Aus Schaden wird man klug – Warum KRITIS wichtig ist

Täglich werden wir in der Tagespresse mit Berichten über Terroranschläge, Hackerangriffen oder schwerwiegenden Unglücken konfrontiert, die nicht selten zum Ziel haben, die Gesellschaft zu destabilisieren. Nach einem solchen Unglücksfall stellt sich nicht nur die Frage nach der Aufklärung, sondern auch der Prävention. Um das gesellschaftliche Zusammenleben nicht von einem einzelnen Unglücksereignis gefährden zu lassen, wurde mittlerweile mit KRITIS reagiert. KRITIS, eigentlich der Begriff für Kritische Infrastrukturen, ist Synonym für Regeln zum Schutz eben jener kritischen Strukturen. Damit sind systemrelevante technische und sozioökonomische Infrastrukturen gemeint, deren Ausfall zu nachhaltigen Versorgungsengpässen oder erheblicher Störung der öffentlichen Sicherheit führen würde. Und da Angriffe gegen diese drohen, kommt einem hier die alte Geschichte der Gebrüder Grimm vom Hasen und vom Igel in den Sinn; wer ist schneller, der Angreifer oder der Verteidiger, wer ist Hase, wer ist Igel. Obwohl ich einräume, dass jedem Angreifer der Charme des Hasen bzw. des Igels zur Gänze abgeht.

In Deutschland wurde der Begriff der Kritischen Infrastrukturen erstmals 2008 in das Raumordnungsgesetz (§ 2 Abs. 2 Nr. 3) aufgenommen. Seit dieser Zeit hat der Gesetzgeber die Anforderung an deren Schutz deutlich erhöht, es seien nur das BSIG, das IT-Sicherheitsgesetz von 2015 und die BSI-Kritisverordnung benannt, die einem ständigen Reformzyklus unterworfen sind. Dabei stellt gerade die BSI-Kritisverordnung Praktiker im Prüfungsalltag vor große Herausforderungen: Wie schnell müssen die KRITIS -Anforderungen erfüllt sein, wer setzt es um und wer ist für die weitere Prüfung zuständig? Und zu guter Letzt, wie wird die Umsetzung finanziert?

Doch richtig ist, die Informationssicherheit bei KRITIS -Betreibern muss nach dem ITSG ohnehin schon auf einem derartig hohem Niveau sein, wodurch ein Mehraufwand bei der Umsetzung von KRITIS -Anforderungen eigentlich unwahrscheinlich erscheint. Hier zeigt sich die hohe Relevanz eines guten Informationssicherheitsmanagementsystems (ISMS). Dies bestätigen vor allem die einschlägigen Beispiele der Praxis: Ein Unternehmen hatte über drei Jahre die Einführung eines ISMS aufgrund angeblich zu hoher Kosten abgelehnt, ebenso wie andere wichtige Compliance-Maßnahmen, bis zu dem Tag, an dem ein schwerer Ransomware-Angriff dazu führte, dass nicht nur die gesamte Firmendatenbank verschlüsselt war, sondern die Produktion für die Dauer von 4 Tagen stillstand und es eine Geldforderung zur Freigabe des Entschlüsselungscodes gab. Im Hinblick auf den hohen Reputationsschaden, die Kosten des Produktionsausfalls, etwaige Vertragsstrafen wegen Lieferverzögerungen, einem anstehenden Bußgeldverfahren und dem unsäglichen Vertrauensverlust wurde dann die Implementierung eines ISMS und die Planung vernünftiger Compliance-Strukturen aufgenommen. Und hier drängt sich der Vergleich mit der Haftpflichtversicherung auf: Ich kann ja gerne auf eine Haftpflichtversicherung verzichten, um die Versicherungsprämien zu sparen. Sollte ich aber zu den Unglücksraben gehören, die einen Versicherungsfall ohne Versicherungsschutz zu beklagen haben, werde ich schnell merken, dass ich mit der Schadenshöhe die eingesparten Prämien bis ins nächste Jahrtausend hätten zahlen können.

KRITIS hindert uns daran, ähnlich dem Pflichtversicherungsgesetz, ohne „Versicherungsschutz zu fahren", denn so wie das Autofahren gefahrimmanent ist, ist das Betreiben kritischer Infrastrukturen in heutigen Zeiten mit Hackerangriffen von kriminellen Organisationen und Geheimdiensten, Ransomware-Verschlüsselungen und anderen Gefahren aus dem virtuellen Raum als mindestens genauso kritisch einzustufen.

Getreu dem Vegetius-Grundsatz „Si vis pacem, para bellum" sollte daher jeder seine Informationssicherheitsstrukturen hinterfragen, um sich auf einen kommenden Angriff vorzubereiten. Sicherlich eine nicht zu unterschätzende Herausforderung in Zeiten staatlich-unterstützter Hacker und des allgegenwärtigen Einsatzes von Quantencomputern.

Dominik Bleckmann