Handlungsempfehlung Cyber-Risk

Stellen Sie Ihre IT auf die Probe

Ihre Ansprechpartner bei SHL

Sebastian Kink

sebastian.kink@shlgruppe.de
Tel. +49 89 769772 - 0

Tobias Jagenlauf

tobias.jagenlauf@shlgruppe.de
Tel. +49 89 769772 - 83

Warum ist eine Absicherung gegen Cyber-Angriffe wichtig?

Laut dem Allianz Risk Barometer zählen Cyber-Angriffe seit einigen Jahren zu den größten Risiken für Unternehmen. Die Anzahl an Cyber-Attacken hat in den vergangenen Jahren deutlich zugenommen.

Dabei stellt nicht nur der Verlust oder die Verschlüsselung von Daten ein Risiko dar: Insbesondere auch die Folgen eines Angriffs auf Ihre Unternehmensdaten und die damit verbundenen Informationspflichten (Was ist passiert? Wer war betroffen? Welche Daten sind abhandengekommen? usw.) laut dem Bundesdatenschutzgesetz bzw. der DSGVO sind mit einem hohen Aufwand und Kostenrisiko verbunden.

Eine Cyber-Risk Versicherung kann Sie effektiv vor den Folgen eines Cyber-Angriffs schützen.

Voraussetzung für den Erhalt einer Cyber-Risk Versicherung ist jedoch die Erfüllung gewisser Mindestkriterien, denn letztendlich kann durch technische und Organisationsmaßnahmen das Risiko eines erfolgreichen Cyber-Angriffs bereits deutlich reduziert werden.

Unabhängig davon, ob Sie sich für den ergänzenden Abschluss einer Cyber-Risk Versicherung entscheiden wollen oder nicht, soll Ihnen diese Handlungsempfehlung dabei helfen Ihre Angriffsfläche zu minimieren. Prävention ist der Schlüssel zum Erfolg für die Sicherheit Ihrer wertvollen Unternehmensdaten!

7 zwingende Voraussetzungen für Ihre Unternehmenssicherheit

Kurz gesagt: Es gibt 7 Grundlagen, die jedes Unternehmen in Sachen Datensicherheit erfüllen sollte. Sofern Sie nicht alle der folgenden Punkte erfüllen, ist es derzeit am Markt nach unserem Kenntnisstand nicht möglich, eine Cyber-Risk Versicherung zu erhalten:

- ✓ Beauftragung eines professionellen IT-Dienstleisters für die Betreuung Ihrer IT-Infrastruktur
- ✓ Nutzung von Firewalls
- ✓ Verwendung eines aktuellen Virenschutzes
- ✓ Nutzung aktueller und lizensierter Originalsoftware
- ✓ Regelmäßige Software- und Sicherheitsupdates
- ✓ Regelmäßige Backups aller Daten (mind. 1x pro Woche)
- ✓ Regelmäßige Schulung aller Mitarbeiter zu Datenschutz, Datensicherheit und technischen sowie organisatorischen Maßnahmen (=Datensicherheitsdialog).

Welche Maßnahmen im Unternehmen kann ich umsetzen?

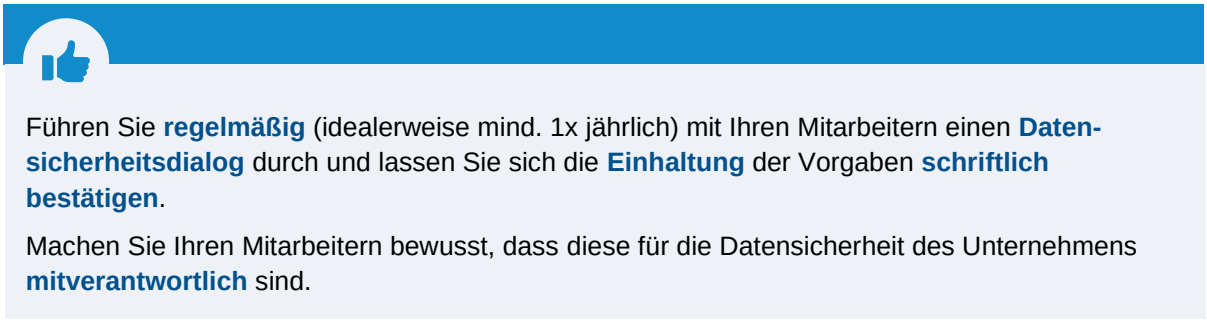
Zur Vermeidung erfolgreicher Cyber-Angriffe ist es maßgeblich, alle Mitarbeiter im Unternehmen in Sachen Datenschutz und Datensicherheit zu informieren.

Daher erläutern wir Ihnen auf den folgenden Seiten die notwendigen Inhalte eines Datensicherheitsdialogs sowie sinnvolle technische und organisatorische Maßnahmen, für deren Umsetzung und Einhaltung möglichst alle Mitarbeiter verantwortlich gemacht werden sollten.

Zu guter Letzt sollten Sie auch einen Plan für den Ernstfall haben, damit Sie Ihren Geschäftsbetrieb auch im Falle eines erfolgreichen Cyber-Angriffs möglichst schnell wiederaufnehmen können.

Datensicherheitsdialog – „der Faktor Mensch“

Rund die Hälfte aller Cyber-Angriffe haben ihren Ursprung im eigenen Unternehmen. Das bedeutet nicht unbedingt, dass es Ihre Mitarbeiter sind, die Unternehmensdaten entwenden. Oft werden Eindringlingen jedoch unbewusst oder fahrlässig Türen geöffnet. Klare Regeln im Umgang mit Zugängen, Passwörtern und Rechten sind der maßgebliche Faktor für die Sicherheit Ihrer Daten.



Führen Sie **regelmäßig** (idealerweise mind. 1x jährlich) mit Ihren Mitarbeitern einen **Daten-sicherheitsdialog** durch und lassen Sie sich die **Einhaltung** der Vorgaben **schriftlich bestätigen**.

Machen Sie Ihren Mitarbeitern bewusst, dass diese für die Datensicherheit des Unternehmens **mitverantwortlich** sind.

- Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit und zur Beachtung der Datenschutzgrundverordnung und der aktuellen Datenschutzgesetze.
- Datenschutzvorfälle jeglicher Art sind umgehend dem Datenschutzbeauftragten und der Geschäftsleitung zu melden.
- Verantwortung der Mitarbeiter dafür, dass
  - die ihnen anvertrauten Daten, Datenträger und Listenausdrucke ordnungsgemäß verwahrt werden, wenn sie nicht unmittelbar daran arbeiten.
  - keinerlei Unterlagen oder Kopien zurückbleiben, wenn sie am Kopierer / Scanner vertrauliche Dokumente vervielfältigt haben.
  - persönliche Geräte / Zugänge zu Anwendungen und Passwörter keinem Unbefugten zugänglich sind.
  - verwendete Passwörter den Mindestvorgaben des Unternehmens entsprechen.
  - nicht mehr benötigte Datenträger so vernichtet werden, dass eine missbräuchliche Verwendung unmöglich ist (Schredder oder Datenentsorgungsbehälter eines zertifizierten Dienstleisters).
  - alle technischen und organisatorischen Maßnahmen durch alle Kollegen gemeinschafts-verantwortlich eingehalten bzw. umgesetzt werden.
- Eine einwandfrei funktionierende IT-Infrastruktur ist Voraussetzung für effektives Arbeiten. Alle Mitarbeiter sind aufgefordert Funktionsstörungen und Leistungseinschränkungen, Fehler oder notwendige Versionsaktualisierungen schriftlich an den Verantwortlichen zu melden.
- Zudem sollten Fehler im Rahmen des kontinuierlichen Verbesserungsprozesses offen angesprochen werden – denn aus Fehlern lernt man schließlich am besten!
- Ein weiterer wichtiger Punkt ist gesundes Misstrauen beim Erhalt von Emails, Anrufen oder sonstiger Kontaktaufnahme durch Fremde, auch wenn sich diese als öffentliche Behörde, oder bekannte Person ausgeben. Vereinbaren Sie klare Regeln für Datenweitergabe, und insbesondere bezüglich der Befugnisse für Überweisungen und Auszahlungen.

Technische und organisatorische Maßnahmen

Die Schulung Ihrer Mitarbeiter reduziert das Risiko durch den „Faktor Mensch“. Gleichermaßen muss jedoch sichergestellt sein, dass Ihre Daten auch durch technische Maßnahmen vor Zugriff geschützt sind. Das beginnt bereits bei der verschlossenen Tür…

Regeln Sie den Zugang und Zugriff zu Arbeitsplätzen und geschäftlichen Daten

- Außerhalb der Geschäftszeiten werden die Büroräume und Fenster verschlossen. Die Einbruchdiebstahlsicherungen entsprechen den Vorgaben SG1 des VDS.
- Zugangs- und Zutrittskontrolle zu Büroräumen und Arbeitsplätzen für Unbefugte. Besucher und Handwerker dürfen sich nicht unbeaufsichtigt in den Büroräumen aufhalten.
- Während der Geschäftszeiten sind die Büroräume ebenfalls geschlossen, bzw. werden Besucher an der Eingangstüre begrüßt. Die Besucher werden in den Besprechungsraum geführt und die Türe geschlossen.
- Mitarbeiter und sonstige Berechtigte dürfen Büroschlüssel nicht an Dritte weitergeben. Dokumentieren Sie die Übergabe von Schlüsseln und Zutrittskarten.
- Sofern Sie einen eigenen Server betreiben oder Backups erstellen sollten sich diese in einem separaten, abgeschlossenen Raum befinden. Der Zugang zu diesem Raum ist auf den notwendigen Personenkreis zu beschränken.
- Bei längerem Verlassen des Arbeitsplatzes muss der Computer „gesperrt“ werden.
- Erstellen Sie ein Berechtigungskonzept für Ihre Mitarbeiter und unterschiedliche Anwendungen. Es sollten z.B. nur Mitarbeiter in der Buchhaltung Zugriff auf die Buchhaltungssoftware haben.
- Der Versand von persönlichen Informationen, Mitarbeiter- und Kundendaten sollte immer passwortgeschützt erfolgen.

Beauftragen Sie einen professionellen IT-Dienstleister mit der Pflege Ihrer Software und Systeme, der Administration von Backups und der Wartung Ihres Netzwerks

- Unterbinden Sie durch Systemrichtlinien die Vergabe schwacher Passwörter. Nutzen Sie komplexe Passwörter und verwalten Sie diese ggfs. in einem Passwortmanager.
- Stellen Sie sicher, dass jeder Mitarbeiter eigene Zugänge verwendet um sich an Geräten, in Programmen und bei Emailkonten anzumelden. Nur so können das Speichern, Bearbeiten, Löschen und Übertragen von Daten einer Person zugeordnet werden.
- Sperren Sie USB-Ports und CD-Laufwerke und erlauben Sie die Nutzung von USB-Sticks nur unter Verwendung von Verschlüsselungssoftware.
- Sämtliche Endgeräte, und auch das Netzwerk sind wirksam mit Antivirensoftware und Firewall geschützt. Die Aktualisierungen erfolgen automatisch bzw. umgehend bei Bedarf.
- Vorhandene W-Lan-Netzwerke sind verschlüsselt.
- Zugriffe zum Firmennetzwerk von extern erfolgen ausschließlich über gesicherte VPN-Verbindungen.

- Soweit mobile Geräte wie Notebooks oder Tablets außerhalb der Büroräume eingesetzt werden sind diese immer persönlich mitzuführen oder an einem sicheren, verschlossenen Ort zu lagern. Alle dienstlichen Geräte sind mit Passwörtern oder Fingerabdruck zu sichern.

Regeln Sie die Private Nutzung von IT am Arbeitsplatz und die Nutzung des Homeoffice

- Das Arbeitszimmer sollte separat liegen und abschließbar sein und dienstliche Unterlagen sind in einem abschließbaren Schrank aufzubewahren.
- Auf dem Desktop des PCs sollten personenbezogene Daten generell nicht gespeichert werden, die Ablage erfolgt auf dem vorgesehenen zentralen Speicher.
- Der Einsatz privater IT-Ausstattung für dienstliche Zwecke ist nicht gestattet
- Der Einsatz dienstlicher IT- Ausstattung für private Zwecke ist nicht gestattet, das gilt auch für das betriebliche E-Mail Postfach.

Sofern Sie Ihren Mitarbeitern die private Nutzung des Internets, z.B. in den Pausen erlauben, müssen Sie über (auch theoretische) bestehende **Möglichkeiten der Auswertung informieren**!

Erstellen Sie einen Krisenplan und proben Sie den Ernstfall – jährlich!

- Können Sie jederzeit auf aktuelle Backups zugreifen?
- Testen Sie das Rückspielen eines Backups auf eine neue Hardware.
- Wie lange benötigen Sie für die Beschaffung neuer Hardware und Aufspielen der gesicherten Daten aus einem Backup?
- Können Sie Ihren Betrieb für eine bestimmte Zeit in anderen Räumen oder im reinen Homeoffice Betrieb aufrechterhalten?

Bitte beachten Sie, dass unser Maßnahmenkatalog keinen Anspruch auf Vollständigkeit oder Allgemeingültigkeit erhebt.

Die Unternehmensgröße ist ein maßgeblicher Faktor Ihre gesetzliche Verpflichtung hinsichtlich des Datenschutzes und der Datensicherheit. Die Einhaltung der genannten Maßnahmen verringert zwar die Möglichkeit einer Störung oder Manipulation Ihres IT-Systems, völlig ausschließen lässt sich diese Gefahr jedoch nicht. Erst ein passendes IT-Sicherheitskonzept, in Verbindung mit einer Cyber-Police, bietet Ihnen den maximalen Schutz vor den Folgen eines Cyber-Vorfalls.

Weitere, ausführliche Informationen zum Thema IT-Sicherheit erhalten Sie unter www.bsi.bund.de.

Sie haben Fragen?

Sich auf Stärken zu konzentrieren ist der Schlüssel zum Erfolg.
Unsere Stärke ist die Analyse und Absicherung Ihrer Risiken und Engpässe.

Und das schon seit über 20 Jahren als unabhängiger und
inhabergeführter Versicherungsmakler.

Gemeinsam finden wir die auf Sie individuell zugeschnittene Lösung.
Dafür gehen wir auch neue und unkonventionelle Wege.

Melden Sie sich gerne bei uns!

Sebastian Kink

Geschäftsführer

sebastian.kink@shlgruppe.de
Tel. +49 89 769772 - 0

Tobias Jagenlauf

Spezialist Gewerbeversicherung

tobias.jagenlauf@shlgruppe.de
Tel. +49 89 769772 - 83