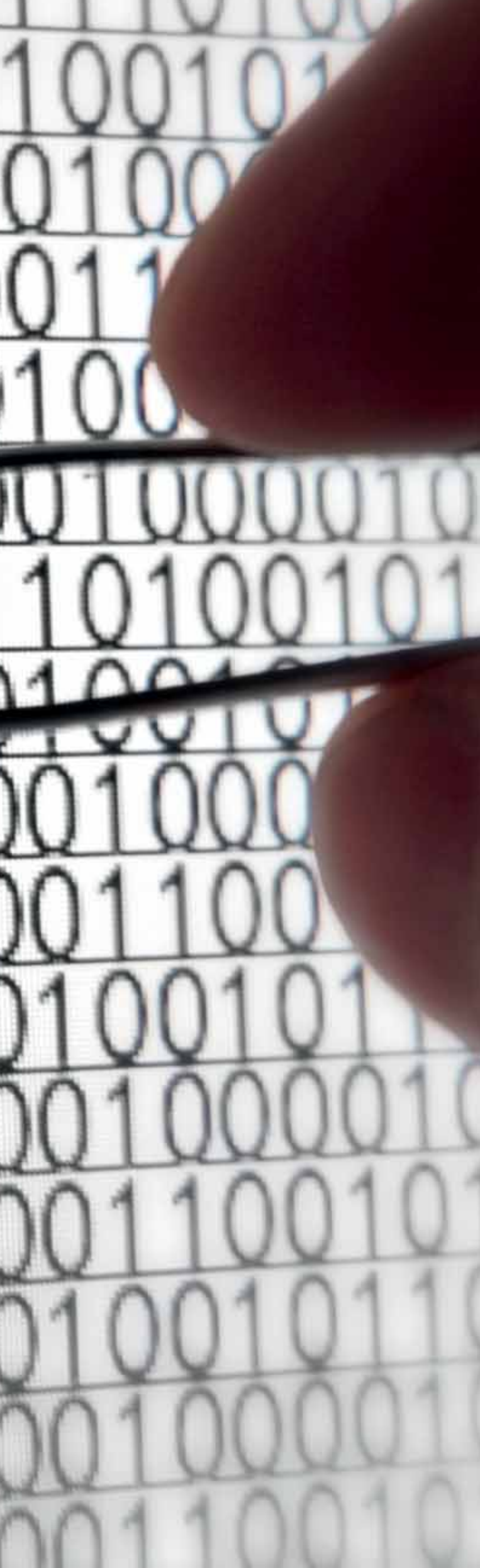




PASSWORD

# LOYALE MITARBEITER SIND DER BESTE DATENSCHUTZ

Gerade innovationsfreudige Unternehmen leiden nicht selten unter Kriminellen, die ihre Ideen klauen, illegal kopieren oder Daten an Mitbewerber verkaufen. Hundertprozentigen Schutz dagegen gibt es nicht – aber Schäden können zumindest minimiert werden.



---

## Von Ina Hönicke

---

Intercity München-Düsseldorf: Junge Männer im dunklen Zwirn schlagen sich in einem Großraumabteil begeistert auf die Schulter, weil der Termin bei einem Elektronikkonzern so erfolgreich war. Geradezu euphorisch besprechen sie jede Menge Details des neu entwickelten und jetzt gemeinsam zu vertreibenden Produkts. Dass dieses Gespräch besser nicht coram publico hätte über die Bühne gehen sollen, merken sie spätestens, als sie zu einem Gespräch bei ihrem Vorgesetzten zitiert werden.

Natürlich ist ein solches Öffentlichmachen von brisanten Details weder der Normalfall noch kriminell, sondern grob fahrlässig. Doch in einem erheblich größeren Umfang leiden Unternehmen unter echten Wirtschaftskriminellen, die Daten stehlen, sie sich illegal beschaffen oder verkaufen. Dabei zieht sich Wirtschaftskriminalität quer durch alle Branchen. Pharmafirmen bezichtigen Mitbewerber des Ideenklau bei neuen Medikamenten, IT-Unternehmen wie Nokia oder Microsoft werfen Konkurrenten Patendiebstahl vor und Handykonzerne wie Motorola wundern sich, wenn kurz nach Veröffentlichung eines neuen Designs Handys auftauchen, die ihrem eigenen Modell sehr ähnlich sehen. Eines steht fest: Es handelt sich in all diesen Fällen nicht um Kavaliersdelikte. Hier geht es um Geld, um sehr viel Geld. Der Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA) schätzt, dass allein seine Mitgliedsunternehmen jährlich einen Schaden von mehreren Milliarden Euro durch Produkt- und Markenpiraterie erleiden. Da aber der Erfindergeist von Unternehmen gerade in einem Land wie Deutschland überlebenswichtig ist, wird auch der Schutz vor Ideenklau und Nachahmung immer wichtiger.

„Kriegsgewinnler“ dieser misslichen Lage sind neben Sicherheitsfirmen vor allem Patentanwälte. „Hinter einer Erfindung steht immer mindestens eine Person“, erklärt der Münchener Patentanwalt Albrecht Dehmel. Handle es sich um einen Arbeitnehmer, sei dieser über das Arbeitnehmerfindergesetz verpflichtet, die Erfindung dem Arbeitgeber zu melden. Während Konzerne zumeist eine Rechts- oder sogar Patentabteilung unter ihrem Dach hätten, sollten kleinere Firmen rasch einen Patentanwalt einschalten. Denn von dem Zeitpunkt an, an dem die Patentanmeldung eingereicht ist, hat das Unternehmen einen Beleg, dass die Erfindung ihm gehört. „Trotzdem gibt es immer wieder Böswillige, die die Erfindung eines anderen Unternehmens nutzen“, erklärt der Patentanwalt. Um dagegen vorzugehen, brauche eine Firma gegebenenfalls viel Geld. Sei dieser finanzielle Background nicht vorhanden, kann es laut Dehmel durchaus auch mal angeraten sein, das Wissen über eine neue Idee im Unternehmen geheim zu halten. Der Patentanwalt: „Nach innen wird es nur der Abteilung bekanntgegeben, die es gerade benötigt, nach außen darf nichts dringen.“ Für Dehmel steht fest, dass es trotz diverser Schutzmaßnahmen die hundertprozentige Sicherheit gegen Ideenklau nicht gibt.

„Nach innen wird das Wissen über eine neue Idee nur der Abteilung bekanntgegeben, die es gerade benötigt, nach außen darf nichts dringen.“

Patentanwalt Albrecht Dehmel



Jörg Schecker, langjährig erfahrener Informationssicherheitsexperte und Inhaber von Pointhope, vergleicht Ideen mit einem Puzzle: „Ein Mitarbeiter hat nicht einfach eine Blitzidee, dahinter steht ein langer Entwicklungsprozess.“ Deshalb müssten alle Beschäftigten, die an der Entwicklung mitwirkten, dafür sensibilisiert werden, wie wertvoll und gefährdet selbst Teilinformationen sind. Kurzum: Wer darf welche Daten sehen, wie vertraulich müssen sie gehandhabt werden, inwieweit sind sie für Mitbewerber interessant?



Jörg Schecker, Informationssicherheitsexperte und Inhaber von Pointhope

Auf Basis dieser Risikobewertung können frustrierte Mitarbeiter, die ihren Arbeitgeber im Schlechten verlassen, nicht allzu viele Informationen mitnehmen und missbrauchen. „Hier kommt es darauf an, wie viel der Beschäftigte über ein neues Produkt weiß“, erklärt Schecker. „Besitzt er Informationen über die gesamte Prozesskette, kann er in der Tat großen Schaden anrichten.“ Handle das Unternehmen allerdings nach einem ausgewogenen „need to know“-Prinzip, kenne der Mitarbeiter nur die Details, die er für seinen Job benötige. Damit werde das Risiko minimiert. Das Gleiche gelte für Mitarbeiter, die gedankenlos, fahrlässig oder aus Überzeugung Daten an andere weitergeben. Fazit des Sicherheitsexperten: „Die Technik für den Schutz von Ideen ist vorhanden, die Verantwortung liegt allein beim Menschen.“

Wie aber reagieren Verantwortliche in den Unternehmen auf das Damoklesschwert des Ideenklau? Einhelliger Tenor der Befragten: Einen hundertprozentigen Schutz gibt es nicht, diverse Sicherheitsmaßnahmen dagegen schon.

So sollte der Kreis derer, die an neuen Entwicklungen teilhaben, nicht nur überschaubar gehalten werden, sondern die Beteiligten sollten auch vertrauenswürdig sein. Darüber hinaus sollten nicht alle Mitarbeiter Informationen über die gesamte Prozesskette, sondern nur über einzelne Schritte besitzen. Der beste Schutz, darin sind sich die Chefs einig, sind indes loyale Mitarbeiter. Letztlich würden die besten technischen Schutzmaßnahmen nichts nutzen, wenn die Beschäftigten unzufrieden sind. Fazit: Loyalität ist sicherer als jeder Datenschutz.

## GESCHÜTZT WIE IN FORT KNOX



Dass die Google-Algorithmen gehackt wurden, geistert zwar immer wieder als Gerücht durch die Internetwelt – bewahrheitet hat sich diese Information nie. Wenn es jemals dazu kommen würde, könnten sich viele Unternehmen warm anziehen. Schließlich basieren Millionen von ihnen auf den Services von Google. Eine „versehentliche“ Bekanntgabe der Geheiminformationen ist nicht zu erwarten, denn der Algorithmus wird durch ein ausgeklügeltes Sicherheitssystem geschützt.