Stiftung Neue Verantwortung

Umfassende Cyber-Sicherheitspolitik für Deutschland 2.0[1]

Die Digitalisierung birgt nicht nur Chancen, sondern stellt uns auch vor neue Herausforderungen. Jeder unserer digitalisierten Lebensbereiche kann potenziell Ziel eines Cyber-Angriffs werden. Die Gefährdungslage hat sich dadurch in den letzten Jahren stark gewandelt. Der Ausbruch der "Schadsoftware-Epidemien" WannaCry und NotPetya hat uns das 2017 eindrucksvoll vor Augen geführt. Neben Einzelpersonen und Firmen geraten auch immer öfter kritische Infrastrukturen und politische Institutionen in das Fadenkreuz der Angreifer. Diesem Bedrohungsszenario kann nur mit einer ganzheitlichen Sicherheitspolitik und einer klaren Cyber-Sicherheitsarchitektur entgegengewirkt werden.

In der kommenden Legislaturperiode muss es ein deutliches Bekenntnis zu mehr Cyber-Sicherheit in Deutschland geben. Als Fundament hierfür dienen eine klare Rollenverteilung in der Cyber-Sicherheitsarchitektur und starke Position des Bundesamtes für Sicherheit in der Informationstechnik, sowie neue Ansätze in der Personalpolitik. Gleichzeitig müssen Entwicklungen, die zu einer Verringerung an IT-Sicherheit führen können, national und international entgegengewirkt werden.

Stärkung des Bundesamts für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik ist technisch und strukturell der Kern der deutschen Cyber-Sicherheitsarchitektur. Als IT-Krisenreaktionszentrum, zentrale Anlaufstelle der Allianz für Cyber-Sicherheit und mit dem Computer Emergency Response Team Bund verbindet das BSI die zentralen Akteure der deutschen Cyber-Sicherheitslandschaft miteinander. Mit dem Cyber-Abwehrzentrum beherbergt es darüber hinaus das operative Zentrum der zwischen-behördlichen Zusammenarbeit und kann dieses so direkt mit technischer Expertise versorgen.

Mit der Schaffung des BSI 1991 wurde in Deutschland das "Code Making" vom "Code Breaking" getrennt. Hierbei handelt es sich um eine aus Perspektive der IT-Sicherheit elementare organisatorische Maßnahme. Die Schaffung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) führte 2017 zu einer Wiederverknüpfung von Code Maker und Code Breaker auf Unterabteilungsebene im Bundesministerium des Innern. Neben anderen Herausforderungen, kann dies aus Sicht der Wirtschaft, Wissenschaft und Zivilgesellschaft zu einem essentiellen Vertrauensverlust in die staatliche Cyber-Sicherheitsvorsorge führen. Als warnendes Beispiel hierfür dient die BMI-Weisung an das BSI zur Unterstützung des Bundeskriminalamtes bei der Entwicklung des "Staatstrojaners" 2015[2]. Vertrauen dient in der Cyber-Sicherheit als wichtigste Währung für Kooperation und effektive Koordinierung - ohne Vertrauen droht daher die Sicherheitsarchitektur zu erodieren.

Die Erfahrungen aus den Cyber-Operationen gegen den Bundestag 2015, vor allem aber gegen das Democratic National Committee und die Wahlsysteme in den USA, sowie die französische Wahlkampagne "En Marché" haben gezeigt,

[1] Es handelt sich hierbei um eine erweiterte Form des im Oktober 2017 veröffentlichten Dokuments "Umfassende Cyber-Sicherheitspolitik für Deutschland". Die vorliegende Ausführung bezieht zusätzlich die Ergebnisse des am 12. Dezember 2017 in der SNV durchgeführten intersektoralen ExpertInnen-Workshops zum Thema "Cyber-Sicherheit in Deutschland 2018-2021" mit ein.

[2] https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

dass demokratische Prozesse und politische Institutionen vermehrt Ziel von Einflussnahmen im Cyber-Raum werden. Um dieser Bedrohung erfolgreich zu begegnen bedarf es Anpassungen in der Cyber-Sicherheitsarchitektur.

Das BSI sollte daher auch über 2018 hinaus mit einem signifikanten Ressourcen-Aufbau bedacht werden. Eine weitere dauerhafte Verankerung des Cyber-Abwehrzentrums im BSI ist zweckdienlich, damit es seiner zentralen Funktion als der nationalen Cyber-Sicherheitsbehörde effektiv nachkommen kann. Darüber hinaus sollte eine Rechtsgrundlage für das Cyber-Abwehrzentrum (und ggf. andere Kooperationsplattformen) geschaffen werden. Zusätzlich sollte eine Analyse über die zukünftige institutionelle Verankerung des BSI - mit dem Ziel größerer Unabhängigkeit von den "Code Breakern" (ZITiS, BfV, BKA …) - erfolgen.

Über die Verantwortung für die Regierungsnetze hinaus sollte das BSI außerdem im Zuge seiner gesamtgesellschaftlichen Verantwortung mit dem digitalen Schutz der Bundes- und Landeswahlprozesse und -institutionen betraut und entsprechende Kompetenzen ausgebaut werden.

Effiziente Personalpolitik bei IT-Sicherheit

Nach wie vor gibt es einen Mangel an Fachkräften in der IT-Sicherheit, vor allem im öffentlichen Dienst. Hinzu kommt, dass in den letzten Jahren in immer mehr Behörden mit Cyber-Sicherheit betraute Organisationseinheiten geschaffen worden sind. Dies führt im besten Fall zu Abstimmungsproblemen und im schlimmsten Fall zu Parallelstrukturen und Grabenkämpfen und zu einer zusätzlichen Verknappung der ohnehin spärlichen Ressourcen. Gleichzeitig führen die fortschreitende Digitalisierung und die zunehmende Gefährdungslage zu einer immer höheren Nachfrage an entsprechend ausgebildetem Personal.

Um der Personalknappheit im öffentlichen Dienst kurzfristig zu begegnen, sollten zusätzliche "Pooling und Sharing"-Modelle (wie z. B. die "Cyberwehr" des Bundesamts für Sicherheit in der Informationstechnik) geprüft werden. Gleichzeitig muss eine Überarbeitung der vertragsrechtlichen Rahmenbedingungen (TVöD-Reform/ Überprüfung des Laufbahnrechts) in Betracht gezogen werden. Mittel- und langfristig gilt es Ausbildungen und Umschulungen in diesem Bereich zu fördern, sowie zusammen mit den Ländern die Curricula für Schulen und Universitäten zu prüfen. Hierzu sollte die Regierung eine konsolidierte Strategie zum Abbau des IT-Fachkräftemangels erarbeiten.

Spannungsfeld zwischen IT-Sicherheit und Öffentlicher Sicherheit auflösen

Der Aufbau von ZITiS im BMI und die Erweiterung der Rechtslage zum Einsatz von Werkzeugen wie dem Bundestrojaner durch Strafverfolgungsbehörden und Nachrichtendienst, werden oft fälschlicherweise unter dem Thema "Cyber-Sicherheit" gefasst. Es handelt sich hierbei jedoch um den Einsatz von Cyber-Werkzeugen zur Herstellung Öffentlicher Sicherheit unter Schädigung von IT-Sicherheit, und damit um weniger und nicht mehr Cyber-Sicherheit. Hinzu kommt, dass bei diesen Themen die IT-Sicherheit bisher noch nicht bzw. zu selten mitbetrachtet wird. So ist eines der Grundprobleme bei der Arbeit von ZITiS das Management von Schwachstellen, die den Einsatz des Bundestrojaners in viele Fällen erst ermöglicht. Ohne ein entsprechendes Schwachstellenmanagement-System wird mehr Scha-

den angerichtet als Sicherheit hergestellt, da möglicherweise kritische Schwachstellen in IT-Systemen von Behörden, Unternehmen und Bundeswehr offen bleiben und von Kriminellen und ausländischen Nachrichtendiensten ausgenutzt werden können.

Es bedarf der Schaffung eines umsichtigen Schwachstellenmanagement-Systems und -Transparenzvorgaben, sowie einer Erarbeitung von Rahmenbedingungen für Hacking durch Strafverfolgungsbehörden und Geheimdienste im Inland. In diesen Bereichen ist die internationale Dimension der sogenannten "Spillover-Effekte" mit einzubeziehen. Deutschland kann so Vorbild für die EU und darüber hinaus werden. Es gilt daher gute Lösungen zu erarbeiten, die die IT-Sicherheit stärken und somit international zu einem höheren Niveau an Cyber-Sicherheit führen.

Der Bundessicherheitsrat diskutiert unter Ausschluss der Öffentlichkeit die Notwendigkeit von "Hackbacks". Die bisherige deutsche Diskussion zu diesem Thema war jedoch oft irreführend und basierte auf falschen Prämissen. Es fehlt bisher sowohl eine allgemeingültige Definition, als auch eine klare Verortung staatlicher Institutionen.

Sollte die neue Regierung das Instrument "Hackback" weiter verfolgen, so wird dringend ein offener Expertendiskurs hierzu angeregt, bevor eine rechtliche oder politische Zuweisung erfolgt. Bei all diesen Instrumenten gilt es darüber hinaus ein Höchstmaß an rechtsstaatlicher Kontrolle und öffentlicher Transparenz herzustellen.

Umfassende Analyse der strategischen Ausrichtung der deutschen Cyber-Sicherheitspolitik seit 2010

Es wird eine wissenschaftliche Aufarbeitung der Cyber-Sicherheitsstrategien 2010 und 2016 bzgl. ihrer Effektivität angeregt. Zusätzlich sollte sich eine (u. a. organisations-) wissenschaftliche Analyse mit der Herausforderung einer intersektoralen "Cyber-Sicherheitsstrategie für Deutschland 2019" befassen.

Autoren / Kontakt:
Dr. Sven Herpig, Leiter "Internationale Cyber-Sicherheitspolitik", sherpig@stiftung-nv.de
Julia Schütze, Projektmanagerin "Transatlantic Cyber Forum", jschuetze@stiftung-nv.de