"Cyber-Risiken“

Kurzvortrag zum NFF-Unternehmerfrühstück am 3.11.2016

Das Fairsicherungsbüro

- Versicherungsmakler seit 35 Jahren
- Zusammenarbeit mit etwa 80 Versicherern
- 17 Angestellte, davon 14 in der Beratung tätig
- Nur Festangestellte, kein klassischer Außendienst

Eingangsfragen

- Benutzen Sie eine EDV?
- Speichern Sie Kundendaten?
- Sensible Kundendaten?
- Speichern Sie eigene Daten?
  - Mitarbeiterdaten?
  - Zahlungsdaten?
  - Geschäftsunterlagen?
- Wickeln Sie Geschäfte online ab?
- Haben Sie Mitarbeiter?
- Sind Sie schon einmal Opfer einer „Cyber"-Attacke geworden?

Ein paar Zahlen…

Allensbacher IfD-Umfrage „Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt?“:

- Täglich: 12%
- Mehrmals in der Woche: 8%
- Einmal in der Woche: 5%
- 2 – 3 mal im Monat: 10%
- Einmal im Monat: 9%
- Seltener: 43%
- Nie: 13%

Ein paar Zahlen…

- In 2012 lt. BKA 64.000 gemeldete Fälle in Deutschland
- Gesamtschaden 2011 lt. BKA 70,2 Mio. €
- Durchschnittsschaden bei KMU: 70.000,- €
- Sehr hohe Dunkelziffer
- Steigende Tendenz

Warum tun die das?

- **Kriminelle Energie** – jeder Datensatz bringt Geld, Konten werden leergeräumt, Lösegelder erpresst…
- **Als Racheakt** – ehemalige Mitarbeiter als Innentäter
- **Industrie-/Wirtschaftsspionage** – Wettbewerbsvorteile verschaffen
- **Zweckentfremdung des Serversystems** – „Spielepartys"
- **Vertuschung von Straftaten** – z.B. Nutzung des Serversystems für illegale Tauschbörsen
- **Hacken als Volkssport** - IT-Szeneprofilierung

Schadenbeispiel „Verschlüsselungssoftware“

- Mittels einer als Bewerbung getarnten E-Mail installiert sich ein Verschlüsselungstrojaner im IT System eines mittelständischen produzierenden Betriebes.
- Die Malware wird nicht sofort aktiv und infiziert neben den Rechnern auch die wöchentlich vorgenommen Backups.
- Mit Aktivierung der Schadsoftware wird der Datenbestand der Firma verschlüsselt. Die Rücksicherung aus aktuellen Backups scheitert, da diese bereits ebenfalls infiziert sind.
- Der Betrieb steht mehrere Tage still, da das System komplett neu aufgesetzt werden muss.
- Der Datenbestand kann in Teilen aus einer nicht betroffenen Sicherung zum Quartalswechsel hergestellt werden.
- Die nicht mehr vorhandenen Datenbestände müssen manuell nacherfasst werden.

Schadenbeispiel „Verschlüsselungssoftware“

- Kosten für forensische Untersuchung zur Ermittlung der Schadenursache und des Schadenumfanges sowie Unterstützung des IT Dienstleisters zur Datenrekonstruktion: 2 Forensiker, Tagessatz jeweils 1.500 EUR / 5 AT -> 15.000 EUR
- Ertragsausfall 25.000 EUR
- Manuelle Wiedereingabe der Daten durch die Mitarbeiter (Überstunden): 50 Stunden zu 35 EUR -> 1.750 EUR

Schadenbeispiel „Forderungen wegen Verletzung von PCI Standards“

- Mit Hilfe von an ein Hotel ausgelieferten Tastaturen werden Kreditkartendaten von ca. 5000 Hotelgästen ausspioniert. Die Tastaturen wurden im Vorfeld manipuliert und mit einem Datenlogger versehen.
- Wegen Verletzung der vereinbarten Datensicherheitsstandards machen Kreditkartenunternehmen vertraglich vereinbarte Strafen geltend.
- Zusätzlich werden die Aufwendungen für Monitoring und Benachrichtigung der betroffenen Kunden gegenüber dem Hotel geltend gemacht.

Schadenbeispiel „Forderungen wegen Verletzung von PCI Standards“

- Kosten für forensische Untersuchung zur Ermittlung der Schadenursache und des Schadenumfanges: 1 Forensiker, Tagessatz 1.500 EUR / 5 AT -> 7.500 EUR
- Vertragsstrafe: 125.000 EUR
- Schadenersatz für zusätzlichen Aufwand: 250.000 EUR
- Die betroffenen Kunden müssen benachrichtigt werden: 6 EUR je Datensatz -> 30.000 EUR

Schadenbeispiel „Weiterverbreitung eines Computer-Virus an Dritte“

- Über das IT-System des Versicherungsnehmers wird ein Computer-Virus unbewusst an die Firmenemail eines Geschäftskunden weitergegeben.
- Die Systeme des Betriebes werden dadurch für eine längere Zeit lahmgelegt.
- Gesamtschaden 164.000 EUR.

Schadenbeispiel „Verlust von physischen Datenträgern“

- Eine Mitarbeiterin einer Arztpraxis lässt auf dem Heimweg die auf CD durchgeführte Datensicherung in der U-Bahn liegen.
- Auf der CD waren ca. 10.000 Patientendaten.
- Gesamtschaden: 44.000 EUR.

Rechtlicher Rahmen

- Datenschutz als unternehmerische Pflicht (§ 91 Abs. 2 AktG / §§ 239 Abs. 4, Satz 2, 261 HGB)
- Deliktsrecht (§ 823 BGB)
- § 130 Abs. 1 i.V.m. §30 OWiG -> Haftung der Geschäftsleitung für Unterlassen von Aufsichtsmaßnahmen; Haftung des Unternehmens für Ordnungswidrigkeit (Geldstrafe bis € 1,0 Mio)
- Vertragliche Ansprüche (PCI = Payment Card Industry)
- Neue EU-Datenschutzverordnung 2012 (u.a. „unverzügliche Anzeigepflicht", höhere Strafen etc.)
- Schadenersatzansprüche für Geschädigte (§7 BDSG)

Probleme bei KMU

Fehlendes Know-how und Kapazitäten in den Unternehmen, um bei Datenpannen und Angriffen

- schnell
- rechtskonform
- effektiv

zu reagieren

Überforderung im Schadenfall

- was ist die Ursache?
- was ist zu tun?
- welche Daten sind betroffen?
- wer muss informiert werden?

Versicherungslösung

Bausteine:

- Cyber-Haftpflichtversicherung zur Absicherung bei Ansprüchen von dritter Seite, auch bei Verletzung von geistigem Eigentum/Persönlichkeitsrechten
- Cyber-Eigenschadenversicherung zur Abdeckung intern entstandener Schäden/Kosten
- Assistance im Versicherungsfall auf technischer und rechtlicher Ebene
- U.U. Präventive Beratung

Versicherungslösung

Versicherbare Kosten

- Kosten für IT-Forensik
- Betriebsunterbrechungsschäden
- Rechtsberatung
- Vertragsstrafen (PCI)
- Informationskosten
- Lösegeld
- Kreditüberwachungsdienstleistungen
- Wiederherstellungskosten
- Kosten für Krisenmanagement
- Sicherheitsverbesserungen
- Kosten für PR-Beratung

Empfehlung

Die Leistungen der am Markt angebotenen „Cyber"-Versicherungen unterscheiden sich stark. Es ist z.B. ein Unterschied, ob nur gezielte Angriffe auf Ihr Unternehmen versichert sind, oder auch der Fall, dass Sie zufällig Opfer werden.

Daher: Lassen Sie sich beraten!

Vielen Dank!