Fazit und Ausblick

10

Vor dem Hintergrund des stark wachsenden Cloud-Marktes und der Digitalisierung werden Cloud-Services zukünftig eine gewichtige Rolle bei der Einhaltung von IT-Sicherheitsfragen spielen. Die Ressourcenbündelung und Vernetzung von Clouds führt zu Herausforderungen für das IT-Risikomanagement, insbesondere im Kontext der IT-Sicherheit und damit für Betreiber Kritischer Infrastrukturen (Ackermann 2013; Adelmeyer und Teuteberg 2018). Sofern KRITIS-Betreiber für ihre Funktion maßgebliche Systeme oder Prozesse in eine Cloud auslagern, verbleibt die Verantwortung der Einhaltung der Anforderungen des IT-Sicherheitsgesetztes beim auslagernden Unternehmen. Dieses muss Cloud-Dienstleister folglich zur Einhaltung von IT-Sicherheitsstandards verpflichten, bspw. durch eine entsprechende Vertragsgestaltung und die Definition und Überwachung von KPIs, SLAs oder über Prüfrechte und Zertifikate. Insbesondere bei Zertifikaten und externen Nachweisen sollte jedoch der Scope dieser genau analysiert werden, um das IT-Risikomanagement entsprechend ausgestalten zu können. Die vertraglichen Regelungen spielen bei der Übertragung der Anforderungen des IT-SiG an KRITIS auf den Cloud-Dienstleister eine wichtige Rolle. Eine Herausforderung für Wissenschaft und Praxis wird sein, Entwicklungen im Zuge der Digitalisierung der Gesellschaft und Industrie 4.0 beim Schutz Kritischer Infrastrukturen entsprechend zu integrieren. Der vorliegende Anforderungskatalog sowie das Framework zum IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen können in diesem Kontext als Basis zur konkreten Umsetzung eines IT-Sicherheits- bzw. Risikomanagements von Cloud-Services dienen.

M. Adelmeyer et al., *IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen,* essentials, https://doi.org/10.1007/978-3-658-22742-5_10