

## **Beispiel 1:**

Ein Mitarbeiter kopiert **unternehmensinterne Informationen** (Kundendatenbank, Entwicklungsunterlagen, Projektunterlagen, Vertragsunterlagen, Marketingpläne oder gar Fusionspläne ...) bevor er das Unternehmen verlässt, bewirbt sich bei einem Wettbewerber, will sich selbständig machen oder bietet die Informationen zum Verkauf an.

## **Beispiel 2:**

Ein Administrator erstellt sich die gleichen Profile (**Zugangsberechtigungen**) wie sie neuen Mitarbeitern u.a. einem neuen Entwicklungsleiter, eingerichtet werden, auf seinem PC. So erlangte er Zugang u.a. zu allen Entwicklungsunterlagen, die eigentlich nur dem neuen Entwicklungsleiter zugänglich sein sollten.

## **Beispiel 3:**

Einem Mitarbeiter fiel auf, dass sein Kollege sehr oft im Internet surft. Mit Einverständnis des Betriebsrates und des Datenschutzbeauftragten ließ man den PC dieses Mitarbeiters untersuchen. Wir fanden ca. 40.000 **pornographische Bilder und Videos**. Die meisten davon wurden nachweislich aus dem Internet geladen.

## **Beispiel 4:**

Im **Vorstand** werden Übernahmestrategien besprochen und entsprechend protokolliert. Zur großen Überraschung des Vorstandes tauchten genau diese Protokolle auch beim Übernahmekandidaten auf. Eine Untersuchung der PCs aller Vorstände und deren Assistentinnen ergab, dass eine Email mit angehängter Übernahmestrategie „versehentlich“ an eine falsche Emailadresse geschickt wurde.

## **Beispiel 5:**

Einem Mitarbeiter fiel die **hohe Einsatzbereitschaft** einer Chinesischen Kollegin auf, die auch noch lange nach Feierabend fleißig mit ihrem Notebook beschäftigt war. Erste Untersuchungen ihres Notebooks ergaben massenweise Daten, die sie eigentlich gar nicht haben sollte. Bei einer auf Basis unseres Berichtes, durch den der Verdacht erhärtet war, ergangene Strafanzeige und erlangte **Hausdurchsuchung** durch die Polizei, fanden sich neben weiteren 4 PCs bzw. Notebooks rund 70 gebrannte CDs mit hochbrisanten, mit CONFIDENTIAL gekennzeichneten Unternehmensinformationen.

## **Beispiel 6:**

Ein **Außendienstmitarbeiter** scheidet aus dem Unternehmen aus, löscht aber alle Daten seines Notebooks komplett – inklusive solcher Daten, die sonst nirgends mehr verfügbar waren – z.B. Kundendaten, Vertragsunterlagen, Absprachen ...

In einem unserer Fälle war das Notebook „versehentlich“ in einen Brunnen gefallen, in einem weiteren fiel das Notebook versehentlich vom Dach, bevor es zurück gegeben wurde.

## **Beispiel 7:**

Bei einem **insolventen Finanzmakler**, der mittlerweile in U-Haft saß, wurde vermutet, dass er verwaltete Kundeneinlagen veruntreut hat, denn der **Insolvenzverwalter** konnte keine Verwendungsnachweise über mehrere Millionen Euro finden. Vermögenswerteverchiebung? Eine Untersuchung seines PCs, der allerdings zwischenzeitlich von der Staatsanwaltschaft beschlagnahmt war, wir aber eine Kopie der Festplatte erhielten, erwies sich als Treffer. In den Internet Protokollen fanden sich u.a. Hinweise auf mehrfache Besuche von Webseiten von Immobilienmaklern in USA. Eine daraufhin konkrete Email Recherche brachte eine Email mit einem unterschrittsreifen Kaufvertrag über eine Villa in Florida (2,3 Mio. US \$) zutage.