IHK Darmstadt Rhein Main Neckar

IHK REPORT 03-19

10 KONJUNKTUR
Boom schwächt sich ab

22 WIRTSCHAFTSSPIONAGE
Der Feind aus den eigenen Reihen

34 DIESELFAHRVERBOT
IHK fordert grundlegende Ausnahmen

MAGAZIN DER INDUSTRIE- UND HANDELSKAMMER
DARMSTADT RHEIN MAIN NECKAR

Raus aufs Land?

Seite 12
Problemfall Fläche

„Dass uns das eigene Mitarbeiter angetan haben, war ein Schock“

Bei Cyber-Attacken und Wirtschaftskriminalität denken die meisten zuerst an Hacker, Industriespione oder missgünstige Wettbewerber. Kaum jemand vermutet, dass der Feind aus den eigenen Reihen kommen kann. Eine vielfach unterschätzte Gefahr, wie Unternehmer Gerd Meyer-Philippi am eigenen Leib erfahren musste.

Foto: Compware Medical

Die Erkenntnis traf ihn mit voller Wucht: Dass seine eigenen Mitarbeiter die sensiblen Daten gestohlen haben, um ein preisgünstigeres Konkurrenzprodukt auf den Markt zu bringen – damit hätte Gerd Meyer-Philippi nie gerechnet. „Ich hätte für sie meine Hand ins Feuer gelegt. Schließlich waren zwei von ihnen schon elf Jahre bei uns“, sagt der geschäftsführende Gesellschafter von Compware Medical. So wie es der hessische Weltmarktführer für Methadon-Dosiersysteme erlebt hat, ergeht es vielen. Laut einer vom Digitalverband Bitkom und dem Bundesamt für Verfassungsschutz 2017 veröffentlichten Studie sind für fast zwei Drittel der in Unternehmen durch Datendiebstahl, Spionage und Sabotage entstandenen Schäden die eigenen Mitarbeiter verantwortlich.

Nicht immer geschieht das in böser Absicht. Aber wenn, dann haben Mitarbeiter Möglichkeiten, von denen externe Angreifer nur träumen können. Für die sogenannten Innentäter ist es einfach, an weiterführende Informationen, Verfahrensdokumentationen und Kundendaten heranzukommen. „Das hätte uns in den Ruin treiben können“, so Gerd Meyer-Philippi. Im Fall von Compware Medical war der Schaden besonders groß, weil sich vier Mitarbeiter aus unterschiedlichen Bereichen – ein Vertriebler und seine in der Verwaltung arbeitende Frau, ein Produktmanager und ein ehemaliger Azubi mit IT-Kenntnissen – zusammengetan haben. Glück im Unglück für den Mittelständler aus Gernsheim: Die Täter, die mittels der gestohlenen Daten ein Konkurrenzprodukt für Opiatabhängige entwickelt haben, brauchten ein Jahr, um das medizinische Gerät auf den Markt zu bringen.

Generalverdacht zerstört das Betriebsklima

„In dieser Zeit waren wir natürlich nicht untätig. Wir haben uns eine auf IT-Recht spezialisierte Anwaltskanzlei genommen, sind in die Öffentlichkeit gegangen und haben unsere Kunden kontaktiert“, erklärt Gerd Meyer-Philippi. Obwohl ein von Compware Medical beauftragter Datenforensiker den Diebstahl eindeutig nachweisen konnte und bei Hausdurchsuchungen der Polizei sensible Firmendaten auf dem Rechner eines Beschuldigten gefunden wurden, dauert der Streit bis heute an. Die Mühlen der Justiz mahlen langsam. Bisher wurde noch keiner der Täter verurteilt und das neue Konkurrenzunternehmen darf seine Produkte zu Niedrigpreisen weiter vertreiben.

Hilfe hat sich Compware Medical nicht nur bei IT-Spezialisten, PR-Beratern und Juristen geholt. Nach dem internen Datendiebstahl beauftragte der Mittelständler auch eine Psychologin. „In unserem Unternehmen herrscht eine sehr familiäre Atmosphäre. Wir duzen uns alle und essen jeden Freitag gemeinsam zu Mittag. Dass uns das eigene Mitarbeiter, die schon so lange bei uns sind, angetan haben, war ein richtiger Schock. Da kann man den Glauben an die Menschheit verlieren“, erzählt Gerd Meyer-Philippi. Doch genau das wollten er und Mitinhaber Günther Kalka nicht. Im Unternehmen wurden ein neues Sicherheitskonzept installiert und die Zugriffsrechte begrenzt, aber im Umgang mit den Mitarbeitern haben sie nichts geändert. „Wir haben ein gutes Betriebsklima und das wollen wir behalten.“ Alle Mitarbeiter zukünftig unter Generalverdacht zu stellen, würde das zerstören – und entspricht in vielen Fällen auch nicht der Wahrheit. Denn keinesfalls alle durch eigene Mitarbeiter verursachten Schäden passieren vorsätzlich.

Mitarbeiter müssen sensibilisiert werden

Oftmals sind es reine Nachlässigkeiten, die zum Verlust sensibler Unternehmensdaten führen. Sei es ein beim Geschäftstermin vergessener USB-Stick →

→ mit geheimen Firmendetails, lautstarke Gespräche über einen erfolgreichen Abschluss während der Zugfahrt oder der auf einer Dienstreise gestohlene Laptop, gespickt mit wettbewerbsrelevanten Kennzahlen. Weitere Sicherheitslücken sind digitale Geschenke, über die Hacker, wenn sie ans Unternehmensnetzwerk angeschlossen werden, Zugriff auf Firmeninterna erhalten können, oder mobile Privatgeräte, die viele Mitarbeiter für ihre Arbeit nutzen, die aber nur selten den Security-Anforderungen genügen.

Um diese oft auf Unachtsamkeit zurückzuführenden Risiken zu minimieren, müssen Unternehmen ihre Mitarbeiter im Umgang mit schützenswerten Daten regelmäßig sensibilisieren und schulen. Diese Präventivmaßnahmen können den Datenmissbrauch durch vorsätzlich handelnde Innentäter allerdings nicht verhindern. Daher gilt es zusätzlich einen guten Weg zu finden, Mitarbeiter in die Verantwortung zu nehmen, auffälliges Verhalten wie exzessives Drucken von Dokumenten, ungewöhnliche Datentransfers, verdächtige Kontakte zu Konkurrenzunternehmen zu melden – ohne jedoch eine Atmosphäre des Misstrauens zu schaffen. Gelingt das, ist der Faktor Mensch kein Sicherheitsrisiko, sondern erfolgreiche Spionageabwehr.

— feh

Liegt eine Datenschutzverletzung vor, müssen Unternehmen gesetzliche Vorgaben einhalten. Die IHK informiert über Melde- und Benachrichtigungspflichten und kann darüber hinaus Auskunft geben, ob eine Rechtsberatung durch einen Anwalt zu empfehlen ist, um im weiteren Verlauf die wirtschaftlichen Schäden so gering wie möglich zu halten.

↘ **www.darmstadt.ihk.de, Nr. 4029712**

Allgemeine Informationen zum Thema Wirtschaftsspionage und IT-Sicherheit stehen hier zur Verfügung:

↘ **www.darmstadt.ihk.de, Nr. 130360**

Illustration: Levente Janos, Fotolia

Arbeitsrecht

Arbeiten trotz Krankschreibung

Manche Krankheit ist schneller ausgeheilt als vermutet. Es besteht jedoch immer wieder Unsicherheit: Darf ein Arbeitnehmer nach einer Krankschreibung oder einer durch den Arzt bescheinigten Arbeitsunfähigkeit vorzeitig wieder an seinen Arbeitsplatz zurückkehren?

Ja, das darf er. Das gilt jedoch nur, wenn der Arbeitnehmer sich tatsächlich wieder fit genug für die Arbeit fühlt. Darüber entscheidet er nach eigenem Ermessen selbst – eine „Gesundschreibung" vom Arzt ist nicht erforderlich oder vorgesehen. Der Arbeitgeber hat kein Mitspracherecht und darf nicht zur vorzeitigen Rückkehr drängen. Sollte aber ein Arbeitgeber im umgekehrten Fall Bedenken haben, ob der Mitarbeiter tatsächlich wieder arbeitsfähig ist, kann er den Betriebsarzt zur Untersuchung hinzuziehen.

Ein Gerücht, dass sich in diesem Zusammenhang hartnäckig hält: Mitarbeiter, die trotz Krankschreibung zur Arbeit kommen, hätten keinen Versicherungsschutz. Das ist falsch. Wird ein Arbeitnehmer früher wieder gesund, als vom Arzt angenommen und bescheinigt, hat er vollen Versicherungsschutz am Arbeitsplatz und auf dem Arbeitsweg.

Information:
Andrea Freunscht
Arbeitsrecht, Insolvenzrecht, Vertragsrecht
T: 0 61 51 871 - 1307
E: andrea.freunscht@darmstadt.ihk.de

Vorsicht Falle

Domainregistrierung zum Schutz vor vermeintlichem Missbrauch

Immer wieder werden massenhaft E-Mails an Inhaber von Webseiten verschickt, die darauf hinweisen, dass ein anderer Nutzer Interesse an einer Domain mit gleichem Namen, jedoch einer anderen Endung, habe. Gegen eine Gebühr von 197,50 Euro plus Mehrwertsteuer, heißt es in diesen Schreiben, könne man sich den Eintrag für zehn Jahre sichern und vor Missbrauch schützen. Die jüngsten Angebote kamen von European Trademarks & Domains mit Betreff: „Ihre Domain-Erweiterung wurde beantragt" oder „Anfrage von einem Dritten erhalten". Verbraucherschützer warnen vor diesen Angeboten, denn sie seien Täuschungen und die dahinter steckenden Webseiten erwecken fälschlicherweise den Eindruck, es handele sich um eine Bundesbehörde.

Auf der Webseite der European Trademarks & Domain EUTD sind beispielsweise weder Impressum noch weitere Informationen zu finden. Vor einiger Zeit kamen die Mails von German Domain and Trademark Office. Solche Registrierungsangebote, bei denen sich der Anbieter noch nicht einmal offen durch ein ordentliches Impressum zu erkennen gibt, sind in der Regel unseriös, teuer – und gehören in den Papierkorb.

Information:
Isabelle Monz
Datenschutz, Handels- und Gesellschaftsrecht, Internetrecht
T: 0 61 51 871 - 1187
E: isabelle.monz@darmstadt.ihk.de