Kann Mr. Cyber das Problem des E-Voting lösen?

Im Dezember 2017 ist im Parlament die Motion der Ständerate Dittli und Eder angenommen worden. Die Idee dahinter lautet, es soll ein neues Cyber–Kompetenz-Zentrum im Bund entstehen. Eine Fachbehörde dieser Art ist genauso nötig wie die FINMA oder die Nationalbank. Die komplexen Zusammenhänge der Cyberbedrohungen haben Auswirkungen auf die Sicherheit des Landes, die in zunehmenden Fällen nicht mehr einfach von Polizei und Justiz erfasst und bewältigt werden können. Sowohl im präventiven als auch im reaktiven Bereich von Cyber-Vorfällen muss rasch und wirksam gehandelt werden können. Alle Geschäfts-Bereiche des Bundes sind mit betroffen, denn alle Bereiche verwenden IT am Internet, insbesondere auch die kritischen Infrastrukturen. Auf strategischer und regulativer Ebene ist schon viel gemacht worden[1]. Im operativen Bereich ist aber der Handlungsbedarf nach wie vor gross.

Die Frage stellt sich nach der **Rolle und Pflichtenheft** dieser neuen Behörde. Offenbar muss sie landesweit alle Interessen vernetzen[2] und sie scheint für alles zuständig zu sein, was Cyberfragen in der Schweiz betrifft. Aber wofür genau ist sie verantwortlich? Gibt sie Zertifizierungen ab für kritische Infrastrukturen anstelle der KPMG oder gibt sie nur Ratschläge? Und: Untersteht sie der Verwaltung und hat die Interessen der Regierung zu vertreten[3] oder kann sie unabhängig – nur ihrem Wissen und Gewissen entsprechend - über den Einsatz von Systemen entscheiden, genauso wie die verglichenen Institutionen?

Sicher ist zu begrüssen, dass eine **interne Stelle** diese Pflichten übernimmt und das nicht mehr durch externe Stellen auf Mandatsbasis erfolgt. Es wird dabei nicht an der fachlichen Kompetenz dieser bisherigen Dienstleister gezweifelt. Aber es dort geht klar um einen Interessenskonflikt: Der externe Dienstleister ist existentiell von der Zufriedenheit seiner Auftraggeber abhängig. Die Darstellung des Endresultates wird daher konform zu den Vorstellungen des Auftraggebers sein. Diesen Zusammenhang in Zweifel zu ziehen wäre komplett naiv. Eine unabhängige interne Behörde wäre zwar wohl auch irgendwo rechenschaftspflichtig. Aber sie hat im Idealfall keine anderen Interessen zu vertreten die Sicherheit der betroffenen kritischen Infrastrukturen.

Seit 14 Tagen ist der neue **Chef** dieser internen Behörde bekannt: Es handelt sich um Florian Schütz von der RUAG. Was man zu dieser Wahl sagen kann ist, dass der neue Chef bestimmt eine passende Ausbildung hat und offenbar auch schon über einschlägige Erfahrungen in der Praxis verfügt. Ob die fehlende Erfahrung in der Bundesverwaltung ein Vor- oder ein Nachteil ist, kann man noch nicht mit Bestimmtheit sagen.

Entscheidend dürften – selbst bei einer idealen Besetzung dieser Stelle - das **Pflichtenheft** sowie das Stellenkontingent sein, welches dieser Stelle die Verantwortungen und Kompetenzen zuschreibt. Diese sollten die für den Staat kritischen Infrastrukturen abdecken, welche aber genauer beschrieben und abgegrenzt sein müssten. **Abgrenzungen** mit der eigenverantwortlichen Wirtschaft und solche mit den übrigen Sicherheits-Organen des Bundes müssten gezogen werden. Und eben auch die Abgrenzung zwischen Bund und Kantonen muss detailliert beschrieben sein, um eine Verzettelung zu

[1] https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
[2] https://www.nzz.ch/schweiz/von-der-ruag-zu-zalando-diese-erfahrungen-bringt-der-neue-mr-cyber-des-bundes-mit-ld.1489630
[3] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73839.html

vermeiden oder mindestens zu minimieren. Eine weitere Koordinationsbehörde, die unendliche viele Informationen von unendlich vielen Teilnehmern sammelt und an sie verteilt, braucht es nicht. Es braucht die Verantwortlichkeit, angemessene und zweckmässige Entscheidungen über Eingriffe in kritische IT-Infrastrukturen des Bundes zu fällen. Es bedarf gewiss noch einiger Zeit, bis involvierte Stellen sich auf passende und doch genügend spezifische Rahmenbedingungen und Abgrenzungen geeinigt haben.

Auch für die Cybersicherheit selbst gibt es bereits heute mehrere Institutionen innerhalb der Bundesverwaltung. Sie sichern jeweils ihren Verwaltungs-Bereich mit ihren mehr oder weniger wirkungsvollen Mitteln. Es geht einerseits um das Wissen der aktuellen Bedrohungen, aber andererseits auch um die Konsequenzen, die aus den gewonnenen Erkenntnissen zu ziehen sind. Dabei sollten sich diese nicht einfach auf gute Ratschläge an die Benutzer beschränken. Diese Konsequenzen müssen gegebenenfalls Wirkung bei der IT der betroffenen Stellen und Ämtern zeigen, sonst sind die Anstrengungen eben wirkungslos. Das generiert u.U. – wenn z.B. mehrere Departemente oder die Kantone betroffen sind - einen enormen Koordinationsbedarf, welcher sehr aufwendig ist und viele hochkarätige Stellen einbindet.

Wenn diese Koordination den regulären Dienstweg nehmen muss, um eine Wirkung zu erzielen, so wird diese (teure) Energie verpuffen, weil zu viele Stellen involviert werden müssen. Daraus folgt, es muss eine **unabhängige Stelle** sein, die Konsequenzen – natürlich nach sorgfältiger Prüfung – auch anordnen kann. Wenn die Sicherheit neu als gefährdet betrachtet wird, muss man entsprechende Einrichtungen revidieren, überwachen, einstellen oder verhindern. Die Revision selbst kann zwar eine Begleitung von der Sicherheitsbehörde verlangen aber diese darf nicht selbst die Revision durchführen. Eine **Trennung der Verantwortlichkeiten** (ACT/CHECK) ist absolut zwingend.

E-Voting wäre eine typische kritische Infrastruktur zwischen Bund und Kantonen und darum bedürfte dies – falls man diese Einrichtung nicht als unnötig und riskant, sondern als zwingend betrachtet - einer zentralen Sicherheitskonzeption mit detaillierten Spezifikationen von vielen neuen Überwachungselementen, die heute gänzlich fehlen. Die ganzheitliche Betrachtung und Beurteilung der Sicherheit und Vertrauenswürdigkeit des Abstimmungs-Prozesses (Risiko Management) sowie Überprüfungen und Zertifizierungen von Systemen, welche nachweislich höchste Anforderungen erfüllen müssen, müsste ein zentrales Anliegen eines solchen bundesweiten Cyber-Kompetenz-Zentrums sein. Dabei müssten zwingend Netzwerke, deren Provider, die angeschlossenen staatlichen und nicht-staatlichen Dienstleister wie IT Betreiber, Druckzentren sowie die Anforderungen an die Endgeräte der Benutzer mit eingeschlossen ein. Dies würde bei der Umsetzung wohl einen beträchtlichen Kostenschub auslösen, den man politisch abstützen können müsste, **bevor** man dieses Vorhaben angeht. Da die Bundeskanzlei E-Voting bisher vor allem als juristisches Vorhaben betrachtet hat und alle technisch-betrieblichen Kostenfolgen ohnehin den Kantonen überlässt, ist eine Übergabe einer solchen Problemstellung an eine nationale Fachbehörde dringend notwendig.

Darum ist die Einrichtung einer solchen staatlichen Institution grundsätzlich eine gute Idee. Die Sicherung der kritischen Infrastrukturen gegen Cyberbedrohungen bedarf einer Fachbehörde. Bei E-Voting geht es aber nicht nur um die **Sicherheit**, sondern auch um den **Transparenzanspruch**. Kann die Sicherheitsbehörde mit ihrem Spezialwissen und ihrem Fachjargon den gewöhnlichen Bürger von der Richtigkeit der sicherheitstechnischen Einschätzung überzeugen? Und ist dieser mit der Behandlung des Restrisikos einverstanden? Nur wenn diese Fragen für die Mehrheit der Bürger zufriedenstellend gelöst werden kann, ist eine Lösung E-Voting überhaupt denkbar. Angesichts der

realen Cyberbedrohungen unserer Zeit dürfte das ein sehr schwieriges und aufwendiges Unterfangen werden. Und darum stellt sich spätestens dann wiederum die Kosten/Nutzen-Frage: Warum brauchen wir eigentlich E-Voting?

Ob man deshalb mit dieser neuen Behörde Problemstellungen wie die des E-Voting in den Griff bekommen könnte, wenn man denn überhaupt wollte, wird sich erst noch zeigen müssen.