Hans-Peter Bauer (links) im Gespräch mit Dr. Dietmar Neugebauer Fotos: Wolfgang Taschner

Security ist ein wichtiger Faktor in den Unternehmen. Dr. Dietmar Neugebauer, Vorstandsvorsitzender der DOAG, und Wolfgang Taschner, Chefredakteur der DOAG *News*, sprachen darüber mit Hans-Peter Bauer, Vice President Central und Eastern Europe der McAfee GmbH.

„Sicherheit fängt bei der Bewusstseinsbildung an …“

Welche Unternehmensziele hat McAfee?
Bauer: McAfee ist weltweit der größte Anbieter, der sich rein auf IT-Sicherheit spezialisiert hat. Wir liefern unseren Kunden präventive, praxiserprobte Sicherheits-Lösungen und -Dienstleistungen, um sie vor Angriffen zu schützen. Unterstützt durch die einzigartige Global-Threat-Intelligence-Technologie helfen wir sowohl Privatnutzern als auch Organisationen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern.

Bisher ist McAfee nicht als Anbieter von Sicherheitslösungen für Datenbanken erkennbar gewesen. Ihr Unternehmen hat sich jedoch im letzten Jahr in diesem Bereich durch Zukäufe verstärkt. Wo sehen Sie Chancen, diese Sichtbarkeit zu verbessern?
Bauer: Durch die Sentrigo-Akquisition sind Sicherheitslösungen für Datenbanken ein ganz heißes Thema für uns. Wir haben frühzeitig erkannt, dass IT-Sicherheit sehr viel mit Schutz und Sicherheit der Daten zu tun hat. Sentrigo war schon zuvor Partner unserer Security Innovation Alliance, in deren Rahmen wir auch Datacenter absichern.

Gibt es aus Ihrer Sicht ein Patentrezept, um globale Sicherheit in einem Unternehmen einzuführen?
Bauer: Unsere Strategie beinhaltet einen globalen Cloud-basierenden Service, der so aussieht, dass wir über sogenannte „Fingerprints“ weltweit alle Sicherheitsvorfälle in Form von neutralisierten Hash-Codes unserer eigenen Sensoren sowie der unserer Kunden – sofern diese dem zustimmen und den Service aktiviert haben – einsammeln und in unserer Cloud (GTI) ablegen. Diesen Service stellen wir unseren Kunden zur Verfügung und deren Systeme können dort eine CGut“- oder „Schlecht“-Antwort in fast „Real-Time“ beziehen.

Worin sehen Sie die größte Herausforderung bei der Umsetzung einer unternehmensweiten Security-Policy?
Bauer: Ich glaube, dass Security in vielen Unternehmen sowohl technisch als auch organisatorisch sehr stark fragmentiert ist. Da gibt es zum Beispiel einen Chief Security Officer, der aber mit den Netzwerk-Leuten nichts zu tun hat. Zudem sollte dieser Chief Security Officer direkt dem CIO unterstellt sein und Einfluss auf alle Abteilungen innerhalb der IT haben. Außerdem haben die Unternehmen es mittlerweile weniger mit Angriffen zu tun, die Daten zerstören, sondern vielmehr mit Vorfällen, bei denen Daten abgezogen werden.

Wo sollte der Bereich „Sicherheit“ organisatorisch im Unternehmen angesiedelt sein?
Bauer: In jedem Fall direkt unterhalb des CIOs. Nur so besteht die Möglichkeit, Sicherheit von den Datenbanken über die Netzwerke bis hin zur Produktion zu gewährleisten.

Wo sollte nach Ihrer Meinung ein mittelständisches Unternehmen mit der Sicherheit anfangen?
Bauer: Das fängt bei der Bewusstseinsbildung an. Man muss seine gesamte Infrastruktur kennen und deren Schwachstellen analysieren. Dann gilt es, alle Sicherheitssysteme zu synchronisieren und aufeinander abzustimmen. Die Gesamtsicherheit resultiert immer aus der Zusammenarbeit aller Teilsysteme. Das Maturity-Modell bietet hier sehr gute Checklisten für ein Unternehmen.

Was würden Sie einem Sicherheitsbeauftragen in einem Unternehmen raten?
Bauer: Er sollte auf keinen Fall ein fragmentiertes Sicherheitssystem betreiben, denn das ist kein zukunftsträchtiger Weg. Er sollte hingegen mit renommierten Sicherheitsunternehmen zusammenarbeiten. Darüber hinaus gibt es einige Beratungsfirmen, die ihm dabei helfen, ein Sicherheitskonzept zu definieren. In jedem Fall sollte er sich eine integrierte Sicherheitslösung anschaffen, anstatt die Systemintegration selbst zu erledigen.

Wie lassen sich Aufwand und Kosten für die Sicherheit im Verhältnis zum Nutzen im Rahmen halten?
Bauer: Das hängt stark davon ab, in welchem Bereich sich ein Unternehmen bewegt. Die wenigsten Kosten fallen an, wenn man nur reaktiv beispielsweise eine Firewall einsetzt. Will man hingegen proaktive Sicherheit – also einen fragmentierten Ansatz – betreiben, fallen darüber hinaus auch Personalkosten und weitere Systeme an, sodass das Budget bei knapp zehn Prozent der gesamten IT-Kosten liegt. Im optimierten, integrierten Level kann man den höchsten Sicherheitgrad erreichen und die Kosten sollten sich maximal zwischen vier bis sechs Prozent des IT-Budgets bewegen.

Wie stellt man in der Praxis sicher, dass die User nur die Daten sehen, die sie auch sehen sollen?
Bauer: Dafür gibt es entsprechende Systeme. Bei uns ist jeder User in seiner Rolle einem bestimmten Profil zugeordnet. Wird nun im Unternehmen ein neues System wie beispielsweise das iPhone eingeführt, übernimmt unser Enterprise-Mobility-Management-System dieses Profil und gewährt jedem Benutzer seine ihm entsprechenden Rechte.

Wann beziehungsweise wie ist ein Monitoring von auffälligen Zugriffen sinnvoll?
Bauer: Ein Monitoring von Datenbanken ist zu jeder Zeit wichtig. Dieses Monitoring hilft dem Unternehmen, sich selbst zu definieren, denn niemand hat heute schon die Datenstrukturen, um Missbrauch zu verhindern. Ein weiteres Problem ist die Vielzahl der Datenbanken. Es nutzt nichts, wenn man seine zentrale Datenbank

Zur Person: Hans-Peter Bauer

Hans-Peter Bauer ist Vice President Central und Eastern Europe bei McAfee. Er wechselte zum 1. Januar 2008 von Juniper Networks, wo er zuletzt als Vice President für das Enterprise-Geschäft in EMEA verantwortlich war. Er bringt eine mehr als 20-jährige Erfahrung in der Computer- und Informationstechnologie-Branche in seine Position ein.

Hans-Peter Bauer begann seine Laufbahn bei der Siemens AG in der Beratung und dem Vertrieb für Daten und Informationssysteme. 1988 wechselte er zu Digital Equipment (DEC), wo er in verschiedenen Management-Positionen im nationalen und internationalen Vertrieb tätig war. 1993 stieg er in das Consulting und Systemintegrations-Business bei der Computer Sciences Corporation (CSC) ein. Dort war Hans-Peter Bauer als Mitglied der Geschäftsleitung verantwortlich für den Geschäftsbereich Kommunikation und Medien in Central und Eastern Europe. 1997 kam Hans-Peter Bauer zu Lotus als Managing Director für Lotus Consulting Central und Eastern Europe und übernahm 1999 die Gesamtverantwortung als Geschäftsführer und General Manager der Lotus Development Deutschland, Österreich und der Schweiz. Nach erfolgreich durchgeführter Integration von Lotus in die IBM war er als Director und zuletzt als Vicepresident Software Group Central Europe der IBM Deutschland GmbH für das gesamte Software-Geschäft im deutschsprachigen Europa verantwortlich. Ab August 2002 übernahm Hans-Peter Bauer als Vicepresident und General Manager die Verantwortung für Symantec Central and Eastern Europe. Nach Abschluss der Akquisition von Veritas durch Symantec wechselte er im April 2005 zu Macromedia als Geschäftsführer für Deutschland, die Schweiz und Österreich. Mit der Übernahme von Macromedia durch Adobe wurde Hans-Peter Bauer zum Managing Director and General Manager Adobe North European Region befördert. Hier verantwortete er das gesamte Produkt- und Lösungsportfolio in den Ländern UK, Irland und Skandinavien.

schützt und sich nicht um die Kopien der Daten auf diversen PCs oder Abteilungsservern kümmert.

Wie sollte man mit Vorfällen im Unternehmen umgehen?
Bauer: Totschweigen ist die schlechteste Lösung. Für viele Unternehmen ist es sicherlich schwierig, mit Vorfällen offen umzugehen, um das Vertrauen der Partner nicht zu verlieren. Ich empfehle, zunächst forensisch vorzugehen, um den exakten Hergang und den Schaden sowie die damit verbundenen Auswirkungen festzustellen. Daraus lassen sich dann Maßnahmen ableiten, um sich zukünftig davor zu schützen. Jeder Angriff ist immer eine Lehre dafür, wie man sich entsprechend schützen kann.

Jede Sicherheitsmaßnahme behindert meist in irgendeiner Form den operativen Betrieb. Wie stellt man sicher, dass die beschlossenen Vorhaben auch in den Fachabteilungen wie geplant umgesetzt werden?
Bauer: Dem stimme ich nicht zu. Man kann heute Sicherheit einführen, ohne die Kreativität einzuschränken. Es gilt lediglich, eine gewisse Disziplin zu wahren und jedem Benutzer nur die Rechte zu gewähren, die er für die Ausführung seiner Arbeit benötigt.

Wie lässt sich Sicherheit messen?
Bauer: Eine entsprechende Scorecard muss jedes Unternehmen für sich definieren. Sicherheit bedeutet für mich Risiko-Management. Das Unternehmen muss seine Assets kennen und die jeweiligen Risiken entsprechend bewerten.

Zu viele Sicherheitsmaßnahmen führen zu Misstrauen der Mitarbeiter gegenüber dem Unternehmen. Wie geht man damit um?
Bauer: Es gilt immer, die optimale Sicherheit zu gestalten. Zu viele Sicherheitsmaßnahmen bringen keinem Unternehmen etwas.

Sicherheit ist immer eine Reaktion auf Bedrohungen. Wird nach Ihrer Ansicht die Lücke zwischen Bedrohungen und Schutzmaßnahmen kleiner oder größer?
Bauer: Wir stellen fest, dass die Komplexität der Bedrohungslage ansteigt. Der Wunsch, dass moderne Software immer fehlerfreier wird, tritt leider nicht ein. Auf der anderen Seite reicht die Bedrohung durch Rootkits bis in den Bootsektor der Rechner, sodass ein einfacher Neustart nicht mehr weiterhilft.

Was muss Oracle tun, um Unternehmen bei der notwendigen Sicherheit zu unterstützen?
Bauer: Ich wünsche mir von Oracle mehr Offenheit. Wir kommen nur bedingt an alle Informationen heran, um die Sicherheitsfunktionalität zu erfüllen. Darüber hinaus würden wir auch gerne mit Oracle zusammen ein Sicherheitsmodul entwickeln, wie wir es mit SAP bereits für NetWeaver getan haben.

Wie sehen Sie die Rolle der DOAG in diesem Bereich?
Bauer: Die DOAG kann aufgrund ihrer enormen Reichweite zur Bewusstseinsbildung beitragen. Sie erreicht auch Datenbank-Beauftragte, die üblicherweise sehr weit vom Chief Security Officer entfernt sind.