Begriffe

QUELLE: ISO/IEC 27000:2018 und ISO/IEC 29100:2011

Angriff

Erfolgreicher oder erfolgloser unbefugter Versuch, einen Wert zu zerstören, zu verändern, unbrauchbar zu machen, sich Zugang zu einem Wert zu verschaffen oder jeder Versuch, einen Wertpreiszugeben, zu stehlen oder unbefugt zu nutzen.

Aufzeichnung

Informationen, die von einer Organisation oder Person in Erfüllung rechtlicher Verpflichtungen oder im Rahmen der Geschäftsabwicklung als Beweismittel und als Wert erstellt, erhalten und aufbewahrt werden.

Auftragsdatenverarbeiter

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die personenbezogene Daten (pbD) im Namen und nach den Anweisungen einer verantwortlichen Stelle verarbeiten.

Authentisierung

Sicherstellung, dass die von einer Entität behaupteten Eigenschaften richtig sind .

Authentizität

Eigenschaft, dass eine Entität das ist, was sie angibt zu sein.

Bedrohung

mögliche Ursache eines unerwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation führen kann.

Benutzer

Interessierte Partei mit Zugang zu den Informationssystemen der Organisation. Beispiel: Personal, Kunden, Lieferanten.

Betroffene/r

Natürliche Person, auf die sich die personenbezogenen Daten (pbD) beziehen.

Datenschutz-Folgenabschätzung (DSFA)

Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung personenbezogener Daten, eingebettet in den unternehmensweiten Rahmen zum Risikomanagement.

Endpunktgerät

Netzwerkgebundenes Hardware-Gerät der Informations- und Kommunikationstechnologie (IKT) Anmerkung 1 zum Begriff: Endpunktgeräte können sich auf Desktop-Computer, Laptops, Smartphones, Tablets, Thin-Clients, Drucker oder andere Spezialhardware wie intelligente Zähler und IoT-Geräte (Internet der Dinge, en: Internet of Things) beziehen.

Endpunktgerät des Benutzers

Endpunktgerät , das von Benutzern für den Zugriff auf Informationsverarbeitungsdienste verwendet wird. Endpunktgeräte des Benutzers können sich auf Desktop-Computer, Laptops, Smartphones, Tablets, Thin-Clients usw. beziehen.

Entität

Begriff, der für den Betrieb einer Domäne relevant ist und erkennbar eine eigene Existenz hat. Eine Entität kann eine physische oder eine logische Ausführungsform haben. BEISPIEL Eine Person, eine Organisation, ein Gerät, eine Gruppe solcher Begriffe, ein menschlicher Teilnehmer an einem Telekommunikationsdienst, eine SIM-Karte, ein Reisepass, eine Netzwerkkarte, eine Softwareanwendung, ein Dienst oder eine Website.

Handhabung von Informationssicherheitsvorfällen

Ausübung einer konsistenten und wirksamen Herangehensweise für die Handhabung von

Informationssicherheitsvorfällen.

Informationssicherheitsereignis

Vorkommnisse, die auf eine mögliche Verletzung der Informationssicherheit oder ein Versagen der Maßnahmen hinweisen.

Informationssicherheitsvorfall

Ein oder mehrere zusammenhängende und identifizierte Informationssicherheitsereignisse, die den Werten einer Organisation schaden oder ihren Betrieb gefährden können.

Informationssicherheitsverletzung

Beeinträchtigung der Informationssicherheit, die zur unerwünschten Zerstörung, zum Verlust, zur Veränderung, zur Offenlegung von oder zum Zugriff auf geschützte Informationen bei deren Übertragung, Speicherung oder sonstiger Verarbeitung führt.

Informationssystem

Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten.

Informationsverarbeitende Einrichtung

jedes informationsverarbeitende System, jeder informationsverarbeitende Dienst oder jede informationsverarbeitende Infrastruktur oder der physische Standort, der diese beherbergt.

Interessierte Partei / Anspruchsgruppe

Person oder Organisation, die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann, oder die sich davon beeinflusst fühlen kann.

Kontrollkette

Nachweislicher Besitz, Bewegung, Handhabung und Verbleib von Material von einem Zeitpunkt bis zu einem anderen.

Nichtabstreitbarkeit

Fähigkeit, das Eintreten eines behaupteten Ereignisses oder einer behaupteten Handlung samt ihren ursächlichen Entitäten nachzuweisen.

Personal

Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten Der Begriff „Personal“ umfasst die Mitglieder der Organisation, z. B. das Steuerungsgremium, die oberste Leitung, die Beschäftigten, die Zeitarbeiter, die Auftragnehmer und die Freiwilligen.

Personenbezogene Daten (pbD)

Alle Daten bzw. Informationen, die (a) dazu verwendet werden können, eine Verbindung zwischen ihnen und der natürlichen Person, auf die sie sich beziehen, herzustellen, oder (b) direkt oder indirekt mit einer natürlichen Person verknüpft sind oder verknüpft werden können.

Politik

Absichten und Ausrichtung einer Organisation, wie von der obersten Leitung formell ausgedrückt.

Prozess

Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben verwendet oder umwandelt, um ein Ergebnis bereitzustellen.

Regel

Anerkannter Grundsatz oder Anweisung, der/die die Erwartungen der Organisation in Bezug auf das, was getan werden muss, erlaubt oder nicht erlaubt ist, festlegt. Regeln können in themenspezifischen Richtlinien und in anderen Arten von Dokumenten formell ausgedrückt werden.

Schwachstelle

Schwäche eines Wertes oder einer Maßnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann.

Sensible Informationen

Informationen, die vor Nichtverfügbarkeit, unbefugtem Zugriff, Veränderung oder öffentlicher Bekanntgabe geschützt werden müssen, weil sie potentiell nachteilige Auswirkungen auf eine Person, eine Organisation, die nationale Sicherheit oder den Schutz der Öffentlichkeit haben könnten.

Sicherheitsbereich

Sicherheitsbereiche (Domänen) sind ein Eigenschaften (Attribute), mit dem Maßnahmen aus der Perspektive von folgenden Informationssicherheitsdomänen betrachtet werden können:

- **Governance und Ökosystem**
  - Governance und Risikomanagement für die Sicherheit von Informationssystemen
  - Cybersicherheitsmanagement im Ökosystem
- **Schutz**
  - IT-Sicherheitsarchitektur
  - IT-Sicherheitsverwaltung
  - Identitäts- und Zugangssverwaltung
  - IT-Sicherheitswartung
  - physische und umgebungsbezogene Sicherheit
- **Verteidigung**
  - Erkennung
  - Management von Computersicherheitsvorfällen
- **Wiederstandsfähigkeit**
  - Betriebskontinuität
  - Krisenmanagement

Steuerung

Maßnahme, die das Risiko beibehält und/oder verändert

Statement of Applicability

Das Statement of Applicability (SoA) – die Erklärung zur Anwendbarkeit – ist das zentrale Dokument im Informationssicherheitsmanagement (ISMS) nach [ISO 27001](0.5.1, 0.5.5). Es verknüpft die identifizierten Sicherheitsrisiken mit den gewählten Maßnahmen (Controls) und begründet deren Umsetzung oder den Verzicht darauf.

Störung

Zwischenfall, ob vorhergesehen oder unvorhergesehen, der entsprechend den Zielsetzungen einer Organisation eine ungeplante, negative Abweichung von der erwarteten Lieferung von Produkten und Dienstleistungen verursacht.

Themenspezifische Richtlinie

Absichten und Ausrichtung zu einem bestimmten Subjekt oder Thema, wie sie von der zuständigen Managementebene formell zum Ausdruck gebracht wurden.

- Anmerkung 1 zum Begriff: Themenspezifische Richtlinien können formell Regeln oder Organisationsnormen ausdrücken.
- Einige Organisationen verwenden andere Ausdrücke für diese themenspezifischen Richtlinien.
- Die themenspezifischen Richtlinien, auf die in diesem Dokument Bezug genommen wird, beziehen sich auf die Informationssicherheit.

Verfahren

Festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen.

Vertrauliche Informationen

Informationen, die nicht dazu bestimmt sind, unbefugten Personen, Entitäten oder Prozessen zugänglich gemacht oder offengelegt zu werden

Werte

Alles, was für die Organisation von Bedeutung und/oder von Nutzen ist.

Primärwerte

- Informationen
- Geschäftsprozesse

Unterstützenden Werte

- Hardware
- Software
- Netzwerk
- Personal (verrichten unter Aufsicht der Organisation Tätigkeiten)
- Standort
- Struktur der Organisation

Wiederherstellungspunkt

Zeitpunkt, bis zu dem die Daten nach einer Störung wiederherzustellen sind.

Wiederherstellungsdauer

(RTO, en: recovery time objective) Zeitspanne, innerhalb derer ein Mindestmaß an Diensten und/oder Produkten sowie die unterstützenden Systeme, Anwendungen oder Funktionen nach einer Störung wiederherzustellen sind.

Zugangssteuerung

Mittel, um sicherzustellen, dass der physische und logische Zugang zu Werten aufgrund von Geschäfts- und Informationssicherheitsanforderungen befugt und eingeschränkt ist.

Zuverlässigkeit

Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen.