Risikoschutz

Das Plus für mehr Datensicherheit.
Die Cyber-Police.

Die optimale Lösung gegen Internetkriminalität

Warum ist eine Versicherung gegen Internet-Kriminalität wichtig?
Die rasanten Entwicklungen in der Informations- und Kommunikationstechnik bieten nicht nur Chancen, sondern auch völlig neue Risiken – unabhängig von der Größe oder Branchenzugehörigkeit der Betriebe:

- Immer mehr Kriminelle verschaffen sich Zugang zu Netzwerken von Unternehmen. Dabei werden nicht nur vertrauliche Daten gestohlen, sondern oft auch die gesamte EDV-Technik lahm gelegt.
- Fehler von Mitarbeitern führen oft zu Ansprüchen Dritter z. B. wegen Urheberrechtsverletzung.
- Eine wachsende Anzahl von Datenschutz-Anforderungen bergen zusätzliche Risiken.

Welche Daten sind betroffen?
Die über IT-Systeme verwalteten Daten in Unternehmen sind vielschichtig:

- Kunden- und Mitarbeiterdaten.
- Produktdaten, Konstruktionspläne oder Patentanmeldungen.
- Kassen- und Kreditkartendaten.
- Angebots- und Abrechnungsdaten.
- Dokumente, Korrespondenzen.

Ein Ausfall der IT-Systeme führt zu erheblichen Aufwänden.

Unsere Lösung: Die Cyber-Police.
Die Cyber-Police schützt Unternehmen nicht nur vor den wirtschaftlichen Folgen von IT- und Cyberrisiken. Im Schadenfall stehen Ihnen über unsere Experten-Hotline IT-Spezialisten an Ihrer Seite und leisten Ihnen schnelle und unbürokratische Hilfe. Selbst wenn sich herausstellt, dass es sich um kein ersatzpflichtiges Ereignis handelt, ist dieser Service für Sie kostenfrei. Gemeinsam mit Ihnen leiten sie die notwendigen Maßnahmen ein.

Welche Unternehmen sind besonders gefährdet?
Versicherungsschutz benötigen alle dienstleistenden, produzierenden oder verarbeitenden Unternehmen. Insbesondere Untenehmen und Freiberufler,

- die mit vertraulichen Daten umgehen
- deren Unternehmensabläufe von der IT abhängen oder
- deren IT für den Unternehmenserfolg von wesentlicher Bedeutung ist.

Vorteile der Cyber-Police.

- ✓ Im Schadenfall schnelle und unbürokratische Hilfe über unsere Experten-Hotline (Forensiker)
- ✓ Übernahme der Kosten für Ursachenermittlung, Behebung der Schadenursache und Rekonstruktion von Daten und Systemen nach einem Hackerangriff.
- ✓ Mitversicherung von Mehrkosten- und Ertragsausfällen aufgrund Betriebsunterbrechung.

W&W württembergische
Der Fels in der Brandung.

Die Cyber-Police.
Beispiele aus der Praxis.

Es kann jeden treffen, z. B.

- Internet-Kriminelle verschaffen sich Zugang zu den Kreditkarten- und Bankdaten aus dem Ticket-Server eines Konzertveranstalters. In den kommenden Wochen buchen Unbekannte mehrfach Beträge von den Kreditkarten-Konten der Rock-Fans ab. Alle Kunden müssen angeschrieben und auf den Diebstahl hingewiesen werden. Der Ticketserver muss neu aufgesetzt und gesichert werden und Schadenersatzforderungen stehen auch noch aus.

- Eine Firma bietet Telekommunikations-Anlagen und -Geräte sowohl über den Einzel- und Großhandel als auch online an. Über einen Zeitraum von 5 Tagen wird der Firmen-Server über einen Denial-of-Service (DoS)-Angriff (absichtlich herbeigeführte Serverüberlastung) zum Absturz gebracht, sodass keine Geschäftsabwicklung mehr möglich ist. Neben dem Ertragsausfall entstehen Kosten für die Beendigung des DoS-Angriffs und der Verhinderung weiterer Angriffe.

- Über soziale Netzwerke werden gezielt Mitarbeiter ausgespäht, um auf sie zugeschnittene E-Mails versenden zu können, die einen Trojaner beinhalten. Dieses „Spear Phishing“ ist eine gezielte Angriffsmethode gegen ausgesuchte Personen wie z. B. Mitarbeiter mit Administratorenrechten oder Mitglieder der Führungsebene eines Unternehmens. Eine Sensibilisierung der Mitarbeiter hinsichtlich der Methoden des Social Engineering ist daher erforderlich.

- Von einem Hacker wurden die Kreditkartendaten von Hotelgästen abgefangen. Wird der vorgegebene Standard der Kreditkartenindustrie nicht eingehalten, kann es zusätzlich zu empfindlichen Forderungen kommen. Und natürlich wird die Reputation eines Hauses dadurch beeinträchtigt.

- Die Gäste eines Restaurants und Nutzer einer Kreditkarte sind unbemerkt Opfer einer großangelegten Datenklau-Attacke geworden. Shoppingtouren in New York, die die Kreditkarteninhaber niemals tätigten, wurden von ihren Karten abgebucht. Alle Geschädigten hatten zuvor in dem Restaurant mit Kreditkarte bezahlt. Das IT-System des Restaurants war so manipuliert, dass beim Einlesen der Karten die Daten entwendet und auf neue Karten überspielt wurden. Entweder haben Hacker das Virus eingeschleust oder ein entsprechend präparierter USB-Stick wurde in einem unbemerkten Moment an die Kasse angeschlossen, um das Schadprogramm aufzuspielen. Der Virus konnte trotz langwieriger Arbeiten nicht aus dem IT-System entfernt werden, die Hardware musste ausgetauscht werden.

- Das Softwaresystem eines Unternehmens wird gehackt. Die Hacker suchen gezielt Orginal-Rechnungen von Lieferanten und leiten den Rechnungsbetrag durch Manipulation der Rechnung auf ein fremdes Konto um. Die E-Mail-Adresse des Lieferanten wurde dabei nur um ein Zeichen abgeändert, sodass der Mitarbeiter im Unternehmen das übersehen hat.

- Unbekannte hatten sich Zugang zum EDV-System eines Online-Reifenmarktes verschafft und einen Trojaner eingeschleust, der alle Daten auf dem Server verschlüsselte. Sie forderten ein Lösegeld für die Entschlüsselung. Der Unternehmer schaltete einen Computerfachmann und die Kripo ein, die dringend von der Bezahlung der Lösegeldforderung abrieten. Stattdessen musste der Trojaner entfernt und die vorhanden Datensicherungen neu aufgespielt werden. Der Betrieb stand 5 Tage still und es hat weitere 4 Tage gedauert, bis das System wieder störungsfrei arbeitsfähig war.

Versicherungsumfang.

Versichert ist die Informationssicherheitsverletzung. Dazu gehören:

1. Verletzungen der Netzwerksicherheit

- Zielgerichtete Verletzung der Netzwerksicherheit durch
  - eine Übermittlung von Schadsoftware (Malware, wie z. B. Viren, Trojaner etc.) mit dem Ziel, die auf den IT-Systemen des Versicherungsnehmers oder mitversicherter Unternehmen befindlichen Daten oder Programme zu löschen oder zu verändern oder den Funktionsablauf des IT-Systems zu stören (Integrität und Verfügbarkeit von Daten und IT-Systemen);
  - einen Denial-of-Service-Angriff auf IT-Systeme des Versicherungsnehmers oder mitversicherter Unternehmen;
  - eine Verhinderung des autorisierten Zugangs Dritter zu ihren Daten;
  - eine unberechtigte Aneignung von Authentifizierungsinformationen (Zugangscodes, Passwörter) des Versicherungsnehmers, mitversicherter Unternehmen oder mitversicherter Personen;
  - eine Verletzung der Netzwerksicherheit des IT-Systems des Versicherungsnehmers oder mitversicherter Unternehmen durch Dritte im Sinne von § 303b StGB (Computersabotage);
  - eine unberechtigte Veränderung oder Löschung von in IT-Systemen des Versicherungsnehmers oder mitversicherter Unternehmen gespeicherten Daten; einen Diebstahl von IT-Systemen des Versicherungsnehmers oder mitversicherter Unternehmen durch Dritte oder deren Verlust.
- Nicht zielgerichtete Verletzung der Netzwerksicherheit durch eine Übermittlung von Schadsoftware (Malware wie z. B. Viren, Trojaner etc.), die auf den IT-Systemen des Versicherungsnehmers oder mitversicherter Unternehmen befindliche Daten oder Software löscht oder verändert oder den Funktionsablauf des IT-Systems stört (Integrität und Verfügbarkeit von Daten und IT-Systemen).
- Eine unberechtigte Veröffentlichung oder Weitergabe von Daten Dritter durch Mitarbeiter des Versicherungsnehmers oder mitversicherter Unternehmen.

2. Verletzung datenschutzrechtlicher Bestimmungen, wie beispielsweise des Bundesdatenschutzgesetzes

3. Verletzung der Datenvertraulichkeit von Daten Dritter durch die Versicherten

Was ist konkret versichert?

Versicherungsumfang/Entschädigungsleistung:

Haftpflicht

- Schadenersatzansprüche Dritter wegen eines Vermögensschadens durch eine Informationssicherheitsverletzung
- Haftungsfreistellung bei Datenverarbeitung durch Dritte
- Rechtsverteidigungskosten bei strafrechtlichen Ermittlungs- und Ordnungswidrigkeitenverfahren
- Ansprüche der Payment Card Industry einschließlich Vertragsstrafen
- Haftung bei Weitergabe eines Computervirus an Dritte
- Ansprüche wegen unrechtmäßiger Kommunikation/Veröffentlichung von digitalen Medieninhalten
  - Verletzung von Patenten, Markenrechten, Urheberrechten
  - Plagiat, widerrechtliche Verwendung oder Diebstahl von Ideen oder Informationen oder missbräuchliche Verlinkung
  - Rufschädigung
  - Verletzung des Persönlichkeitsrechts einer Person
  - Veröffentlichung von Informationen aus der Privatsphäre
  - Kommerzielle Verwendung des Namens
  - Verletzung des Wettbewerbsrechts

Eigenschaden

Datenschaden (Nachteilige Veränderung von Daten durch eine Netzwerksicherheitsverletzung)

- Maschinelle Wiedereingabe von Daten aus Sicherungsdatenträgern
- Wiederbeschaffung/Wiedereingabe von Stamm- und Bewegungsdaten
- Wiederbeschaffung/Wiedereingabe von Betriebssystemen und Standardprogrammen
- Wiedereingabe von individuell hergestellten Programmerweiterungen
- Kosten durch Kopierschutzstecker oder Verschlüsselungsmaßnahmen (Lizenzerwerb)

Mehrkosten- und Ertragsausfall

- infolge einer Netzwerksicherheitsverletzung
- infolge einer Datenschutzverletzung

Kosten (die infolge einer Informationssicherheitsverletzung entstehen)

Forensik-Kosten (Kosten für Ursachenermittlung)
- Feststellung ob eine Informationssicherheitsverletzung vorliegt
- Ermittlung der Ursache der Informationssicherheitsverletzung
- Ermittlung des Umfangs der Informationssicherheitsverletzung
- Empfehlung geeigneter Maßnahmen zur Reaktion und künftigen Abwehr auf diese Informationssicherheitsverletzung
- Kostenübernahme auch wenn nach Prüfung kein ersatzpflichtiger Schaden vorliegt
- Verzicht auf SB

Krisenkommunikation, Mediation, Reputationssicherung
- Angemessene und notwendige Kosten für PR- oder Krisenmanagement-Maßnahmen
- Kosten für angemessene Marketingmaßnahmen und Öffentlichkeitsarbeit
- Abwendung einer Rufschädigung und Wiederherstellung der positiven öffentlichen Wahrnehmung durch Beauftragung eines Mediators oder Krisenkommunikationsunternehmens

Informations-/Benachrichtigungskosten Kreditkartenmonitoring
- Kosten für die Benachrichtigung der Betroffenen und der verantwortlichen Datenschutzbehörde
- Kosten für Kreditkartenmonitoring zur Prüfung und Benachrichtigung der Betroffenen

Kosten für den Austausch von Hardware
- Elektronischer Zahlungsverkehr
- Fehlerhafter Versand von Waren/Warenverluste
- Telefonmehrkosten (bspw. unberechtigte Nutzung von gebührenpflichtigen Hotlines)

Nicht versichert sind:

- Personen- oder Sachschäden (mit Ausnahme von versicherten Daten, Programmen, fehlerhaftem Versand von Waren und Austausch von Hardware), kaufmännische Betriebsunterbrechung (Kundenabwanderung)
- Bußgelder

Versicherungssummen

- Kombinierte Haftstrecke für alle versicherten Deckungs-Bausteine
- Mögliche Versicherungssummen (einfache Maximierung): 125.000 €, 250.000 €, 500.000 €, 1 Mio. €, 2 Mio. €
- Keine Anrechnung einer Unterversicherung

Sublimits (Entschädigungsgrenzen)

- 10.000 € für nicht zielgerichtete Verletzung der Netzwerksicherheit durch Übermittlung von Schadsoftware
- 50% der Versicherungssumme
  - für Datenvertraulichkeitsverletzungen
  - für Kostenpositionen

Laufzeit

- Einjährige Verträge
- Versicherungsjahr entspricht dem Geschäftsjahr.
- Versicherungsschutz besteht auch für Versicherungsfälle, die während der Wirksamkeit des Vertrags eintreten (Schadenereignis), deren Ursache aber bereits vor Vertragsbeginn gesetzt und dem Versicherungsnehmer nicht bekannt war.

Betriebsarten, Selbstbehalte und Voraussetzungen.

Betriebsarten

mit einfacher Prüfung

Alle Betriebsarten, sofern nicht als Risiko mit detaillierter Prüfung oder Ausschlussrisiko definiert und Umsatz bis 5 Mio. €.

mit detaillierter Prüfung

Risiken ab einem Gesamtumsatz von 5 Mio. € und Risiken, die aufgrund ihrer Betriebsart einer besonderen Prüfung bedürfen; z. B. Druckerei, Verlag, Werbeagentur, Fotolabor, Film- und Tonstudio, Journalist, Architekt, Ingenieur, Rechts-, Wirtschafts- und Steuerberater, Reisebüro, IT-Dienstleister sofern nicht Softwareentwicklung, Online-Handel (auch teilweise), Versandhandel.

Nicht versichert werden

z. B. Krankenhaus, Blutuntersuchungslabor, Softwareentwicklung, Webhoster, Provider, Bank, öffentliche Verwaltung.

Selbstbehalt

- Generell 1.000 € (Betriebsarten mit einfacher Prüfung)/2.500 € (Betriebsarten mit detaillierter Prüfung).
- Für Ertragsausfall und Mehrkosten zeitlicher Selbstbehalt 24 Stunden.
- Der Selbstbehalt wird bei einem Schadenereignis nur einmal in Abzug gebracht. Es zieht der jeweils höhere Selbstbehalt.
- Bei der Nutzung der Experten-Hotline der Württembergischen wird kein Selbstbehalt angerechnet.

Voraussetzungen für den Versicherungsschutz.

- Mindestens wöchentliche Datensicherung.
  - Getrennte Aufbewahrung.
  - Möglichkeit der Rücksicherung.
- Übliche, ständig aktualisierte Schutzmaßnahmen und regelmäßige Überprüfung der Rücksicherung gegen die bestimmungswidrige Veränderung/Löschung gespeicherter Daten durch Firewalls, Antiviren-programme, Zugriffsrechte und unverzügliche Installationen von Updates und Patches.
- Prüfung digitaler (Medien-)inhalte vor deren Veröf-fentlichung.
- Bei vom Hersteller nicht mehr gepflegten (supporte-ten) Systemen, geeignete Sicherungsmaßnahmen tref-fen, z.B. keine Netzanbindung bei betroffenen Geräten.
- Sofern ein IT-Dienstleister eingesetzt wird, werden die genannten Maßnahmen mit dem Dienstleister vertrag-lich vereinbart.

Die Cyber-Police.
Die Anforderungen an den Datenschutz steigen.

Auch Freiberufler und kleinere Unternehmen sind betroffen.
Die Möglichkeiten, wie personenbezogene Daten gefährdet sein können, sind vielfältig:

- Gerichtsakten werden auf einer Mülldeponie gefunden. Ein Rechtsanwalt hatte sie nicht ordnungsgemäß entsorgt.
- Auf einem Laptop, der aus dem verschlossenen Auto eines Bäckereimitarbeiters gestohlen wurde, befanden sich personenbezogene Daten aktueller und ehemaliger Mitarbeiter.
- Ein verlorener USB-Stick eines Wirtschaftsprüfers enthielt vertrauliche Bilanzdaten von Kunden.

Die Verantwortung liegt bei dem Unternehmen, das personenbezogene Daten von Mitarbeitern oder Kunden verarbeitet oder verarbeiten lässt. Unabhängig von der Größe des Unternehmens.

In Datenschutzangelegenheiten gelten für Unternehmen in Deutschland folgenden Rechtspflichten:

- Benachrichtigung betroffener Kunden/Mitarbeiter.
- Benachrichtigung der Datenschutzaufsichtsbehörde des Bundeslandes.

Einzige Ausnahme: Geringes Schadenrisiko und Datenverschlüsselung.
Kann das Unternehmen nachweisen, dass es unwahrscheinlich ist, dass auf personenbezogene Daten zugegriffen wurde, kann die Informationspflicht hinfällig werden. Bestehen Zweifel, ob eine Ausnahmeregelung greift, gelten die Informationspflichten in vollem Umfang.

Bei Hardwareverlusten (z. B. Laptop) muss festgeststellt werden, welche Betroffenen im Einzelnen zu benachrichtigen sind. Bei besonders sensiblen Daten müssen die Benachrichtigungen teilweise als Brief versandt werden. Zusätzlich fallen Kosten für die Aufklärung des Sachverhalts, Rechtsberatungskosten und ggfs. Haftpflichtansprüche gegen das vom Datenverlust betroffene Unternehmen an.

Bitte beachten Sie auch unsere Tipps und Hinweise zur IT-Sicherheit.

9318 [6] 6/2017