Cyber-sicherheits-strategie

für das Land Sachsen-Anhalt

Strategische Handlungsfelder zur Stärkung der Cybersicherheit in Verwaltung, Wirtschaft und Gesellschaft

Ministerium für Infrastruktur und Digitales

Stand: Juni 2026

SACHSEN-ANHALT
Ministerium für Infrastruktur und Digitales

#moderndenken

Abkürzungsverzeichnis

Abkürzung	Bedeutung
4C	Cybercrime Competence Center (LKA Sachsen-Anhalt)
AG InfoSic	Arbeitsgemeinschaft Informationssicherheit (des IT-Planungsrates)
BCM	Business Continuity Management
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER-Richtlinie	Critical Entities Resilience Directive / Richtlinie (EU) 2022/2557
CERT Nord	Computer Emergency Response Team Nord (SH, HH, HB, ST)
CISO	Chief Information Security Officer
CSIRT	Cyber Security Incident Response Team
EGovG LSA	E-Government-Gesetz des Landes Sachsen-Anhalt
GDST	Gemeinsam Digital für Sachsen-Anhalt
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
IHK	Industrie- und Handelskammer
IKT	Informations- und Kommunikationstechnologien
IMK	Innenministerkonferenz
InfSG (LSA)	Informationssicherheitsgesetz des Landes Sachsen-Anhalt
ISMS	Informationssicherheitsmanagementsystem
KI	Künstliche Intelligenz
KITU	Kommunale IT-Union eG
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
LAG	Länderarbeitsgruppe
LKA	Landeskriminalamt
MID	Ministerium für Infrastruktur und Digitales
MINT	Mathematik, Informatik, Naturwissenschaften und Technik
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148
NIS-2-Umsetzungsgesetz	Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
PKI	Public Key Infrastructure
VCV	Verwaltungs-CERT-Verbund
VHS	Volkshochschulen
VZSA	Verbraucherzentrale Sachsen-Anhalt
ZAC	Zentrale Ansprechstelle Cybercrime

Grußwort

Das Land Sachsen-Anhalt gestaltet die digitale Zukunft aktiv mit. Das schließt die Verantwortung ein, einen sicheren Rahmen für diese Zukunft zu schaffen. Als Staatsekretär für Digitalisierung im Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt und Beauftragter der Landesregierung für die Informationssicherheit ist es mir ein persönliches Anliegen, dass die Chancen der Digitalisierung nicht durch vermeidbare Sicherheitslücken gefährdet werden. Denn die Zukunft soll die Potenziale der Digitalisierung bestmöglich und zum größten Nutzen aller zur Entfaltung bringen können.

Cyberangriffe sind keine abstrakte Bedrohung. Sie treffen Behörden, Krankenhäuser, Unternehmen und Privatpersonen – in Sachsen-Anhalt ebenso wie anderswo in Deutschland und Europa. Die Folgen können gravierend sein: Datenverluste, ein Ausfall von Verwaltungsleistungen, finanzielle Schäden oder der Missbrauch persönlicher Informationen. Die Räder, die den Alltag, wie wir ihn kennen, aufrechterhalten, stehen plötzlich still. Dieser Realität zu begegnen, verlangt eine gleichermaßen entschlossene wie vorausschauende Antwort des Landes.

Mit dieser Cybersicherheitsstrategie setzen wir einen wichtigen Meilenstein. Erstmals legt das Land Sachsen-Anhalt eine Strategie für den Bereich Cybersicherheit vor, die Verwaltung, Kommunen, Wirtschaft und Gesellschaft gleichermaßen in den Blick nimmt. Sie beschreibt, wo wir heute stehen, aber sie zeigt auch den Weg, den wir gemeinsam gehen wollen.

Cybersicherheit ist eine Gemeinschaftsaufgabe. Sie gelingt nur, wenn alle Beteiligten – ob in der Landesverwaltung, in den Kommunen, in Unternehmen oder im privaten Alltag – die Risiken kennen und Verantwortung übernehmen. Das Land Sachsen-Anhalt stellt die dafür notwendigen Strukturen, Instrumente und Unterstützungsangebote bereit. Diese Strategie bildet den Rahmen, der uns dabei leitet.

Magdeburg, im Juni 2026

Bernd Schlömer
Staatssekretär

Inhaltsverzeichnis

1. Ausgangslage und Zielsetzung

Die digitale Transformation verändert das Zusammenwirken von Staat, Wirtschaft und Gesellschaft im Land Sachsen-Anhalt grundlegend. Neue Technologien und digitale Verwaltungsleistungen eröffnen erhebliche Chancen für eine bürgernahe, moderne Verwaltung und einen leistungsfähigen Wirtschaftsstandort. Gleichzeitig lässt sich beobachten, dass die Angriffsfläche für Cyberbedrohungen wächst und die Professionalisierung von Angriffen stetig zunimmt. Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* dokumentierte hierzu in seinem Lagebericht 2025, dass in Deutschland täglich durchschnittlich 119 neue Schwachstellen in IT-Systemen bekannt wurden – ein Wachstum von rund 24 Prozent gegenüber dem vorigen Berichtszeitraum.[1] Ferner wurden im gleichen Zeitraum rund 950 Anzeigen wegen Ransomware-Angriffen auf Organisationen in Deutschland gestellt, 80 Prozent davon betrafen kleine und mittlere Unternehmen.[2]

Auch im Land Sachsen-Anhalt gab es im Jahr 2025 – abseits der überwiegend (>1 Mio. pro Jahr) automatisiert und ohne Erfolg durchgeführten Cyberangriffe und Vorbereitungshandlungen – einen Anstieg von in der Landesverwaltung gemeldeten Überlastungsangriffen auf IT-Systeme. Dies betraf besonders stark Webserver sowie betrügerische E-Mails, die im Vergleich zum Vorjahr um 60 Prozent zugenommen haben. Weiterhin ist angesichts der rasanten Entwicklung im Bereich der Künstlichen Intelligenz (KI) mit einer zunehmenden Komplexität der Bedrohungslage zu rechnen. In diesem Zusammenhang werfen insbesondere große Fortschritte in den Feldern der agentischen KI und der anweisungsgesteuerten KI zur Schwachstellenausnutzung[3] ihre Schatten voraus.

Mit der Cybersicherheitsstrategie begegnen wir den bekannten, aber auch den neu heraufziehenden Herausforderungen. Dazu ist die strategische Ausrichtung des Landes Sachsen-Anhalt zur nachhaltigen Stärkung der Cybersicherheit anhand der zentralen Schutzziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* formuliert. Unser Ziel ist es, die Resilienz der Geschäftsprozesse, Daten und Systeme der Landesverwaltung, der kommunalen Strukturen, der Wirtschaft und der Gesellschaft gegenüber Gefahren aus dem Cyberraum systematisch zu erhöhen.

Das Land Sachsen-Anhalt versteht Cybersicherheit[4] in einem vollumfänglichen Schutzsinn: Sie umfasst alle Aspekte der Sicherheit in der Kommunikations- und Informationstechnik sowie den Schutz gesellschaftlich relevanter Verwaltungsprozesse, Infrastrukturen und Systeme. Dieses Verständnis geht bewusst über die bloße Abwehr von Straftaten hinaus und betont explizit die aktive Befähigung aller Akteure, den digitalen Raum sicher und souverän mitzugestalten.

Die Landesverwaltung Sachsen-Anhalt versteht digitale Souveränität folgendermaßen: Digitale Aufgaben sollen dauerhaft rechtskonform, sicher und wirtschaftlich erfüllt werden können, ohne dabei irreversibel von einzelnen Anbietern, proprietären Technologien oder fremden Rechts- und Kontrollräumen abhängig zu sein. Dazu soll die Wechsel-, Prüf- und Steuerungsfähigkeit über Systeme, Daten und Betriebsmodelle jederzeit gewährleistet sein. In diesem Sinne bedeutet Digitale Souveränität auch die Entscheidung für ein bewusstes Management von Abhängigkeiten.

1 Die Lage der IT-Sicherheit in Deutschland 2025 (Zusammenfassung), S. 3, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.html?nn=129410#download=1 (abgerufen am 29.04.2026).

2 Die Lage der IT-Sicherheit in Deutschland 2025 (Zusammenfassung), S. 7, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.html?nn=129410#download=1 (abgerufen am 29.04.2026).

3 https://www.heise.de/news/Anthropics-gefaehrliche-KI-Mythos-Unbefugte-wohl-mit-Zugriff-seit-dem-ersten-Tag-11266891.html (abgerufen am 17.04.2026).

4 Der Begriff der Cybersicherheit, wenn nicht anders dargestellt, wird im nachfolgenden Dokument als übergreifender Begriff für alle Themen der IT-Sicherheit, Informationssicherheit und Cybersicherheit verwendet, obgleich es inhaltliche Unterschiede zwischen den einzelnen Bereichen gibt (siehe hierzu auch die Begriffserklärung im Anhang).

Die strategische Ausrichtung orientiert sich an fünf übergeordneten Zielen:

1. Standardisierte Verfahren und verbindliche Sicherheitskonzeptionen für die Informationstechnik in Landesverwaltung und Kommunen.	2. Ausbau der Fähigkeit zur Prävention und Detektion durch resiliente, digital souveräne Infrastrukturen.
3. Fortbildung und Sensibilisierung auf allen Ebenen – von der Verwaltung über die Wirtschaft bis in die Zivilgesellschaft.	4. Besondere Beratung und Unterstützung für Landesverwaltung, Kommunen und Betreiber Kritischer Infrastrukturen.
5. Vernetzung von und Kooperation mit relevanten Akteuren aus den Bereichen Resilienz und Innovation, in Sachsen-Anhalt und darüber hinaus.	

Diese Ziele finden sich durchweg in den Maßnahmen der im Folgenden dargestellten Handlungsfelder wieder (Kapitel 4). Sie können künftig auch als Leitlinien für strategische und organisatorische Maßnahmen herangezogen werden.

2. Einordnung in die Strategie „Sachsen-Anhalt Digital 2030“

Als aktiver Mitgestalter treibt das Land Sachsen-Anhalt die Digitalisierung in Deutschland und Europa voran. Für die Strategie „Sachsen-Anhalt Digital 2030“ wurden drei Zielkategorien gewählt: *digitale vernetzte Verwaltung*, *digitale Innovation* und *digitale vernetzte Gesellschaft*. Sie umreißen die Themenfelder, in denen das Land seine digitalen Aktivitäten intensivieren möchte. Die Cybersicherheit ist dabei ein Querschnittsthema, das als unverzichtbare Grundlage über alle Zielkategorien hinweg verankert ist.[5]

Die vorliegende Cybersicherheitsstrategie flankiert die Digitalstrategie und trägt zu ihrer Weiterentwicklung bei. Wir machen damit transparent, wie die ambitionierten digitalpolitischen Ziele des Landes Sachsen-Anhalt durch ein hohes Sicherheitsniveau geschützt werden, und dass dieses selbst fortlaufend geprüft und an neue Herausforderungen angepasst werden wird. Wir sind davon überzeugt, dass Cybersicherheit als unverhandelbarer Anspruch von Beginn an in jedes Digitalisierungsvorhaben eingebettet werden muss, damit der entstehende digitale Staat das Vertrauen der Gesellschaft gewinnen, erhalten und weiter ausbauen kann.

5 Strategie „Sachsen-Anhalt Digital 2030“, https://mid.sachsen-anhalt.de/digitales/strategie-sachsen-anhalt-digital-2030 (abgerufen am 29.04.2026).

3. Umsetzung der NIS-2-Richtlinie und weiterer rechtlicher und strategischer Rahmen

Die zweite europäische Richtlinie zur Sicherung von Netz- und Informationssystemen (Richtlinie (EU) 2022/2555 oder auch *NIS-2-Richtlinie*)[6] verpflichtet die Mitgliedstaaten, ein hohes gemeinsames Cybersicherheitsniveau sicherzustellen. Gemäß Art. 7 NIS-2-Richtlinie müssen Mitgliedstaaten eine nationale Cybersicherheitsstrategie erlassen. Durch die föderale Struktur in Deutschland besteht diese Anforderung auch für die Bundesländer.

Auf Bundesebene ist das *Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung* (NIS-2-Umsetzungsgesetz) am 6. Dezember 2025 in Kraft getreten.[7] Es verpflichtet nach Schätzungen rund 29.500 Einrichtungen bundesweit zur Einhaltung erhöhter Sicherheitsanforderungen und stellt damit einen Meilenstein im weiteren Aufbau der nationalen Cyberresilienz dar.[8] Ergänzend ist das *Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITISDachG)*[9] zur Umsetzung der *Critical Entities Resilience Directive (CER-Richtlinie)*[10] am 17.03.2026 in Kraft getreten. Es soll die Anforderungen an den Schutz Kritischer Infrastrukturen erhöhen, auch über die IT hinaus.

Im Land Sachsen-Anhalt wurde im Jahr 2019 das *E-Government-Gesetz Sachsen-Anhalt (EGovG LSA)* verabschiedet, welches bereits Regelungen für eine sichere, moderne und bürgerfreundliche E-Government-Landschaft bietet.[11] Das Gesetz regelt das elektronische Verwaltungshandeln sowie die Organisation und Koordinierung der Informations- und Kommunikationstechnologie für die gesamte Landesverwaltung, insbesondere auch für die Kommunen. Zudem wird im Land aktuell ein Informationssicherheitsgesetz erarbeitet, das eine verbindliche Grundlage für Pflichten, Befugnisse und Zuständigkeiten im Bereich der Informationssicherheit nach Vorgaben der NIS-2-Richtlinie auf Landesebene schafft. Ergebnisse der begleitenden Diskussionen zu diesen Maßnahmen fanden bereits Einzug in die Cybersicherheitsstrategie.

Die Strategie orientiert sich an der „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien“ der Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz (IMK). Zudem berücksichtigt sie die Vorgaben der Leitlinie des IT-Planungsrates zur Informationssicherheit.[12] Diese Leitlinien schaffen einerseits Freiräume für landesspezifische Innovation und tragen andererseits punktuell zur Harmonisierung und Vergleichbarkeit zwischen den Ländern bei.

6 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333/80 vom 27.12.2022, https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:32022L2555 (abgerufen am 29.04.2026).

7 BGBl. 2025 I Nr. 301 vom 05.12.2025, https://www.recht.bund.de/bgbl/1/2025/301/VO.html (abgerufen am 29.04.2026).

8 Schätzungen nach Berichten des BSI, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Starterpaket/nis-2-start.html (abgerufen am 29.04.2026).

9 Vollständiger Text des KRITISDachG https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html (abgerufen am 29.04.2026).

10 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333 vom 27.12.2022, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32022L2557 (abgerufen am 29.04.2026).

11 Einordnung des Gesetzes, https://ozg.sachsen-anhalt.de/umsetzung-im-land/rechtliche-grundlagen (abgerufen am 29.04.2026).

12 Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung, https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage_Leitlinie.pdf (abgerufen am 29.04.2026).

4. Handlungsfelder der Cybersicherheit

Zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus identifizieren wir entlang der Länderarbeitsgruppe Cybersicherheit der IMK zwölf zentrale Handlungsfelder. Diese umfassen sowohl die innere Organisation der Landesverwaltung als auch die Zusammenarbeit mit Kommunen, Wirtschaft, Wissenschaft und Zivilgesellschaft:

1. **Umsetzung regulatorischer Anforderungen**
2. **Governance und Organisation**
3. **CERT Nord, CSIRT und Vorfallmanagement**
4. **Technische und organisatorische Sicherheitsmaßnahmen**
5. **Sensibilisierung, Schulung und digitale Kompetenzen**
6. **Risikomanagement**
7. **Notfallmanagement und Business Continuity Management**
8. **Gefahrenabwehr und Strafverfolgung**
9. **Wirtschaft und Schutz Kritischer Infrastrukturen**
10. **Fachkräftegewinnung und -entwicklung**
11. **Innovative Forschung und Entwicklung**
12. **Nationale und regionale Kooperationen**

4.1 Umsetzung regulatorischer Anforderungen

Die NIS-2-Umsetzung auf Bundesebene, die Beschlüsse des IT-Planungsrates als Steuerungsgremium von Bund und Ländern sowie bestehende und angestrebte Landesgesetze verpflichten öffentliche Stellen zur Einhaltung hoher Sicherheitsstandards. Das Land Sachsen-Anhalt setzt auf eine harmonisierte IT-Architektur, um die Anforderungen der NIS-2-Richtlinie effizient bewältigen zu können. Dazu orientiert sich das Land Sachsen-Anhalt an den Richtlinien des BSI[13] und integriert international anerkannte Normen wie die Normenreihe ISO 2700X, was etwa die Umsetzung des neu entwickelten Modells „Grundschutz++“[14] des BSI einschließt. So schaffen wir ein Sicherheitsniveau nach Stand der Technik. Die geplante Umsetzung dieser Vorgaben wird in diesem und folgenden Kapiteln dargestellt.

Zur Umsetzung der dargelegten regulatorischen Anforderungen melden die obersten Landesbehörden dem für Informationssicherheit verantwortlichen Ministerium, *wichtige Stellen* der unmittelbaren Landesverwaltung in ihrer Zuständigkeit. Hierdurch werden die Empfehlungen des vom IT-Planungsrat beschlossenen Identifizierungskonzepts[15] umgesetzt. Dieser Prozess wird alle zwei Jahre wiederholt. Auch wenn diese wichtigen Stellen innerhalb des Vorgehens zur IT-Sicherheitserhöhung priorisiert werden, wird stets bei allen Strategien und Maßnahmen die Befähigung der ganzen Landesverwaltung angestrebt.

13 Übersichtseite des BSI zum IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (abgerufen am 29.04.2026).

14 Grundschutz++, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Grundschutz-in-der-Informationssicherheit/Grundschutz-Plus-Plus/grundschutz-plus-plus_node.html (abgerufen am 29.04.2026).

15 Vorschlag für ein Konzept zur Identifizierung der AG Informationssicherheit des IT-Planungsrats, https://www.it-planungsrat.de/fileadmin/beschluesse/2023/Beschluss2023-39_NIS-2-Richtlinie_Identifizierungskonzept.pdf (abgerufen am 29.04.2026).

4.2 Governance und Organisation

Die Herstellung und Erhaltung eines angemessenen Sicherheitsniveaus ist eine gemeinsame Aufgabe des Landes Sachsen-Anhalt, der Kommunen sowie weiterer Dienstleister wie Dataport und der Kommunalen IT-Union (KITU). Zuständig für Cybersicherheit im Land Sachsen-Anhalt ist das für Informationssicherheit verantwortliche Ministerium. In der laufenden 8. Wahlperiode ist die Aufgabe dem *Ministerium für Infrastruktur und Digitales (MID)* zugeordnet.

Das Land Sachsen-Anhalt baut in Zusammenarbeit mit dem Ministerium für Inneres und Sport gegenüber Bundesbehörden, anderen Ländern und den relevanten nationalen Sicherheitsakteuren eine übergreifende Kontaktstelle auf. Innerhalb dieser Kontaktstelle werden cybersicherheitsrelevante Informationsflüsse in der öffentlichen Verwaltung koordiniert. Das Ministerium steuert den übergreifenden Cybersicherheitsprozess im Land Sachsen-Anhalt und nimmt die Aufgabe der operativen Meldestelle für Sicherheitsvorfälle innerhalb der Landesverwaltung über das Computersicherheitsnotfalleinsatzteam (CSIRT) mit dem CERT Nord wahr. Dazu wird innerhalb des für Informationssicherheit verantwortlichen Ministeriums eine Anlaufstelle eingerichtet, die operativ unabhängig und weisungsfrei agiert.

Die Vernetzung innerhalb der Landesverwaltung hinsichtlich Informations- bzw. Cybersicherheit wird durch die Arbeitsgruppe Informationssicherheit des Landes sichergestellt.

Die Arbeitsgruppe Informationssicherheit besteht aus der oder dem CISO und den Beauftragten für Informationssicherheit der obersten Landesbehörden. Weitere Mitglieder können dauerhaft oder zeitweilig aufgenommen werden. Die Arbeitsgruppe Informationssicherheit wird von der oder dem CISO geleitet.

Der oder die Informationssicherheitsbeauftragten des Landtags, des Landesverfassungsgerichts, des Landesrechnungshofs, der oder dem Landesbeauftragten für Datenschutz und der oder dem Landesbeauftragten für Informationsfreiheit, der Gerichte und der Staatsanwaltschaften sowie das CERT Nord können an den Sitzungen teilnehmen.

Auch der IT-Kontrollbeirat nach § 7 Absatz 1 Satz 1 des Gesetzes zur Regelung des Einsatzes der Informations- und Kommunikationstechnik bei den Gerichten und Staatsanwaltschaften des Landes Sachsen-Anhalt (Justiz-IT-Gesetz – JITG LSA) vom 3. Mai 2021 kann eine Vertreterin oder einen Vertreter zur Teilnahme an den Sitzungen entsenden.

Die Arbeitsgruppe erarbeitet Leit- und Richtlinien und ist als zentrales Austausch- und Abstimmungsgremium für die verwaltungsträgerübergreifende Zusammenarbeit zwischen dem Land und den Gemeinden, Verbandsgemeinden und Landkreisen in der Cybersicherheit in der öffentlichen Verwaltung tätig. Für die Zusammenarbeit zwischen Land und Kommunen wurde ebenfalls das Projekt „Gemeinsam Digital für Sachsen-Anhalt“ (GDST) eingerichtet.[16] Dort förderten themenspezifische Arbeitsgruppen das gegenseitige Verständnis und ermöglichten eine dauerhafte Zusammenarbeit bei der Umsetzung digitaler und sicherheitsrelevanter Vorhaben. Nach dem offiziellen Projektende im Dezember 2025 arbeitet das Projektteam nun gemeinsam im Rahmen der Nachbereitung an der Verstetigung der aufgebauten Strukturen.

4.3 CERT Nord, CSIRT und Vorfallmanagement

Das *Computer Emergency Response Team* (CERT) *Nord* bildet einen zentralen Baustein des Vorfallmanagements und Monitorings im Land Sachsen-Anhalt.[17] Als gemeinsames CERT der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt unterstützt es die Landesverwaltungen und seit der Erweiterung des Dienstleistungsangebots Anfang 2025 auch die sachsen-anhaltischen Kommunen. Die angeschlossenen Stellen profitieren von dessen 24/7-Notfalldienst und dem Austausch von Hinweisen auf Sicherheitsvorfälle (Indicators of Compromise), Bedrohungsanalysen, Warnungen und Handlungsempfehlungen zu sicherheitsrelevanten Themen.

16 Gemeinsam Digital für Sachsen-Anhalt, https://ozg.sachsen-anhalt.de/grundlagen/gemeinsam-digital-fuer-sachsen-anhalt (abgerufen am 29.04.2026).

17 CERT Nord, https://www.certnord.de/ (abgerufen am 29.04.2026).

Für schwerwiegende Vorfälle stehen BSI-zertifizierte Dienstleister bereit, die innerhalb von 24 Stunden vor Ort einsatzfähig sind. Weiterhin organisiert das CERT Nord in der Landesverwaltung Sachsen-Anhalt Übungen zur Cybersicherheit und führt diese vor Ort zum praktischen Erfahrungsgewinn durch.

Überdies ist die Einrichtung eines landeseigenen *Computer Security Incident Response Teams* (CSIRT) innerhalb des für Informationssicherheit verantwortlichen Ministeriums geplant. Es soll als zentrale Meldestelle für Cybersicherheitsvorfälle in der unmittelbaren Landesverwaltung und als Kontaktpunkt zum Verwaltungs-CERT-Verbund fungieren. Gleichzeitig sind wichtige Stellen der unmittelbaren Landesverwaltung zu gestaffelten Meldungen (Erstmeldung, Folgemeldung, Zwischenbericht und Abschlussbericht) bei erheblichen Sicherheitsvorfällen verpflichtet (§ 9 Abs. 1 InfSG LSA). Das CERT Nord wird als externer Partner die Expertise des CSIRT ergänzen.

4.4 Technische und organisatorische Sicherheitsmaßnahmen

Die IT-Infrastruktur der unmittelbaren Landesverwaltung wird in wesentlichen Teilen durch den Dienstleister Dataport betrieben und in Abstimmung mit dem für Informationssicherheit verantwortlichen Ministerium koordiniert. Neben den zentral bereitgestellten Diensten müssen auch dezentrale Einrichtungen – etwa ressorteigene Fachanwendungen oder kommunale Standorte – eigenständige Sicherheitskonzepte auf Basis fundierter Risikoanalysen umsetzen. Hierbei ist der IT-Grundschutz des BSI in Form von Standards, Hilfestellungen und Unterstützungsangeboten für die öffentliche Verwaltung maßgeblich. Im Einklang mit den Zielen der Digitalstrategie wird beispielsweise gezielt die Ausweitung des Einsatzes von Verschlüsselungsverfahren und PKI-Systemen in der unmittelbaren Landesverwaltung gefördert. Ferner werden wichtige Stellen der unmittelbaren Landesverwaltung verpflichtet, Lösungen zur Mehrfaktor- oder kontinuierlichen Authentifizierung zu verwenden.

Darüber hinaus stellt das Datenschutzrecht nach Art. 32 DSGVO verschiedene Anforderungen an die Sicherheit der Datenverarbeitung. Dem Datenschutzrecht liegt ein risikobasierter Ansatz zugrunde, der insbesondere durch das Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ausgestaltet wird. Diese Empfehlungen zu den datenschutzrechtlichen Gewährleistungszielen und Anforderungen sowie zum Datenschutzmodell fördern die datenschutzrechtliche Ausgestaltung und Organisation von informationstechnischen Verfahren, Anwendungen und Infrastrukturen. Es ist als Methode geeignet, die Wirksamkeit der technischen und organisatorischen Maßnahmen einer Datenverarbeitung auf der Grundlage und nach den Kriterien der DSGVO regelmäßig zu überprüfen und fachgerecht zu bewerten. Datenschutzrechtliche Sicherheit und IT-Sicherheit greifen an dieser Stelle ineinander, obwohl sie auf unterschiedliche Ziele ausgerichtet sind, nämlich einerseits auf den Schutz personenbezogener Daten und andererseits auf den Schutz der Institutionen. Deshalb befasst sich auch der IT-Grundschutz mit dem Datenschutz und verweist auf das Standard-Datenschutzmodell.

Grundlage eines hohen Cybersicherheitsniveaus ist die flächendeckende Einführung eines *Informationssicherheitsmanagementsystems* (ISMS) nach den BSI-Standards 200-1 bis 200-3[18] mithilfe der Arbeitswerkzeuge des IT-Grundschutzes und im weiteren Verlauf des Standards „Grundschutz++“[19]. Umgesetzt worden sind hier bereits z. B. standardisierte Meldewege und ein zentrales Asset-Register für die relevanten Informationswerte. Die Einführung wird stetig vorangetrieben: Viele Behörden und Einrichtungen verfügen bereits über ein funktionsfähiges Informationssicherheitsmanagementsystem.

Die Sicherheit von Produkten und Lieferketten der Informations- und Kommunikationstechnologien (IKT) ist integraler Bestandteil eines Informationssicherheitsmanagementsystems. Die öffentlichen Stellen der unmittelbaren Landesverwaltung stellen sicher, dass bei der Beschaffung und dem Betrieb von IKT-Produkten und IKT-Diensten die Sicherheitsanforderungen gegenüber Dienstleistern, Auftragnehmern und Unterauftragnehmern vertraglich verankert werden. Dies umfasst insbesondere Anforderungen an Verschlüsselungsstandards und den Nachweis anerkannter Zertifizierungen.

18 Überblick über die BSI-Standards des IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html (abgerufen am 29.04.2026).

19 Grundschutz in der Informationssicherheit, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Grundschutz-in-der-Informationssicherheit/isms_node.html (abgerufen am 29.04.2026).

Das Land entwickelt hierzu in Abstimmung mit den zuständigen Vergabestellen einheitliche Anforderungsbausteine für IT-Vergabeverfahren und orientiert sich dabei an den Empfehlungen des BSI zur Lieferkettensicherheit.[20]

Kommunen werden bei der Implementierung von erhöhten Cybersicherheitsmaßnahmen durch die KITU, Dataport sowie durch das Landesprojekt „SicherKOMMUNAL“ unterstützt. Nachdem das Projekt mit drei Pilotkommunen gestartet war, steht das Programm seit 2025 allen 133 Kommunen im Land Sachsen-Anhalt offen.[21] In Zusammenarbeit mit dem BSI, der KITU und einem Beratungsunternehmen werden Landkreise, Städte und Gemeinden beim Aufbau eines Informationssicherheitsmanagementsystems unterstützt. Die Investition in Unterstützungsleistungen wird vollständig vom Land getragen.

Zusätzlich unterstützen die „Digital-Lotsen“ der KITU die Kommunen und Landkreise individuell bei Digitalisierungs- und Sicherheitsprojekten.[22]

4.5 Sensibilisierung, Schulung und digitale Kompetenzen

Cybersicherheit beginnt bei jedem Einzelnen. Technische Schutzmaßnahmen können ihre Wirkung nur entfalten, wenn die Nutzenden für Gefahren sensibilisiert und in sicherem Verhalten geschult sind. Als Land verfolgen wir deshalb einen umfassenden Ansatz, der alle Lebensbereiche und Altersgruppen adressiert.

Verwaltung und Fachbehörden: Das für Informationssicherheit zuständige Ministerium hat ein landesweites Fortbildungsprogramm für die Beschäftigten der unmittelbaren Landesverwaltung zur Informationssicherheit entwickelt.[23] Seit 2024 werden Fortbildungen dezentral an verschiedenen Standorten und online in Zusammenarbeit mit dem Aus- und Fortbildungsinstitut Sachsen-Anhalt angeboten. Zur Gewährleistung der Nachhaltigkeit und Erfüllung kommender Kompetenznachweispflichten ist grundsätzlich vorgesehen, die Fortbildungen mit einer Zertifizierungsprüfung und ggf. Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik abzuschließen.

Schulische und außerschulische Bildung: Seit 2024 ist Informatik Pflichtfach an allen Sekundar- und Gemeinschaftsschulen Sachsen-Anhalts; an Gymnasien ist sie in den Klassen fünf bis acht im Themenkomplex „Lernen in der digitalen Welt“ verankert. Lehrkräfte werden sowohl durch bundesweite Projekte wie „DigiBitS“[24] und das „Internet-ABC“[25] als auch durch landeseigene Projekte wie „Digitalassistenz“[26] und medienpädagogische Beratung im Medienkompetenzzentrum fortlaufend weitergebildet. Die Medienmobile[27] und das Medienscout-Programm zur Fortbildung von Peer-Coaches[28] befähigen Schülerinnen und Schüler zum sicheren Umgang mit digitalen Medien.

20 Anforderungen an die Sicherheit für Lieferketten gemäß den aktuellen Grundschutz-Praktiken des BSI, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-lieferkette_grundschutz-checkliste.html (abgerufen am 29.04.2026).
21 SicherKOMMUNAL, https://www.kommunales-sachsen-anhalt.de/media/custom/2348_30852_1.PDF?1764687662 (abgerufen am 29.04.2026).
22 Digital-Lotsen Sachsen-Anhalt, https://www.kitu-genossenschaft.de/Digital-Lotsen/ (abgerufen am 29.04.2026).
23 Fortbildungsportfolio Informationssicherheit 2026 des CISO, https://mid.sachsen-anhalt.de/digitales/informationssicherheit/fortbildungen-im-bereich-informationssicherheit-ministerium-fuer-infrastruktur-und-digitales (abgerufen am 29.04.2026).
24 DigiBitS, https://www.digibits.de/ (abgerufen am 29.04.2026).
25 Internet-ABC, https://www.internet-abc.de/ (abgerufen am 29.04.2026).
26 Digitalassistenz, https://www.bildung-lsa.de/informationsportal/schule/schulentwicklung/digitalassistenz.htm (abgerufen am 29.04.2026).
27 Medienmobile, https://medienanstalt-sachsen-anhalt.de/medienkompetenz/medienmobile/index.html (abgerufen am 29.04.2026).
28 Medienscouts, https://www.bildung-lsa.de/informationsportal/schule/schulentwicklung/medienscouts.htm (abgerufen am 29.04.2026).

Gesellschaft und Verbraucherschutz: Die Verbraucherzentrale Sachsen-Anhalt (VZSA) berät zu digitalen Rechtsfragen[29], während das Medienkompetenzzentrum[30] der Medienanstalt Sachsen-Anhalt niedrigschwellige Kursangebote für Erwachsene, Kinder und Jugendliche bereithält und über seine Netzwerkstelle „Medienkompetenz" medienpädagogische Akteure im Land miteinander vernetzt. Die Volkshochschulen (VHS) ergänzen dieses Angebot als Kompetenzzentren der digitalen Grund- und Fortbildung.[31] Die Förderung von zielgruppenspezifischen Angeboten wie jenen unter dem Schirm „DigitalPakt Alter" für die Generation 65+[32] oder die digitale Befähigung von ehrenamtlichen Strukturen durch das Programm „Engagement digital"[33] trägt ebenfalls zu einer Kompetenzförderung bei. Regelmäßige Kampagnen wie der Tag der Medienkompetenz[34] oder der Safer Internet Day[35] runden das Gesamtangebot ab und sorgen für eine breitere öffentliche Aufmerksamkeit für die Themen Cybersicherheit und Medienkompetenz im Land.

4.6 Risikomanagement

Weder beim Betrieb zentraler IT-Infrastrukturen noch bei fachbereichsspezifischen Anwendungssystemen kann ein lückenloser präventiver Schutz vor Bedrohungen der Verfügbarkeit, Integrität oder Vertraulichkeit von Daten und Systemen vollumfänglich garantiert werden. Da sowohl finanzielle Rahmenbedingungen als auch unvermeidbare technische Restrisiken berücksichtigt werden müssen, bedarf es eines methodisch fundierten Risikomanagementansatzes, um die Mitigation von Risiken bestmöglich zu gewährleisten.

Als Land setzen wir dabei auf die etablierten Verfahren des Risikomanagements gemäß BSI-Standard 200-3.[36] Prozesse zur Risikobehandlung unter Berücksichtigung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmaßes werden systematisch eingeführt und weiterentwickelt. Die regelmäßige Evaluierung gewährleistet zudem, dass auf veränderte oder neu entstehende Bedrohungslagen zeitnah reagiert werden kann.

4.7 Notfallmanagement und Business Continuity Management

Als übergreifendes Steuerungsinstrument schafft das Notfallmanagement und *Business Continuity Management* (BCM) den Rahmen, innerhalb dessen sowohl Notfall- als auch Krisensituationen gehandhabt werden. Dabei steht an erster Stelle, die Widerstandsfähigkeit des laufenden Betriebs zu stärken, die Wiederherstellung der Betriebsbereitschaft zu systematisieren und Folgeschäden zu begrenzen, die beispielsweise aus gezielten Angriffen auf die IT-Infrastruktur resultieren können. Deshalb fördern wir die Umsetzung des BCM-Modells nach BSI-Standard 200-4[37] in Landesverwaltung und Kommunen. Das Projekt „SicherKOMMUNAL" unterstützt etwa kommunale Stellen bei der Etablierung durch Fortbildungen und Beratung.[38]

Das CERT Nord steht in IT-Notfällen als Ansprechpartner, Koordinator und Vorfallbearbeiter bereit. Das Land hält Ersatztechnik vor, die bei schwerwiegenden Vorfällen an betroffene Stellen ausgegeben werden kann, um die Funktionsfähigkeit in Krisensituationen zu sichern.

29 Rechtsberatung (Digitale Welt), https://www.verbraucherzentrale-sachsen-anhalt.de/digitale-welt/rechtsberatung-digitale-welt-114370 (abgerufen am 29.04.2026).
30 Medienkompetenzzentrum, https://medienanstalt-sachsen-anhalt.de/medienkompetenz/medienkompetenzzentrum/index.html (abgerufen am 29.04.2026).
31 Volkshochschule Sachsen-Anhalt, https://vhs-st.de/ (abgerufen am 29.04.2026).
32 Rolle des Landes Sachsen-Anhalt im Digitalpakt Alter, https://www.digitalpakt-alter.de/partner/sachsen-anhalt/ (abgerufen am 29.04.2026).
33 Engagement Digital, https://www.lagfa-lsa.de/engagement-digital (abgerufen am 29.04.2026).
34 Medienkompetenztag, https://medienkompetenztag.de/ (abgerufen am 29.04.2026).
35 Safer Internet Day 2026, https://medienanstalt-sachsen-anhalt.de/infothek/pressemitteilungen/safer-internet-day-2026-digitale-medien-im-familienalltag501.html (abgerufen am 29.04.2026).
36 BSI-Standard 200-3 (Risikomanagement), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html (abgerufen am 29.04.2026).
37 BSI-Standard 200-4 (Business Continuity Management), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html (abgerufen am 29.04.2026).
38 SicherKOMMUNAL, https://www.kommunales-sachsen-anhalt.de/media/custom/2348_30852_1.PDF?1764687662 (abgerufen am 29.04.2026).

4.8 Gefahrenabwehr und Strafverfolgung

Die fortschreitende Digitalisierung hat die Bedrohungslandschaft für Gefahrenabwehr- und Strafverfolgungsbehörden grundlegend verändert. Die Herausforderungen im Cyberraum zeichnen sich durch ihre grenzüberschreitende Natur, die Geschwindigkeit der Angriffe und die Komplexität der Methoden aus.

Die *Zentrale Ansprechstelle Cybercrime (ZAC)* der Polizei Sachsen-Anhalt fungiert als Schnittstelle zwischen Sicherheitsbehörden und Wirtschaft. Sie bietet bei Cyberangriffen schnelle Unterstützung, vermittelt Kontakte zu spezialisierten Ermittlungsbehörden und leistet einen wichtigen Beitrag zur Prävention durch Informationsveranstaltungen. Das *Cybercrime Competence Center (4C)* im Landeskriminalamt bündelt die kriminalpolizeiliche Expertise bei der Bekämpfung von Cyberkriminalität.

Innerhalb der Staatsanwaltschaften des Landes haben spezialisierte Sonderdezernate mit dem Schwerpunkt Cybercrime besondere Fachkompetenz bei der Verfolgung digitaler Straftaten aufgebaut. Ergänzend dazu errichtete die Staatsanwaltschaft Halle im Jahr 2023 die Zentralstelle zur Bekämpfung von Hasskriminalität im Internet, die eine gebündelte und einheitliche Bearbeitung entsprechender Verfahren durch eigens ausgebildete Experten ermöglicht.

Der Verfassungsschutz des Landes Sachsen-Anhalt unterstützt Unternehmen präventiv im Wirtschaftsschutz und in der Spionageabwehr.[39] Durch Formate wie den Wirtschaftsschutztag und die Sensibilisierung und Beratung, auch in Kooperation mit den Industrie- und Handelskammern (IHK), werden Unternehmen bei der Identifizierung und Bewertung von Schwachstellen unterstützt. Bei konkreten Gefährdungshinweisen geht der Verfassungsschutz aktiv auf betroffene Akteure zu.

Für eine wirksame Cyberkriminalitätsbekämpfung sind regelmäßige Evaluierungen, systematische Bedrohungsanalysen und umfassende Lagebilder entscheidend. Das CERT Nord erstellt sowohl vorfallspezifische als auch ganzheitliche Lagebilder für das Land Sachsen-Anhalt, die eine fundierte strategische Planung ermöglichen.

4.9 Wirtschaft und Schutz Kritischer Infrastrukturen

Die Auswirkungen von Cyberangriffen auf Unternehmen (und insbesondere auf Betreiber Kritischer Infrastrukturen) können gravierend sein. Wir setzen auf eine enge Zusammenarbeit von Wirtschaft, Forschung und Staat, um die Funktions- und Leistungsfähigkeit der Wirtschaft und vor allem der kritischen Einrichtungen (KRITIS) zu schützen.

Besonderes Augenmerk liegt auf kleinen und mittleren Unternehmen (KMU), denen häufig die Kapazitäten für ein eigenständiges hohes Cybersicherheitsniveau fehlen. Deswegen unterstützen wir Verbände und Kammern hinsichtlich der Schaffung gezielter Beratungs- und Präventionsangebote. Informationen und Sensibilisierungen des Verfassungsschutzes (Wirtschaftsschutz) für Unternehmen, Kammern und Verbände tragen dazu bei, aktuelle Überblicke über Bedrohungslagen zu gewinnen und Awareness und Resilienz zu verbessern.

Das Zukunftszentrum Digitale Arbeit Sachsen-Anhalt dient als Service- und Beratungsplattform und erleichtert über den inhärenten Förderkompass die Suche nach passenden Förderangeboten.

Mit den Programmen „DIGITAL INNOVATION“ und „Sachsen-Anhalt Digital“ fördern wir neben anderen Schwerpunkten die Entwicklung und Umsetzung von Cybersicherheitsprojekten auch finanziell. Über die Investitions- und Marketinggesellschaft Sachsen-Anhalt ist das Land Kooperationspartner des Cluster IT Mitteldeutschland e. V. und damit Teil eines starken regionalen Netzwerks.

39 Verfassungsschutzbericht Sachsen-Anhalt 2024, S. 166–168, https://mi.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MI/MI/3._Themen/Verfassungsschutz/Referat_44/VSB_2024_Druckfassung.pdf (abgerufen am 29.04.2026).

4.10 Fachkräftegewinnung und -entwicklung

Mit dem Fortschreiten der Digitalisierung, auch in der Verwaltung, steigt der Bedarf an qualifizierten Fachkräften im Bereich Cybersicherheit und erfordert zudem gezielte Maßnahmen entlang des gesamten Bildungs- und Berufswegs. Wir fördern deshalb lebenslanges Lernen und die Abstimmung zwischen den verschiedenen Lernphasen. Dazu bündelt der „Fachkräftesicherungspakt Sachsen-Anhalt“ die Anstrengungen von Kammern, Arbeitgeberverbänden, Gewerkschaften, Hochschulen und der Bundesagentur für Arbeit.[40]

An den Hochschulen des Landes steht ein breites Studienangebot im Bereich Informatik und Cybersicherheit bereit, das stetig weiterentwickelt wird. Der duale Studiengang „Verwaltungsdigitalisierung und -informatik“ an der Hochschule Harz verbindet etwa Cybersicherheits-Know-how mit Verwaltungswissenschaften. Das Programm „FEM POWER“[41] fördert gezielt den Einstieg von Frauen in MINT-Disziplinen (Mathematik, Informatik, Naturwissenschaften und Technik).

Förderung in der allgemeinen Weiterbildung, auch im Bereich der Cybersicherheit, wird durch das Programm „Sachsen-Anhalt WEITERBILDUNG“[42] systematisch gestärkt. Zum Ausbau der Standortattraktivität setzen wir auf die Initiative „Fachkraft im Fokus“[43] und das *WelcomeCenter Sachsen-Anhalt*[44]. Die Ansiedlung der *Agentur für Innovation in der Cybersicherheit* (Cyberagentur) in Halle (Saale) festigt ebenfalls Sachsen-Anhalts Position als Innovationsstandort und schafft neue Stellen für hochspezialisiertes Personal in der Technologieforschung.[45]

4.11 Innovative Forschung und Entwicklung

Die bestehende Förderung von Forschung und Entwicklung im Bereich der Cybersicherheit bildet die Grundlage für technologischen Vorsprung und langfristige Wettbewerbsfähigkeit auf Landes-, Bundes- und EU-Ebene. Ziel ist es, neben der universitären Forschung auch Innovationen aus dem außeruniversitären Bereich zu unterstützen und Forschungsergebnisse zügig in die praktische Anwendung zu überführen. Hierfür werden auch der Auf- und Ausbau von Verbünden, Netzwerken und Clustern zum Austausch von Trends und Strategien sowie deren Integration in ein umfassendes Innovations-Ökosystem gefördert.

Besonders hervorzuheben ist in diesem Zusammenhang der CyberSecurity-Verbund Sachsen-Anhalt II – ein Gemeinschaftsprojekt der Hochschule Harz, der Martin-Luther-Universität Halle und der Otto-von-Guericke-Universität Magdeburg.[46] Das Projekt verfolgt das Ziel, die Innovationskraft in Wirtschaft, Verwaltung und Bildungswesen gemäß den Vorgaben der Regionalen Innovationsstrategie Sachsen-Anhalt zu stärken, insbesondere bei kleinen und mittelständischen Unternehmen. Im Rahmen des Projekts sollen Lösungen in den Bereichen Digitalisierung, IT-Sicherheit und Vertrauen erforscht, entwickelt und demonstriert werden, wobei auch die Qualifizierung von Fachkräften im Fokus steht. Die Forschung konzentriert sich auf neue Sicherheitsverfahren und Vertrauensmechanismen für Anwendungen und Infrastrukturen mit hohem Sicherheitsniveau, insbesondere unter Berücksichtigung von Regulierungen und Innovationen zur erhöhten Sicherheit, wie eIDAS2.0/EUDI-Wallet, NIS2, OZG, RegMod und SDG. Unterstützt wird das Projekt durch weitere Netzwerke wie das Cluster IT Mitteldeutschland, den Bundesverband IT-Sicherheit TeleTrust, die Cyberagentur des Bundes sowie wissenschaftliche Kooperationen in Deutschland und der EU.[47]

40 Fachkräftesicherungspakt Sachsen-Anhalt, https://ms.sachsen-anhalt.de/themen/arbeit/fachkraeftesicherungspakt (abgerufen am 29.04.2026).
41 FEM POWER, https://www.fempower-lsa.de/ (abgerufen am 29.04.2026).
42 Förderprogramm „Sachsen-Anhalt WEITERBILDUNG“, https://www.foerderdatenbank.de/FDB/Content/DE/Foerderprogramm/Land/Sachsen-Anhalt/individuelle-berufliche-weiterbildung.html (abgerufen am 29.04.2026).
43 Fachkraft im Fokus, https://www.fachkraft-im-fokus.de/ (abgerufen am 29.04.2026).
44 WelcomeCenter Sachsen-Anhalt, https://www.welcomecenter-sachsen-anhalt.de/ (abgerufen am 29.04.2026).
45 Cyberagentur, https://www.cyberagentur.de/ (abgerufen am 29.04.2026).
46 CyberSecurity Verbund Sachsen-Anhalt, https://cslsa.de/ (abgerufen am 29.04.2026).
47 https://cybersec.hs-harz.de/ (abgerufen am 17.04.2026).

Mit der Cyberagentur in Halle, dem Technologiepark Weinberg Campus und den Förderprogrammen „DIGITAL INNOVATION“ und „Sachsen-Anhalt Digital“ unterstützen wir als Land gezielt Start-ups und KMU als Treiber des Wissenstransfers, unter anderem im Bereich der Cybersicherheit.

4.12 Nationale und regionale Kooperationen

Regionale und nationale Kooperationen sind für eine wirksame Cybersicherheitsstrategie von zentraler Bedeutung. Das Land Sachsen-Anhalt ist daher in die wesentlichen Kooperationsstrukturen des Bundes eingebunden:

- Arbeitsgemeinschaft Informationssicherheit (AG InfoSic) des IT-Planungsrates
- Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz (LAG-Cybersicherheit)
- Verwaltungs-CERT-Verbund (VCV) als Austauschplattform der CERTs von Bund und Ländern
- Direkte Kooperationsvereinbarung mit dem BSI (seit November 2023)[48]
- Gemeinsames Extremismus- und Terrorismusabwehrzentrum (GETZ)
- Direkte Mitwirkung an nationaler und EU-Gesetzgebung durch Vertretung im Bundesrat

Die Kooperation mit dem BSI umfasst eine intensivierte Zusammenarbeit in der Cyberabwehr, die gemeinsame Vorhaben, Wissensaustausch und verstärkte gegenseitige Unterstützung in den Fokus nimmt.
Der Mehrwert übergreifender Kooperation wird in verschiedenen Dimensionen deutlich: Gemeinsame Bedrohungsabwehr durch den Austausch aktueller Bedrohungsinformationen, Standardisierung und Effizienz durch einheitliche Verfahren, Wissensaustausch und Kompetenzaufbau durch gemeinsame Fortbildungen und Übungen sowie Interoperabilität und Rechtssicherheit durch abgestimmte Regelungen für die sichere länderübergreifende Kommunikation.

48 Pressemitteilung zur Kooperationsvereinbarung vom 19.10.2023, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/231019_Kooperation_Sachsen-Anhalt.html (abgerufen am 29.04.2026).

5. Fazit und Ausblick

Die Umsetzung der Cybersicherheitsstrategie des Landes Sachsen-Anhalt ist eine andauernde Aufgabe, die ein ebenso beständiges wie lernfähiges Engagement aller Beteiligten erfordert – in der Landesverwaltung, in den Kommunen, in der Wirtschaft und in der Gesellschaft. Die vorliegende Strategie benennt die Handlungsfelder, innerhalb derer das Land Sachsen-Anhalt dieses Engagement strukturiert und zielgerichtet entfalten möchte.

Als lebendiges Instrument erfüllt die Strategie damit zwei Funktionen: Sie stellt den aktuellen Entwicklungsstand unseres strategischen Rahmens dar und gibt zudem die Richtung vor, in die wir uns als Land entwickeln wollen. Aufgrund der sich stetig verändernden Bedrohungslage müssen die enthaltenen Maßnahmen regelmäßig anhand der aktuellen Gegebenheiten geprüft und gegebenenfalls angepasst werden. Diese Überprüfung ist als fester Bestandteil im Strategierahmen verankert. Damit ist spätestens in fünf Jahren eine vollständige Revision der Strategie geplant. Die notwendige Transparenz gegenüber Politik, Verwaltung und Öffentlichkeit wird durch die begleitende Kommunikation sichergestellt.

Denn Cybersicherheit gelingt nur mit gemeinsamer Anstrengung. Nicht durch Zufall setzen die beschriebenen Handlungsfelder deshalb auf Zusammenarbeit zwischen Behörden, Ebenen und Akteuren. Auch wenn das Land Sachsen-Anhalt in der Verantwortung steht, eine sichere digitale Basis für das staatliche Handeln und das Zusammenleben im Land zu schaffen, so kann nur durch das Engagement von allen Akteuren eine Gesamtresilienz gegenüber den analogen und digitalen Herausforderungen des 21. Jahrhunderts geschaffen werden. Als Land Sachsen-Anhalt freuen wir uns, diesen Weg mit unserer Bevölkerung zu gehen.

Begriffsverzeichnis

Begriff	Erklärung
Business Continuity Management (BCM)	Alle Maßnahmen einer Organisation, um den Betrieb auch in Krisenzeiten aufrechtzuerhalten. Konkret bedeutet dies: Notfallpläne erstellen, Ausweichsysteme vorhalten und regelmäßig einüben, was passiert, wenn IT-Systeme ausfallen oder Gebäude nicht zugänglich sind.
Computer Emergency Response Team (CERT) / Computer Security Incident Response Team (CSIRT)	Ein Computer-Notfallteam, das rund um die Uhr erreichbar ist und bei Sicherheitsvorfällen schnell eingreift. Vergleichbar mit einer Feuerwehr für digitale Notfälle: Es analysiert Angriffe, koordiniert Gegenmaßnahmen und gibt Warnungen an betroffene Stellen weiter.
Cyberkriminalität	Straftaten, die mithilfe von Computern oder dem Internet begangen werden. Dazu gehören etwa der Betrug durch gefälschte E-Mails (Phishing), das Eindringen in fremde Computersysteme (Hacking), das Verbreiten von Schadsoftware oder die Erpressung durch Datenverschlüsselung (Ransomware).
Cyberresilienz	Die Fähigkeit, Cyberangriffe nicht nur abzuwehren, sondern sich nach einem Angriff schnell zu erholen.
Cybersicherheit	Der Schutz digitaler Systeme, Netzwerke und Daten vor Angriffen aus dem Internet. Der Begriff betont die Abwehr externer Bedrohungen im vernetzten Raum.
Digitale Souveränität	Die Fähigkeit, digitale Aufgaben dauerhaft rechtssicher, technisch sinnvoll und wirtschaftlich effizient erfüllen zu können, ohne irreversibel von einzelnen Anbietern, proprietären Technologien oder fremden Rechts- und Kontrollräumen abhängig zu werden, weil Wechsel-, Prüf- und Steuerungsfähigkeit über Systeme, Daten und Betriebsmodelle jederzeit gewährleistet sind.
Indicators of Compromise	Digitale Spuren oder Artefakte, etwa auffällige IP-Adressen, Datei-Hashes, Domainnamen oder Registry-Einträge, die auf eine vergangene oder laufende Kompromittierung eines IT-Systems hinweisen.
Informationssicherheit	Der Schutz von Informationen vor unbefugtem Zugriff, unerlaubter Veränderung oder unbeabsichtigtem Verlust – unabhängig davon, ob sie digital oder analog vorliegen.
Informationssicherheitsmanagementsystem (ISMS)	Ein systematischer Rahmen, bestehend aus Regeln, Prozessen und Verantwortlichkeiten, mit dem eine Behörde oder ein Unternehmen Informationssicherheit dauerhaft planen, umsetzen und verbessern kann – vergleichbar mit einem Qualitätsmanagementsystem, speziell angepasst bzgl. der Sicherheit von Daten und IT-Systemen.
IT-Grundschutz	Ein vom BSI entwickeltes Regelwerk, das Behörden und Unternehmen Schritt für Schritt beim Aufbau ihrer Informationssicherheit unterstützt. Es beinhaltet konkrete Checklisten und Empfehlungen für typische Sicherheitsprobleme.
IT-Sicherheit	Schutz informationstechnischer Systeme – also Hardware, Software und Daten – vor Ausfällen, Missbrauch und unberechtigtem Zugriff.

Begriff	Erklärung
Kritische Infrastrukturen (KRITIS)	Einrichtungen, deren Ausfall oder Beeinträchtigung weitreichende Folgen für Staat, Wirtschaft oder Gesellschaft hätte. Dazu zählen bspw. Energieversorger, Wasserwerke, Krankenhäuser, Banken, Verkehrsinfrastruktur und Behörden der öffentlichen Verwaltung.
Multi-Faktor-Authentifizierung	Ein Anmeldeverfahren, das mindestens zwei unabhängige Nachweise verlangt – etwa ein Passwort und einen Code auf dem Mobilgerät. Dadurch bleibt ein Konto auch dann geschützt, wenn das Passwort in fremde Hände gelangt.
Ransomware	Schadsoftware, die alle Dateien auf einem Computer verschlüsselt und unzugänglich macht. Die Angreifer verlangen danach ein Lösegeld (engl. “ransom”), um die Daten wieder freizugeben. Ransomware gehört zu den häufigsten und schädlichsten Bedrohungen für Behörden und Unternehmen.
Schwachstelle	Eine Sicherheitslücke in einem Programm oder System, die von Angreifern ausgenutzt werden kann. Vergleichbar mit einem defekten Schloss – solange es nicht durch ein Software-Update repariert wird, können Eindringlinge einbrechen.
Verwaltungs-CERT-Verbund	Ein Zusammenschluss der Computer Emergency Response Teams von Bund und Ländern unter Koordination des IT-Planungsrats. Die Mitglieder tauschen aktuelle Bedrohungsinformationen aus und stimmen ihre Reaktion auf Sicherheitsvorfälle ab, um ein einheitliches Schutzniveau in der öffentlichen Verwaltung zu gewährleisten.

Impressum

Herausgeben vom
Ministerium für Infrastruktur und Digitales
des Landes Sachsen-Anhalt
Turmschanzenstraße 30
39114 Magdeburg
Presse- und Öffentlichkeitsarbeit
E-Mail: presse-mid@sachsen-anhalt.de
mid.sachsen-anhalt.de

Federführung:
Ministerium für Infrastruktur und Digitales

Stand:
Juni 2026