KRITIS als Teil einer modernen Gesellschaft

Wir wussten es bereits lange, die Berücksichtigung und die Umsetzung der Informationssicherheit ist wichtig und sollte auf gar keinen Fall vernachlässigt werden. Nicht ohne Grund wird hierzu seit Jahren Aufklärungsarbeit geleistet und zum Beispiel mithilfe vorgegebener Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) versucht, den jeweiligen Akteuren entsprechende Hilfsmittel an die Hand zu geben.

Die vergangenen Monate der Arbeit – zumeist im Homeoffice – haben folglich bestehende Lücken und Anwendungsprobleme vorhandener Informationssicherheitssysteme nur bestätigt bzw. verstärkt aufgezeigt. Unternehmen und Behörden mussten in kürzester Zeit gewährleisten, dass die Kommunikation und der Datentransfer von den verschiedenen Arbeitsplätzen aus sichergestellt wurde, selbst wenn diese im privaten Umfeld lagen bzw. liegen. Dabei führten die allenfalls im Hintergrund laufenden Schwierigkeiten, mit überlasteten VPN-Tunneln, Problemen beim Einspielen erforderlicher Updates oder der Einwahlmöglichkeit privater Endgeräte in das Firmennetz, auf den ersten Blick erst einmal nur in der Administration zu Überstunden. Die Notwendigkeit – und der Wunsch – auf Nutzung diverser Kommunikationssysteme (bspw. zum Videomeeting), zeigte dann aber wohl auch der Geschäftsführung und den Beschäftigten schnell die diversen Herausforderungen an eine stabil laufende IT-Infrastruktur auf. Bewusst sollte hingegen allen sein, nur weil wir zurzeit eine „besondere Lage" haben, darf das Thema der Informationssicherheit zu keiner Zeit vernachlässigt werden.

Besonders deutlich wird dies im Bereich der Kritischen Infrastrukturen (KRITIS), wenn es sich um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen handelt, würde deren Ausfall oder Beeinträchtigung doch möglicherweise zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen für die Gesellschaft führen. Infolgedessen verpflichtet das IT-Sicherheitsgesetz die Betreiber kritischer Dienstleistungen, geeignete Vorkehrungen zur Vermeidung von Störungen an informationstechnischen Systemen, Komponenten und Prozessen zu treffen. Dabei ist der „Stand der Technik" zu berücksichtigen und deren Umsetzung dem BSI mindestens alle zwei Jahre nachzuweisen. Doch obwohl die bestehende Notwendigkeit der Umsetzung entsprechender technischer und organisatorischer Maßnahmen nicht neu ist, bereitet die Frage danach, was eigentlich der „Stand der Technik" ist, allen Beteiligten weiterhin Probleme.

Das vorliegende Schwerpunktheft zeigt zunächst in einem Beitrag von *Fabian Mangels* auf, welche Unternehmen überhaupt zur Kritischen Infrastruktur gehören, welche rechtlichen Grundlagen berücksichtigt werden müssen und welche Informationssicherheitsmaßnahmen umzusetzen und kontinuierlich angepasst bzw. weiterentwickelt werden müssen. Sodann werden von *Annika Woitke* die notwendigen Schritte dargestellt, die bei der Einführung und Pflege eines Informationssicherheitsmanagementsystems durch „KRITIS"-Unternehmen eingehalten werden müssen, um diese im Rahmen eines Audits prüfen lassen zu können. Diesem Beitrag schließt sich eine Darstellung der notwendigen Prüfungsschritte bei der Auditierung von KRITIS-Unternehmen aus Sicht eines Auditors von *Christopher Stradomsky* an, bevor zuletzt von *Steffen Sundermann* die kritische Frage aufgeworfen wird, ob betroffene Personen das Recht besitzen auf die Umsetzung technischer und organisatorischer Maßnahmen zu verzichten.

Die im Heft enthaltenen Beiträge sollen wieder die Möglichkeit bieten, sich einen Überblick über die in der täglichen Arbeit relevanten Themen zu verschaffen und nicht zuletzt durch eine mögliche Diskussion dazu beitragen, offene Fragen und damit aufgezeigte Lücken in den Anwendungsmöglichkeiten rechtlicher Vorgaben zu schließen.

Britta Alexandra Mester