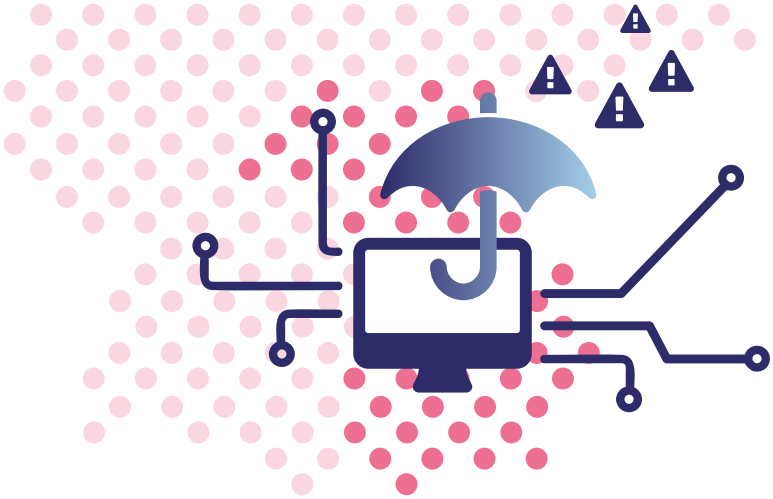
Bayerisches Staatsministerium des Innern, für Sport und Integration

BAYERISCHE CYBERSICHERHEITS-STRATEGIE 2.0

modern.präventiv.resilient



Strategische Ziele und Maßnahmen zur Stärkung der Resilienz von Staat, Wirtschaft und Gesellschaft gegen Cyberngriffe

„Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe und ein Schlüsselfaktor für das Gelingen der Digitalisierung."

(Staatsminister Joachim Herrmann, MdL)

VORWORT

Cybersicherheit ist ein zentrales Tätigkeitsfeld moderner Gefahrenabwehr. Entlang ihres verfassungsmäßigen Auftrags tragen die Länder besondere Verantwortung für deren Gewährleistung. Bayern zeichnet sich seit vielen Jahren durch ein hohes Maß an innerer Sicherheit aus. Dieser Anspruch muss auch für den Cyberraum gelten. Das Internet darf kein rechtsfreier Raum sein. Auch in der digitalen Welt hat der Staat, trotz aller Notwendigkeit der Eigenvorsorge, eine Schutzpflicht gegenüber den Menschen. Diesem Leitbild folgend hat die Bayerische Staatsregierung bereits 2013 die Bayerische Cybersicherheitsstrategie auf den Weg gebracht und seither sukzessive weiterentwickelt. Sie bildet die strategische Grundlage für die Cybersicherheitsarchitektur in Bayern und das Handeln der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben.

Neben der Erweiterung bestehender und Schaffung neuer Präventionsangebote, erfolgt die Umsetzung der aus der Cybersicherheitsstrategie abgeleiteten Maßnahmen regelmäßig durch operative und strukturelle Ergänzungen der jeweiligen Ressorts. Bayern hat so in den vergangenen Jahren eine am Bedarf orientierte, schlagkräftige Cybersicherheitsarchitektur aufgebaut.

Mit der rasanten Technologieentwicklung sowie der stetig voranschreitenden Digitalisierung und Vernetzung geht auch eine Veränderung von Staat, Wirtschaft und Gesellschaft einher. Nach wie vor erkennen Gesellschaft und Wirtschaft in der Digitalisierung und globalen Vernetzung eine große Chance, beispielsweise um persönliche Freiräume oder höhere Wertschöpfung zu schaffen. Die digitale Transformation erhöht gleichzeitig die Verwundbarkeit im Cyberraum.

Die Folgen eines erfolgreichen Cyberangriffs betreffen zunehmend die „reale" Welt und können, insbesondere, wenn für das Gemeinwesen kritische Bereiche getroffen werden, sehr weitreichend sein.

Cybersicherheit ist damit unstreitig eine zwingende Voraussetzung für das Gelingen der digitalen Transformation. Neben der rein technischen Dimension hat Cybersicherheit aber auch eine politische und gesellschaftliche Dimension. Ihre Gewährleistung ist daher eine gesamtgesellschaftliche Aufgabe, die eine enge und vertrauensvolle Zusammenarbeit aller Akteure über Ressort- und Landesgrenzen hinweg erfordert.

Vor dem Hintergrund der dynamischen Bedrohungslage im Cyberraum gilt es, die strategische Ausrichtung staatlichen Handelns im Handlungsfeld Cybersicherheit fortwährend auf den Prüfstand zu stellen und die hierfür getroffenen Maßnahmen auf Vollständigkeit, Wirksamkeit und Verhältnismäßigkeit zu prüfen. Mit dieser Fortschreibung der ganzheitlichen Cybersicherheitsstrategie für Bayern stellen wir uns dieser Verantwortung und tragen so den aktuellen und zukünftigen Herausforderungen Rechnung.

Joachim Herrmann, MdL
Bayerischer Staatsminister

Sandro Kirchner, MdL
Staatssekretär

INHALT

ZIELSETZUNG

Für eine nachhaltige Stärkung der Resilienz von Staat, Wirtschaft und Gesellschaft gegen Cyberangriffe in Bayern gilt es, die wesentlichen Bestandteile und Herausforderungen moderner Cybersicherheitspolitik zielsicher zu identifizieren und strukturiert zu bewältigen.

INHALT UND AUFBAU

Die Bayerische Cybersicherheitsstrategie 2.0 (BayCSS 2.0) beschreibt hierzu den strategischen Rahmen und definiert die vorrangigen operativen Maßnahmen.

Sie formuliert in den Handlungsfeldern

- Schutz der Bürgerinnen und Bürger,
- Schutz der staatlichen Handlungsfähigkeit,
- Schutz der Wirtschaft, KRITIS und Wissenschaft sowie
- Querschnittsaufgaben „Cybersicherheit"

ein praxistaugliches Instrumentarium und legt so die Ziele für alle Bereiche staatlichen Handelns im Bereich Cybersicherheit fest.

Mit Blick auf die aus der Bedrohungslage erwachsenden Herausforderungen erfolgt hierbei nachfolgende Schwerpunktsetzung in den strategischen Zielen und den daraus abgeleiteten Maßnahmen.

Die Reihenfolge der Aufstellung stellt dabei keine Priorisierung dar. Vielmehr gilt es die Umsetzung der Maßnahmen in den einzelnen Handlungsfeldern bedarfsgerecht, parallel und ressortübergreifend abgestimmt voranzutreiben.

A. SCHUTZ DER BÜRGERINNEN UND BÜRGER

Information und Sensibilisierung der Bürgerinnen und Bürger für das Thema Cybersicherheit sowie Unterstützung des Ehrenamts bei der Umsetzung wichtiger Informationssicherheitsmaßnahmen und datenschutzrechtlicher Anforderungen.

A 1. VERBESSERUNG DES DIGITALEN SELBSTSCHUTZES

Ziele (Was wollen wir erreichen?)

- Sensibilität für das Thema Cybersicherheit in der Gesellschaft weiter erhöhen.
- Digitale Kompetenzen in der gesamten gesellschaftlichen Breite fördern.

Herausforderungen (Warum sind die Ziele relevant?)

Mit Blick auf die zunehmende Vernetzung und Digitalisierung aller Lebensbereiche ist ein vertieftes Problembewusstsein in der Gesamtbevölkerung sowie eine zunehmende Sensibilität bei der Erkennung von Bedrohungen und Souveränität im Umgang mit Gefährdungen erforderlich. Die Gesellschaft ist für diese Thematik durchaus erreichbar. So ist es dank entsprechender Sensibilisierung mittlerweile zum Allgemeinplatz geworden, dass etwa eine aktuelle Virenschutzlösung bzw. vergleichbare technische Schutzmaßnahmen für die Sicherheit sehr wichtig sind.

Cyberkriminelle passen sich den verbesserten technischen Schutzmaßnahmen laufend an und adressieren mit ihren Angriffen zudem vermehrt die „Schwachstelle Mensch". Neben der Sensibilisierung für die Gefahren durch dieses sogenannte „Social Engineering" gilt es in den nächsten Jahren die Verbraucherbildung über „klassische" IT-Sicherheitsthemen (z.B. Virenschutz) hinaus weiterzuentwickeln. Die Präventionsinhalte müssen zukünftig auch neue Phänomene wie gezielte Desinformationen und andere illegitime Einflussnahmeaktivitäten im Kontext hybrider Bedrohungen abdecken sowie technologische Entwicklungen wie beispielsweise Generative KI in den Blick nehmen.

Die Vermittlung von Medienkompetenz für alle Altersstufen ist Bestandteil einer ganzheitlichen digitalen Bildung. Medienkompetenz hat Anteil am digitalen Selbstschutz. In einer zunehmend digitalen Welt gehört der Umgang mit Medien und die Fähigkeit, Informationen, insbesondere solchen in sozialen Netzwerken, „richtig" einzuordnen, zu den zentralen Schlüsselqualifikationen für eine verantwortungsvolle Teilhabe an unserer demokratischen Gesellschaft. Die Förderung von Medienkompetenz ist daher auch unverzichtbar, um die digitale Transformation verantwortungsbewusst voranzutreiben.

Darüber hinaus ist es wichtig, dass Bürgerinnen und Bürgern die regelmäßigen Gefährdungen bei der Nutzung digitaler Dienste besser erkennen und Handlungen mit schädlichen Folgen weitestmöglich vermeiden können.

Mit der BayCSS 2.0 wollen wir daher den digitalen Selbstschutz weiter stärken. Unser Ziel ist es, Bürgerinnen und Bürger in die Lage zu versetzen, die neuen Technologien souverän, selbstbestimmt und sicher nutzen zu können. Hierzu sollen Maßnahmen und Projekte der Prävention sowie zur schnellen und unbürokratischen Unterstützung von Bürgerinnen und Bürgern im „worst case" gefördert werden.

Ausgangslage (Wo stehen wir?)

Schon heute misst Bayern der digitalen Bildung einen hohen Stellenwert bei. Mit einer Vielzahl von Angeboten erhalten die Bürgerinnen und Bürger zielgruppenorientierte Angebote zur Vermittlung digitaler Kompetenzen. Die Bildungsangebote und geförderten Projekte der jeweils zuständigen Ressorts bedienen sich hierbei altersgerechter pädagogischer Konzepte und adressieren die gesamte gesellschaftliche Breite vom Kita-Alter bis hin zur Generation 50plus.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Um die digitalen Kompetenzen der Bürgerinnen und Bürger in Bayern weiter zu stärken, soll u. a.

- mit dem Programm PIT – Prävention im Team der angemessene Umgang mit digitalen Medien an Schülerinnen und Schüler vermittelt werden.
- das Referat „LSI für die Öffentlichkeit" beim Landesamt für Sicherheit in der Informationstechnik, insbesondere in Zusammenarbeit mit den BayernLabs, zusätzliche Angebote für den sicheren Umgang mit IT schaffen.
- die Rubrik „Digitale Welt" des unabhängigen Informationsportals www.verbraucherportal.bayern.de kontinuierlich ausgebaut werden.
- das Infoangebot von webhelm.de für pädagogische Fachkräfte und interessierte Erwachsene sowie weitere gamebasierte Ansätze zur Steigerung der Sensibilität der Bevölkerung – insbesondere von jungen Menschen – zu Aspekten der Cybersicherheit erweitert werden.
- das altersgemäße Angebot für Kinder im Portal knipsclub.de zu einer zentralen Grundlage der Bildungsarbeit im Hinblick auf Cybersicherheit fortentwickelt werden.
- die digitale Kompetenz in der Zielgruppe Kinder von 8-10 Jahren durch die App „Wo ist Goldi" weiter gestärkt werden.
- im Rahmen der Entwicklung neuer Materialien der Initiative „Medienführerschein Bayern" soll das Thema Cybersicherheit inhaltlich weiter mitgedacht werden.
- das Kursangebot im Bereich Digitales und Datenschutz an staatlich anerkannten Einrichtungen der Erwachsenenbildung weiter ausgebaut werden. Durch die Stützpunkte für Verbraucherbildung soll insbesondere die Seminarreihe „Smart Surfer – Fit im digitalen Alltag" (www.smartsurfer.bayern.de), die sich an die Generation 50plus richtet, in der Zielgruppe noch stärker verbreitet werden.
- die etablierte Verbraucherarbeit durch die insgesamt 31 Beratungsstellen der beiden staatlich geförderten Verbraucherverbände Verbraucherzentrale Bayern e.V. und Verbraucher-Service e.V. nachhaltig unterstützt und gefördert werden.
- Durch die Initiative „zusammen digital" Menschen mit keinen oder nur geringen Digitalkenntnissen ein niederschwelliges Unterstützungsangebot bereitgestellt werden (https://www.zusammen-digital.de/).
- die bestehenden Initiativen zur Bürger- bzw. Arbeitnehmerfortbildung (IHK-Schulungen, VHS-Angebote, ...) durch die Verbände und Kammern im Bereich der Erwachsenenbildung fortgesetzt und intensiviert werden.
- Mit der Allianz für Digitale Kompetenzen ein umfassendes Weiterbildungsangebot von in Bayern ansässigen digitalaffinen Unternehmen für die Bürgerinnen und Bürger geöffnet werden (https://www.allianz-digitale-kompetenzen.de/).
- durch Unterrichtsbeispiele und teachSHARE-Kurse auf mebis zu Datenschutz, Privatsphäre, Urheberrecht und Passwortsicherheit Schülerinnen und Schüler aller Jahrgangsstufen für rechtliche Problemfelder bei der Selbstinszenierung im Netz mittels multimedialer Erzeugnisse sensibilisiert werden.
- Lehrkräfte im Rahmen der flächenwirksamen Fortbildungsoffensive mit dem Modul „technisches Grundverständnis für die digitale Welt" dabei unterstützt werden, technische Zusammenhänge in Bezug auf die digitale Sicherheit zu verstehen und Schülerinnen und Schülern vermitteln zu können.

Synergien

Eine ständige Fortbildung im digitalen Bereich führt zu einer kritisch-reflektierten Nutzung von IT-Systemen, sozialen Netzen und Internetdiensten und kann mittelfristig auch zum Abbau des Fachkräftemangels beitragen.

Eine zielgruppenspezifische digitale Bildung macht Kinder sowie Erwachsene fit für die digitale Welt und unterstützt somit mittelbar auch die Zielerfüllung in den Selbst- und Unternehmensschutzbereichen (Schutz personenbezogener Daten und Privatsphäre, Schutz vor Social-Engineering-Angriffen, Schutz vor Sabotage und Erpressung).

A 2. FÖRDERUNG DER CYBERSICHERHEIT IM EHRENAMT

Ziele (Was wollen wir erreichen?)

- Förderung der Cybersicherheit im Bereich der ehrenamtlichen Tätigkeiten
- Unterstützung der Vereine in Bayern bei der Umsetzung datenschutzrechtlicher Anforderungen

Herausforderungen (Warum sind die Ziele relevant?)

Bayern ist ein Mitmach-Land. Das Ehrenamt ist eine wichtige Stütze unserer Gesellschaft. Ob im Sport, bei den Rettungsdiensten oder im Bereich Gesellschaft und Kultur. 47 % der Bürgerinnen und Bürger, und damit fast jeder Zweite über 14 Jahre, engagiert sich ehrenamtlich. Die Digitalisierung hat auch bei Vereinen und gemeinnützigen Organisationen Einzug gehalten. Der Sicherheit von Geräten, Anwendungen und der digitalen Verwaltung der Daten kommt auch dort eine immer gewichtigere Rolle zu. Gerade im breiten Spektrum des ehrenamtlichen Engagements der Bürgerinnen und Bürger Bayerns und der damit verbundenen verantwortungsvollen Aufgaben, existieren teilweise erhebliche Defizite im Umgang mit digitalen Daten sowie in den Bereichen IT-Sicherheit im Allgemeinen und (technischer) Datenschutz im Besonderen. Handlungsbedarf besteht insbesondere in den kritischen Bereichen des operativen Betriebs (z. B. Mitgliederverwaltung, Geschäftsstelle, Finanzbuchhaltung).

Ausgangslage (Wo stehen wir?)

Die bayernweite Initiative „Digital Verein(t)“ unterstützt Vereine mit Handbüchern, Workshops, Online-Seminaren sowie einem mobilen Ratgeberteam an 21 Standorten im Freistaat bei der Digitalisierung. Die angebotenen Themen reichen vom Schutz der Vereinsdaten, der sicheren Gestaltung der Vereinshomepage, dem Austausch über Messenger und soziale Medien bis zur Organisation von Videokonferenzen, Wikis und Webinaren.

Auch die BayernLabs adressieren mit ihren Angeboten alle ehrenamtlich Tätigen.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir wollen durch speziell auf das Ehrenamt und insbesondere auf Funktionsträger in gemeinnützigen Vereinen und Organisationen (NPO – non-profit-organisations) zugeschnittene staatliche Angebote das dortige IT-Sicherheitsniveau stärken und diese so bei der Erfüllung ihrer wichtigen Aufgaben für die Gesellschaft entlasten.

Davon umfasst sind insbesondere

- die Erstellung und Fortschreibung eines breit angelegten Schulungskonzepts speziell für ehrenamtliche Mitarbeiter gemeinnütziger Organisationen,
- die Erstellung von Leitfäden zur sicheren Nutzung digitaler Dienste (z. B. Cloud, Onlineangeboten, Zahlungsdienstleister) durch NPO sowie
- die Prüfung, ob und mit welchem Umfang ein Förderprogramm für IT-Sicherheitsmaßnahmen im Rahmen der Digitalisierung bei NPO aufgelegt werden kann.

Um gerade im ländlichen Raum, abseits der Ballungsräume Angebote vor Ort machen zu können, werden auch zusätzliche Kooperationen mit den BayernLabs geprüft.

Synergien

Da die ehrenamtlich Tätigen das über die vorgenannten Maßnahmen vermittelte Wissen auch in ihr berufliches und privates Umfeld tragen, werden hier starke Synergien für Gesellschaft und Wirtschaft begründet.

B. SCHUTZ DER STAATLICHEN HANDLUNGSFÄHIGKEIT

Schaffung und Verstetigung eines einheitlich hohen IT-Sicherheitsniveaus in der gesamten Staatsverwaltung sowie weiterer Ausbau und Stärkung der bayerischen Sicherheitsbehörden zur Bekämpfung von und Prävention gegen Cyberkriminalität, Cyberspionage und -sabotage.

B 1. SCHUTZ DER STAATLICHEN INFORMATIONSTECHNIK

Ziele (Was wollen wir erreichen?)

- Verstetigung eines einheitlich hohen IT-Sicherheitsniveaus in der gesamten Staatsverwaltung durch zentrale und dezentrale Maßnahmen.
- Erhaltung und Ausbau der Eigenkompetenzen der Behörden und Einrichtungen des Freistaats in Bezug auf IT-Sicherheit.

Herausforderungen (Warum sind die Ziele relevant?)

Ein nachhaltiges und hohes Informations- und Cybersicherheitsniveau in der staatlichen Verwaltung ist wesentliche Voraussetzung für eine erfolgreiche Digitalisierung der Verwaltung.

Einhergehend mit der zunehmenden Digitalisierung von Verwaltungsleistungen steigt allerdings auch das diesbezügliche Bedrohungspotenzial im Cyberraum. Die Anzahl, Komplexität und Professionalität von Cyberangriffen nimmt stetig zu. Die staatliche IT ist längst ins Fadenkreuz von Cyberkriminellen und Akteuren fremder Staaten gerückt.

Aus der steigenden Anzahl an IT-Projekten und dem weiteren Ausbau der Digitalisierungsstrategie, erwächst zudem ein Bedarf an hochqualifiziertem Personal. Für die notwendige Stärkung der IT-Sicherheit in den Behörden ist es unabdingbar, die vorhandenen Sicherheitsstrukturen personell und fachlich auf Basis neuer Sicherheitskonzepte weiterzuentwickeln und auszubauen.

Die Ressorts und Behörden verfolgen bedarfsgerechte Ansätze, um die IT-Sicherheit zu stärken. Mit Blick auf die dynamische Bedrohungslage muss dieses Engagement verstetigt und das Cybersicherheitsniveau weiterhin harmonisiert werden.

Ausgangslage (Wo stehen wir?)

Bayern hat leistungsfähige, zentrale IT-Strukturen und damit beste Rahmenbedingungen für ein einheitlich hohes IT-Sicherheitsniveau in der staatlichen Verwaltung geschaffen. Insbesondere das vom LSI überwachte Behördennetz und die Konsolidierung des Serverbetriebs in den staatlichen Rechenzentren gewährleisten die IT-Sicherheit staatlicher Behörden und eine effektive Abwehr von Cyberbedrohungen.

Art. 43 Abs. 4 BayDiG verpflichtet die Behörden des Freistaats dazu, bei der Planung und Umsetzung von maßgeblichen neuen Digitalisierungsvorhaben das LSI zur Gewährleistung der Informationssicherheit frühzeitig zu beteiligen.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Durch geeignete Maßnahmen werden wir – im Rahmen der zur Verfügung stehenden Stellen und Haushaltsmittel – sowohl auf die wachsende Bedrohungslage reagieren als auch auf neue Fragestellungen, die sich insbesondere durch den zunehmen Einsatz von Clouddiensten ergeben. Davon umfasst sind insbesondere folgende zentrale und in Ressortverantwortung stehende dezentrale Handlungsfelder:

- Erarbeitung einer neuen IT-Strategie für die Staatsverwaltung, die im Bereich IT-Sicherheit u. a. folgende Punkte adressiert:
  - Stärkung des Landesamts für Sicherheit in der Informationstechnik
  - Kontinuierliche weitere Verbesserung der Sicherheitsmaßnahmen im Behördennetz.
- Weiterer Ausbau bzw. bedarfsgerechte Anpassung des Sicherheitsmonitorings durch das Security Operation Centers (SOC) beim LSI. Die Erkennung von Bedrohungen für das Bayerische Behördennetz (BYBN) wird so durch den Ausbau der automatisierten Übernahme von Logdaten sowie des automatisierten Austauschs von technischen Angriffsindikatoren (IoC) mit Partnern weiter verbessert.
- Die Behörden müssen auch außerhalb konkreter Projekte verfügbare, für den IT-Betrieb zugewiesene Haushaltsmittel in die IT-Sicherheit investieren, etwa in Maßnahmen zur Systemhärtung und Client-Sicherheit (End-Point-Security).
- Neue Anwendungsszenarien, z.B. Cloudnutzung, müssen fortlaufend mit entsprechenden Policies adressiert und die zentralen Sicherheitsmechanismen und -systeme an diese Herausforderungen angepasst werden. Hierzu bedarf es u.a. der Definition eines behördenübergreifenden ZeroTrust-Modells für das BYBN.
- Implementierung und Pflege eines Informationssicherheitsmanagements auf Basis des IT-Grundschutzes.
- Die bedarfsgerechte und verbindliche Schulung/Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter muss weiter vorangetrieben und daneben die IT-Fachkompetenzen in der Breite und Tiefe verbessert werden.

- Für eine nachhaltige Erhöhung des Cybersicherheitsniveaus soll die Standardisierung (u. a. Art. 51 Abs. 1 BayDiG) so vollzogen werden, dass „security by design“ und „security by default“ gewährleistet sind. Die Nutzung zentraler Dienste des IT-DLZ hat weiterhin Vorrang.

B 2. STÄRKUNG DER KOMMUNALEN IT-SICHERHEIT

Ziele (Was wollen wir erreichen?)

Wir wollen die Stärkung der kommunalen IT-Sicherheit als weiteren wichtigen Baustein zur Schaffung eines hinreichenden IT-Sicherheitsniveaus in der gesamten staatlichen IT (siehe B1) erreichen. Den bayerischen Kommunen soll insbesondere durch die Unterstützung durch das LSI ermöglicht werden, trotz wachsender Cybergefahren die Vorzüge kommunaler Selbstverwaltung auch im digitalen Zeitalter aufrechtzuerhalten.

Herausforderungen (Warum sind die Ziele relevant?)

Bayern ist ein Flächenland. Von den 2.134 Gebietskörperschaften in Bayern haben 72,5% (1.546) weniger als 5.000 Einwohner. Gerade diese kleinen Kommunen sind durch die voranschreitende Digitalisierung (z.B. Angebot digitaler Leistungen schaffen, Schuldigitalisierung, Einhaltung DSGVO) stark herausgefordert.

Die aus der kommunalen Selbstverwaltung resultierende Heterogenität der dortigen IT-Infrastruktur führt zu einer großen Lösungsbandbreite und erfordert daher eine individuelle Herangehensweise.

Ein hinreichendes Sicherheitsniveau erscheint auch in Hinblick auf die Vernetzung innerhalb der kommunalen Ebene oder mit der Landes- und Bundesverwaltung erforderlich.

Ausgangslage (Wo stehen wir?)

Mit Gründung des Landesamts für Sicherheit in der Informationstechnik (LSI) und der dort etablierten Beratung für die bayerischen Kommunen wurden bundesweit einmalige strukturelle Voraussetzungen für eine Steigerung des dortigen IT-Sicherheitsniveaus geschaffen.

Aus dem Portfolio des LSI sind insbesondere

- das Siegel „Kommunale IT-Sicherheit“ des LSI, mit dem ein – auch von kleinen Kommunen – leistbarer Maßstab für Grundsicherheit geschaffen wurde,
- die Handreichung Notfallmanagement und
- die kostenlosen Mitarbeitersensibilisierungen

als beispielhafte Angebote für Kommunen zu nennen.

Darüber hinaus wird durch den Anschluss der Kommunen an das Bayerische Behördennetz die IT-Sicherheit bei den bayerischen Gebietskörperschaften wesentlich gestärkt. Bereits in 66 von 71 Landkreisen existiert eine entsprechende Anschlussmöglichkeit.

Flankierend dazu unterstützt das Bayerische Staatsministerium des Innern, für Sport und Integration im Rahmen eines sukzessive fortentwickelten Förderprogramms die bayerischen Gebietskörperschaften seit Juli 2015 mit dedizierten Angeboten bei der Implementierung eines hinreichenden Informationssicherheits-Managementsystems.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Mit Blick auf die hinsichtlich der Cyber- und Informationssicherheit bestehenden wechselseitigen Bezüge und Verpflichtungen zwischen Landes- und Kommunalverwaltungen wollen wir die IT-Sicherheit bei den bayerischen Gebietskörperschaften weiter stärken und hierfür die staatlichen Unterstützungsangebote wie folgt fortentwickeln:

- Ausbau des kommunalen Beratungsangebots des LSI,
- Fortsetzung des Roll-Out „Warn- und Informationsdienst“ und Kommunal-MISP (Malware Information Sharing Plattform),
- weitere Stärkung des Lagezentrums des LSI als Kommunal-CERT sowie
- Ausbau und Definition der Unterstützung im Sicherheitsvorfall.

Synergien

Als Behördennetz-Teilnehmer sind die IT-Infrastrukturen der Kommunen Teil der staatlichen IT. Die Stärkung der dortigen IT-Sicherheit fördert somit auch das gesamtstaatliche IT-Sicherheitsniveau.

B 3. ANFORDERUNGSGERECHTE AUSSTATTUNG DER STRAFVERFOLGUNGSBEHÖRDEN

Ziele (Was wollen wir erreichen?)

- Die fachliche Befähigung von Strafverfolgungsbehörden und die entsprechenden Aus- und Fortbildungsinhalte bedarfsorientiert weiterentwickeln.
- Erforderliche Anpassungen des Rechtsrahmens, insbesondere dringend benötigte Befugnisse im Bereich der Datenerhebung und -speicherung anstoßen.

Herausforderungen (Warum sind die Ziele relevant?)

Seit Jahren verzeichnen wir im Deliktsfeld „Cybercrime" ein hohes Niveau an Straftaten. Die Täter nutzen fortwährend neue Angriffsstrategien und organisieren sich häufig arbeitsteilig und hochprofessionell in der Anonymität des Internets. Sie agieren regelmäßig aus dem Ausland, verursachen hohe Schäden und stellen mitunter eine reale Gefahr für unsere Demokratie und die wirtschaftlichen Grundlagen unserer Gesellschaft dar.

Dieser Entwicklung muss seitens der Strafverfolgungsbehörden weiterhin kraftvoll begegnet werden. Eine erfolgreiche Strafverfolgung im Cyberraum ist Grundvoraussetzung für die Umsetzung des staatlichen Gewaltmonopols im Cyberraum. Das Internet darf sich nicht zu einem rechtsfreien Raum entwickeln. Dies gilt in besonderem Maße für neuartige Technologien wie beispielsweise fortschrittliche Künstliche Intelligenz, das Metaverse und IoT.

Ausgangslage (Wo stehen wir?)

Bayern ist bei der Bekämpfung von Cyberkriminalität bereits hervorragend aufgestellt. Das ist das Ergebnis einer konsequenten und erfolgreichen Sicherheitspolitik und der daraus abgeleiteten Bekämpfungsstrategien. In den Bereichen, in denen der Freistaat Bayern Handlungs- und Regulierungsmöglichkeiten hat, setzt er sich aktiv für mehr Sicherheit ein. Um entschlossen und wirkungsvoll auf die gleichermaßen qualitativ als auch quantitativ steigende Anzahl an Straftaten im Deliktsfeld „Cybercrime" reagieren zu können, hat Bayern starke, hochspezialisierte Einheiten bei Polizei und Staatsanwaltschaften geschaffen.

Hierzu zählen u.a.

- das im Bayerischen Landeskriminalamt zur Bekämpfung der Cyberkriminalität errichtete Dezernat 54 mit der Zentralen Ansprechstelle Cybercrime (ZAC),
- die Kommissariate 11 – Cybercrime bei jeder Kriminalpolizeiinspektion bzw. Kommissariate Cybercrime bei grundsätzlich jeder Kriminalpolizeiinspektion mit Zentralaufgaben und
- die Schwerpunktsachbearbeiter für Cybercrime bei allen Polizeiinspektionen, sowie
- die Zentralstelle Cybercrime Bayern (ZCB) bei der GenStA Bamberg,
- IT-Sonderdezernate bzw. IT-Ansprechpartner bei allen 22 Staatsanwaltschaften für Fälle, in denen die ZCB nicht zuständig ist sowie
- die Cyberstrafkammer beim Landgericht Bamberg.

Als Reaktion auf die dynamischen Veränderungen der Kriminalitätsformen wurden in der Bayerischen Polizei flächendeckend die bisherigen Arbeitsbereiche „Regionale EDV-Beweismittelsicherung und -auswertung (RBA)" organisatorisch in die Kommissariate Cybercrime integriert und gleichzeitig in „Digitale Forensik" umbenannt.

Bei allen Landespolizeipräsidien und dem BLKA wurden zum 1. Juli 2021 im Rahmen des Stellenprogramms „Die Bayerische Polizei 2025" sog. Quick-Reaction-Teams (QRT) eingerichtet, um bei schwerwiegenden Vorfällen eine schnelle Reaktionsfähigkeit zu gewährleisten. Bei der ZCB ist eine Rufbereitschaft eingerichtet, die rund um die Uhr, auch an den Wochenenden, erreichbar ist. Daneben wurde die Sonderlaufbahn der IT-Kriminalisten geschaffen. Hierbei werden studierte Informatiker in einer einjährigen polizeifachlichen Unterweisung zu Polizeivollzugsbeamten ausgebildet und unterstützen die Dienststellen in der Bekämpfung der Cyberkriminalität. Mittlerweile haben bereits 196 ausgebildete IT-Kriminalisten ihren Dienst aufgenommen.

Aktuell werden über 400 Spezialisten in diesem Bereich eingesetzt. Dabei handelt es sich um ca. 300 speziell aus- und fortgebildete Ermittler bei den Kommissariaten und Dezernaten für Cybercrime und ca. 100 IT-Forensiker, die durch Sicherung und Aufbereitung der digitalen Spuren die Ermittlungen unterstützen.

Die ZCB wurde seit ihrer Gründung im Jahr 2015 in den vergangenen Jahren personell und vom Aufgabenzuschnitt kontinuierlich ausgebaut. Waren es zu Beginn nur zwei Staatsanwälte, ist die ZCB heute mit 23 hochspezialisierten Staatsanwälten und 4 IT-Spezialisten eine der größten und erfahrensten Spezialstaatsanwaltschaften Deutschlands.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir werden die Fähigkeiten, Strukturen und Kapazitäten der Strafverfolgungsbehörden für die Verfolgung von Cyberdelikten weiter tatsächlich und rechtlich bedarfsgerecht ausbauen.

Für die weitere Verbesserung der Fähigkeiten im Bereich der digitalen Forensik werden die Expertise von Polizei und Staatsanwaltschaft mit IT-Sicherheitsexperten und Wissenschaftlern der anwendungsorientierten Forschung angereichert und durch nationale und internationale Kooperationen mit hochrangigen Einrichtungen der Forschung und der Industrie (weiter) vorangetrieben.

Es soll geprüft werden, inwieweit bestehende Kompetenzzentren in Bayern (LSI) und beim Bund (BSI, ZITiS) anlassbezogen in die Ermittlungen eingebunden werden können. Gegebenenfalls ist hierfür eine Anpassung des Rechtsrahmens auf den Weg zu bringen.

Cyberangriffe werden immer professioneller und damit gefährlicher. Diesen Entwicklungen müssen das Straf- und Strafprozessrecht Rechnung tragen – durch angemessene Strafrahmen und adäquate Ermittlungsinstrumente. Wir werden uns daher weiter dafür einsetzen, dass digitale Daten strafrechtlich genauso geschützt werden wie körperliche Gegenstände. Notwendig sind daher etwa eine Erhöhung der Strafrahmen oder die Erweiterung der aktuellen Straftatbestände um Regelbeispiele und Qualifikationstatbestände, z.B. für Angriffe auf kritische Infrastrukturen, auf eine große Menge von Daten oder auf Daten, die den höchstpersönlichen Lebensbereich berühren. Zur wirksamen Bekämpfung von Cybercrime setzen wir uns auch weiter für eine Erweiterung der Ermittlungsbefugnisse der Strafverfolgungsbehörden im Bereich Cybercrime i.e.S. ein. Insbesondere müssen beim Verdacht einer Straftat nach §§ 202a ff., 303a f. StGB eine Telekommunikationsüberwachung in Form der „Serverüberwachung" oder eine Online-Durchsuchung rechtlich ermöglicht werden. Gerade diese Ermittlungsinstrumente liefern in diesem Deliktsbereich häufig die einzig erfolgversprechenden Ansätze und müssen den Strafverfolgungsbehörden daher zügig zur Verfügung gestellt werden. Darüber hinaus machen wir uns weiter insbesondere dafür stark, dass die vom EuGH in ständiger Rechtsprechung bestätigten Spielräume für die Verkehrsdatenspeicherung genutzt werden, wonach insbesondere eine allgemeine und unterschiedslose Speicherung von IP-Adressen für einen auf das absolut Notwendige begrenzten Zeitraum u.a. zur Bekämpfung schwerer Kriminalität mit dem Unionsrecht vereinbar ist. Die Verkehrsdatenspeicherung (insbesondere auch von IP-Adressen) ist für erfolgreiche Ermittlungen im digitalen Zeitalter unerlässlich. Sie kann im Einzelfall auch für die Ermittlung der Täter von Cyberangriffen von großer Bedeutung sein.

Synergien

Eine effektive Strafverfolgung trägt durch ihre generalpräventive Wirkung auch zur Sicherheit der ITInfrastruktur von Staat, Wirtschaft und Gesellschaft bei. Gleichzeitig können Erkenntnisse aus der Strafverfolgung auch die Sicherheit der staatlichen IT verbessern.

B 4. WEITERE INTENSIVIERUNG DES INFORMATIONSAUSTAUSCHES

Ziele (Was wollen wir erreichen?)

- Vertiefung eines schnellen umfassenden Informationsaustausch der Behörden und Einrichtungen mit Cybersicherheitsaufgaben in Bayern
- Durch Informationsvorsprung „vor die Lage" kommen.

Herausforderungen (Warum sind die Ziele relevant?)

Um der dynamischen Bedrohungslage im Cyberraum weiterhin wirkungsvoll begegnen zu können, besteht Bedarf an einem regelmäßigen, zügigen Austausch wichtiger Informationen im Bereich der Cybersicherheit zwischen allen Behörden und Einrichtungen mit Cybersicherheitsaufgaben sowie einer Sammlung, zeitnahen Aufbereitung und Weiterverteilung von Informationen.

Die mit Cybersicherheit und Cyberkriminalität befassten Behörden arbeiten teilweise nach dem Legalitätsprinzip, teilweise sichern sie ihren Zielgruppen aber auch eine hohe Vertraulichkeit zu. Diese Vertrauensstellung gilt es zu bewahren und zu stärken, um den stetig steigenden Anforderungen bestmöglich Rechnung tragen zu können.

Ausgangslage (Wo stehen wir?)

Als zentrale ressortübergreifende Maßnahme wurde Anfang 2020 die „Cyberabwehr Bayern (CAB)" errichtet. Dabei handelt es sich um eine behördeninterne Informations- und Kooperationsplattform für alle bayerischen Landesbehörden mit Cyber-Sicherheitsaufgaben. Das dortige Cyber-Lagezentrum hat u.a. die Aufgabe, Lageerkenntnisse zu dokumentieren und behördenübergreifend abgestimmte Cyber-Lagebilder zu erstellen.

Ein umfassendes, behördenübergreifendes Cyber-Lagebild ist die Voraussetzung für die qualifizierte Bewertung der Cybersicherheitslage in Bayern und für die zielgerichtete Veranlassung angemessener darauf aufbauender Maßnahmen. Dies wurde durch die Informations- und Kooperationsplattform Cyberabwehr Bayern (CAB) erreicht. Die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben arbeiten nach dem Grundsatz „security is for sharing" eng und vertrauensvoll zusammen.

Ergänzend bietet der tägliche Lagebericht des LSI umfassende Informationen für die mit Informationssicherheit befassten Stellen der Ressorts sowie für die an der CAB beteiligten Behörden.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir wollen die bestehenden Verfahren zur Organisation und Teilung von Informationen zum operativen Lagebild weiterentwickeln. Der Informationsaustausch innerhalb der CAB soll hierzu standardisiert und mittelfristig weitestgehend automatisiert erfolgen. Ebenso soll eine regelmäßige Auswertung durch das Cyberlagezentrum der CAB erfolgen.

Die rechtlichen Schranken für den Informationsaustausch, insbesondere hinsichtlich rein technischer Information, werden überprüft und ggf. bedarfsorientiert angepasst.

B 5. ETABLIERUNG EINES BEHÖRDENÜBERGREIFENDEN CYBERTRAININGS

Ziele (Was wollen wir erreichen?)

- Die Bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben „Raum“ schaffen die notwendigen Rahmenbedingungen für gemeinsame Übungen.
- Planung und Durchführung (Koordination) regelmäßiger ressort- und sektorübergreifender Übungen von Cyberlagen.

Herausforderungen (Warum sind die Ziele relevant?)

Bestehenden Strukturen und Prozesse müssen mit regelmäßigen Übungen einem praxistauglichen Stresstest unterzogen werden, auch um eine detaillierte Analyse über Schwere und Auswirkungen im Falle einer ernsten Cyberkrise erstellen zu können.

Neben der ständigen perspektivischen Fortschreibung der entsprechenden Aus- und Fortbildungskonzepte bedarf es auch der regelmäßigen Übung an praxisnahen Anwendungsfällen und in behördenübergreifenden Szenarien.

Ausgangslage (Wo stehen wir?)

In der Vergangenheit haben gemeinsame Übungen auf unterschiedlichen Ebenen (z. B. LÜKEX) jeweils nicht nur zum Training und Routinegewinn der beteiligten Behörden und Mitarbeiter beigetragen, sondern auch Regelungs- und Optimierungsbedarfe offenbart.

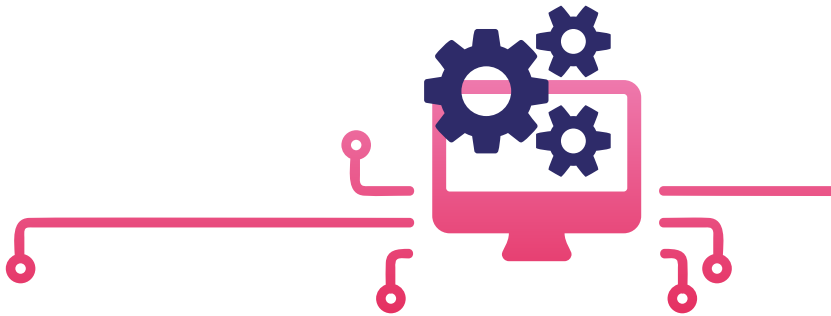
Die Gemeinsame Rahmenkonzeption der ZCB und des BLKA für die Bewältigung von Großlagen bei einem Cybercrime-Angriff beschreibt Regelungen zur Bewältigung einer „Großlage Cybercrime“ und somit den Fall von umfangreichen Ermittlungen mit hoher Wertigkeit und damit einhergehender großer Öffentlichkeitswirksamkeit. Das Konzept ist darauf ausgerichtet, organisatorische und kriminaltaktische Grundlagen zu schaffen bzw. zu gewährleisten, indem an den jeweiligen Schnittstellen das Vorgehen abgestimmt und Informationen ausgetauscht werden. Darüber hinaus haben sich auch die Übungen im LSI bewährt und sind zu einem übergreifenden Angebot ausbaufähig.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir wollen die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben in personeller, technischer und infrastruktureller Hinsicht bestmöglich für die Herausforderungen, die aus ihrem Aufgabenbereich erwachsen, ausrüsten und ausbilden.

Durch die Konzeption, Planung und Durchführung behördenübergreifender Cyber-Trainings wollen wir hierfür noch bessere Rahmenbedingungen setzen. Im ersten Schritt werden die bei den Behörden und Einrichtungen mit Cybersicherheitsaufgaben – insbesondere bei der ZAC, ZCB und dem LSI – vorhandene Konzepte konsolidiert und zu einem behördenübergreifende Schulungs- und Übungskonzept weiterentwickelt. Die fakultative Teilnahme von Unternehmen, insbesondere solche im besonderen öffentlichen Interesse sowie KRITIS und KMU, sollten in der Konzeption – unter Einbindung der zuständigen Ressorts – mittelfristig berücksichtigt werden.

Szenarien von Cyberangriffen sollen auch in Katastrophen- und Zivilschutzübungen auf Landkreis- oder auf höheren Ebenen einbezogen werden.



C. SCHUTZ DER WIRTSCHAFT UND WISSENSCHAFT

Stärkung der Resilienz von Wirtschaft und Forschung in Bayern gegen Cyberkriminalität, Cyberspionage und -sabotage sowie weitere Verbesserung des Anzeigeverhaltens (Dunkelfeldaufhellung) im Deliktsfeld Cybercrime

C 1. ERHÖHUNG DER RESILIENZ IN DER BAYERISCHEN WIRTSCHAFT (INSBESONDERE BEI KMU)

Ziele (Was wollen wir erreichen?)

- Stärkung der Resilienz insbesondere von kleinen und mittleren Unternehmen (KMU) gegen Cyberkriminalität, Cyberspionage und-sabotage

Herausforderungen (Warum sind die Ziele relevant?)

Die Bedrohungslage für die bayerische Wirtschaft ist auf einem anhaltend hohen Niveau. Dies schlägt sich auch in tendenziell seit Jahren stetig steigenden Angriffszahlen nieder.

Die bayerischen Sicherheitsbehörden beobachten, dass sich die Aktivitäten von Cyberkriminellen und von Akteuren ausländischer Nachrichtendienste zunehmend auch gegen kleinere und mittlere Unternehmen (KMU), als Teil größerer Lieferketten (Supply-Chain-Angriffe), richten.

Für den Schutz der IT-Infrastrukturen sind vorrangig die Unternehmen selbst verantwortlich. Große Konzerne sind in Sachen Cybersicherheit meist gut aufgestellt und vernetzt. Staatliche Angebote zur Stärkung der Resilienz von Wirtschaft und Versorgung sollten ihre Schwerpunkte daher im Bereich KMU, mit Schwerpunkt auf wesentliche und wichtige Einrichtungen, setzen.

Ausgangslage (Wo stehen wir?)

Angesichts der Bedrohungen für Unternehmen, insbesondere auch KMU, wurde durch das BLKA in Ergänzung zum Angebot der ZAC eine „Rahmenkonzeption Cybercrime-Präventionsberatung" erarbeitet und im Januar 2020 in Kraft gesetzt.

Mit Cybercrime Quick-Reaction-Teams (QRT), die über eine Rund-um-die-Uhr-Erreichbarkeit verfügen wird bei schwerwiegenden Cybervorfällen seit 1. Juli 2021 eine schnelle Reaktionsfähigkeit gewährleistet. Bei der ZCB ist eine Rufbereitschaft eingerichtet, die rund um die Uhr, auch an den Wochenenden, erreichbar ist.

Um dem Bedarf an zielgruppenspezifischen Präventionsmaßnahmen gerecht zu werden, wurde von der ZAC im BLKA das Projekt Digitale Prävention im Bereich Cybercrime entwickelt. Das Projekt besteht aus drei Modulen (Online-Seminare, Präventionsvideos, Online-Planspiele). Diese werden seit Projektstart in 2020 stark nachgefragt. Das Staatsministerium der Justiz hat im Mai 2021 in Zusammenarbeit mit der ZCB die Broschüre „CYBERCRIME – Hilfe für betroffene Unternehmen" erarbeitet, die sich spezifisch an Unternehmen richtet. Die Broschüre behandelt insbesondere die Punkte „Prävention" und „Anzeigeerstattung". Sie informiert zudem über die Kontaktdaten der Ansprechpartner.

Im Jahr 2022 wurde bei der ZCB zusätzlich eine Taskforce für Cyberangriffe auf Unternehmen und Einrichtungen eingerichtet sowie ein persönlicher Ansprechpartner für Unternehmerinnen und Unternehmer benannt.

Im Rahmen seines gesetzlichen Auftrags verteilt das Cyber-Allianz-Zentrum Bayern (CAZ) beim Landesamt für Verfassungsschutz proaktiv und anlassbezogen (anonymisierte) Warnhinweise an potenziell betroffene Unternehmen in Bayern. Auch finden regelmäßig Informations- und Sensibilisierungsgespräche, Vorträge, Veranstaltungen und Tagungen statt. Freiwillig gemeldete Cyber-Sicherheitsvorfälle werden darüber hinaus forensisch-technisch untersucht und nachrichtendienstlich bewertet. Im Verdachts- oder gar Schadensfall bietet das CAZ individuelle Hilfestellung und konkrete Handlungsempfehlungen an.

Daneben unterstützt auch digitalbonus.bayern seit 2016 bei der Einführung oder Verbesserung der IT-Sicherheit in kleinen Unternehmen. Weiterhin werden Unternehmen im Rahmen des Förderaufrufs IT-Sicherheit des Bayerischen Verbundforschungsprogramms (BayVFP), Förderlinie Digitalisierung des StMWi gewerbliche Unternehmen bei der industriellen Forschung und experimentellen Entwicklung gefördert sowie ihre Vernetzung mit Forschungseinrichtungen gestärkt.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben werden ihre ohnehin schon umfangreichen Präventionsprogramme bedarfsgerecht erweitern und fortentwickeln. Sie unterstützen und fördern dabei auch die Vernetzung der Unternehmen untereinander im Hinblick auf den Austausch zu Cybersicherheit.

In Zusammenarbeit mit den Vertretungen der Wirtschaft prüfen wir, wie die KMU in geeigneter Weise dabei unterstützt werden können, geeignete Zertifizierungsverfahren für ihre Sicherheitsmaßnahmen durchzuführen. Hierzu erfolgt auch der Dialog mit IT-Dienstleistern und Cyber-Versicherungen.

Der Warndienst des Landesamts für Verfassungsschutz (BayLfV), insbesondere für geheimschutzbetreute bayerische Unternehmen im Rahmen des Wirtschaftsschutzes, soll weiter ausgebaut und intensiviert werden.

Für den „Fall der Fälle“ etablieren wir – insbesondere für KMU – eine einheitliche Notfallnummer (Hotline) und werden Unternehmen für das Thema „Notfallmanagement/Krisenbewältigung“ (Business Continuity Management- BCM i.S. BSI-Standard 100-4) beraten und sensibilisieren.

Um die Bereitschaft zur Anzeigenerstattung zu erhöhen, werden wir potenzielle Angriffsopfer in einer breit angelegten Informationskampagne noch intensiver über die Möglichkeiten, Fähigkeiten und Zuständigkeiten der Strafverfolgungsbehörden im Bereich Cybercrime aufklären.

C 2. AUSBAU DES SCHUTZES KRITISCHER INFRASTRUKTUREN (KRITIS)

Ziele (Was wollen wir erreichen?)

Die Resilienz kritischer Infrastrukturen soll weiter gestärkt werden. Im besonderen Fokus stehen kleine KRITIS-Betreiber mit insgesamt hoher Auswirkung auf die Versorgung der Bevölkerung.

Herausforderungen (Warum sind die Ziele relevant?)

Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit hoher Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Nicht zuletzt der Angriffskrieg Russlands gegen die Ukraine hat gezeigt, dass auch mit erhöhter Wahrscheinlichkeit mit Kollateralschäden sowie gezielten Angriffen auch auf KRITIS in Bayern gerechnet werden muss.

Zudem gilt es die gestiegenen Anforderungen an KRITIS aus der NIS-2- und der CER-Richtlinie umzusetzen. Eine besondere Herausforderung bei der Erfüllung des staatlichen Schutzauftrags erwächst hier in manchen Sektoren aus dem fließenden Übergang von versorgungskritischen Bereichen der Daseinsvorsorge zur allgemeinen/unreglementierten Wirtschaft und dem hohen Anbietervolumen (z. B. Lebensmittelmärkte, niedergelassene Ärzte, private Busunternehmen).

Ausgangslage (Wo stehen wir?)

Für den Schutz Kritischer Infrastruktur ist vorrangig der jeweilige Betreiber selbst verantwortlich. KRITIS-Betreiber sind gehalten, durch geeignete technische wie organisatorische Maßnahmen Vorkehrungen zum Schutz und zur Sicherung ihrer Anlagen zu ergreifen.

Auf staatlicher Seite gehören Prävention und angemessene Krisenvorsorge zum originären Aufgabenspektrum der Sicherheitsbehörden sowie der für die jeweiligen KRITIS-Sektoren zuständigen Fachressorts. Polizei und Verfassungsschutz, insbesondere die Dienststellen der sicherheitstechnischen Prävention sowie die Zentrale Ansprechstelle Cybercrime (ZAC) sowie das Landesamt für Sicherheit in der Informationstechnik (LSI), stehen den Betreibern diesbezüglich mit ihrer Expertise beratend zur Seite. Bei allen Landespolizeipräsidien und dem BLKA wurden darüber hinaus sog. Quick-Reaction-Teams (QRT) eingerichtet, um bei schwerwiegenden Vorfällen eine schnelle Reaktionsfähigkeit zu gewährleisten. Bei der ZCB ist eine Rufbereitschaft eingerichtet, die rund um die Uhr, auch an den Wochenenden, erreichbar ist.

Als Reaktion auf die Bedrohungslage im Zusammenhang mit dem Angriffskrieg Russlands gegen die Ukraine hat das Cyber-Allianz-Zentrum Bayern (CAZ) sein Präventionsangebot für Bayerische Unternehmen, insbesondere im Bereich der KRITIS weiter ausgebaut.

Das LSI hat gemäß Art. 42 Abs. 2 BayDiG den Auftrag, KRITIS-Betreiber zu beraten und zu unterstützen. Das Angebot wird mit dem Aufbau des LSI sukzessive ausgebaut, wobei versorgungskritische Sektoren mit Betreibern in kommunaler Trägerschaft priorisiert werden.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Bei der staatlichen Unterstützung zur weiteren Stärkung der Resilienz kritischer Infrastrukturen setzen wir vorrangig auf den Ausbau bewährter Strukturen und die bedarfsgerechte Fortentwicklung bestehender Präventionsprogramme.

Im Rahmen des weiteren Ausbaus des LSI werden nach Priorität weitere KRITIS-Sektoren erschlossen. Positive Erfahrungen aus den Bereichen Krankenhäuser und Wasserversorgung/-entsorgung bekräftigen dabei den Ansatz mit Experten aus dem jeweiligen Sektor, Angebote „aus der Praxis für die Praxis“ zu entwickeln. Dabei sollen die KRITIS-Betreiber von den Erfahrungen der staatlichen IT-Sicherheitsexperten profitieren. Der bundesweit beispielgebende Ansatz, zusätzlich zur Prävention eine spezialisierte IT-Sicherheitsberatung anzubieten wird dabei fortgesetzt, ebenso der weitere Roll-Out des „Warn- und Informationsdiensts“ durch das Lagezentrum des LSI.

Synergien

Der weitere Ausbau des „Warn- und Informationsdienstes“ trägt auch zur Stärkung der Informationssicherheit bei den bayerischen Gebietskörperschaften bei.

C 3. STÄRKUNG DER IT-SICHERHEIT IN STAATLICHEN HOCHSCHULEN

Ziele (Was wollen wir erreichen?)

- Die technische und personelle Verstärkung der IT-Sicherheitsinfrastruktur der staatlichen Hochschulen

Herausforderungen (Warum sind die Ziele relevant?)

Bayern ist ein Hochtechnologieland. Auch bayerische Hochschulen werden zunehmend zu Zielobjekten von Cyberangriffen, Cyberspionage und -sabotage. Ausgehend von dieser Bedrohungslage gilt es die Informationssicherheit im Hochschulumfeld zu stärken.

Durch die große Breite an Aufgabengebieten in Forschung und Lehre sowie durch die dezentrale Organisation ergeben sich in den Hochschulen zwangsläufig heterogene IT-Landschaften und unterschiedlichste Ausprägungen in deren (Sicherheits-) Management.

Als international kooperierende Einrichtungen stehen die Hochschulen in Bayern in Bezug auf die Gewährleistung eines hinreichenden Cybersicherheitsniveaus folglich vor besonderen Herausforderungen.

Ausgangslage (Wo stehen wir?)

Die bayerischen Universitäten, Hochschulen für Angewandte Wissenschaften/ Technischen Hochschulen und Kunsthochschulen koordinieren IT-Infrastrukturen und -Dienste entsprechend ihrer Ende 2021 beschlossenen landesweiten IT-Strategie im „Digitalverbund Bayern“ auf Grundlage von Art. 6 BayHIG. Zur Unterstützung der hochschulinternen Sicherheitsteams wurde ein „Hochschulübergreifender IT-Service Informationssicherheit“ (HITS-IS) eingerichtet, der kooperativ von der Technischen Hochschule und der Universität Augsburg sowie vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften erbracht wird. Der HITS-IS startete 2022 mit den beiden Aufgabenbereichen Informationssicherheitsmanagement und Security Operations; er arbeitet eng mit den IT-Sicherheitsinstanzen im Deutschen Forschungsnetz (DFN) zusammen.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir wollen die IT-Sicherheitsinfrastruktur an den bayerischen Hochschulen im Rahmen der verfügbaren Stellen und Mittel technisch und personell bedarfsgerecht verstärken und durch weitere landesweite Services ergänzen.

In der „Rahmenvereinbarung Hochschulen 2023 bis 2027“ zwischen der Bayerischen Staatsregierung und den staatlichen Hochschulen vom 30. Juni 2023 wurde festgelegt, dass die Hochschulen ein internes Informationssicherheitsmanagementsystem (ISMS) entsprechend dem bayerischen Hochschul-Informationssicherheitsprogramm (HISP) einrichten und die Zusammenarbeit mit dem HITS-IS sicherstellen.

Das HITS-IS wird durch ein Cyber Security Incidence Response Team (eduCSIRT Bayern) ergänzt.

Die Weiterentwicklung der Sicherheitsinfrastruktur an Hochschulen orientiert sich grundsätzlich an wissenschaftsadäquaten Regelwerken (ISIS12, ISO27001/27002, IT-Grundschutzprofil für Hochschulen).

D. CYBERSICHERHEIT IM QUERSCHNITT

Vertiefung des Informationsaustausches zwischen den Behörden und Einrichtungen mit Cybersicherheitsaufgaben sowie Intensivierung der Vernetzung von Staat, Wirtschaft und Forschung im Themenfeld „Cybersicherheit"; Bekämpfung des IT-Fachkräftemangels im Öffentlichen Dienst.

D 1. BEDARFSGERECHTER AUSBAU DER BAYERISCHEN CYBERSICHERHEITSARCHITEKTUR

Ziele (Was wollen wir erreichen?)

- Vertiefung des Informationsaustausches zwischen den Behörden mit Cybersicherheitsaufgaben und wichtigen Akteuren beim Bund und in anderen Ländern,
- Ausbau und Verstetigung einer bedarfsgerechten vertikalen und horizontalen Vernetzung.

Herausforderungen (Warum sind die Ziele relevant?)

Bei der Bekämpfung von Cybercrime und Cyberspionage setzt Bayern vorrangig auf eigene leistungsfähige Strukturen. Föderale Kompetenzverluste durch eine Zentralisierung von Aufgaben bei Bundesbehörden gilt es ebenso abzuwehren, wie es die bewährte Arbeitsweise des LSI zu erhalten gilt.

Die schnelle Reaktion auf neue Bedrohungen ist einer der Schlüsselfaktoren im Kampf gegen Cyberkriminalität und Cyberspionage. Hierzu gilt es insbesondere sicherzustellen, dass relevante Informationen die zuständigen Stellen möglichst schnell erreichen und zur Cybersicherheitslage ein einheitlicher Erkenntnisstand unter den Behörden und Einrichtungen mit Cybersicherheitsaufgaben in Bayern und beim Bund hergestellt ist.

Neben dem bereits mit der CAB erreichten Informationsaustausch gilt es, die Schnittstellen von und zum Bund weiterzuentwickeln.

Ausgangslage (Wo stehen wir?)

Bayern hat eine schlagkräftige und überschneidungsfreie Cybersicherheitsarchitektur und ist in allen relevanten Säulen der Cybersicherheit gut aufgestellt.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Für den weiteren Ausbau der vertikalen und horizontalen Vernetzung prüfen wir entsprechende Kooperationen, u.a. mit den (zentralen) Kompetenzzentren und Bündelungsstellen beim Bund, den Ländern auf mögliche Synergien.

Die Vernetzung der CAB zum Cyber-AZ (NCAZ) des Bundes gilt es zu verstetigen. Das LSI wird sein Engagement im Verwaltungs-CERT-Verbund (VCV) erhöhen und so weiterhin zu einem hohen gemeinsamen Sicherheitsniveau von Bund und Ländern beitragen. Eine vertiefte Zusammenarbeit im Rahmen des VCV wollen wir fördern. Ebenso wird die Zusammenarbeit des LSI mit Partnern, z.B. über andere CERT-Verbünde, wie Trusted Introducer, verstärkt.

D 2. INTENSIVIERUNG DER VERNETZUNG ZU PARTNERN IN WIRTSCHAFT UND FORSCHUNG

Ziele (Was wollen wir erreichen?)

- Intensivierung der Vernetzung von Staat, Wirtschaft und Forschung
- Vertiefung des fachlichen Austausches im Handlungsfeld Cybersicherheit
- Mögliche Best Practices aus Partnerländern für Bayern adaptieren

Herausforderungen (Warum sind die Ziele relevant?)

Cybersicherheit ist eine gesamtgesellschaftliche Aufgabe. Ihre Gewährleistung liegt zwar grundsätzlich in der Verantwortung jedes Einzelnen, doch nur durch kooperatives Zusammenwirken von Staat, Wirtschaft und Forschung kann der Bedrohungslage wirkungsvoll und nachhaltig begegnet werden.

Für den erforderlichen Austausch über das Thema Cybersicherheit bedarf es der nationalen und internationalen Vernetzung der Akteure von Staat und Wirtschaft und der Erörterung der Anliegen und Erwartungen der Wirtschaft an die Politik, aber auch der Anliegen der Politik an die Wirtschaft.

Ausgangslage (Wo stehen wir?)

Das Staatsministerium des Innern, für Sport und Integration hat hierzu gemeinsam mit dem Bitkom e.V. und hochrangigen Vertretern aus der Wirtschaft einen sog. „Round-Table Cybersicherheit" erfolgreich ins Leben gerufen.

Der Austausch auf nationaler und internationaler Ebene zu Bedrohungen aus dem Cyberraum, Best Practice-Beispielen und die Kooperation mit Partnerländern ist in Bayern seit Jahrzehnten gelebte Praxis.

Ergänzend dazu unterstützt das StMWi seit vielen Jahren das Sicherheitsnetzwerk München e.V. (SNM), zur Vernetzung zwischen Forschung, Wirtschaft und Wissenschaft und welches die jährliche internationale Cybersecurity Conference ausrichtet. Darüber hinaus werden durch die Themenplattform Cybersecurity des Zentrums Digitalisierung Bayern (ZD.B) bei Bayern Innovativ vielfältige Leistungen für Wissenschaft und Unternehmenspraxis angeboten.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir werden den „Round-Table Cybersicherheit" – als hochrangig besetztes Forum für Cybersicherheit mit Teilnehmern aus Politik, Verwaltung, Wirtschaft und Forschung – zu einem regelmäßigen „Impulsgeber" für die strategische Ausrichtung und die Abstimmung zu Zukunftsthemen im Handlungsfeld Cybersicherheit fortentwickeln.

Der Teilnehmerkreis wird themenbezogen auf die Vertretungen der Wirtschaft und Interessensverbände erweitert.

Der Austausch und die Zusammenarbeit mit nationalen und internationalen Partnern wird konsequent fortgeführt.

D 3. AUSBAU DER FACHKOMPETENZEN IM BEREICH CYBERSICHERHEIT

Ziele (Was wollen wir erreichen?)

- Stärkung des fachlichen Niveaus der Behörden und Einrichtungen mit Cybersicherheitsaufgaben.
- Steigerung der Bekanntheit des öffentlichen Diensts als attraktiver Arbeitgeber für IT-Fachkräfte im Cybersicherheitsbereich.

Herausforderungen (Warum sind die Ziele relevant?)

Der Fachkräftemangel im öffentlichen Dienst verschärft sich. Dass sich dies vor allem in den digitalen Berufen zeigt, ist insbesondere mit Blick auf die voranschreitende Digitalisierung der öffentlichen Verwaltung eine große Herausforderung.

Ausweislich aktueller Studien[1] wird sich diese Situation in den kommenden Jahren weiter zuspitzen. Dies geht auf den erhöhten Personalbedarf zurück, der vor allem aus der fortschreitenden Digitalisierung und den hohen Pensionierungszahlen in den kommenden Jahren resultiert, und auf eine ausbaufähige Bekanntheit des öffentlichen Dienstes als vielseitiger und durchaus auch für IT-Fachkräfte attraktiver Arbeitgeber trifft.

Ausgangslage (Wo stehen wir?)

Das in der Hightech Agenda Bayern formulierte Ziel, über 13.200 zusätzliche Studienplätze in technischen Zukunftsfeldern (insb. Informatik einschl. Cybersicherheit) an den bayerischen Hochschulen zu schaffen, wird konsequent und zügig umgesetzt.

Zur Fachkräftegewinnung wurden und werden vielfältige Maßnahmen umgesetzt:

Für Berufseinsteiger (Beamte) im IT-Bereich wurde der IT-Fachkräftegewinnungszuschlag von bis zu 400 Euro monatlich eingeführt. Die bereits bestehenden laufbahnrechtlichen Möglichkeiten, Interessierte schnell zu verbeamten, werden aktuell weiter ausgedehnt. Möglich wird auch die bayernweite Gewährung von weiteren Zuschlägen für IT-Fachkräfte in Höhe von bis zu 10% der ersten Stufe des Grundgehalts.

Im Arbeitnehmerbereich: IT-Spezialisten, die nicht verbeamtet werden können, kann eine Fachkräftezulage von bis zu 1.000 Euro monatlich gezahlt werden. Die Eingruppierung in die Entgeltgruppen des TV-L wurde ab 1. Januar 2021 zum Großteil neu geregelt. Für eine Reihe von Beschäftigten ergab sich eine höhere Eingruppierung mit finanziellen Vorteilen.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Wir werden alle Möglichkeiten ausschöpfen, um Neueinstellungen zu beschleunigen, Weiterbildungsangebote auszubauen und flexiblere Arbeitsmodelle zu ermöglichen. So können wir den öffentlichen Dienst als Arbeitgeber attraktiver machen und die notwendigen IT-Fachkräfte gewinnen.

Durch fachliche Entwicklung und Bindung vorhandener IT-Fachkräfte werden wir die Personallücke verringern. Ein besonderes Augenmerk wird dabei auf die Steigerung der Frauenquote im stark technisch geprägten Betätigungsfeld „Cybersicherheit" gerichtet.

1 Fachkräftemangel im öffentlichen Dienst: Bis 2030 fehlen 140.000 IT-Fachkräfte | McKinsey & Company www.mckinsey.de > Publikationen

D 4. KOOPERATION MIT DER CYBERSICHERHEITSFORSCHUNG

Ziele (Was wollen wir erreichen?)

- Weitere Verbesserung der Reaktionsfähigkeit bei und Schutz vor Cybersicherheitsvorfällen
- Kontinuierliche Beobachtung neuartiger Technologien in Bezug auf mögliche Angriffsvektoren.

Herausforderungen (Warum sind die Ziele relevant?)

Bayern soll im Bereich Cybersicherheit weiterhin eine Vorreiterrolle in Deutschland und Europa einnehmen und diese Position ausbauen. Dies zeigt positive Auswirkungen auf die Wirtschaftskraft und Zukunftsfähigkeit Bayern. Zudem kann die Investition in anwendungsorientierte Forschung eine verbesserte Reaktionsfähigkeit bei und Schutz vor Cyber-Sicherheitsvorfällen bewirken.

Die Möglichkeit der Forschung, auf gravierende, thematisch zum Forschungsprojekt gehörende Cybersicherheitsvorfälle schnell unterstützend reagieren zu können, würde den Betroffenen und den damit befassten Behörden und Einrichtungen sehr helfen.

Ausgangslage (Wo stehen wir?)

Das LSI arbeitet aktuell mit Fraunhofer AISEC zum Thema „Zero-Trust“ zusammen.

Die bayerische Justiz kooperiert im Rahmen mehrerer Projekte mit nationalen und internationalen Partnern z.B. im Bereich Dark-Web-Ermittlungen und Blockchain-Analyse zur Verfolgung von Kryptowährungsströmen.

Festlegungen (Wie wollen wir die Ziele erreichen? Unsere wichtigsten Maßnahmen)

Um den großen und komplexen IT-Systemen der Zukunft und auch der Gegenwart in der Cyber-Sicherheitsforschung gerecht zu werden, wird im Rahmen von Forschungsaufträgen ein weiterer Schwerpunkt auf Vorhaben gelegt werden, die „Security at Large“ in großen Systemen gezielt in den Blick nehmen. Hierzu erhöhen wir die Mittel des LSI für Cybersicherheitsforschung, insbesondere Spitzen- und anwendungsorientierte Forschung.

Um der Schnelligkeit der IT-Entwicklung gerecht zu werden, schöpfen wir alle Möglichkeiten aus, um – im Rahmen des Vergaberechts – die Erteilung von Forschungsaufträgen agiler, flexibler und einfacher zu gestalten.

Wir werden die Forschungsnähe der Behörden und Einrichtungen mit Cybersicherheitsaufgaben auch unter dem Aspekt der Personalgewinnung vertiefen.

UMSETZUNG UND ÜBERPRÜFUNG

Rechtsrahmen

Die Umsetzung obiger Maßnahmen erfolgt nach Maßgabe des vorhandenen Rechtsrahmens. Bei der Realisierungsplanung identifizierte Anpassungsbedarfe sind rechtzeitig in die jeweilige Projektierung einzubeziehen.

Zuständigkeiten

Die in der Verordnung über die Geschäftsverteilung der Bayerischen Staatsregierung (StRGVV) festgeschriebenen Geschäftsbereiche der Ressorts bleiben durch die in diesem Dokument beschriebenen strategischen Ziele und Maßnahmen unberührt. Soweit nicht anders aufgeführt, erfolgt die Umsetzung durch das jeweils zuständige Ressort.

Handlungsgrundsätze

Eine ressortübergreifende Umsetzungsplanung findet nicht statt. Greifen Maßnahmen im Zuständigkeitsbereich mehrerer Ressorts ineinander, so erfolgt eine Koordination im Rahmen des Ressortkreises Strategie für Cybersicherheit (RSC) unter Federführung des Staatsministeriums des Innern, für Sport und Integration.

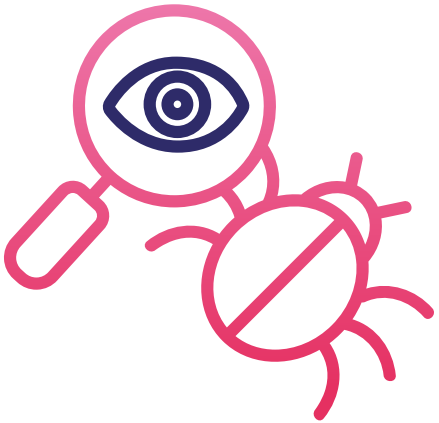
Haushaltsvorbehalt

Die Umsetzung der in den einzelnen Handlungsfeldern beschriebenen Maßnahmen erfolgt im Rahmen der zur Verfügung stehenden Stellen und Mittel bzw. bleibt künftigen Haushaltsverhandlungen vorbehalten.

EVALUATION UND FORTSCHREIBUNG

Ausgehend von der dynamischen Bedrohungslage im Cyberraum gilt es, die getroffenen Maßnahmen zur Gewährleistung eines hinreichenden Cybersicherheitsniveaus ständig auf Wirksamkeit, Vollständigkeit und Verhältnismäßigkeit zu prüfen.

Ergänzend zu dieser ständigen Qualitätssicherung hat sich ein Evaluationszeitraum von maximal 5 Jahren bewährt.



Impressum

Herausgeber: Bayerisches Staatsministerium des Innern, für Sport und Integration
Odeonsplatz 3, 80539 München
www.innenministerium.bayern.de

Bildrechte: AdobeStock/vectorwin
Grafik: Saskia Kölliker
Stand: Juli 2023
Druck: Landesamt für Digitalisierung, Breitband und Vermessung,
Alexandrastraße 4, 80538 München
Gedruckt auf umweltzertifiziertem Papier (PEFC, FSC)

Das Bayerische Innenministerium im Internet:

www.innenministerium.bayern.de

www.twitter.com/BayStMI

www.instagram.com/BayStMI

www.facebook.com/BayStMI

www.youtube.de/BayerischesInnenministerium

„Let's talk Innenpolitik" mit Joachim Herrmann – unser Podcast auf allen großen Plattformen