Mitteilung nach § 109 Absatz 5 Telekommunikationsgesetz

(Das Mitteilungsformular ist an die in der Fußzeile genannten Kontaktadressen zu senden)

1. Kontaktdaten

1.1. Meldendes Unternehmen

1.1.1. Name mit Rechtsform

1.1.2. Sitz des Unternehmens

PLZ:	Ort:	Straße, Hausnummer:

1.2. Ansprechpartner

Ansprechpartner für allgemeine Fragen:

Name:		E-Mail:
Festnetz:	Mobil:	Fax:

Ansprechpartner für technische Fragen:

Name:		E-Mail:
Festnetz:	Mobil:	Fax:

1.3. Zeitpunkt des letzten Sachstands

Datum:	Uhrzeit:	☐ Folgemeldung	☐ Abschlussmeldung

2. Beschreibung der mitteilungspflichtigen Beeinträchtigung

(Welche Grundwerte der Sicherheit sind in Telekommunikationsnetzen und/oder Telekommunikationsdiensten beeinträchtigt?)

☐ Verfügbarkeit ☐ Integrität ☐ Vertraulichkeit ☐ Authentizität

2.1. Wie wurde die Beeinträchtigung erkannt?

☐ Testbetrieb ☐ Auswertung von Logfiles ☐ Technisches (Netz-) Monitoring
☐ Systemwartung ☐ Hinweise von Dritten ☐ Audit, Prüfung, Zertifizierung
☐ Veröffentlichung gestohlener Informationen durch Dritte
☐ Sonstiges: _____

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

2.2. Zeitraum der Beeinträchtigung

Wann wurde die Beeinträchtigung erstmalig entdeckt?

Datum:	Uhrzeit:

☐ zeitlich begrenzt ☐ andauernd

Falls zeitlich begrenzt:

Beginn:

Datum:	Uhrzeit:

Ende:

Datum:	Uhrzeit:

2.3. Geographische Ausprägung

(beispielsweise Stadtgebiet, Bundesland, Bundesrepublik Deutschland)

Beschreibung der Ausprägung:

2.4. Betroffene Teilnehmerstunden

(Produkt aus Anzahl der betroffenen Teilnehmer und der Dauer der Beeinträchtigung in Stunden)

Anzahl der betroffenen Teilnehmer:	Dauer der Beeinträchtigung in Stunden:	Betroffene Teilnehmerstunden:

2.5. Internationale Zusammenschaltungen

Beschreibung der Auswirkung:
Welches Land außerhalb Deutschlands ist betroffen?
Wurde bereits jemand im betroffenen Land in Kenntnis gesetzt und wenn ja, wer?

2.6. Notruflenkung

Beschreibung der Auswirkung:

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

2.7. Außergewöhnliche IT-Störung

(Die Ursache der Beeinträchtigung ist außergewöhnlich oder nicht nachvollziehbar und die Beeinträchtigung kann nicht mehr im Rahmen des Tagesgeschäfts durch übliche Maßnahmen bewältigt werden. Das Kriterium gilt nur für Betreiber öffentlicher Telekommunikationsnetze oder Erbringer öffentlich zugänglicher Telekommunikationsdienste, welche unter die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom Stand 21.06.2017 (Anhang 4) fallen.

☐ die IT-Störung ist außergewöhnlich

Anmerkung:

2.8. Weiteres fallspezifisches Kriterium

(Es obliegt hier dem Verpflichteten, weitere fallspezifische Kriterien zur Bewertung der Beeinträchtigung heranzuziehen)

Beschreibung der Auswirkung:

3. Betroffene Telekommunikationsnetzabschnitte und/oder -schnittstellen

3.1. Netzabschnitte

☐ Zugangsnetz: ☐ leitungsgebunden ☐ drahtlos

(Netzabschnitt inklusive aller Netzelemente zwischen Teilnehmeranschluss und Konzentrationsnetz)

☐ Konzentrationsnetz: ☐ leitungsgebunden ☐ drahtlos

(Netzabschnitt inklusive aller Netzelemente (z.B. Konzentrator, Switch) zwischen Zugangsnetz und Edge-Knoten)

☐ Kernnetz: ☐ leitungsgebunden ☐ drahtlos

(Netzabschnitt inklusive aller Netzelemente zwischen Edge Knoten und Border Gateway)

Anmerkung:

3.2. Netzschnittstellen

☐ Edge-Knoten (Vermittlungseinrichtung an den Rändern des Kernnetzes als Übergang zum Zugangsnetz)
☐ Border Gateway (Vermittlungseinrichtung zwischen Kernnetzen)

Anmerkung:

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

4. Betroffene Telekommunikationsdienste

4.1. Festnetzdienste

☐ Sprache ☐ Daten ☐ Internetzugang ☐ E-Mail ☐ OTT
☐ Sonstige: _____

Beschreibung des Telekommunikationsdienstes:

4.2. Mobilfunkdienste

☐ Sprache ☐ Daten ☐ Internetzugang ☐ E-Mail ☐ OTT
☐ Sonstige: _____

Beschreibung des Telekommunikationsdienstes:

5. Vermutete oder tatsächliche Ursache der mitteilungspflichtigen Beeinträchtigung

5.1. Physischer Schaden

☐ Unzureichende Absicherung schutzbedürftiger Räume und Gebäude
☐ Diebstahl ☐ Zerstörung
☐ Sonstiges: _____

5.2. Fehlhandlung von Mitarbeitern oder Dritten

☐ Fehlbedienung ☐ Social Engineering ☐ Fehlkonfiguration

☐ Verletzung von Service Level Agreements durch einen Dienstleister
☐ Verstoß gegen interne Richtlinien und Anweisungen
☐ Unautorisierte Nutzung von Ressourcen
☐ Sonstiges: _____

5.3. Systemfehler

(Technik/Prozess/Infrastruktur)

☐Wiederherstellung nicht möglich
☐ Netzwerküberlastung
☐ Überspannung
☐ Defekt nach Softwareupdate
☐ Kabel-/Leitungsdefekt
☐ Stromausfall
☐ Kühlsystemausfall
☐ Fehlverhalten vom System
☐ Sonstiges: _____
☐ Elektromagnetische Interferenz/Störung
☐ Prozessablauf-, Verfahrensfehler
☐ Softwarefehler
☐ Defekte Hardware
☐ Sicherheitslücke in Hard- oder Softwarekomponente
☐ Notstromaggregat ohne Brennstoff
☐ Netzwerkausfall

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

5.4. Beschreibung der vermuteten oder tatsächlichen Ursache, den technischen Rahmenbedingungen sowie der betroffenen Informationstechnik

(Naturkatastrophe, Verkettung von verschiedenen Ursachen, weiterführende Informationen wie z.B. Common Vulnerabilities and Exposures, Schadsoftware oder sonstiges)

5.5. Informationstechnischer Angriff mit vermuteter oder tatsächlicher Ursache

5.5.1. Ausnutzung von Schwachstellen

☐ Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)
☐ Code Execution ☐ Privilege Escalation ☐ Protokollschwachstelle
☐ Injection-Angriff ☐ Cross-Site-Scripting ☐ Cross-Site-Request-Forgery
☐ Schwache Algorithmen/Schlüssel
☐ Sonstiges: _____

5.5.2. Advanced Persistent Threat

☐ Initialer Angriff per E-Mail ☐ Initialer Angriff über Webseiten (Watering hole attack)
☐ Initialer Angriff über manipulierte Hardware (z.B. USB-Stick)
☐ Sonstiges: _____

5.5.3. Schadprogramme

☐ Malware-Infektion, z.B. durch Trojaner, Rootkits zum Zwecke der Kontrollübernahme, der Datenmanipulation oder des Datenabflusses
☐ Ransomware z.B. Sperren von IT-Systemen zu Erpressungszwecken
☐ Adware, Scareware z.B. zu Betrugszwecken
☐ Multifunktionale Malware z.B. Viren, Würmer, Riskware
☐ Sonstiges: _____

5.5.4. Hacking und Manipulationen

☐ Webanwendungsbasierte Angriffe, z.B. Drive by-Exploits
☐ Angriffe auf Webanwendungen, z.B. SQL-Injection, Buffer Overflow
☐ Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP
☐ Systematisches Ausprobieren von Passwörtern
☐ Sonstiges: _____

5.5.5. Identitätsmissbrauch

☐ Diebstahl von Zugangsdaten, z.B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming
☐ Verschleierung einer Identität
☐ Diebstahl oder Fälschung von Zertifikaten
☐ Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting)
☐ Sonstiges: _____

5.5.6. Missbrauch (Innentäter)

☐ Weitergabe interner Informationen
☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrationsrechten
☐ Missbräuchliche Nutzung von Berechtigungen (insbesondere von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge
☐ Sonstiges: _____

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

5.5.7. Angriff auf die Verfügbarkeit von Diensten

☐ Überlastung, z.B. (D)DoS
☐ Gezielter Systemabsturz, z.B. DoS
☐ Sonstiges: _____

5.5.8. Angriffsart

☐ Gezielter Angriff ☐ Ungerichteter Angriff ☐ Unbekannt

5.5.9. Anzahl der Angriffe

Bei mehreren Angriffen, bitte vermutete Anzahl angeben:

5.5.10. Vermutete Motivation[1]

☐ Unbekannt ☐ Finanziell ☐ Politisch ☐ Persönlich
☐ Kriminell
☐ Terroristischer Hintergrund
(Pflicht **für das BSI** zur Weitergabe der Meldung an das Bundeskriminalamt (BKA))
☐ Nachrichtendienstlicher Hintergrund
(Pflicht **für das BSI** zur Weitergabe der Meldung an das Bundesamt für Verfassungsschutz)
☐ Sonstiges: _____

5.5.11. Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können zur Verfügung gestellt werden?

☐ Malware-Samples ☐ Hashsummen ☐ Dateiname ☐ Signaturen
☐ Logfiles ☐ IP-Adressen ☐ URLs
☐ Sonstiges: _____

5.5.12. Strafverfolgung

(Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA **durch das BSI** wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.)

☐ Unbekannt/keine Angabe ☐ Es wurde keine Strafanzeige gestellt
☐ Strafanzeige wurde gestellt:

Aktenzeichen:	Polizeidienststelle:	Bundesland:

☐ Weiterleitung der Meldung an BKA **durch das BSI** ist erwünscht
☐ Täter wurde ermittelt

6. Maßnahmen

6.1. Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung zu mindern bzw. zu beheben?

Beschreibung:

[1] Freiwillige Angabe

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171

6.2. Welche Maßnahmen werden ergriffen, um das Eintreten dieser/einer derartigen Beeinträchtigung zukünftig zu verhindern/zu erschweren?

Beschreibung:

Mitteilungseingang (von entsprechender Behörde auszufüllen)

Behörde:		
Name, Stellenbezeichnung:	Datum, Uhrzeit:	Eingangsbestätigung gesendet am:

Das Mitteilungsformular muss (per E-Mail oder Fax) an die Bundesnetzagentur und das BSI gesendet werden:

Bundesnetzagentur
sicherheitsverletzung.109@bnetza.de
+49(681)9330-775

BSI
meldungen-tkg@bsi.bund.de
+49(228) 9910 9582 6171