Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

Leitbild und Eckpunkte für eine Cybersicherheitsstrategie Baden-Württemberg

I. Vision

Gesellschaft, Wirtschaft und Verwaltung nutzen in Baden-Württemberg die Chancen und die Innovationskraft der zunehmenden Vernetzung von IT-Produkten, Dienstleistungen und Prozessen.

Über die dadurch gleichzeitig steigenden Gefahren von Angriffen sind sich alle Bereiche der Gesellschaft bewusst. Die Akteure arbeiten zusammen und entwickeln gemeinsame Aktivitäten und Maßnahmen, um auch im Cyberraum ein hohes Niveau an Sicherheit zu gewährleisten. Das Prinzip »Security by Design« ist in allen Produktentwicklungsprozessen etabliert und ein Informationssicherheitsmanagement fester Bestandteil des Risikomanagements eines jeden Unternehmens und der staatlichen und kommunalen Verwaltung. Damit werden mögliche Angriffsflächen minimiert.

Die freiheitlichen Grundsätze unserer Gesellschaft gelten auch im digitalen Zeitalter, da jede einzelne Bürgerin und jeder einzelne Bürger souverän mit vernetzten Geräten und Dienstleistungen umgeht. Die Nutzung von verschlüsselter Kommunikation unterstützt sie dabei, ihre Privatsphäre zu schützen.

II. Leitlinien

Die Absicherung des Cyberraums und der Schutz vor Cyber-Angriffen ist eines der zentralen Themen für die Zukunft Baden-Württembergs. Die staatliche Handlungsfähigkeit und digitale Souveränität muss auch in Fällen von Cyberangriffen gewährleistet sein und die Risiken beherrschbar bleiben.

Der Einsatz von stets aktuellen Sicherheitsprodukten und die Umsetzung von technischen, organisatorischen und personenbezogenen Standards können viele Angriffe abwehren. Prävention, Detektion und Reaktion werden durch zukunftsorientierte, nachhaltige Lösungen und eine enge Zusammenarbeit aller Akteure gestärkt. Staat, Kommunen, Wirtschaft, Wissenschaft und Gesellschaft tragen dafür eine gemeinsame Verantwortung.
Der Schutz personenbezogener Daten, die Authentizität, Integrität, die Vertraulichkeit und Verfügbarkeit von Daten und der miteinander verbundenen Netzwerke sind für unseren Wohlstand und unsere Sicherheit unverzichtbar.

Baden-Württemberg leistet seinen Beitrag für mehr digitale Souveränität in Europa. Das Land behält die Hoheit über seine eigenen Sicherheits- und Datenschutzinteressen und verringert seine Abhängigkeiten von Dritten. Voraussetzungen hierfür sind:

- eine leistungsfähige und sichere Infrastruktur,
- die Beherrschung von Schlüsselkompetenzen und Technologien sowie
- innovationsoffene Rahmenbedingungen der digitalen Souveränität.

Die nachfolgenden Handlungsfelder beschreiben den Rahmen für eine erfolgreiche Cybersicherheit in Baden-Württemberg. Sie betreffen die Akteure der Cybersicherheit in Baden-Württemberg in unterschiedlicher Ausprägung.

III. Handlungsfelder

Staatliche Verwaltung und Kommunen
Land und Kommunen stehen vor der gemeinsamen Herausforderung, die Digitalisierung und neue gesetzliche Anforderungen bewältigen zu müssen. Bürgerschaft und Unternehmen haben einen Anspruch darauf, dass ihre Daten beim Land Baden-Württemberg und seinen Kommunen sicher sind. Im Hinblick auf die Risiken im Cyberraum ist es notwendig, die Fachverfahren von staatlichen Behörden und Kommunen auf professionellem Niveau abzusichern. Das Land bietet hierfür Beratung und aktive Unterstützung der Kommunen.

In der gesamten Landesverwaltung muss ein hohes Sicherheitsniveau erreicht werden. Die derzeit laufende Einführung eines Informationssicherheitsmanagementsystems (ISMS) in allen Ressorts ist hierfür ein wichtiger Schritt. Leistungsfähige Security Operation Center (SOC) in den Rechenzentren tragen wirksam zur Sicherheit der IT-Landschaft bei.

Bei allen zu entwickelnden und zum Einsatz kommenden IT-Anwendungen des Landes müssen Aspekte der Cybersicherheit in den Produkten und Prozessen von Anfang an berücksichtigt werden (Security by Design).

Die vom BSI und in den Bundesländern eingeführte Sicherheits-Gütesiegel und Zertifizierungen sind hierbei zu beachten und anzuwenden. Bei Beschaffungen und IT-Strukturen streben wir an, deutsche oder europäische Produkte, Zertifikate, Soft- und Hardware sowie IT-Sicherheitsunternehmen zu nutzen. Darüber hinaus werden in Baden-Württemberg subsidiär entwickelte Standards den Ländern und der Bundesebene zur Verfügung gestellt.

Schutz kritischer Infrastrukturen und vergleichbarer Einrichtungen
Bei Angriffen auf kritische Infrastrukturen sind eine effektive Krisenkommunikation und eine schnelle Reaktion erfolgskritische Faktoren für eine professionelle Vorfall-bearbeitung in Krisensituationen. Klare Strukturen, Kommunikations- und Entscheidungswege für eine professionelle Krisenkommunikation sind festzulegen und konsequent umzusetzen. Im Fall einer Cyberkrise ist der effiziente, kontinuierliche Informationsfluss zwischen den verantwortlichen öffentlichen und privaten Stellen für eine angemessene und wirksame Reaktion erfolgsentscheidend.

Notfallplanungen und realitätsnahe Cyberabwehrübungen von staatlichen und privaten Institutionen sind periodisch wiederkehrend durchzuführen und zu evaluieren.

Öffentlich-private Partnerschaften
Die Mehrheit der kritischen Infrastrukturen befindet sich in der Hand privater Unternehmen. Daher ist die Frage von öffentlich-privaten Partnerschaften für eine Stärkung der Cybersicherheit von zentraler Bedeutung.

Dabei ist für die Zusammenarbeit ein klarer Rahmen zu definieren, der einen präskriptiven staatlich orientierten und einen kooperativen, marktorientierten Ansatz verbindet.

Die öffentlich-privaten Partnerschaften als Eckpfeiler von Cybersicherheitsstrategien werden vorwiegend als operativ aufgestellte kooperative Plattformen gestaltet, um künftigen Cybersicherheitsbedrohungen gemeinsam mit dem privaten Sektor zu begegnen.

Staat und Wirtschaft gemeinsam
Sensibilisierung, Information, Beratung und aktive Unterstützung von kleinen und mittleren Unternehmen im Bereich IT-Sicherheit sind wichtige Bausteine für eine erfolgreiche digitale Transformation der Wirtschaft. Der Informationsaustausch zwischen Stakeholdern aus Wirtschaft, Wissenschaft und öffentlicher Verwaltung wird kontinuierlich verbessert und institutionalisiert. Dazu werden die im Land vorhandenen Angebote für Cybersicherheit identifiziert, miteinander vernetzt und ihre Sichtbarkeit erhöht.

Vorhandene Strukturen und Plattformen sollten intensiv für einen fortlaufenden Dialog zum wirtschaftspolitischen Handlungsbedarf im Bereich Cybersicherheit und IT-Sicherheit mit den wesentlichen Wirtschaftsakteuren genutzt werden.

Insbesondere bei kleinen und mittleren Unternehmen wird die Bewusstseinsbildung gestärkt, dass sie gegenüber ihren Kunden, Mitarbeitern, Geschäftspartnern und anderen Anspruchsgruppen Verantwortung für einen angemessenen Umgang mit Cybersicherheitsrisiken tragen. Cybersicherheit muss in den Unternehmen Chefsache, professionelle Risikoanalysen und eine angemessene Risikovorsorge sollten bei allen Unternehmen Standard sein.

Privatwirtschaftliche Angebote von IT-Sicherheitsleistungen dürfen dabei nicht von staatlicher Seite ersetzt werden, sondern sollen wo möglich in ihrer Entstehung und Entwicklung unterstützt werden.

Bei der Entwicklung von Standards wird das Know-how der Wirtschaft eingebunden. So wird im Sinne einer kohärenten Regulierung sichergestellt, dass Unternehmen die Standards technisch umsetzen können.

Förderung der digitalen Kompetenzen
Die Digitalisierung durchdringt alle Lebensbereiche bis hinein ins Private. Der digitalen Unbekümmertheit bei Nutzern bzw. Verbrauchern muss entgegengewirkt werden, um so auch im unmittelbaren privaten Umfeld, bei PCs und Mobilgeräten die Gefahr zu senken, Opfer einer Cyberattacke zu werden oder persönliche Daten zu verlieren.

Die digitale Kompetenz der Menschen stellen wir in den Mittelpunkt und fördern sie im Rahmen der zur Verfügung stehenden Haushaltsmittel gezielt. Dies beginnt bereits in der Schule. Das Grundverständnis für Prävention und Reaktion in der Informations- und Cybersicherheit sowie beim Datenschutz wird bereits hier geschaffen.

Wir benötigen zunehmend hochqualifizierte Fachkräfte für Wirtschaft und Verwaltung. Cybersicherheit wird in Studien- und Ausbildungsgängen für unterschiedliche Zielgruppen stärker verankert oder neue Angebote werden implementiert.

Die Gewinnung und Bindung von qualifiziertem Fachpersonal bei Staat, Kommunen und Wirtschaft ist eine zentrale Herausforderung. Zielgruppenorientierte Personalgewinnungs- und Entwicklungskonzepte sollten entwickelt, landesweit aufeinander abgestimmt und umgesetzt werden.

Innovative Forschung und Entwicklung
Die IT-Sicherheitsforschung im Land wird weiter vorangetrieben. Junge Start-Up-Unternehmen werden gefördert und bei ihrer Entwicklung zu einer schnellen Marktreife unterstützt.

Forschungsverbünde müssen unter Einschluss der nationalen und europäischen Ebene vernetzt werden. Die wissenschaftlichen Spitzenergebnisse müssen effektiv geschützt werden.

Die innovativen Forschungen der Hochschulen und der außeruniversitären Forschungseinrichtungen zu Cybersicherheitstechnologien leisten einen wichtigen Beitrag zur Cybersicherheit. Mit prozessorientierten und plattformunterstützten Lösungen kann die Zusammenarbeit von Wissenschaft und Wirtschaft gestärkt und Cybersicherheit zu einem Markenkern Baden-Württembergs werden. So können Cybersicherheit, Informationssicherheit und Datenschutz als Wettbewerbsvorteil bei Produkten und Dienstleistungen „made in Baden-Württemberg“ etabliert und die Innovations- und Wertschöpfungspotenziale in diesen Bereichen gehoben werden.

Nationale und internationale Zusammenarbeit
Grundlegend für eine Stärkung der Cybersicherheit und insbesondere der IT-Sicherheit ist eine flächendeckende Umsetzung der vom BSI und IT-Planungsrat empfohlenen Standards und Maßnahmen. Darüberhinausgehende Empfehlungen für eine ganzheitliche Cybersicherheit von EU, Vereinten Nationen, OSZE, NATO, OECD, Europarat sowie multilateraler Foren (Global Conference on Cyberspace, Central European Cyber Security Plattform, Freedom Online Coalition) werden periodisch überprüft.

Baden-Württemberg wird sich in die bestehenden Netzwerke mit der Cybersicherheitsagentur einbringen. Die Cybersicherheitsagentur wird weitestgehend der zentrale Ansprechpartner für die Landesverwaltung, für die Kommunen, für die Länder, nationale und internationale Behörden und Organisationen für Anliegen der Cybersicherheit, soweit keine ressort- oder aufgabenspezifische Zuständigkeit vorrangig ist. Eine entsprechende Zentralisierung dürfte nur im Hinblick auf wenige Einzelbereiche nicht umsetzbar sein, insbesondere etwa im Hinblick auf die Zusammenarbeit und den Informationsaustausch des Landesamtes für Verfassungsschutz mit anderen Nachrichtendiensten oder im Hinblick auf dessen direkte Zuständigkeit für den Bereich des amtlichen Geheimschutzes in der Wirtschaft.

Baden-Württemberg wird die Cybersicherheit national und international aktiv mit Impulsen mitgestalten und Kooperationen auf internationaler Ebene zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building) nutzen. Vorhandene nationale und europäische Programme für eine Aus- und Fortbildung sowie Weiterbildung, wie beispielsweise für den „Netz- und Informationssicherheits-Führerschein“ sollen im Rahmen der zur Verfügung stehenden Haushaltsmittel genutzt und im Land umgesetzt werden.

IV. Folgen für die Cybersicherheitsarchitektur

Die Stärkung der Cybersicherheitsarchitektur, die Zusammenarbeit, die Bündelung und der Austausch von Wissen und Fähigkeiten aller Akteure ist ein zentrales Anliegen der Cybersicherheitsstrategie Baden-Württembergs.

Die justizielle und polizeiliche Strafverfolgung im Cyberraum gegen Cyberkriminalität und die Fähigkeiten des Nachrichtendienstes im Land gegen Cyberspionage und Cybersabotage werden gestärkt.

Bestehende Akteure, Gremien und Strukturen sollten wo immer möglich gebündelt oder mindestens auf zentralen Informationsplattformen operativ und effektiv miteinander vernetzt werden. Die Cybersicherheitsagentur Baden-Württemberg koordiniert die bereits bestehenden Gremien wie beispielsweise die länderoffene Arbeitsgruppe Cybersicherheit, die Koordinierungsgruppe Informationssicherheit, die KG Cybersicherheit der Interministeriellen Arbeitsgruppe Digitalisierung, den Steuerungskreis Cyberwehr und pflegt die Zusammenarbeit mit dem CISO-Land, der Justiz, der Polizei und den Nachrichtendiensten, dem BSI sowie mit der Europäischen Kommission (z.B. ENISA) und internationalen Partnern. Davon ausgenommen sind die existenten fachspezifischen Gremienstränge der Polizei und der Nachrichtendienste.

Die Zusammenarbeit mit staatlichen und privaten SOC-Strukturen (Security-Operation-Center) sind zu intensivieren und prozessorientiert auszugestalten. Alle weitergabefähigen Informationen externer Stellen sollten weitestgehend zentral durch die Cybersicherheitsagentur aufgenommen, analysiert, bewertet und ggf. mit Handlungshinweisen versehen sofort allen betroffenen Stellen zur Verfügung gestellt werden. Für ein tagesaktuelles ganzheitliches Lagebild für Baden-Württemberg sollen auch die Möglichkeiten der Künstlichen Intelligenz genutzt werden.