württembergische

Fragebogen

Die Cyber-Police.
Das Plus für mehr Datensicherheit.

Versicherungsnehmer/Interessent

Interessent/Gesprächspartner	Vermittler-Nr.
Straße und Hausnummer	Vermittler – Name/Gesprächspartner
PLZ, Ort	Versicherungsschein-Nr,
Telefon/Fax	Kunden-Nr.
E-Mail	Homepage

Allgemeine Unternehmensinformationen

Nennen Sie die konkrete Firmierung aller zu versichernden Unternehmen und alle Standorte:

Beschreiben Sie kurz Ihre Geschäftstätigkeit und die einzelnen Geschäftsbereiche:

Gesamtumsatz des letzten Geschäftsjahres

Umsatz gesamt in EUR _____

davon USA/Kanada in EUR _____

Gewünschte Versicherungssumme in EUR

☐ 125.000 ☐ 1.000.000
☐ 250.000 ☐ 2.000.000
☐ 500.000

Anzahl der Beschäftigten _____

Anzahl der PC-Arbeitsplätze (inkl. Außendienst-/Homeoffice-Arbeitsplätze) _____

Werden Umsätze über Online-Handel (E-Commerce) getätigt? ☐ ja ☐ nein
Falls ja, bitte den ausführlichen Fragebogen (Formular 9316) ausfüllen.

Werden Sicherheitsupdates (Patches) unverzüglich durch zentrale Softwareverteilung installiert? ☐ ja ☐ nein

Nutzen Sie eine Antivirensoftware und ist die automatische Update-Funktion aktiviert? ☐ ja ☐ nein

Sofern Sie WLAN nutzen, haben Sie hierfür mindestens eine WPA2-Verschlüsselung eingerichtet? ☐ ja ☐ nein
☐ keine WLAN-Nutzung

Wie häufig sichern Sie Ihre Daten?

Teilsicherung (nur die seit letzter Sicherung geänderten Dateien) ☐ täglich ☐ wöchentlich ☐ _____

Vollsicherung (alle Dateien) ☐ täglich ☐ wöchentlich ☐ _____

Anzahl der verfügbaren Sicherungsgenerationen? Anzahl: _____

Wie oft wird die Verwendbarkeit der Datensicherung getestet?
☐ mindestens halbjährlicher Turnus ☐ nie
☐ mindestens jährlicher Turnus ☐ _____

Nutzen Sie Betriebssysteme (z.b. auf Servern oder Produktionsanlagen), die vom Hersteller nicht mehr gewartet oder unterstützt werden (z. B. Windows XP)? ☐ ja ☐ nein
Falls ja, bitte den ausführlichen Fragebogen (Formular 9316) ausfüllen.

Werden Rechteprüfungen an urheberrechtlich geschütztem Material vorgenommen? ☐ ja ☐ nein

Bestand oder besteht eine Vorversicherung gegen Cyber-Gefahren? ☐ ja ☐ nein

Wenn ja, bitte geben Sie an:

Versicherer _____ Versicherungsschein-Nr. _____ Gekündigt durch ☐ VN ☐ Versicherer

Kam es infolge oder aufgrund eines Angriffs auf das IT-System Ihres Unternehmens oder im Online-Banking in den letzten 5 Jahren zu ☐ ja ☐ nein
– einem Datenverlust?
– einer Datenveränderung?
– einem Ausfall des IT-Systems?
– einem Datendiebstahl?
– einer Unterbrechung des Betriebsablaufs?

Wenn ja, bitte erläutern Sie den Hergang des Vorfalls und welche Maßnahmen danach ergriffen wurden.

Ort, Datum	Unterschrift des Antragstellers/Versicherungsnehmers

Hinweise zur IT-Sicherheit

Ein angemessenes IT-Sicherheitskonzept ist die Voraussetzung für eine wirksame Reduzierung der Gefahr von Störungen des betrieblichen Ablaufs. Für die Absicherung des Restrisikos haben Sie über die Cyber-Police einen exzellenten Versicherungsschutz. Um die Gefahr einer Betriebsstörung von vornherein zu reduzieren, empfehlen wir Ihnen untenstehende Maßnahmen und zusätzlich die Einschaltung eines qualifizierten IT-Dienstleisters:

Organisatorische Maßnahmen
- Datensicherheit ist Chefsache.
- IT-Risiken müssen klar kommuniziert werden. Sensibilisieren Sie Ihre Mitarbeiter.
- Verwenden Sie für jeden Nutzer und Administrator benutzerindividuelle, ablaufende Passwörter. Schützen Sie auch Ihre Daten auf mobilen Geräten mit einem Passwort. Sperren Sie Rechner und mobile Geräte bei Inaktivität automatisch.
- Datenschutz: Achten Sie auf die sichere Entsorgung von Papier und Datenträgern (Festplatten, USB-Sticks etc.).

Präventive Maßnahmen
- Öffentliche WLAN-Netze sind unsicher. Geben Sie keine vertraulichen Daten wie Passwörter und Kontodaten ein, solange Sie einen öffentlichen Netzwerkzugang nutzen.
- Schützen Sie Ihren Server im Idealfall durch eine physische Zutrittsbeschränkung zum Server-Raum.
- Prüfen Sie, ob Sie digitale Medieninhalte (beispielsweise Bilder) veröffentlichen dürfen.

Absicherung des IT-Netzwerkes
- Schützen Sie Ihren elektronischen Firmenzugang durch eine für Ihr Unternehmen geeignete Firewall, durch VPN-Zugänge oder ähnliches. Im Idealfall als eigenständige Hardware-Firewall, die nicht im DSL-Router integriert ist.
- Richten Sie für Ihr WLAN mindestens eine WPA2-Verschlüsselung ein

Umgang mit mobilen Geräten
- Schalten Sie bei mobilen Geräten (Smartphone, Tablet, Laptop etc.) die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur ein, wenn Sie diese bewusst zur Kommunikation einsetzen.
- Schließen Sie keine USB-Sticks, SD-Karten und andere Speichermedien von nicht vertrauenswürdigen Quellen an einen Rechner an.

Schutz vor Schadsoftware
- Verwenden und aktualisieren Sie regelmäßig Ihre Antivirensoftware. Lassen Sie den Virenscanner im Hintergrund laufen. Dateien werden so bei Zugriff gescannt.
- Verwenden Sie Software und Links nur aus vertrauenswürdigen Quellen. Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Sie können Trojaner und Viren enthalten.
- Übernehmen Sie sicherheitsrelevante Patches der Softwarehersteller über die automatische Updatefunktion.

Sicherung der Daten
- Sichern Sie mindestens einmal wöchentlich auf einem separaten Datenträger. Überschreiben Sie die wöchentliche Datensicherung frühestens nach vier Wochen.
- Um zusätzliche Sicherheit zu gewährleisten, sollte darüber hinaus je Quartal mindestens eine Sicherung auf einem separaten Datenträger durchgeführt werden. Überschreiben Sie die längerfristige Datensicherung frühestens nach vier Quartalen.
- Die Sicherungsdatenträger müssen eindeutig gekennzeichnet sein und der Zeitpunkt der Datensicherung nachvollziehbar dokumentiert werden.
- Die Sicherungsdatenträger sollten mit einem Passwort geschützt werden. Die Sicherungsdatenträger sollten nur zur Datensicherung mit dem Netzwerk verbunden werden und ansonsten vom Netzwerk getrennt sein.
- Testen Sie den Notfall: Können die gesicherten Daten auch wieder auf die Anlage zurückgespielt werden?
- Lagern Sie Ihre Sicherungsdatenträger in einem anderen Gebäude oder in einem geeigneten Datensicherungsschrank.

Bitte beachten Sie, dass dieser Maßnahmenkatalog keinen Anspruch auf Vollständigkeit oder Allgemeingültigkeit erhebt. Die Einhaltung dieser Maßnahmen verringert zwar die Möglichkeit einer Störung Ihres IT-Systems, völlig ausschließen lässt sich diese Gefahr jedoch nicht.

! Erst ein mit Ihrem qualifizierten IT-Dienstleister erstelltes Sicherheitskonzept bietet Ihnen in Verbindung mit unserer Cyber-Police den maximalen Schutz vor wirtschaftlichen Nachteilen bei einem Cyber-Vorfall.