Cyber-Risiken - die unterschätzte Gefahr

Sind Sie vorbereitet, wenn es Ihr Unternehmen trifft?

Funk Versicherungsmakler GmbH
Johann Ulferts
07.06.2019

Ein neues Risiko

Die Hintergründe

Globalisierung

- Abbau von Handels-hemmnissen
- Schneller Datentransfer
- Automatisierung von Prozessen
- Höhere Produktivität

Neuer Wettbewerb

- Zusätzlicher Wettbewerbsdruck
- Kundenbedürfnisse und Erwartungen haben sich angepasst
  Bsp.: Onlineshops statt Kataloge / Lieferservices per App

IT als zentrale Ressource

- Neue Verantwortung
  Chief Technology Officer / Chief Innovation Officer
- Hohe Budgets für Innovationen und Teilhabe an Geschäfts-modellen

Neue Player

- Große Unternehmen sind ausgeschieden
  Kodak, Blockbuster
- Neue Giganten sind entstanden
  Google, facebook, Netflix, amazon

Cyber-Risiken

Die Ausgangslage

Täglich
werden rund 380.000 neue Varianten von Schadprogrammen entdeckt.
BSI 2016

43 Prozent der KMU
betrachten Cyber-Risiken als größte Gefahr für ihr Unternehmen

52 Prozent der Täter
sind aktuelle oder ehemalige Mitarbeiter.
Bitkom 2015

Cyberattacken werden dramatisch steigen.
Studien zählen Cyber-Risiken zu den **Top-Risiken der Zukunft**.

Die IT-Infrastruktur stellt heute das **zentrale Nervensystem** eines jeden Unternehmens dar.

Jedes 5. kleine oder mittlere Unternehmen
war bereits Opfer eines Cyber-Angriffs.
KMU-Studie 2019 (Gothaer)

EU-DSGVO - neue Spielregeln

Ein Korrektiv

Erwägungsgrund 1 - Datenschutz als Grundrecht

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Erwägungsgrund 13 - Berücksichtigung von Kleinstunternehmen sowie kleinen und mittleren Unternehmen

Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten sowie eine wirksame Zusammenarbeit zwischen den Aufsichtsbehörden der einzelnen Mitgliedstaaten gewährleistet.

Fazit

Die neuen Regelungen der EU-DSGVO stellen Verantwortliche vor große Herausforderungen, bedingt durch

- einen praktisch allumfassenden Anwendungsbereich,
- die Pflicht zur Errichtung bzw. Anpassung inner-betrieblicher Prozesse und
- - im wahrsten Sinne des Wortes - „abschreckende“ Geldbußen.

EU-DSGVO - Regelungen und Pflichten

Was Sie beachten müssen…

Grundsätze für die Verarbeitung personenbezogener Daten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Festgelegte, eindeutige und legitime Zwecke
- Richtigkeit & Datenminimierung

Rechtmäßigkeit der Datenverarbeitung:

- Einwilligung
- Vertragserfüllung
- rechtliche Verpflichtung
- Schutz lebenswichtiger Interessen
- Wahrung berechtigter Interessen

Rechte der Dateninhaber:

- Art. 13 Informationspflicht
- Art. 15 Auskunftsrecht
- Art. 16 Recht auf Berichtigung
- Art. 17 Recht auf Löschung
- Art. 21 Widerspruchsrecht

Art. 24 – Verantwortung des für die Verarbeitung Verantwortlichen:

- Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Art. 33 – Meldung von Datenschutzverletzungen:

- Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

EU-DSGVO - Haftung und Sanktionen

Welche Konsequenzen drohen…

Art. 82 - Haftung und Recht auf Schadensersatz

- Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein **materieller oder immaterieller Schaden** entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
- **Jeder an einer Verarbeitung beteiligte Verantwortliche haftet** für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde […].
- Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Art. 83 - Allgemeine Bedingungen für die Verhängung von Geldbußen

- Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall **wirksam**, **verhältnismäßig** und **abschreckend** ist.
- Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 **Geldbußen von bis zu 20 000 000 €** oder im Fall eines Unternehmens von bis zu **4 %** seines **gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
  - die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5 , 6, 7 und 9
  - die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22

Bislang festgesetzte Bußgelder

Bereits in 2018 gingen EU-weit ca. 55.000 Beschwerden zur DSGVO ein

Google Frankreich: 50.000.000 €

Informationen zur Verwendung der erhobenen Daten und dem Speicher-Zeitraum für Nutzer nicht einfach genug zugänglich. Zustimmung zur Anzeige personalisierter Werbung sei ungültig, weil Nutzer nicht ausreichend informiert würden. So sei die Vielfalt der beteiligten Google-Dienste wie YouTube, Google Maps oder der Internet-Suche nicht ersichtlich. Außerdem seien Informationen zur Verwendung erhobener Daten und dem Speicher-Zeitraum für Nutzer nicht einfach genug zugänglich. Nutzer müssten sich über diverse Links und Buttons Zugang zu den Dokumenten erarbeiten. Auch seien einige Informationen unklar formuliert.

Krankenhaus Barreiro Montijo: 400.000 €

Krankenhaus hatte laut Datenschutzaufsicht bewusst den Zugriff zahlreicher Nutzer auf Daten zugelassen, die eigentlich nur für Ärzte einsehbar sein durften. So seien insgesamt 985 aktive Benutzer mit dem Profil „Arzt“ registriert gewesen, obwohl lediglich 296 Ärzte in dem Krankenhaus beschäftigt waren. Dritten einen Zugriff auf solch sensible Informationen, wie Patientendaten, zu gewähren, stellte einen besonders groben Verstoß gegen die DSGVO dar.

Knuddels.de: 20.000 €

Nach Datenleak offenbarte sich, dass Passwörter unverschlüsselt / ungehasht gespeichert worden waren.

Kolibri Image: 5.000 €

Fehlen eines Auftragsverarbeitungsvertrags. Beauftragtes Dienstleistungsunternehmen, welches Kundendaten verarbeitet hatte, hatte trotz mehrfacher Anforderung keinen Vertrag zur Auftragsverarbeitung übersandt. Das auftraggebende Unternehmen erhielt schließlich das Bußgeld.

Österreich: 4.800 €

Betrieb einer Überwachungskamera, die unzulässigerweise auch gleich den Großteil des Gehsteigs überwachte. Auch hatte der Betreiber die Besucher nicht ausreichend auf die Kamera hingewiesen.

Risikotransfer

Die Cyber-Versicherung

Risikotransfer im digitalen Zeitalter

- Die IT ist heutzutage eine zentrale Unternehmens-Ressource. Hinterfragen Sie einmal selbst, welche Auswirkungen auch eine nur kurzzeitige Nichtverfügbarkeit der Unternehmens- und Kundendaten haben würde.
- Die Cyber-Versicherung bezweckt die Absicherung der Folgen einer Verletzung der Informationssicherheit - diese umfasst die Verfügbarkeit und Integrität von Daten sowie den vertraulichen Umgang damit.
- Erfahren Sie eine Absicherung im Falle von Eigen- und Drittschäden, ausgelöst durch Cyber-Attacken oder Datenpannen.

Ihre Mehrwerte:

- ☐ Sie schützen das, was zunehmend wichtiger wird: Eigene und fremde Daten.
- ☐ Sie stellen Ihr Unternehmen auf eine neue und komplexe Bedrohungslage ein.
- ☐ Der umfassende Kostenschutz stärkt Ihre Handlungsfähigkeit im Krisenfall.
- ☐ Der Risikotransfer unterstützt Sie bei der Implementierung innerbetrieblicher Prozesse aufgrund datenschutzrechtlicher Vorgaben und flankiert diese dauerhaft.

Häufige Missverständnisse

Welchen Schutz die Versicherung bezweckt und was ausgeschlossen ist.

- **Häufiger Irrtum:**
  Weit verbreitet ist die Auffassung, man benötige keine Versicherung, da die IT gut aufgestellt sei. Eine gute IT-Infrastruktur ersetzt aber keine Cyber-Versicherung, sondern ist - im Gegenteil - Voraussetzung zur Erlangung des Versicherungsschutzes.
- **Schutzzweck:**
  Die Cyber-Versicherung schützt Sie, wenn aufgrund einer Informationssicherheitsverletzung Kosten entstehen. Informationssicherheitsverletzungen können aus kriminellen Handlungen sowie eigenen Fehlern resultieren.
- **Kein Schutzzweck:**
  Die Cyber-Versicherung ist keine „Software-Versicherung“ und umfasst daher keine Schäden infolge nicht funktionierender bzw. inkompatibler Computerprogramme bzw. -systeme.

Ausschlüsse:

- Systemausfall durch Inkompatibilität oder Softwareoptimierungen
- Umstellung auf neue informationstechnische Abläufe oder Computersysteme, Erprobung , Wartungs-arbeiten oder Notfallübungen
- Nicht betriebsbereite, unerprobte oder unberechtigt genutzte Daten und Programme
- Versicherungsansprüche im Zusammenhang mit wissentlich unrechtmäßig erhobenen Daten

Leistungsumfänge und Inhalte

Für welche Fälle Sie gewappnet sind…

Versicherte Gefahren – Typische Schadenursachen

- Netzwerksicherheitsverletzungen - z. B.:
  - Zugriff auf das Computersystem durch Nichtberechtigte oder Berechtigte in Schädigungsabsicht
  - Übertragung von Schadprogrammen in das eigene Computersystem oder in dasjenige Dritter
  - Denial-of-Service-Attacken (Nichtverfügbarkeit von Computer-systemen durch eine künstlich hervorgerufene System-Überlastung)
  - Löschung, Unterdrückung, Veränderung von gespeicherten Daten Dritter
  - Zerstörung, Beschädigung, Abhandenkommen des Computersystems - durch Mitarbeiter oder Dritte
- Datenschutz- und Vertraulichkeitsverletzungen
- Verletzung von Benachrichtigungspflichten
- u.v.m.

Versicherungsumfang – Praxisrelevante Positionen

- Kosten für die Wiederherstellung der IT
- Kosten für die Inanspruchnahme von IT-Forensikern, Rechtsanwälten und Sicherheitsberatern
- Kosten zur Benachrichtigung von Behörden und Betroffenen im Falle einer Datenschutzverletzung
- Ertragsausfallschäden
- Schadensersatzansprüche Dritter
- Kostenschutz bei Straf- und Ordnungswidrigkeiten-verfahren aufgrund von Datenschutzverletzungen
- Ersatz des Verlustes von Geldern im Falle von Cyber-Diebstahl oder -Erpressung

Versicherungsoptionen - worauf Sie achten sollten

Highlights

Präventive Kosten

Bei Datenvorfällen entstehen häufig Kosten, bevor die Ursache dafür abschließend geklärt ist (z.B. IT-Dienst-leistungen). Diese Kosten sind bereits im Verdachtsfall abgesichert, auch wenn sich im Nachhinein herausstellt, dass der Auslöser gar kein versichertes Ereignis war.

Weitgehender Verzicht auf den Selbstbehalt

z.B. bei Dienstleistungs- und Beratungskosten, Benachrichtigungskosten, Präventiven Kosten, Kosten zur Abwehr von Haftpflichtansprüchen oder Kosten im Rahmen von Straf- und Ordnungswidrigkeitenverfahren

Pauschalisierter Betriebsunterbrechungsschaden

Je Ausfalltag wird in Höhe von 1/365 des Umsatzes des letzten Kalenderjahres erstattet.

Beweiserleichterung

Die Beantwortung der Frage, ob ein Schaden auf ein versichertes Ereignis zurückzuführen ist, kann komplex sein. Daher gilt eine Beweiserleichterung als vereinbart. Hierbei unterwirft sich der Versicherer der Feststellung des eingeschalteten Dienstleisters darüber, ob der Schaden mit überwiegender Wahrscheinlichkeit aufgrund einer versicherten Gefahr eingetreten ist.

Was passiert im Schadenfall?

Support durch exklusive Dienstleister-Netzwerke

- Im Schadenfall muss sofort gehandelt werden, damit sich Nachteile nicht verfestigen und Schäden kein noch größeres Ausmaß annehmen. Betroffene müssen schnell wieder auf ihre Daten zugreifen können und Datenabflüsse müssen effektiv gestoppt werden.
- Wir schalten daher Dienstleister ein, die Herr der Lage sind und wissen, was zu tun ist. Bereits im Verdachtsfall muss den Betroffenen ein - permanent verfügbarer - Zugang zu einem professionellen IT-Dienstleister gewährt werden.
- Dieser Dienstleister koordiniert regelmäßig ein ganzes Dienstleister-Netzwerk, bestehend aus renommierten Rechts- und Krisenberatern. So erhalten Betroffene den entscheidenden Support, sei es fernmündlich oder direkt vor Ort.
- Schadenfälle werden dadurch frühzeitig koordiniert, eingedämmt und schließlich behoben. Idealerweise übernimmt die Versicherung auch die zeitweilig entstandenen Kosten, wenn sich später herausstellt, dass für die Störung doch kein versichertes Ereignis ursächlich war.

Verhalten im Schadenfall

Was zu tun ist…

- Handeln Sie besonnen; idealerweise nach Maßgabe eines vorab erarbeiteten Notfall-Management-Plans.
- Binden Sie die - für die IT verantwortlichen - Mitarbeiter und Dienstleister ein.
- Prüfen Sie mögliche Sofortmaßnahmen.
- Versuchen Sie, mögliche Beweise zu sichern.
- Prüfen Sie, ob und inwieweit der Vorfall Benachrichtigungspflichten ggü. Behörden und Dateninhabern auslöst.
- Im Falle einer Erpressung - Stellen Sie Kontakt zu den Sicherheitsbehörden her und erstatten Sie Anzeige.

Die Cyber-Erpressung

Schon jetzt ein Klassiker

- Immer wieder erpressen Kriminelle die Unternehmen mit der Verschlüsselung von Daten. Sie bieten daraufhin eine Entschlüsselung an, aber nur gegen Zahlung eines Lösegeldes.
- *„Unsere ‚business first, security second'-Einstellung machte es den Angreifern enorm leicht, unsere IT-Systeme zu kompromittieren." (CFO)*
- *Ein Schadenfall aus 2018 zeigt, was genau einem etablierten mittelständischen Unternehmen passiert ist…*

Der IT-Abteilung fällt eine Unregelmäßigkeit bei der Serverauslastung auf. Kurz darauf fällt der Mail-Server kurzzeitig aus.

Am nächsten Morgen dann der Schock! Es wird festgestellt, dass die Daten auf 17 von 22 Servern vollständig verschlüsselt worden sind. Auch die Back-Up-Dateien sind davon betroffen.

Das Unternehmen entscheidet sich zunächst gegen die Zahlung des geforderten Lösegeldes. Da jedoch keine passende Decryptor-Software aufzutreiben ist, tritt man in Verhandlungen mit den Erpressern ein. Hierzu wird eigens ein spezialisierter Unterhändler beauftragt. Wenigstens die Laptops können zwischenzeitlich „gereinigt" werden, auch ein Not-Server wird angeschafft. Immerhin kann dadurch die Kommunikation mit den Kunden wieder aufgenommen werden.

Die Verhandlungen des Unterhändlers sind erfolgreich und die IT-Abteilung erhält ca. 7 Tage nach der Attacke den Entschlüsselungs-code. Die Entschlüsselung dauert weitere 48 Stunden. Erst 10 Tage später kann die Geschäftstätigkeit wieder aufgenommen werden.

Aktuelle Schadenfälle

Kunden in der Immobilienwirtschaft

Verschlüsselung nach **Öffnen eines „Bewerbungs-anhangs“**. Der Dienstleister konnte den Schadenfall inzwischen abschließen. Die gute IT-Sicherheit beim Betroffenen hat den Schaden verhältnismäßig gering ausfallen lassen. Schadenhöhe: **3.312 €**

Beginnende **Verschlüsselung eines E-Mail-Servers**. Durch rechtzeitiges Erkennen konnte dieser sofort vom Netzwerk getrennt werden. Eine Rücksicherung des Servers verhinderte einen noch größeren Schaden. Schadenhöhe: mind. vierstellig / **Arbeitsaufwand: 36,5 h**

Falsch aufgespieltes Update legt das Computersystem lahm. Es wurde bei der Installation versehentlich ein zweiter Datenbankserver installiert. Beide beanspruchten entsprechende Ressourcen und behinderten sich teilweise gegenseitig. Der Schaden wird aktuell reguliert. Schadenhöhe: mind. vierstellig / **Arbeitsaufwand: 20-25 h**

Verschlüsselung des Terminalservers durch bislang nicht identifizierten Eintrittspunkt der Schadsoftware beim Kunden. Auch die Sicherungskopie (Back-Up) wurde mit verschlüsselt, was den Schaden vergrößert hat. Schaden ist noch in Bearbeitung, erwartet werden Kosten für die Datenwiederherstellung, Forensik sowie Mehrkosten durch Wiedereingabe von Daten in das System.
Schadenhöhe: mind. vierstellig

Das Risikomanagement

Risiken erkennen und reduzieren

Top Risiken

- Mitarbeiter sind nicht ausreichend geschult, um mit Angriffen korrekt umzugehen
- Oftmals einmalige oder sogar gar keine Investition in IT-Sicherheit (Antivirensoftware, Firewall)
- Nur ein (unsicheres) Passwort für alle Geräte/Konten
- Fehlender Überblick über Geräte und Infrastruktur
- Keine Sicherheitsabläufe etabliert
- Keine IT-Abteilung bzw. kein IT-Verantwortlicher
- Regularien - Überblick über Gesetze und Vorgaben ist schwierig

Risikovermeidung

- Eingesetzte Technologie korrekt konfigurieren
- Umfassende Sicherheitsstrategie mitsamt Verantwortlichkeiten und regelmäßige Überprüfung
- Schwachstellen erkennen und umgehend schließen
- Datensicherungskonzept, Zutrittskontrolle und Datenschutzerklärung
  (für Mitarbeiter, Partner und Dienstleister)
- Regelmäßige Sicherung von Geschäfts- und Kundendaten
- Sichere Entsorgung von Informationen
  (Papier und Datenträger)

Funk CyberProfessional für Mitglieder des IVD

Prämientableau*

Vers.Summe	SB	Umsatzgröße bis max.				
100.000 €		250.000 €	500.000 €	1.000.000 €	2.500.000 €	5.000.000 €
	1.000 €	380 €	440 €	510 €	----- €	----- €
	2.500 €	320 €	380 €	440 €	570 €	----- €
Vers.Summe	SB	Umsatzgröße bis max.				
250.000 €		250.000 €	500.000 €	1.000.000 €	2.500.000 €	5.000.000 €
	1.000 €	530 €	590 €	680 €	----- €	----- €
	2.500 €	470 €	520 €	600 €	740 €	890 €
Vers.Summe	SB	Umsatzgröße bis max.				
500.000 €		250.000 €	500.000 €	1.000.000 €	2.500.000 €	5.000.000 €
	1.000 €	680 €	790 €	950 €	----- €	----- €
	2.500 €	630 €	710 €	870 €	1.170 €	1.390 €
Vers.Summe	SB	Umsatzgröße bis max.				
1.000.000 €		250.000 €	500.000 €	1.000.000 €	2.500.000 €	5.000.000 €
	1.000 €	----- €	1.180 €	1.340 €	----- €	----- €
	2.500 €	----- €	1.110 €	1.250 €	1.500 €	1.770 €
Vers.Summe	SB	Umsatzgröße bis max.				
2.000.000 €		250.000 €	500.000 €	1.000.000 €	2.500.000 €	5.000.000 €
	2.500 €	----- €	----- €	1.700 €	2.030 €	2.450 €
	5.000 €	----- €	----- €	1.620 €	1.940 €	2.350 €

* zzgl. Versicherungssteuer 19 %

Ihre Ansprechpartner

Funk Gruppe | Valentinskamp 20 | 20354 Hamburg | funk-gruppe.com

Bernhard Schwanke
Geschäftsführer Funk Versicherungsmakler GmbH
fon +49 40 35914-228 | fax +49 40 3591473-228 | b.schwanke@funk-gruppe.de

Johann Ulferts
Referent der Geschäftsführung
fon +49 40 35914-487 | fax +49 40 3591473-487 | j.ulferts@funk-gruppe.de

Werte für die Zukunft bewahren.
Die beste Empfehlung. Funk.