Datenschutz und Cyber-Risk-Management

Qualitativ beraten – Restrisiken absichern

FAIRNANCIAL
Finanz- & Versicherungsmakler

in Kooperation mit Alchimedus

Goldene Regeln für mehr IT-Sicherheit in Ihrem Unternehmen

Was wird in Ihrem Unternehmen schon umgesetzt?

Identifizieren Sie Ihre Risiken

Analysieren Sie Ihre IT gezielt auf Schwachstellen. Durch diese Risikoanalyse werden bestehende Risiken ermittelt und einem möglichen Schadensausmaß gegenübergestellt.

O Ja O Nein

Testen Sie Ihr Backup

Nur ein Backup, das funktioniert, ist ein gutes Backup. Ihre Daten brauchen Sie für Ihren Geschäftserfolg. Stellen Sie deshalb sicher, dass es regelmäßige verschlüsselte Backups gibt, welche gesichert aufbewahrt werden und auch einwandfrei funktionieren.

O Ja O Nein

Updates

Installieren Sie Updates und Patches immer sofort. Halten Sie nicht nur Ihr Betriebssystem, sondern alle genutzten Programme und Plug-Ins immer auf dem neuesten Stand. Durch die Updates werden neu entdeckte Sicherheitslücken umgehend geschlossen. Für größere Netzwerke sollte es eine zentrale Updatesteuerung geben.

O Ja O Nein

Passwörter

Benutzen Sie verschiedene Passwörter für verschiedene Anwendungen. Nutzen Sie komplexere Passwörter, die sich durch Merksätze einprägen, z.B. "Ich esse 2017 gerne Spargel" = "Ie2017gS". Passwörter niemals aufschreiben, sondern regelmäßig erneuern und z.B. durch Zahlen oder Sonderzeichen komplexer gestalten. Niemals Passwörter an andere Personen weitergeben.

O Ja O Nein

Mitarbeiter

Die eigenen Mitarbeiter werden sehr häufig als das schwächste Glied in der Kette der Cyber-Sicherheit benannt. Falsches Verhalten von Mitarbeitern, z.B. im Umgang mit Mails, kann zu einem Datenverlust oder einer Manipulation führen. Gut informierte Mitarbeiter sind aber gleichzeitig auch das beste Frühwarnsystem für mögliche Vorfälle im Firmennetzwerk. Binden Sie deshalb Ihre Mitarbeiter aktiv in ihr IT-Sicherheitskonzept ein.

O Ja O Nein

Zugriffe

Bei den Zugriffen sollten Sie das folgende Prinzip berücksichtigen: "So wenig wie möglich, so viel wie nötig!" Dies sollte u.a. bei personenbezogenen Daten beachtet werden. Legen Sie schriftlich fest, welcher Mitarbeiter oder welche Abteilung auf welche Daten zugreifen darf. Achten Sie darauf, dass niemand auf die USB-Ports Ihrer Rechner zugreifen kann, auch nicht, wenn Sie den Raum verlassen. Platzieren Sie die Rechner so, dass ein direkter Zugriff nicht so einfach möglich ist.

O Ja O Nein

„Restrisiken“ trotz Umsetzung der DSGVO und umfangreicher IT-Sicherheit

Es gibt keinen 100%igen Schutz, beziehen Sie deshalb in Ihr Sicherheitskonzept das Outsourcen der Geschäftsrisiken mit ein. Zu einem ganzheitlichen Risk-Management gehört neben der Verminderung der Risiken auch die Übertragung an Versicherer. Durch eine Versicherung sind nicht nur die wirtschaftlichen Folgen eines Angriffs abgesichert, es stehen Ihnen des Weiteren Experten und Fachanwälte zur Seite, um die notwendigen Maßnahmen umgehend in die Wege zu leiten.

- Diebstahl oder Verlust von mobilen Geräten (Laptop, Handy, USB-Sticks etc.)
- Fahrlässiger Umgang mit Kunden-/Lieferantedaten und / oder der IT durch Mitarbeiter
- Datenrechtsverletzungen und Cyber-Erpressung, versteckte Computerviren in Mails
- Hacker erbeuten sensible Daten und veröffentlichen sie. Die betroffenen Kunden machen wegen Verletzung ihrer Persönlichkeitsrechte Ansprüche geltend
- Die Computer werden von einem Virus befallen und die gespeicherten Daten können nicht mehr geöffnet werden – Ihr Betrieb muss schließen, bis das Problem behoben ist

Ihr Ansprechpartner

Felix Anrich TÜV-zertifizierter Fachberater für Cyber-Risiken anrich@fairnancial.de

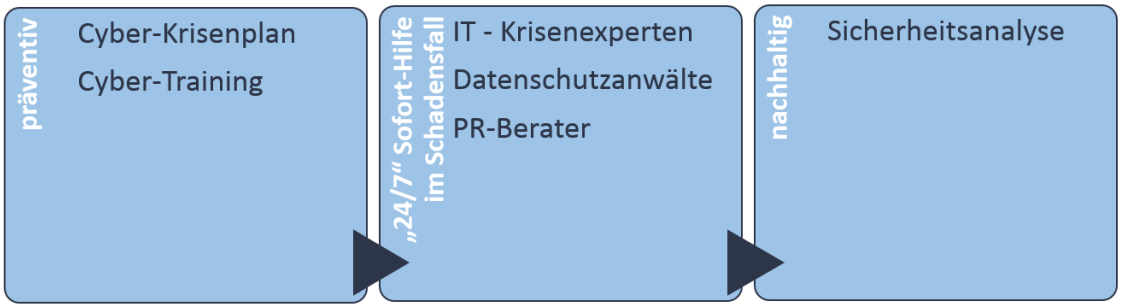
Datenschutz und Cyber-Risk-Management

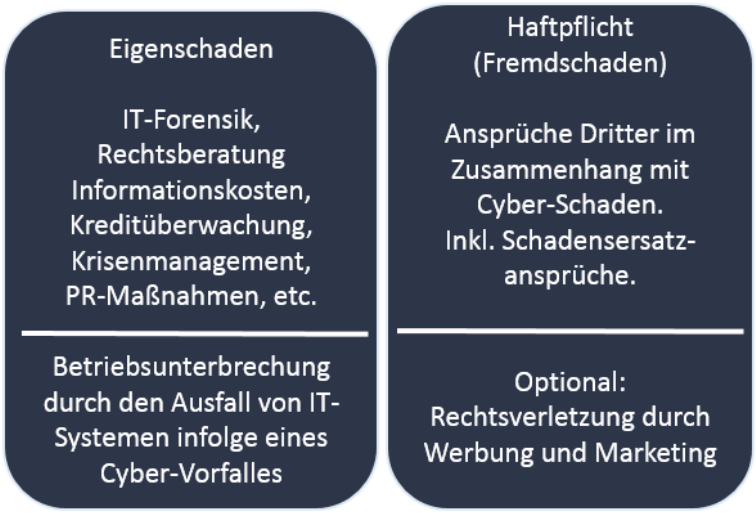
Qualitativ beraten – Restrisiken absichern

FAIRNANCIAL
Finanz- & Versicherungsmakler
in Kooperation mit Alchimedus

Cyber-Versicherung – für Sie ein „umfangreicher Dienstleister“

Herausforderung: Die Vielfalt der Cyber-Kriminalität fordert eine situative und dynamische Reaktion. Die Cyber-Versicherung fungiert und unterstützt als Krisendienstleister und Serviceanbieter. Sie deckt nicht nur resultierende Kosten, sondern unterstützt mit einem aktiven Krisenmanagement, diversen Assistance-Leistungen und einem Netzwerk an Experten. Versichert gelten Fremd- und Eigenschäden.





Reale Fakten zum virtuellen Risiko

Die Cyber-Kriminalität ist ständig im Wandel. Die Viren-Übertragung zur Verschlüsslung von Daten ist das häufigste Cyber-Delikt. Im Jahr 2016 wurden **täglich ca. 350.000 neue Schadprogrammvarianten** gesichtet. BSI Lagebericht IT-Sicherheit 2017

60 % aller Cyber-Vorfälle werden laut der IBM-IT-Security-Studie **durch die eigenen Mitarbeiter** verursacht. Der Zugang zu den IT-Systemen teils absichtlich, jedoch häufig unabsichtlich durch Unwissenheit oder Unachtsamkeit ermöglicht.

Wussten Sie, dass jedes zweite Unternehmen (52 Prozent) in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen war? Weitere 26% sind vermutlich betroffen. Bitkom Research Wirtschaftsschutz in der digitalen Welt 2017

Ihr Ansprechpartner
Felix Anrich TÜV-zertifizierter Fachberater für Cyber-Risiken anrich@fairnancial.de