Cybersicherheitspolitik: Noch nicht „erstklassig“

TAGESSPIEGEL BACKGROUND

T. Reinhold, S. Herpig & M. Schulze (Foto: Thomas Reinhold/Sebastian Heise/Jana Neumann)

veröffentlicht am 24.01.2020

„Erstklassig“ findet Innenminister Horst Seehofer seine Cybersicherheitspolitik, eher wenig Fortschritt bei den wichtigen Fragen bescheinigen die Cybersicherheitsexperten Sven Herpig, Thomas Reinhold und Matthias Schulze der Bundesregierung.

Lernen Sie den Tagesspiegel Background kennen

exklusive und aktuelle Hintergrundinformationen für 30 Tage kostenfrei.

Jetzt kostenfrei testen

In einem Interview sprach Bundesinnenminister **Horst Seehofer** (CSU) Ende vergangener Woche davon, sein Ministerium habe in allen Bereichen, für das es zuständig sei, „**erstklassige Arbeit**“ geleistet. Damit kann der Behördenchef nicht den Bereich „Cybersicherheit“ gemeint haben. Denn hier wäre **etwas mehr Bescheidenheit** durchaus angebracht. Zahlreiche Vorhaben des Bundesministeriums des Innern, für Bau und Heimat (BMI) laufen nicht so erstklassig wie behauptet.

Zunächst ist die **Bedrohungslage im Cyberraum** auch 2019 noch „**anhaltend hoch**“ resümierte vor einigen Monaten der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), **Arne Schönbohm**. Das **Cybercrime Lagebild** des Bundeskriminalamts bescheinigt zwar **sinkende Schäden** aus Computerbetrugsfällen im Vorjahresvergleich, die Behörde verweist jedoch selbst auf die **fragliche Aussagekraft** seiner eigenen Datenerhebung, wegen der „überdurchschnittlich großen Anzahl von Cybercrime-Straftaten, die bei der Polizei nicht zur Anzeige gebracht werden“.

Wie ist die Arbeit der Bundesregierung der letzten zwei Jahre in Sachen Cybersicherheit zu bewerten? Wir haben uns die zentralsten Versprechen angeschaut.

IT-Sicherheitsgesetz 2.0: Verspätet

Das **neue IT-Sicherheitsgesetz** sollte eigentlich höchste Priorität haben, hängt aber im politischen Prozess fest (Tagesspiegel Background berichtete). Nach der Veröffentlichung der Daten von Bundestagsabgeordneten zum Jahreswechsel 2019 kündigte das Innenministerium an, das Gesetz noch vor der Sommerpause

verabschieden zu wollen. Außer einem geleakten Entwurf, der **viel Kritik** nach sich zog, ist jedoch bis heute wenig passiert. Es scheint so, als wäre der Entwurf nicht mit dem Bundesministerium der Justiz und für Verbraucherschutz abgesprochen gewesen – und als hätte er es unter anderem deswegen noch nicht in die parlamentarische Verhandlung geschafft.

Cyber-Abwehrzentrum Plus: Nicht der große Wurf

Seit vielen Jahren steht eine **Reform der Cyber-Abwehrzentrums** an. Letztmalig angekündigt als Reaktion auf die Veröffentlichung der Daten von Bundestagsabgeordneten Anfang 2019. Dieses „Cyber-Abwehrzentrum Plus“ sollte strukturell verstetigt werden und laut Koalitionsvertrag eine wichtige Rolle bei der Zusammenarbeit von Bund und Ländern zur Cyber-Abwehr spielen. Ein **Schritt in die richtige Richtung** war es, **BSI-Verbindungsbüros** für jede Region zu schaffen. Auch der Umbau des Cyber-Abwehrzentrums wird anscheinend **seit Monaten im Stillen vorangetrieben**; für den versprochenen großen Wurf reicht das alles aber bisher nicht aus.

Fachkräfte: Reform bleibt aus

Schaut man sich den **Fachkräftemangel in der IT-Sicherheit der öffentlichen Verwaltung** an, so stellt man fest, dass in den letzten Jahren verschiedene neue Studiengänge eingerichtet worden sind, zum Beispiel der **Duale Diplomstudiengang „Digital Administration and Cyber Security“** an der Hochschule des Bundes für öffentliche Verwaltung. Auch **IT-Zulagen** wurden in verschiedenen Behörden als Instrument benutzt, um diese begehrten Fachkräfte zu binden. Leider wurde das Hauptproblem bisher nicht angegangen: IT-Spezialistinnen und -Spezialisten ohne formellen Studienabschluss in die Behörden zu bekommen. Hierzu ist eine **Reform des Laufbahn- und Tarifrechts** dringend notwendig.

Aktive Cyber-Abwehr: Keine Debatte, keine rechtliche Grundlage

Auch das Versprechen nach einer **gesetzlichen Regelung zur aktiven Cyber-Abwehr** wurde Anfang letzten Jahres nochmals bekräftigt. Wie auch bei den anderen Bereichen ist hier bisher wenig geschehen. Der **wissenschaftliche Dienst des Bundestages** hat eine sehr kritische Bewertung zu Aktiver Cyber-Abwehr abgegeben. Wenn Deutschland in Friedenszeiten außerhalb des eigenen Territoriums Cyber-Operationen durchführen will, sind schwerwiegende verfassungsrechtliche, völkerrechtliche und strategische Fragen im Vorfeld zu klären. Eine **Grundgesetzänderung** wäre hierbei vermutlich notwendig und eine **nuancierte öffentliche Debatte** daher Pflicht. Davon ist bisher wenig zu sehen.

Cybersicherheitsarchitektur: Keine Konsolidierung

Statt die Vielzahl an Behörden mit cybersicherheitspolitischen Aufgaben zu konsolidieren, schafft das Innenministerium **immer neue Behörden**, die **keinen erkennbaren Mehrwert** für die Cybersicherheit in Deutschland liefern. Hierzu gehören der Pakt für Cybersicherheit genauso wie das Cyberbündnis mit der Wirtschaft und der Zweitstandort des BSI im sächsischen Freital. Der Plan zur **Schaffung der Cyberagentur** wurde sogar vom Bundesrechnungshof als „nicht haltbar“ eingestuft.

Auf die eigenen Experten hören

Um den aktuellen Fortschritt der Bundesregierung bei der Cybersicherheitspolitik zu analysieren, lud der Bundestag im April Sachverständige ein. Die Bewertung war **alarmierend**. Es war daher auch wenig verwunderlich, dass sich gegen ein weiteres Vorhaben des Innenministeriums – den **Einbau von Hintertüren in Messengern** wie WhatsApp – ein breiter Widerstand organisierte. Mehr als 200 Sachverständige, Firmen, Organisationen und Abgeordnete

unterzeichneten im Juni einen offenen Brief, um das Innenministerium aufzufordern, dieses Vorhaben zu unterlassen.

Natürlich ist es schwierig, in einem komplexen Bereich wie der Cybersicherheitspolitik **verschiedene Interessen** zu vereinen. Das braucht eine konkrete Vision, harte Arbeit und vor allem Verantwortungsbewusstsein. Um wirklich „erstklassige" Politik in diesem Bereich zu gestalten, muss die Regierung mehr auf die eigenen Expertinnen und Experten, etwa im BSI, hören, kritisch Vorhaben evaluieren und dafür auch das Wissen von Vertreterinnen und Vertretern von Zivilgesellschaft, „Hacker Community" und Wissenschaft aktiv in Projekte einbinden. Das fehlt bisher. Dabei könnte eine solche **gemeinsame Politikgestaltung** in diesem schnelllebigen Feld dafür sorgen, dass wir belastbare, gemeinwohlverträgliche Lösungen erarbeiten, die die Cybersicherheit in Deutschland nachhaltig verbessern.

Dr. Sven Herpig ist Projektleiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung. Bevor er zur SNV kam, hat er mehrere Jahre beim Bundesamt für Sicherheit in der Informationstechnik und dem Auswärtigen Amt gearbeitet. Thomas Reinhold ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) der Universität Darmstadt. Er betreibt den Blog cyber-peace.org. Dr. Matthias Schulze ist wissenschaftlicher Mitarbeiter bei der Stiftung Wissenschaft und Politik. Dazu podcastet und bloggt er unter Percepticon.de.

Jetzt kostenfrei testen

Das könnte Sie auch interessieren