SAP im Feuer der Kritik – Anwendervereinigung warnt vor Clouddiensten

Von Joachim Jakobs

Der Hamburger Beauftragte für den Datenschutz Johannes Caspar und Marco Lenck, Vorstandsvorsitzender der Deutschsprachigen SAP-Anwendergruppe (DSAG) e. V kritisieren den Softwarekonzern SAP: „Die mangelnde Transparenz in Fragen der Zusammenarbeit auf dem Gebiet der inneren Sicherheit überrascht und ist beunruhigend“, so Caspar. Zuvor hatte sich Gordon Mühl, Chief Technical Officer (CTO) für Security von SAP im Interview mit der Fachzeitschrift „Deutsche Polizei“ wenig auskunftsfreudig zur Zusammenarbeit seines Arbeitgebers mit US-Geheimdiensten und deren Firmen präsentiert: „Bitte haben Sie Verständnis dafür, dass wir uns über Geschäftsbeziehungen nicht äußern.“

Den Gefallen tut ihm Datenschützer Caspar jedenfalls nicht – er hat kein Verständnis für Mühl's Schweigen: „Immerhin handelt es sich bei SAP um ein deutsches Unternehmen das zwar global agiert, bei dem man aber auch erwartet, dass es dem digital-technologischen US-Überwachungskomplex mit einer gewissen Distanz gegenübersteht.“ Überlegungen, sich künftig stärker auf nationale oder europäische Lösungen bei der Datenverarbeitung zu stützen, unterstellten unausgesprochen, dass der Datenschutz und die Datensicherheit hier besser aufgehoben seien. „Vor diesem Hintergrund stärkt es nicht das Vertrauen in diese Grundannahme, wenn auf Fragen nach der Verbindung zu US-Sicherheitsbehörden oder deren Dienstleistern mit dem Hinweis auf Kunden- und Geschäftsbeziehungen ausgewichen wird“, so Caspar.

Ins gleiche Horn bläst Marco Lenck, Vorstandsvorsitzender der Deutschsprachigen SAP-Anwendergruppe (DSAG) e. V: Nachdem „ein US-Cloud-Anbieter“ (nämlich Microsoft, Anm. d. Autors) – von einem Gericht verpflichtet worden sei, Daten an US-Behörden herauszugeben, obwohl sich der Server nicht in den USA befände, herrscht nach Lencks Beobachtung „große Unsicherheit“: „Kunden amerikanischer Cloud-Dienste müssen ständig damit rechnen, dass US-Behörden an ihre Daten und damit auch an unternehmenskritische Informationen gelangen.“ Da SAP auch in den USA präsent sei, könne die Herausgabe der Daten ebenfalls verlangt werden.

Gordon Mühl hält das für „reine Spekulation“ und bittet „auch hier“ „um Verständnis, dass wir uns hierzu ebenfalls nicht äußern“.

Das kann Marco Lenck nicht beirren – er warnt: „Kunden sollten sich daher genau überlegen, welche Daten sie in die Cloud auslagern. Ihre Pflicht ist es, gewissenhaft mit ihrer 'intellectual property' umzugehen und Sorge dafür zu tragen, dass

unternehmenskritische Daten gar nicht erst in einer Cloud landen."

Wenigstens kommt Sachar Paulus, Gordon Mühls Amtsvorgänger, seinem früheren Arbeitgeber zu Hilfe: „Im Rahmen der Zurverfügungsstellung von Bibliotheken zur Verschlüsselung der Kommunikation zwischen SAP Servern bei Kunden hatte ich in meiner Rolle als Chief Security Officer der SAP mehrfach mit Anfragen der NSA zu tun, die darauf drängten, Zugang zu den Sourcen zu bekommen und darauf hinwiesen, dass sie befugt seien, dort eine Möglichkeit zu bekommen, die Verschlüsselung „zu umgehen". Die SAP musste dem aber aufgrund der gewählten Export-Strategie für die Krypto-Bibliotheken nicht nachkommen."

SAP kooperiert auf mehreren Ebenen mit Spionage-Firmen und -Diensten; 2011 gab SAP eine „globale Reseller-Vereinbarung" mit Palantir bekannt — damals textete die SAP-Pressestelle: „In Zusammenarbeit mit Palantir Technologies wird SAP eine Softwarelösung für Behörden anbieten, die sie bei der Wahrnehmung ihrer Sicherheitsaufgaben unterstützt." Das Ziel sollte es sein, die Palantir-Plattform für Informationsanalyse unter dem Namen "SAP Intelligence Analysis for Public Sector application by Palantir" an den öffentlichen Dienst zu verkaufen. Palantir genießt unter Geheimdienstlern einen guten Ruf wegen seiner Fähigkeit, große Datenmengen aus unterschiedlichen Quellen in anschauliche Bilder und Diagramme umzusetzen. So soll Palantir nicht nur dabei geholfen haben, Osama bin Laden, den mutmaßlichen Initiator des Anschlags auf das New Yorker World Trade Center, ausfindig zu machen.

Palantir wird außerdem vorgeworfen, 2011 an der Entwicklung einer „Angriffsstrategie" gegen die Enthüllungsplattform Wikileaks beteiligt gewesen sein. Nach Informationen des Internetmagazins „The Tech Herald" soll zu diesem Plan nicht nur gehört haben, den Journalisten Glenn Greenwald, den heutigen Intimus von Edward Snowden unter Druck zu setzen, sondern auch Cyberattacken, Desinformation „und andere proaktive Maßnahmen". Nachdem dieser Plan öffentlich wurde, hat sich Palantir aus dem Projekt zurückgezogen und bei Greenwald entschuldigt.

Das Wirtschaftsmagazin Forbes hat eine präzise Wahrnehmung von dem Partner der Walldorfer — bei Palantir handele es sich um eine vom Geheimdienst „CIA finanzierte Datamining-Dampfwalze". Tatsächlich hat die CIA über ihr Risikokapitalunternehmen 'IN-Q-TEL' 2005 erstmals in Palantir investiert. Doch auch SAP scheint einige Fähigkeiten in diesem Bereich entwickelt zu haben. Ex-SAP'ler Sachar Paulus bestätigt die Existenz einer „separaten SAP Company für den Support in den USA" und betont: „Ich halte es für sehr wahrscheinlich, dass SAP Kooperationen mit Verteidigungsorganisationen unterhält, um neue Lösungen auf der Basis von Big Data Analytics zu entwickeln und zum Einsatz zu

bringen.“

Bei der von Paulus angesprochenen „separaten SAP Company“ handelt es sich womöglich um die 'SAP National Security Services' (SAP NS2), ein Unternehmen, das nach eigener Darstellung ein „vollständiges Angebot an Weltklasse-Unternehmenslösungen“ von SAP vorhält. Spezielle Sicherheits- und Betreuungsdienste sollen dazu dienen, der „einmaligen Aufgabe der nationalen Sicherheit der Vereinigten Staaten zu entsprechen.“ Von der Sicherheit Deutschlands ist dabei keine Rede. Um die nationale Sicherheit der USA zu gewährleisten, hat SAP gleich mehrere Gremien bei der SAP NS2 eingerichtet: Ein 'Management Team', ein 'Board of Directors' und ein 'Advisory Board'. Alle sind gespickt mit früheren Geheimdienstlern.

Zu dieser Tochtergesellschaft äußert sich Gordon Mühl so: „Auch dazu werden wir keine Informationen verbreiten. Was die NS2 selbst angeht: Sie ist eine Tochterfirma der SAP USA und ist aufgesetzt worden, damit Software im öffentlichen Bereich verkauft werden kann.“

Um erfolgreich in den USA Geschäfte machen zu können, spannt die SAP Tochter auch Mike Hayden, den früheren Direktor der Geheimdienste CIA und NSA, für Vorträge ein.

General Mike Hayden
Former Director, CIA and NSA

SAP sonnt sich im vermeintlichen Glanz des früheren Geheimdienstlers Mike Hayden. Bild: SAPNS2.

Hayden bestätigte im vergangenen Mai: „Wir töten auf der Basis von Metadaten“. So können etwa die Positionsdaten eines Handys genutzt werden, um einen vermeintlichen Terroristen in Afgahnistan zu identifizieren und anschließend zu töten. Kritiker weisen allerdings auf die Unzuverlässigkeit der Metadaten hin. Und selbst wenn die Daten korrekt sind, ist es notwendig, dass der mutmaßliche Terrorist sein Handy nicht aus der Hand gibt.

Nachfrage an Sachar Paulus: „Werden mit den von Ihnen genannten 'neuen Lösungen auf der Basis von Big Data Analytics' Drohnen in in Afghanistan gesteuert?“ Antwort Paulus: „Möglicherweise“.

Auch das ist einmal mehr vor dem Hintergrund des Interviews mit der Deutschen Polizei interessant. So liegt dem Konzern auch die Sicherheit seiner Kunden am Herzen, wenn diese mobil auf ihre SAP-Installationen im Unternehmen zugreifen. Gordon Mühl weist darauf hin, dass es riskant sein könnte, etwa vom Flughafen SAP-Systeme aufzurufen, „wo die halbe Konkurrenz zuschaut“. Auf die Frage, ob

SAP Standortinformationen des Nutzers verwendet, um zu entscheiden, ob der Nutzer Zugang zu SAP erhält oder nicht, antwortet Gordon Mühl: „Eine kontextsensitive Zugriffsberechtigung haben wir deshalb nicht implementiert, weil die Angabe, wo sich das Handy aktuell befindet, sehr leicht zu fälschen ist. Sollte die Information über den Aufenthalt eines Handys irgendwann tatsächlich verlässlich sein, könnten wir das für unsere Kunden einbauen“.

Es wäre wichtig, dass sich SAP zu den Dienstleistungen äußert, die sie weltweit anbieten. So scheint es immerhin denkbar, dass SAP Software von den Militärs – womöglich im pfälzischen Ramstein – genutzt wird, um Menschen zu töten. Wenn das der Fall wäre, würde das bedeuten, dass SAP aus Sicherheitsgründen keine ortsbezogenen Informationen nutzen will, um über den Zugang zu seinen Systemen zu entscheiden. Für das Töten von Menschen wäre das Sicherheitsniveau aber ausreichend.

Das vollständige Interview mit Gordon Mühl ist ab 1.3.2015 unter gdp.de nachzulesen.