

# VORSICHT: WENN DIE IT ZUM RÄTSEL WIRD

Mit den Jahren ist der Computer zum selbstverständlichen Begleiter am Arbeitsplatz geworden. Und zum vertrauten Geheimnisträger. Doch welche Gefahren ein bewährtes IT-System, das „doch immer ganz gut gelaufen“ ist, oder ein verloren gegangenes Notebook bergen, ist uns nur selten bewusst. Dabei kann der unvorsichtige Umgang mit der IT sogar die Existenz des eigenen Unternehmens bedrohen.



Stephan und Alexandra Henseler

Oft treten Sicherheitsvorfälle wie aus heiterem Himmel auf - und doch sind viele vorhersehbar. Häufigste Anlässe für einen Datenverlust sind nicht etwa ein Brand oder ein Einbruch, sondern Unvorsichtigkeit oder Sabotage durch Mitarbeiter. In Konsequenz kann dies zur Übermittlung von Betriebsgeheimnissen an direkte Mitbewerber oder gar zu schmerzenden Produktionsausfällen führen.

## Leichtsinn und Blauäugigkeit

Ein klassisches Beispiel: Der Entwicklungsleiter eines Unternehmens speichert aktuelle Projekte regelmäßig auf einem USB-Stick, um auch am Wochenende Daheim weiter daran arbeiten zu können. Doch dann verliert er den Stick. Gelangt er in falsche Hände, könnten so brisante Informationen in die Hände von Mitbewerbern gelangen - jahrelange Entwicklungen wären umsonst gewesen.

Ein anderes Beispiel: Ein Mitarbeiter lädt an seinem Arbeitsplatz zum privaten Gebrauch unerlaubt Dateien aus dem Internet herunter und lagert sie auf dem Datenserver der Firma zwischen. Wird er dabei erwischt, kann dies auch für das Unternehmen unangenehme Folgen haben: Dem Mitarbeiter droht ein Ermittlungsverfahren, für das die

Staatsanwaltschaft auch Teile der Unternehmens-IT zur Beweissicherung beschlagnahmen könnte.

## Das läuft doch, oder?

Diese Beispiele mögen extrem erscheinen und dennoch sollte man die Risiken nicht unterschätzen. Es reicht oft, sich einige gezielte Fragen zu beantworten, um häufige Fehlerquellen aufzudecken. Meist stellt sich dann heraus, dass der Unternehmer ganz sicher war, einen wirksamen Virenschutz zu besitzen oder regelmäßig eine Datensicherung durchzuführen - doch nie wurde geprüft, ob die Systeme auch wie gewünscht arbeiteten. Hier gilt es dann, nach einer sorgfältigen Abwägung von Kosten und Risiken, eine geeignete Lösung zu finden, um diese Fehlerquellen zu beseitigen.

Bei einer näheren Betrachtung rücken auch Themen wie beispielsweise der Betrieb der IT-Systeme und die Lizenzierung der eingesetzten Software in den Fokus. Abgesehen von veralteter und ungesicherter Software oder IT-Systemen, die schon an sich ein Risiko darstellen, werden schnell Einsparungspotenziale aufgedeckt. Oft ist festzustellen, dass zu viele Lizenzen vorhanden sind oder mehrere IT-Systeme aus Effizienzgründen zu-

sammengefasst werden könnten. Um als Geschäftsführer, Inhaber oder IT-Leiter einen schnellen Überblick über den aktuellen Stand zu bekommen, sollte man einen gründlichen Check-up durch Spezialisten durchführen lassen.

## Der Test beweist es

Bei dem von unserem Hause entwickelten „BIN-Control IT-Smart-Check“ etwa wird binnen zwei bis drei Tagen die gesamte IT eines Unternehmens analysiert und auf Sicherheitslücken sowie Optimierungspotenziale abgeklopft. So erhalten die Verantwortlichen eine Bestätigung der Funktionalität, einen rechtzeitigen Einblick über aktuelle oder potentielle Problemfelder und können darauf aufbauend die Risikominimierung planen und durchführen. ■

**Die Autoren sind Geschäftsführerin Alexandra Henseler und IT-Consulting-Leiter Stephan Henseler der BIN-Control GmbH in Wuppertal.**

**BIN-Control GmbH**  
**Hauptstraße 51a - 42349 Wuppertal**  
**Tel.: 0202/974646 0**  
**info@bin-control.com**  
**www.bin-control.com**