

## Unser Angebot zur Stellung des Beauftragten für Informationssicherheit (BfIS)

Bis zum 31.12.2020 musste jede sächsische Kommune gemäß § 8 und 20 SächsISichG einen **Beauftragten für Informationssicherheit (BfIS)** benennen. Gemäß der SächsISichG kann dies auch ein externer BfIS sein. Zudem ist das **Sicherheitskonzept** erstmals im Jahre **2024** einer **Revision nach § 14 Satz 2 SächsISichG** zu unterziehen.



Ein **Interessenkonflikt** kann unterstellt werden, wenn der **Datenschutzbeauftragte** oder **Administrator** zum **Beauftragten für Informationssicherheit** benannt werden und sich daher selbst überprüfen muss.

In Deutschland entstehen laut Bitkom **jährlich** mehr als **200 Mrd. € Schaden** durch Cyberkriminalität. Ein immer größer werdender Trend der **Cyberkriminalität** ist „**Ransomware-as-a-Service**“, eine Dienstleistung, bei der erfahrene Hacker ihre Schadprogramme an jedermann vermieten. So können selbst Unerfahrene mit minimalem Aufwand erhebliche Schäden verursachen.

Ein erfahrener BfIS ist besonders in diesen Zeiten für Kommunen unerlässlich, da er nötiges **Fachwissen** in einer Zeit bietet, in der die **Cyber-Bedrohung** durch Zukunftstechnologien wie Künstliche Intelligenz stark ansteigt.

- **2 Ransomware-Angriffe** auf **Kommunalverwaltungen** oder kommunale Betriebe wurden durchschnittlich **pro Monat** bekannt
- Durchschnittlich rund **775 E-Mails** mit **Schadprogrammen** wurden **an jedem Tag** im Berichtszeitraum in deutschen Regierungsnetzen abgefangen
- **66 %** aller **Spam-Mails** im Berichtszeitraum waren **Cyberangriffe**, davon 34 % Erpressungsmails und 33 % Betrugsmails
- **84 %** aller betrügerischen E-Mails waren **Phishing-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen
- **370 Webseiten** wurden im Durchschnitt **an jedem Tag des Berichtszeitraums** für den Zugriff aus den Regierungsnetzen gesperrt, Ursachen waren **Schadprogramme**
- eine **250.000** neue **Schadprogramm-Varianten** wurden durchschnittlich **an jedem Tag** im Berichtszeitraum gefunden

Quelle: BSI : Die Lage der IT-Sicherheit in Deutschland, 2023 im Überblick

## Aufgaben des Beauftragten für Informationssicherheit

- Erstellung und Umsetzung von Regeln und **Richtlinien zur Informationssicherheit**
- **Schulung der Mitarbeiter** im Bereich der IT-Sicherheit
- **Dokumentation** der Aktivitäten zur IT-Sicherheit
- **Risikoanalyse** / Unterrichtung der Verwaltung zum Status quo der IT-Sicherheit
- Anpassung, Aktualisierung und Prüfung **der IT-Sicherheitskonzepte**
- Funktion als **zentraler Ansprechpartner** im Bereich der IT- Sicherheit
- Entwicklung und Umsetzung eines **Notfallmanagements** sowie einer **IT-Sicherheitsleitlinie**
- Führung und Weiterentwicklung von der **IT-Sicherheitsorganisation**



## Ihre Vorteile bei einem externen Beauftragten für die Informations- bzw. IT-Sicherheit

- wir unterstützen Sie bei der **Einführung des Informationsmanagementsystems**
- **keine Weiterbildungskosten** für Sie, wir bilden uns regelmäßig weiter
- Unterstützung bei der Erstellung der **gesetzlich vorgeschriebenen IT-Sicherheitskonzeption**
- **langjährige Erfahrung** im Bereich kommunaler Datenschutz und Informationssicherheit

## Wir unterstützen Sie gerne!



### 1997- 2000

Studium der Betriebswirtschaft  
Berufsakademie Sachsen in Glauchau

### 2001- 2005

Studium der Wirtschaftspädagogik  
Universität Leipzig

### seit 2007

Inhaber conceptic Leipzig  
Unternehmensberatung  
nebenberuflich: freiberuflicher Dozent

### seit 2018

externer Datenschutzbeauftragter (TÜV®)

### seit 2023

Informationssicherheitsbeauftragter (TÜV®)

Für eine unverbindliche **Beratung** und eine erste **Kostenabschätzung** kontaktieren Sie uns bitte telefonisch unter der **0172 3532932** oder per E-Mail an **[mh@conceptic-leipzig.de](mailto:mh@conceptic-leipzig.de)**.