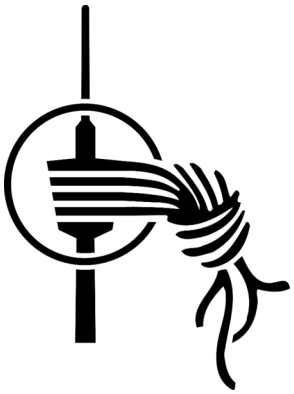
Chaos Computer Club Stuttgart



Stellungnahme zum Gesetzentwurf „Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften“ der Landesregierung Baden-Württemberg

Stefan Leibfarth

Chaos Computer Club Stuttgart

02. November 2020

Vorbemerkung

Gerne machen wir von unserer Möglichkeit der Kommentierung des Gesetzentwurfes der Landesregierung, veröffentlicht über das Beteiligungsportal, Gebrauch. Grundsätzlich bewertet der Chaos Computer Club Stuttgart die Ziele, welche die Landesregierung mit dieses Gesetzentwurf erreichen will, positiv. Im Folgenden finden Sie jedoch, sofern zuordenbar, unsere Kritik bzw. Verbesserungsvorschläge an den jeweiligen Passagen des Gesetzentwurfs.

Möglichkeit Sitzungen digital durch zu führen

Um die Vertraulichkeit der Sitzungen sicher zu stellen, sollte das von Komm.ONE bereitgestellte System die Kommunikation mittels Ende-zu-Ende-Verschlüsselung absichern. Die verwendete Technologie muss dem Stand der Technik entsprechen und der Quellcode der verwendeten Software öffentlich zugänglich sein, denn nur so kann dessen Vertrauenswürdigkeit und Sicherheit überprüft werden.

Zu §1 (3)

Um seinen unzweideutigen Auftrag („Verbesserung der Cybersicherheit“) ohne Interessenkonflikt folgen zu können, darf die Cybersicherheitsagentur Baden-Württemberg nicht dem Innenministerium unterstellt werden und einen unzweifelhaften Status als unabhängige Landesbehörde erhalten. Sollte die Cybersicherheitsagentur Baden-Württemberg dem Innenministerium unterstehen, kann diese ihren Auftrag nicht kompromisslos gerecht werden, weil dem selben Ministerium unterstellten Behörden konträre Interessen verfolgen (z.B. Nutzung von Sicherheitslücken zur Quellen-TKÜ). Ein solche Unabhängigkeit hat sich beispielsweise beim LfDI deutlich positiv bemerkbar gemacht und das Vertrauen von Bürgen und Unternehmen in die Institution gestärkt.

Zu §3 (1) Punkt 3

Hier empfehlen wir explizit ein proaktives Monitoring der IT-Systeme im Zuständigkeitsbereich auf:

A. Zeitnahes einspielen von Sicherheits-Updates

sofern noch kein Update zur Verfügung steht, die Lücke aber bereits öffentlich ist:

B. Die proaktive Überwachung der Implementierung von wirksamen Mitigations-Strategien

Zu §3 (1) Punkt 4

Durch die Gründung der ‚Cybersicherheitsagentur Baden-Württemberg‘ besteht die Gefahr die, ohnehin schon unübersichtliche, staatliche IT-Sicherheitsstruktur noch weiter zu verkomplizieren.

Der Gesetzgeber sollte die Verantwortlichkeiten und Zuständigkeiten der ‚Cybersicherheitsagentur Baden-Württemberg‘ klar, für alle Beteiligten verständlich definieren und gegen die anderen Behörden des Landes (z.B. ZAC BW, CERT BWL) und des Bundes (z.B. BSI) abgrenzen.

Betroffenen Behörden und Unternehmen muss klar ersichtlich sein, welchen alleinigen Ansprechpartner diese jeweils haben und ein reibungsloser Informationsfluss zwischen allen Beteiligten muss zu jedem Zeitpunkt gewährleistet sein. Gerade bei zeitkritischen IT-Sicherheitsvorfällen unter massenhafter Ausnutzung von (ggf. bis dato unbekannten) Sicherheitslücken ist dies von entscheidender Bedeutung.

Zu §5 (10) + (11)
Im Sinne der Transparenz staatlichen Handelns sollten die dem LfDI und dem Innenausschuss vorgelegten Berichte zeitgleich der Öffentlichkeit zugänglich gemacht werden.

Zu §8 (2)
Die Cybersicherheitsagentur Baden-Württemberg darf ausschließlich der Sicherheit von Computern und Netzen verpflichtet sein und Informationen über Sicherheitslücken ausschließlich zu deren Beseitigung anwenden. Bei Kenntnisnahme von öffentlich bisher unbekannten IT-Sicherheitslücken, sind diese unverzüglich an das BSI und den Hersteller zu melden. Die Sicherheitslücken sollen im Rahmen sogenannten Coordinated/Responsible Disclosure-Verfahren behoben und veröffentlicht werden. Eine Geheimhaltung von Sicherheitslücken oder gar deren Weitergabe an andere staatliche Stellen (z.B. ZITiS) um diese ggf. gezielt aus zu nutzen, muss ausgeschlossen sein.