

Statement of the Month – August 2008

Datensicherheit

Mit Sicherheit (k)ein gutes Gefühl

Irgendwie war früher doch alles besser. Heute gibt man seine Daten vertrauensselig beim Einkaufen an, freut sich über die rasche Zusendung der erworbenen Ware und denkt, es sei alles wie vor 20 Jahren, nur schneller und praktischer. Aber das dicke Ende kommt schon wenig später. Auf einmal scheinen die persönlichen Daten die Runde gemacht zu haben – viel schneller als einem lieb ist. Datenlücken haben immer verheerende Folgen, nicht nur für die Kunden, die plötzlich von ganz anderer Stelle Post bekommen, sondern auch für die Unternehmen, wo das Leck entstanden ist. Finanzielle Schäden sind da noch vergleichsweise harmlos. Marina Walser, Director Identity & Security Management bei Novell Central Europe, untersucht, wie Datenlecks zustande kommen und was Unternehmen gegen die wachsende Verunsicherung auf Kundenseite tun können:

In den meisten Fällen liegt die Schuld nicht mal beim Anbieter – viele Kunden geben ihre persönlichen Daten allzu freiwillig an, ohne über die Folgen nachzudenken. Gerade im Internet macht man Angaben zur Person und zum Kontostand leichter und oftmals gedankenlos. Während die meisten Kunden bei einer persönlichen Befragung von Angesicht zu Angesicht zum Beispiel Auskünfte zum Gehalt oder ähnlich vertrauliche Informationen eher zurückhalten, scheint es im Internet diese Barriere nicht zu geben. Das World Wide Web ist anonym, so die Annahme - dem Inhalt lässt sich kein Gesicht zuordnen. Noch nicht, muss man vielleicht sagen. Aber durch immer mehr „Pannen“ oder bewusste Datenweitergabe werden die Nutzer hellhörig. Welchem Unternehmen kann man wirklich vertrauen, wer nutzt die Daten tatsächlich nur für die eigene Verwendung? Und wie sicher sind die Internetleitungen wirklich? Im Prinzip ist ja alles schon mal „gehackt“ worden, so die breite Meinung. Die Verunsicherung ist groß.

An Möglichkeiten, die Datenweitergabe einzuschränken, wird derzeit sowohl von proprietären Herstellern als auch im Open Source-Bereich mit Hochdruck gearbeitet. Beim Bandit-Projekt der Open Source-Community beispielsweise steht der Nutzer im Vordergrund, der selbst all seine Informationen sowie den Zugriff darauf verwalten und kontrollieren kann. Dies soll für eine höhere Sicherheit sorgen, da die Anwender nur die Informationen preisgeben, die für eine Transaktion nötig sind und somit sensible Informationen nicht an Webseiten übermitteln, die auf diese nicht angewiesen sind.

Und auch wenn sich ein Nutzer entschieden hat, einem Unternehmen sein Vertrauen zu schenken und seine Daten mitzuteilen, sollte das eigentlich noch lange nicht heißen, dass diese automatisch vervielfältigt werden. Aber selbst wenn das Unternehmen die Daten seiner Kunden im besten Wissen und Gewissen sowie mit den besten Absichten speichert, um dem Kunden seine Einkäufe zukommen zu lassen und die Kosten abzurechnen, ist das keine Garantie. Die Daten sind zwar in einem CRM-System im Unternehmen hinterlegt und werden nur für die unternehmenseigenen Zwecke verwendet. Vermeintlich zumindest. Was nun, wenn sich ein findiger Mitarbeiter, der dazu eigentlich nicht befugt ist, diese Daten mal anschaut und plötzlich das große Geschäft wittert? Kundendaten verkaufen sich bestens. Leider. Hat wirklich jedes Unternehmen, dem Kunden ihre Daten anvertrauen, ein sicheres Identitätsmanagement im Einsatz und kann Rollen- und Rechtebasiert Zugriffe gestatten oder verweigern? Und wird sofort erkannt, wenn sich jemand unbefugten Zugriff verschafft, so dass automatisch und in Echtzeit Prozesse zur

Behebung des Schadens angestoßen werden können? Es ist natürlich gut, im Nachhinein zu prüfen, ob ein unbefugter Zugriff vorliegt und den Übeltäter zu entlarven. Wesentlich besser und sinnvoller ist es aber, es gar nicht erst soweit kommen zu lassen und schon alleine den Versuch zu unterbinden.

Sicherheit, die auf Rollen und Rechten basiert, ist allerdings natürlich immer nur so gut, wie die Regularien und Zugriffsregelungen, die dahinter stehen. In den meisten Fällen haben Mitarbeiter zu viel Zugriff auf Daten und Systeme, die sie eigentlich für ihre Arbeit nicht benötigen. Aus Bequemlichkeit oder weil die Systeme es nicht besser hergeben, werden eher zu viele Rechte eingeräumt, als umgekehrt. Mal abgesehen davon, dass einmal gewährte Rechte selten wieder entzogen werden, wie es oft bei Auszubildenden oder externen Mitarbeitern der Fall ist, die nicht selten noch Jahre später auf bestimmte Systeme zugreifen könnten. Ein Großteil der Sicherheitslücken entsteht durch Angriffe von innen, so die Marktforscher, gerade in Firmen mit hoher Fluktuation oder häufigen Umorganisationen lauert hier echte Gefahr.

Denn was passiert, wenn ein Mitarbeiter die Abteilung gewechselt hat und sich noch ein kleines Abschiedsgeschenk mitnehmen möchte? In Form von lukrativem Datenmaterial? Wenn dieser Mitarbeiter zufällig während der Urlaubszeit gewechselt ist und bislang einfach noch niemand dazu gekommen ist, seine Rechte der neuen Rolle anzupassen? Immer wenn solche Prozesse nicht automatisiert von sich gehen, entstehen kleine aber gefährliche Lücken. Organisationen, die gefährdet sind – und das ist im Prinzip jedes Unternehmen und jede Institution in Bezug auf Datenmissbrauch und -Schutz – benötigen eine integrierte Identitäts-, Zugriffs- und Sicherheitslösung, mit der sie nachverfolgen können, wer, was, wo, wann, warum und wie innerhalb der IT-Infrastruktur gemacht hat.

Eine weitere erhebliche Ursache für Datenlecks ist auch die stetig steigende Mobilität. Heutzutage ist ja eigentlich jeder mobil, ob als Privatperson oder in geschäftlichen Angelegenheiten. Alle nutzen vertrauliche Daten, egal wo sie sich gerade aufhalten – im Hotel, im Internetcafé, am Flughafen oder von zuhause über ungeschützte Leitungen. Unternehmen müssen die Kontrolle über die so genannte „Endpoint Security“, das heißt die Sicherheit am Endgerät, zurückerobern und behalten.

Die wichtigsten Gefahrenquellen mit denen Unternehmen – und damit auch deren Kunden – konfrontiert werden, wenn es um die Sicherheit von Daten geht, sind also unbefugte Zugriffe auf vertrauliche Daten von intern oder von extern, über interne Systeme oder mobile Geräte. Egal, ob es sich dabei um ein Versehen oder einen vorsätzlichen Missbrauch handelt: Abhilfe schaffen nur umfassende Identitätsmanagement-Systeme. In Zeiten der Verunsicherung, was mit den persönlichen Daten passiert, können Unternehmen, die solche Systeme im Einsatz haben, das sogar als entscheidenden Wettbewerbsvorteil nutzen. Jeder kauft schließlich am liebsten bei einem Anbieter, bei dem er mit Sicherheit ein gutes Gefühl haben kann.

Über Novell

Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachusetts (USA), beschäftigt weltweit rund 4.700 Mitarbeiter.

Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter www.novell.com oder www.novell.de.

Pressekontakt:

Lars Basche
Text 100 Public Relations
Tel: +49 - (0)89 - 99 83 70-33
E-Mail: novell@text100.de

Ulrike Beringer
Novell GmbH
Tel.: +49 (0)89 20600 2118
Email: uberinger@novell.com