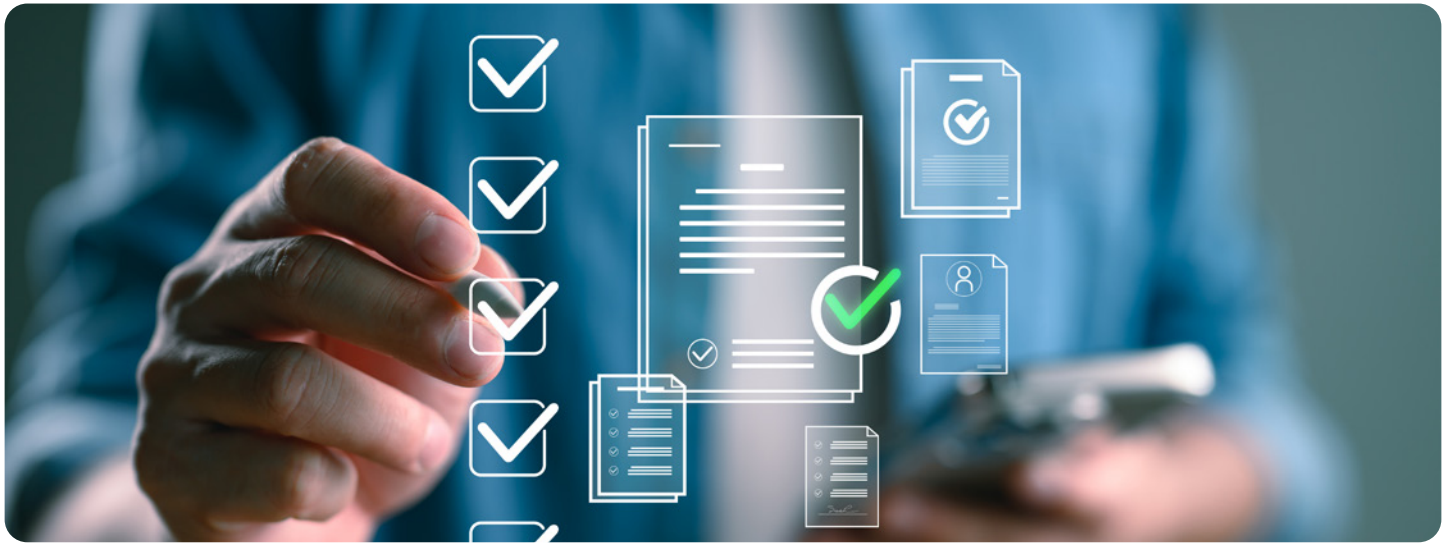
CAIRO CyberSecurityCheck

CAIRO
Your IT. Our Mission.

Schützen Sie Ihre IT vor Cyberangriffen – mit dem CAIRO CyberSecurityCheck (CSC)



Der CSC besteht aus zwei Hauptteilen:

CAIRO Experten führen einen nach der **ISACA** & dem **BSI** entwickelten **Cyber-Sicherheits-Check** aus. Viele Schwachstellen resultieren aus Lücken in der Organisation oder in Prozessen & Verfahren.

Eine **risikoorientierte Analyse** Ihrer IT-Infrastruktur in allen Bereichen, von Personal bis hin zur Organisation, Dokumentation & IT- Applikationen bzw. IT-Technik hilft, Schwachstellen zu identifizieren und zeigt konkrete Maßnahmen zu deren Behebung auf – alles basierend auf bewährten Standards wie **ISO 27000** und **BSI-Grundschutz**.

Der CAIRO CSC enthält optional auch eine effektive **NI2-GAP-Analyse** zur Erlangung der **NIS2-Konformität. Hier kann man Zeit und Geld sparen, da die kommenden NIS2-Anforderungen** sich mit der obigen Prüfung teilweise überdecken.

ACHTUNG !

Ein erfolgreicher Cyberangriff hat schwerwiegende Folgen inklusive Ihrer Nachweispflicht, wie lange der Angriff lief und welche Daten abgeflossen sind.

Ihre Vorteile

- **Unsere „Cyber Security Practitioner“ zertifizierten Berater haben langjährige Technologie- & Sicherheitserfahrungen**
- **Transparenz auf allen Ebenen:** Klare Orientierung für das Management & konkrete Handlungsempfehlungen für die IT-Administration, inklusive Prüfungen bzgl. Ihrer **Organisation** und **Dokumentation**
- **Objektive Bewertung:** Unabhängige Analyse und Priorisierung von Schwachstellen
- **Effizienz:** Fokus auf die wichtigsten Sicherheitslücken und fundierte Investition in IT-Sicherheit
- **Flexibilität:** Der Check setzt **keine** komplexen technischen Lösungen voraus und ist auch für kleinere Unternehmen geeignet
- **Erlangung der NIS2-Konformität**

Ablauf des CyberSecurityChecks

1) Risikoeinschätzung

Gemeinsam mit Ihnen bewerten wir die potenziellen Risiken und Schwachstellen Ihrer IT-Infrastruktur sowie Ihrer Organisation

2) Dokumentensichtung

Wir analysieren relevante Dokumente, um einen ersten Überblick über Ihre Systeme und Sicherheitsmaßnahmen zu erhalten

3) Vor-Ort-Prüfung

Unsere Experten führen eine umfassende Beurteilung vor Ort durch – von Interviews mit Verantwortlichen bis hin zur Analyse der IT-Systeme

Der Aufwand für einen CAIRO CyberSecurityCheck inkl. NIS2 GAP-Analyse liegt im Bereich von 3-5 Tagen.

Startseite des CSC-Berichtes

Maßnahmenziel	Bewertet	Ergebnis
A - Absicherung von Netzübergängen	Ja	Schwerwiegender Sicherheitsmangel
B - Abwehr von Schadprogrammen	Ja	Sicherheitsmangel
C - Inventarisierung der IT-Systeme	Ja	Sicherheitsmangel
D - Vermeidung von Sicherheitslücken	Ja	Sicherheitsmangel
E - Sichere Interaktion mit dem Internet	Ja	Sicherheitsmangel
F - Logdatenerfassung und -auswertung	Ja	Schwerwiegender Sicherheitsmangel
G - Sicherstellung eines aktuellen Informationsstands	Ja	Sicherheitsmangel
H - Bewältigung von Sicherheitsvorfällen	Ja	Schwerwiegender Sicherheitsmangel
I - Sichere Authentisierung	Ja	Schwerwiegender Sicherheitsmangel
J - Verfügbarkeit notwendiger Ressourcen	Ja	Sicherheitsmangel
K - Sensibilisierung und Schulung von Mitarbeitern	Ja	Sicherheitsmangel
L - Sichere Nutzung sozialer Netzwerke	Ja	Sicherheitsmangel
M - Durchführung von Penetrationstests	Ja	Sicherheitsmangel
N - Sicherer Umgang mit Cloud-Anwendungen	Ja	Sicherheitsmangel
O - Governance und organisatorische Sicherheitsmaßnahmen	Ja	Sicherheitsmangel
P - Kritische Lieferanten und Drittanbieter	Ja	Keine Mängel festgestellt
Q - Datenschutz und Vertraulichkeit	Nein	Nicht geprüft
R - Prüf- und Betriebspflichten	Nein	Nicht geprüft
S - Zusammenarbeit mit Behörden und anderen Organisationen	Nein	Nicht geprüft
T - Krisenmanagement und Widerstandsfähigkeit	Ja	Schwerwiegender Sicherheitsmangel
U - Sicherheit der Lieferkette	Ja	Keine Mängel festgestellt
V - Kryptografie und Verschlüsselung	Nein	Nicht geprüft

Die finale Risikoeinschätzung

Beispielhafte Kurzdarstellung einer Risikoanalyse nach den Norm-Kriterien C, I, A (Confidentiality, Integrity, Availability):

Bestimmung des Bedrohungsgrads	Vertraulichkeit	Verfügbarkeit	Integrität
Wert der Daten und Prozesse	3	3	2
Schadenswert	**3**	**2**	**2**
Abhängigkeit von der IT und Grad der Vernetzung (Attraktivität für den Angreifer)	2	2	1
Kompetenz (Wissen) der Angreifer	2	2	2
Angriffe in der Vergangenheit	1	1	1
Eintrittswahrscheinlichkeit (Summe)	**5**	**5**	**4**
Ergebnis der **Risikoeinschätzung** (Schadenswert x Eintrittswahrscheinlichkeit)	**15**	**10**	**8**

Für die optionale NIS2-Konformität bewerten wir zusätzlich:

- Sicherheitsrichtlinien
- Vorfallsmanagement & Notfallpläne
- Krisenmanagement
- Lieferkettensicherheit
- Schulung und Bewusstsein
- Verschlüsselung und Zugangskontrolle
- Schwachstellen- und Patch-Management

Leistungen auf einen Blick

- Risikoorientierte Analyse Ihrer IT-Infrastruktur und Organisation
- Bewertung und Priorisierung von Schwachstellen
- Umfassender, normkonformer Bericht mit konkreten Handlungsempfehlungen
- Ganzheitliche Betrachtung Ihrer IT-Sicherheit – zugeschnitten auf Ihr Unternehmen

Der CAIRO CSC ist ein schneller, zielführender Einstieg in ein ISMS oder ein zentrales IT-Schwachstellen-Management z.B. mit CAIRO HackGuard.

Der CAIRO CyberSecurityCheck ist Teil unseres Security- & Compliance-Portfolios von normgerechten Security-Prüfungen über Schwachstellenmanagement bis hin zum sicheren IT-Betrieb mit modernen Lösungen, CAIRO Security Managed Services, Awareness Trainings oder der Erstellung eines ISMS.

CAIRO als Sicherheitsspezialist ist nach VdS 10000 für ein Informationssicherheits-Managementsystem zertifiziert.

CAIRO
Your IT. Our Mission.

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