DEUTSCHER MITTELSTANDS-BUND

Digitalisierung | Internationalisierung | Finanzen | Nachfolge

Stefanie Lebek

Cyberkriminalität

Wirksame Datensicherung im Unternehmen

12. April 2019

Kontakt zur Redaktion:
Deutscher Mittelstands-Bund (DMB) e.V.
Grafenberger Allee 125
40237 Düsseldorf

www.mittelstandsbund.de
Tel. +49 (0) 211 / 2005 25-0
Fax +49 (0) 211 / 2005 25-99
Mail: info@mittelstandsbund.de

Herausgeber (V.i.S.d.P.):
Marc S. Tenbieg
Geschäftsführender Vorstand
meinung@mittelstandsbund.de

Stefanie Lebek[1]

Cyberkriminalität

Wirksame Datensicherung im Unternehmen

Ein neuer Mitarbeiter mit Bankvollmacht – gerne bei einer Auslandstochtergesellschaft – erhält eine E-Mail des Geschäftsführers, er möge einen fünfstelligen Betrag auf ein bestimmtes Konto überweisen. Es handele sich um ein wichtiges Geschäft, bei dem kurzfristig eine Anzahlung geleistet werden muss. Variante der Email: der Geschäftsführer stecke privat in der Klemme, er bitte um kurzfristige Überweisung eines Betrags, der auch schnell wieder ausgeglichen werden würde. Alles streng vertraulich. Nach einer ersten Email folgt nach einer Stunde eine weitere Email oder ein Anruf – wurde die Überweisung bereits ausgeführt?

Möglich ist auch, dass ein Lieferant per Email mitteilt, dass die Kontodaten geändert wurden und die Zahlungen in Zukunft auf die neue Bankverbindung erfolgen soll. Der arglose Mitarbeiter veranlasst die Überweisung – und erhält nach einem Monat eine Mahnung. Eine weitere Alternative ist, dass die Rechnung eines Lieferanten bezahlt wird, der gar nicht existiert.

Datensicherung durch Technik und Sensibilisierung der Mitarbeiter

Diese Vorfälle treten in letzter Zeit immer häufiger auf und gehen teilweise mit einem echten „Data Breach“ einher – dann, wenn echte Emailadressen verwendet werden. Es werden hier nicht nur IT-Systeme von außen gehackt, sondern insbesondere auch auf der psychologischen Kommunikationsebene – besondere Wertschätzung, Pflichtbewusstsein, Aufbau einer Drucksituation - gearbeitet. Dem aufmerksamen Mitarbeiter, der per Email nachfragt, wird bei einem echten Data Breach direkt von einer zwischengeschalteten Adresse des Cyberangreifers geantwortet und die Korrektheit der Anfrage bestätigt.

In einer Zeit, in der praktisch alle Daten elektronisch gespeichert und nicht immer ausreichend geschützt werden – wobei eine absolute Datensicherheit nicht möglich sein dürfte -, ist es also nicht nur erforderlich, in den elektronischen Schutz der Daten zu investieren. Es muss insbesondere auch durch die geeigneten Abläufe, Entscheidungsstrukturen sowie konsequente Sensibilisierung und Fortbildung der Mitarbeiter im Unternehmen sichergestellt werden, dass Angriffe dieser Art erkannt und entlarvt werden – bevor ein finanzieller Schaden entsteht, der zum Teil erheblich sein und selten behoben werden kann.

In diesem Zusammenhang wird die ganz praktische Bedeutung der Anforderungen der DS-Grundverordnung – hier insbesondere der Schutz der Daten durch geeignete technische und organisatorische Maßnahmen, das Verzeichnis der Verarbeitungstätigkeiten und die Risikofolgenabschätzung – einmal mehr deutlich.

---

[1] Dr. Stefanie Lebek ist Rechtsanwältin bei Derra, Meyer & Partner am Standort Mailand und berät in den Bereichen Internationales Arbeitsrecht und Internationales Recht - Schwerpunkt Italien.