COMPUTERWELT
IT. TELEKOMMUNIKATION . BUSINESS . AT

.06 Unternehmen vor dem Kadi

Roland Kisslinger 10.3.2006

Fast unbemerkt von Öffentlichkeit und Betroffenen ist seit ersten Jänner das neue Unternehmensstrafrecht in Kraft getreten, welches eine weit reichende Haftung für Firmen vorsieht. Die Strafen können abhängig von der Ertragslage bis zu 1,8 Mio. Euro betragen. Ganz besonders ist hier auch die IT-Abteilung betroffen, bzw. Händler, die Produkte irrtümlicherweise als „compliant“ mit diversen internationalen Standards weiterverkaufen.

HAFTUNG BEI DATENKLAU

Früher waren Unternehmen nicht für unangenehme Affairen haftbar, wenn Mitarbeiter etwas ausgefressen hatten. Das neue „Verbandsverantwortlichkeitsgesetz (VbVG)“ schiebt dem nun einen Riegel vor – allerdings so weitgehend, dass sich auch der gewöhnliche Manager und Mitarbeiter damit befassen sollten: Kinderpornografie im Dienst, mangelhafte Rechteverwaltung und Fehler aufgrund veralteter Systeme können jetzt ziemlich teuer werden – und auch die zuständigen Manager vor Gericht bringen. Ausgelöst wurde diese Verschärfung durch die Seilbahn-Katastrophe in Kaprun. Der Gesetzgeber will damit ein stärkeres Verantwortungsbewusstsein für Unternehmen schaffen.

Künftig können Unternehmen wie ZB eine GmbH für gerichtlich strafbare Tatbestände ihrer Entscheidungsträger und Mitarbeiter selbst dann haften, wenn diese vor Gericht dafür nicht verurteilt wurden - ja sogar dann, wenn nicht einmal der Name des Mitarbeiters bekannt ist. Neu ist also, dass nicht nur die Mitarbeiter zum Handkuss kommen, wenn sie vorsätzlich oder ohne Sorgfalt gehandelt haben – sondern das ganze Unternehmen, wenn dessen Entscheidungsträger die gebotene Sorgfaltspflicht für die Mitarbeiter vernachlässigt haben. „Das ist gerade für IT-Abteilungen von besonderer Brisanz“, meint Rainer Knyrim von Preslmayr Rechtsanwälte im Interview mit der COMPUTERWELT.at. Als Beispiel führt er Mitarbeiter an, die aufgrund mangelhafter Zugriffsberechtigungen Datenbestände löschen. Auch besonders eifrige Programmierer, die sich mal eben bei der Konkurrenz ‚einhacken’, um neueste Betriebsgeheimnisse in Erfahrung zu bringen, könnten laut Knyrim zu einer Verurteilung des Unternehmens führen – selbst dann, wenn es von den konkreten Umtrieben nichts mitbekommen hat, aber nicht die notwendigen Vorsorgemaßnahmen getroffen hat. Auch wenn Daten abhanden kommen, die zu wenig gesichert gewesen seien, würde der Kopf bereits in der Schlinge hängen. Dies bezieht sich nicht nur auf sorglose Transporte von Datenbändern, sondern auch auf fehlende Backups. Die Unternehmen müssten laut Knyrim Sorge tragen, dass Maßnahmen unter Bedachtnahme auf den Stand der Technik getroffen würden – soweit diese wirtschaftlich vertretbar sind.

STRAFMASS EXISTENZ-BEDROHEND

Als Strafmaß sind bis zu 180 Tagessätze von maximal 10.000 Euro vorgesehen, bemessen an der Ertragslage des Unternehmens. Als potentielle Höchststrafe drohen großen Firmen damit bis zu 1,8 Mio. Euro. Schwere Datenbeschädigung durch Mitarbeiter kann damit ZB bis zu

einer Mio. Euro kosten. Verschärft werden die Auswirkungen des Gesetzes durch eine der COMPUTERWELT.at bekannt gewordene, interne Anweisung an die Staatsanwälte, dass in Zukunft Straffälle mit Unternehmensbezug immer auch auf Verstöße gegen das VbVG zu prüfen seien. Künftig will man damit vor allem dem als „white collar crime“ bezeichneten Betrug unter Geschäftsleuten einen Riegel vorschieben. Auch die von manchen Sachverständigen als „Gang und Gebe“ bezeichnete Praxis, Versicherungsbetrug mit EDV-Systemen zu betreiben, wird sich mit dem neuen Gesetz aufhören – zu hoch sind mittlerweile die Strafen, falls man bei der bewussten „Zerstörung durch Blitzschlag“ erwischt wird.

AUCH IT-RESELLER BETROFFEN

Auch IT-Händler sind von der Regelung betroffen, wenn sie ZB Produkte weiterverkaufen, die als „compliant mit allen internationalen Standards“ ausgezeichnet sind. Sollte sich dies als Irrtum herausstellen und die Firma , die das Produkt gekauft hat, verurteilt werden, würde sich diese künftig wohl auch am Händler schadlos halten können, meint Knyrim. Dies gelte ZB für Computersysteme, die mit Beratung und Implementierung installiert worden seien, dann aber doch entscheidende Fehlfunktionen produziert hätten. Oder sich als fernab vom Stand der Technik oder der konkreten österreichischen Rechtslage herausgestellt hätten. Hier könnte sich das betroffene Unternehmen künftig auf zivilrechtlichem Weg durch Regress-Forderungen an dem Verkäufer schadlos halten. Knyrim sieht das durchaus auch als Verkaufsargument für gewissenhafte Hersteller: „Alle reden von Compliance und schauen dabei auf amerikanische Gestze. Das VbVG gibt aber auch hierzulanden einen sehr konkreten Anlass für Compliance, denn Unternehmen haften künftig und sind gezwungen, Sicherheitsmaßnahmen zu ergreifen.“

WIE SICH UNTERNEHMEN SCHÜTZEN KÖNNEN

Was können Unternehmen tun, um sich vor den Auswirkungen des Gesetzes zu schützen? Knyrim gibt hier klare Empfehlungen ab: Zum einen wären betriebliche IT Policies sinnvoll, in denen genau geklärt und erläutert wird, was erlaubt und was verboten ist. Zum anderen enthält auch das Datenschutzgesetz in §14 sehr konkrete Datenschutzmaßnahmen. So muss ZB die Zutrittsberechtigung zu Räumlichkeiten geregelt, sowie ein Zugriffsschutz auf Daten installiert sein, bzw. eine Berechtigung für den Betrieb von EDV-Systemen eingerichtet sein. Zudem muss die Verwendung von Daten protokolliert werden, eine Einschulung der Mitarbeiter vorliegen und es müssen klare Arbeitsanweisungen und eine strukturierte Arbeitsorganisation vorhanden sein.