

Ursula Sury

Berechtigungen

UM WAS ES GEHT

Im Rahmen der heute gängigen Diskussionen über interne Kontrollsysteme und Compliance (auch IT-Compliance) wird häufig der Begriff Identity Management in Verbindung mit der Vergabe von Berechtigungen verwendet. Viele der diesbezüglichen Anliegen und Fragen sind dabei von der Rechtsordnung mitgesteuert.

ROLLEN

Aufgaben, Kompetenzen und Verantwortungen verschiedener Funktionen spiegeln sich im Bereich der IT in sogenannten Berechtigungen. Es stellt sich dabei konkret die Frage, wer darf mit welchen Daten und Informationen wann, was und warum machen? Für verschiedene Berechtigungsklassen werden sogenannte Rollen definiert. Rollen spiegeln sich in rechtlich-organisatorischer Hinsicht im Organisations- und Funktionsdiagramm der Unternehmung und auf individueller Ebene im einzelnen Stellenbeschrieb. Eine Rolle ist aber immer auch auf einen konkreten Businessprozess bezogen und kann sich über die Zeit verändern oder gar wegfallen. Beim Managen von Rollen sind also immer mindestens drei Dimensionen dynamisch zu berücksichtigen, nämlich die individuelle Funktion in einzelnen Geschäftsprozessen (1) mit der Veränderung der Funktion und der Geschäftsprozesse (2) über eine bestimmte Zeit (3).

Die Definition von Rollen muss mit grosser Sorgfalt vorgenommen werden, in der Praxis findet man nämlich immer wieder Kumulierungen von Rollen auf einzelne Personen, welche Interessenkonflikte implizieren und somit den Grundsätzen von Corporate Governance widersprechen.

BERECHTIGUNGEN

Je nach Rolle werden den IT-Benutzern verschiedene Berechtigungen zugeteilt. Inhalt und Umfang dieser Berechtigungen orientiert sich meist an einem internen Zugriffs- oder Berechtigungskonzept. Leider fehlt bei diesen internen Konzepten häufig die Berücksichtigung gesetzlicher Vorgaben. Beispielsweise ist es in datenschutzrechtlicher

Hinsicht zwingend, dass nur diejenigen Mitarbeitenden und nur so viele Mitarbeitende auf personenbezogene Daten zugreifen dürfen, wie unbedingt notwendig.

Meist sind Berechtigungen aus Gründen der Bequemlichkeit und organisatorischen Vereinfachung zu weit gefasst. Dies erhöht beispielsweise auch die Risiken des Abzuges oder der Verletzung der Geschäftsgeheimnisse, Intellectual Property etc.

IDENTITÄTEN

IT-Programme, die helfen Rollen und Berechtigungen zu definieren und zu verwalten, werden häufig Identity-Management-Systeme genannt. Wie in einem früheren Artikel schon dargelegt (Identity Management und Recht, Ursula Sury, Informatik-Spektrum Juni 2004) beschäftigt sich Identität im Rahmen von solchen Systemen, entgegen dem Wortlaut, nicht mit der Identifikation einer natürlichen Person (wer bin ich) sondern der Verifikation (stimme ich überein), also der Frage, ob die Authentifizierung desjenigen, der sich ans System anmeldet, mit der hinterlegten Information übereinstimmt.

Dies bedeutet, dass bei der Vergabe und Verwaltung von Identitäten und den dazugehörigen Authentifikationen grösste Sorgfalt geboten ist, diese Sorgfaltspflicht den Mitarbeitenden überbunden und die Einhaltung kontrolliert werden muss. Über das Ausleihen und Weitergeben von Authentifikationen können grosse Missbräuche geschehen.

Schliesslich wissen wir alle seit Jahren: *“In the Internet (or Intranet) nobody knows you are a dog.”*

MONITORING

Identity Management impliziert nicht nur das Zuweisen und Verwalten von Identitäten und die damit verknüpften Rollen und Berechtigungen, sondern auch das Aufzeichnen und die Überprüfung der getätigten Zugriffe.

Die Durchführung solcher Kontrollen wird denn auch durch verschiedene gesetzliche Grundlagen direkt oder indirekt gefordert, sei es um gegenüber der Revision belegen zu können, welche Transaktionen durch wen gemacht werden, sei es um Urheberrechtsverletzungen zu vermeiden (DRM), um die Konsumation strafbarer Inhalte über Internet zu vermeiden, um die Betriebssicherheit generell einzuhalten, oder um allgemein Risiken zu vermeiden.

Dieses Monitoring resp. diese Überwachungen werden in datenschutzrechtlicher Hinsicht regelmässig diskutiert. Sofern man die Monitoringaktivitäten aber mit einer gesetzlichen Grundlage begründen kann oder die betroffenen Personen konkret eingewilligt

haben, sind diese grundsätzlich kein Problem. Wichtig ist aber auf jeden Fall, dass den Mitarbeitenden klar gemacht wird, dass, warum und auf welche konkrete Art und Weise Monitoring betrieben wird und wie sich ein mögliches Incident Management gestaltet. Zudem ist das Monitoring selbstverständlich nur soweit zulässig, wie es durch den gesetzlichen Zweck oder die konkrete Einwilligung der betroffenen Person gedeckt ist.

IDENTITY PROVIDER

Mit Identity Provider wird diejenige, (natürlich oder juristisch), Person bezeichnet, welche die digitalen Identitäten zuweist und verwaltet. Dieser Begriff wird auch extern verwendet, beispielsweise für die Institutionen, welche Zertifikate zur Erstellung digitaler Signaturen vergeben. In Unternehmungen braucht es Identity Provider, welche die verschiedenen Identitäten und die zugewiesenen Rollen und Berechtigungen vergeben und verwalten.

In unternehmerischer und organisatorischer Hinsicht stellt sich hier die Frage, wer mit dieser äusserst wichtigen und sensiblen Aufgabe betraut ist. Welche Fachkompetenzen braucht es dafür, in welcher hierarchischen Einordnung steht der Identity Provider und wer kontrolliert ihn. Diese Fragen sind sorgfältig abzuklären, denn der Identity Manager muss unbedingt grosses Vertrauen geniessen, da er faktisch eine sehr grosse Machtstellung inne hat.