Foto: AdobeStock©gopixa

Großteils unbemerkt von der Öffentlichkeit steht die neue EU-Richtlinie für Cybersicherheit NIS 2.0 kurz vor der Verabschiedung. Diese kann für viele Unternehmen eine böse Überraschung bedeuten.

Über das Ziel hinausgeschossen

Auch wenn die befürchteten Cyberattacken als Begleiterscheinung des Angriffs Russlands auf die Ukraine gottseidank weitestgehend ausgeblieben sind, gewinnt die Frage des Schutzes kritischer Infrastrukturen immer stärkere Bedeutung. Deshalb ist es ein gutes Zeichen, dass nach Verabschiedung des IT-Sicherheitsgesetzes (IT-SiG) 2.0 im letzten Jahr mit der Arbeit an der NIS 2.0-Richtlinie auch das europäische Gegenstück Kontur annimmt. Denn das ist eine Lehre nicht nur aus Corona- und Ukraine-Krise, eine nationalstaatliche Herangehensweise wird zwangsläufig zu kurz greifen. Wie in der „ersten Runde" war der deutsche Gesetzgeber schneller und die EU zog nach.

Als NIS 1 entwickelt wurde – durchaus mit dem schon existierenden IT-SiG 1.0 als Blaupause – war Deutschlands größte Sorge, dass die EU dahinter zurückfallen könnte. In der zweiten Runde droht nun das umgekehrte Phänomen: Die EU wird deutlich über die deutsche Position hinausgehen. Dabei geht es nicht um die Regelungstiefe. Vieles von dem, was in NIS 2 geplant wird, ist unterstützenswert bis überfällig. Das Problem liegt in erster Linie in der Anzahl der einzubeziehenden Unternehmen: Es sollen alle mittleren Betriebe ab 50 Mitarbeitern aus den betroffenen Sektoren einbezogen werden.

Nach einer Auswertung des Statistischen Bundesamtes würden statt bisher 4.500 in Zukunft 45.000 Unternehmen in Deutschland unter diese Regulierung fallen. Natürlich ist es zu begrüßen, wenn möglichst alle Unternehmen ausreichend Eigenschutz betreiben. Aber sollte dies wirklich gesetzlich geregelt werden und wer soll das angesichts des extremen Fachkräftemangels umsetzen? Die Aufgabe ist schlicht nicht zu bewältigen und wirft die Frage auf, ob man Gesetze beschließen sollte, die nicht umsetzbar sind.

Sinnvoller erscheint es, bei den essentiellen kritischen Infrastrukturen alles dafür zu tun, dass diese sicher sind, anstatt die „Gießkanne" über ganze Branchen auszuschütten und einen „one size fits all"-Ansatz zu fahren. Grundsätzlich sind im Gesetzentwurf Differenzierungen möglich, diese werden aber zu restriktiv genutzt. So droht vielen Unternehmen ein böses Erwachen, wenn das Gesetz unverändert beschlossen wird.

Um dies greifbar zu machen: Wenn die Gesetzgebung wie geplant durchläuft, fallen in Zukunft etwa auch eine Molkerei oder Spedition mit 55 Mitarbeitern darunter. Ist Wohl und Wehe unserer Gesellschaft von diesen „kritischen Infrastrukturen" abhängig? Selbstverständlich sollten sich die

Betriebe im eigenen Interesse um ihre IT-Security kümmern, da sonst jede Ransomware-Attacke in die Insolvenz führen kann. Aber muss man ihnen gesetzlich mit einer Geldstrafe von bis zu zwei Prozent des Jahresumsatzes drohen, wenn sie eine Attacke nicht in 24 Stunden melden? Und warum ist die Frist kürzer als in den USA und in der Datenschutzgrundverordnung, die 72 Stunden vorsehen? Wer einmal eine Attacke erlebt hat, weiß welches Chaos danach herrscht und wie knapp Ressourcen und Zeit sind. Große kritische Infrastrukturen können sicher schneller agieren und auch zu schnelleren Reaktionen verpflichtet werden, aber auch Mittelständler mit 50 Mitarbeitern? Und, ja, ein umfassendes Lagebild ist wichtig, aber überfordert man nicht auch das Bundesamt für Sicherheit in der Informationstechnik durch eine Flut an Meldungen? Die Konsequenz wird sein, dass ein Auge zugedrückt wird, weil die Aufgabe einfach nicht umsetzbar ist. Wird dann aber sichergestellt, dass dies nur für die weniger kritischen Strukturen gilt?

Schaut man angesichts der traurigen Ereignisse in der Ukraine endlich rationaler auf das Thema Sicherheit und Verteidigung, sollte der Staat weniger darauf fokussieren, immer mehr Unternehmen losgelöst von ihrer Bedeutung für die Gesellschaft zu verpflichten – oder zumindest diese Pflichten in einem angemessenen Rahmen lassen. Wir müssen so ehrlich sein, dass dies bestenfalls einen Schutz vor Unfällen, normalen Hackern und Cyberkriminellen bieten kann. Wenn wir das Szenario offener staatlicher Cyberangriffe betrachten, ist auch ein vermeintlicher „Energieriese“ nur ein „Cyberzwerg“. Die Asymmetrie zwischen Angreifer und Verteidiger immens. Ein Schutz vor solchen Gefahren ist aber auch keine Aufgabe mehr, die der Staat als Vorgabe an die Betreiber weiterleiten kann.

Prof. Timo Kob
Vorstand HiSolutions AG und Professor für Cybersecurity und Wirtschaftsschutz, FH Campus Wien; Vorsitzender der Bundesarbeitsgruppe des Wirtschaftsrates und Mitglied im Hauptvorstand des BITKOM

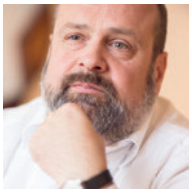

Foto: Timo Kob

„Wenn die Gesetzgebung wie geplant durchläuft, fallen in Zukunft etwa auch eine Molkerei oder Spedition mit 55 Mitarbeitern darunter.“

Hier ist er auch zur Unterstützung der finanziellen und ressourcentechnischen Anforderungen gefordert. Dies senkt unsere Angreif- und Erpressbarkeit deutlich stärker als die Verpflichtung der sprichwörtlichen Molkerei zur schnellen Meldung. □