Wie steht es um Ihre Cyber-Sicherheit?

- **Sind die IT-Systeme, die für Ihre kritischen Geschäftsprozesse notwendig sind, genügend vor Cyber-Attacken geschützt?**
- **Wissen Ihre Mitarbeitenden, wie sie sich gegen Cyber-Risiken (z.B. Phishing, Social Engineering, CEO Fraud) schützen können?**
- **… und ist dann doch einmal etwas passiert. Wurden Vorbereitungen getroffen, wie das Unternehmen schnellstmöglich wieder arbeiten kann?**

Nehmen Sie sich 10 Minuten Zeit und beantworten Sie die folgenden 12 Fragen zur IT-Sicherheit. Sie erhalten damit einen guten Überblick über den Zustand Ihrer Fitness hinsichtlich der Risken im Cyber-Space.

Kunde

Firma

E-Mail

12 Fragen zur Cyber-Sicherheit

			Antwort Ja	Antwort Nein	Bemerkungen
Strategie & Regelungen	1.1	Kennen Sie die schützenswerten Informationen (Technologiewissen, geistiges Eigentum, etc.), in Ihrem Unternehmen und wissen Sie welche Geschäftsprozesse von einem Ausfall der IT betroffen wären?	☐	☐	
	1.2	Haben Sie die IT-Sicherheits-Risiken für Ihre kritischen Geschäftsprozesse identifiziert und gibt es Massnahmen zur Verhinderung von Schäden aus Cyber-Attacken?	☐	☐	
	1.3	Gibt es IT-Sicherheitsvorgaben und Regelungen in Form von Grundsätzen und Sicherheitskonzepten?	☐	☐	
	1.4	Besteht die Gewissheit über die Einhaltung der notwendigen gesetzlichen und regulatorischen Bestimmungen, insbesondere auch der neuen europäischen Regelung DSGVO/GDPR?	☐	☐	
Organisation & Prozesse	2.1	Gibt es die Funktion des IT-Sicherheitsbeauftragten/-Datenschutzbeauftragten und ist dieser genügend qualifiziert?	☐	☐	
	2.2	Ist bekannt, wer sich von wo in das Firmennetzwerk einloggt, wie Daten ausgetauscht werden und auf welche Informationen die Personen zugreifen dürfen?	☐	☐	
	2.3	Würde es auffallen oder liesse es sich nachvollziehen, wenn ein Mitarbeiter unerlaubt sensible Informationen kopiert oder versendet und gibt es Regelungen wie mit Daten auf Mobilgeräten umgegangen wird?	☐	☐	
	2.4	Führen Sie regelmässige Trainings oder Awareness Kampagnen für alle Ihre Mitarbeitenden zu den Gefahren im Umgang mit IT-Mitteln und Cyber-Risiken durch?	☐	☐	
Infrastruktur & Vorsorge	3.1	Werden die digitalen Kommunikationskanäle und die damit verbundenen Informationen an der Schnittstelle zum Internet überwacht?	☐	☐	
	3.2	Werden alle relevanten Daten in angemessenen Zeitintervallen gesichert und werden die Sicherungen ausserhalb des Unternehmens offline aufbewahrt? (Schutz vor Verschlüsselungstrojaner, Brand, etc.)	☐	☐	
	3.3	Werden bekannt gewordene IT-Sicherheitslücken zeitnah geschlossen und gibt es klare Verantwortlichkeiten für Updates und Softwareaktualisierung?	☐	☐	
	3.4	Gibt es für schwerwiegende Ausfälle der IT-Systeme aktuelle Notfallpläne mit Anweisungen und Checklisten?	☐	☐	
		Anzahl:	☐	☐	

Auswertung Fragebogen

Mit diesem Fragebogen wollen wir Sie über die aktuellen Risiken beim Betrieb Ihrer IT-Systeme sensibilisieren und Ihnen erste Anhaltspunkte liefern, wo Sie allenfalls Lücken haben und wie anfällig Sie gegenüber Cyber-Attacken sind.

Wenn Sie alle Fragen in den drei Bereichen mit „Ja“ beantworten können, sind Sie auf dem richtigen Weg!

Fragen mit Nein-Antworten in einem oder mehreren Bereichen zeigen Ihnen auf, wo Handlungsbedarf besteht.

Konnten Sie weniger als 6 Fragen mit Ja beantworten, dann bestehen aus unserer Sicht grosse Risiken im Bereich der Informationssicherheit und somit dringender Handlungsbedarf. Ein länger andauernder Ausfall der IT durch einen schwerwiegenden Sicherheitsvorfall kann die Geschäftstätigkeit massiv stören und einen erheblichen finanziellen Schaden verursachen.

Oft gehörte Aussagen:

«Bei uns ist in den letzten Jahren noch nie etwas passiert!»

«Ich bin doch nicht wichtig und wer interessiert sich schon für meine Daten!»

«Wenn ich regelmässig alle notwendigen Updates einspielen müsste, bräuchte ich einen zusätzlichen Mitarbeitenden!»

«Meine Mitarbeitenden wissen doch Bescheid und rufen nur sicheren Internetseiten auf!»

«Ich brauche keine Sicherheitsregelungen – ich vertraue meinen Mitarbeitenden!»

“If you think safety is expensive, try an accident!” **Trevor Kletz**

Warten Sie nicht, bis etwas passiert! Packen Sie es noch heute an. Die Spezialisten von Secnovum unterstützen Sie und tragen dazu bei, dass Sie gegenüber den Gefahren im Cyber-Space gewappnet sind.