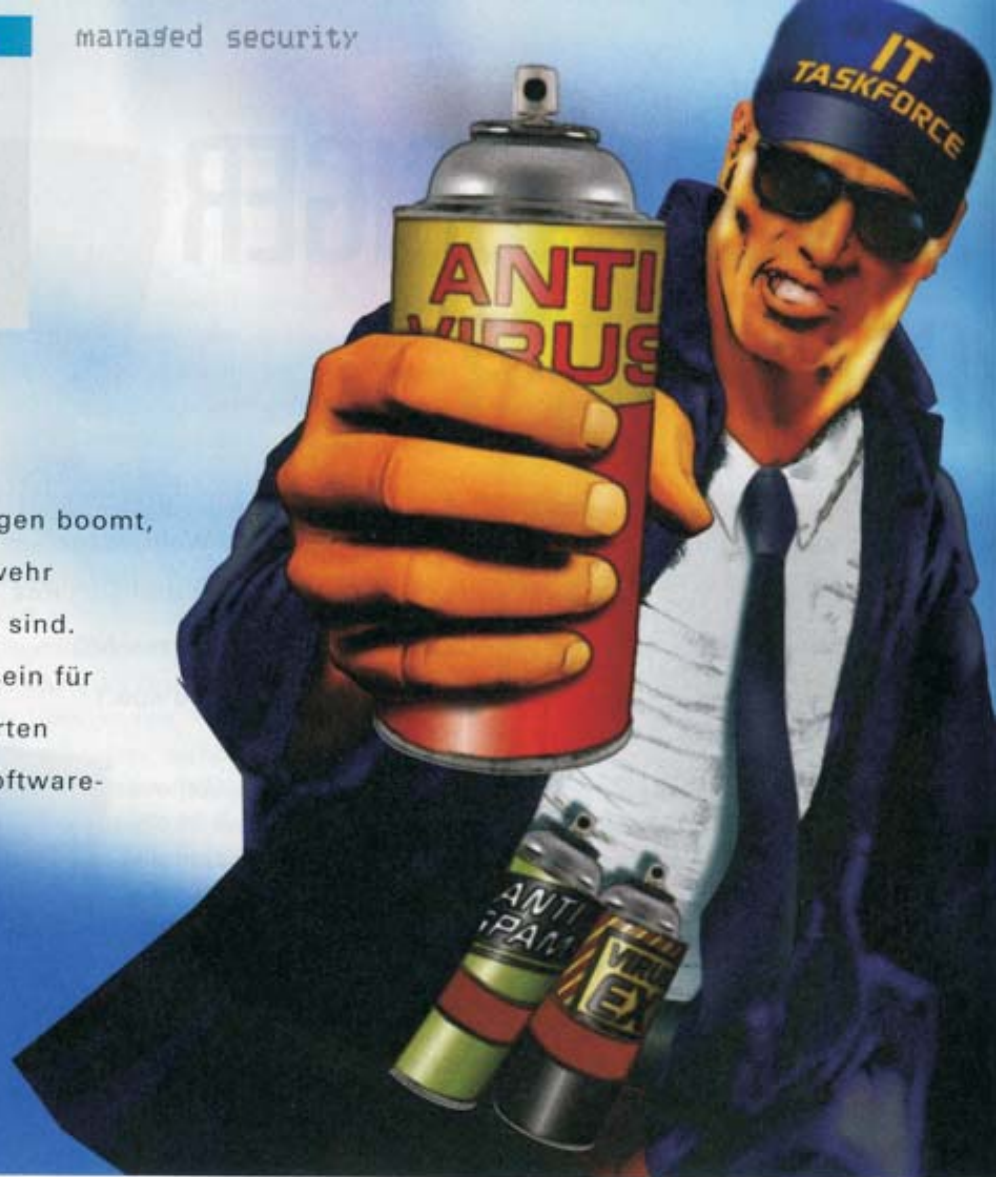


Inhalt

Sicherheit als Service	58
Auslagern oder selber machen?	63
In sicheren Händen	68



Das Auslagern von Sicherheitslösungen boomt, weil viele Mittelständler mit der Abwehr komplexer Bedrohungen überfordert sind. Der Markt scheint jedenfalls reif zu sein für Hosted Security, denn neben etablierten Providern treten zunehmend auch Software-Hersteller als Dienstleister auf.

Mittelständische Unternehmen haben anders als große Firmen oft nicht das notwendige Know-how und die erforderlichen Ressourcen, um sich effektiv gegen immer raffinierter werdende Bedrohungen aus dem Internet abzusichern. Die Materie ist zu komplex, Sicherheitsspezialisten sind rar und teuer. Und da IT-Sicherheit nicht zum Kerngeschäft gehört, wird sie oft vernachlässigt.

Hinzukommen gesetzliche Vorgaben, die das Management dazu verpflichten, im Rahmen des Risikomanagements für umfassende IT-Sicherheit zu sorgen. Die Auslagerung der unternehmenseigenen Netzwerk- und Datensicherung an einen Anbieter von Hosted Security Services bzw. Managed Security Services (MSS) kann Unternehmen dabei helfen, diese Herausforderungen zu meistern und gleichzeitig die Kosten für Hard- und Software sowie die Administration zu reduzieren.

Mit dieser Strategie schützt zum Beispiel das Kölner Druck- und Medienunternehmen Moeker Merkur GmbH sein Firmen-

JOHANNES FRITSCHKE

SICHERHEIT ALS SERVICE

netz. Etwa 30 Mitarbeiter des Unternehmens nutzen das Internet, teils von Windows-Arbeitsplätzen, teils von Mac-Rechnern aus. E-Mail und Webnutzung sind die Standard-Applikationen. „Die Kommunikation über E-Mail ist zur unternehmens-

kritischen Applikation geworden, da Angebote, Bestellungen und Layoutdaten auf diese Weise schnell und direkt ausgetauscht und weiterverarbeitet werden können“, berichtet Geschäftsführer Friedhelm Spöhr. Eine Schwachstellen-Analyse hatte

zudem gezeigt, dass die bisherige Schutzlösung an ihre Grenzen gekommen und der Virenschutz auf den einzelnen Arbeitsplätzen uneinheitlich war.

Um die Internet-Sicherheit auf einem gleich bleibend hohen Niveau zu halten, lagerte Firmenchef Spohr Virenschutz und Firewall zum monatlichen Festpreis an die Pallas GmbH im rheinischen Brühl aus. Der IT-Dienstleister betreibt in einem Security Center abgesicherte Internet-Server und Applikationen und berät bei der Netzwerksicherheit. Durch eine Virtual-Private-Network-Verbindung (VPN) wird sichergestellt, dass auf das Firmennetz nur über das Security Center zugegriffen werden kann.

„Moeker Merkur wird sozusagen hinter dem Security Center versteckt, und durch die zentralen, von Experten rund um die Uhr betreuten Systeme wird die Sicherheit eines professionellen Rechenzentrums erreicht“, erläutert Dr. Kurt Brand, Geschäftsführer der Pallas GmbH. Wächst der Bedarf, lassen sich die Schutzfunktionen flexibel anpassen, ohne dass Investitionen bei Moeker Merkur erforderlich sind.

Deutsche Dienstleister werden bevorzugt

Dass Firmenchef Spohr einen regionalen deutschen Dienstleister auswählte, liegt im Trend: Insgesamt nur sechs Prozent der auslagernden Unternehmen ordern IT-Dienstleistungen in anderen europäischen und außereuropäischen Ländern. Dies zeigt eine repräsentative Befragung von rund 4300 Unternehmen mit mindestens fünf Beschäftigten im verarbeitenden Gewerbe und in ausgewählten Dienstleistungsbranchen, die das Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim Anfang 2007 mit finanzieller Unterstützung der Landesstiftung Baden-Württemberg durchgeführt hat.

„Es zeigt sich hier, dass die Unternehmen beim Bezug ihrer IT-Dienstleistungen auf regionale Nähe setzen“, sagt Dr. Irene Bertschek, Leiterin der Forschungsgruppe Informations- und Kommunikationstechnologien am ZEW. Wie nötig eine solche externe Unterstützung ist, zeigen die Auswertungen der Security-Audits von Panda Security. 76 Prozent aller Netzwerke, die mit Pandas Netzwerk-Audit-Tool *MalwareRadar* gescannt wurden, waren trotz vorhandener klassischer Sicherheitslösungen infiziert.

Aus solchen Gründen setzt auch Michael Brüning, IT-Leiter bei der Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA) in Berlin, auf die Unterstützung externer Profis. Gemeinsam mit vier Kollegen betreut er 120 Mitarbeiter in der Berliner Zentrale.

„Wir haben uns eine ganze Zeit lang selbst mit Spam- und Virenfiltern befasst. Das erwies sich auf Dauer aber als zu kompliziert, zu zeitaufwändig und nicht wirklich wirksam. Die ständigen Software-Updates einzuspielen erforderte einfach zu viel Manpower“, erklärt Brüning. „Allein von Januar bis August 2007 mussten wir uns mit rund sieben Millionen Spam-Mails befassen. In Spitzenzeiten mit ca. 200 eingehenden E-Mails pro Minute waren nicht mehr als acht Prozent des gesamten eingehenden Mail-Verkehrs tatsächlich sinnvolle und gewünschte Nachrichten.“

Statt weiter die aufwändige interne Lösung zu verfolgen, entschied sich der Verband, als externen Dienstleister die Münchener Retarus GmbH zu beauftragen. Alle ein- und ausgehenden Mails laufen jetzt über die Münchener Rechenzentren des Messaging-Dienstleisters. Die mehrstufigen Filter reduzieren das bei der BDA eintreffende Mailvolumen um bis zu 95 Prozent. Nur fünf Prozent der Nachrichten sind tatsächlich geschäftsrelevant und werden weitergeleitet. Betrieb und Administration der Sicherheits-Infrastruktur liegen bei Retarus. Die Systemlast auf den Servern und Leitungen der BDA sinkt, und die Mitarbeiter werden im Alltag nicht mehr durch E-Mail-Probleme und Sicherheitslücken belastet.

„Attraktiv ist die Lösung auch unter finanziellen Aspekten, die IT-Abteilung kann jetzt ohne permanente Investitionen in Hard- und Software für eine hohe Performance,

Pro & contra: Checkliste zum Security Outsourcing

Der Sicherheits-Anbieter Securepoint hat einige zentrale Fragen zusammengestellt, die man sich vor der Entscheidung für oder gegen Security Outsourcing stellen sollte:

- Welche Sicherheitsfunktionen werden benötigt?
- Ist im Unternehmen zu jeder Zeit so viel Security-Know-how vorhanden, dass Geschäftsprozesse sicher ablaufen können?
- Ist eine outgesourcete Security-Lösung zuverlässiger und einfacher als das eigene System?
- Senkt Security Outsourcing die Gesamtkosten?
- Ist das Security Outsourcing mit dem Wachstum des Unternehmens gleichermaßen skalierbar?

Sollte die Entscheidung zu Gunsten von Security Outsourcing fallen, stellen sich grundlegende Fragen, die bei einer Auswahl eines geeigneten Security-Providers helfen können. Um Angebote bewerten zu können, ist es sinnvoll, sich zunächst einen realistischen Überblick über die anfallenden Aufgaben zu verschaffen:

- Welche Security-Leistungen (Firewall, VPN, Antivirus, Spam-/Content-Filtering, IDS, Monitoring etc.) werden angeboten?
- Welche Security-Überprüfungen und -Reports werden wie oft für das Unternehmen durchgeführt?
- Wie hoch ist die garantierte Uptime der Security-Systeme?
- Werden SLAs (Service Level Agreements) garantiert? Wie sind diese geregelt (garantierte Verfügbarkeiten, Support, Wartungsarbeiten)?
- Wie sieht es mit dem User-Support (Verfügbarkeit, Sprache, Remote) aus?
- Werden regelmäßig Backups/Archivierungen von Security Policies und Security Reports/Logfiles durchgeführt?
- Besitzt der Security Provider einen Notfallplan?
- Wie hoch sind umgerechnet die Kosten pro Arbeitsplatz?
- Kann von einer outgesourceten Lösung einfach auf eine innerbetriebliche gewechselt werden?
- Ist der Security Provider gegen Ausfälle versichert?

Verfügbarkeit und Sicherheit der Kommunikations-Infrastruktur sorgen“, berichtet IT-Leiter Brüning.

Ein solcher Rundumschutz ist auch für Selbstständige und Kleinunternehmen mit wenigen Mitarbeitern interessant, die sich keine eigene ausgefeilte IT-Sicherheitslösung leisten können oder wollen. Für die könnte der externe E-Mail-Spam- und Virenschutz *SecureMX* der Münchener InterNetWire Communications GmbH in Frage kommen: Die Tarifstaffel für *SecureMX* bezieht sich auf die Anzahl der E-Mail-Postfächer (Benutzer). Mail-Durchsatz oder -Größe spielen keine Rolle. „Um *SecureMX* zu nutzen, ist keine zusätzliche Soft- oder Hardware auf Empfängerseite nötig, das Ändern des MX-Records im DNS-Eintrag der Domain genügt“, erläutert Johannes Steck, bei InterNetWire zuständig für den Vertrieb dieser Dienstleistung. Mehrere Server mit jeweils 16 GByte Arbeitsspeicher, einem RAID-System für Log-

leister die Sicherheits-Infrastruktur günstiger als das IT-Team eines Unternehmens betreiben, zum anderen ist er stark spezialisiert und erfahrener, man traut ihm deshalb mehr Kompetenz zu.

„Diese Argumente sind sicherlich korrekt, dennoch warne ich davor, die Kontrolle über die eigenen Daten leichtfertig aus der Hand zu geben. Bei manchen Outsourcern weiß man hinterher nicht einmal, auf welchem Kontinent die eigenen Daten liegen und welche Personen darauf Zugriff haben“, erklärt Sebastian Schreiber, der sich als Geschäftsführer der Tübinger SySS GmbH einen Ruf als unabhängiger Sicherheitsexperte erworben hat. Mitarbeiter in einem gut geführten Unternehmen hätten ein erhebliches Maß an Loyalität gegenüber ihrer Firma und würden mit den eigenen Unternehmensdaten sorgfältiger und verantwortungsvoller umgehen als mit den Daten eines anonymen Kunden, der sich irgendwo auf der Welt befindet.



Nicht nur die Bedrohungen kommen aus dem Internet, sondern auch der Schutz davor – das ist der Kern des Hosted-Security-Konzepts.



Files und die Quarantäne sowie performante Prozessoren im gesicherten Rechenzentrum von InterNetWire ermöglichen einen hohen Durchsatz. Die Zuverlässigkeit der Spam- und Virus-Abwehr und auch den datenschutztechnisch einwandfreien Umgang mit den Kunden-E-Mails hat die tekit Consult Bonn GmbH, ein Unternehmen der TÜV Saarland Gruppe, bewertet und das Prüfzeichen „TÜV-zertifizierte Managed Services“ erteilt. Im Rahmen des Audits wurde auch die Wirkung des Spam-Filters mit einer Test-Domain geprüft. Das Resultat: Über 98 Prozent des Spam-Aufkommens wurde geblockt.

Das Outtasking von IT-Security scheint also eine attraktive Alternative zum Selbstbetrieb zu sein. Zum einen kann der Dienst-

Diese verständliche Skepsis von Firmen- und IT-Chefs versuchen die internationalen Anbieter von Hosted Security Services zu zerstreuen. „MessageLabs beschäftigt sich seit vielen Jahren mit den rechtlichen Anforderungen von Kunden an die IT-Sicherheit und ist sich somit der Probleme bewusst, die eine Umleitung von Internet-Kommunikation außerhalb des regionalen Rechtsraumes mit sich bringen würde“, erklärt zum Beispiel Alexander Peters, Global Client & Partner Services Manager bei MessageLabs. Während die EU-Datenschutzrichtlinie einen gemeinsamen Nenner bietet, halte sich MessageLabs als ein ISO 27001:2005-zertifiziertes Sicherheitsunternehmen an die striktesten Sicherheitsanforderungen in diesem Rechtsraum.

„Die MessageLabs-Infrastruktur ist zwar global aufgestellt, jedoch logisch strikt nach geografischen Regionen getrennt: Europa (EU-Rechts-Zone), USA und Asien. Hierbei wird auch garantiert, dass der Datenverkehr gemäß den regionalen Anforderungen der Kunden innerhalb des entsprechenden Rechtsprechungsraumes bleibt. Somit können Kunden in Deutschland sicher sein, dass die Daten niemals die EU verlassen“, fügt Peters hinzu. Die EU-Rechenzentren befinden sich in Frankfurt am Main, Amsterdam und London.

Ähnlich äußert sich Kai Gutzeit, Regional Sales Director DACH & Eastern Europe & Italy beim Mitbewerber Postini: „Deutsche Firmenchefs können bei der Lösung von Postini beruhigt sein: Im Gegensatz zu anderen Anbietern, die nach dem Store-and-Forward-Konzept arbeiten, werden keine Daten in den Rechenzentren von Postini gespeichert, die Bearbeitung erfolgt in Echtzeit.“

Möchte ein deutsches Unternehmen darüber hinaus seine E-Mails mit Postini archivieren, werden diese in den hochsicheren Rechenzentren in der Schweiz gespeichert. „Dortige Anforderungen an die Sicherheit sind noch höher als in Deutschland. Einen unberechtigten Zugriff auf die Unternehmensdaten im Ausland brauchen die Kunden von Postini somit nicht zu fürchten“, verspricht Kai Gutzeit.

Auch Michael Neumayr, Regional Manager Central Europe bei Websense in Köln, glaubt seine Kunden gegen Angriffe von Hackern und Wirtschaftsspionen gut gesichert: „Als Anbieter von Managed Services sind wir verpflichtet, das größtmögliche Maß an Sicherheit in Bezug auf die Kundendaten zu gewährleisten. Hier werden entsprechende geltenden Zertifizierungen und Standards gehandelt wie zum Beispiel ISO 27001.“

Marktoffensive

Auch die Anbieter von Schutz-Software haben erkannt, dass die Zeit jetzt reif ist, Auslagerungs-Dienstleistungen anzubieten. So will zum Beispiel Symantec mit *Hosted Mail Security* die E-Mail-Infrastruktur von Unternehmen vor Spam-E-Mails, Viren und anderen unerwünschten Inhalten schützen, ohne dass vor Ort zusätzliche Hardware, Software oder eine fortlaufende Wartung erforderlich ist. Die Lösung wird von Symantec als Host Service ausgeführt und

Jörg Kurowski, Regional Director DACH
bei McAfee



Warum Sicherheit auslagern?

„Unternehmen, die nur sehr wenig Zeit für den Schutz ihrer IT-Systeme haben, fahren oft besser, wenn sie damit einen Dienstleister beauftragen. Wer Sicherheit als Service kauft und damit in die Hände von Experten legt, kann die eigene Arbeitskraft guten Gewissens anderweitig einsetzen. Außerdem stehen ihm dadurch möglicherweise technische Lösungen zur Verfügung, die sonst außerhalb seiner finanziellen Möglichkeiten wären.“

enthält neben *Brightmail AntiSpam*- und *Symantec AntiVirus*-Technologien auch Funktionen zur Verwaltung isolierter Dateien, zum Erstellen grafischer Berichte und zum Schutz vor Directory-Harvest-Angriffen (Diebstahl von Adressdatenbanken) und anderen E-Mail-Bedrohungen. Die Managed Security Services von Symantec basieren auf dem so genannten Symantec Global Intelligence Network, das sich aus den Frühwarnsystemen *Symantec DeepSight* und vier Security Operations Centers zusammensetzt.

„Durch Managed Security Services können Unternehmen ihre IT-Sicherheit verbessern, dennoch schrecken viele davor zurück, Daten und Sicherheits-Infrastruktur an einen externen Sicherheitsdienstleister auszulagern, da sie einen Kontrollverlust oder den Rückgang der unternehmenseigenen Kompetenz auf diesem Gebiet fürchten“, erklärt Olaf Lindner, Senior Solutions Marketing Manager EMEA bei Symantec. Oftmals würde eine Entscheidung für Managed Security Services erst dann getroffen, wenn akuter Handlungsbedarf besteht oder der Krisenfall bereits eingetreten ist.

„Die Skepsis vieler Unternehmen ist jedoch unbegründet, wenn das Projekt sorgfältig geplant wird und Experten sowie alle beteiligten Unternehmensbereiche früh in die Prozesse eingebunden werden“, versichert Lindner. Ein entscheidender Erfolgsfaktor sind präzise formulierte Service Level Agreements. Diese gewährleisten, dass ein Service Provider die zugesagten Sicherheitsdienste tatsächlich leistet, und bilden die Grundvoraussetzung dafür, dass Managed Security Services ihren vollen Nutzen für Unternehmen entfalten können.

Auch Kaspersky Lab bietet seinen Kunden zusätzlich zur lokalen Installation einer Sicherheitslösung vermehrt Dienstleistungen: Mit den neuen *Hosted Security*-Angeboten können Unternehmen ihren Internet- und Kommunikationsverkehr vor Schad-Software und Spam schützen, ohne lokal Software zu installieren.

„Kaspersky Lab verkauft Sicherheit. Um vor Schad-Software und Spam zu schützen, ist es aber nicht zwangsläufig notwendig, lokal Software zu installieren, um deren Wartung sich dann die Unternehmen kümmern müssen“, sagt Günter Fuhrmann, Director Hosted Security Europe bei dem Sicherheitsspezialisten.

Das größte Einfallstor für Schadprogramme ist die E-Mail-Kommunikation, zudem ist ein Großteil der Nachrichten unerwünschter Spam. *Kaspersky Hosted E-Mail Security* garantiert hundertprozentige Virenfreiheit bezüglich bekannter Schad-Software und mindestens 95-prozentige Spam-Freiheit. Die Nachrichten können sowohl einzeln als auch ausgehend kontrolliert werden. Mit Content Control werden zudem Mails auf eine bestimmte Größe oder Inhalte hin überprüft und bei Bedarf aussortiert.

Nicht nur die E-Mails, auch der gesamte Internet-Traffic kann über ein Kaspersky-Datenzentrum umgeleitet werden. Dort wird der Datenverkehr durch *Kaspersky Hosted Web Security* auf Schad-Software und Inhalte überprüft und entsprechend geblockt. Ein URL-Filter sperrt je nach Firmen-Policy den Zugriff auf Webseiten in vorab festgelegten Kategorien und stellt so die Einhaltung der Unternehmens-Richtlinien sicher.

Da Instant Messaging (IM) im Unternehmensumfeld zuletzt enorm an Bedeutung ge-

wonnen hat, prüft *Kaspersky Hosted IM Security* den IM-Datenstrom auf Viren und IM-Spam (SPIM). Auch eine Überprüfung der Inhalte ist möglich.

Alle drei Dienste können separat oder in Kombination gebucht werden. In allen Fällen wird der Datenverkehr über Server von Kaspersky Lab umgeleitet und anschließend frei von Schad-Software und Spam an die Kunden ausgeliefert. Kaspersky Lab hat dafür bereits im Oktober in Deutschland, Frankreich und den Niederlanden Datenzentren in Betrieb genommen. Für dieses Jahr ist noch ein weiteres in Großbritannien geplant.

„Kaspersky hat von Anfang an Datenzentren in den Regionen eröffnet, in denen auch unsere Kunden sitzen. Damit ist dem Gefühl und dem Fakt Sorge getragen, dass die Daten nur im Land des Kunden gemäß seiner Policy überprüft werden“, versichert Hosted Security Director Fuhrmann.

Fazit

Die Bedrohung der IT-Infrastruktur eines Unternehmens wird immer komplexer. Klassische Viren-, Hacker- und Spam-Attacken stagnieren zwar, allerdings auf sehr hohem Niveau; raffiniertere und mehr Erfolg versprechende Angriffe mit Social-Engineering-Methoden und verseuchten Webseiten nehmen rasant zu. In eigener Regie die Abwehr wirksam zu organisieren übersteigt zunehmend die Möglichkeiten der IT-Teams in mittelständischen Unternehmen, die sich vor allem um das Tagesgeschäft kümmern müssen.

So zeichnet sich ab, dass der Markt der IT-Sicherheit für Angebote zur Arbeitsteilung reif ist: Externe regional und international agierende Dienstleister schützen mit Hosted Security Services professionell und kostengünstig Netz und Daten ihrer Kunden. Und da die Umsätze mit Software-Lösungen gegen Viren, Hacker und Spam nicht beliebig weiter zu steigern sind, springen Lösungsanbieter auch auf diesen Zug auf, um als Service Provider von dieser Entwicklung zu profitieren.

Doch wie bei allen digitalisierten Geschäftsprozessen gilt auch für die IT-Sicherheit: „Ich empfehle Firmen- und IT-Chefs, dosiert auszulagern – und das nur unter der Voraussetzung, dass ein erhebliches Maß an Vertrauen zum Dienstleister besteht“, erklärt SySS-Geschäftsführer Schreiber. *mm*