Sachstand

Cyberangriff als unabwendbares Ereignis im Sinne des § 96 Abs. 1 Nr. 1 SGB III

Cyberangriff als unabwendbares Ereignis im Sinne des § 96 Abs. 1 Nr. 1 SGB III

Aktenzeichen:	WD 6 - 3000 - 041/22
Abschluss der Arbeit:	22.06.2022, zugleich letzter Abruf der Internetlinks
Fachbereich:	WD 6: Arbeit und Soziales

Inhaltsverzeichnis

1. Einleitung

Kurzarbeitergeld ist eine Leistung der Bundesagentur für Arbeit, die bei einem erheblichen Arbeitsausfall in einem Betrieb den Verdienstausfall der Beschäftigten teilweise kompensiert. Durch die Zahlung von Kurzarbeitergeld sollen auch Kündigungen und Arbeitslosigkeit vermieden werden. Das Kurzarbeitergeld ist in den §§ 95 bis 109 des Dritten Buches Sozialgesetzbuch - Arbeitsförderung (SGB III) geregelt.

Nach § 96 Abs. 1 Nr. 1 SGB III ist ein Arbeitsausfall unter anderem erheblich, wenn er auf wirtschaftlichen Gründen oder einem unabwendbaren Ereignis beruht. Im Folgenden sollen die Anforderungen an das unabwendbare Ereignis für Unternehmen im Falle eines sogenannten Cyberangriffs skizziert werden.

2. Voraussetzungen des Anspruchs auf Kurzarbeitergeld

Gemäß § 95 Satz 1 SGB III haben Arbeitnehmerinnen und Arbeitnehmer einen Anspruch auf Kurzarbeitergeld, wenn ein erheblicher Arbeitsausfall mit Entgeltausfall gemäß § 96 SGB III vorliegt, die betrieblichen Voraussetzungen nach § 97 SGB III und persönlichen Voraussetzungen nach § 98 SGB III erfüllt sind und der Arbeitsausfall der Agentur für Arbeit gemäß § 99 SGB III angezeigt worden ist. Zudem muss die Kurzarbeit arbeitsrechtlich wirksam vereinbart sein, um einen Entgeltausfall im Sinne des § 106 SGB III zu begründen. Dauer und Höhe des Kurzarbeitergeldes bestimmen sich nach den §§ 104 und 105 SGB III.

Die Voraussetzungen für einen **erheblichen Arbeitsausfall** bestimmen sich nach § 96 Abs. 1 SGB III. Danach liegt ein erheblicher Arbeitsausfall vor, wenn er auf wirtschaftlichen Gründen oder einem unabwendbaren Ereignis beruht, vorübergehend und nicht vermeidbar ist und im jeweiligen Kalendermonat (Anspruchszeitraum) mindestens ein Drittel der in dem Betrieb beschäftigten Arbeitnehmerinnen und Arbeitnehmer von einem Entgeltausfall von jeweils mehr als zehn Prozent ihres monatlichen Bruttoentgelts betroffen ist. Die folgenden Ausführungen konzentrieren sich auf die Voraussetzung des unabwendbaren Ereignisses im Sinne des § 96 Abs. 1 Nr. 1 Alternative 2 SGB III.

2.1. Unabwendbares Ereignis

„Unter einem ‚unabwendbaren Ereignis' im Sinne des § 96 Abs. 1 Nr. 1 Alternative 2, Abs. 3 SGB III verstand der Regierungsentwurf zum AFG[1] […] jedes

- objektiv feststellbare Ereignis, das heißt ein plötzliches, zeitlich abgegrenztes Geschehen und kein langfristiger, sich entwickelnder Trend,

1 Arbeitsförderungsgesetz (BGBl. I 1969, S. 582), das als Vorgängergesetz des SGB III bis 31. Dezember 1997 galt.

– das auch durch die äußerste, nach den Umständen des Falles gebotene Sorgfalt durch den Arbeitgeber oder seine Mitarbeiter nicht abzuwenden war.“[2]

Nach der Rechtsprechung des Bundessozialgerichts (BSG) ist es dabei erforderlich, dass es sich um ein von außen kommendes, vom Arbeitgeber nicht beeinflussbares Ereignis handelt.[3]

Bei dem Ereignis muss es sich um ein gerade auch in zeitlicher Hinsicht begrenztes Geschehen handeln. „Dies folg[e] schon aus dem allgemeinen Verständnis des Begriffs ‚Ereignis‘, welcher eine vom bestehenden Zustand abweichende, überraschend und plötzlich eintretende Lage beschreib[e].“[4] Sich über längere Zeit entwickelnde Vorgänge genügen demgegenüber nicht.[5]

Unabwendbar ist ein Ereignis nach der Rechtsprechung des Bundessozialgerichts, wenn es „selbst durch äußerste, nach den Umständen des Falles gebotene und vernünftigerweise zu erwartende Sorgfalt nicht abzuwenden war.“[6] „Die Abwendbarkeit des Ereignisses für den Betrieb richtet sich danach, ob es vorhersehbar ist und Präventionsmaßnahmen objektiv möglich und subjektivwirtschaftlich vertretbar sind. Bei der ‚äußersten‘ Sorgfalt, die für die Vorhersehbarkeit und Vermeidbarkeit aufzuwenden ist, sind stärkere Maßstäbe anzulegen, als für die objektive Sorgfalt des allgemeinen Rechts- und Geschäftsverkehrs.“[7] Für die Feststellung der Unabwendbarkeit spielt aber auch eine Rolle, „was dem einzelnen Betrieb noch als Vorbeuge- und Schutzmaßnahmen […] angesichts der besonderen ökonomischen Lage des Betriebes, der Branche und den technischen Möglichkeiten etc. wirtschaftlich zumutbar ist.“[8]

---

2 Gagel/Bieback, SGB II, III, 84. Ergänzungslieferung Dezember 2021, § 95 SGB III Rn. 39 unter Verweis auf den Entwurf eines Arbeitsförderungsgesetzes (AFG), Bundestagsdrucksache V/2291 vom 16. November 1967, S. 70 zu § 59 Nr. 1 AFG.

3 BSG Urteil vom 15. Dezember 2005 - B 7a AL 10/05 R Rn. 18 (zitiert nach juris).

4 BSG Urteil vom 21. Juni 2018 - B 11 AL 4/17 R Rn. 19 (zitiert nach juris) mit Nachweisen aus der BSG-Rechtsprechung.

5 BSG Urteil vom 21. Juni 2018 - B 11 AL 4/17 R Rn. 21 (zitiert nach juris).

6 BSG Urteil vom 29. Oktober 1997 - 7 RAr 48/96 Rn. 23 (zitiert nach juris) mit Nachweis aus der BSG-Rechtsprechung.

7 Gagel/Bieback, SGB II, III, 84. Ergänzungslieferung Dezember 2021, § 96 SGB III Rn. 42 mit Nachweisen aus der BSG-Rechtsprechung.

8 Gagel/Bieback, SGB II, III, 84. Ergänzungslieferung Dezember 2021, § 96 SGB III Rn. 40a.

2.2. Unvermeidbarkeit des Arbeitsausfalls

Weitere Voraussetzung § 96 Abs. 1 Nr. 3 SGB III ist schließlich die Unvermeidbarkeit des Arbeitsausfalls. Der Arbeitsausfall muss zunächst unmittelbar auf dem unabwendbaren Ereignis beruhen, wobei bei einem Zusammentreffen mehrerer Ursachen ein wesentlicher Beitrag ausreichen kann.[9]

Unvermeidbarkeit bedeutet, „dass alle Maßnahmen ergriffen werden müssen, die Kurzarbeit zu verhindern vermögen. Insoweit richtet sich dieses Erfordernis sowohl an den Arbeitgeber, der auch vom Kurzarbeitergeld begünstigt wird und in der Regel Hauptakteur zur Vermeidung von Arbeitsausfällen ist, als auch an die Arbeitnehmer, die Anspruchsinhaber des Kurzarbeitergeldes sind, wie auch an den Betriebsrat als betriebliche Vertretung der Arbeitnehmer […]. Ein Fehlverhalten der Arbeitnehmer kann aber nur dann berücksichtigt werden, wenn sie als leitende Angestellte eine besondere, dem Arbeitgeber und dem Betrieb zuzurechnende Sorgfaltspflicht haben oder gerade ihnen die Funktionsfähigkeit und Sicherheit des Betriebes obliegt.“[10]

3. Cyberangriff als unabwendbares Ereignis

3.1. Begriff

Die Bundesregierung definiert den im Einzelnen umstrittenen Begriff des Cyberangriffs[11] in einer Antwort auf eine Kleine Anfrage unter Rückgriff auf die von ihr angenommene „Cyber-Sicherheitsstrategie für Deutschland 2016“ wie folgt:

> „Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.“[12]

Das Kriminologische Forschungsinstitut Niedersachen e.V. (KFN) hebt in einer 2020 veröffentlichten Studie als Ergebnis einer Unternehmensbefragung zum Thema Cyberangriffe hervor, dass etwa zwei Fünftel der Unternehmen in dem zwölf Monate umfassenden Untersuchungszeitraum

---

9 Vgl. zur Kausalität: BSG Urteil vom 21. Februar 1991 - 7 RAr 20/90; Gagel/Bieback, SGB II, III, 84. Ergänzungslieferung Dezember 2021, § 96 SGB III Rn. 61 f.

10 Gagel/Bieback, SGB II, III, 84. Ergänzungslieferung Dezember 2021, § 96 SGB III Rn. 110 f. mit weiteren Nachweisen.

11 Vgl. zum Streitstand: Petersen, Luca Alexander, Cyberangriffe - Definition, Regulierung, Pönalisierung, Göttinger Rechtszeitschrift (GRZ) 1/2020, S. 25 (26).

12 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP - Drucksache 19/7321 -, Bedrohung durch Cyberangriffe, Bundestagsdrucksache 19/7607 vom 11. Februar 2019, S. 2.

2018/2019 von einem Cyberangriff betroffen waren.[13] Die Betroffenheitsrate erhöhe sich aufgrund ihrer höheren Komplexität in organisatorischer, personeller und technischer Hinsicht mit der Unternehmensgröße sowie bei kleineren Unternehmen mit der Anzahl der Standorte des Unternehmens im In- und Ausland. Die jeweilige Wirtschaftszweigzugehörigkeit stehe ebenfalls im Zusammenhang mit der Betroffenheit. Mit dem Anstieg des Risikos eines Angriffs steige auch die Notwendigkeit des zusätzlichen Schutzes gegen Cyberangriffe.[14] Das KFN unterscheidet zwischen technischen und organisatorischen IT-Sicherheitsmaßnahmen. Es genüge danach nicht, diese IT-Sicherheitsmaßnahmen bloß zu haben; erforderlich sei zudem die aktive Umsetzung im Unternehmen.[15] Abschließend bewertet das KFN „Cyberkriminalität" als „unternehmerisches Risiko, das nur schwer eingeschätzt, bewertet und gesteuert werden kann".[16] Insbesondere die seit der Corona-Krise von vielen Arbeitgebern eröffnete Möglichkeit, vom Homeoffice aus zu arbeiten, biete neue Risiken für Cyberangriffe.[17]

3.2. Ereignis

Die Frage, unter welchen Umständen ein Cyberangriff ein unabwendbares Ereignis im Sinne des § 96 Abs. 1 Nr. 1 Alternative 2 SGB III als Voraussetzung für die Zahlung von Kurzarbeitergeld darstellt, war bisher - soweit ersichtlich - noch nicht Gegenstand der höherinstanzlichen sozialgerichtlichen Rechtsprechung.

Soweit die Voraussetzung der zeitlichen Abgrenzbarkeit des Cyberangriffs nach den oben genannten Kriterien gegeben ist, kann er ein Ereignis im Sinne des § 96 Abs. 1 Nr. 1 SGB III darstellen. Trägt der Cyberangriff wesentlich dazu bei, dass die technischen Möglichkeiten zur Verrichtung der Tätigkeit nicht genutzt werden können, dürfte er auch unmittelbar zu einem erheblichen Arbeitsausfall führen können.

3.3. Unabwendbarkeit

Liegt ein solcher Cyberangriff vor, stellt sich die Frage nach dessen Unabwendbarkeit. Ob ein Cyberangriff unabwendbar ist hängt wesentlich davon ab, welche Schutzmaßnahmen der betroffene

---

13 KFN, Cyberkriminalität gegen Unternehmen - Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019, Forschungsbericht Nr. 152, Hannover 2020, S. 12. Die Studie wurde durch das Bundesministerium für Wirtschaft und Energie sowie durch die Wirtschaftsprüfungsgesellschaft Pricewaterhouse-Coopers (PwC) und die Stiftung der Vereinigten Hannoverschen Versicherung (VHV) gefördert; abrufbar im Internetauftritt des KFN: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf.

14 KFN, Cyberkriminalität gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019, Forschungsbericht Nr. 152, Hannover 2020, S. 14, 18 ff.

15 KFN, Cyberkriminalität gegen Unternehmen - Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019, Forschungsbericht Nr. 152, Hannover 2020, S. 27 f.

16 KFN, Cyberkriminalität gegen Unternehmen - Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019, Forschungsbericht Nr. 152, Hannover 2020, S. 33.

17 Vgl. KFN, Cyberangriffe gegen Unternehmen in Deutschland, Ergebnisse einer Folgebefragung 2020, Forschungsbericht Nr. 162, Hannover 2021, S. 45; abrufbar im Internetauftritt des KFN: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf.

Arbeitgeber im Rahmen der ihm obliegenden „äußersten, nach den Umständen des Falles gebotenen und vernünftigerweise zu erwartenden Sorgfalt“ (siehe oben Abschnitt 2.1) hätte treffen müssen, um den Angriff und damit einen erheblichen Arbeitsausfall im Sinne des § 96 Abs. 1 SGB III zu verhindern.

Rechtlich verbindliche Mindeststandards für technische und organisatorische Maßnahmen durch Unternehmen zur Abwehr von Cyberangriffen gibt es nicht.

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** hat als nationale Cyber-Sicherheitsbehörde (§ 1 Satz 2 des Gesetzes über das BSI (BSI-Gesetz - BSIG)[18]) unter anderem folgende Aufgaben:

- Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (§ 3 Abs. 1 Nr. 14 BSIG) sowie
- Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (§ 3 Abs. 1 Nr. 14a BSIG).

Zur Erfüllung dieser Aufgaben hat das BSI die Befugnis, Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen auszusprechen (§ 7 Abs. 1 Nr. 1 Buchstaben a-d BSIG) sowie Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte zu empfehlen (§ 7 Abs. 1 Nr. 2 BSIG).

Hierzu wurde beim BSI das Computer Emergency Response Team der Bundesverwaltung (CERT-Bund) eingerichtet. Zu den Hauptaufgaben des CERT-Bund zählen

- „Erstellen und Veröffentlichen von präventiven Handlungsempfehlungen zur Schadensvermeidung,
- Hinweisen auf Schwachstellen in Hardware- und Softwareprodukten,
- Vorschlagen von Maßnahmen zur Behebung von bekannten Sicherheitslücken,
- Warnen oder Alarmieren bei besonderen Bedrohungslagen (bezogen auf Informationstechnik) und
- Empfehlen von reaktiven Maßnahmen zur Schadensbegrenzung oder -beseitigung.“[19]

Über den Warn- und Informationsdienst (WID) von CERT-Bund werden täglich Warnungen und Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für

---

18 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I 2009, S. 2821), das zuletzt durch Artikel 12 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 23. Juni 2021 (BGBl. I 2021, S. 1982) geändert worden ist.

19 Vgl. im Internetauftritt des CERT-Bund: https://www.cert-bund.de/about.

IT-Systeme publiziert, die tagesaktuell abgerufen werden können. „Die frühzeitige Verteilung dieser Informationen soll dazu beitragen, Sicherheitsvorfälle zu vermeiden oder zumindest deren Auswirkungen zu beschränken.“[20]

Das BSI unterscheidet bei seinen Veröffentlichungen Warnungen nach § 7 BSIG, Cyber-Sicherheitswarnungen und Technische Sicherheitshinweise.[21] „Eine Warnung nach § 7 BSIG spricht das BSI dann aus, wenn seitens des Herstellers keine oder ungenügende Maßnahmen gegen die Gefährdung ergriffen werden, die von einer bekannt gewordenen Sicherheitslücke ausgeht.“[22] „Mit Cyber-Sicherheitswarnungen informiert das BSI über neue, bedrohliche Angriffsvektoren, die z. B. durch herausgehobene Einzelvorfälle bekannt werden, über Herstellermaßnahmen gegen bekanntgewordene Schwachstellen, wenn z. B. Patches oder Sicherheitsupdates zur Verfügung stehen, sowie in Management-Infos z. B. über auslaufenden Update- oder Patch-Support von Herstellern.“[23]

Daneben veröffentlicht das BSI Checklisten und Handlungsempfehlungen für Unternehmen, die einen IT-Sicherheitsvorfall haben oder vorbeugende Maßnahmen treffen wollen.[24]

Auch das Bundeskriminalamt (BKA) verweist auf den IT-Grundschutz des BSI und hat für Unternehmen Handlungsempfehlungen für technische Präventionsmaßnahmen veröffentlicht.[25]

Die von BSI und BKA formulierten Sicherheitsinformationen und Handlungsempfehlungen für Präventionsmaßnahmen dienen der Information der Wirtschaft und sollen die Unternehmen in die Lage versetzen, Bedrohungen einzuschätzen und sich erforderlichenfalls davor zu schützen. Sie erheben keinerlei Anspruch auf allgemeine rechtliche Verbindlichkeit.

Sie sind zum Teil sehr allgemein formuliert, sodass es unsicher erscheint, ob sie geeignet sein könnten, die zur Abwendung eines Cyberangriffs gebotene „äußerste Sorgfalt“ näher zu konkretisieren. Auch wenn diese strengeren Maßstäben entsprechen muss als die objektive Sorgfalt des

---

20 Vgl. im Internetauftritt des CERT-Bund https://www.cert-bund.de/wid.

21 Vgl. im Internetauftritt des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/technische-sicherheitshinweise-und-warnungen_node.html.

22 BSI-Warnungen gemäß § 7 und § 7a BSIG, abrufbar im Internetauftritt des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html; eine Liste der Warnungen nach § 7 BSIG der vergangenen sechs Monate kann hier abgerufen werden.

23 Cyber-Sicherheitswarnungen, abrufbar im Internetauftritt des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Cyber-Sicherheitswarnungen/cyber-sicherheitswarnungen_node.html; Cyber-Sicherheitswarnungen können hier tagesaktuell nach Bedrohungsstufen abgerufen werden.

24 Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen, abrufbar im Internetauftritt des BSI: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen_node.html.

25 BKA, Cybercrime. Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime, Oktober 2019, S. 13 f., abrufbar im Internetauftritt des BKA: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Wirtschaftsunternehmen/wirtschaftsunternehmen_node.html.

allgemeinen Rechts- und Geschäftsverkehrs (siehe oben, Abschnitt 2.1), dürfte die lückenlose Verfolgung und Umsetzung der Warnungen und Informationen des BSI dafür nicht erforderlich sein.

Zumindest grundlegende Schutzmaßnahmen wird man jedoch in diesem Rahmen fordern müssen. Auch dürfte den vom BSI veröffentlichten Warnungen nach § 7 BSIG in diesem Zusammenhang eine größere Bedeutung zukommen als bloßen Hinweisen und Empfehlungen. Im Übrigen bestimmen sich die Anforderungen an die erforderliche Sorgfalt aber nach Wirtschaftszweig, Art und Größe des konkreten Betriebs oder Unternehmens sowie der finanziellen Leistungsfähigkeit des betroffenen Arbeitgebers im jeweiligen Einzelfall, sodass eine allgemeingültige Aussage dazu nicht möglich ist.

Unternehmen im besonderen öffentlichen Interesse im Sinne des § 2 Abs. 14 Nr. 1 und 2 BSIG sind allerdings nach § 8f Abs. 1 BSIG verpflichtet, mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim BSI vorzulegen, aus der unter anderem hervorgehen muss, wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und ob dabei der Stand der Technik eingehalten wird.

Der in diesem Zusammenhang gegenüber dem BSI erklärte Schutzstandard dürfte für diese Unternehmen jedenfalls auch von der nach § 96 Abs. 1 SGB III erforderlichen Sorgfaltspflicht umfasst sein.

***