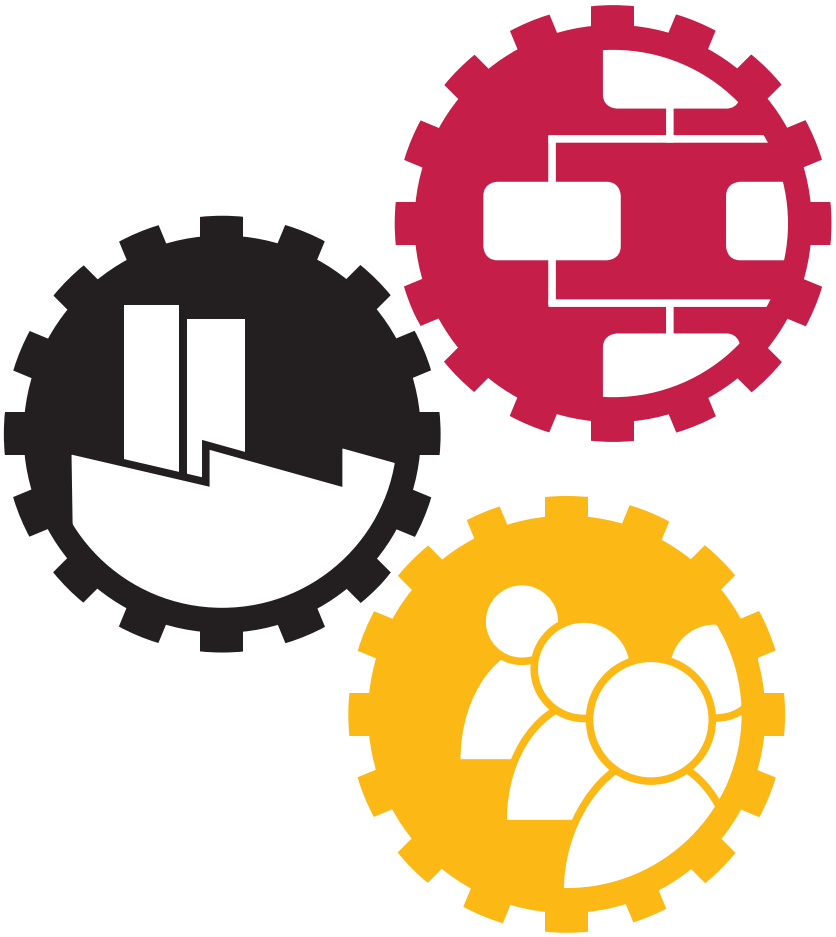
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Glossar



Alarmierung	Ziel der Alarmierung ist es, verantwortliche Entscheider und Akteure möglichst schnell nach Eintritt eines Schadensereignisses zu informieren und damit die Bewältigung des Notfalls oder der Krise einzuleiten.
Außenhaut	Außenhaut bezeichnet die äußere Umrandung eines Gebäudes. Die Außenhaut umfasst nicht nur Wände, sondern auch Glasflächen, Dächer, Schächte etc.
Ausweichstandort	Ein Ausweichstandort ist ein alternativer Standort, der genutzt werden kann, wenn der ursprüngliche Standort aufgrund von Ereignissen nicht mehr genutzt werden kann. Je nach gewünschter Bereitstellungszeit können hier z. B. die folgenden Kategorien unterschieden werden: • Heißer Standort (hot site): Der Standort wird kontinuierlich aktiv betrieben. Eine Aktivierung kann ohne zeitliche Verzögerung erfolgen. • Warmer Standort (warm site): Standort mit vorbereiteter Umgebung inklusive aller notwendigen Versorgungseinrichtungen. Eine Inbetriebnahme kann nach geringfügigen Anpassungen (z. B. Konfigurationen) erfolgen. • Kalter Standort (cold site): Standort erfüllt die Voraussetzung für einen Notbetrieb, ist jedoch noch nicht ohne weiterführende Maßnahmen (z. B. Installation) betriebsbereit.
Auswirkung/Impact	Gesamtheit des erwarteten Geschäftsverlusts, wenn eine Gefährdung oder ein sonstiges unerwünschtes Ereignis eintritt
BCM	Business Continuity Management ganzheitlicher Managementprozess zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Notfalls
Bedrohung	Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.
Befriedung	Befriedung bezeichnet die äußere Umrandung einer Fläche oder eines Grundstücks. Dies können z. B. Zäune, Mauern oder Schranken sein.

Behörden und Organisationen mit Sicherheitsaufgaben (BOS)	Staatliche (polizeiliche und nichtpolizeiliche) sowie nichtstaatliche Akteure, die spezifische Aufgaben zur Bewahrung und/oder Wiedererlangung der öffentlichen Sicherheit und Ordnung wahrnehmen. Konkret sind dies z. B. die Polizei, die Feuerwehr, das THW, die Katastrophenschutzbehörden der Länder oder die privaten Hilfsorganisationen, sofern sie im Bevölkerungsschutz mitwirken.
BIA	Business Impact Analyse, Folgeschädenabschätzung Analyse zur Ermittlung potentieller direkter und indirekter Folgeschäden für die Institution, die durch das Auftreten eines Notfalls oder einer Krise und den Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden
CERT	Computer Emergency Response Team spezielles Team von IT-Sicherheitsfachleuten, das bei der Lösung konkreter IT-Sicherheitsvorfälle als koordinierende Instanz mitwirkt, Warnungen vor IT-Sicherheitslücken herausgibt und Lösungsansätze anbietet (sogenannte Advisories)
Corporate Intelligence	methodische Vorgehensweise zur Beschaffung und Analyse fragmentierter Informationen und deren Transformation sowie von Verwertung als anwendbare Entscheidungsgrundlage für das Management der Institution Corporate Intelligence beschreibt den Transformationsprozess von Rohdaten in verwertbare Informationen sowie verwertbaren Informationen in Strategien zur Unterstützung konkreter Entscheidungen zur Umsetzung von Strategien, um damit die Performance und Betriebsfähigkeit der Institution zu verbessern.
Deeskalation	Deeskalation beschreibt die formale Beendigung des Vorfalls, die Rückkehr in den Normalbetrieb sowie damit verbunden die Übernahme des Betriebs durch die reguläre Organisationsstruktur.
Ereignis	Eintritt oder Veränderung einer bestimmten Kombination von Umständen
Eskalation	Eskalation beschreibt die Übergabe der Ereignisbewältigung an eine höhere bzw. zuständige Instanz innerhalb der definierten Bewältigungsorganisation. Beispiel: Nach Erreichen eines definierten Schwellenwerts wird ein Vorfall vom Vorfallmanagement an das Notfallmanagement übergeben.

Gefahr	„Gefahr“ wird oft als übergeordneter Begriff gesehen, wogegen unter „Gefährdung“ eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, „Gefahr“ und „Gefährdung“ als gleichbedeutend aufzufassen.
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.
Informationssicherheit	Informationssicherheit dient dem Schutz von Informationen hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität. Der Wirtschaftsgrundschutz befasst sich ausschließlich mit Aspekten der Sicherheit nicht elektronisch vorgehaltener Informationen. Aspekte des Schutzes von Informationen, die in IT-Systemen erfasst, gespeichert oder verarbeitet werden, sind somit nicht Bestandteil des Wirtschaftsgrundschutzes. Hierfür steht mit dem BSI IT-Grundschutz ein spezialisierter Standard zur Verfügung.
Institution	Der Begriff „Institution“ wird im Wirtschaftsgrundschutz als Oberbegriff für Behörden, Unternehmen und sonstige Organisationen verwendet.
Issue	Issues stellen eine Abweichung der Handlungen der Institution von der Erwartungshaltung ihrer Interesseneigner dar. Merkmale von Issues sind: • Konfliktpotential in Bezug auf mögliche Lösungen, Wertebezug oder Verteilung von Services • Einfluss auf Handlungsmöglichkeiten • Herstellung einer Beziehung zwischen Teilöffentlichkeiten und der Institution • Zusammenhang mit einem oder mehreren Ereignissen

Katastrophe	Eine Katastrophe ist ein Großschadensereignis, das zeitlich und örtlich kaum begrenzbar ist und großflächige Auswirkungen auf Menschen, Werte und Sachen hat oder haben kann. Die Existenz einer Institution oder das Leben und die Gesundheit von Personen sind gefährdet. Auch das öffentliche Leben wird stark beeinträchtigt. Eine Katastrophe wird durch die zuständige Institution in dem betroffenen Bundesland festgestellt und kann nicht ausschließlich durch eine Institution selbst behoben werden. Durch die geografische Ausbreitung und die Auswirkungen für die Bevölkerung sind insbesondere der Katastrophenschutz und das Zusammenwirken der verschiedenen Hilfsorganisationen gefordert. Aus Sicht der Institution stellt sich eine Katastrophe als eine Krise dar und wird intern durch das Krisenmanagement, ggf. in Zusammenarbeit mit den externen Hilfsorganisationen, bewältigt.
Kontrolle	Durchführung eines Vergleichs zwischen geplanten und realisierten Größen sowie Analyse der Abweichungsursachen Nicht eingeschlossen ist die Beseitigung der festgestellten Mängel. Kontrolle ist eine Form der Überwachung, durchgeführt von direkt oder indirekt in den Realisationsprozess einbezogenen Personen oder Organisationseinheiten.
KPI	Key Performance Indicator Kennzahlen, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich einer Zielsetzung gemessen werden kann
Krise	Unter einer Krise wird eine vom Normalzustand abweichende Situation verstanden, die trotz vorbeugender Maßnahmen in einer Institution jederzeit eintreten und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann. Das Krisenmanagement wird aktiv. Für die Bewältigung existieren keine Ablaufpläne, sondern lediglich Rahmenanweisungen und -bedingungen. Ein typisches Merkmal einer Krise ist die Einmaligkeit des Ereignisses. Notfälle, die die Kontinuität von Geschäftsprozessen beeinträchtigen, können eskalieren und sich zu einer Krise ausweiten. Als Krise wird bspw. die Gefährdung der Existenz der Institution oder des Lebens und der Gesundheit von Personen bezeichnet. Die Krise konzentriert sich auf die Institution und beeinträchtigt nicht breitflächig die Umgebung oder das öffentliche Leben. Sie kann, zumindest größtenteils, innerhalb der Institution selbst behoben werden. Es existiert jedoch eine Vielzahl von Krisen, die die Geschäftsprozesse nicht direkt betreffen. Beispiele hierfür sind Wirtschaftskrisen, Führungskrisen etc. Diese werden institutionsspezifisch ggf. auch mit anderen Strukturen behandelt.

Krisenmanagement	Gesamtheit aller konzeptionellen, organisatorischen und technischen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen Schadenssituation in den Normalzustand unterstützen Ziel ist, die Handlungs- und Entscheidungsfähigkeit der Institution sicherzustellen und eine zielgerichtete sowie koordinierte Bewältigung der Krise zu ermöglichen. Das Krisenmanagement ist für alle Arten von Krisen zuständig.
Krisenstab	Das zentrale Führungsgremium der Krisenbewältigung ist der Krisenstab. Analog zur Krise wird im Notfall der Notfallstab aktiviert. Der Krisenstab ist ein planendes, koordinierendes, informierendes, beratendes und unterstützendes Organ. Er stellt eine besondere temporäre Aufbauorganisation dar, die die normale Aufbauorganisation zur Bewältigung einer Krise außer Kraft setzt und abteilungsübergreifende Kompetenzen bündelt. Der Krisenstab funktioniert auf einer hierarchielosen Entscheidungsebene. Er plant, koordiniert, veranlasst und überwacht die Aktivitäten der Notfallbewältigung und steuert die Bereitstellung aller relevanten Informationen und Ressourcen zur Bewältigung des Schadenereignisses.
Kritikalität eines Geschäftsprozesses	skalierbare Wertung (Klassifizierung) von Geschäftsprozessen anhand ihrer Bedeutung für die Wertschöpfung einer Institution Die Klassifizierung erfolgt meist anhand der Wiederanlaufanforderung an den Geschäftsprozess oder des über die Dauer der Ausfallzeit zu erwartenden Schadens, kann jedoch durch weitere Kriterien ergänzt werden.
kritische Ressource	Ressource einer Institution, die bei Ausfall zur Unterbrechung bzw. zum Ausfall eines kritischen Geschäftsprozesses führt
kritischer Geschäftsprozess	Ein kritischer Geschäftsprozess ist ein wertschöpfender (Kern-)Prozess, der für die Aufrechterhaltung des Betriebs einer Institution essentiell notwendig ist. Kritische Geschäftsprozesse werden im Rahmen des Notfallmanagements besonders abgesichert. „Kritisch“ im Sinne des Notfallmanagements bedeutet „zeitkritisch“, also dass dieser Prozess eine schnellere Wiederaufnahme der Tätigkeit erfordert, da sonst ein hoher Schaden für die Institution zu erwarten ist.
Lagezentrum	Das Lagezentrum bildet die Schnittstelle zwischen den operativen Notfallteams und dem strategisch ausgerichteten Krisenstab. Das Lagezentrum ist die zentrale Sammelstelle für Informationen während einer Krise. Es gibt Informationen an den Krisenstab zur Entscheidung, die im nächsten Schritt an die einzelnen Fachabteilungen bzw. Notfallteams delegiert werden.

Notbetrieb	auf kritische Geschäftsprozesse reduzierter Alternativbetrieb mit vordefinierter Minimalfunktion bis zur Wiederherstellung des Normalbetriebs
Notfall	Ein Notfall ist ein Schadensereignis, bei dem Ressourcen der Institution nicht wie vorgesehen funktionieren oder bedroht werden. Die Sicherheitsanforderungen der entsprechenden Ressourcen können innerhalb einer geforderten Zeit nicht wiederhergestellt werden. Damit ist der Geschäftsbetrieb stark beeinträchtigt. Eventuell vorhandene Service Level Agreements (SLAs) können nicht eingehalten werden. Es drohen oder entstehen hohe bis sehr hohe Schäden, die sich signifikant und in einem nicht akzeptablen Rahmen auf das Gesamtjahresergebnis oder die Aufgabenerfüllung einer Institution auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallorganisation.
Notfallarbeitsplatz	Bei einem Notfallarbeitsplatz handelt es sich um einen alternativen Arbeitsplatz für den Fall, dass der ursprüngliche Arbeitsplatz aufgrund von Ereignissen nicht mehr genutzt werden kann.
Notfallhandbuch	Das Notfallhandbuch beinhaltet alle Informationen, die während der und für die Notfallbewältigung benötigt werden. Es umfasst somit alle Notfallpläne sowie die Wiederanlauf- und Wiederherstellungspläne.
Notfallkonzept	Das Notfallkonzept umfasst das Notfallvorsorgekonzept und das Notfallhandbuch.
Notfallmanagement	die koordinierten Tätigkeiten, die die Institution ausführt, um drohende oder bereits eingetretene Notfälle zu bewältigen Das Notfallmanagement geht über das Vorfallmanagement hinaus, es wird aber noch kein Krisenmanagement mit Stabsarbeit durchgeführt.
Notfallteam	Aufgabe der Notfallteams ist die operative Bewältigung des Notfalls. Sie leiten Informationen an das Lagezentrum weiter und bearbeiten eingehende Aufträge.
Notfallvorsorgekonzept	Das Notfallvorsorgekonzept beinhaltet alle bei der Konzeption des Notfallmanagements anfallenden Informationen, die nicht direkt für die Notfallbewältigung benötigt werden.

Organisationseinheit	logische Einheit einer Institution Dabei kann es sich beispielsweise um einen Standort, eine Abteilung, einen Fachbereich oder eine sonstige Einheit der Institutionsstruktur handeln.
personelle Sicherheit	Personelle Sicherheit beinhaltet alle Sicherheitsmaßnahmen zum Schutz vor Gefährdungen, die sich gegen das Personal (z.B. Mitarbeiter, Vertragspartner, Besucher) richten oder durch dieses herbeigeführt werden können. Daher umfasst diese Disziplin bspw. gleichermaßen Bewerber- und Integritätsprüfungen als auch Reisesicherheit und Veranstaltungsschutz.
physische Sicherheit	Physische Sicherheit beinhaltet den Schutz von Mitarbeitern, Immobilien und Wertgegenständen vor äußeren Gefahren und Ereignissen, die zu einem ernsthaften Verlust oder Schaden einer Institution führen können. Dies umfasst bspw. sowohl die Perimeter- und Außenhautsicherung als auch die Sicherheit der Arbeitsplätze in den Büroflächen. Die physische Sicherheit stellt somit einen essentiellen Bestandteil eines ganzheitlichen Sicherheitskonzepts dar.
Risiko	Auswirkung von Unsicherheit auf Ziele der Organisation (ISO 3100) Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird häufig auch als die Kombination aus der Wahrscheinlichkeit definiert, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.
Risikoappetit	Bereitschaft der Institution, Chancen wahrzunehmen und damit auch Risiken einzugehen
Risikobeurteilung	Gesamtprozess zur Identifizierung, Analyse und Bewertung von Risiken
Risikoexposition	Zustand, in dem Menschen, Sachen oder die Umwelt einer oder mehreren Gefahren ausgesetzt sind
Risikomanagement	koordinierte Aktivitäten, die darauf ausgerichtet sind, eine Institution bezüglich deren Risiken zu steuern und zu überwachen

Risikoprofil	Beschreibung und Struktur einer Anzahl von Risiken Die Anzahl von Risiken kann sich auf die ganze Institution, auf einen Teil davon, auf ein System oder auf eine andere Einheit beziehen.
Schadenspotential	Maß für die durch das Eintreten eines Ereignisses zu erwartenden Auswirkungen Die Ausprägung der Auswirkungen wird in einer Bewertungsskala ausgedrückt.
Schutz- bzw. Sicherheitszone	Die Planung von physischen Sicherheitsmaßnahmen sollte sich an dem Schutzbedarf der jeweiligen Räume und Bereiche orientieren. Mithilfe von Schutz- bzw. Sicherheitszonen können Bereiche mit vergleichbarem Schutzbedarf zusammengefasst werden. Beispielsweise werden Serverräume einer anderen Schutz- bzw. Sicherheitszone zugeordnet als Pausenräume, da hier andere Schutzmaßnahmen notwendig sind und ergriffen werden.
Sicherheitskonzept	Im Sicherheitskonzept werden die Erkenntnisse der Bedrohungs- und Sicherheitsrisikoanalyse dokumentiert und geeignete Maßnahmen beschrieben, die das angestrebte Schutzniveau ermöglichen sollen.
Sicherheitsniveau	das von der Institution festgelegte Level, ab dem ein Restrisiko vertretbar ist
Sicherheitsvorfall	Als Sicherheitsvorfall wird eine bestehende oder drohende Abweichung vom definierten Sicherheitsniveau der Werte der Institution bezeichnet, die durch menschliche oder technische Fehler, durch höhere Gewalt oder auch gezielt durch menschliches Handeln herbeigeführt wurde. Sicherheitsvorfälle sind damit besondere Vorfälle und stellen eine Abweichung vom regulären Geschäftsbetrieb dar. Beispiele: • Verlust vertraulicher Informationen • Bedrohung von Personen • Betrug von Mitarbeitern, Partnern oder Kunden Ein Sicherheitsvorfall kann sich durch seine Ausprägung und Art der Regelverletzung auch zu einem Notfall oder einer Krise entwickeln.
SLA	Service Level Agreement SLAs sind Dienstleistervereinbarungen. Diese umfassen eine Vereinbarung bzw. die Schnittstelle zwischen dem Auftraggeber und dem Dienstleister, wobei Regelungen bezüglich des Leistungsumfangs, der Reaktionszeit oder der Schnelligkeit der Bearbeitung festgelegt werden.

Sofortmaßnahmen	Sofortmaßnahmen beschreiben die Erstreaktion auf ein Ereignis, insbesondere Evakuierung, Retten und Löschen sowie ähnliche Reaktionsmaßnahmen.
Stabsarbeit	Stabsarbeit bezeichnet das standardisierte Zusammenwirken einer arbeitsteilig organisierten Personengruppe zum Zweck der Unterstützung und Beratung des verantwortlichen Leiters bei der Erledigung der Führungsaufgaben (z. B. im Krisenstab).
Stabsraum	Krisenstabsraum Räumlichkeiten, die dem Krisenstab als Arbeitsumgebung dienen und für die besondere Anforderungen bezüglich des Standorts und der Ausstattung gelten
Stakeholder/Interessengruppen	Personen oder Gruppen, die Interesse an der Organisation bzw. einem Ereignis haben oder davon betroffen sind Stakeholder können bspw. Mitarbeiter, Kunden, Lieferanten, Branchenverbände oder der Gesetzgeber sein.
Unfall	Ein Unfall ist ein plötzliches, zeitlich und örtlich bestimmbares und von außen einwirkendes Ereignis, bei dem ein Mitarbeiter oder Besucher unfreiwillig einen Körperschaden erleidet oder eine Ressource unbeabsichtigt beschädigt wird.
Vorfall	Ein Vorfall ist ein Ereignis, das störend oder schädigend auf Ressourcen der Institution wirkt. Der Schaden an den betroffenen Ressourcen ist als gering einzustufen. Ein „geringer“ Schaden ist bspw. ein Schaden, • der im Verhältnis zum Gesamtjahresergebnis oder zum Haushaltsvolumen zu vernachlässigen ist • der die Aufgabenerfüllung nur unwesentlich beeinträchtigt • bei dem Fehlverhalten einzelner in überschaubarem Maß vorliegt • der nur einzelne Mitarbeiter in einem geringen Maß schädigt • bei dem Ressourcen der Institution nicht wie vorgesehen funktionieren Vorfälle werden durch das in das allgemeine Tagesgeschäft integrierte Vorfallmanagement beseitigt. Vorfälle können sich jedoch zu einem Notfall ausweiten und sind deshalb genau zu beobachten, sorgfältig zu dokumentieren und zeitnah zu beheben. Dies ist jedoch nicht Teil des Notfallmanagements, sondern Aufgabe des Vorfallmanagements.

Vorfallmanagement	in der Regelorganisation verankerte Struktur, die dazu dient, Unfälle oder Vorfälle des jeweiligen Organisationsteils zu behandeln
Szenario	konkrete und bildhafte Darstellung eines Risikos, aus dem sich Gefahren für die Institution ergeben
Verwundbarkeit	Verletzlichkeit und Anfälligkeit von Menschen, Anlagen, Infrastruktur, Organisation, Informationen und Reputation gegenüber einer definierten Gefährdung
Wert	materielle und immaterielle Bedeutung einer Person, eines Objekts, des Vermögens, der Reputation und/oder von Informationen für die Institution
Wiederanlaufzeit (WAZ)	Zeitspanne von der Unterbrechung eines Prozesses bis zum Beginn des Notbetriebs
Wiederherstellungszeit (WHZ)	Zeitspanne von der Unterbrechung des Prozesses bis zum Start des Normalbetriebs Die Wiederherstellungszeit muss kleiner oder gleich der festgelegten Wiederanlaufzeit plus dem maximal tolerierbaren Notbetrieb sein (WHZ ≤ WAZ+MTN).
Zugang	Möglichkeit eines Zugriffs auf bzw. einer Nutzung von bspw. Anwendungen, Dokumenten, Informationen etc.
Zutritt	physischer Zutritt/das Betreten von Gebäuden oder Bereichen Der Zutritt kann bspw. durch Zutrittskontrollsysteme (über Schlüssel, Ausweise, PIN-Codes etc.) geregelt werden.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Druck
SunCopy GmbH, Berlin

Stand
August 2016

Auflage
1. Auflage