

## | IT-Sicherheitsberatung

### Kurzbeschreibung des Produktes

IT-Sicherheit ist gerade im Umfeld der öffentlichen Verwaltung von besonderer Bedeutung. In der Verwaltung werden vielfach personenbezogene Daten verarbeitet, die einen besonderen Schutzbedarf haben. Hierbei ist ein professionelles Sicherheitsmanagement nötig.

Das ITDZ Berlin berät Sie in allen Phasen des Sicherheitsmanagements von der Planung bis zum Betrieb Ihrer Systeme und unterstützt Sie, diese sicher und rechtskonform zu gestalten. Folgende Dienstleistungen und Produkte bieten wir Ihnen an:

#### IT-Sicherheitsanalysen

Eine IT-Sicherheitsanalyse ist ein Verfahren zur Erkennung von Bedrohungen, die bei der Nutzung der Informationstechnik entstehen. Für die erkannten Bedrohungen werden Eintrittswahrscheinlichkeit und das Schadenspotenzial geschätzt oder, wenn es möglich ist, ermittelt. Das Ergebnis einer IT-Sicherheitsanalyse kann ein Maßnahmenkatalog sein, dessen Umsetzung zur Erhöhung der Sicherheit der Datenverarbeitung innerhalb der betrachteten IT-Infrastruktur oder des IT-Verfahrens führt.

Die Sicherheitsanalyse kann unabhängig von der Erstellung eines Sicherheitskonzeptes durchgeführt werden. Das Ziel der Beauftragung kann aber auch sein, zu überprüfen, ob die Notwendigkeit zur Erstellung eines IT-Sicherheitskonzeptes besteht.



## | IT-Sicherheitsberatung

### IT-Sicherheitsaudits

IT-Sicherheitsaudits dienen der Überprüfung des Umsetzungsgrades der existierenden Sicherheitskonzepte oder der Sicherheitsuntersuchung einer Netz- und/oder Systemkonfiguration. Ein IT-Sicherheitsaudit wird mit einem Bericht abgeschlossen, in dem die vorgenommene Untersuchung, die während des Audits ergriffenen Maßnahmen und die als Ergebnis der Untersuchung vorgeschlagenen Sicherheitsvorkehrungen beschrieben werden.

### IT-Sicherheitsgutachten

Im Rahmen von IT-Sicherheitsgutachten werden sicherheitsrelevante Sachverhalte geprüft. Beispielsweise kann ein vorliegendes IT-Sicherheitskonzept auf Eignung für den vorgesehenen Einsatz geprüft werden. Diese Art des Gutachtens beinhaltet die Prüfung der methodischen Richtigkeit des Sicherheitskonzeptes. Des Weiteren wird die Konformität des Dokuments mit den in Berlin geltenden Vorschriften und die Kontrolle der Vollständigkeit der Sicherheitsbetrachtungen und der Richtigkeit der Schlussfolgerungen untersucht.

### IT-Sicherheitskonzepte

Zielstellung eines Sicherheitskonzeptes ist die Analyse der Gefährdungen und Risiken, die beim Einsatz der Informationstechnik entstehen sowie die Ableitung adäquater Sicherheitsmaßnahmen. Im Rahmen dieses Produkts wird ein Sicherheitskonzept erstellt, in dem die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben werden.

## Leistungsbeschreibung

### IT-Sicherheitsanalysen

Im Rahmen einer IT-Sicherheitsanalyse wird ein Standort, ein IT-Verfahren oder eine IT-Infrastruktur auf mögliche Sicherheitsrisiken hin untersucht. Als Teil der IT-Infrastruktur kann die Kommunikationssicherheit allein Gegenstand der IT-Sicherheitsanalyse sein.

Die IT-Sicherheitsanalysen sind nach folgendem Schema gegliedert:

- Beschreibung des Anwendungsbereichs (Behörde, Verfahren, Infrastruktur, Kommunikation)

## | IT-Sicherheitsberatung

- Systematisierung und generische Beschreibung der bedrohten Objekte
- Schutzbedarfsfeststellung
- Ermitteln der Bedrohungen aus der Schwachstellenanalyse unter Berücksichtigung bereits realisierter IT-Sicherheitsmaßnahmen
- Bewertung der Risiken
- Zusammenfassung von Gefährdungs- und Objektgruppen zur Ableitung von IT-Sicherheitsbausteinen

Damit werden fundierte Aussagen zur IT-Sicherheit geleistet, die ggf. auch die Grundlage für abzuleitende IT-Sicherheitsmaßnahmen darstellen. Zwischen den Produkten IT-Sicherheitsanalyse und IT-Sicherheitskonzept besteht ein Zusammenhang: Für die Anforderungen des hohen Schutzbedarfs ist im IT-Sicherheitskonzept eine Risikoanalyse durchzuführen. Sie basiert auf den Ergebnissen der IT-Sicherheitsanalyse. Daher schließt das Produkt IT-Sicherheitskonzept für diesen Fall die Leistungen der IT-Sicherheitsanalyse ein.

### **IT-Sicherheitsaudits**

Im Prozess des IT-Sicherheitsaudits werden die in existierenden Sicherheitskonzepten berücksichtigten Sicherheitsmaßnahmen auf ihre Wirksamkeit und die zu erreichende Sicherheit geprüft. Die Überprüfungen basieren auf Anforderungen der IT-Grundschutz-Kataloge und des IT-Sicherheitshandbuchs des BSI.

In der ersten Stufe des IT-Sicherheitsaudits findet eine Konkretisierung des Prüfungsauftrages statt. Dazu wird die IT-Umgebung beschrieben und die seit der letzten Prüfung an der IT-Infrastruktur vorgenommenen Veränderungen dokumentiert. Ebenfalls werden die Änderungen organisatorischer Art berücksichtigt.

Im nächsten Schritt werden die vorhandenen Sicherheitskonzepte auf Aktualität und Vollständigkeit untersucht. Danach folgt die Prüfung des Grades der Umsetzung der durch die Sicherheitskonzepte vorgeschlagenen Maßnahmen, aber auch die Aktualität der umgesetzten Maßnahmen. Die Ergebnisse der Untersuchung werden dokumentiert. Als Ergebnis können Folgemaßnahmen empfohlen werden (z.B. Durchführung einer Risikoanalyse).

Das Audit wird mit der Auswertung der Prüfungsergebnisse und Formulierung der Empfehlungen zur Steigerung der Sicherheit abgeschlossen.

## | IT-Sicherheitsberatung

### IT-Sicherheitsgutachten

Ein IT-Sicherheitsgutachten hat das Ziel, einen beschriebenen sicherheitsrelevanten Sachverhalt zu bewerten. Das kann die Prüfung eines IT-Sicherheitskonzepts sein, aber auch die Evaluation von Verfahrensbeschreibungen oder Lösungsansätzen. Das IT-Sicherheitsgutachten bewertet diesen nach formalen (z.B. Übereinstimmung mit den Vorgaben des BSI) und inhaltlichen Aspekten.

### IT-Sicherheitskonzepte

Bei der Erstellung eines Sicherheitskonzepts werden mögliche Angriffs- und Schadensszenarien analysiert. Ziel ist es mit der Festlegung geeigneter Maßnahmen ein definiertes Schutzniveau zu erreichen.

Die IT-Sicherheitskonzepte sind nach folgendem Schema gegliedert:

- Beschreibung des Anwendungsbereichs (Behörde, Verfahren, Infrastruktur, Kommunikation)
- Schutzbedarfsfeststellung
- Anwendung des IT-Grundschutzes
- Risikoanalyse bei hohem Schutzbedarf
- Entwicklung von Maßnahmen zur Reduzierung des Risikos bzw. des Schadens
- Restrisikoanalyse bei hohem Schutzbedarf und Bewertung des Restrisikos
- Verantwortlichkeiten für die Umsetzung der vorgesehenen Maßnahmen
- Umsetzungsplan (Zeitplan mit Prioritäten und Fortschreibung, Kosten)

Das methodische Vorgehen stützt sich dabei je nach Art des Sicherheitskonzepts auf die IT-Grundschutz-Kataloge oder auf das IT-Sicherheitshandbuch des BSI. Die Schutzbedarfsfeststellung analysiert anhand der Gewährleistung der Schutzgütekriterien

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität und
- Nachweisbarkeit.

Für hochschutzbedürftige IT-Systeme, wie sie in der öffentlichen Verwaltung in der Regel vorliegen, sehen beide Methodiken des BSI die Durchführung einer Risikoanalyse vor. Diese hat unter anderem das Ziel, Maßnahmen zu finden, die über den Grundschutz hinausreichen, um den ermittelten Gefährdungen genügend zu begegnen.

## | IT-Sicherheitsberatung

### Rahmenbedingungen

Die Dienstleistungen basieren auf gesicherten Kenntnissen der IT-Infrastruktur in der Berliner Verwaltung und spezialisiertem Sicherheitswissen im ITDZ Berlin. Erforderlichenfalls wird externes Expertenwissen eingebunden.

Vor Beauftragung ist es notwendig, in einem gemeinsamen Gespräch mit unseren Sicherheitsberatern die Zielsetzung, den Bedarf und die Randbedingungen des Auftrags zu vereinbaren. Danach wird der zeitliche Aufwand vom ITDZ Berlin bestimmt und ein Angebot erstellt. Bei komplexen Vorhaben wird ein Stufenkonzept angeboten.

Der Auftraggeber hat Mitwirkungspflichten, die sich aus dem vereinbarten Vorgehen ableiten.

Die durch diese Dienstleistungen erstellten Dokumente werden in gedruckter und in elektronischer Form als pdf-Dateien übergeben. Auf Wunsch werden die Ergebnisse im Rahmen einer Präsentation erläutert.

### Lieferzeit und Gewährleistung

Die Lieferzeit richtet sich nach Umfang, Komplexität des Systems oder der Sicherheitsdomäne sowie den zur Verfügung stehenden Kapazitäten und liegt zwischen 4 und 26 Wochen ab der Beauftragung. Die Gewährleistung beträgt drei Monate.

### Kontakt

Für Fragen und Informationen zu Details der Dienstleistungen oder Konditionen, steht Ihnen gerne der Vertrieb im ITDZ Berlin zur Verfügung:

IT-Dienstleistungszentrum Berlin  
Berliner Straße 112 - 115 · 10713 Berlin  
Tel.: +49 30 90222 (9222) 8090  
Fax: +49 30 90222 (9222) 5864  
E-Mail: [Info@itdz-berlin.de](mailto:Info@itdz-berlin.de)