

IT-SICHERHEIT

BSI-Anforderungen erfüllen mit econet

Die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik stellen hohe Anforderungen an die Verwaltung von Benutzern und Berechtigungen:

- Transparente und lückenlose Erfassung und Darstellung der Zugriffsrechte
- Ein geregeltes Verfahren für die Vergabe und den Entzug von Zugriffsrechten
- Eindeutige Dokumentation aller Änderungen in diesem Bereich

Nachfolgend eine Auswahl der hierzu in den IT-Grundschutzkatalogen geforderten Maßnahmen und Prüffragen (Stand: Mai 2014). Die Umsetzung der Maßnahmen wird von den Software-Lösungen und Spezialisten der econet GmbH entscheidend unterstützt.

M 2.8 Vergabe von Zugriffsrechten

- Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?
- Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?
- Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?
- Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?

M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle

- Existieren dem Schutzbedarf der Organisation angemessene Regelungen zur Zugangs- und Zugriffskontrolle?
- Existieren Standard-Rechteprofile, die den Funktionen und Aufgaben der Nutzer entsprechen?
- Existieren schriftliche Zugriffsregelungen sowie eine Dokumentation der Benutzereinrichtung und der Rechtevergabe?

M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen

- Bei zusätzlichen Zugriffsberechtigungen, die über das Standardprofil hinausgehen: Werden diese nur nach zusätzlicher Begründung vergeben?
- Gibt es eine geregelte Vorgehensweise zur Einrichtung von Benutzern und Benutzergruppen?
- Existiert eine separate administrative Rolle für das Einrichten von Rechten bzw. Rechteprofilen?

M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile

- Sind die zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile dokumentiert?
- Wird die Dokumentation der zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile regelmäßig auf Aktualität überprüft?

M 4.1 Passwortschutz für IT-Systeme

- Ist sichergestellt, dass nur berechtigte Personen auf Anwendungen und IT -Systeme zugreifen können?

M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

- Wird der Zugriff auf Systemdateien auf einen möglichst kleinen Kreis von Administratoren beschränkt?
- Erfolgt die Vergabe von Zugriffsrechten restriktiv und im Einklang mit den organisationseigenen Sicherheitsrichtlinien?
- Wird die Rechtevergabe aller Programme inklusive der von diesen aufgerufenen weiteren Programme überprüft?

M 4.149 Datei- und Freigabeberechtigungen unter Windows

- Wurde ein bedarfsgerechtes Berechtigungs- und Zugriffskonzept für Windows erstellt?
- Sind die Berechtigungen aller Verzeichnisse und Dateien auf allen, von einem älteren Windows-Betriebssystem aktualisierten, Rechnern überprüft worden?
- Sind die eingestellten Datei- und Verzeichnisberechtigungen von freigegebenen Verzeichnissen für den Netzzugriff geeignet? Wurden die Freigaben so restriktiv wie möglich vergeben?

M 4.163 Zugriffsrechte auf Exchange-Objekte

- Wurde die Rolle Exchange-Administrator definiert und eine entsprechende Benutzergruppe eingerichtet?
- Wurden die Zugriffsberechtigungen auf Exchange-Objekte auf der Grundlage der Sicherheitsrichtlinie festgelegt?

M 4.309 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste

- Wurden die Zugriffsrechte der Benutzer- und Administratorgruppen gemäß der erstellten Sicherheitsrichtlinie konfiguriert?
- Sind die Administratorrollen und die Delegation von Administrationsrechten konsistent konfiguriert?

Weiterführende Informationen

Die **IT Grundschutzkataloge** auf den Seiten des BSI

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html

Mehr über **IT Grundschutz** auf wikipedia.org

<http://de.wikipedia.org/wiki/IT-Grundschutz>

„**Was ist die ISO 27001 auf Basis IT-Grundschutz wert?**“ Artikel auf computerwoche.de vom 13.5.2014

<http://www.computerwoche.de/a/was-ist-die-iso-27001-auf-basis-it-grundschutz-wert,3060521>

Mehr über **IT-relevante Richtlinien und Gesetze** auf econet.de

<http://www.econet.de/consulting/compliance>