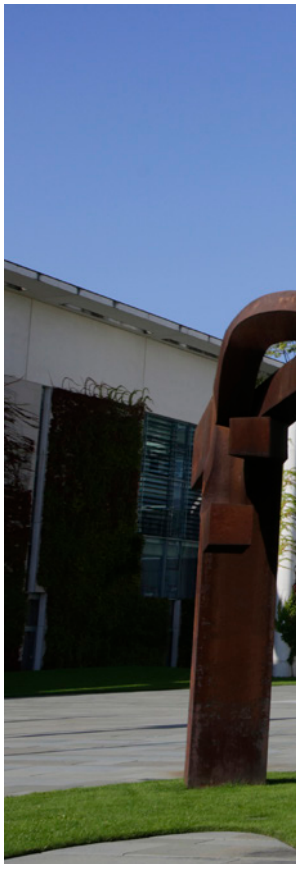
Doppel-Wumms nicht gehört?



Deutschland braucht einen Masterplan für Cybersecurity mit einfachen Strukturen und am besten einer klar verantwortlichen Person wie dem Bundeskanzler.

Die Erkenntnis, welche Bedeutung die Cybersecurity für das Wohlergehen unserer Gesellschaft hat, hat sich mit geradezu disruptiver Kraft durch den politischen und ökonomischen Raum ihren Weg gebahnt. Dies hat natürlich mit der „Zeitenwende" nach Putins Überfall auf die Ukraine zu tun, aber es war nur der letzte Tropfen in das überlaufende Fass. Die gesellschaftlichen und wirtschaftlichen Konsequenzen durch kriminelle oder politisch motivierte Angriffe waren auch zuvor bekannt und führten zu einem massiven Umdenken. Doch leider erlebt man mehr hektischen Aktivismus und einen Wettbewerb der Ankündigungen, als einen integrierten strategischen Ansatz, der heute wichtiger denn je wäre. Die vielen Ankündigungen bezeugen, dass wir – wie so oft in Deutschland – kein Erkenntnis-, sondern ein Umsetzungsproblem haben. Dass etwas gemacht werden muss ist unstrittig, aber es scheitert daran, dass das Richtige von den richtigen Instanzen richtig gemacht wird. So verschwenden wir viel Energie, Zeit und Geld.

Überall wo digitalisiert wird, braucht es ein Streben nach Cybersecurity. Da überall digitalisiert wird, braucht es überall Cybersecurity. Dies führt zu einem Wildwuchs an Verantwortlichkeiten, Mitspracherechten und auch Föderalismusdiskussionen. Wer sich die Begeisterung für Wimmelbilder aus der Kindheit bewahrt hat, mag an der jährlich von der Stiftung Neue Verantwortung veröffentlichten Aufstellung der Verantwortlichkeiten in Deutschland für Cybersecurity Freude empfinden, für alle anderen wird dort visuell greifbar, warum wir das Thema nicht in den Griff bekommen. Natürlich wird es nie den einen Verantwortlichen geben, aber ohne klarere und einfachere Struktur werden wir nicht vorankommen.

Diese Vielzahl von Verantwortlichkeiten führt zu einer Kakophonie der unkoordinierten Ankündigungen: Digitalstrategie des Bundes, internationale Digitalstrategie des BMDV, Cybersicherheitsstrategie, Nationale Sicherheitsstrategie, „Aktionsplan Cybersicherheit" des Auswärtigen Amtes, Umsetzung der neuen europäischen NIS2-Richtlinie, KRITIS-Dachgesetz, diverse Förderprogramme – auch Experten verlieren langsam den Überblick, was hier gerade wann von wem angekündigt wird. Die Anzahl der Initiativen und Strategien wächst proportional zur Anzahl der sich verantwortlich fühlenden Institutionen – national und international. Jede Initiative ist berechtigt, aber die Zweifel in der Fachwelt, inwieweit diese Ansätze zueinander kompatibel, widerspruchsfrei und in der Summe vollständig und konsistent sind, sind groß und wohl auch nicht ganz unberechtigt.

Und mag man bei geo- oder verteidigungspolitischen Themen noch nachvollziehen können, warum sie hinter verschlossenen Türen stattfinden, so führt der Ansatz, die Anzahl der Aktivitäten und der staatlichen Verantwortlichen zu maximieren, aber die betroffene Wirtschaft nicht einzubinden, zu noch mehr Verärgerung und definitiv nicht zur Qualitäts-

Foto: privat

Prof. Timo Kob
Gründer und Vorstand HiSolutions AG;
Vorsitzender der Bundesarbeitsgruppe Cybersicherheit im Wirtschaftsrat

„Diese Vielzahl von Verantwortlichkeiten führt zu einer Kakophonie unkoordinierter Ankündigungen."

steigerung. Als Beispiel sei das KRITIS-Dachgesetz genannt, wo jetzt mit hohem Tempo Schutzanforderungen für Kritische Infrastrukturen jenseits der Cybersecurity etabliert werden sollen, aber im ersten geleakten Entwurf die Verknüpfung zur Cybersicherheit komplett fehlte. Dafür wurde aber vorgeschlagen, eine weitere Behörde – das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – auf die Liste der Verantwortlichen zu setzen. Die fehlende Einbindung der Cybersecurity wurde auf der Ankündigungsebene zwar korrigiert. Aber woran bis heute niemand gedacht hat, ist, mit den Betroffenen, den kritischen Infrastrukturen selbst, zu sprechen.

Ebenso warten wir seit Regierungsantritt auf eine Konkretisierung der Ankündigung, das Bundesamt für Sicherheit in der Informationstechnologie (BSI) unabhängiger aufzustellen und zu stärken. Papier ist geduldig, besonders das von Koalitionsverträgen, die Digitalisierung im Allgemeinen und Angreifer im Cyberspace im Besonderen sind es nicht. Was unser Land dringend braucht, ist ein Masterplan, der anerkennt und umsetzt, dass das Thema Cybersecurity sich durch fast alle Politikfelder von Innenpolitik bis über Außenpolitik, von Wirtschaft bis Bildung, von Verteidigung bis Forschung zieht und auch nur integriert betrachtet gemeistert werden kann. Nur so werden wir die mannigfaltigen Gefahren bewältigen. Wer heute neue Sicherheitsanforderungen stellt, ohne gleichzeitig in den Schulen zu beginnen, gegen den Fachkräftemangel von morgen zu kämpfen, springt zu kurz. Wer in der Cybersecurity nur Risiken sieht, ohne auch die Chancen für die Wirtschaft zu erkennen und systematisch zu generieren, betrachtet nur eine Seite der Medaille. Doch dafür braucht es denjenigen, der sich für das Thema in allen Facetten verantwortlich fühlt – und dieser ist nicht in Sicht.

Foto: Jens Schicke

Dass dies keine Fantastereien und Hirngespinste sind, zeigt uns Israel seit fast 20 Jahren. Aus einer Gefährdungslage die richtigen Schlüsse ziehen, koordiniert alle Beteiligten etwa aus Wirtschaft, Sicherheitsbehörden und Forschung einzubinden und mit dem vollen Instrumentenkasten der Politik eine konsistente Strategie zu entwickeln und konsequent umzusetzen – das funktioniert. Und führt dazu, dass Israel nicht nur trotz massivster Bedrohung wenige Cybersecurity-Vorfälle zu beklagen hat, sondern als Nebeneffekt auch eine der erfolgreichsten Industrien der Branche aufgebaut hat.

Israel bündelt all dies direkt beim Premierminister. Der Wirtschaftsrat würde sich etwas Vergleichbares im Kanzleramt wünschen. Oft genug stellen wir in Deutschland unser Licht unter den Scheffel. Auch in der Cybersecurity sind wir an vielen Punkten nicht so schlecht, wie wir glauben. Um das BSI beneiden uns viele Länder, unsere Cybersecurity-Industrie ist in gewissen Sparten mehr als wettbewerbsfähig. Wie gut könnten wir sein, wenn wir dieses Potential nicht nur erkennen, sondern konzertiert und konsequent nutzen würden!