

Statement of the Month – Novell Identity & Security

Düsseldorf im April 2007

Dauerlauf statt Sprint - Informationssicherheit erfordert Durchhaltevermögen

Sicherheitsbedrohungen wie Trojaner, Phishing-Angriffe und andere Formen von Malware erhalten derzeit zu Recht große Aufmerksamkeit in Unternehmen und Öffentlichkeit. Darüber darf allerdings die Gefahr durch Angriffe von innen, d.h. durch Mitarbeiter und Dienstleister mit ansonsten legalem Zugriff auf das Firmennetz nicht unterschätzt werden. Dabei muss es sich nicht um Vorsatz handeln, selbst unbewusstes Fehlverhalten birgt Risiken für die Sicherheit von Daten und Systemen. Und mit der Sicherheit der Daten setzt ein Unternehmen auch das eigene Image aufs Spiel. Dr. Harald Meyer, Principal Security & Compliance bei Novell, erläutert, wie diesen Bedrohungen Einhalt geboten werden kann.

Das jüngste Beispiel der anglo-amerikanischen Kaufhaus-Kette TJX zeigt, dass die aktuelle Diskussion nicht nur einer gesteigerten Sensibilisierung entspringt, sondern auf konkreten Risiken und Schäden beruht. Dort wurden über einen Zeitraum von mehr als einem Jahr vermutlich mehr als 45 Millionen Kreditkartendaten gestohlen und teilweise zu betrügerischen Transaktionen genutzt. Auch wenn die Ermittlungen noch nicht abgeschlossen sind, ist bereits heute absehbar, dass alleine Strafzahlungen und Schadenersatzforderungen an TJX Kosten im dreistelligen Millionenbereich verursachen werden, vom Imageschaden für TJX ganz abgesehen.

Vor diesem Hintergrund ist es nicht verwunderlich, dass die rechtlichen und vertraglichen Anforderungen an die Informationssicherheit zunehmend schärfer und detaillierter werden.

In vielen Fällen sind zwar die Vorgaben und Konsequenzen zur Informationssicherheit beispielsweise des GmbH-Gesetzes oder von KontraG bekannt, nicht zuletzt wegen der darin festgeschriebenen Haftungspflichten für Vorstände und Geschäftsführer. Aber selbst Unternehmen, die aufgrund ihrer Rechtsform diesen Vorgaben nicht unterliegen, müssen beispielsweise personenbezogene Informationen gemäß den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) schützen. Dort sind bereits bei fahrlässigem Verschulden empfindliche Strafen vorgesehen. Ebenso sind alle Händler, die Kreditkartenzahlungen akzeptieren, spätestens ab dem 30. Juni 2007 zu stringenten Sicherheitsmaßnahmen für den Schutz von Kreditkarteninformationen verpflichtet, wie sie von der Kreditkartenindustrie definiert wurden.

Diese und andere der zahlreichen gesetzlichen und vertraglichen Regelungen bringen im Schadensfall erhebliche Haftungsrisiken für das betroffene Unternehmen mit sich – zusätzlich zum Imageschaden, der in vielen Fällen die direkten Kosten bei weitem noch übersteigt und schwer quantifizierbar ist. Viele Unternehmen wiegen sich fälschlicherweise in Sicherheit. Sie sind der Meinung, dass Sicherheitsrisiken durch Betriebsausfall- und -haftpflichtversicherungen immer komplett abgedeckt sind. Das ist nicht der Fall; denn es reicht nicht, irgendwann eine derartige Versicherung abzuschließen und dann ruhen zu lassen. Es gibt Beispiele, in denen eine Betriebsausfallversicherung die Regulierung eines Schadens im mittleren sechsstelligen Euro-Bereich erfolgreich abgelehnt hat, weil das betroffene Unternehmen seine Risikobewertung über zwei Jahre hinweg nicht aktualisiert hatte.

Ebenso gibt es oft Ansprechpartner im Unternehmen, die glauben, dass mit der Übergabe des IT-Betriebs an einen Outsourcing-Partner auch die Verantwortung für Informationssicherheit übergeben wurde. Ihre Auditoren sehen das aber anders – und die Geschäftspartner und Kunden sowieso.

Es stellt sich daher nicht die Frage, wie Unternehmen mit diesen Sicherheitsrisiken und auch den damit verbundenen Haftungsrisiken umgehen *können*, sondern wie sie damit umgehen *müssen*. Insellösungen für die jeweiligen Normen und Vorgaben sind hier wenig hilfreich, wie dies beispielsweise in den USA im Rahmen der SOX-Compliance anfangs oft geschehen ist.

Sehr viel sinnvoller ist es, stattdessen ein umfassendes Informations-Sicherheits-Management-System (ISMS) zu etablieren. Auf seiner Basis können dann unterschiedliche gesetzliche und vertragliche Sicherheitsanforderungen kostengünstig und trotzdem wirksam umgesetzt werden. Aber mit der einmaligen Einrichtung eines Systems ist es nicht getan.

Informationssicherheit ist ein kontinuierlicher Prozess. Die ISO-Norm 27001 beschreibt, wie dieser Prozess aussehen kann: Sie stellt den internationalen Standard für Informationssicherheit dar und bildet die Klammer für die meisten anderen einschlägigen Detailnormen wie beispielsweise ISO 13335, ISO 17799 und künftig auch das in Deutschland vielerorts bekannte Grundschriftbuch (GSFB).

Das Grundschriftbuch orientiert sich im Kern an dem auch in der Qualitätssicherung altbekannten Plan-Do-Check-Act Modell, oft auch als Deming-Zyklus bezeichnet. Nach dieser Vorgabe ist der erste Schritt zur Informationssicherheit im Unternehmen die systematische Identifikation und Bewertung der konkreten geschäftlichen Risiken. Nur auf dieser Basis können adäquate Schutzmaßnahmen überhaupt implementiert werden. Aber damit ist es noch längst nicht getan, wie viele Verantwortliche oftmals annehmen. Es reicht nicht aus, Firewalls zu beschaffen und Anti-Malware-Software zu installieren oder die Mitarbeiter auf einer Richtlinie zur Informationssicherheit zu verpflichten. Richtlinien sind schön und gut, müssen aber auch mit Leben gefüllt und vor allem überprüft werden. In der Vergangenheit landeten diese aber auf Hochglanzpapier ausgedruckt im Schrank und waren auch im Intranet verfügbar, sofern man wusste, wo man suchen sollte. Ihre Einhaltung wurde aber nicht wirksam überprüft. Ebenso wurden beispielsweise Logfiles kritischer Systeme zwar regelmäßig archiviert, aber gar nicht oder nur unzureichend auf sicherheitsrelevante Vorfälle analysiert – außer im Nachhinein, wenn der Schaden bereits aufgetreten war, wie das eingangs erwähnte Beispiel TJX zeigt. Es geht also nicht darum, zum Ziel loszusprinten, auf dem Weg im Eiltempo alle sicherheitsrelevanten Aktivitäten abzuhaken und sich dann auszuruhen. Die Angemessenheit und die Wirksamkeit der getroffenen Schutzmaßnahmen muss vielmehr kontinuierlich überwacht werden. Das kann sowohl durch ein zeitnahes Monitoring als auch durch eine aussagekräftige Dokumentation, die zudem vor Manipulationen weitgehend geschützt ist, passieren. Diese Dokumentation muss auch erkannte Vorfälle und ihre Nachverfolgung einschließen.

Die Erkenntnisse und Verbesserungen, die durch diese kontinuierliche Überwachung gewonnen werden, helfen wiederum dabei, Risikobewertung und Schutzmaßnahmen auf dem neuesten Stand zu halten. So schließt sich der Kreis eines kontinuierlichen IT-Sicherheitsprozesses, der dafür sorgt, dass ein einmal erreichtes Sicherheitsniveau dauerhaft gehalten werden kann, auch bei geänderten internen und externen Rahmenbedingungen. Kurz gesagt: Dauerlauf kräftigt Herz und Gefäße, steigert die Durchblutung und bringt die Abwehrkräfte in Position.

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:

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

Ihre Ansprechpartnerin bei Novell:
Ulrike Beringer
PR Manager Novell Central Europe
Tel: +49 - (0)89 - 206002118
E-Mail: uberinger@novell.com