

Breitband / IT

## Cyber-Kriminalität – Warum ist Cyber-Sicherheit für jedes Unternehmen essentiell, Frau Bestmann?

„Das betrifft uns nicht“ und „Bei uns gibt es nichts zu holen, was sich lohnt“ – Antworten wie diese bekommt Julia Bestmann aus dem Fachbereich der AVW Unternehmensgruppe häufig zum Thema Cyber-Sicherheit zu hören. In diesem Artikel zeigt sie zwei Dinge auf. Erstens: Überall dort, wo digital gearbeitet wird, ist auch digital „etwas zu holen“. Zweitens: Die Folgen eines Hacker-Angriffs sind ernster, als die meisten von uns vermuten.



Julia Bestmann, Ass. jur. . Foto: AVW

In der Wohnungswirtschaft wird nicht mit Staatsgeheimnissen hantiert. Und dennoch: Sensible Daten haben Sie alle auf Ihren Rechnern. Ich bitte Sie, einmal in Gedanken die Informationen durchzugehen, die Ihr Unternehmen digitalisiert hat. Schriftverkehr, Mietverträge, Mieterdaten – in den Händen von Fremden hat nichts davon etwas zu suchen.

Was haben Sie digitalisiert?

### Datenklau und Vertrauensverlust

Bei personenbezogenem Datendiebstahl sind Sie verpflichtet, Ihre Mieter über den Datenabgriff zu informieren. Die erste Konsequenz: Ein enormer Vertrauensverlust. Und man muss eingestehen: berechtigterweise. Niemand möchte seine Anschrift und seinen vollständigen Namen, Geburtsdatum, gegebenenfalls Daten vom Ehepartner und Kindern in Kombination mit Informationen über Kontodaten und die monatlichen Mietzahlungen (und damit einem Anhaltspunkt zum Einkommen) in den Händen von Kriminellen wissen. Der Missbrauch der Daten für Online-Einkäufe ist eine der wahrscheinlichsten Konsequenzen. Doch der Umfang der personenbezogenen Informationen reicht aus, um noch weitreichender Identitätsbetrug zu begehen.

Missbrauch der Daten für Online-Einkäufe

### Schaden durch Betriebsausfall

Soweit die unangenehme Sichtweise Ihrer Mieter. Doch auch für Ihr Unternehmen ist es mit dem Schrecken nicht getan: Das verursachte Daten-Chaos sorgt mindestens für stundenweise Arbeits-Unterbrechungen. Legen Hacker Programme oder ganze Systeme lahm, muss Ihr Betrieb sogar bis zu mehreren Tagen zwangspausieren. Abgesehen von den Kosten für IT und Administration entsteht Ihnen so zusätzlicher Schaden durch Betriebsausfall. Auch an Ihre IT angeschlossene Hardware kann durch den Angriff beschädigt werden. Im schlechtesten Fall muss sie komplett ersetzt werden.

Daten-Chaos bei Serverausfall

### Haftungsrisiko steigt

Schon der drohende Verlust personenbezogener Daten löst eine Meldepflicht aus (§§ 42a, 43 BDSG): Behörde und Betroffene (in Ihrem Fall die Mieter) sind unverzüglich und effektiv zu informieren. Bei Missachtung droht je Vorfall ein Bußgeld in gesetzlich nicht limitierter Höhe. Das „IT-Sicherheitsgesetz“ vom 24.07.2015 hat die Anforderungen an IT-Sicherheit, Benachrichtigungs- und Meldepflichten weiter verschärft und die Ermittlungs- und Eingriffsbefugnisse des BKA im Bereich der Cyberkriminalität ausgebaut. Die derzeit im Entwurf befindliche EU-Datenschutz-GrundVO sieht weitere empfindliche Regelungen vor, wie zum Beispiel die Pflicht zur unverzüglichen Selbstanzeige an die Aufsichtsbehörden innerhalb von 24 Stunden mit einer Bußgeldandrohung in Millionenhöhe. Das Haftungsrisiko wird also in naher Zukunft spürbar größer.

Die AVW Unternehmensgruppe berät Sie gern persönlich: Wenden Sie sich an unsere Kundenmanager, um sich über die Präventionsmaßnahmen und die Versicherungsmöglichkeiten im Bereich Cyber Sicherheit und D&O zu informieren. Mehr zum Thema Versicherung von Immobilien finden Sie unter [www.avw-gruppe.de](http://www.avw-gruppe.de)

### IT-Sicherheit ist Chefsache

Doch nicht nur die Unternehmen treffen die hohen Strafen: Auch das Risiko für alle Geschäftsleiter wächst, ganz persönlich von den Bußverfahren getroffen zu werden. Eine D&O-Versicherung zum Schutz seiner Organmitglieder ist daher obligatorisch für jedes Unternehmen. Da die Konsequenzen einer möglichen Cyber-Attacke Chefsache sind, sollte es die IT-Sicherheit selbst auch sein. Und zwar als vollwertiges Segment des Risikomanagements – denn ihre Bedeutung wächst zunehmend: Haftpflichtexperten gehen davon aus, dass die Cyberversicherung in 10 Jahren schon auf Platz 3 hinter der Sach- und Haftpflichtversicherung stehen kann.

### Wie entstehen Sicherheitslücken?

Der größte Risikofaktor sind Ihre eigenen Mitarbeiter – doch das in der Regel absolut unbeabsichtigt. Unbedarfte genutzte USB-Sticks, versehentlich geöffnete Spam-Mails, privates Surfen auf schadhaften Websites – viele Situationen können der Türöffner für folgenschwere Viren und Malware allgemein sein. Interne Aufklärungsarbeit, Sensibilisierung und sinnvolle Regeln zum Umgang mit externen Datenträgern sind daher eine unumgängliche Ergänzung zu jedem digitalen Virenschutz.

Informationssicherheits-Managementsysteme wie ISO 27001 oder VdS 3473 bieten Unternehmen eine Richtschnur für Prozesse, mit denen sie sich angemessen vor Cyber-Gefahren schützen können – sowohl technisch als auch organisatorisch.

Ass. jur., Fachbereich HUK / Financial Lines, AVW Unternehmensgruppe

**Julia Bestmann**

## Wohnungswirtschaft *heute.*

Fakten und Lösungen für Profis

Sind sie schon regelmäßiger Leser von  
**Wohnungswirtschaft-*heute* Technik ?**  
wenn nicht, dann melden Sie sich *heute* an . . .