KRITIS: Compliance schaffen mit betreibersicheren Infrastrukturen

München – 26. Februar 2019: Was ist das eigentlich: der „Stand der Technik“? Wer in Deutschland so genannte „Kritische Infrastrukturen“ betreibt, ist nach dem IT-Sicherheitsgesetz und dem BSI-Gesetz dazu verpflichtet, IT-Systeme, -Prozesse und -Komponenten angemessen zu schützen.[1] Unter „Kritischen Infrastrukturen“ versteht man Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, deren Ausfall dramatische Folgen hätte. Wer als KRITIS-Betreiber gilt, ist wiederum in der KRITIS-Verordnung geregelt.[2]

Betroffene Unternehmen müssen sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren und erhalten dafür alle sie betreffenden Informationen zu Gefahren in der IT-Sicherheit, um entsprechende „technische und organisatorische Maßnahmen“ treffen zu können (BSI-Gesetz §8 a). Hierbei soll, so fordert es der Gesetzgeber, „der Stand der Technik“ eingehalten werden.[3]

Genau definiert ist dieser „Stand der Technik“ im Gesetz allerdings nicht. Das macht es KRITIS-Betreibern nicht gerade leichter, ihren Verpflichtungen nachzukommen.

Im „Stand der Technik“ ist die technische Entwicklung schon mitgedacht

Dabei muss man wissen: Die Formulierung „Stand der Technik“ ist deshalb gewählt, weil sich die IT-Sicherheitstechnik stets und schnell weiterentwickelt – und dem müssen die KRITIS-Betreiber kontinuierlich Rechnung tragen.

Wann aber ist nun beispielsweise eine Cloud-Infrastruktur auf dem „Stand der Technik“? IT-Sicherheitsexperte Dr. Hubert Jäger, CTO der TÜV SÜD-Tochter Uniscon, erklärt: „Anders als beispielsweise im Patentrecht ist der ‚Stand der Technik‘ in der IT-Sicherheit und im Datenschutz nicht mit dem fortschrittlichsten ‚Stand der Wissenschaft und Technik‘ identisch, insgesamt aber fortschrittlicher zu bewerten als die so genannten ‚Anerkannten Regeln der Technik‘.“

„Eine IT-Infrastruktur muss also, um auch den Anforderungen von IT-Sicherheitsgesetz bzw. BSI-Gesetz zu genügen, nicht nur den bewährten und allgemein anerkannten Sicherheitsregeln entsprechen. Sie sollte außerdem mindestens dasselbe Sicherheitsniveau einhalten wie fortschrittliche Verfahren, die in der Praxis erfolgreich erprobt und von führenden Fachleuten anerkannt sind.“

KRITIS-Betreiber müssen „regelmäßig nachweisen, dass ihre Systeme entsprechend geschützt sind“, betont Jürgen Bruder, Mitglied der Geschäftsleitung von TÜV Hessen. Das gelte natürlich auch für die Dienstleister, die sie beauftragen. Bruder: „Gerade im Back-End, das näher am System liegt, dort also, wo über den Server Daten verarbeitet werden.“

Betreibersicherheit setzt den Stand der Technik

Betreibersichere Infrastrukturen wie die Versiegelte Cloud der Telekom, ucloud von regio iT oder die Sealed Platform von Uniscon erfüllen diese Ansprüche für die KRITIS-Betreiber. Durch einen Satz rein technischer Maßnahmen sind Daten und Anwendungen hier zuverlässig gegen Angriffe von außen und

[1] https://blog.tuev-hessen.de/447/beitraege/543kritische-infrastrukturen-angemessen-schuetzen/
[2] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html
[3] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

innen geschützt. Auch der Betreiber der Infrastruktur und Administratoren sind vom Zugriff auf gespeicherte, übertragene oder verarbeitete Daten ausgeschlossen.

„Lösungen wie diese bieten ein Sicherheitsniveau, das höher als das vergleichbarer Cloud-Plattform-Produkte am Markt ist. Betreibersichere Infrastrukturen sind seit mehreren Jahren im gewerblichen Umfeld im Einsatz – unter anderem in Kliniken, Kanzleien und Banken“, sagt Jäger. „Darüber hinaus sind sie von führenden Fachleuten anerkannt sowie zertifiziert und bilden mittlerweile die Basis für digitale Geschäftsmodelle, die ohne das hohe Sicherheitsniveau nicht denkbar wären.“

Weiterführende Informationen und druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de

Uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die Uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet Uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist Uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zu Partnern und Produkt: www.uniscon.de

Pressekontakt

Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.de
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20