

Lizenzbestimmungen

- Diese Materialien sind lizenziert für @USERINFONAME@.
- Die Materialien dürfen **ausschließlich** für die Implementation, Verbesserung oder den Betrieb von Sicherheitsmaßnahmen innerhalb der genannten Organisation genutzt werden.
- Hierfür dürfen die Materialien beliebig verändert, ergänzt oder neu gestaltet werden.
- Für alle anderen Einsatzzwecke - insbesondere für die Veröffentlichung der Materialien und deren Einsatz für Kunden des Lizenznehmers - muss im Vorfeld eine schriftliche Genehmigung der 3473 Gurus GbR eingeholt bzw. eine entsprechende Lizenz erworben werden.

Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.

Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!



10.3.6 Starten von fremden Medien

Ref	VdS 10000	Kommentar
B1	Es MUSS sichergestellt werden, dass IT-Systeme nur von autorisierten Medien gestartet werden können.	<ul style="list-style-type: none"> • Diese Maßnahme soll verhindern, dass durch das Starten von fremden Medien wichtige Sicherheitsmaßnahmen umgangen (z.B. Zugriffsbeschränkungen) oder Schadprogramme eingeschleppt werden. • Um den Aufwand für die Umsetzung dieser Maßnahme zu verringern kann sie (in Anlehnung an den Geltungsbereich, siehe Abschnitt 1.2 E1) technisch, geographisch und/oder organisatorisch eingegrenzt werden. Es können bestimmte IT-Systeme (z. B. bereits bestehende IT-Systeme) oder Netzwerksegmente, Standorte oder Abteilungen von der Umsetzung ausgenommen werden. • Wenn die Maßnahme nicht bei allen IT-Systemen umgesetzt wird, bei denen es technisch möglich ist, muss in Risikoanalyse und -behandlung durchgeführt werden (siehe Abschnitt 10.3 B2).
E1	Die KANN z. B. über BIOS-Passwörter oder über den Zutrittschutz umgesetzt werden.	<ul style="list-style-type: none"> • Zur Umsetzung dieser Maßnahme kann z. B. das Boot-Rollenfolge im BIOS so festgelegt werden, dass das IT-System nur von den fest definierten Medien gestartet werden kann. Die Einstellung muss (z. B. über BIOS-Passwörter) vor Änderungen geschützt werden. • Für Server ist ein Zutrittschutz vorzusehen (siehe Abschnitt 13.1 G1), der die Umsetzung dieser Maßnahme ermöglicht werden kann. • Die Abwesenheit der Dokumentation von Lebenszyklen und Schnittstellen kann beeinflusst werden. Die Trennung der Medien voneinander (siehe Abschnitt 10.3.4 E1).



Die Seiten dieses Bereiches sollen Ihnen nur einen Eindruck vermitteln, welche Inhalte wir für Sie erarbeitet haben. **Deshalb sind die Inhalte absichtlich „verpixelt“**: mehr und mehr Buchstaben werden auf jeder Seite durch Punkte ersetzt.

Wenn Sie auf alle Inhalte zugreifen möchten, benötigen Sie einen entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren Informationen!