Stellungnahme von LOAD e.V.
- Verein für liberale Netzpolitik
zum Gesetzesentwurf der Hessischen Landesregierung
Hessisches Gesetz zum Schutz der elektronischen Verwaltung
(Hessisches IT-Sicherheitsgesetz – HITSiG)
von LOAD-Vorstandsmitglied Caroline Krohn
zur Öffentlichen Anhörung am 15.05.2023 in Wiesbaden

LOAD e.V.
Verein für liberale Netzpolitik

Reinhardtstraße 5
10117 Berlin

Fon: (030) 69203242
Fax: (030) 2000 3893

info@load-ev.de
www.load-ev.de

Vorsitzende:
Ann Cathrin Riedel

Berlin, 15.05.2023

Für die Gelegenheit zur Stellungnahme bedanken wir uns.

ALLGEMEINES

Der Gesetzesentwurf hat sich zum Ziel gesetzt, eine Rechtsgrundlage für die Befugnisse des Hessen CyberCompetenceCenter (Hessen 3C) zu schaffen. Dieses Zentrum ist eine zentrale Stelle zur Unterstützung aller öffentlichen Stellen im Land, mit Hilfe von Datenschutz- und Informationssicherheits-expertise die Verwaltungsdigitalisierung rechtskonform und sicher zu gestalten. Zudem soll die Stelle eines Chief Information Security Officers (CISO) der Landesverwaltung eingerichtet werden.

Hessen3C wurde 2019 im Hessischen Ministerium des Innern und für Sport als Referat der Abteilung VII - Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung eingerichtet. Aufgabe des Hessen3C ist es, die Sicherheit in der Informations-technik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren sowie die Effizienz der Bekämpfung der Cyberkriminalität zu steigern.

Hessen3C arbeitet hierzu eng mit der hessischen Polizei sowie dem Landesamt für Verfassungsschutz Hessen zusammen.

Zunächst einmal ist in aller Deutlichkeit zu loben, dass sich das Land Hessen der Verwaltungsdigitalisierung in verantwortlicher Weise annimmt und erkennt, dass Digitalisierung allein, also ohne Datenschutz und Informationssicherheit, nicht nachhaltig ist. Maßnahmen zu ergreifen und Strukturen zu schaffen, die eine Erhöhung der Sicherheit staatlicher Stellen und letztlich der Bürger:innen zum Ziel zu haben, ist notwendig und begrüßenswert.

LOAD e.V. steht für den Schutz der Bürger:innenrechte und der individuellen Grund- und Freiheitsrechte, also auch der Abwehrrechte gegenüber dem Staat. Die Fürsorgepflicht des Staates muss sich folglich an den treuhändischen Pflichten bei der Verarbeitung der Personenbezogenen Daten orientieren (und sind hier auch unabdingbar). Gleichzeitig aber verwahrt sich der Verein vor übermäßigen Zugriffsrechten einer jedweden staatlichen Institution. Personenbezogene Daten, die der Staat zur Erfüllung seiner Aufgaben nutzt, müssen dem Grundsatz der Notwendigkeit und der Transparenz gegenüber den Bürger:innen folgen. Der Mensch muss jederzeit die Kontrolle darüber haben, was mit den eigenen Daten geschieht.

Grundsätzlich ist anzumerken, dass LOAD e.V. auf Bundes- und Landesebene Moratorien für weitere Sicherheitsgesetze fordert. Grund hierfür ist eine seit dem 11. September 2001 immer wieder verschärfte, fragmentierte und ineinandergreifende Gesetzgebung, bei der eine Anpassung an abnehmende Gefahrenlagen nicht zu einer Reduktion staatlicher Überwachung des/der Bürger:in geführt hat, sondern Bürger:innenrechte kontinuierlich eingeschränkt werden. So auch im vorliegenden Gesetzesentwurf (§20). Mit zunehmender Digitalisierung aller Lebensbereiche nimmt die Verunsicherung des Regulators zu, die im Zweifel zugunsten restriktiver Sicherheitsmaßnahmen und zu Lasten bürgerlicher Freiheiten ausfällt. Darum fordert LOAD e.V. den Beschluss und die Aufrechterhaltung eines Moratoriums bis zu dem Zeitpunkt, an dem eine

Überwachungsgesamtrechnung angestellt wurde, die evidenzbasiert die einzelnen Sicherheitsmaßnahmen auf den Prüfstand stellt.

Insbesondere im Land Hessen, in dem beispielsweise die Vorfälle der digitalen Datenabgriffe bei der Frankfurter Polizei, die einzelnen Vorfälle im Rahmen der Untersuchung des NSU-Terrors sowie des rassistischen Attentats von Hanau sowie jüngst das Urteil des Bundesverfassungsgerichts zur Nutzung von Palantir durch die Hessische Polizei noch größtenteils unaufgearbeitet sind, wäre geboten, mit weiteren Maßnahmen - seien sie auch noch zu gut gemeint - nicht noch mehr zur innenpolitischen Verunsicherung beizutragen, sondern ein solches Gesetz auf ein solides und bereinigtes Fundament aufzubauen. Dies käme dem Vertrauen der informierten Öffentlichkeit in die Integrität und Verlässlichekeit der staatlichen Stellen ebenfalls zugute.

Im Hinblick auf das im vorliegenden Gesetzesentwurf beschriebene Vorhaben ist daher im Wesentlichen und im Grundsatz folgendes anzumerken:

1. Koordination zwischen dem Bund und den Ländern
Im Vorwort wird Bezug genommen auf die aktuelle Bedrohungslage und man bezieht sich auf Cybersicherheitsvorhaben in Bund und Ländern. Da stellt sich unmittelbar die Frage, warum es keine geschlossene Bund-Länder-Strategie zur Bewältigung vorhandener Sicherheitsprobleme gibt. Ein Kompetenzgerangel zwischen den föderalen Ebenen ist in dieser Frage besonders kontraproduktiv. Die in der Zivilgesellschaft als "Cyber-Wimmelbild der Verantwortungsdiffusion" bekannte Zusammenstellung aller Behörden, Zentren und Institutionen, die sich auf irgendeiner Ebene in irgendeiner Weise mit dem Thema Cybersicherheit befassen und einander zuarbeiten sollen wird mit dem angedachten Zentrum für Informationssicherheit um eine weitere Behörde ergänzt. Ob dies für die Bedrohungslage zuträglich ist, sei dahingestellt. Kompetetive Auseinandersetzungen sind vorprogrammiert. Im vorliegenden Gesetzesentwurf wird dieses Problem leider verfestigt.

2. Unabhängigkeit des Zentrums und die Zusammenarbeit mit dem BSI
Besonders wichtig ist die sich hier anschliessende Frage: In welchem Verhältnis soll diese Institution zum Bundesamt für Sicherheit in der Informationstechnik (BSI) stehen? LOAD e.V. fordert seit langem die Unabhängigkeit des BSI vom Bundesministerium des Innern. Der Grund dafür ist die sich immer wieder als kontraproduktiv zeigende politische Interventionsmöglichkeit, die nicht selten fachliche Expertise überstimmt. Dies ist der Sache nicht dienlich. Auch in der Frage des Hessischen Zentrums für Informationssicherheit zeigt sich eine viel zu enge Verflechtung mit dem verantwortlichen Ministerium. Der CISO wird nicht etwa wie der Landesbeauftragte für Datenschutz und Informationssicherheit von der Landesregierung vorgeschlagen und vom Landtag gewählt, sondern soll vom verantwortlichen Minister oder der verantwortlichen Ministerin eingesetzt werden. Einsätze des Zentrums sollen durch "eine:n Beschäftige:n des verantwortlichen Ministeriums mit der Befähigung zum Richteramt" legitimiert werden. Indes ist eine Anbindung an das BSI nicht vorgesehen. Die Implementierung der jahrelang entwickelten und bewährten Empfehlungen des BSI bleiben im Gesetzesentwurf eine weitgehend unverbindliche Empfehlung. Diese vier Faktoren sind in keiner Weise nachvollziehbar und der Sachlage nicht dienlich; hier steht der politische Machtanspruch dem sachgerechten Handeln im Wege.

3. Widersprüche in den konkreten Aufgaben und Befugnissen
Der Gesetzesentwurf zeigt in der Gesamtheit ein hohes Maß an technischer Kompetenz im Hinblick auf die Bestimmung von Protokoll- bzw. Metadaten, ist jedoch in der Frage der Definition und der Verarbeitungsweise von "Inhaltsdaten" maximal ungenau. Es ist verständlich, dass zum Zweck der Durchführbarkeit operativer Sicherheitsmaßnahmen bestimmte Einblicke in Daten, auch zuweilen personenbezogenen Daten (wie z.B. IP-Adressen, Emails, etc.) rechtlich legitimiert werden müssen. Auch ist zu begrüßen, dass die Verwendbarkeit personenbezogener Daten intensiv eingeschränkt wird und

dass die Dokumentation sämtlicher Verfahrensschritte und die Löschung von Daten vorgeschrieben wird. Dass eine Automatisierung bestimmter Sicherheitsmaßnahmen angesichts der schieren Menge der zu schützenden Infrastruktur notwendig ist, ist verständlich, aber in bestimmen Fragestellungen zugleich gefährlich. Dass Anonymisierung bzw. Pseudonymisierung gefordert wird, ist positiv zu bewerten. Doch lassen Erwähnungen wie "Kernbereiche privater Lebensgestaltung" - Wendungen, die sonst einschlägige Sicherheitsorgane verwenden - aufschrecken: Warum sollte ein Zentrum, das IT-Systeme sichert, "Kernbereiche privater Lebensgestaltung" verwenden? Wieso bedarf dies einer Limitierung? In diesem Kontext irritiert die Zusammenarbeit mit der Polizei und dem Verfassungsschutz, wie in §5, Nr. (2), 5 genannt: Meldungen von Cybervorfällen müssen natürlich gemacht werden; an Ermittlungen und Strafverfolgung mitwirken: nein. Diese Art der Überbrückung der gesetzlich mit Recht getrennten Institutionen ist schon bei der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) hoch problematisch. Für ein Zentrum, das sich mit der Sicherheit der Landesverwaltung befasst, erscheint zusätzlich die Zuarbeit zu den strafverfolgungs- und nachrichtendienstlichen Behörden unangemessen, falsch und im Hinblick auf die Zugriffe des Staates auf seine Bürger:innen äußerst gefährlich. LOAD e.V. weist an dieser Stelle darauf hin, dass jedwede Cybersicherheitsstrategie mitsamt jeder organisationalen und prozessualen Umsetzung zwingend immer rein defensiv sein muss. Nichts anderes erhöht die Sicherheit der Bürger:innen - weder außen- noch innenpolitisch. Hierbei spielt auch die föderale Ebene keine Rolle. Es muss bei einem Zentrum für Informationssicherheit vornehmlich um Systemhärtung, Verschlüsselung und Monitoring gehen, um Authentifizierungs- und Authorisierungsverfahren, um Backups und die Unterstützung der BSI-Standards. Hierauf muss sich das Zentrum konzentrieren.

4. Realitäten hinsichtlich der Verfügbarkeit finanzieller und personeller Ressourcen

Die Vorstellungen der personellen Besetzung ist unbegründet optimistisch. Es herrscht ein massiver Fachkräftemangel im IT- und speziell im IT-Sicherheitsbereich. Bei einer engen Anbindung des Zentrums an das jeweilige Landesministerium (wahrscheinlich Innen) ist davon auszugehen, dass nach TVöD bezahlt wird - ein Problem für die IT des öffentlichen Dienstes, das allseits bekannt ist. Der Marktwert für diese Aufgabe wirklich qualifierter Expert:innen liegt so hoch, dass im Falle einer Struktur, die marktgerechte Gehälter zuliesse, kaum mehr als 5-7 Personen (ohne administratives Personal) zu dem veranschlagten Budget arbeiten könnten. Mit dem Budget und der avisierten Struktur hat man absehbar also entweder ein qualitatives oder ein quantitatives Problem hinsichtlich der Aufgabenbewältigung. Im Vorblatt wird darauf hingewiesen, dass die Alternative zu diesem Gesetz der Erhalt des Status quo ist. Gleichzeitig wird im Gesetzestext selbst darauf hingewiesen, dass die Stellen, denen das Zentrum zuarbeiten soll, selbst primär für ihre Sicherheit verantwortlich bleiben, dass die jeweilige Leitung Budget und Personal dafür vorhalten muss und später, dass es keinen Anspruch auf Leistungen des Zentrums für Informationssicherheit gibt. Also wird die Personalnot insbesondere durch die Tarifbindung sowohl in den Landesbehörden bestehen bleiben - und zudem im neuen Zentrum für Informationssicherheit neu entstehen. Auch deswegen sollte eine engere Anbindung an das BSI zur Konsolidierung von Expertise in Erwägung gezogen werden.

IM EINZELNEN:

a) Zum Vorblatt:

“Die Analyse von Daten in dem für eine schlagkräftige Abwehr von Bedrohungen aus dem Cyberraum erforderlichen Maße wäre (weiterhin) rechtlich nur eingeschränkt zulässig, da hier die Interessen des Datenschµtzes

(Sicht des Betroffenen) und der IT-Sicherheit (Schutz der Systeme) miteinander konkurrieren.”

→ Dieser Satz ist auf zweierlei Art falsch: Datenschutz und Datensicherheit konkurrieren nicht miteinander. Es ist diskutierbar, ob die rechtliche Sicht und die technische Sicht miteinander konkurrieren, aber prinzipiell dient der Datenschutz nicht dem Schutz der Daten, sondern dem Schutz des Menschen, dem die Daten gehören, und seiner Selbstbestimmung - die IT-Sicherheit ist nicht der Schutz der Systeme, sondern der Schutz des Menschen und seiner Informationen mittels Systemen. Beide Ebenen haben den Schutz des Menschen im Blick und zum Ziel.

b) zum Gesetz:

ERSTER TEIL: ALLGEMEINE VORSCHRIFTEN

§3 Grundsätze der Informationssicherheit

(1) Die Orientierung an der IT-Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik und die Umsetzung eines Informationssicherheitsmanagement sollte für alle Stellen grundsätzlich verbindlich sein und entsprechend ständig auditiert werden. Die Befähigung dazu sollte Kernaufgabe des Hessischen Zentrums für Informationssicherheit sein.

(2) Die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik sollten nicht nur zur Anwendung empfohlen werden, sondern verbindlich gelten (s.o.). Wieso lässt sich das HITSiG hier eine wichtige Chance entgehen, das verbindlich zu gestalten?

(3) Was bedeutet es konkret, dass die Verantwortung die Gewährleistung der Informationssicherheit die jeweilige Leiterin oder der Leiter der Stelle für ihren oder seinen jeweiligen Verantwortungsbereich trägt? Was passiert bei Fahrlässigkeit oder grober Fahrlässigkeit, die zu einem Cybervorfall führt? Wer hat im Falle eines Cybervorfalls, bei dem das Hessische Zentrum für Informationssicherheit involviert wird, das Kommando?

ZWEITER TEIL: ORGANISATION

§4 Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

(1) Der CISO darf kein politischer Posten sein; die Politik darf die Fachexpertise nicht dominieren. Die Ernennung und die Aufhängung ist hier entscheidend. Die Regelung im vorliegenden Entwurf muss zwingend nachgebessert werden. Denkbar wäre eine Parallelstruktur zum Landesbeauftragten für Datenschutz und Informationssicherheit.

weiterhin

“Der oder die CISO ist […] von den Dienststellen des Landesverwaltung bei ihrer oder seiner Aufgabenerfüllung zu unterstützen, soweit Rechtsvorschriften nicht entgegenstehen.” → Das schränkt den CISO ein; warum? Welche Rechtsvorschriften könnten dem spezifisch entgegenstehen? Wo bieten sich hier Auslegungspotenziale, die eine erfolgreiche Arbeit des/der CISO unterminieren?

§5 Zentrum für Informationssicherheit

(1) LOAD e.V. appelliert sehr dringend an die Unabhängigkeit und Abkopplung von Ministerien

(2) Die Aufgaben sind insgesamt sehr vage und unspezifisch. LOAD e.V. weist noch einmal ausdrücklich auf die Notwendigkeit einer rein defensiven Sicherheitsimplementierung hin. Aktive Cyberabwehr darf zu keiner Zeit Thema sein.

Die Zusammenarbeit mit Polizei- und Strafverfolgungsbehörden muss hier sehr genau spezifiziert werden: Diese darf technisch bestenfalls interne IT-Sicherheitsfragestellungen betreffen und keine Teilnahme bzw. Amtshilfe bei Ermittlungen, auch weil es hier zu erheblichen Interessenskonflikten kommen kann, wenn Informationen auf diesem Wege zusammengeführt und weiterverarbeitet werden können. Die Polizei und die Nachrichtendienste sollen eigene Cyberkapazitäten für die Strafverfolgung, Ermittlung und Beurteilung aufbauen. Dieser Bereich ist hochproblematisch und erscheint wie eine Umgehung / ein Schlupfloch zur Zusammenarbeit der Institutionen, für die der Gesetzgeber aus guten Gründen eine Zusammenarbeit bisher unterbunden hat – so wie bei Palantir schon geschehen. LOAD e.V. weist zudem darauf hin, dass der Zugriff des Staates auf personenbezogene Daten einer wirksamen Kontrolle durch unabhängige Instanzen wie die Justiz unterliegen muss.

(7) Warum müssen Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit ausgewertet und gesammelt werden? Es gibt Verzeichnisse über bekannte Angriffe, Zerodays, etc. - Wozu eine weitere Sammlung? Warum überlässt man dies nicht dem BSI und/oder definiert den Informationsfluss?

(9) Wem geht die werktägliche Übersicht zu?

DRITTER TEIL: MASSNAHMEN

§7 Datenverarbeitung

(1) Welche der genannten Aufgaben des Zentrums für Informationssicherheit sind die Aufgaben, die im öffentlichen Interesse liegen? Wozu wird hier die Spezifizierung genannt?

(2) Wie kann die betroffene Person nachvollziehen, dass ihre personenbezogenen Daten für eine Sicherheitsmaßnahme angewendet worden ist?

(4) Warum ist die Hinderung der Funktionsweise eines Schadprogramms eine "KANN"-Regelung? Dies muss unmittelbar und verpflichtend geschehen und zudem muss gemeldet und dokumentiert werden. Jede Sicherheitslücke ist zudem umgehend zu schließen. Eine entsprechend scharfe Verpflichtungsklausel muss in einem jeden Cybersicherheitsgesetz in Deutschland stehen.

§8 Verwendung von auf informationstechnischen Systemen gespeicherten Datenabgriffe

(2) Was sind Inhaltsdaten genau?

§13 Übermittlung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten

(3) Die richterliche Zustimmung ist hier entscheidend - diese Verfahren müssen eine unmittelbare Ausnahmeregelung bleiben, sonst geht von dieser Befugnis eine erhebliche Gefahr aus.

§15 Sicherheitskonzept
Welche Stelle genau nimmt die Revision vor? Welcher Sachverstand wird hier vorausgesetzt und an wen soll berichtet werden? LOAD e.V. weist weiterhin darauf hin, dass eine Anbindung an ein Ministerium wenig Checks & Balances zulässt.

VIERTER TEIL: INFORMATIONS- UND DOKUMENTATIONSPFLICHTEN

FÜNFTER TEIL: SCHLUSSVORSCHRIFTEN

§20 Einschränkung von Grundrechten

LOAD e.V. gibt zu Protokoll, dass dies in der Sache hoch problematisch ist.

c) Zur Begründung nimmt LOAD e.V. vorerst keine Stellung.

Über LOAD e.V.

LOAD e.V. - Verein für liberale Netzpolitik, ist ein unabhängiger Verein, der sich für den Erhalt eines freien Internets einsetzt und Bürgerinnen und Bürger dazu ermächtigt, ihre Grundrechte zu verwirklichen. LOAD e.V. möchte den gesellschaftlichen digitalen Wandel konstruktiv unterstützen. Der Verein finanziert sich ausschließlich durch die Mitgliedsbeiträge seiner Mitglieder. Der Verein wurde 2014 gegründet und hat seinen Sitz in Berlin.