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 entdprechende Lizenz erworben werden.

 © 2016 by 3473 Gurus GbR

include:free_version

←→

10.3.3 Protokollierung

Ref	VdS 10000	Kommentar
B1	Jedes IT-System MUSS erfolgreiche und erfolglose Anmeldeversuche, Fehler und Informationssicherheitsereignisse protokollieren.	• Eine strukturierte Protokollierung ist in der Praxis für das Erkennen und Analysieren von Störungen und Ausfällen (siehe Kapitel 17) sowie von Sicherheitsvorfällen (siehe Kapitel 18) unbedingt notwendig. • Die Maßnahme spricht davon, dass IT-Systeme protokollieren müssen. Damit ist gemeint, dass für die Umsetzung der Maßnahme die gesamte System- und Anwendungssoftware auf einem IT-System berücksichtigt werden muss. • Di. g.ford.rt. Protokolli.rung wird b.i d.n üblich.n B.tri.b..y.t.m.n im D..ktop- und S.rv.rumf.ld (Window., MacOS, Linux) b.r.it. mit d.n Standard-Ein.t.llung.n .rfüllt. Für di. voll.tändig. Um..tzung d.r Maßnahm. i.t .. j.doch notw.ndig, di. in.talli.rt. Anw.ndung..oftwar. zu unt.r.uch.n und - w.nn möglich - d.r.n Protokolli.rung anzupa…n. • Da. Logging d.r B.tri.b..y.t.m. iOS und Android kann nicht (od.r nur ..hr b.gr.nzt) konfiguri.rt w.rd.n. Für di… B.tri.b..y.t.m. mu.. di. Anford.rung nicht umg…tzt w.rd.n. • Vi.l. aktiv. N.tzw.rkkompon.nt.n (Rout.r, Switch.., Acc…point. .tc.) .ind in d.r Lag., d.tailli.rt. Protokoll. zu .r.t.ll.n, wodurch di. F.hl.r.uch. im N.tzw.rk oft .rh.blich v.r.infacht und b..chl.unigt wird. • Protokolld.t.n ..nd .n .ll.r R.g.l p.r.on.nb.zog.n. D.t.n, d. … .ntw.d.r d.r.kt m.t ..n.m Zug.ng v.rknüpft ..nd od.r ..n. .nt.pr.ch.nd. Zuordnung m.t w.n.g Aufw.nd h.rg..t.llt w.rd.n k.nn. D..h.lb .ollt. j.d. Protokoll..rung d.n Anford.rung.n d.. D.t.n.chutz.. und d.n .nt.pr.ch.nd.n R.g.lung.n für Nutz.r (…h. Ab.chn.tt 6.3 G1.6.) .nt.pr.ch.n. • D…. Vorg.b. b.z..ht ..ch .uf Anm.ld.v.r.uch., F.hl.r und Inform.t.on…ch.rh..t..r..gn…., d.. d.. j.w..l.g. IT-Sy.t.m b.tr.ff.n. Au. .hr k.nn n.cht .bg.l..t.t w.rd.n, d… .kt.v. N.tzw.rkkompon.nt.n (w.. z. B. F.r.w.ll.) .ämtl.ch. Inform.t.on…ch.rh..t..r..gn…. protokoll..r.n mü…n. D.. Anford.rung.n .n d.. Protokoll..rung von Inform.t.on…ch.rh..t..r..gn….n durch .kt.v. N.tzw.rkkompon.nt.n w.rd .n Ab.chn.tt 11.3 B1.3 und Ab.chn.tt 11.4.2 B2 f..tg.l.gt (wob.. b..d. M.ßn.hm.n durch ..n. R…ko.n.ly.. und -b.h.ndlung fl.x.b.l umg…tzt w.rd.n könn.n). • Um d.n A.fw.nd g.r.ng z. h.lt.n k.nn d.. M.ßn.hm. z. B. n.r f.r …g.w.hlt. IT-Sy.t.m. (w.. S.rv.r .nd .kt.v. N.tzw.rkk.mp.n.nt.n) .d.r …g.w.hlt. N.tzw.rk..gm.nt. .mg…tzt .nd ..n. .nt.pr.ch.nd. R…k..n.ly.. .nd - b.h.ndl.ng d.rchg.f.hrt w.rd.n („W.lch. R…k.n .nt.t.h.n d.r Org.n…t..n, w..l n.cht .ll. IT-Sy.t.m. .rf.lgr..ch. .nd .rf.lgl… Anm.ld.v.r..ch., F.hl.r .nd Inf.rm.t..n…ch.rh..t..r..gn…. pr.t.k.ll..rt w.rd.n?“).

Ref	VdS 10000	Kommentar
E1	Pr…k…d…n SOLLTEN z.n.r.. ……ch.r. w.rd.n.	• D.. z.n.r… S…ch.r.n. v.n Pr…k…d…n .r…ch..r. .hr. A..w.r..n., .ch..z. … v.r M.n……..n.n, k.nn .hr. V.rf..b.rk… .rh.h.n .nd v.rm..d.. S…ch.r….z.r.b..m. ..f d.n .r…k…..r.nd.n IT-Sy…m.n. • N.ch. …. IT-Sy….. k….. Pr…k…….. .. ….. z…r…. S.rv.r ……. • D.. U….z… …..r M.ß..h… b……. … z.r Üb.r.r….. ..r Pr…k…….. …..z.. N..zw.rk … z….z..ch.. V.rk.hr, w.. ….r ….r.. b.. N..zw.rk.. .. Ech.z…b..r..b …r …rk ……. N..zw.rk.. z. Pr.b….. ..hr.. k…. • D.. ..r … z…r… Pr…k…..r… ……..z… IT-Sy….. ……. k….q…. v.. r…..ch.. N..z …r…. …., ….. M…….. .. .h… … .. … ……. Pr…k…….. …..ch.. w… ……ch…… w.r… k…… S. ……. w…r ……..r…v. l…r..c.. .x…..r. …., ..ch V.r.r……. z. … r…..ch.. T….. ..r IT-I..r…r.k..r b….h.. (w.. … z. B. .. R.h… ….r D…..-S.r.k..r v.rz……. ….). E… U….z… ..r Tr…… k… …… z. Ab.ch…. 10.3.2 B1, Ab.ch…. 10.5.3 Z2 … Ab.ch…. 11.4.2 …….z. w.r….
@…h.b…:B2	Pr…k…….. MÜSSEN 6 M….. …. …b.w.hr. w.r…, ….r. k…. …..z..ch.. L..ch- …r A..b.w.hr……..ch… ……..h…	D. … Pr…k…….. h….. … … V.rh….. …z….r N..z.r …ch…… w.r… k…, ……. … ….r… … ..r…..b.z….. D…. ……h.. w.r…. E….r.ch…. H..w…. … L..ch- … A..b.w.hr……..ch… …… ..ch .. … K……..r….. ..r M.ß..h.. Ab.ch…. 6.3 G1.6.. … ..r E….h…. Ab.ch…. 6.3 E1.
@…h.b…:B3	D.. Uhr.. ….r IT-Sy….. MÜSSEN … …. ……. Z… .y.chr……r. …., .. A..w.r…… v.. L……r…. z. .r…..ch…	D.. Sy.chr…….. ..r Sy….z….. .r…ch..r. … A..w.r…. v.. Pr…k……., .. ….. … ….. Z……. v.r..h.. ….. D.. U….z… …..r M.ß..h.. .r..r..r. … N..z… ….. z…r…. Z…..b.r. (z. B. .b.r … NTP-Pr…k… …r … H…. ….. DCF77-E…….r.).

←→

include:free_version