Informationssicherheit - Industrial Security

Dieses Dokument wurde erstellt am 17.06.2019

Inhaltsverzeichnis

- Grundlagen der Informationssicherheit – Industrial Security
  - Festlegung einer Struktur
  - Erlassen von Verhaltensvorschriften
  - Klassifizierung
  - Unterweisungen – "Need to know"
  - Rechtsgrundlagen
- Schutz des Unternehmens
  - Informationssicherheitshandbuch
  - ÖNORM S 2450 Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen (Ausgabe vom 1. Mai 2014)
  - Physische Sicherheit – Punktesystem
  - Abhörsicherheit
  - Kryptostrategie
  - Weiterführende Links
  - Rechtsgrundlagen
- Sicherheitsunbedenklichkeitsbescheinigung – Facility Security Clearance
  - Merkblatt
- Österreichische Organisationsstruktur
  - Die Informationssicherheitskommission (ISK)
  - Das Büro der Informationssicherheitskommission (ISB)
  - Weiterführende Informationen und Unterlagen
  - Kontakt

Informationssicherheit – Industrial Security

Aktuelle Informationen über Informationssicherheit Industrial Security, Sicherheitsunbedenklichkeitsbescheinigung, Facility Security Clearance, Schutz des Unternehmens etc.

Information für Einsteiger

Im Zuge von Ausschreibungen und Forschungsaufträgen in Programmen auf EU-Ebene verlangen ausschreibende Stellen von den bewerbenden Unternehmen vermehrt eine Bestätigung über die Einhaltung von Standards auf dem Gebiet der Informationssicherheit. Die Bestätigungen über die Einhaltung von Standards auf dem Gebiet der Informationssicherheit werden gemäß Informations-Sicherheitsgesetz in Österreich **"Sicherheitsunbedenklichkeitsbescheinigungen"** für Unternehmen und Anlagen genannt und durch die Informationssicherheitskommission im Bundeskanzleramt nach Überprüfung der Einhaltung entsprechender Vorschriften im Umgang mit klassifizierten Informationen ausgestellt. Als Grundlage für diese Überprüfungen dient die ÖNORM S 2450 "Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen" vom 1. Mai 2014.

Aber nicht nur auf Grund derartiger Formalerfordernisse ist es für Unternehmen wichtig und ratsam, seine Daten gut zu schützen. Vor dem Hintergrund der rasch fortschreitenden Globalisierung und der wirtschaftlichen Entwicklung im Osten und im asiatischen Raum ist in den letzten Jahren eine zunehmende **Bedrohung** der westeuropäischen und damit auch der österreichischen Wirtschaft **durch ungewollten Informationsabfluss bzw. die Ausspähung österreichischer Unternehmen** entstanden.

Um dieser Entwicklung entgegenzuwirken, wurden in nahezu allen europäischen Ländern und in diversen Bereichen des öffentlichen und privaten Sektors Schutzmaßnahmen entwickelt, mit denen es mitzuhalten gilt.

Schließlich erhält Österreich aufgrund völkerrechtlicher Verpflichtungen immer wieder Informationen, für die ein besonderes Schutzbedürfnis besteht und für die geeignete Schutzmechanismen vorzusehen sind. Derartige Maßnahmen umfassen sowohl die physische Sicherheit (wie beispielsweise bauliche Maßnahmen, Zutrittskontrollen etc.) als auch personelle, organisatorische und – bei Verarbeitung mittels Informationstechnologie – die EDV-mäßige Sicherheit (INFOSEC).

Die folgenden Informationen sollen dazu beitragen, Unternehmen und vor allem unternehmenswichtige Informationen ausreichend zu schützen. Sie geben Unternehmerinnen/Unternehmern weiters ein einfaches Instrument in die Hand, die Position ihres Unternehmens im Bereich der Informationssicherheit selbst zu beurteilen.

Stand: 01.01.2018

Abgenommen durch:

- Bundeskanzleramt

Grundlagen der Informationssicherheit – Industrial Security

Festlegung einer Struktur

Für jedes Unternehmen ist eine für die Informationssicherheit verantwortliche Person zu bestellen, die sämtliche Maßnahmen koordiniert und auch als Ansprechpartnerin/Ansprechpartner innerhalb und außerhalb des Unternehmens fungiert.

Erlassen von Verhaltensvorschriften

Durch verbindliche Verhaltensvorschriften für alle Mitarbeiterinnen/Mitarbeiter werden im Unternehmen die Regeln für die Informationssicherheit festgelegt.

Als Anhaltspunkte dafür können folgende Unterlagen herangezogen werden:

- Gesetze und Verordnungen, wie beispielsweise die Geheimschutzordnung des Bundes (GSO), das Informationssicherheitsgesetz (InfoSiG), die dazu ergangene Informationssicherheitsverordnung (InfoSiV), Dienstanweisungen zur Erstellung unternehmensspezifischer Anweisungen für Informationssicherheit
- systemspezifische Sicherheitsanforderungen (System-specific Security Requirement Statements, kurz SSRS genannt) und sicherheitsrelevante Betriebsverfahren (Secure Operating Procedures, kurz SecOPs genannt):
  - IT-Anlagen, in denen klassifizierte Informationen verarbeitet werden, müssen abgesichert werden. Die Verfahrensvorschriften müssen dokumentiert werden.

Klassifizierung

Besonders schützenswerte Informationen unterschiedlichen Inhaltes werden je nach erforderlichem Schutzniveau einer **Klassifizierungsstufe** zugeordnet (entsprechend dem Informationssicherheitsgesetz: **Eingeschränkt**, **Vertraulich**, **Geheim** oder **Streng Geheim**) und mit einem der Stufe entsprechendem Klassifizierungs-vermerk versehen.

Unterweisungen – "Need to know"

Der Zugang zu klassifizierten Information darf nur nach einer entsprechenden Unterweisung und – ab der Stufe **Vertraulich** – nach erfolgter Sicherheitsüberprüfung der Person erfolgen, sofern der Zugang zur Erfüllung der dienstlichen Aufgaben erforderlich ist (Need-to-Know-Prinzip).

Rechtsgrundlagen

- ≫ Informationssicherheitsgesetz (InfoSiG)
- ≫ Informationssicherheitsverordnung (InfoSiV)

Stand: 01.01.2018

Abgenommen durch:

- Bundeskanzleramt

Schutz des Unternehmens

Die Informationssicherheitskommission (ISK) im Bundeskanzleramt erarbeitete eine Reihe von Unterlagen, um es Unternehmen und Dienststellen zu erleichtern, ein hohes Maß an Informations-sicherheit in ihrem Bereich umzusetzen.

Informationssicherheitshandbuch

Das **Österreichische Informationssicherheitshandbuch** ist ein Leitfaden, mit dessen Hilfe einfach und effizient ein umfassender Grundschutz in Unternehmen und Organisationen realisiert werden kann. Sicherheit berührt jede Einzelne/jeden Einzelnen in öffentlichen Institutionen, Unternehmen und Organisationen – von der Standortwahl bis zur Systemadministration, vom Management bis zur Anwenderin/zum Anwender.

Das Handbuch besteht aus den Teilen **Informationssicherheitsmanagement** und **Informationssicherheitsmaßnahmen**. Die Thematik "Sicherheit von Informationen" wird darin ganzheitlich dargestellt, unabhängig davon, ob sich diese auf Papier befinden oder in elektronischer Form vorliegen. Bewusst werden die Themen in allgemein formulierter Weise behandelt, um sowohl einen breiten Personenkreis anzusprechen, als auch um auf eine Vielfalt von Informationssystemen anwendbar zu sein. Das Informationssicherheitshandbuch kann über ≫ www.sicherheitshandbuch.gv.at aus dem Internet heruntergeladen werden.

ÖNORM S 2450 Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen (Ausgabe vom 1. Mai 2014)

Diese ÖNORM legt allgemeine Sicherheitsanforderungen an natürliche und juristische Personen fest, die im Rahmen von Auftragsverfahren Zugang zu klassifizierten Informationen bis zur Stufe **Geheim** erlangen wollen. Die geforderten Maßnahmen dienen dem Schutz klassifizierter Informationen vor unbefugtem Zugriff oder unberechtigter Weitergabe. Damit definiert sie zugleich die Anforderungen für die Erlangung einer Sicherheitsunbedenklichkeitsbescheinigung gemäß § 12 Abs 4 Informationssicherheitsgesetz (InfoSiG).

Physische Sicherheit – Punktesystem

Um die physische Sicherheit eines Unternehmens zu beurteilen wurde als Hilfestellung ein Punktesystem entwickelt **(Richtlinien für den materiellen Geheimschutz klassifizierter Informationen)**, mit dessen Hilfe die Qualität der baulichen Absicherungsmaßnahmen abgeschätzt werden kann. Die Richtlinien können über das Büro der Informationssicherheitskommission im Bundeskanzleramt bezogen werden.

Abhörsicherheit

Um die Abhörsicherheit von bestimmten Bereichen zu gewährleisten, müssen diese verschiedenen Qualitätskriterien entsprechen, die bereits beim Bau derartiger Räumlichkeiten beachtet werden. Weiterführende Unterlagen können über das Büro der Informationssicherheitskommission im Bundeskanzleramt bezogen werden.

Kryptostrategie

Ein wesentlicher Teil der elektronischen Absicherung ist die Verschlüsselung schützenswerter Daten sowohl bei der Ablage in elektronischen Systemen als auch bei deren elektronischer Übermittlung. Dabei ist neben dem anzuwendenden Verschlüsselungsalgorithmus auch auf das erforderliche Schlüsselmanagement zu achten. Weiterführende Unterlagen darüber können über das Büro der Informationssicherheitskommission im Bundeskanzleramt bezogen werden.

Weiterführende Links

- ≫ Österreichisches Informationssicherheitshandbuch (BKA)

Rechtsgrundlagen

- § ≫ 12 Abs 4 ≫ Informationssicherheitsgesetz (InfoSIG)

Stand: 01.01.2018

Abgenommen durch:

- Bundeskanzleramt

Sicherheitsunbedenklichkeitsbescheinigung – Facility Security Clearance

International werden für bestimmte Aufträge, insbesondere, wenn sie im Zusammenhang mit staatlich klassifizierten Informationen stehen, sogenannte "Sicherheits-unbedenklich-keits-bescheinigungen" (internationale Bezeichnung " Facility Security Clearance", kurz "FSC") von den Auftragnehmerinnen/den Auftragnehmern verlangt. Sie stellen eine staatliche Bestätigung dar, dass das Unternehmen einen ausreichenden Schutz für klassifizierte Informationen bieten kann. Die Basis für derartige Überprüfungen stellt die ÖNORM S 2450 "Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen" vom 1. Mai 2014 dar.

Merkblatt

Für die Erlangung einer derartigen Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen und Anlagen wurde seitens der Informationssicherheitskommission im Bundeskanzleramt ein Merkblatt ausgearbeitet, in dem alle relevanten Informationen übersichtlich zusammengefasst sind. Das Merkblatt kann über das Büro der Informationssicherheitskommission im Bundeskanzleramt bezogen werden.

Stand: 01.01.2018

Abgenommen durch:

- Bundeskanzleramt

Österreichische Organisationsstruktur

Die Informationssicherheitskommission (ISK)

Die Informationssicherheitskommission im Bundeskanzleramt fungiert als nationale und international anerkannte Anlaufstelle (NSA – National Security Authority) für alle Fragen auf dem Gebiet der Informationssicherheit und den dafür relevanten Bereichen wie personelle Sicherheit, physische Sicherheit, Dokumentensicherheit bzw. Registerführung und Information Security, sowie als nationale Akkreditierungsstelle für innerstaatliche Einrichtungen im Zusammenhang mit der Verarbeitung klassifizierter Informationen.

Das Büro der Informationssicherheitskommission (ISB)

Die Abteilung I/12 des Bundeskanzleramts ist einerseits die Geschäftsstelle für die Informationssicherheitskommission und andererseits für Fragen der Informationssicherheit für das Bundeskanzleramt zuständig. Darüber hinaus werden/wird durch das Büro der Informationssicherheitskommission gemeinsam mit Fachleuten anderer Ressorts Richtlinien und Empfehlungen für den Bereich klassifizierter Informationen erarbeitet, Österreich in international sicherheitsrelevanten Gremien der EU vertreten, internationale Inspektionen seitens EU und in Österreich koordiniert und die gesetzlich vorgeschriebenen Unterweisungen für Mitarbeiterinnen/Mitarbeiter durchgeführt.

Weiterführende Informationen und Unterlagen

Im Büro der Informationssicherheitskommission des Bundeskanzleramtes, Abteilung I/12, können weiterführende Unterlagen wie beispielsweise die Richtlinien für den materiellen Geheimschutz klassifizierter Informationen und Informationen zum Thema Informationssicherheit eingeholt werden.

Kontakt

Büro der Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2, Abt. I/12
1014 Wien
Tel.: 01/53-115-202594
E-Mail: isk@bka.gv.at

Stand: 01.01.2018

Abgenommen durch:

- Bundeskanzleramt