Lizenzbestimmungen

←→

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

Ref	VdS 10000	Kommentar
Z1	Alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen MÜSSEN jährlich erfasst und daraufhin überprüft werden, ob sie gemäß der Verfahren aus Abschnitt 15.1 angelegt wurden und benötigt werden.	Die gewählte Formulierung macht es erforderlich, dass die zum Zeitpunkt der Implementation bestehenden Zugänge zu kritischen IT-Systemen und Zugriffsrechte auf kritische Informationen strukturiert erfasst und analysiert werden.
Z2	Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte MÜSSEN als Sicherheitsvorfall (siehe Kapitel 18) behandelt werden.	• Neben nicht ordnungsgemäß angelegten Zugängen und Zugriffsrechten zu kritischen IT-Systemen sowie nicht ordnungsgemäß angelegten Zugriffsrechten auf kritische Informationen muss der Verlust eines mobilen IT-Systems (siehe Abschnitt 10.4.3 G4) und Hinweise an Netzübergängen auf Schadsoftware in der IT-Infrastruktur der Organisation und Angriffe aus der IT-Infrastruktur der Organisation heraus (siehe Abschnitt 11.3 B1.3 als Sicherheitsvorfall behandelt werden. • Darüb.r hinau. r.gt di. VdS 10000 an, Auffälligk.it.n zu d.fini.r.n, di. zur M.ldung .in.. pot.nti.ll.n Sich.rh.it.vorfall.. führ.n mü...n (.i.h. Ab.chnitt 18.1 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 eine entsprechenden Zugang.

Sie möchten einen Zugang erwerben? Hier finden Sie alle weiteren

Informationen!