmal eine E-Mail mit vertrauenswürdigem Absender. Der Text dieser Mail enthält ein Codewort, welches das Trojaner-Programm aktiviert und dem Spammer ein Hintertürchen im Computer öffnet. Dieses Schlupfloch nutzt der Spammer, um über den Zombie-PC Spam zu verschicken – wobei der Besitzer des PCs gar nicht realisiert, dass in seinem Namen gespammt wird. Für den guten Ruf kann das sehr schlecht sein – zum Beispiel wenn eine renommierte Bank dubiose Aktien empfiehlt …

Phase 3: Der vom Zombie-PC aus verschickte Spam hat meist einen Trojaner im Anhang … So entstehen Zombie-Netze mit bis zu 50'000 PCs, über die mittlerweile über 80 % aller Spam-Mails verschickt werden.

In Ihrem PC sitzt ein Spion. Mehr als nur rufschädigend ist Spyware. Diese heimtückischen Programme gelangen per E-Mail in Ihren Computer.  Dort nisten sie sich ein und sammeln sensible Daten (Passwörter, PINs, Kreditkartennummern, E-Banking-Codes und vieles mehr, das Sie geheim halten wollen) auf Ihrer Festplatte. Oder sie registrieren jeden einzelnen Tastendruck. Die gesammelten Angaben übermittelt die Spyware dem Hacker. Der kann damit Ihre Bankkonten plündern, auf Ihre Rechnung einkaufen oder Sie mit besonders delikaten Informationen erpressen: Entweder Sie zahlen. Oder er veröffentlicht.

Ignorieren, investieren oder delegieren? Sie haben die Wahl.

Was tun? Zumindest haben Sie jetzt eine Ahnung, wie gefährlich die restlichen 90 % des Eisbergs sind. Wahrscheinlich  stimmen Sie uns zu, dass Spam nicht nur lästig ist. Sondern auch sehr teuer. Und eine echte Bedrohung. Nun stellt sich natürlich die Frage, wie Sie mit dem Problem umgehen. Und was Sie gegen Spam unternehmen.  Zur Wahl stehen drei Szenarien:

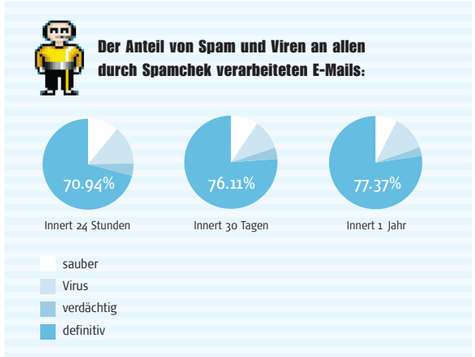
1. Sie ignorieren das Problem. Sie finden den Müll in Ihrer Mailbox primär lästig. Sie glauben der Aussage Ihres Internet-Providers, seine Virenfilter seien leistungsfähig und vor allem aktuell. Sie konfigurieren den Spamfilter Ihres E-Mail-Programms so, dass er nur Mails durchlässt, wenn der Absender in Ihrem Adressbuch steht. (Leider landen dann auch alle Anfragen von neuen Kunden im Papierkorb.) Durch Ignorieren lösen Sie das Problem zwar nicht. Aber wenigstens bereiten Ihnen Spam und Viren keine schlaflosen Nächte.

2. Sie investieren in die Lösung. Sie investieren in eine gründliche Analyse der Bedrohung. Sie investieren in qualifizierte IT-Fachleute. Sie investieren in Firewalls, Virenprogramme und andere Sicherheitsmassnahmen. Nie haben Sie  eine Ruhepause oder genügend investiert. Denn jede neue Gefahr erfordert neue Investitionen. Einen Return on Investment gibt es nicht, denn Sie investieren in einen zwar notwendigen, aber auch unproduktiven Bereich. Das frustriert Sie sehr. Aber wenigstens fühlen Sie sich einigermassen sicher vor Spam und Viren.

3. Sie delegieren Problem und Lösung. Sie realisieren, dass die Bekämpfung von Spam und Viren nicht zu Ihren Kernkompetenzen gehört. Sie investieren lieber dort, wo Sie eine Rendite erwarten können. Also in effizientere Produktionsmittel oder in die Entwicklung neuer Produkte. Sie suchen einen Anbieter, dessen Kernkompetenz das Bekämpfen von Spam und Viren ist. Sie stossen auf Spamchek. Sie testen Spamchek während 30 Tagen kostenlos und unverbindlich. Nach wenigen Tagen sind Sie überzeugt und entscheiden sich für ein Spamchek-Jahresabonnement. Ab sofort sind Spam und Viren für Sie kein Thema mehr, keine Gefahr und auch kein Grund für schlaflose Nächte.

Wir haben etwas gegen Spam und Viren.

Mit Spamchek sind Spam und Viren kein Thema mehr. Punkt. Knapper lassen sich die Vorteile von Spamchek nicht formulieren. Etwas ausführlicher dagegen schon:



1. Sie haben keinen Spam mehr in Ihrer Mailbox.
2. Sie spüren nichts von Virenattacken.
3. Sie ersparen sich kostspielige Investitionen, denn Sie müssen weder die Technologie entwickeln, noch qualifizierte Spezialisten für diese Aufgabe finden und einstellen, noch laufend Ihre Spam- und Virenfilter aktualisieren, noch in teure Systeme und deren Unterhalt investieren.
4. Sie setzen Kapazität frei in Ihren bestehenden IT-Systemen, weil das E-Mail-Volumen massiv zurückgeht.
5. Sie können Ihre IT-Spezialisten für produktive Aufgaben einsetzen anstatt für das Desinfizieren virenverseuchter Computer.
6. Sie erhalten bei Spamchek im Vergleich mit einer internen Lösung für viel weniger Geld ein viel besseres Produkt.

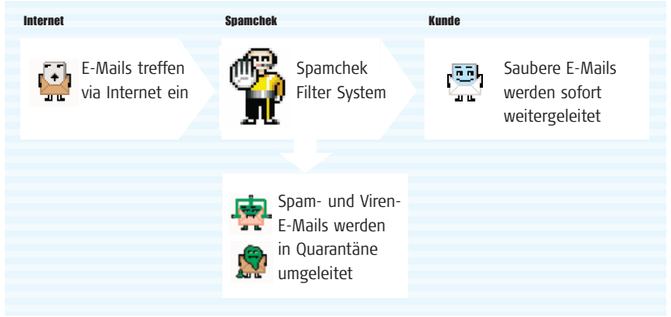
Einen geschäftskritischen Bereich auslagern? Eine berechtigte Frage, denn schliesslich wird Ihre E-Mail ja in unseren Servern verarbeitet. Und E-Mail ist mittlerweile für die meisten Unternehmen geschäftskritisch. Die Antwort liegt auf der Hand: *Wir können uns einen Ausfall noch viel weniger leisten als Sie.* Denn für Spamchek ist die Spam- und Virenfilterung der einzige geschäftskritische Bereich, und nicht einer von vielen. Deshalb arbeiten wir mit leistungsfähigen, zuverlässigen Systemen, die auch extrem grosse Mengen von E-Mails in Echtzeit verarbeiten können. Alle Systeme sind mehrfach redundant, Hauptsystem und Fallback-System sind räumlich getrennt. Selbst wenn mehrere Systeme ausfallen sollten (ein überaus unwahrscheinliches Szenario!), läuft der Betrieb ohne Unterbruch weiter.

Spamchek auf einen Blick

- Eliminiert 98,6 % aller Spam-E-Mail
- Stoppt 99,9 % aller Viren-E-Mail
- E-Mail-Verarbeitung in Echtzeit
- Tagesaktuelle Spam- und Virenfilter
- Funktioniert mit allen Betriebssystemen und E-Mail-Programmen
- Weder Kauf, Miete oder Investition
- Keine zusätzliche Soft- oder Hardware
- Spätestens 1 Arbeitstag nach Anmeldung implementiert
- Kein Betriebsunterbruch, keine Installation
- Detaillierte Statistiken und Statusberichte
- Extrem flexible Verwaltung von Spam- und Viren-E-Mail
- Intuitive Benutzeroberfläche in mehreren Sprachen

Spam und Viren bleiben auf der Umleitung auf der Strecke.

Wenn doch nur alles so einfach wäre … Es braucht keine Hard- oder Software und auch keine zusätzliche Installation, um alle E-Mails Ihres Unternehmens zu Spamchek umzuleiten, bevor sie auf Ihrem Mailserver landen. Geändert werden muss einzig die DNS-MX-Datei auf Ihrem Mailserver – eine Sache von Minuten.



Wir filtern Ihre E-Mail in Echtzeit auf Spam und Viren und stufen sie in vier Klassen ein:

1. Zweifelsfrei sauber
2. Möglicherweise Spam
3. Definitiv Spam
4. Virus

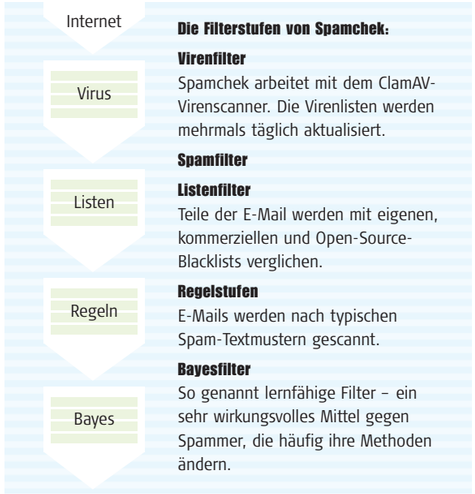
Zweifelsfrei saubere E-Mail geht sofort an Sie weiter. Die drei anderen Kategorien landen in separaten Quarantänebereichen auf unseren Servern. Ihr Systemadministrator hat Zugang zu allen drei Quarantänebereichen; die Benutzer können an sie adressierte E-Mails freigeben, die irrtümlich als «möglicherweise Spam» zurückbehalten wurden.

Lieber zwei Spam-Mails zuviel als eine saubere E-Mail zu wenig. Wahrscheinlich ist auch für Ihr Unternehmen eine reibungslos funktionierende E-Mail-Kommunikation überlebenswichtig. Sie müssen sicher sein, dass jede an Sie adressierte E-Mail auch bei Ihnen ankommt. Aber auch wirklich jede. Darauf können Sie sich bei

Spamchek verlassen. In Ihrem Interesse sind unsere Filter so eingestellt, dass lieber zwei harmlose (da sicher virenfreie) Spam-Mails weitergeleitet werden, als dass wir eine saubere, für Sie wichtige Mail zurückbehalten. Unsere Quarantäneverwaltung ist so aufgebaut, dass mögliche Spam-Mails bis zu vier Wochen und definitive Spam-Mails bis zu vier Tage lang gespeichert werden. Und deshalb informieren wir Sie auch schnell und übersichtlich, welche E-Mails wir als Spam eingestuft und unter Quarantäne gestellt haben.

Mehr über die drei Komponenten von Spamchek – *Filter*, *Verwaltung*, *Information* – erfahren Sie, wenn Sie die Ausklappseiten öffnen.

Unsere Filter kennen sich aus mit Viren, Viagra & Co.



Die Filterstufen von Spamchek:

Virenfilter
Spamchek arbeitet mit dem ClamAV-Virenscanner. Die Virenlisten werden mehrmals täglich aktualisiert.

Spamfilter

Listenfilter
Teile der E-Mail werden mit eigenen, kommerziellen und Open-Source-Blacklists verglichen.

Regelstufen
E-Mails werden nach typischen Spam-Textmustern gescannt.

Bayesfilter
So genannt lernfähige Filter – ein sehr wirkungsvolles Mittel gegen Spammer, die häufig ihre Methoden ändern.

1. Filter: Räuber und Polizist. Filter für Spam und Viren haben eine ähnlich undankbare und unlösbare Aufgabe wie die Polizei: Sie sollen Übeltäter unschädlich machen, bevor diese überhaupt übel tun konnten. Und das natürlich ohne falsche Verdächtigungen oder irrtümliche Verhaftungen. Doch zum Glück ist die Erfolgsquote unserer Filter höher als die der Polizei:

Spamchek stoppt rund 99,9 % aller Viren und 98,6 % der Spam-Mails. Falls Sie sich wundern, dass es nur 98,6 % sind: Wir könnten noch mehr Spam abfangen – mit dem Risiko, saubere Mails irrtümlich zurückzuhalten (hier liegt unsere Quote bei 0,2 %). Das wollen wir nicht. Und Sie wahrscheinlich auch nicht.

11fach genäht hält besser. Sobald eine an Sie adressierte E-Mail bei uns eintrifft, analysieren wir sie auf Herz und Nieren, respektive auf Spam und Viren. Dabei verlassen wir uns nicht auf einen einzelnen Filter. Sondern teilen die Arbeit auf mehrere und verschieden konzipierte Filter auf (zur Zeit sind es 11), die wie eine Pipeline hintereinander angeordnet sind. Jeder Filter hat eine andere Funktion und prüft nach genau definierten Kriterien jeweils nur einen Bestandteil der E-Mail. Also zum Beispiel die Kopfzeilen, den Absender, das Datum oder den Inhalt auf Spam. Oder die Anhänge auf Viren. Oder … Wir sind stolz auf unsere Filterpipeline. Erstens, weil sie sehr zuverlässig und effizient arbeitet. Und zweitens, weil wir auf neue Spam-Methoden oder Viren sehr schnell reagieren und die Pipeline um zusätzliche Filter erweitern können.

Ja. Nein. Vielleicht. Nicht nur die Aufgaben der Filter, auch die Resultate sind unterschiedlich: Das Resultat eines Virenfilters ist entweder Ja oder Nein. Die einzelnen Spam-Filterstufen hingegen liefern eine Anzahl Punkte. Am Schluss wird zusammengezählt, und je nach Punktetotal gilt die E-Mail entweder als sauber, als mögliche Spam-Mail, definitiv als Spam oder als virenverseucht. Saubere E-Mail wird sofort weitergeleitet, der Rest landet im Quarantänebereich.

Lassen Sie unser Management für sich arbeiten.

2. Verwaltung: alles im Griff. Sie wollen nicht nur wirkungsvolle Filter, sondern auch die volle Kontrolle über Ihre E-Mails? Das haben wir uns gedacht. Und deshalb den *Spamchek Account Manager* entwickelt, kurz und liebevoll SAM genannt. Mit SAM erledigen Sie alle Verwaltungs- und Kontrollaufgaben Ihrer E-Mail-Domäne; mit SAM definieren Sie verschiedene Parameter und können Spamchek so individuell Ihren Bedürfnissen anpassen.

SAM macht, was Sie wollen. Zum Beispiel können Sie mit SAM festlegen, wie lange Ihre Spam- und Viren-E-Mails im Quarantänebereich zurückbehalten werden. Oder ab welchen Schwellenwerten eine E-Mail möglicherweise respektive definitiv als Spam eingestuft und unter Quarantäne gestellt wird. Oder schwarze und weisse Listen anlegen und Ihre eigenen Filterregeln aufstellen. Oder unter Quarantäne gesetzte E-Mails anschauen und freigeben oder löschen.

Das liest sich komplizierter als es tatsächlich ist. Denn bei aller Vielseitigkeit ist SAM sehr einfach zu bedienen. Vor allem aber ist bei SAM alles freiwillig: Sie können individuelle Parameter festlegen und/oder aktiv in die Verwaltung und Verarbeitung Ihrer E-Mail eingreifen. Sie müssen aber nicht, denn häufig entsprechen unsere Standard-Einstellungen weitgehend den Bedürfnissen unserer Kunden.

Wir informieren Sie auch über unsere Fehler.

3. Information: Nicht jede Lolita ist Spam. Irren ist menschlich – und Computer sind auch nur Menschen. So kann es vorkommen, dass unser Filter eine E-Mail über Nabokovs Buch oder Stanley Kubriks Film als Schmuddel-Mail und Spam einstuft. Doch dank unseren regelmässigen Quarantäneberichten erkennt der Empfänger unseren Irrtum noch gleichentags auf einen Blick. Und mit einem Klick ist die E-Mail freigeschaltet. Worauf die saubere Lolita dort landet, wo sie hingehört: im Postfach des Benutzers.

Transparenter geht's nimmer. Information ist die dritte und letzte Komponente des Spamchek-Service. Eine sehr wichtige notabene. Denn es braucht grosses Vertrauen, einen geschäftskritischen Bereich wie die Spam- und Virenkontrolle auszulagern. Mit absolut transparenten Prozessen und Abläufen rechtfertigen wir das Vertrauen, das uns entgegengebracht wird. Deshalb zählt Spamchek nicht nur punkto Filterleistung zu den führenden Lösungen weltweit. Sondern auch punkto Informationsangebot. Dieses umfasst erstens aktuelle Statistiken und komplette Event-Logs der E-Mail-Domäne via SAM. Zweitens erhalten die Administratoren unserer Kunden täglich, wöchentlich oder monatlich komplette, übersichtliche Statusberichte. Und drittens informieren wir wie erwähnt die Benutzer mit regelmässigen Quarantäneberichten.

So viel Effizienz kostet Sie ein Lächeln.

Spamchek zahlt sich aus. 98,6 Prozent weniger Spam und 99,9 Prozent weniger Viren in der Inbox zu haben, schont Ihre Nerven. Aber auch Ihr Portemonnaie. Denn aus verschiedenen Gründen werden Sie die Kosten für das Spamchek-Abonnement innert kürzester Zeit amortisieren:

1. Weil Ihre Mitarbeiter keine Zeit mehr mit dem Identifizieren und Löschen von Spam-Mails verlieren.
2. Weil Sie viel weniger und fast nur noch spamfreie E-Mails erhalten ist das  Risiko auch kleiner, dass wichtige E-Mails in der Spamflut untergehen und aus Versehen gelöscht werden.
3. Weil sich Ihre IT-Verantwortlichen wieder um ihre eigentlichen Aufgaben kümmern können, anstatt mit Rettungsaktionen beschäftigt zu sein.
4. Weil Ihre bestehende IT-Infrastruktur plötzlich wieder viel freie Kapazität hat, da Spam und Viren gar nicht erst auf Ihren Mailserver gelangen und Ihre Netzwerke belasten.
5. Weil Sie keine teuren (und doch nie genügend aktuelle) Anti-Virenprogramme mehr brauchen.
6. Weil Sie vor Phishing-Attacken, Spyware, Viren, Trojanischen Pferden oder Würmern geschützt sind, die Ihren guten Ruf oder Ihr Unternehmen ruinieren können.
7. Weil Sie dank unserem Reporting und unseren Statistiken viel mehr Überblick und bessere Kontrolle über Ihren E-Mail-Verkehr haben.

Spamchek ist günstiger, als Sie denken. Die Preisspanne für ein Spamchek-Jahresabonnement bewegt sich zwischen CHF 300.– für eine bis fünf E-Mail-Adressen und CHF 15'000.– für E-Mail-Domänen mit 500 Benutzern. Gemeinnützigen Unternehmen, Schulen und Universitäten offerieren wir speziell attraktive Konditionen.

Spamchek kennt nur eine einzige Voraussetzung: Die DNS MX-Dateien Ihres Mail-Servers müssen Spamchek als Mail-Exchanger identifizieren. In anderen Worten: Sie brauchen eine eigene E-Mail-Domäne (zum Beispiel @ihrunternehmen.ch), um Ihre E-Mails an Spamchek umzuleiten. E-Mail-Adressen wie @yahoo.com, @hotmail.com und ähnliche können deshalb von Spamchek nicht profitieren.

Überzeugen Sie sich selbst – gratis.

Glauben Sie nicht unseren Worten, sondern Ihren Augen. Denn das beste Argument für Spamchek können Sie jeden Tag selbst erleben: eine Mailbox ohne Spam und Viren. 30 Tage lang gratis und unverbindlich. Stellen Sie uns auf die Probe!

Können Sie es sich leisten, auf Spamchek zu verzichten?

Spamchek lässt den Eisberg verschwinden. In dieser Broschüre war viel von Eisbergen die Rede. Denn Spam und Eisberge haben einiges gemeinsam: Oberflächlich betrachtet, ist Spam vor allem lästig. Doch die verborgenen 90 % bergen die eigentlichen Risiken und verursachen die grossen Kosten. Mit Spamchek müssen Sie sich keine Sorgen mehr machen – weder um die lästigen 10 % noch um die teuren, gefährlichen 90 %. Spamchek bringt den Eisberg zum Verschwinden. Denn mit Spamchek gelangen Spam und Viren gar nicht erst auf Ihren Mailserver. Daraus resultieren die zahlreichen Vorteile von Spamchek:

- stoppt 98,6 % aller Spam-E-Mails
- eliminiert garantiert 99,9 %, tatsächlich aber 99,99 % aller Viren
- für alle Betriebssysteme und E-Mail-Programme
- keine Installation; erfordert keine Soft- oder Hardware
- kein Betriebsunterbruch, keine Wartezeit (max. innert 1 Arbeitstag nach Anmeldung implementiert)
- detaillierte Statistiken und Statusberichte
- E-Mail-Verarbeitung in Echtzeit
- aktuellste Spam- und Virenfilter
- äussert flexible Verwaltung von Spam- oder Viren-E-Mail, individuell anpassbare Filter
- einfache Bedienung; Benutzeroberfläche in mehreren Sprachen
- besseres Preis-Leistungsverhältnis als vergleichbare interne Lösungen

Wir schnüffeln in Ihrer Post herum.
Und verdienen trotzdem Ihr Vertrauen.

Konzentration aufs Wesentliche. Um Ihr Vertrauen zu verdienen, verzichten wir auf viel. Zum Beispiel darauf, etwas anderes zu tun, als E-Mail zu filtern und zu verarbeiten – wir sind überzeugt, dass die Konzentration auf eine Kernkompetenz der Grund ist für die überlegene Qualität, Präzision und Zuverlässigkeit von Spamchek.

Hinter Spamchek steht Enidan. Enidan wurde 1998 in England gegründet und ist seit 2001 in der Schweiz domiziliert. In unserem Hauptsitz in Herrliberg bei Zürich arbeiten hoch qualifizierte und motivierte IT-Spezialisten. Das nötige (und seltene!) Know-how für die Echtzeit-Verarbeitung von grossen E-Mail-Volumen basiert auf unserer intensiven Forschung und Entwicklung zum Clustering von Hochleistungsrechnern und -netzen.

spamchek
Let your spam stop here.

ENIDAN Technologies GmbH
Bergstrasse 170
CH-8704 Herrliberg
Schweiz
+41 (0) 43 443 9000

www.spamchek.com
info@spamchek.com

Konzept und Text: Christian Rintelen, Art Direction: Stacy Müller, Illustrationen: Franziska Nyffeler