CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

CISPA | Stuhlsatzenhaus 5 | D-66123 Saarbrücken

Sächsischer Landtag
Innenausschuss
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Ninja Marnau
Senior Researcher

Helmholtz Center for Information Security (CISPA)
Saarland Informatics Campus
Stuhlsatzenhaus 5
66123 Saarbrücken | Germany

PHONE +49 681 302-71943
FAX +46 681 302-71942
E-MAIL marnau@cispa.saarland
WEB www.cispa.saarland

1. April 2019

Anhörung zur Drucksache 6/16724 „Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen“

Sehr geehrter Herr Vorsitzender, sehr geehrte Abgeordnete,

ich bedanke mich für die Einladung zur Sachverständigenanhörung. Ich freue mich, dass der Freistaat Sachsen ebenso wie einige andere Bundesländer ein eigenes Informationssicherheitsgesetz nach dem Vorbild des BSI-Gesetzes plant. Dieses schafft die dringend notwendigen Rechtsgrundlagen und Rahmenbedingungen, um die Landesbehörden und Bürgerdaten vor Angriffen und weiteren IT-Sicherheitsvorfällen zu schützen.

Der Gesetzentwurf zur Neuordnung der Informationssicherheit im Freistaat Sachsen ist insgesamt gelungen. Positiv hervorheben möchte ich die umfangreichen und ambitionierten Pflichten aus §4 Abs. 1 für staatliche Stellen. Diese gehen weiter als die meisten anderen Landesgesetze. Ebenfalls sehr positiv ist, dass der Freistaat Sachsen anerkennt, dass hierfür signifikant zusätzliche Stellen und Mittel bereitgestellt werden müssen und dies laut der Gesetzesbegründung auch vorsieht.

Zu einigen Regelungen möchte ich im Folgenden detaillierter Stellung nehmen.

§ 3 Begriffsbestimmungen

Der Entwurf begrenzt den Begriff der Informationssicherheit in Abs. 1 auf die Gewährleistung der drei IT-Sicherheitsschutzziele im Hinblick auf Daten. Er wählt daher bewusst einen anderen Begriff als das BSI-Gesetz, das von Informationen spricht. Dies muss nicht zwingend zu Schutzlücken führen. Allerdings gibt es Angriffe, über sogenannte Seitenkanäle (Side Channels), bei denen der Angreifer aus beispielsweise Abstrahlung oder Verarbeitungsdauer Rückschlüsse auf die Informationen zieht ohne zwangsläufig die Vertraulichkeit konkreter Daten i.S.d. § 202a Abs. 2 StGB zu verletzen. Diese Fälle können aus meiner Sicht jedoch im Rahmen der Auslegung aufgefangen werden.

In den Abs. 8 und 9 werden Inhalts- und Protokolldaten definiert. Die Definition von Protokolldaten ist dabei so formuliert, dass sie auf den ersten Blick primär auf klassische Logfiles von IT-Systemen abzielt. Vom reinen Wortlaut scheinen Verkehrsdaten i.S.d. TKG wie zum Beispiel IP-Adressen und andere Kommunikationsmetadaten nicht erfasst. Die Gesetzesbegründung sieht Verkehrsdaten aber explizit als Protokolldaten. Aus meiner Sicht müsste der Wortlaut aber sehr weit interpretiert werden, um z.B. IP-Adressen als „Beschreibung eines Zustands oder einer Aktion“ zu umfassen. Hier kann es entgegen des Willen des Gesetzgebers zu Schutzlücken kommen, wenn Gerichte Verkehrsdaten als nicht vom Wortlaut erfasst sehen. Dem könnte abgeholfen werden durch die explizite Aufnahme von Verkehrsdaten und anderen Kommunikationsmetadaten, die keine Inhaltsdaten sind, in die Definition.

§ 4 Grundsätze der Informationssicherheit

§ 4 enthält sehr umfangreiche Pflichten im Hinblick auf die Qualität der technischen Schutzmaßnahmen. Ähnlich wie nach der Vorgabe aus Art. 32 DSGVO muss bei der Auswahl von Maßnahmen der Stand der Technik berücksichtigt werden. Abs. 1 verweist zusätzlich explizit auf das jeweils geltende BSI-Grundschutz-Kompendium, was ebenfalls zu berücksichtigen ist. Die Auswahl und sichere Implementierung von Sicherheitsmaßnahmen aus dem 5000-seitigen Kompendium ist jedoch keineswegs trivial. Hierfür braucht es nicht nur IT-Fachkräfte, sondern regelmäßig in IT-Sicherheit geschulte IT-Fachkräfte. Diese sind derzeit nicht leicht für den öffentlichen Dienst zu gewinnen. Um auch kleinere Landesbehörden und Stellen bei der Umsetzung zu unterstützen, wird es entscheiden darauf ankommen, dass der Beauftragte für die Informationssicherheit des Landes neben den Mindeststandards (§5 Abs. 6) auch praktische Orientierungshilfen und Leitlinien (§5 Abs. 1) veröffentlicht. Diese müssen in gewissem Maße auch Interkompatibilität zwischen den Landesstellen gewährleisten.

§ 5 Beauftragter für die Informationssicherheit des Landes

Die Etablierung eines hauptamtlichen Beauftragten für die Informationssicherheit des Landes im Rahmen des Gesetzesentwurf ist zu begrüßen. Etwas unklar bleibt meines Erachtens im Gesetzentwurf jedoch, ob die Verantwortlichkeit für Informationssicherheit im Landesnetz und bei stellenübergreifenden Vorfällen beim Landesbeauftragten liegt. Dies deutet §5 Abs. 3 zwar an, wenn eine explizite Verantwortlichkeitszuweisung für die Sicherheit des sächsischen Verwaltungsnetzes gewünscht ist, sollte diese ins Gesetz aufgenommen werden.

Die durch den Landesbeauftragten initiierten und koordinierten Sensibilisierungs- und Schulungsmaßnahmen sollten sich auf alles Landesangestellten erstrecken und auch nicht-staatlichen Stellen und Kommunen offenstehen.

Nach Abs. 9 unterrichtet der Landesbeauftragte die Öffentlichkeit über wesentliche Entwicklungen. Zusätzlich wäre ein zusätzlicher regemäßiger Informationsrückfluss an die am Landesnetz beteiligten Stellen sinnvoll. Dies kann auch durch das Lagebild des Sicherheitsnotfallteams geschehen (§ 6 Abs. 1).

§ 6 Sicherheitsnotfallteam

Im Hinblick auf die Kompetenzen und Datenverarbeitungsbefugnisse des Sicherheitsnotfallteams aus Abs. 2, 3 und 4 bleibt unklar, worauf sich diese infrastrukturell erstrecken. Geht es nur um die interbehördliche Kommunikation und Schnittstellen des Landesnetzes nach außen oder soll das Sicherheitsnotfallteam auch in lokalen Netzen tätig werden? Hier wäre eine präzisere Formulierung wünschenswert. Falls auch in lokalen Netzen agiert werden soll, sollte dies nur unter Mitwirkung der betroffenen Stelle und deren Datenschutzbeauftragten geschehen.

§ 7 Beauftragter für die Informationssicherheit der staatlichen Stellen

Es erscheint sinnvoll, hier ähnlich wie bei Datenschutzbeauftragten Anforderungen an die persönliche und fachliche Eignung zu stellen. Dies würde den ausgewählten Beauftragten Argumente für erforderliche Aus- und Fortbildungen geben. Dasselbe gilt für § 8.

§§ 12 und 13 Abwehr von Gefahren und Datenspeicherung und -auswertung

Die Befugnisse und Schutzmaßnahmen im abgestuften Verfahren orientieren sich am BSI-Gesetz und erscheinen daher sachgerecht.

Für sinnvoll um die Rechte der betroffenen Landesmitarbeiter und Bürger zu gewährleisten halte ich eine zusätzliche Regelung wie die des §5 Abs. 8 BSIG: eine Einbeziehung des Landesbeauftragten in die Konzepterstellung, Kriterienauswahl und Kontrolle der automatisierten und manuellen Verarbeitung.

§5 Abs. 8 BSIG: Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 24 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.

§ 14 Sicherheitskonzept

Zu begrüßen wäre, wenn das Sicherheitskonzept ebenfalls vorab durch den Landesbeauftragten für Datenschutz geprüft werden würde.

Fazit

Insgesamt erscheint der Gesetzesentwurf gelungen. An einigen Stellen bleiben jedoch Umfänge von Kompetenzen unklar. Zusätzlich sieht das Gesetz keine Rechtsfolgen vor, wenn Stellen die gesetzlichen Anforderungen nicht erfüllen. Dieser Verzicht auf Rechtsfolgen kann bis zur Evaluierung jedoch sinnvoll für die Erprobung sein.

Eine stärkere Einbindung des Landesbeauftragten für Datenschutz in die Datenverarbeitung nach §§ 12 und 13 ist sinnvoll. Zusätzlich könnte für eine größere Akzeptanz der Betroffenen der aufgrund der Zweckbindung rein deklaratorische Passus aufgenommen werden, dass die Daten keinesfalls zur Verhaltens- und Leistungskontrolle verwendet werden dürfen.

Unklar bleibt auch, wie sich die neuen Pflichten aufgrund des Entwurfs mit den bereits bestehenden Pflichten aus Art. 32 DSGVO sowie der Umsetzung der Richtlinie 2016/680 ergänzen. Hier wären ebenfalls Leitlinien der Landesregierung oder des Landesbeauftragten für Informationssicherheit von Vorteil.

Mit freundlichen Grüßen

Ninja Marnau

Senior Researcher
CISPA Helmholtz-Zentrum für Informationssicherheit