wokatsch-felber
Professionelles Versicherungsmanagement

Cybercrime und Versicherung

Existenzielle Risiken für Unternehmer

„Es gibt nur zwei Arten von Unternehmen:
Solche, die schon gehackt wurden und solche, die es noch werden.“
Robert Mueller, Direktor des FBI, März 2012

Rechtliche Geheimhaltungsverpflichtung:

Gemäß Datenschutzgesetz haben **Auftraggeber, Dienstleister** und ihre **Mitarbeiter Daten** aus Datenanwendungen, die ihnen anvertraut werden, **geheim zu ha**lten, soweit kein rechtlicher Grund für eine **Übermittlung** der anvertrauten oder zugänglich gewordenen Daten besteht.

Datensicherheitsmaßnahmen:

Alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, **müssen Maßnahmen zur Datensicherheit** treffen. Dabei ist auf die Art der verwendeten Daten und nach Umfang und Zweck der Verwendung, sowie im Rahmen des Standes der techn. Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die **Daten** vor unrechtmäßiger Zerstörung, Verwendung und Verlust **geschützt** sind. Die Daten dürfen Unbefugten nicht zugänglich sein.

Mögliche Maßnahmen (Nachweis sicherstellen!):

- Aufgabenverteilung bei der Datenverwendung ausdrücklich festlegen
- Die Verwendung von Daten an das Vorliegen gültiger Aufträge der OE und Mitarbeiter binden.
- Jeder Mitarbeiter ist über seine nach dem Datensicherheitsgesetz und nach innerorganisatorischen Datenschutzvorschriften bestehenden Pflichten zu belehren.
- Die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleister regeln.
- Die **Zugriffsberechtigung** auf Daten und Programme und den **Schutz der Datenträger** vor der Einsicht und Verwendung durch Unbefugte regeln.
- Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und **jedes Gerät** durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen **gegen die unbefugte Inbetriebnahme abzusichern**.
- **Protokoll** führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.
- Eine **Dokumentation** über die getroffenen Maßnahmen führen.
- **DVR Nummer** auf allen Drucksorten und email-Signaturen anführen.

Aufbewahrungspflicht:

- Sofern gesetzlich nicht ausdrücklich anders angeordnet ist, sind Protokoll- und Dokumentationsdaten **drei Jahre lang** aufzubewahren.

Informationspflicht:

Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren!!

Diese Informationspflicht besteht nur dann nicht, wenn der Schaden der Betroffenen sicher nur gering sein kann oder die Kosten der Information einen unverhältnismäßigen Aufwand erfordern.

Wokatsch-Felber Versicherungsmakler GmbH
Versicherungsvermittler als Versicherungsmakler und Berater in Versicherungsangelegenheiten
A-3300 Amstetten | Ardaggerstraße 15
Tel. 0 74 72/621 56 | Fax 0 74 72/621 56 23
office@wf-versicherungsmakler.at
www.wf-versicherungsmakler.at
UID ATU 67079537 | FN377394t
Vermittlernummer AMW1-G-08499
BH Amstetten
DVR3004094

Rechtliche Konsequenzen:

Sind Daten entgegen den Bestimmungen des Datenschutzgesetzes verwendet worden, so hat der Betroffene Anspruch auf **Unterlassung** und **Beseitigung** des dem Datenschutzgesetzes widerstreitenden Zustandes.

Zur Sicherung der **Ansprüche auf Unterlassung** können einstweilige Verfügungen erlassen werden.

Ein Auftraggeber oder Dienstleister, der Daten **schuldhaft** (dh jeder Grad der Fahrlässigkeit reicht!) entgegen den Bestimmungen des Datenschutzgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden zu ersetzen. Auch wenn der Anwender es ermöglicht, dass aus seinem System

Der Anspruch auf angemessene Entschädigung für erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen.
Der Auftraggeber und der Dienstleister haften auch für das Verschulden ihrer Leute, soweit deren Tätigkeit für den Schaden ursächlich war.

Missbräuchliche Datenverwendung kann auch zu verwaltungsrechtlichen und strafrechtlichen Konsequenzen führen.

§ 126b StGB: Störung der Funktionsfähigkeit eines Computersystems
Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu 6 Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Versicherungsmöglichkeiten:

Schadenfälle:

- Ein **Online-Shop** wurde Opfer einer **„denial-of-Service-Attacke“**. Der Online-Shop war 23 h nicht verfügbar, da er von „Anfragen“ überflutet wurde. Schaden: 185.000,00
- **Hochregallager** mit **Virus** infiziert: Schaden 695.000,00
- **Stillstand der Produktion:** Durch böswillige Löschung der Entwicklungsdaten und Produktionsparameter einer gesamten Produktreihe: Schaden 1.775.000,00
- **Datenklau E**-Commerce: Über mehrere Monate konnten sich Hacker Zugang zu dem eigentlich streng gesicherten onlin-basierten Abrechnungssystem für Bezahlkarten verschaffen. Es wurden 2 Mio Kundendaten kopiert und unrechtmäßig genutzt: Schaden : 5.098.000,00

Lt. Studie KPMG bereits jedes 4. Unternehmen Ziel von Hackerattacken!

wokatsch-felber
Professionelles Versicherungsmanagement

Versicherungsmöglichkeiten:

I) Cyber-Haftpflichtversicherung

Schutz gegen Inanspruchnahme wegen

1. Datenschutzverletzung gemäß DSG:
   Ist jede Verletzung anwendbarer datenschutzrechtlicher Bestimmungen, wie bspw. Des DSG oder vergleichbarer inländischer oder ausländischer Rechtsnormen = unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Dritter.

2. Datenvertaulichkeitsverletzung gem. DSG:
   - Die unbeabsichtigte oder fahrlässige Veröffentlichung von Kundeninfo durch das UN oder einen externen Dienstleister.
   - Der unberechtigte Zugriff auf oder die unberechtigte Nutzung von Kundeninfo, die im System des UN gespeichert ist.

3. Freistellungsverpflichtungen gegen externe Dienstleister, betrifft 1) und 2)

4. Netzwerksicherheitsverletzung
   Ist jedes behauptete oder tats. Pflichtwidrige Tun oder Unterlassen eines Versicherten, das einen Netzwerkeingriff zur Folge hat. → Cyber/Hackerangriff

5. Verletzung eines veröffentlichten Payment Card Industry Data Security Standard (PCI oder PCI-DSS Kreditkarten):
   Versicherungsschutz für Ansprüche oder Forderungen zur Zahlung einer Vertragsstrafe, die wg. Eine Verletzung eines veröffentlichten PCI geltend gemacht werden.

6. Rechtswidrige Kommunikation
   Veröffentlichung von Inhalten, die unbeabsichtigt oder fahrlässig führen zu
   a) Verletzung Patenten, Markenrechten, Urheberrechten
   b) Rufschädigung, Beeinträchtigung der Persönlichkeitsrechte einer Person …..
   c) Verletzung des Wettbewerbsrechtes resultierend aus a) und b)

II) Cyber-Eigenschaden-Deckung

Versichert sollen sämtliche Aufwendungen werden, durch Schäden am eigenen System, insbesondere:

- Kosten für Computer-Forensik
- Kosten für die Anzeige und Bekanntmachung von Datenrechtsverletzungen
- Kosten für Kreditüberwachungsdienstleistungen
- Kosten für Krisenmanagement und Public-Relations-Maßnahmen
- Betriebsunterbrechung
- Wiederherstellungskosten
- Zahlung von Lösegeld aufgrund einer Cyber Erpressung
- Datenmanipulation (Überweisung von Geld)
- Kosten für Sicherheitsanalyse und Sicherheitsverbesserungen

III) Assistance bei Krisenprävention und Krisenmanagement (24h Hotline)