

Firmen unterschätzen Datenklau

Geschäftsinformationen sind in IT-Systemen oft unzureichend geschützt. Neue Fahndungsmethoden helfen bei der Überführung von Tätern.

M. PISACANE | DÜSSELDORF

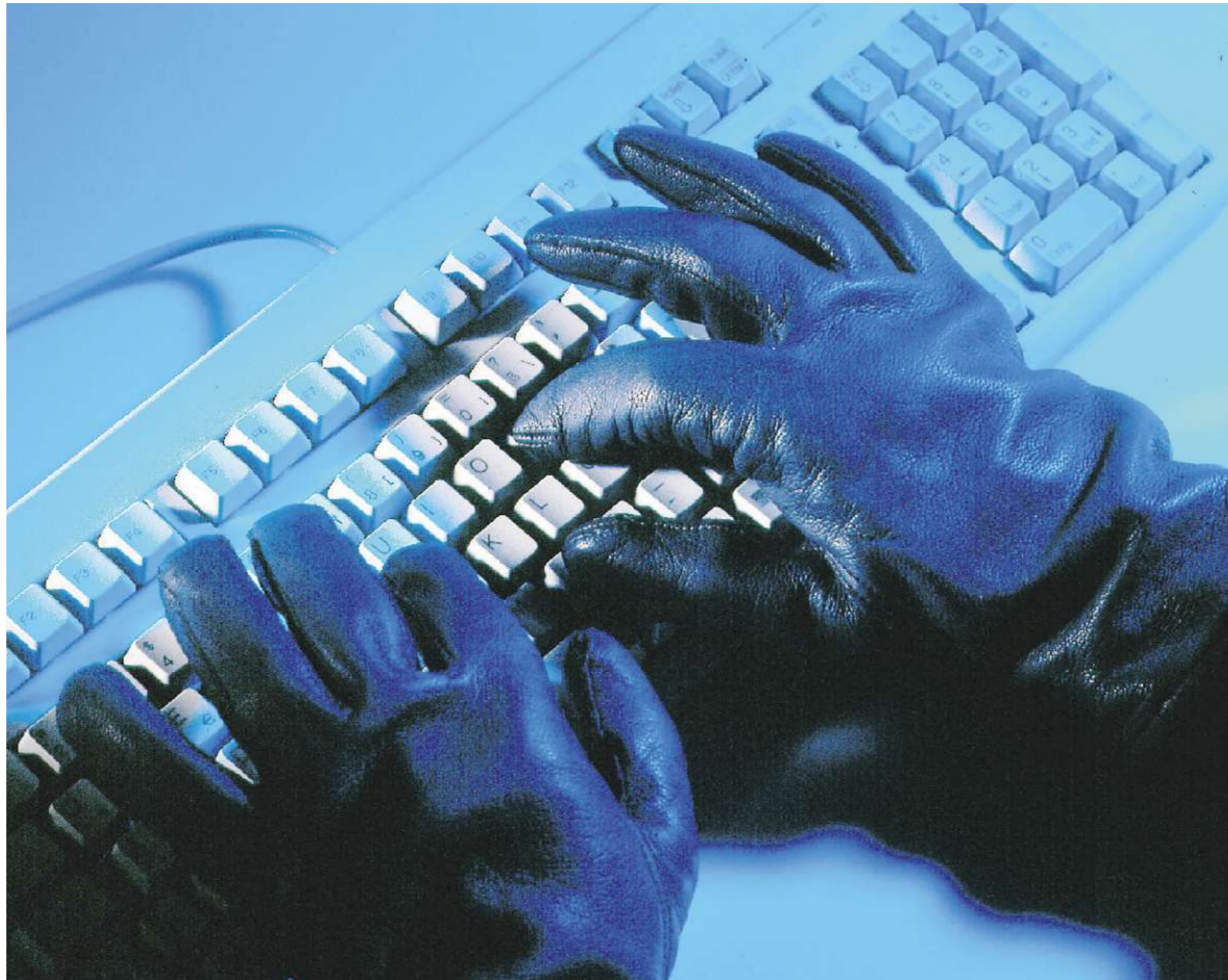
Alle waren überrascht, keiner hätte ihn verdächtigt. Schließlich galt er als sympathischer Kollege, schon sein Vater hatte für die Maschinenbau-Firma gearbeitet – bei kleinen und mittleren Unternehmen keine Seltenheit. Den Vertrauensvorschuss nutzte Oliver C. aus: Er verriet brisante Kunden- und Produktdaten an die Konkurrenz, ganz einfach per E-Mail.

Ein realer Fall, wie er in vielen Unternehmen vorkommen kann. Bei 13 Prozent der wirtschaftskriminellen Fälle im vorigen Jahr kam es zu Know-how-Verlusten durch Datenklau, ergab eine Studie der auf Krisenmanagement spezialisierten Result Group. Neben Diebstahl, Unterschlagung, Untreue und Betrug zählt dies zu den häufigsten Risiken für Unternehmen.

„Wir sehen häufig eine Mischung von Industriespionage, Veruntreuung und Diebstahl von Daten“, erläutert Reinhold Kern, Manager der auf Datenrettung und elektronische Beweissicherung spezialisierten Kroll Ontrack GmbH in Böblingen. „Selbst komplette Datenbank-Inhalte werden gestohlen.“

Diese Gefahr werde vor allem in kleinen und mittleren Unternehmen unterschätzt, beobachtet Steffen Salvenmoser, Experte bei der Prüfungsgesellschaft Pricewaterhouse-Coopers. Eine Untersuchung der Prüfungsgesellschaft KPMG ergab ebenfalls, dass es gerade in inhabergeführten Unternehmen an Risikobewusstsein mangle. Dass sich in der offiziellen Statistik mehr wirtschaftskriminelle Delinquenten bei den großen Firmen finden als bei Unternehmen mit weniger als 200 Mitarbeitern, liegt nach Ansicht der Experten daran, dass dort die Kontrollsysteme ausgefeilter sind.

Unternehmer sehen IT-Risiken oft an der falschen Stelle. „Viele denken bei Datensicherheit nur an Viren- und Hacker-Angriffe; dabei machen sie nicht den größten Schaden aus“, sagt Christian Götz, Geschäfts-



Diebstahl per Knopfdruck: Vor allem kleine und mittlere Unternehmen sind für diese Risiken nicht gerüstet.

fürer von Corporate Integrity Solutions, einer Ausgliederung der Wirtschaftsprüfungsgesellschaft Deloitte&Touche, die sich auf Prävention und Aufklärung von Wirtschaftskriminalität spezialisiert hat. Das bedeutet: Vor Angriffen auf IT-Systeme und Datenbanken von außen schüt-

zen sich Unternehmen zwar – doch die Täter kommen vielfach aus den Reihen der eigenen Mitarbeiter.

Ihnen wird der Datenklau über E-Mail, USB-Stick oder Handy einfach gemacht. Nach einer Studie des Marktforschungsunternehmens Dynamic Markets speichern 92 Prozent

der Manager unternehmenskritische Informationen auf ihren Handys oder PDAs. Manche Firmen gehen geradezu sorglos mit ihren Daten um, beobachtet Götz: So verkaufte eine Versicherung ihre alten Rechner samt Festplatte und damit allen gespeicherten Daten. Aber selbst wenn

Daten vorher gelöscht werden, sind sie noch vorhanden, können von Fachleuten auch nach einer Formatierung noch gelesen werden.

Um Schwachstellen aufzudecken, können Unternehmen Spezialisten für so genannte IT-Forensik engagieren. Die Anbieter haben mittlerweile

eine ausgefeilte Technik für die Aufklärung und Beweisführung im Verdachtsfall: Per Software können gelöschte Dokumente auf Computern verdächtiger Mitarbeiter wiederhergestellt werden. Forensische Analysen werten Festplatten, Handys oder E-Mail-Verkehr aus. Selbst große Datenmengen durchforsten die Programme nach Schlagwort-Verbindungen und spüren Daten auf, die gelöscht oder überschrieben wurden.

Ziel der IT-Forensik ist es, rechtswirksame Beweise zu bekommen. Oft sind solche neuartigen Analysen aber nur möglich, wenn im Unternehmen festgelegt ist, dass etwa E-Mail und Internet nur geschäftlich genutzt werden dürfen.

Vorsorgen können Unternehmen auch bei der Auswahl ihrer Mitarbeiter, wie Jens Hoffmann, Leiter des Instituts für Psychologie & Sicherheit in Darmstadt, unterstreicht. Hoffmann hat zusammen mit der Arbeitsstelle für Forensische Psychologie der TU Darmstadt und der Uni Regensburg einen „Psychologischen Integritätstest“ entwickelt – er soll potenziell weniger ehrliche Mitarbeiter erkennen helfen.

Ein probateres Mittel dürften aber Regelungen im Arbeitsvertrag sein, die erläutern, was erlaubt und was verboten ist – und in denen Konsequenzen genannt werden. Alles was nicht verboten ist, gilt juristisch gesehen als geduldet. Technisch kann das IT-System mit Zugangskontrollen und passwortgeschützten Zugriffsrechten sicherer gemacht werden. „Der direkte Kontakt zu den Mitarbeitern sollte aber nicht unterschätzt werden“, sagt Götz. „Eine Big-Brother-Mentalität ist kontraproduktiv; besser sind klare Verhaltensregeln, Kontrollsysteme und das richtige Maß an Vertrauen und Kontrolle.“



Text weiterleiten: Mail an forward@handelsblatt.com Betreff: **Risiken** (Leerzeichen) **17** (Leerzeichen) **Mailadresse des Empfängers**



Die Redaktion dieser Seite erreichen Sie unter hb.familienunternehmen@vhb.de

UNTERNEHMENSPRAXIS

MO FAMILIENUNTERNEHMEN

DI STRATEGIE

MI RECHT & STEUERN

DO MARKETING

IT-Kriminalität

Schwer zu messen

In der jüngsten Kriminalstatistik fehlen genaue Daten über Höhe und Auswirkungen des Verrats von Geschäfts- und Betriebsgeheimnissen in Deutschland. Experten sprechen von „erheblichen Schäden, die nur schwer quantifizierbar sind.“ Messbar ist aber das Risikobewusstsein: Laut Pricewaterhouse-Coopers hält es nur jedes fünfte deutsche Unternehmen für realistisch, Opfer von Wirtschaftskriminalität zu werden.

Täterprofile

Etwa die Hälfte aller Wirtschaftskriminellen kommt aus den Reihen der Mitarbeiter – das gilt auch beim Datenklau. Bei vielen Tätern sei eine „kalte Wut“ zu erkennen, sagt Jens Hoffmann, Leiter des Instituts für Psychologie & Sicherheit in Darmstadt. Täter hätten oft überzogene Ansprüche und würde die Taten lange planen.

Prävention

Prävention kann die Aufklärung von Datenklau deutlich erleichtern und Täter abschrecken. Folgende Fragen von Corporate Integrity Solutions helfen, Schwachstellen aufzudecken:

- Können Mitarbeiter es leicht schaffen, sensible Daten per E-Mail oder USB-Stick aus dem Unternehmen herauszutragen?
- Kann die Kundenkartei kopiert werden – von wem?
- Werden E-Mails regelmäßig gesichert. Dürfen Sie im Verdachtsfall auf E-Mail zugreifen?
- Werden alle WLAN-Anschlüsse geblockt?
- Werden Firmen-Laptops ausreichend verschlüsselt?