Wirtschaft in Baden-Württemberg

Position
Seite 26
Rubrik

Kunde All for One Steeb AG

Ausgabe
01.10.2014

Medienart Printmedien
Medientyp Fachpresse
Erscheinungsweise 3 x jährlich
Branche Wirtschaft Allgemein
Bundesland Baden-Württemberg
Nielsengebiet Nielsen IIIb

Auftrags-Nr. 13612
Kunden-Nr. 31272
Thema-Nr. 051.069

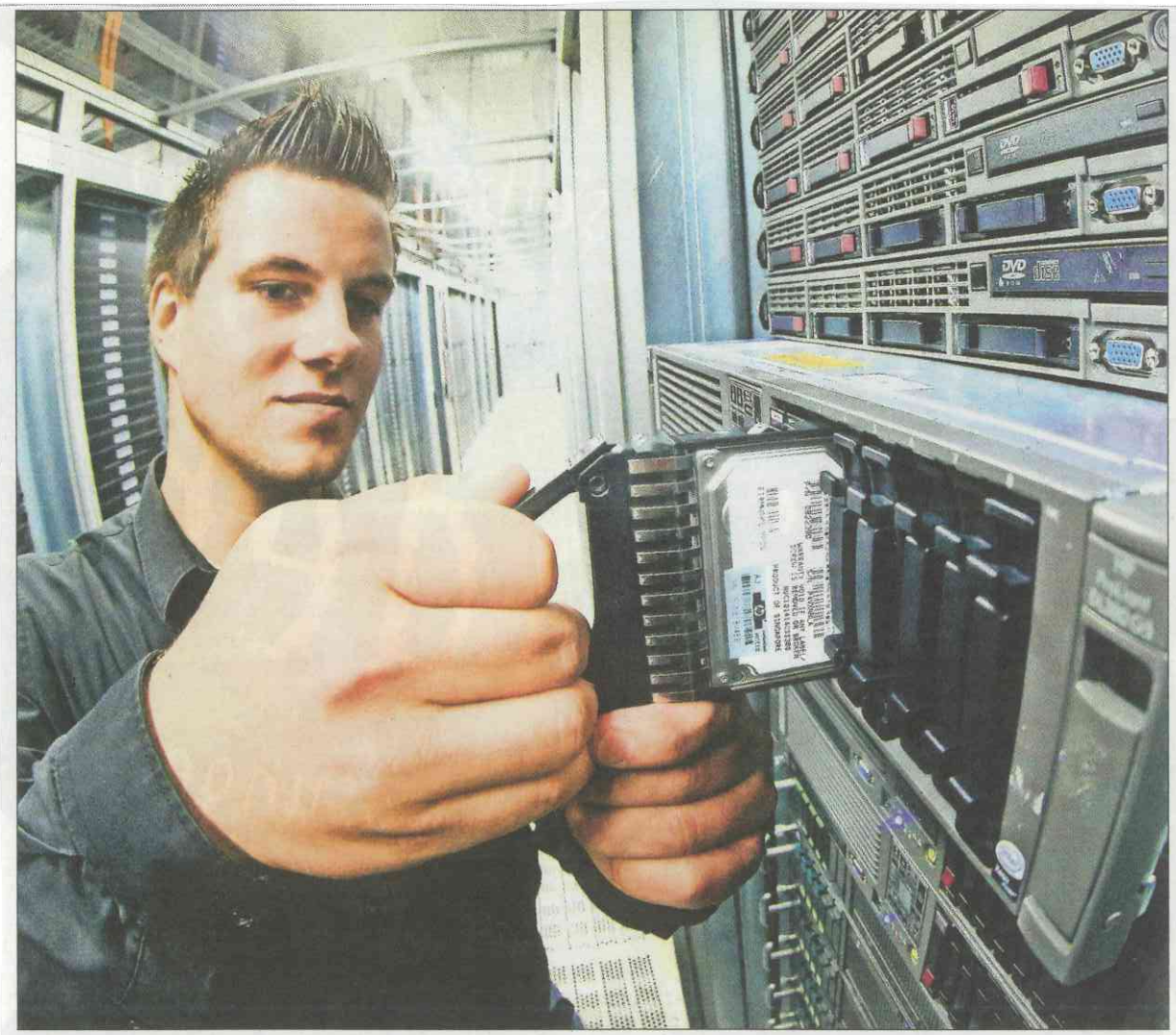
Suchbegriff(e) 1. All for One, -Steeb AG

Verlag Stuttgarter Zeitung Verlagsgesellschaft mbH, 70567 Stuttgart, Plieninger Straße 150, Tel.: 0711 72050, Fax: 0711 7205507
E-Mail: anzeigen@stzw.zgs.de, URL: www.stuttgarter-zeitung.de

Redaktion Wirtschaft in Baden-Württemberg Redaktion, 70567 Stuttgart, Plieninger Straße 150, Tel.: 0711 7205 1211, E-Mail: redaktion@wirtschaft-in-bw.de, URL: www.wirtschaft-in-bw.de

Publikation	Auflage * verkauft	verbreitet	gedruckt	Reichweite** (in Mio.)	Medien-Nr.
Wirtschaft in Baden-Württemberg	k.A.	k.A.	20.800 [1]	k.A. [a]	88052

Quelle
© Cop



Wo sind meine Daten am sichersten? Diese Frage stellen sich Unternehmen nicht erst seit der NSA-Affäre. Foto: dpa

IT-DIENSTLEISTER AUS FILDERSTADT

Unternehmen Die All for One Steeb AG ist ein auf SAP-Programme spezialisierter IT-Dienstleister für mittelständische Unternehmen. Der in Filderstadt-Bernhausen angesiedelte IT-Spezialist beschäftigt rund 1000 Mitarbeiter. Zum Angebot gehören unter anderem Cloud- und Big-Data-Anwendungen.

Kunden All for One Steeb betreut nach eigenen Angaben mehr als 2000 Kunden aus den Branchen Maschinen- und Anlagenbau, Autozulieferer, Konsumgüter, Großhandel und Dienstleistungen. Schwerpunkt ist dabei der deutschsprachige Raum, allerdings gibt es Geschäftsverbindungen in insgesamt 54 Länder. Im Geschäftsjahr 2012/13 erzielte All for One Steeb einen Umsatz in Höhe von 186 Millionen Euro. *age*

Mitarbeiter sind der größte Risikofaktor

IT-Strategie Die Datensicherheitsdebatte läuft in die falsche Richtung, sagt der Chef von All for One Steeb. Sein Fazit: Systemausfälle können gefährlicher sein als Hacker und Spione. *Von Andreas Geldner*

Datensicherheit? Ist das nicht eine dramatische Geschichte von Hackern, Spionen und Geheimdiensten? Wenn Lars Landwehrkamp, Vorstandssprecher des IT-Dienstleister All for One Steeb in Filderstadt-Bernhausen, von den Problemen erzählt, mit denen seine Kunden zu tun haben, dann tauchen zunächst einmal weder die NSA noch chinesische Plagiatoren auf. Stattdessen Baggerbisse, überschwemmte Keller oder schlampige Mitarbeiter. „Die wichtigste Herausforderung in der IT-Sicherheit ist es, erst einmal zu verhindern, dass ihr IT-System ausfällt", sagt Landwehrkamp, dessen Unternehmen sich auf Kunden des Softwareriesen SAP spezialisiert hat. Hier sei das Schadenspotenzial am größten.

Wenn eine Online-Verkaufsplattform in die Knie geht oder der Mailserver für die interne Kommunikation ausfällt, kann das schlimmstenfalls den wirtschaftlichen Ruin bedeuten. Und die Gründe dafür sind zumeist kein Fall für einen Spionagethriller, sondern ganz banal: Es sind die fehlenden Reservebatterien, wenn etwa ein Bagger bei Bauarbeiten eine Stromleitung kappt. Es ist die fehlende Absicherung der Server gegen Brand oder Wassereinbruch. Und es ist immer wieder die Schwachstelle Mensch.

Ein häufiges Sicherheitsrisiko ist der Mitarbeiter, dem das halbe Dutzend Passwörter, mit dem er sich im Betrieb herumschlagen muss, zu viel wird – und der sie deshalb auf Klebezettel schreibt, die er neben den Computer heftet. Es ist der Kollege, der sein Dienst-Smartphone am Flughafen liegen lässt. Oder es ist der im Zorn aus dem Unternehmen geschiedene Vertriebsmitarbeiter, der seine Kundendaten zur Konkurrenz mitnimmt. Sicherheit sei nicht nur eine Frage der Technologie. „Jede Sicherheitsphilosophie, die den Faktor Mensch außen vor lässt, wird scheitern", sagt Landwehrkamp. „Die Trickkiste, in die Anwender greifen, um lästige Schutzmechanismen zu unterlaufen, ist nahezu unergründlich." Wer die Zahl der Passwörter in der Hand eines Mitarbeiters von sechs auf eines reduziert, weil verschiedene IT-Anwendungen besser gebündelt werden, tut deshalb manchmal mehr für die Sicherheit, als wenn er nach einer komplexen Verschlüsselungstechnologie für die Firmenmails sucht.

Für Landwehrkamp ist es an der Zeit, die in Deutschland intensiv geführte Debatte um die Datensicherheit, die sich auf die großen anonymen Bedrohungen fokussiert, vom Kopf auf die Füße zu stellen. Die Diskussion sei teilweise auf die falschen Themen fixiert. „Ich wüsste von keinem unserer mittelständischen Kunden, dass er jemals direkt von Wirtschaftsspionage im klassischen Sinn betroffen gewesen wäre", sagt er. Es sei auch eine verzerrte Wahrnehmung der Wirklichkeit, wenn behauptet werde, dass erst die NSA-Enthüllungen die deutsche Wirtschaft wachgerüttelt hätten. Viele Mittelständler stünden beim Thema IT-Sicherheit schon lange unter dem Druck der Großunternehmen, die ihre Kunden sind. Große Konzerne verlangen immer öfter von jedem Glied ihrer Lieferkette, dass dort dieselben zertifizierten Sicherheitsmaßstäbe gelten wie im eigenen Haus.

Dass der Begriff Datensicherheit made in Germany nun die Schlagzeilen beherrsche, habe auch eine psychologische Komponente. „Der verlässliche rechtliche Rahmen hierzulande und die Sicherheitskultur haben bei den Kunden schon immer eine Rolle gespielt." Sicherheit sei nämlich keine Extrakomponente, die man sich nachträglich zur IT dazukaufen könne. „Sie müssen schon ganz zu Anfang eine Risikoanalyse machen: Kann ich es etwa verkraften, wenn meine Internetseite einen halben Tag ausfällt? Diese Abschätzung sieht für einen Anlagenbauer anders aus als für den Betreiber eines Online-Shops", so Landwehrkamp. Schon beim Aufbau der IT-Architektur müsse das Thema Sicherheit mit bedacht werden – genau aufgeschlüsselt danach, welches Schutzniveau man sich in welchem Bereich leisten will. Sicherheit ist nicht die Frage einzelner Komponenten, sondern der ganzen IT-Architektur.

Dass das Thema Datensicherheit bei den Firmen immer mehr in den Mittelpunkt

Fünf Mythen über Datensicherheit

1 Die NSA-Affäre hat einen Run auf die IT-Sicherheit provoziert
Diesen Nachfrageschub gibt es – aber schon seit Jahren. Die Abhängigkeit der Firmen von einer 100-prozentig funktionierenden, immer komplexeren IT wächst. Das ist die entscheidende Antriebskraft, die von Schlagzeilen unabhängig ist.

2 Firmen haben mehr Angst vor Wirtschaftsspionage
Die Bedrohung durch Spionage und Datenkriminalität ist nur ein kleiner Teil der Gefährdungen, denen ein IT-System unterliegt. Viel größer ist das Risiko von Datenverlust und Funktionsstörungen.

rückt, ist nicht das Resultat einer Spionageaffäre, sondern der Kulminationspunkt vieler schon seit Jahren zu beobachtenden technischen Trends. „Es gibt niemanden mehr, der Daten nur für sich im eigenen Haus verarbeitet – selbst der Handwerker, der einst noch seine selbst geschriebenen Rechnungen per Fax verschickt hat, ist heute meist bereits online unterwegs." Auch der kleinste Mittelständler sei heute Teil einer weltweiten Lieferkette und tausche seine Daten rund um den Globus mit Lieferanten und Kunden aus – und jeder Datenaustausch sei ein potenzielles Leck.

Wo Daten früher gesichert, aber auch ungenutzt in der eigenen IT-Zentrale gelagert waren, sind sie von immer mehr Stellen abrufbar und ständig in Bewegung. Statt am stationären PC hinter der Büro-Firewall operieren Mitarbeiter mit einer Vielfalt von Mobilgeräten, auf die jederzeit ein Zugriff möglich sein muss, sollten sie etwa verloren gehen. Wer bekommt welche Berechtigung und welches Passwort für welchen Teil einer intern und extern immer dichter vernetzten IT? Wie ist der Ablauf geregelt, wenn ein Mitarbeiter die Firma verlässt? Und wer schaltet die Geräte wieder frei, wenn eines der immer komplizierteren Passwörter unterwegs vergessen wird?

Unter dem Stichwort Industrie 4.0 erreicht der Datenstrom inzwischen auch die Produktion. „Es hilft nichts, wenn sie dem Mitarbeiter an der Maschine sagen, dass er ein 13-stelliges Passwort eingeben muss, wenn das mit seinen dicken Handschuhen nicht funktioniert", sagt Landwehrkamp. „Die Komplexität des Themas Sicherheit wird immer noch unterschätzt", fügt er hinzu. „Das Thema kommt nicht erst auf sie zu, wenn sie sich dazu entschieden haben, die Internet-Cloud zu nutzen." Im Gegenteil: Cloud-Anbieter hätten in der Regel mehr Sicherheitsexpertise als die eigene IT-Abteilung. „In den USA ist die Angst vor der Cloud überhaupt kein Thema – das ist wirklich ein sehr westeuropäisches Problem."

Auch Big Data, das vermeintlich die Risiken zu mehren scheine, sieht Landwehrkamp eher als Teil der Lösung. Mit geballter Rechenkraft sei es einfacher, den Datenverkehr live zu überwachen und etwa ungewöhnliche Muster herauszupicken – die ein Indiz dafür sein können, dass etwas nicht stimmt. Das muss ein IT-Dienstleister wie All for One Steeb natürlich auch aus eigenem Interesse so sehen. Dort hofft man, dass Datensicherheit auch im Mittelstand verstärkt zur Angelegenheit externer Anbieter wird, die vom Vertrieb bis zur Produktion, vom E-Mail-Server bis zum Firmennetz und von den Datenspeichern bis zu den Übertragungswegen die gesamte IT im Blick haben.

„Bei bloßen punktuellen Schutzversuchen sind Fehlschläge programmiert", sagt Landwehrkamp. Nur ein Spezialist sei in der Lage, die Sicherheitsarchitektur auf dem neuesten Stand zu halten und neue Einfallstore sogleich zu schließen. „Für ein normales Unternehmen ist es zum Beispiel zu teuer, einmal einen richtigen Hackerangriff simulieren zu lassen."

3 Sicherheitsmaßnahmen werden immer komplexer

Für ein gesamtes IT-System ist diese Aussage wohl richtig. Aus Sicht der Mitarbeiter sollte aber das Gegenteil der Fall sein: sie brauchen Lösungen, die komfortabel und alltagstauglich sind. Überzogene Sicherheitsanforderungen schrecken ab – und verführen dazu, sie bei jeder Gelegenheit zu unterlaufen.

4 Cloud-Computing und Big Data schaffen weitere Bedrohungen

Niemand ist eine Insel – das gilt auch für Firmen, die ihre Daten in den eigenen Händen halten wollen. Im Zeitalter des Internet sind sie so oder so nicht mehr abzuschotten. Auch Big Data ist beim Thema Sicherheit ein zweischneidiges Schwert. Es erhöht den Datendurchsatz und erfordert damit per se erhöhte Sicherheitsvorkehrungen, gibt Unternehmen aber auch neue Diagnoseinstrumente zum Aufspüren von Sicherheitslücken in die Hand.

5 Europa ist beim Thema IT-Sicherheit eine Bastion

Der transatlantische Graben mag tief sein. Doch auch in der EU gibt es weder eine einheitliche Sicherheitskultur noch einen halbwegs einheitlichen Rechtsrahmen. Auch Internetkriminalität wird nicht zentral verfolgt. Ein Daten-Binnenmarkt ist noch in weiter Ferne – auch wenn die Datenströme keine Landesgrenzen kennen.