


11/06

SHE

news

Aktuelle Informationen zur IT-Sicherheit in Unternehmen



Bring doch bitte mal den Spam runter!

**Warum die Spam-Flut immer mehr
zunimmt und welche Strategien
wirklich helfen**

IT-Thema des Monats

Wirtschaftlicher Schaden durch
Spam geht in die Milliarden

Unternehmen

SHE wächst weiter und gründet
neue Geschäftsstelle

Sicherer Betrieb

Outsourcing auf dem Prüfstand –
SHE evaluiert, plant und realisiert

Unternehmen Wechsel in der Vorstandsebene der SHE AG



Klaus Schulz, bisher zuständig für Vertrieb und Marketing, wird Alleinvorstand

Zum 1. Oktober hat sich in der Führungsmannschaft der SHE AG eine Änderung ergeben: SHE-Mitgründer und Vorstandsvorsitzender Thomas Köhler hat nach elf Jahren in der Geschäftsführung des IT-Sicherheitspezialisten seinen Vorstandsposten abgegeben, um sich neuen beruflichen Herausforderungen zuzuwenden. Klaus Schulz, bislang zuständig für Vertrieb und Marketing, verantwortet seitdem Köhlers Ressorts mit. Köhler bleibt dem Unternehmen jedoch in anderer Funktion erhalten und wechselt in den Aufsichtsrat. Zu seiner Entscheidung erklärt Köhler: „Die erfolgreich abgeschlossene Spezialisierung der SHE AG auf das Thema IT-Sicherheit zeigt sich jetzt im erfolgreichsten Geschäftsjahr unserer Geschichte. Das ist ein guter Zeitpunkt, um sich persönlich neuen Aufgaben zu widmen.“



Bei SHE weiter „in einem Boot“:
Vorstand Klaus Schulz und der zukünftige Aufsichtsrat Thomas Köhler (von oben).

SHE – Spezialist für integrierte IT-Sicherheitskonzepte

Mit der neuen Besetzung von Aufsichtsrat und Vorstand sieht die SHE AG im 20. Jahr ihrer Unternehmensgeschichte der Zukunft sehr optimistisch entgegen. SHE zählt heute zu den führenden Anbietern für integrierte IT-Sicherheitskonzepte. Als Partner für IT-Sicherheit konzipiert, liefert und betreibt die SHE AG IT-Sicherheits-Lösungen aus einer Hand. Dazu gehören Risikomanagement, die Erstellung von Sicherheits-Policies, Security Audits, Application Security, Service- und System-Integration, Service und Support 24 Stunden an 365 Tagen. Selbstverständlich gehören dazu anspruchsvolle IT-Projekte, nationale und internationale Kunden sowie weltweite Partnerschaften.



IT-Sicherheit von Experten

SHE Service SHE wächst weiter – jetzt auch in Köln



Neuer SHE-Geschäftsstellenleiter in Köln: Ralph Grieser.

Nur zwei Monate nachdem „Zuwachs“ in München gemeldet wurde, baut die SHE AG ihr Geschäftsstellennetz weiter aus: Seit 15. Oktober sind Ihre IT-Sicherheitsexperten auch in Köln und Umgebung für alle Fragen und Anliegen zur Absicherung Ihrer IT für Sie da. Zum Leiter der Geschäftsstelle wurde Ralph Grieser ernannt, der in dieser Position für den Aufbau verantwortlich ist. Grieser, zuvor bei BASF IT Services zuständig für das Geschäft mit der Gruppentochter BASF, ist auf seine neue Aufgabe bei SHE bestens vorbereitet. Insgesamt kann Grieser auf über 10 Jahre Erfahrung mit stetig wachsender Verantwortung in der IT-Branche zurückblicken. Zu seiner Motivation und seinen Zielen bei SHE führt Ralph Grieser aus: „SHE gehört zu den renom-

mierten Dienstleistern in der IT-Sicherheit und wir wollen hier zukünftig der Schrittmacher sein. Unsere gute Positionierung im wachsenden Markt für IT-Sicherheitslösungen, ein hervorragendes Team und die zahlreichen Referenzprojekte bieten beste Voraussetzungen für die künftige Entwicklung.“ Eines seiner wichtigsten Ziele ist es, gemeinsam mit dem SHE-Team das Profil des Unternehmens dahingehend zu schärfen, dass SHE zum Synonym für IT-Sicherheitslösungen wird.

■ **Wünschen Sie einen Beratungstermin? Sie erreichen Herrn Grieser telefonisch unter 0221-5540-5550, per Mail unter ralph.grieser@she.net oder persönlich im MediaPark 8, 50670 Köln.**

Sicherer Betrieb Unternehmen fordern SLA-Redesign

Der Einkauf und das Management von IT-Leistungen in Form von Service-Level-Agreements (SLA) haben sich durchgesetzt. Heute werden neben der IT zahlreiche weitere Geschäftsprozesse „gesourct“. Die Abweichung von gemessener und „gefühlter“ Servicequalität veranlasst jedoch viele Unternehmen dazu, ein Redesign der SLA beim Outsourcing-Anbieter durchzusetzen. Die Ursache dafür liegt häufig in der Planungsphase, der zu wenig Bedeutung beigemessen wurde. Beispielsweise werden die Anforder-

ungen der Endanwender häufig nicht mit berücksichtigt. SHE verfolgt hingegen ein „ganzheitliches“ Konzept: Der IT-Sicherheitsexperte evaluiert, plant und implementiert die Outsourcing-Projekte seiner Kunden – als Full Service-Dienstleister. Dabei entwickelt SHE nicht nur „Empfehlungen“, sondern erzielt messbare Ergebnisse: Kostensenkung, Verbesserung von Transparenz, Flexibilität und Servicequalität sowie Verschlankeung der internen Organisation.

■ **Wir beraten Sie gerne! Rufen Sie einfach an unter 0621-5200-0 oder schreiben Sie eine E-Mail an info@she.net**



„Unerwünschte Werbemails“ bringen immer mehr Mailboxen zum Überlaufen

IT-Thema des Monats

Wirtschaftlicher Schaden durch Spam-Mails wächst stetig – SHE realisiert effektive Lösungen gemeinsam mit Partner IronPort

Der Montag hat es erfahrungsgemäß in sich: Dutzende Mails mit äußerst dubiosen Pharma- und Software-Offerten verstopfen das E-Mail-Postfach im Büro. Die meisten User haben sich zwar mit den nervigen Spam-Mails arrangiert und drücken fleißig die „Delete“-Taste. Tatsächlich sind die wirtschaftlichen Verluste, die durch Spam verursacht werden, immens: Auf etwa 4,4 Milliarden Dollar werden die Schäden durch Spam für das Jahr 2005 allein in Deutschland geschätzt. Das kalifornische Marktforschungsinstitut Ferris rechnete 2005 weltweit mit jährlichen wirtschaftlichen Einbußen in Höhe von 50 Milliarden Dollar.

Spam ist Arbeitsbremse und Sicherheitsrisiko

Der weitaus größte Schaden entsteht, weil Spam-Mails ihre Empfänger vom Arbeiten abhalten. Die Arbeitsleistung der Mitarbeiter leidet, weil unter Umständen auch wichtige Mails von falsch eingestellten Spam-Filtern oder schlechten Antispam-Programmen abgefangen werden. Trotzdem: Ohne diese Tools wäre der Schaden noch weitaus höher. Spam-Mails stellen zudem ein Sicherheitsrisiko dar, vor allem die so genannten „Phishing-Mails“ sind nicht zu unterschätzen. „Besonders gefährlich für die Unternehmenssicherheit sind jedoch Phishing-Mails, die Benutzer dazu verleiten, Webseiten zu besuchen, welche wiederum diverse Sicherheitslücken im WWW-Browser ausnutzen, um lokal auf dem PC des Benutzers Schadprogramme zu installieren“, führt Ralf Nägele, Antispam-Experte der SHE AG aus. Dies kann dann bis zur kompletten Fremdkontrolle eines Rechners führen.

Spammer sind leider sehr anpassungsfähig

Antispam-Lösungen erleben derzeit einen Boom. Dies bestätigt auch SHE-Partner IronPort Systems, führender Hersteller von Gateway-Sicherheitslösungen für kleine und mittelständische bis hin zu Global 2000-Unternehmen. Dieses hohe Wachstum erklärt sich dadurch, dass Spam-Versender flexibel ihre Strategien anpassen. So verändern Spammer innerhalb kurzer Zeit die in über 85 Prozent aller Spam-Mails angepriesenen Links. Im Juni 2006 lag die durchschnittliche Bestandsdauer einer Spam-URL nur noch bei vier Stunden - im Vergleich zu 48 Stunden im Juni des Vorjahres. Außerdem sind neue, raffiniertere Varianten des so genannten Image-Spams auf dem Vormarsch. Diese in ständig veränderten Bildern integrierten Spam-Botschaften sind für herkömmliche Filter nicht erkennbar. Auch die Spam-Quellen haben sich in den letzten zwei Monaten verändert.

So kommen bereits über 80 Prozent aller unerwünschten Nachrichten von Zombie-PCs (mit Trojanern verseuchte Rechner).

Welche Gegenstrategie ist die beste?

In enger Zusammenarbeit mit dem Antispam-Spezialisten IronPort setzt SHE deshalb auf die Implementierung einer Abwehrkette, die je nach Anforderung aus verschiedenen Komponenten bestehen kann (siehe „Was hilft gegen die Spam-Flut?“). IronPort verfügt beispielsweise über eine riesige Datenbank „Senderbase“ mit Spam-Merkmalen, die regelmäßig aktualisiert werden und als Erkennungsgrundlage für Spam-Mails dienen. Über Schnittstellen in der Antispam-Software von IronPort werden Analyseergebnisse zu eingehenden Mails geliefert, so dass IronPort seine Datenbank ständig verbessern kann.

Die beste Abwehr beginnt bereits an der Eingangstür

Idealerweise sollten Spam-Mails dort analysiert und blockiert werden, wo sie zuerst eintreffen: auf dem Mailserver, der E-Mails direkt aus dem Internet empfängt. „Schon hier wird gefiltert, ob Mails an bekannte Empfänger im Unternehmen gerichtet sind oder Spam-typisch differenziert verschickt werden“, erklärt Ralf Nägele und ergänzt: „Dann müssen die dahinterliegenden Mail-Gateways diese Entscheidung nicht mehr treffen.“ So wird die Infrastruktur spürbar entlastet, da keine Mails (ob Spam oder nicht) an unbekannte Empfänger durchgereicht werden müssen. Aber auch auf lange Sicht ist klar: Der Kampf gegen den Spam wird immer wieder neue Gegenmaßnahmen erfordern. Eine gute Abwehr muss mindestens so flexibel sein wie die Spammer selbst.

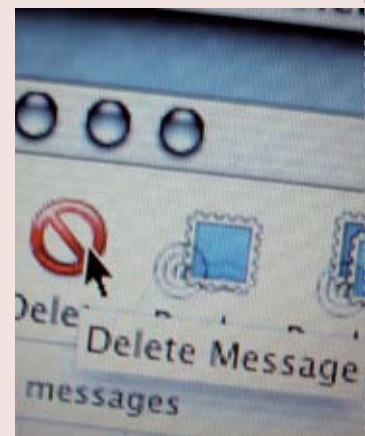
■ **Sie interessieren sich für effektive Lösungen gegen Spam? Wir beraten Sie gerne. Ihr Ansprechpartner: Ralf Nägele, Tel. 0621-5200-217, ralf.naegle@she.net**



Viele Mailbox-Papierkörbe stehen unter „Dauerstress“: Häufig sind unerwünschte Werbemails Schuld daran.



Gemeinsam mit Technologie-Partner IronPort entwirft SHE maßgeschneiderte Antispam-Strategien.



Sichere Infrastruktur

Was hilft gegen die Spam-Flut?

Spam-Versender sind sehr einfallsreich – zumindest wenn es darum geht, Spam-Mails an den Mann (oder die Frau) zu bringen. Meist hilft nur eine Kombination verschiedener Maßnahmen, die im Folgenden beschrieben werden.

Client-basierte Abwehrmaßnahmen sind primär für den privaten Bereich interessant. Für größere Mail-Infrastrukturen bieten sich eher Gateway-Lösungen an. Die meisten Antivirus-Hersteller bieten für ihre Antivirusbösungen Antispam-Zusatzmodule mit an, welche sich problemlos in die bestehende Antivirus-Lösung integrieren lassen.

„Realtime Black Lists“ (RBL): Hier überprüft der Mailserver beim Empfang einer Mail, ob die Mailadresse des sendenden Mailservers sich in einer so genannten „Blacklist“ befindet. Die Abfrage erfolgt meist per DNS-Anfrage. Befindet sich die Mail in einer RBL, verweigert der Mailserver die Annahme schon beim Verbindungsaufbau.

Protokollbasierte Verfahren, wie beispielsweise EHLO/HELO-Check können ebenfalls schon auf Transportebene eine unerwünschte Verbindung verhindern und filtern so wirkungsvoll im Vorfeld Spam-Mails aus.

Weitergehende Analysen der eingehenden Mail können im Mailteil (im so genannten „mail body“) selbst erfolgen. So wird aufgrund bestimmter Muster im „Subject“ (Betreff), im Mailheader, im Mailteil oder aufgrund bestimmter Worte oder Zeichenhäufigkeiten entschieden, ob es sich um eine Spam-Mail handelt oder nicht.

Einsatz eines „Bayes-Filter“: Vereinfacht gesagt, wird hier über die charakteristischen Wörter von Spam-Mails auf die Eigenschaft der Mail geschlossen (Spam oder kein Spam).

Einige Hersteller von Antispam-Lösungen bieten neben den obigen Methoden auch Verfahren an, die denen von Virenschernern ähneln. In diesem Fall werden feste Muster („Patterns“) regelmäßig vom Hersteller übermittelt, mit denen eingehende Mails dann verglichen werden.

Gute Antispam-Lösungen kombinieren verschiedene Methoden, wie beispielsweise OCR-Texterkennung in Bildern, Absenderauthentifizierung, Greylisting, Reputation, Bounce Kontrolle, etc.

Generell sollte der Empfänger niemals auf eine Spam-Mail antworten – und auch nicht die Abmeldelinks am Ende einer Mail verwenden.

Die HTML-Ansicht des Mailprogramms sollte ebenso deaktiviert sein wie die Möglichkeit, HTML-Mails zu verschicken. Ersteres kann helfen, verdächtige Mail besser zu erkennen. Letzteres kann vermeiden helfen, dass evtl. die eigene Mail in Spam-Filtern hängen bleibt.

„Unerwünschte Werbemails“ sind auch in Ihrem Unternehmen längst mehr als ein „Nerv“-Thema?

Wir beraten und unterstützen Sie gerne bei der Konzeption und Umsetzung wirksamer Maßnahmen gegen Spam. Rufen Sie uns an!



Ralf Nägele, Antispam-Experte und Security Consultant bei SHE.



Sichere Infrastruktur

IT-Thema des Monats

„Spam“

So schützen Sie sich vor den nervigen und gefährlichen Werbemails

Jetzt Infos anfordern!



Zeit für eine sichere IT!

IT-Risikoanalyse

Prozessorientierte IT-Risikoanalyse

Sichere Applikationen

Application Layer Gateways • Sichere Entwicklung • SecureDocXpress • Sicherheits-Audit

Sichere Infrastruktur

Firewall • VPN • Content-Security • Mobile Lösungen • Intrusion Prevention Systeme • VoIP

Sicherer Betrieb

Systempflege • Systemüberwachung • Change-Management • Disaster-Recovery • ITIL

Innovative IT-Sicherheitslösungen sind gefragt

Die SHE Informationstechnologie AG in Ludwigshafen zählt zu den führenden Anbietern für integrierte IT-Sicherheitskonzepte. Das derzeit etwa 80 Mitarbeiter starke Unternehmen konzipiert, liefert und betreibt seit mehr als 19 Jahren IT-Security Lösungen aus einer Hand.

Anspruchsvolle IT-Projekte, nationale und internationale Kunden, weltweite Partnerschaften: Renommierete Unternehmen aus den unterschiedlichsten Branchen setzen auf die Lösungskompetenz der IT-Sicherheits-Experten von SHE.



SHE bietet Ihnen ein umfassendes Leistungsportfolio:

- ▶ Für jede Branche effiziente und intelligente IT-Sicherheitskonzepte – insbesondere für mittelständische Unternehmen
- ▶ Beratung, Konzept, Umsetzung durch erfahrene IT-Sicherheitsexperten
- ▶ Outsourcing & Outtasking – überzeugende Angebote für Ihr Unternehmen!
- ▶ Hochverfügbares Multi-Standort-Rechenzentrum
- ▶ SHE-Sicherheitslösungen werden mit namhaften Anbietern wie Aladdin, Check Point, Cisco, IronPort, ISS, Kobil, Nokia, RSA, Visonys und Vordel realisiert
- ▶ Bedarfsorientierte Service-Level-Agreements & Support

IT-Sicherheit in allen Prozessen. SHE zeigt Ihnen, wie!

Nutzen Sie die Kompetenz der SHE IT-Sicherheits-spezialisten

Mehr über SHE unter:
www.she.net

Ihre direkten SHE Ansprechpartner zum Thema „Spam“ und zu allen weiteren IT-Sicherheitsthemen

Haben Sie Fragen, wünschen Sie weitere Infos oder möchten Sie gleich einen Termin vereinbaren? Wir freuen uns über Ihren Anruf, Ihr Fax oder Ihre E-Mail.



Klaus Schulz
Vorstand

fon 0621.5200-170
fax 0621.5200-550
E-Mail klaus.schulz@she.net



Ralf Nägele
Security Consultant

fon 0621.5200-217
fax 0621.5200-558
E-Mail ralf.naegele@she.net



Florian Lenz
Business Unit Manager
Sicherer Betrieb

fon 0621.5200-203
fax 0621.5200-555
E-Mail florian.lenz@she.net

Zu unseren Referenzen zählen Unternehmen wie BASF, T-Mobile, DIS AG, Inter Versicherung, Pepperl+Fuchs, Karlsruher Messe- und Kongress-GmbH, Landratsamt Rhein-Neckar-Kreis, Pluradent, AZO, Wiley-VCH-Verlag, Mannheimer Morgen, Roche Diagnostics, Suzuki, Vattenfall sowie die Stadtverwaltung Ludwigshafen u.v.a.

Impressum

Herausgeber
SHE Informationstechnologie AG
Konzept & Gestaltung
Xmedias GmbH, Mannheim



IT-Sicherheit von Experten

Aktuelle SHE Veranstaltungen und Termine

21. November 2006:

VMware-Tag Köln

Viele von Ihnen kennen VMware in Verbindung mit Themen wie Server-Virtualisierung, Hochverfügbarkeit und Disaster Recovery. Auf unserer Roadshow „Fit für Virtualisierung“ möchten wir Ihnen das Produkt-Portfolio von VMware im Hinblick auf Technik, Sicherheit und Wirtschaftlichkeit näher bringen. Einen Agenda-Überblick erhalten Sie unter www.she.net. Melden Sie sich noch heute an – am schnellsten per E-Mail unter veranstaltungen@she.net oder über unsere Webseite. Die Teilnehmerzahl ist begrenzt.

Vorschau auf die nächste SHE news

„Virtualisierung ist mehr als Serverkonsolidierung!“ Sie haben diesen Satz schon oft gehört, möchten jetzt aber auch gerne wissen, was sich dahinter verbirgt? In der nächsten **SHE news** erfahren Sie mehr über die faszinierenden Möglichkeiten, die Virtualisierungs-Software Ihrem Unternehmen bieten. Erhebliche Einsparpotenziale und effiziente Workflows in der IT sind dabei die wichtigsten Stichworte. Doch auch hier zeigt sich: Nur mit dem richtigen Know-how ist Virtualisierung auch eine sichere Sache.

SHE Informationstechnologie AG
Donnersbergweg 3
Fon +49(0)621.5200-0
E-mail info@she.net
D-67059 Ludwigshafen
Fax +49(0)621.5200-558
www.she.net