Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im November 2012

Sehr geehrten Damen und Herren,

sensible Daten sind vor allem dann in Gefahr, wenn Mitarbeiter die Arbeitsstelle wechseln. Europaweit haben die Hälfte aller Büroangestellten schon vertrauliche Unternehmensdaten mitgenommen. Deutsche Angestellte gaben an, in diesem Fall zumeist Unternehmenspräsentationen (57 Prozent) und die Kunden-Kontaktdatenbank (54 Prozent) mit in den neuen Job transferiert zu haben.

Zu diesem Ergebnis kommt eine Studie von Iron Mountain, einem Spezialisten für Informationsmanagement und dem Schutz geistigen Eigentums. Dabei wurden 2000 Büroangestellte aus allen Branchen in Deutschland, Frankreich Spanien und Großbritannien befragt.

Gut ein Drittel der Befragten hat sogar alle Dokumente aus dem Unternehmensnetz entfernt, an deren Entstehung sie beteiligt waren. Strategische Pläne wechselten in 30 Prozent der Fälle die Seiten. In all diesen Fällen, so die Studienautoren, handelt es sich um sensible und wertvolle Unternehmensdaten, deren Verlust zu Wettbewerbsvorteilen für die Konkurrenz sowie zu Verlust von Markenreputation und Kundenvertrauen führen kann.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung und auch das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen bleibt unberührt.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

Wieder möchten wir ihnen einen Fall aus unserer aktuellen Arbeit näherbringen.

Ein Mitarbeiter aus dem Vertrieb eines mittelständischen Maschinenbauunternehmens kündigt aus Verärgerung über eine zu geringe Lohnerhöhung. Im Nachgang gründet er ein eigenes Unternehmen im Wettbewerbsumfeld seines alten Arbeitgebers.

Kunden des ehemaligen Arbeitgebers meldeten sich bei diesem mit dem Hinweis, dass der jetzt selbständig tätige Ex-Mitarbeiter Angebote mit Firmeninterna seines alten Arbeitsgebers unterbreite. Eine Prüfung ergab, dass diese Informationen nur in dem alten Unternehmen vorhanden waren und geistiges Eigentum der Maschinenbaufirma sind.

Wie der ehemalige Mitarbeiter die umfangreichen Daten aus dem Unternehmen geschleust hat, ist zurzeit Gegenstand von Ermittlungen.

Eine Strafanzeige ist, nach erfolgter Beratung durch den Wirtschaftsschutz, bei der zuständigen Polizeidienststelle erstattet worden.

<u>Folgende Fragen sollten Sie sich bei ausscheidenden Mitarbeitern stellen:</u>

- Auf welche unternehmensrelevanten Daten hat der Mitarbeiter Zugriff?
- Sind diese Informationen für Unbefugte interessant?
- Sind diese Daten ausreichend vor unberechtigtem Zugriff geschützt?
- Welche Zugangsberechtigungen hat der Mitarbeiter?
- Wer ist unternehmensintern über das Ausscheiden zu informieren?

Folgendes sollten Sie wissen:

Ausscheidende Mitarbeiter glauben aus verschiedenen Gründen, dass sie Daten aus dem Unternehmen mitnehmen können:

- Weil sie maßgeblich an der Entstehung der Daten mitgewirkt haben.
- Weil sie die Daten bei ihrem neuen Arbeitgeber gut gebrauchen können.
- Weil sie die alte Firma schädigen wollen.

Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern nach BSI Grundschutzkatalog (eine beispielhafte und nicht abschließende Aufzählung):

- Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden.

- Von dem Ausscheidenden sind sämtliche Unterlagen (wie auch entliehene institutionseigene Bücher), ausgehändigte Schlüssel, ausgeliehene Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise sowie sonstige Karten zur Zutrittsberechtigung einzuziehen. Ferner sind bei biometrischen Verfahren (z. B. Irisscanner, Fingerabdruck- und Handrückenerkennung) entsprechende Zutrittsberechtigungen zu löschen bzw. auf die getroffene Vertreterregelung anzupassen.

- Es sind sämtliche für den Ausscheidenden eingerichteten Zugangs-berechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen

geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Weggang einer der Personen die Zugangsberechtigung zu ändern.

- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.

- Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren.

- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.

- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen, zu verwehren. Auch bei Funktionsänderungen muss unter Umständen die Zutrittsberechtigung zu bestimmten Räumlichkeiten wie Serverräumen entzogen werden.

- Optional kann sogar für den Zeitraum zwischen Aussprechen einer Kündigung und dem Weggang der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.