Stärken Sie Ihre IT-Sicherheit mit dem CAIRO CyberRisikoCheck

CAIRO

secure • digital • IT-infrastructures

Schützen Sie Ihr Unternehmen effektiv mit dem CAIRO CyberRisikoCheck (CRC), der auf dem neuesten IT-Sicherheitsstandard des BSI und Cyber-Versicherung-Fragebögen basiert. Innerhalb weniger Tage erfahren Sie, wie Sie Ihre IT-Sicherheit signifikant verbessern können. Wir leiten Sie durch den Prozess und zeigen auf, wie der CAIRO CyberRisikoCheck Ihr Unternehmen absichert.

Ihr Kompass für IT-Sicherheit

Die neue DIN SPEC 27076 des BSI richtet sich an Unternehmen mit bis zu 50 Mitarbeitenden, die bisher keine oder nur wenige Berührungspunkte mit dem Thema IT-Sicherheit hatten. Sie kann aber auch jederzeit von größeren Unternehmen eingesetzt werden, um einen schnellen Überblick über den Status der eigenen IT-Sicherheit zu erhalten.

Der CyberRisikoCheck ist zum Preis eines Beratertages durch einen CAIRO-Experten erhältlich. Ziel nach der Durchführung des CyberRisikoChecks ist es, ein grundlegendes IT-Sicherheitsniveau zu etablieren, um das eigene Unternehmen entsprechend abzusichern und beispielsweise die Voraussetzungen für den Abschluss einer Cyber-Versicherung zu schaffen. Wer eine detailliertere Analyse benötigt, kann den CyberSecurityCheck in Anspruch nehmen.

Ihre Vorteile auf einen Blick

Überblick und Transparenz

Erhalten Sie einen detaillierten Überblick über den IST-Zustand Ihrer IT-Sicherheit und identifizieren Sie mögliche Schwachstellen.

Verständliche Berichterstattung

Ein klarer BSI-zertifizierter Bericht mit konkreten Handlungsempfehlungen, die auf die spezifischen Bedürfnisse Ihres Unternehmens zugeschnitten sind.

Unterstützung bei Versicherungsanträgen

Dieser Bericht kann bei der Beantragung oder Überprüfung von Cyber-Versicherungen eingereicht werden, was zu besseren Konditionen führen kann.

CyberRisikoCheck mit CAIRO

Wir geben nicht nur Empfehlungen. Wir helfen Ihnen aktiv dabei, diese umzusetzen. Der CRC ist auch Teil von HackGuard.

Was genau ist die DIN SPEC 27076?

Die DIN SPEC 27076 wurde in Zusammenarbeit mit dem BSI, dem Bundesverband mittelständische Wirtschaft und weiteren Partnern entwickelt. Sie dient als Beratungsstandard für die IT-Sicherheit von KMUs und prüft, wie gut Ihr Unternehmen im Bereich IT-Sicherheit aufgestellt ist.

Wie läuft der CyberRisikoCheck ab?

Die Prüfung wird von unseren Compliance- und Security-Experten durchgeführt. Wir führen ein Interview mit Ihrem Unternehmen, um 27 Anforderungen aus sechs Themenbereichen und den Checklisten der Versicherungen zu überprüfen. Danach erhalten Sie einen Bericht mit einer Punktzahl und Handlungsempfehlungen, die nach Dringlichkeit sortiert sind. Die erfassten Daten liegen anonym auf dem Interview-Server des BSI.

Erste Schritte auf dem Weg zur Cyber-Resilienz

Mit dem CyberRisikoCheck bieten wir kleinen und mittleren Unternehmen einen strukturierten Ansatz, um sich gegen Bedrohungen zu wappnen und passende Versicherungen abzuschließen. Unser Check deckt alle wichtigen Bereiche ab, von der Organisation und Sensibilisierung über das Identitäts- und Berechtigungsmanagement bis hin zum Schutz vor Schadprogrammen. Als nächsten Schritt folgen entweder Umsetzungsmaßnahmen oder ein umfangreicher CAIRO CyberSecurityCheck.

1. Erstgespräch	Vorstellung der Normen & Versicherungsanforderungen
2. Interview	Interview nach dem Prüfkatalog mit der Geschäftsführung
3. Auswertung	Auswertung der Antworten aus dem Interview und Erstellung des CyberRisikoBerichts
4. Präsentation	Ergebnispräsentation mit Handlungsempfehlungen

Die sechs Säulen der IT-Sicherheit nach DIN SPEC 27076

1. Organisation und Sensibilisierung

Ein starkes Sicherheitskonzept beginnt an der Spitze. Wir bewerten initial das Engagement des Managements, die Verteilung der Kompetenzen und die Sensibilisierung der Mitarbeitenden, um eine Kultur der Cybersicherheit in Ihrem Unternehmen zu etablieren.

2. Identitäts- und Berechtigungsmanagement

Der Schlüssel zur Sicherheit Ihrer Daten liegt in der Kontrolle des Zugangs. Wir analysieren Ihre Zugangs- und Zutrittsberechtigungen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf Ihre wertvollen Informationen haben.

3. Datensicherung

Daten sind das Herzstück Ihres Unternehmens. Wir prüfen die Zuständigkeiten, den Umfang, die Häufigkeit und die Verfügbarkeit von Daten und deren Backups, um Datenverlust zu verhindern und die Betriebskontinuität zu gewährleisten.

4. Patch- und Änderungsmanagement

Aktualität ist ein Muss in der IT-Sicherheit. Wir evaluieren die Verfügbarkeit und Aktualität Ihrer Hard- und Software, um Schwachstellen zu schließen und Ihre Systeme auf dem neuesten Stand zu halten.

5. Schutz vor Schadprogrammen

Schadsoftware lauert überall. Wir identifizieren die Haupteinfallstore für Schadprogramme und implementieren präventive Maßnahmen, um Ihr Unternehmen vor diesen Bedrohungen zu schützen.

6. IT-Systeme und Netzwerke

Die Infrastruktur Ihres Unternehmens ist das Rückgrat Ihrer IT-Sicherheit. Wir definieren die Sicherheitsmechanismen hinter Ihrer Informations- und Kommunikationstechnik, um eine robuste und sichere Netzwerkumgebung zu schaffen.

Schützen Sie Ihr Unternehmen vor Cyberattacken

Cyberkriminalität kennt viele Gesichter und keine Unternehmensgröße ist vor diesen Bedrohungen sicher. Hier sind einige der typischen Gefahren, die im Netz lauern:

Malware: Viren, Trojaner und Spyware können unbemerkt Daten stehlen, Systeme beschädigen oder kontrollieren. Sie verbreiten sich oft über infizierte Dateien oder Links.

Phishing: Gefälschte E-Mails, Websites oder Nachrichten, die darauf abzielen, sensible Informationen wie Benutzernamen, Passwörter und Finanzdaten zu stehlen.

Ransomware: Eine Art von Malware, die Dateien oder Systeme verschlüsselt und Lösegeld für deren Freigabe verlangt, was zu finanziellen Verlusten und Betriebsunterbrechungen führen kann.

DDoS-Angriffe: Diese Angriffe überfluten Online-Dienste oder Websites mit Traffic, um deren Verfügbarkeit zu beeinträchtigen.

Social Engineering: Die Manipulation von Menschen, um an vertrauliche Informationen zu gelangen oder Zugang zu bestimmten Infrastrukturen zu erhalten.

Zero-Day-Exploits: Schwachstellen in Software oder Systemen, die noch keine Patches oder Sicherheitsupdates haben und von Cyberkriminellen ausgenutzt werden können.

Ergreifen Sie die Initiative für eine stärkere IT-Sicherheit

Neben den obigen externen Gefahren müssen viele interne Maßnahmen für eine verbesserte IT-Sicherheit getroffen werden. Diese werden auch in Cyber-Versicherung-Fragebögen angefordert. Daher beraten wir das ganze Spektrum der Vorkehrungen im CAIRO CRC.

CAIRO CyberRisikoCheck ist ein Teil unseres Security & Compliance Portfolios von normgerechten Security-Prüfungen, über die Behebung aller Schwachstellen bis zum sicheren IT-Betrieb mit modernen Lösungen, CAIRO Security Managed Services oder Security Awareness Trainings.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

Tel.: +49 (0)621 86 75 10
Mail: info@cairo.ag
Web: www.cairo.ag

CAIRO
secure • digital • IT-infrastructures

Kontakt