

Fachartikel vom 07.12.2010

**Rubriken:** Wirtschaftsschutz: Business Continuity Management, Wirtschaftsschutz: Know-how-Schutz, Wirtschaftsschutz: Risk Management, Wirtschaftsschutz: Sicherheitskonzepte

Whistleblowing

## Geschäftsgeheimnisse bald bei Wikileaks?

**Auf der Whistleblower-Webseite Wikileaks wurden Staatsgeheimnisse der USA veröffentlicht. Warum konnten die USA diese Daten nicht schützen? Wenn Staaten ihre Geheimnisse nicht mehr schützen können, wie sieht es dann mit dem Schutz von Informationen bei Unternehmen aus?**



Kleines Leck, großer Schaden: Wenn es im Unternehmen undichte Stellen gibt, fließen vertrauliche Informationen unkontrolliert ab. (Bild: Pixelio.de/Kurt Michel)

Auf einer der ersten Hacker-Konferenzen im Jahre 1984 hat der amerikanische Autor und Herausgeber Stewart Brand die Problematik korrekt vorhergesagt: „Auf der einen Seite will Information teuer sein, weil sie so wertvoll ist. Die richtige Information zur richtigen Zeit verändert Dein Leben. Auf der anderen Seite will Information frei sein, weil die Kosten der Informationsverbreitung ständig geringer werden.“ Dieses Dilemma hat sich in den letzten Jahren deutlich verschärft. Nie waren Informationen so wertvoll wie heute, nie hat ein Informationsvorsprung einen so großen Unterschied für den Erfolg einer Unternehmung gemacht wie in der heutigen Wissensgesellschaft.

### Datenmengen für den Hausgebrauch

Auf der anderen Seite ist es heute dank moderner IT-Technologien einfacher denn je, Informationen zu verbreiten. USB-Sticks und Festplatten werden immer größer und billiger, und die verfügbaren Netzwerkgeschwindigkeiten immer größer. Die Wikipedia findet mit allen Bildern und allen Sprachen Platz auf einer 500 Gigabyte Festplatte, solche Geräte werden für Preise unter 40 Euro an der Kasse der Elektronikhändler verramscht. Es wird vermutet, dass die Daten, die Wikileaks nun in drei Chargen veröffentlicht hat eine Gesamtgröße von 1,4 Gigabyte haben. Mit einem guten DSL-Anschluss könnte diese Datenmenge in 15 Minuten auf den eigenen Rechner geholt werden.

Die IT-Sicherungsmaßnahmen für das amerikanische Geheimnetzwerk „Siprnet“ über das die jetzt veröffentlichten Nachrichten verschickt wurden, wurde weder umgangen noch „gehackt“. Die US-Regierung hat dieses Desaster einem einzelnen Mitarbeiter zu verdanken. Laut Presseberichten haben 2,5 Millionen Ministerial- und Behördenmitarbeiter Zugriff auf das Siprnet-Material. Dass Informationen, die 2,5 Millionen Menschen potentiell lesen können, nicht sonderlich lange geheim bleiben, scheint offensichtlich.

### Gelegenheit macht Daten-Diebe

Gleichzeitig begehen die meisten Firmen denselben Fehler. Oft haben alle Mitarbeiter Zugriff auf Konstruktionspläne, Vertriebsinformationen und andere wettbewerbsrelevante Informationen. Oft schließt dies dann selbst Ferienarbeiter, Werkstudenten und alle Mitarbeiter von ausländischen Produktionsstätten mit ein.

Dabei gilt auch in der Wissensgesellschaft die alte Warnung „Gelegenheit macht Diebe“. Das Sicherheitsprinzip „need to know“ – jeder erhält die Informationen die er benötigt, nicht mehr und nicht weniger – muss also stringent durchgesetzt werden. Dies hat oft weniger mit Technik zu tun, als mehr mit der Definition, welche Informationen welcher Mitarbeiter braucht. In jedem Fall lohnt es sich für ein Unternehmen, den Umsetzungsgrad dieses Prinzips in der eigenen IT zu prüfen. Gute Gradmesser für zu weitgehende Berechtigungen sind langjährige Mitarbeiter oder Praktikanten, die im Rahmen ihrer Ausbildung in verschiedenen Abteilungen des Betriebs eingesetzt wurden.

### Nur 13 Prozent loyale Mitarbeiter

Diese IT-Maßnahmen reduzieren das Risiko, bieten aber keinen zuverlässigen Schutz. Die Praxis zeigt, dass illoyale Mitarbeiter immer wieder Wege finden, technische Sicherheitssysteme zu umgehen. Laut Gallup Institut haben 20 Prozent der Belegschaft in deutschen Unternehmen innerlich schon gekündigt und würden bei einem besseren Angebot das Unternehmen sofort verlassen. Zwei Drittel machen „Dienst nach Vorschrift“ und nur rund 13 Prozent stehen ihrem Arbeitgeber loyal gegenüber.

Dies stellt eine massive Bedrohung und zugleich Herausforderung für Unternehmen dar. Aus diesem Grund konzentrieren sich Unternehmen nicht mehr so sehr auf Mitarbeiterzufriedenheit sondern auf Mitarbeiterloyalität. Mitarbeiterzufriedenheit lässt sich kurzfristig durch eine neue Kaffemaschine oder eine Gehalterhöhung erreichen, ist aber meist wenig verbindlich.

Mitarbeiterloyalität hingegen führt zu einer langfristigen Bindung zum Unternehmen. Der „Loyalitäts-Index“, der Münchner Sicherheitsberatung Corporate Trust, ist beispielsweise ein Werkzeug, um das Gefährdungspotential für eine Organisation systemisch zu ermitteln, die wichtigsten Handlungsfelder zu diagnostizieren und geeignete Interventionen abzuleiten. Er basiert auf einer Online-Mitarbeiterbefragung, aus der ein Loyalitäts-Index errechnet wird. Die Ergebnisse führen zu einer Analyse der Stärken und Schwachstellen, aus der dann geeignete Maßnahmen abgeleitet werden.

### Autoimmunsystem des Unternehmens

Dadurch gelingt es, in einer überschaubaren Zeit das „Autoimmunsystem“ des Unternehmens zu stärken. Aus Verantwortung für die eigene Aufgabe und aus Loyalität zum Unternehmen werden dann kritische Situationen, etwa fahrlässiger Umgang mit sensiblen Informationen oder auffälliges Verhalten von Kollegen identifiziert, angesprochen und entschärft.

Diese Aufmerksamkeit aus Verantwortung entsteht durch Loyalität mit dem Unternehmen (nicht aus Misstrauen gegen andere Personen) und ist neben allen technischen Werkzeugen, der wichtigste Schutz eines Unternehmens gegen sorglosen bis hin zu kriminellen Umgang mit Firmengeheimnissen.

Auch deutsche Unternehmen sollten sich die Berichte über den Geheimnisverrat in der US-Regierung eine Lehre sein lassen. Die regelmäßig notwendigen Prüfungen der Berechtigungssysteme auf Einhaltung des „need to know“ Prinzips sollten weniger als ein Jahr alt sein. Menschliche Probleme lassen sich aber nicht durch Technik lösen. Eine Steigerung der Mitarbeiterloyalität führt dabei nicht nur zu mehr Sicherheit, sondern erhöht auch die eigene Wettbewerbsfähigkeit.

## Mehr zum Thema

- Innentäter als Gefahr für Unternehmen: Tatort Arbeitsplatz
- Mitarbeiterkriminalität: Konfliktfrei geht es nicht
- Korruption: Der interne Feind als unterschätzte Gefahr
- Mitarbeiterkriminalität: Prävention und Repression
- Industriespionage: Mittelstand ist unzureichend geschützt

**Suchbegriffe:** Whistleblowing, Wikileaks, Geschäftsgeheimnisse, Informationsschutz, Staatsgeheimnisse, Forschung, Konstruktionspläne, Wettbewerb, Spionate, Industriespionage, Wirtschaftsspionage, Loyalität, Mitarbeiter, Korruption, Corporate Trust, Firmengeheimnisse, Know-how