

## Statement of the Month – Novell Identity & Security Management

Düsseldorf im April 2008

### Alle meine Ichs

**Selten ging es so schnell, sich eine eigene und neue Identität zu schaffen, wie in den heutigen Zeiten von Web 2.0. Man registriert sich, gibt sich einen Benutzernamen und ein Passwort und schon hat man ein neues, zusätzliches Ich und kann Bücher bestellen, Zeitschriften abonnieren, Konten eröffnen und Kontaktanzeigen aufgeben. Es fällt allerdings nicht leicht, bei den vielen verschiedenen Identitäten und den damit verbundenen Zugangsdaten den Überblick zu behalten. Hersteller und Nutzer kommen daher auf immer neue Ideen, um den Passwortschubel in den Griff zu bekommen oder gar zu umgehen. Marina Walser, Director Identity & Security Management bei Novell Central Europe, wirft einen Blick auf die Ich-Welle, die „kreativen“ Lösungsmöglichkeiten und untersucht, was wirklich weiterhilft.**

Ich habe mindestens 35 verschiedene Identitäten. Was vor nur 30 Jahren noch wie ein beängstigender Fall von Schizophrenie geklungen hätte, ist im heutige Geschäfts- und Privatleben gang und gäbe. Wo man auch hingeht, hinterlässt man eine Identität. Für die Anmeldung bei einem Online-Newsletter wird ein Benutzername und ein selbst gewähltes Passwort gefordert. Warum der Nutzer sogar dafür ein Passwort kreieren muss, ist eine andere Frage; im Prinzip will er ja nur auf dem Laufenden bleiben. Am Kiosk wird schließlich auch nicht nach dem Personalausweis gefragt. Vielleicht soll über die Sicherung durch ein Passwort vermieden werden, dass jemand die Vorlieben für Wirtschaftsnachrichten ausspioniert, heute ist ja schließlich alles denkbar. Also auch hier ein Zugangscode. Ansprüche werden an dieses Passwort nicht gestellt, ganz im Gegensatz zu anderen Systemen, bei denen es nicht selten einem Glücksspiel ähnelt, ein neues Passwort zu finden. „Passwort bereits vergeben“ oder „Passwort zu unsicher“ sind da noch die konkreteren Fehlermeldungen. Aber auch diese helfen nicht weiter, wenn darüber hinaus keine Aussage erfolgt, warum das Passwort eigentlich unsicher ist und wie sich das ändern lässt. Eine Kombination aus willkürlich zusammengestellten, unzusammenhängenden Zahlen und Buchstaben ist auf jeden Fall sicher, aber da versagen selbst die ausgeklügeltsten Eselsbrücken. Schön sind auch Firmensysteme, bei denen alle vier Wochen das Passwort für das mobile Gerät geändert werden muss und sich das neue Passwort wesentlich vom alten unterscheiden sollte. Einfach eine andere Zahl anzuhängen, reicht da längst nicht aus. Die Anforderungen an die Sicherheit der Passwörter sind groß und deutlich, aber wie der Nutzer den Überblick behalten soll, wird leider nicht verraten.

Bei vielen Passwort-Anfragen wie der zitierten Newsletterabonnierung reichen glücklicherweise der Name der Mutter oder sonstige, leicht nachvollziehbare Inhalte. Wichtig ist nur, dass der Nutzer dieses Passwort nicht vergisst. Sollte sich der Lesegeschmack einmal ändern, muss das Passwort eingegeben werden. Es soll ja wankelmütige Geister geben, aber das Leseverhalten der meisten Nutzer ändert sich nicht täglich. Wer sich einmal für einen Newsletter angemeldet hat, möchte ihn meist eine Weile lesen und das Passwort nach sechs Monaten noch zu wissen, ist auch wieder Glückssache. Gerade in der IT-Brache ist das eine fast unvorstellbar lange Zeit. Ganze Firmen werden umgebaut, Trends kommen auf und verschwinden wieder und der Nutzer soll sich ein Passwort merken, dass er erst einmal verwendet hat? Das ist durchaus eine Herausforderung.

Es gibt also im Prinzip zwei Möglichkeiten: Man nimmt ein einfaches Passwort, das aber immer noch komplex genug ist, um die hinterlegten Sicherheitsanforderungen zu erfüllen und verwendet dies dann immer wieder: bei der Buchbestellung, der Kaffeerösterkette, der Reiseplanung, den oben beschriebenen Newslettern, dem privaten E-Mail-Account und am besten auch noch bei den verschiedenen Anwendungen und Systemen im Unternehmen. Das Ganze hat den Vorteil, dass man sich dieses Passwort nicht aufschreiben muss, weil man es beinahe täglich verwendet. Und wenn es mal geknackt wird, verursacht es Angreifern wenig Arbeit, da sich damit dann alles knacken lässt. Ein fragwürdiger Vorteil. Bleibt nur noch das Problem der „erzwungenen“ Kennwortänderung in vielen Unternehmen einmal im Quartal. Ändere ich jetzt nur die firmeninternen Passwörter oder auch die für alle anderen Anwendungen und Dienste im Internet, um wieder ein einheitliches, durchgängig nutzbares Passwort zu haben? Das artet in Arbeit aus.

Bei der zweiten Möglichkeit, die zumindest im Internet immer mehr Anklang findet, lässt der Anwender seiner Kreativität bei einer neuen Registrierung freien Lauf. Für die Sicherheit ist damit gesorgt, sogar so stark, dass sich der Erfinder den Code selbst nicht merken könnte, selbst wenn er das wollte. Kein Problem, es gibt die praktische Funktionalität des „Zurücksetzens“, auf die direkt bei der Anmeldung hingewiesen wird. „Wenn Sie ihr Passwort vergessen haben, klicken Sie hier und wir senden Ihnen ein Neues an die angegebene E-Mail-Adresse“. Das ist einfach, geht meist sehr schnell und wird dementsprechend stark genutzt. Egal wie vergesslich der Nutzer ist, der Zugang zum gewünschten Bereich ist wieder offen. Das

Ganze hat nur einen Haken: E-Mail-Systeme zählen leider nicht zu den sichersten Kommunikationskanälen. Sehr leicht können hier sensible Daten ausspioniert werden oder verloren gehen. Bei der Newsletteranmeldung ist das verschmerzbar, aber bei Passwörtern für Bankzugänge, Lieferdienste und andere Konten mit finanzieller Einbindung, birgt es ein nicht unerhebliches Risiko.

Es gibt viele kreative Ansätze, die sich derzeit um Lösungen des Problems bemühen. So werden Unterstützungshilfen für vergessliche Anwender gebaut, moderne Formen der traditionellen Eselsbrücke sozusagen. Eine einfache und effektive Lösung ist der Einsatz von Single-Sign-On-Technologien. Damit ist zumindest im Unternehmen der Einsatz von nur einem Passwort für alle Systeme gesichert. Sobald das Passwort geändert wird, wird es automatisch auch in allen anderen angebundenen Systemen und Anwendungen geändert. Die Änderung der Zugriffscode ist – nach der kreativen Eigenleistung bei der Schaffung eines neuen Wortes – mit dieser technischen Unterstützung eine Sache von zwei Klicks. Zusätzlich können dann besonders sensible Bereiche über eine starke Authentifizierung, zum Beispiel mittels Smart Card, abgesichert werden. Damit können Hacker dann eben doch nicht mit einem geknackten Passwort in alle Anwendungen eindringen. Ein Passwort-Self-Service, der intelligente Fragen stellt, die nicht über Social Engineering erraten werden können, vermeidet den unsicheren Versand von Passwörtern via eMail.

Auch die Open Source Community beschäftigt sich immer stärker mit dem Thema Identitätsmanagement und der Herausforderung, die digitalen Identitäten in Einklang zu bringen. OSIS (Open Source Identity Systems) beispielsweise vereint viele Open Source Projekte rund um das Thema Identitäten. Ziel ist der Aufbau eines kompatiblen Identitäts-Layers für das Internet aus Open-Source und proprietären Bausteinen. So werden die beiden Welten verschmolzen, mit dem Ziel, die vielen Ichs auf einen, oder zumindest wenige Nenner zu konzentrieren, so dass sich der Nutzer wieder auf das Wesentliche konzentrieren kann: Die eigentliche Bestellung.

### **Über Novell**

Novell, Inc. (Nasdaq: NOVL) bietet eine Linux-Plattform auf höchstem technischen Niveau, die vollständig kompatibel mit den Systemen zahlreicher anderer Anbieter ist. Ergänzt wird das Portfolio durch integrierte IT Management Software, mit der Unternehmen weltweit Kosten, Komplexität und Risiken reduzieren können. Mit dieser Infrastruktur-Software und einem umfassenden Partnernetzwerk integriert Novell heterogene IT-Umgebungen und ermöglicht so, dass Menschen und Technologie als eine Einheit zusammen arbeiten. Weitere Informationen unter [www.novell.com](http://www.novell.com).

### **Pressekontakt:**

Ulrike Beringer  
Novell GmbH  
Tel.: +49 (0)89 20600 2118  
E-Mail: [uberinger@novell.com](mailto:uberinger@novell.com)

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