

Informationen zum Basis-Sicherheitscheck BSI IT-Grundschutz

BSI IT-Grundschutz als Konzept zum IT-Sicherheitsmanagement in Unternehmen

In Zeiten von Viren, Spyware und täglich neu auftretenden Sicherheitslücken ist ein funktionierendes IT-Sicherheitsmanagement wichtiger Bestandteil für den wirtschaftlichen Erfolg eines Unternehmens. Dies hat auch der Gesetzgeber in Deutschland erkannt und eine Reihe von Gesetzen und Vorschriften erlassen, die IT-Sicherheit als zentralen Aspekt der Unternehmensführung definieren.

Das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) und Basel II sind die bekanntesten Stichworte. Basel II legt unter anderem fest, welche Punkte für das Rating eines Unternehmens bei der Kreditvergabe Beachtung finden. „Business Continuity“ ist dabei das Credo - der möglichst unterbrechungsfreie Ablauf der Geschäftsprozesse, den es zu erreichen gilt. Das IT-Grundschutzhandbuch (GSHB) des Bundesamts für Sicherheit in der Informationstechnik (BSI) bietet hierzu ein anerkanntes „Kochrezept“, bei dem neben Eintrittswahrscheinlichkeiten und potentieller Schadenshöhe auch die Kosten der Umsetzung berücksichtigt werden.

IT-Sicherheit sollte Chefsache sein. Unabhängig von den gesetzlichen Bestimmungen und den daraus resultierenden Pflichten, lohnt sich eine intensive Beschäftigung mit diesem Thema. Basel II zeigt, dass ein funktionierendes IT-Sicherheitsmanagement direkte monetäre Vorteile mit sich bringen kann und nicht nur ein notwendiges Übel ist.

Durchführung des Sicherheitschecks

Mit Hilfe des Basisaudits erhalten Sie eine erste Einschätzung der Ist-Situation von IT-Sicherheit und Datenschutz in Ihrem Unternehmen. Hierbei werden grundlegende Elemente und Vorgehensweisen des BSI GSHB und der internationalen Norm ISO 17799 (Code of practice for information security management) berücksichtigt.

Ablauf eines Basis-Sicherheitschecks BSI IT-Grundschutz

1. Definition des IT-Verbunds
2. IT-Strukturanalyse
3. Basis-Sicherheitscheck
4. Dokumentation der Ergebnisse und Maßnahmenempfehlungen

Nach der initialen Definition des IT-Verbunds* erfolgt die IT-Strukturanalyse, bei der ein bereinigter Netzplan angefertigt wird. Auf Basis dieser Informationen wird nun mit Hilfe von Interviews der Status Quo des IT-Verbunds im Bezug auf den Umsetzungsgrad der vom BSI definierten Sicherheitsmaßnahmen ermittelt. Das Ergebnis dieses Sicherheitschecks ist die Grundlage für Maßnahmenempfehlungen, die abschließend ausgesprochen werden. Durch Umsetzung dieser Empfehlungen erhält das Unternehmen ein dokumentiertes Sicherheitsniveau auf Grundlage der Konzepte des IT-Grundschutzes.

Komponenten des Basis-Sicherheitschecks nach BSI Schichtenmodell

Übergreifende Aspekte

Organisation, Personal, Notfallvorsorge-Konzepte, Datensicherungskonzepte, ...

Infrastruktur

Gebäude, Verkabelung, Büroräume, Serverräume, Datenträgerarchivie, ...

IT-Systeme

Server, Clients, Netzkomponenten, TK-Anlagen, Faxgeräte, ...

Netze

Heterogene Netze, Netz- und Systemmanagement, Modems, RAS, ...

IT-Anwendungen

Peer-to-Peer Dienste, E-Mail, Webserver, Datenbanken, Faxserver, ...

*Ein IT-Verbund stellt die Gesamtheit aller infrastruktur-ellen, organisatorischen, personellen und technischen Komponenten dar, die für den Betrieb der IT notwendig sind.



Secutrends GmbH

Secutrends GmbH
Im Westpark 8
D-35435 Wettenberg

Kontakt

Fon: +49 641 250390 0

Fax: +49 641 250390 100

E-Mail: sales@secutrends.com

Web: www.secutrends.com