Anhang I. Glossar

Begriff	Definition	Abkürzung
Advanced Persistent Threats	Ein Advanced Persistent Threat (APT) liegt dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter, Angreifender zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.	APT
Awareness	Awareness beschreibt ein Problembewusstsein und sicheres Verhalten. Im alltäglichen Umgang mit IT-Systemen ist Awareness eine elementare Sicherheitsmaßnahme. Das bedeutet zunächst, dass ein Problembewusstsein für Cybersicherheit geschaffen werden muss. Darauf aufbauend kann man eine Verhaltensänderung hin zu einem sicheren digitalen Umgang erreichen.	
Brandenburgischer IT-Dienstleiser	Der Brandenburgische IT-Dienstleister ist der zentrale IT-Dienstleister für die unmittelbare Landesverwaltung Brandenburg und steht für effizienten und professionellen IT-Service aus einer Hand. Zum umfangreichen Aufgabenportfolio des Brandenburgischen IT-Dienstleisters gehören u. a. die Planung, Steuerung sowie der Betrieb der technischen Infrastruktur der obersten Landesbehörden und ihrer nachgeordneten Behörden und Einrichtungen und die Verfahrensentwicklung, -pflege und -betreuung von Querschnittsverfahren und ressortübergreifender Fachverfahren.	ZIT BB
Brandenburgisches E-Government-Gesetz	Rechtsgrundlage für die Digitalisierung der Verwaltung im Land Brandenburg.	BbgEGovG
BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik	Im BSI-Gesetz werden die Aufgaben, Zuständigkeiten und Befugnisse des BSI geregelt. Zusätzlich werden im BSIG grundlegende Strukturen der deutschen Cybersicherheitsarchitektur auf Bundesebene, wie beispielsweise die Bund-Länder Zusammenarbeit, die Aufsicht über Kritische Infrastrukturen oder die Zertifizierung von IT-Komponenten geregelt.	BSIG
Bundesamt für Sicherheit in der Informationstechnik	Das Bundesamt für Sicherheit in der Informationstechnik ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.	BSI
Computer Emergency Response Team	Computer-Notfallteam, das aus IT-Spezialisten besteht. In vielen Unternehmen und Institutionen sind mittlerweile entsprechende Teams etabliert, die sich um die Abwehr von Cyberangriffen, die Reaktion auf IT-Sicherheitsvorfälle sowie um die Umsetzung präventiver Maßnahmen kümmern.	CERT

Cybersicherheit	Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.
Cybercrime-as-a-Service	Mit dem Konzept des „Cybercrime-as-a-Service“ agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen.
Cyberkriminalität	In Bezug auf Cyberkriminalität unterscheidet man zwischen „Cybercrime im engeren Sinne“ (Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten) und „Cybercrime im weiteren Sinne“ (Straftaten, die mittels Informationstechnik begangen werden). Cybercrime im weiteren Sinne stellt also, vereinfacht gesagt, Taten dar, die auch in der analogen Welt begangen werden können. Cybercrime im engeren Sinne sind hochtechnische Straftaten, die ebensolche hochtechnische Ermittlungsarbeit auf Seiten der Polizei erfordern.
Cyberraum	Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten beziehungsweise vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.
Cybersabotage	Cybersabotage beschreibt Cyberoperationen, die zur Sabotage, also zum Stören von Abläufen, genutzt werden.
Cybersecurity Navigator	Ein Tool, das eine Datenbank aus Tausenden einschlägigen Rechtsvorschriften und korrespondierenden technischen Standards enthält, und auf diese Weise umfassend zur unternehmerischen IT-Compliance beiträgt.
Cybersicherheitsarchitektur	Gesamtheit der staatlichen Akteure – Behörden, Plattformen, Organisationen usw. –, die gemäß der Definition von Cybersicherheit Teil des nationalen Ökosystems sind.
Cybersicherheitsquote	Ein Anteil des Gesamtbudgets einer öffentlichen Projektausschreibung (z. B. 10 %), der für Cybersicherheit verwendet werden muss.
Cyberspionage und -sabotage	Cyberoperationen können zur Spionage, also zum Ausspähen von Daten genutzt werden.
Digitale Souveränität	Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.
Digitalisierung	Digitalisierung bedeutet die Verwendung von Daten und algorithmischen Systemen für neue oder verbesserte Prozesse, Produkte und Geschäftsmodelle.

Distributed Denial of Service	Bei einem Distributed Denial of Service wird ein Server gezielt mit so vielen Anfragen bombardiert, dass er die Menge der Anfragen nicht mehr bewältigen kann und den Dienst verweigert bzw. im schlimmsten Fall zusammenbricht.	DDoS
E-Government	Der englische Begriff E-Government (Elektronische Verwaltung) meint das Dienstleistungsangebot der öffentlichen Verwaltung im Internet, das es den Kundinnen und Kunden der Verwaltung erlauben soll, Behördengänge so weit wie möglich elektronisch abzuwickeln.	
Endogene oder exogene Schocks	Begriffe, die ursprünglich aus der Volks-/bzw. Politikwissenschaft stammen und erhebliche Veränderungen des Status Quo in Folge spezifischer Ereignisse beschreiben. Endogene Schocks haben ihren Ursprung innerhalb der betroffenen Organisation, während exogene Schocks von außen auf diese einwirken.	
EU Critical Entities Resilience Directive (CER-Richtlinie)	Die 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 – sog. CER-Richtlinie verpflichtet Mitgliedstaaten der EU, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotage zu stärken.	CER-Richtlinie
Ganzheitliche Lagebilderstattung	Zielgruppenspezifische, sachliche und auf die wesentlichen Aspekte reduzierte Beschreibung einer vorliegenden Situation über einen klar definierten Zeitraum.	
Grundwerte der Informationssicherheit	Die klassischen Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Daten.	
Hacktivismus	Im Gegensatz zu vielen Bedrohungsakteuren, die ausschließlich ihren finanziellen Vorteil im Sinn haben, beteiligen sich Hacktivisten an störenden oder schädlichen Aktivitäten, um eine politische, soziale oder religiöse Sache zu unterstützen.	
Incident Response	Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren.	
Informationssicherheit	Informationssicherheit ist die Sicherung und Aufrechterhaltung der Verdaulichkeit, Integrität und Verfügbarkeit von Informationen.	

Informationstechnik	Informationstechnik umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.	IT
Informationstechnik-Notfallmanagement	Notfallmanagement in einer Behörde oder einem Unternehmen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Aufgaben eines Notfallmanagements sind daher, die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wiederaufgenommen werden können.	IT-Notfallmanagement
Informationstechnik-Leitstelle	Eine Leitstelle leitet den Einsatzbetrieb der zugeordneten Organisationen, nimmt Informationen entgegen, wertet sie aus und koordiniert die angeschlossenen Dienste.	IT-Leitstelle
Informationstechnik-Systeme	Technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.	IT-Systeme
IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“	Das IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ richtet sich an Kommunalverwaltungen, die einen systematischen Einstieg in die Informationssicherheit suchen. Es ermöglicht Kommunen eine zunächst breite, grundlegende Erst-Absicherung und erleichtert den Einstieg in die Informationssicherheit.	
Kommunale Arbeitsgemeinschaft „Technikunterstützte Informationsverarbeitung im Land Brandenburg	Die kommunale Arbeitsgemeinschaft „Technikunterstütze Informationsverarbeitung im Land Brandenburg“ ist ein gleichberechtigter Zusammenschluss von Ämtern, Gemeinden, Städten, Landkreisen sowie Verbänden, kommunalen Studieninstituten und Planungsgemeinschaften für interkommunale Zusammenarbeit. Dabei hat die TUIV-AG Brandenburg u. a. einen Fachausschuss für IT-Grundschutz und eine Projektgruppe für operative Cybersicherheit.	TUIV-AG
Kommunales Anwendungszentrum	Das Kommunale Anwendungszentrum des Brandenburgischen IT-Dienstleisters begleitet die Kommunen Brandenburgs aktiv auf dem Weg der Transformation zur elektronischen Verwaltung und ist Ansprechpartner für die Kommunen des Landes Brandenburg, wenn es um operative Unterstützungs- und Beratungsleistungen bei der Umsetzung des Onlinezugangsgesetzes und dem Brandenburgischen E-Government-Gesetz geht.	KAZ
Kritische Infrastrukturen	Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung	KRITIS

	nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.	
KRITIS-Dachgesetz	Das KRITIS-DG, das zum Zeitpunkt des Verfassens der vorliegenden Cybersicherheitsstrategie als Gesetzesentwurf vorliegt, ist das deutsche Umsetzungsgesetz der EU Critical Entities Resilience Directive-Richtlinie und hat zum Ziel das physische Schutzniveau kritischer Infrastrukturen in Deutschland zu erhöhen. Es macht den KRITIS-Betreibern diverse Vorgaben zu Sicherheitsmaßnahmen, verfolgt einen „All-Gefahren-Ansatz“ und komplimentiert Vorgaben an die IT-Sicherheit aus der NIS-2-Richtlinie.	KRITIS-DG
Länder- und Ressortübergreifende Krisenmanagementübung	Die **L**änder- und Ressort**ü**bergreifende **K**risenmanagementübung ist eine intervallmäßig in Deutschland stattfindende Krisenübung für den Bevölkerungsschutz. Ziel der LÜKEX ist es, das gemeinsame Krisenmanagement von Bund und Ländern unter Einbeziehung der Hilfsorganisationen und KRITIS-Unternehmen auf strategischer Ebene zu verbessern.	LÜKEX
Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz	Länderarbeitsgruppe der Innenministerkonferenz zur Abstimmung der länderübergreifenden fachlichen Zusammenarbeit auf politischer Ebene.	LAG Cybersicherheit
Landesweiter Informationssicherheitsmanager	Der landesweite Informationssicherheitsmanager (oder die landesweite Infomationssicherheitsmanagerin) prüft die Wirksamkeit der Sicherheitsmaßnahmen in allen Behörden und schreibt zusammen mit dem ISMT die IT-Sicherheitsstandards des Landes Brandenburg.	
Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien	Die Leitlinie für Cybersicherheitsstrategien ist eine Empfehlung zum Aufbau und der Weiterentwicklung der Cybersicherheitsarchitektur in den Ländern und dient damit der Harmonisierung zwischen den Ländern.	Leitlinie der LAG Cybersicherheit
Mobile Incident Response Teams	Mobile Incident Response Teams sind spezialisierte Team, die die Bundesverwaltung und Betreiber Kritischer Infrastrukturen bei Vorfällen vor Ort bei der Vorfallbearbeitung unterstützen können.	MIRT
Nationale Sicherheitsstrategie	Ein sicherheitspolitisches Grundsatzdokument, welches insbesondere das Zusammenwirken aller relevanten Akteure, Mittel und Instrumente beschreibt, durch deren Ineinandergreifen die Sicherheit Deutschlands umfassend erhalten und gegen Bedrohungen von außen gestärkt wird.	
NIS-2-Richtlinie	Richtlinie 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 Nr. 910/2014 und der Richtlinie 2018/1972 sowie zur Aufhebung der Richtlinie 2016/1148, abgekürzt NIS-2-Richtlinie.	

	Sie weitet die Cybersicherheitsvorgaben aus der NIS-Richtlinie auf mehr Sektoren und mehr Unternehmen aus.	
NIS-2-Umsetzungs- und Cyberstärkungsgesetz	Das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) wird ab 2024 in Kraft treten. Es überführt die EU-weiten Mindeststandards für Cybersicherheit der EU-Direktive NIS2 in deutsche Regulierung.	NIS2UmsuCG (vorläufige Abkürzung)
Phishing	Phishing-Angriffe nutzen betrügerische E-Mails, Textnachrichten, Telefonanrufe oder Websites, um Menschen dazu zu verleiten, sensible Daten weiterzugeben, Malware herunterzuladen oder sich auf andere Weise der Cyberkriminalität auszusetzen.	
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „Ransom“) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.	
Resilienz	Resilienz ist die Fähigkeit einer Organisation, etwas abzufedern und sich in einer verändernden Umgebung anzupassen, um so ihre Ziele zu erreichen, zu überleben und zu gedeihen. Die Resilienz von IT-Systemen beschreibt die Widerstandskraft von IT-Systemen und beschreibt die Fähigkeit, nachteilige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die Cyber-Ressourcen nutzen oder durch sie ermöglicht werden, vorherzusehen, ihnen standzuhalten, sie wiederherzustellen und sich an sie anzupassen.	
Security-By-Design	Security by Design versteht sich als Integration von Sicherheitsaspekten in alle Phasen der Softwareentwicklung – von der Anforderungsanalyse, über die Durchführung von Tests bis hin zur Inbetriebnahme beim Endkunden.	
Spam	Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthalten Spam-Nachrichten jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder sie werden für Phishing-Angriffe genutzt.	
Supply-Chain-Angriffe	Anstatt Organisationen direkt anzugreifen, zielen Supply-Chain-Angriffe auf Anbieter, Lieferanten und damit auf die etablierten Lieferketten ab. Indem Produkte	

	bereits bei den Herstellern oder Drittanbietern kompromittiert werden, beschränkt sich der mögliche Schaden nicht nur auf das angegriffene Unternehmen selbst, sondern betrifft alle in der Wertschöpfungskette nachgelagerten Unternehmen.	
Threat Intelligence-Mechanismen	Threat Intelligence ist ein wesentlicher Bestandteil der Bedrohungslage und widmet sich den Angreifer-Gruppen im Cyberraum, ihrer strategischen Motivationslage, ihrer Relevanz für Deutschland und den von ihnen eingesetzten Angriffstechniken.	
Verschlüsselung	Prozess, bei dem eine Nachricht oder Information so kodiert wird, dass nur autorisierte Parteien darauf zugreifen können.	
Verwaltungs-CERT-Verbund	Gremium zur operativen Zusammenarbeit der Länder-CERTS sowie des CERTs des Bundes. Ermöglicht bundesweit effektiver und schneller auf IT-Angriffe reagieren zu können. Im VCV wurde, neben regelmäßigen Treffen und gemeinsamen Übungen, ebenfalls die gegenseitige Unterstützung bei IT-Sicherheitsvorfällen vereinbart.	VCV
Zentraler IT-Dienstleister der Justiz des Landes Brandenburg	Der Zentrale IT-Dienstleister der Justiz des Landes Brandenburg gewährleistet die zentrale IT-Organisation für die Justiz des Landes Brandenburg, welche die gesamte Informationstechnik von ca. 75 Behörden bzw. Gerichten betreut.	ZenIT
Zero Trust	Zero Trust beschreibt ein aus dem „Assume Breach“-Ansatz entwickeltes Architekturdesign-Paradigma, welches im Kern auf dem Prinzip der minimalen Rechte aller Entitäten in der Gesamtinfrastruktur basiert.	