rad übernimmt Getgoods S. 19 ▸ Google-Kampagnen bei iTeam S. 20 www.it-business.de

# IT-BUSINESS

RGANG | € 6,– ISSN 1864-0907 DAS CHANNEL-MAGAZIN FÜR IT UND CLOUD COMPUTING NR. 25, 16. 12. 2013 – 12. 01. 2014

## Vertrauen in Zeiten digitaler Überwachung

**Ralf Nitzgen, Chef der Allgeier IT Solutions, zu den Chancen der Partner beim Schutz vor Ausspähung der Kunden.**


## IN DIESER AUSGABE

### PARTNERMODELL VEREINFACHT

Für VMware plant Mato Petrusic ein weltweites Partnerprogramm – mit einigen Vereinfachungen.

▸ SEITE 8

### EHRGEIZIGE ZIELE

Mit Physical Security und New Energy pusht Marcus Adä Ingram Micro im Value-Geschäft.

▸ SEITE 14

### MEHR MARGE

Eigene Partner-Versionen und neue Jahresgebühren: Lexware krempelt den Channel um.

▸ SEITE 10

### ZUKUNFTSMUSIK

Beim „Smart Home" stehen unterschiedlichste Hersteller und Distributoren in den Startlöchern.

▸ SEITE 48

## SPEZIAL




### PERIPHERIE & ZUBEHÖR

Diese Produkte haben das ganze Jahr Saison – trotz des rückläufigen PC-Markts. Das Zubehör für Smartphones und Tablets könnte zum Bestseller werden.

▸ SEITE 51

ogel Business Media

▸ IT-Security mit Brief und Siegel: Das „BSI Campus 2013" S. 34

# Die „gefühlte IT-Sicherheit“ in Zeiten der Rundumüberwachung

Wem schenke ich Vertrauen? Wie ermittle ich Vertrauenswürdigkeit? Fragen wie diese sind in der IT-Security-Branche aktueller denn je. Ralf Nitzgen, Chef der Allgeier IT Solutions, ist auch auf das Vertrauen seiner Kunden angewiesen. IT-BUSINESS sprach mit ihm über die Zeit nach Snowden.

IT-BUSINESS / Das Interview führte Dr. Stefan Riedl

## Zur Person

Ralf Nitzgen ist Geschäftsführer der Allgeier IT Solutions GmbH aus Bremen. Das 1977 gegründete Unternehmen ist Teil der börsennotierten Allgeier SE und hat sich unter anderem auf Lösungen in den Bereichen Cloud Solutions sowie Compliance & Security spezialisiert.

web | http://www.allgeier-it.de

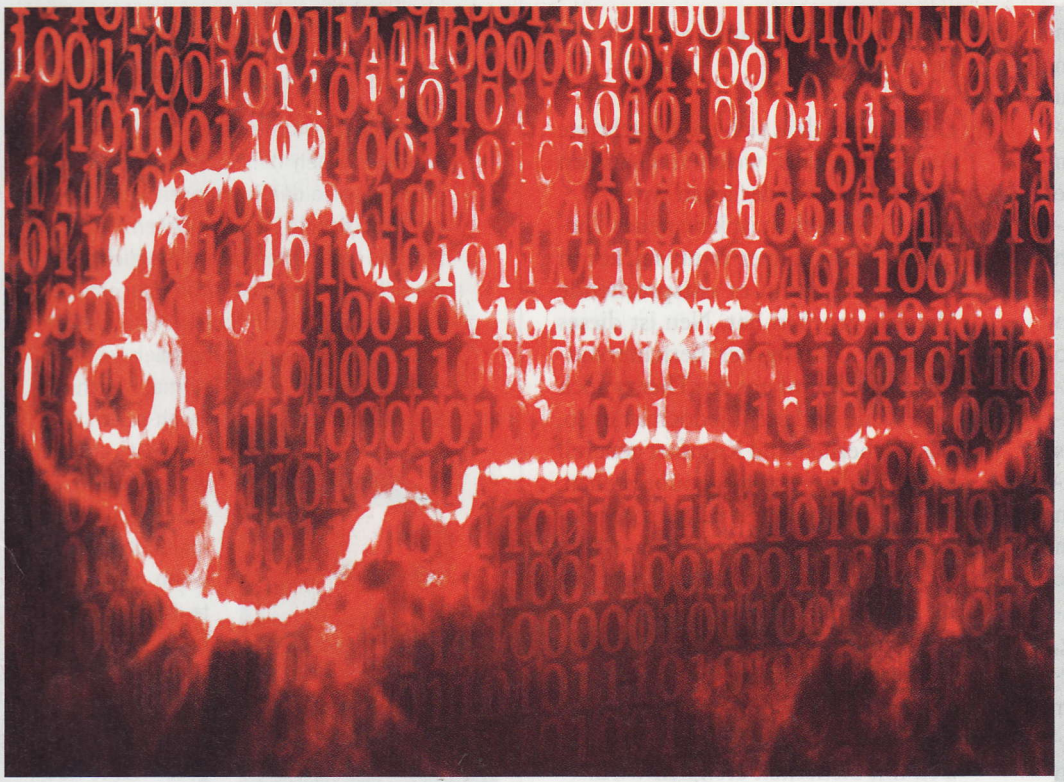
ITB: Nach den Enthüllungen des Whistleblowers Edward Snowden werden IT-Sicherheitsparadigmen neu ausgelotet. Spähprogramme, die Kommunikationsdaten abgreifen, wie Prism und Tempora, sind in aller Munde. Und vieles deutet darauf hin, dass die Bevölkerung und Unternehmen – auch in Deutschland – nicht nur wegen „originärer“ Geheimdienst-Tätigkeit ausgespäht werden, sondern dass auch Wirtschaftsspionage betrieben wird. Wie beurteilen Sie die Gemengelage?

NITZGEN: Letztendlich ist diese Gesamtsituation nicht grundsätzlich neu, denn auch das Spionagenetz Echelon, das seit über zehn Jahren, unter anderem von den USA, Großbritannien, Australien und Kanada betrieben wird, hat die Massendatenspeicherung und das Abhören von Kommunikationskanälen wie Telefon und Mail-Verkehr zur Aufgabe. Der Verwendungszweck dieses Netzes ist bereits 2004 öffentlich bekannt gegeben worden. Auch ist das Recht zur Wirtschaftsspionage einiger Staaten seit jeher in der Verfassung verankert. Vor dem Hintergrund ist mit den aktuellen Enthüllungen in Verbindung mit einer hohen medialen Aufmerksamkeit dieses Thema in das öffentliche Bewusstsein gelangt, was an und für sich schon seit vielen Jahren auf breiter Basis praktiziert wird. Gleichwohl stellen diese Spähprogramme für die hiesige Wirtschaft eine ernsthafte Bedrohung dar. Unternehmen sind daher spätestens heute gefordert, für sich diese Situation neu zu beurteilen und geeignete Sicherheitsmaßnahmen zu betreiben.

ITB: Verschlüsseln lautet das Gebot der Stunde. Zu den Snowden-Enthüllungen zählt aber auch das so genannte „Project Bullrun“, das offenbar sogar SSL-Verschlüsselung knacken kann. Wie schätzen Sie die Möglichkeiten der Geheimdienste ein?

NITZGEN: Man muss an der Stelle etwas differenzieren. In den meisten öffentlich gewordenen Fällen sind die Angriffe auf Schwächen bei der Umsetzung der Sicherheitsmechanismen und nicht auf Schwächen des zugrundliegenden Verfahrens zurückzuführen. Das Verfahren der SSL- beziehungsweise der asymmetrischen Verschlüsselung ist nach dem heutigen Stand der Kryptografie-Wissenschaft nach wie vor nicht ohne weiteres „knackbar“. Es gibt zwar die Möglichkeit einer sogenannten Man-in-the-Middle-Attacke. Dieser Zugriff kann allerdings nicht unbemerkt erfolgen – es sei denn, dass der Herausgeber des jeweiligen SSL-Zertifikats seinerseits Schlupflöcher zur Manipulation des Authentifizierungsvorgangs eingebaut hat. Sofern die Art und Weise, wie die Schlüsselpaare zufällig erzeugt werden, nicht manipuliert wird oder die Parteien vor einem unbefugten Zugriff geschützt sind, sind SSL- beziehungsweise TLS-Verschlüsselungen weiterhin sicher. Das Gebot der Stunde lautet daher hier nach wie vor, auf eine möglichst starke Verschlüsselung – auch hiesiger Zertifikathersteller – zu setzen und die ordnungsgemäße Umsetzung des Verfahrens zu gewährleisten.

ITB: Allgeier IT Solutions dürfte von der gestiegenen Sensibilität in puncto Security profitieren können. In Ihrem Portfolio gibt es das „Julia MailOffice Gateway“, welches nach Unternehmensangaben „eine sichere E-Mail-Kommunikation ermöglicht. Welche Firmen und Behörden setzen auf Julia MailOffice Gateway, wel-



© SPARTAK - FOTOLIA.COM

Kryptographie – alles eine Frage des Schlüssels.

## Kryptografie

Kryptografie ist die der Informationssicherheit zugrunde liegende Wissenschaft der Verschlüsselung. Das Wort stammt vom griechischen „kryptos", was „versteckt" bedeutet. Die Kryptografie wird am häufigsten mit der Konvertierung von Klartext (normalem Text) in Chiffretext (Verschlüsselung) und wieder zurück (Entschlüsselung) in Verbindung gebracht.

Weil Regierungen vermeiden wollen, dass bestimmte Entitäten im In- und Ausland über Empfangs- und Sendemethoden für versteckte Informationen verfügen, die eine Gefahr für die nationale Sicherheit darstellen können, wurden für die Kryptografie in vielen Ländern Beschränkungen eingeführt – von Beschränkungen über die Nutzung und den Export der Software, bis hin zur öffentlichen Verbreitung mathematischer Konzepte, die für die Entwicklung von Kryptosystemen verwendet werden können. Allerdings hat das Internet die Verbreitung von mächtigen Programmen – und was noch wichtiger ist, der zugrunde liegenden Techniken der Kryptografie – ermöglicht, sodass heutzutage viele der fortschrittlichsten Kryptosysteme öffentlich zugänglich sind.

ches in die Kerbe Kommunikationssicherheit bei sensiblen Daten schlägt?

NITZGEN: Julia MailOffice kommt heute dort zur Anwendung, wo sensibelste Daten ausgetauscht werden: bei Banken, Versicherungen, in der Automobilindustrie oder als zentrale E-Mail-Komponente in der gesamten virtuellen Poststelle des Bundes, so etwa auch bei der Bundesagentur für Arbeit, beim Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesinnenministerium und bei diversen Ermittlungsbehörden des Bundes. Insgesamt kommt die Lösung heute bei 50 Behörden und Ämtern des Bundes zum Einsatz.

ITB: Warum ist die Lösung „spionagesicher"? Und sind nicht auch hier generell Zweifel zulässig, wenn die Geheimdienstwelt von außen betrachtet keine klaren Konturen aufweist und die technischen Möglichkeiten der Schlapphüte im Grunde unklar sind?

NITZGEN: Kryptografische Verfahren stehen und fallen letztlich mit der Sicherheit und Genauigkeit ihrer Umsetzung. Wenn man sich auf symmetrische Verschlüsselungsverfahren beschränken würde, bestünde verfahrensbedingt beim Abfangen des Datenstroms immer die Möglichkeit einer sogenannten Brute-Force-Attacke, bei der möglichst viele potenzielle Lösungen nach dem „Trial & Error"-Prinzip nacheinander durchprobiert werden. Setzt man hingegen ordnungsgemäß implementierte asymmetrische Verschlüsselungsverfahren mit entsprechend langen Schlüsseln ein, ist verfahrensbedingt die Chance hingegen sehr gering, dass durch bloßes Abfangen der Daten die Vertraulichkeit verletzt werden kann. Bei asymmetrischen Krypto-Verfahren kann eine Nachricht ja nicht mit dem eigenen Schlüssel des Schlüsselpaares entschlüsselt werden, sondern nur mit dem privaten Schlüssel des Kommunikationspartners. Allerdings ist auch hier wieder eine gewisse Sorgfaltspflicht erforderlich, um eben jenen privaten Schlüssel beim Empfänger vor dem Zugriff Dritter zuverlässig zu schützen. Denn auch asymmetrische Verschlüsselungsverfahren sind wertlos, wenn der private Schlüssel beim Empfänger für Datenspione leicht zugänglich ist. Hierfür gibt es sowohl konzeptionelle, als auch Hardware-unterstützte Schutzmechanismen, die wir ebenfalls in Julia MailOffice verwenden.

ITB: Wie wird es in den nächsten Monaten und Jahren weitergehen im Hinblick auf die Datenschnorchelei? Die Politik scheint es zwar nicht besonders zu begrüßen, aber den Eindruck, dass sich etwas an der Situation ändern wird, bekommt man auch nicht gerade. Wie ist Ihre Meinung?

NITZGEN: Die Umsetzung geeigneter politischer Maßnahmen ist in großem Maße von der Sensibilität und dem Druck der Wirtschaft gegenüber der Datenschnorchelei abhängig. Viele Unternehmen sind erst durch die jüngsten Enthüllungen sensibilisiert worden, über Compliance und Anforderungen des ▸

Datenschutzgesetzes nachzudenken und geeignete Maßnahmen zum Schutz der eigenen Datenhoheit zu ergreifen. Andere Unternehmen hingegen stehen den Spähprogrammen gelassen gegenüber, da sie über ihre kritischen Unternehmensdaten hinaus vermeintlich nichts zu verbergen haben. Hier wird letztlich die Datensicherheit zugunsten des eigenen Komforts geopfert. Solange also keine klaren gesetzlichen Schutzmechanismen oder politischen Einschränkungen bestehen, ist jedes Unternehmen für sich gefordert, entsprechende Schutzmaßnahmen gegen die Wirtschaftsspionage zu ergreifen – je nachdem, wie wichtig ihnen die Compliance und der Schutz ihrer Daten sind. Ich bin jedoch der Meinung, dass die heutige Gesetzeslage Unternehmen geradezu dazu zwingt, über geeignete Sicherheitsstrukturen nachzudenken, um ihr geistiges Eigentum vor Zugriffen Dritter zu schützen.

ITB: Durch den Patriot Act und über das juristische Vehikel von Geheimgerichtsbeschlüssen können US-Anbieter dazu gezwungen werden, mit Geheimdiensten zu kooperieren. Vor diesem Hintergrund und der Intransparenz scheint sich langsam aber sicher vielerorts so etwas wie ein Generalverdacht gegenüber US-Anbietern zu etablieren. Ist das aus Ihrer Sicht gerechtfertigt, und was bedeutet das für Anbieter mit einem Rechtsstand in Deutschland?

NITZGEN: Ob dies gerechtfertigt ist oder nicht, darüber möge sich jeder selbst ein Bild verschaffen. Tatsache ist jedoch, dass es so etwas wie „gefühlte Sicherheit" zu geben scheint. Und in diesem Zusammenhang haben viele, auch international aufgestellte Kunden bereits in der Vergangenheit europäischen Sicherheitslösungen den Vorzug gegenüber Lösungen von US-Anbietern oder von Anbietern aus anderen Ländern gegeben, denen gegenüber es ähnliche Vorbehalte zu geben scheint. Deswegen glaube ich, dass sich diese Faktoren durchaus positiv für die Vermarktung europäischer Security-Lösungen auswirken werden.

ITB: Denken Sie, dass sich die berechtigte Aufregung, aus welchen Gründen auch immer, wieder legen wird?

NITZGEN: IT-Sicherheit ist kein neues Thema. Es gerät immer dann stärker in den Fokus, wenn es entsprechende Vorfälle gegeben hat. Neu ist dieses Mal der Umfang der Berichterstattung, daher wird uns das Thema noch eine Weile begleiten. Jedoch ist es so, dass Sicherheit und Komfort generell einander diametral gegenüberstehen. Und so wird sich mit der Zeit der Fokus wieder von der Sicherheit weg auf andere Themen verschieben, ohne dass der Bereich „Datensicherheit" vollständig vernachlässigt wird. Zu deren Einhaltung gibt es schließlich entsprechende Verpflichtungen. Bis zum nächsten großen Vorfall, der sich mit Sicherheit ereignen wird.

ITB: Was bedeutet das alles im großen Bild für den IT-Channel? Wie ändert sich das Geschäft und welche Fragen stellen sich dadurch neu?

NITZGEN: Definitiv ist „IT-Sicherheit" das Thema, das bestehende Produkte, Vorgehensweisen und Prozesse in den Unternehmen ein weiteres Mal nachhaltig verändern wird. In diesem Zusammenhang muss sich jeder Unternehmer und IT-Verantwortliche die Fragen stellen: Sind alle meine Kommunikationskanäle sicher? Wo stehe ich möglicherweise in einer Haftung? Welchem Dienstleister kann ich meine Daten anvertrauen? Wie ermittle ich dessen Vertrauenswürdigkeit? Genügen seine Maßnahmen und Prozesse meinen Sicherheitsanforderungen und wie kann ich auch langfristig Cloud-Dienste sicher nutzen? Antworten auf diese Fragen zu finden und schließlich im Sinne der Unternehmensziele umzusetzen, wird in den kommenden beiden Jahren vielerorts sicher eine zentrale Herausforderung sein. □

Mehr zum Julia Mail Office:

web | http://tiny.cc/JuliaMO

Kommentar

## Endlich ein klares Signal aus der Internetwirtschaft

Die Spionage-Affäre hat viele befremdliche Aspekte neben den technischen Hintergründen, also den immensen Möglichkeiten der „Dienste", digitale Daten abzugreifen, und den mannigfachen Möglichkeiten, die sich durch Big-Data-Analysen ergeben. Zu diesen nicht-technischen Absonderlichkeiten zählen für mich beispielsweise die vielen Experten, die auf einmal – nach den Snowden-Enthüllungen – eh schon alles gewusst haben wollen. In der IT-Branche kennt man sich halt aus, wenn man Experte ist. Besonders befremdlich fand ich die Reaktion einiger US-Unternehmen, deren guter Name nach den Enthüllungen im Feuer stand. In der Unternehmenskommunikation sprach man zunächst weiterhin über „die Cloud", als ob es all die Enthüllungen über digitale Überwachung, Geheimgerichte und Wirtschaftsspionage nicht gegeben hätte.

DR. STEFAN RIEDL, Leitender Redakteur IT-BUSINESS

Jetzt gibt es endlich eine gemeinsame Website von AOL, Apple, Facebook, Google, Linkedin, Microsoft, Twitter und Yahoo. Die vom Vertrauensverlust betroffenen US-Internetkonzerne sprechen hier direkt den US-Präsidenten Obama und die Mitglieder des Kongresses an. Sie fordern eine Neuausrichtung der Digitalüberwachung seitens der „Dienste", also vor allem der NSA und des britischen GCHQ. Überwachung soll sich nicht auf die breite Masse, sondern auf konkrete Zielpersonen beschränken. Die Behörden müssten viel strenger überwacht werden. Sie wollen veröffentlichen dürfen, wie oft und warum an Behörden Nutzerinformationen weitergereicht werden müssen. Zudem fordern sie einen „freien Fluss von Informationen" und einen internationalen Rechtsrahmen für Anfragen nach Nutzerdaten.

Ob das Statement etwas bringt, bleibt zweifelhaft, aber überfällig war es allemal.