1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden ist oder aus anderen Gründen nicht erfolgt ist;
2. „berechtigte Zugangsnachfrager“
   a) das Bundesamt,
   b) die Landesbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben,
   c) Strafverfolgungsbehörden,
   d) die Polizeien des Bundes und der Länder und
   e) die Verfassungsschutzbehörden des Bundes und der Länder;
3. „Bodeninfrastruktur“ den Sektor Weltraum betreffende Einrichtungen, die der Kontrolle des Startes, Fluges oder der eventuellen Landung von Weltraumgegenständen dienen;
4. „Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind;
5. „Content Delivery Network“ oder „CDN“ eine Gruppe geographisch verteilter, zusammengeschalteter Server, mitsamt der hierfür erforderlichen Infrastruktur, die mit dem Internet verbunden sind, und der Bereitstellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern dienen, mit dem Ziel der Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung mit möglichst niedriger Latenz;
6. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, Abl. L 151 vom 7.6.2019, S. 15);
7. „Datenverkehr“ die mittels technischer Protokolle übertragenen Daten; es können Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten sein;
8. „DNS-Diensteanbieter“ eine natürliche oder juristische Person, die
   a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domain-Namen anbietet oder
   b) autoritative Dienste zur Auflösung von Domain-Namen zur Nutzung durch Dritte, mit Ausnahme von Root- Namenservern, anbietet;
9. „Domain-Name-Registry-Dienstleister“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, insbesondere Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;
10. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;
11. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der
    a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder

b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,

sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;

12. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen;

13. „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung;

14. „IKT-Dienst“ ein IKT-Dienst nach Artikel 2 Nummer 13 der Verordnung (EU) 2019/881;

15. „IKT-Produkt“ ein IKT-Produkt nach Artikel 2 Nummer 12 der Verordnung (EU) 2019/881;

16. „IKT-Prozess“ ein IKT-Prozess nach Artikel 2 Nummer 14 der Verordnung (EU) 2019/881;

17. „Informationssicherheit“ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;

18. „Informationstechnik“ ein technisches Mittel zur Verarbeitung von Informationen;

19. „Institutionen der Sozialen Sicherung“ Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch, die Deutsche Gesetzliche Unfallversicherung e.V. sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist;

20. „Internet Exchange Point“ oder „IXP“ eine Infrastruktur, die

    a) die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, die in erster Linie zum Austausch von Internet-Datenverkehr genutzt wird,

    b) nur der Zusammenschaltung autonomer Systeme dient und

    c) nicht voraussetzt, dass

        aa) der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft oder

        bb) den betreffenden Datenverkehr verändert oder diesen anderweitig beeinträchtigt;

21. „Kommunikationstechnik des Bundes“ Informationstechnik, die von einer oder mehreren Einrichtungen der Bundesverwaltung oder im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Einrichtung der Bundesverwaltung, der Einrichtungen der Bundesverwaltung untereinander oder der Einrichtungen der Bundesverwaltung mit Dritten dient; nicht als „Kommunikationstechnik des Bundes“ gelten die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird;

22. „kritische Anlage“ eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 56 Absatz 4 näher bestimmt;

23. „kritische Komponenten“ IKT-Produkte,

    a) die in kritischen Anlagen eingesetzt werden,

    b) bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und

c) die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift

aa) als kritische Komponenten bestimmt werden oder

bb) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren;

werden für einen der in Nummer 24 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, so gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieser Nummer;

24. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;

25. „Managed Security Service Provider“ oder „MSSP“ ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;

26. „Managed Service Provider“ oder „MSP“ ein Anbieter von Diensten im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne;

27. „NIS-2-Richtlinie“ die 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 (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (Abl. L 333 vom 27.12.2022, S. 80) in der jeweils geltenden Fassung;

28. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 BGB;

29. „Online-Suchmaschine“ ein digitaler Dienst nach Artikel 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (Abl. L 186 vom 11.7.2019, S. 57);

30. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;

31. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die

a) zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind und

b) unabhängig vom Inhalt des Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden;

Protokolldaten können Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten;

32. „Protokollierungsdaten“ Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme;

33. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (Abl. L 257 vom 28.8.2014, S. 73);

34. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter nach Artikel 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

35. „Rechenzentrumsdienst“ ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle;

36. „Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dazu dienen, unbefugt Daten zu nutzen oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken;

37. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, der Informationstechnik von Gruppen von Einrichtungen der Bundesverwaltung oder der Informationstechnik Dritter; nicht als Schnittstellen der Kommunikationstechnik des Bundes gelten die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Nummer 21 genannten Gerichte und Verfassungsorgane betrieben werden;

38. „Schwachstelle“ eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen;

39. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

    a) in informationstechnischen Systemen, Komponenten oder Prozessen oder

    b) bei der Anwendung informationstechnischer Systeme, Komponenten oder Prozesse;

40. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;

41. „Systeme zur Angriffserkennung“ durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme; wobei die Angriffserkennung durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgt;

42. „Top Level Domain Name Registry“ eine natürliche oder juristische Person, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top Level Domain (TLD) verwaltet und betreibt, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, unabhängig davon, ob der Betrieb durch die natürliche oder juristische Person selbst erfolgt oder ausgelagert wird; keine Top Level Domain Name Registry sind Register, die TLD-Namen nur für eigene Zwecke verwenden;

43. „Vertrauensdienst“ ein Vertrauensdienst nach Artikel 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;

44. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter nach Artikel 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;

45. „weltraumgestützte Dienste“ Dienste, die den Sektor Weltraum betreffen, die auf Daten und Informationen beruhen, die entweder von Weltraumgegenständen erzeugt oder über diese weitergegeben werden und deren Störung zu breiteren Kaskadeneffekten, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können, führen kann;

46. „Zertifizierung“ die Feststellung einer Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.