Autor:	André Lippert
Dokumenttyp:	Aufsatz
Literaturnachweis:	CB 2020, 231-235
Quelle:	dfv Mediengruppe, Frankfurt am Main
Fundstelle:	CB 2020, 231-235
Zitiervorschlag:	Lippert, CB 2020, 231-235

Die Cyberangriffs-Verordnung der EU – neue Herausforderungen, bekannte Instrumente

Dr. André Lippert, RA

CB-Beitrag

Mit der neuen Cyberangriffs-Verordnung will die Europäische Union die äußere Bedrohung der Union und der Mitgliedstaaten durch Cyberangriffe sanktionieren und von der zukünftigen Begehung dieser Angriffe abschrecken. Sie ist im Mai 2019 in Kraft getreten und betrifft vor allem kritische Infrastrukturen. Dazu nutzt sie die bekannten außenwirtschaftsrechtlichen Sanktionsinstrumente: Personen, Organisationen oder Einrichtungen, die für (versuchte) Cyberangriffe von außerhalb der EU verantwortlich sind oder mit diesen in Verbindung stehen, sollen finanziell isoliert werden, und zwar durch ein Verfügungs- und Bereitstellungsverbot.

I. Einleitung

Ausgangspunkt der Cyberangriffs-Verordnung1 waren die europäischen Bemühungen, gerade äußeren Bedrohungen der EU und der Mitgliedstaaten durch Cyberattacken zu begegnen. Erster Ausdruck dieser Bemühungen waren die Schlussfolgerungen des Rates der Europäischen Union vom 19. 6. 2017, in denen er seine Besorgnis über die zunehmende Fähigkeit und Bereitschaft staatlicher und nicht staatlicher Akteure, ihre Ziele durch „böswillige Cyberaktivitäten“ zu verfolgen, zum Ausdruck brachte.

Diese Schlussfolgerungen fielen in eine Zeit, in der Cyberangriffe auf Regierungsstellen, Wirtschaftsunternehmen und Forschungsinstitute merklich zunahmen. In seiner Auswertung zu nachrichtendienstlich gesteuerten Cyberangriffen kommt das Bundesamt für Verfassungsschutz (BfV) zu dem Ergebnis, dass Deutschland vor allem durch russische, chinesische und iranische Cyberangriffskampagnen betroffen sei.2 Gerade die russischen Kampagnen seien, so das BfV, Ergebnis einer meist mehrjährigen, international ausgerichteten Cyberspionage-Operation. Sie seien technisch hochqualifiziert, mit starken finanziellen Ressourcen und außergewöhnlichen Operativ- und Auswertefähigkeiten verbunden. Im Zentrum der russischen Cyberspionage stehe die Informationsgewinnung unter anderem im Bereich der Energiewirtschaft, der Außen- und Militärpolitik, der Verteilung von EU-Geldern sowie humanitäre Fragen. Das BfV vermutet, dass eine langjährige Cyberangriffskampagne (genannt APT28) unter anderem für die im August 2016 durchgeführte Angriffswelle gegen die Verwaltung des Deut-

schen Bundestages, verschiedener politischer Parteien, aber auch gegen die Athletendatenbank der Welt-Anti-Doping-Agentur (WADA) verantwortlich ist. Mit den russischen Angriffen vergleichbar sind nach dem BfV auch Cyberangriffe, die chinesischen Spionageeinrichtungen zugeschrieben werden. Das Interesse liege hier zusätzlich im Bereich der Luft- und Raumfahrt, der Elektrotechnik, der Stahl- und Metallindustrie sowie der Hochtechnologie.

Neben der Informationsgewinnung traten gerade in den letzten Jahren vor allem Cyber-Kriminalität, aber auch Cyber-Sabotageakte in den Vordergrund. Während auch bei Wirtschaftsunternehmen sowohl im mittelständischen Bereich als auch bei Großunternehmen – vergleiche nur die Cyberangriffe auf mehrere deutsche DAX-Konzerne Mitte 2019 – weiterhin die Informationsgewinnung ein wichtiges Motiv ist, nehmen auch kriminelle Aktivitäten zu, z. B. zur Erpressung von „Lösegeld"; die Dunkelziffer wird in diesem Bereich als besonders hoch eingeschätzt.3 Schließlich wird zunehmend vor Sabotageakten im Bereich kritischer Infrastrukturen, also vor allem Strom-, Wasserversorgung und Versorgung mit anderen lebenswichtigen Gütern gewarnt.

Die europäischen Bemühungen gipfelten schließlich im Beschluss (GASP) 2019/797 des Rates vom 17. 5. 2019 über restriktive Maßnahmen gegenüber Cyberangriffe, die die Union und ihre Mitgliedstaaten bedrohen. Hieraus ergeben sich bereits die wesentlichen Rahmendaten für die Cyberangriffs-Verordnung. Der Beschluss stellt ausdrücklich fest, dass „gezielte restriktive Maßnahmen" notwendig sind, um eine „abschreckende und vorbeugende Wirkung zu erreichen"; die Feststellung der Verantwortung eines Drittstaats für einen Cyberangriff sei allerdings nicht Gegenstand der gemeinsamen diplomatischen Reaktion der EU, sondern obliege als souveräne politische Entscheidung jedem Mitgliedstaat selbst.

Die Bundesregierung geht aktuell davon aus, dass Cyberangriffe für Staat, Wirtschaft und Gesellschaft nach wie vor ein großes Gefahrpotential darstellen. Die Gesamtzahl stagniere zwar auf hohem Niveau, die Angriffe selbst würden aber qualitativ immer ausgefeilter und für die Betroffenen gefährlicher.4 Aus diesem Grund will die Bundesregierung auch national die Schutzmaßnahmen verstärken und eine

Novellierung des IT-Sicherheitsgesetzes auf den Weg bringen (IT-Sicherheitsgesetz 2.0). Das erste IT-Sicherheitsgesetz war ein Artikelgesetz, das ebenfalls im Jahre 2015, in dem auch die Bestrebungen auf europäischer Ebene forciert wurden, verkündet wurde. Kernpunkt waren Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) und die Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie). Sie bildete den einheitlichen Rechtsrahmen für die EU-weite Koordinierung der Maßnahmen zur Cyber-Sicherheit, z. B. durch eine stärkere Zusammenarbeit der Mitgliedstaaten und Mindestsicherheitsanforderungen. Die nun 2020 von der Bundesregierung geplanten Änderungen sollen die Befugnisse des BSI zum Schutz der Bundesverwaltung ausweiten. Zum Schutz der Wirtschaft sollen für die Betreiber kritischer Infrastrukturen Meldepflichten und Verpflichtungen zur Einhaltung von Mindeststandards ausgebaut werden.5

II. Äußere Bedrohung durch Cyberangriffe

Voraussetzung für die Sanktionen der Cyberangriffs-Verordnung ist eine äußere Bedrohung für die EU oder ihre Mitgliedstaaten durch einen tatsächlichen oder versuchten Cyberangriff, der erhebliche oder potentiell erhebliche Auswirkungen hat.

1. Äußere Bedrohung für die EU oder Mitgliedstaaten

Das sanktionsrechtliche Instrumentarium der EU setzt einen außenwirtschaftsrechtlichen Sachverhalt voraus, hier in Form der äußeren Bedrohung für die EU oder ihre Mitgliedstaaten.

Eine *äußere Bedrohung der Union* wird nach Art. 1 Abs. 2 VO angenommen bei Cyberangriffen, die

- ihren Ausgang außerhalb der EU haben oder von dort durchgeführt werden,
- außerhalb der EU befindliche Infrastruktur nutzen,
- von Personen oder Organisationen, die außerhalb der EU ansässig oder tätig sind durchgeführt bzw. die Durchführung eines solchen Angriffs kontrolliert oder angewiesen wird.

Dazu zählen auch Cyberangriffe, die gegen Organe oder Einrichtungen der EU oder ihrer Operationen bzw. Missionen im Bereich der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) geführt werden (Art. 1 Abs. 5 VO).

Eine *äußere Bedrohung der Mitgliedstaaten* wird angenommen, wenn Cyberangriffe geführt werden gegen

- kritische Infrastrukturen, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder der Gesundheit, Sicherheit und des Wohlergehens der Bevölkerung sind;
- Dienstleistungen, die für die Aufrechterhaltung sozialer oder wirtschaftlicher Tätigkeiten erforderlich sind, insbesondere im Bereich Energie, Verkehr, Banken, Gesundheitswesen, Trinkwasser oder digitale Infrastruktur;
- kritische staatliche Funktionen, insbesondere in den Bereichen Verteidigung, Staatsführung, Wahlen, wirtschaftliche und zivile Infrastruktur, innere Sicherheit sowie Außenbeziehungen.

Bei dieser Aufzählung fällt auf, dass sie sich stark an der Definition kritischer Infrastrukturen, wie sie sich beispielsweise in der EU-Screening-Verordnung für ausländische Direktinvestitionen6 findet, orientiert. Auf diese Verordnung verweist allerdings die Cyberangriffs-Verordnung nicht, sondern fasst die sensiblen Bereiche weiter, indem insbesondere neben kritischen Infrastrukturen auch Dienstleistungen für soziale und wirtschaftliche Tätigkeiten sowie für kritische staatliche Funktionen aufgenommen werden. In Deutschland besteht – nicht zuletzt durch zahlreiche Änderungen der gesetzlichen Grundlagen der Vergangenheit – ein vergleichsweise differenziertes System für kritische Infrastruktu-

ren, die vor allem in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) aufgelistet sind.7 Diese decken sich weitgehend mit den Vorgaben der – zunächst vorrangigen – Cyberangriffs-Verordnung; gleichzeitig lässt sie in bestimmten Bereichen, z. B. im Bereich der wesentlichen sozialen wirtschaftlichen Tätigkeiten, Gestaltungsspielraum für die Mitgliedstaaten.

2. Cyberangriff oder versuchter Cyberangriff

Ein Cyberangriff oder ein versuchter Cyberangriff, der das zentrale Merkmal auf Tatbestandsseite ist, liegt zunächst vor bei Handlungen, die den Zugang zu oder den Eingriff in Informationssysteme bewirken. Informationssysteme werden dabei weit verstanden als ein System der automatischen Verarbeitung von digitalen Daten; in ein solches System wird eingegriffen, wenn dieses System behindert oder gestört wird, durch die Eingabe von digitalen Daten, deren Übermittlung, Beschädigung, Löschung, Veränderung oder Unterdrückung.

Cyberangriffe können jedoch nicht nur Informationssysteme betreffen, sondern liegen auch bei einem Eingriff in Daten oder beim Abfangen von Daten selbst vor. Es reicht also auch schon beispielsweise der Diebstahl von Daten, Geldern, wirtschaftlichen Ressourcen oder geistigem Eigentum oder wenn Daten im Rahmen nicht öffentlicher digitaler Datenübermittlung durch technische Hilfsmittel abgefangen werden (Art. 1 Abs. 7 VO).

3. Erhebliche bzw. potentiell erhebliche Auswirkungen

Zur Beurteilung der Frage, wann ein Cyberangriff erhebliche Auswirkungen bzw. mit Blick auf einen versuchten Cyberangriff potentielle erhebliche Auswirkungen hat, sieht die Verordnung verschiedene Faktoren vor, die bei der Beurteilung anzulegen sind. Entscheidend sollen insoweit sein:

- Umfang, Ausmaß, Wirkung oder Schwere der versuchten Störung für wirtschaftliche und gesellschaftliche Tätigkeiten, kritische staatliche Funktionen, die öffentliche Ordnung oder Sicherheit;
- die Anzahl der betroffenen Personen und Organisationen oder Mitgliedstaaten;
- die Höhe des wirtschaftlichen Schadens;
- der vom Täter selbst oder für andere erlangte wirtschaftliche Nutzen;
- Menge und Art der gestohlenen Daten und
- die Art der wirtschaftlich sensiblen Daten, auf die zugegriffen wurde.

III. Sanktionen gegen gelistete Personen oder Organisationen

Liegen diese Voraussetzungen vor, beschließt der Rat die Aufnahme der entsprechenden Personen oder Organisationen in Anhang I der

Verordnung (Art. 13 VO). Die Vermögenswerte dieser erfassten Personen oder Organisationen werden eingefroren; ihnen dürfen keine Gelder oder wirtschaftliche Ressourcen mehr zur Verfügung gestellt werden. Im Einzelfall können die Mitgliedstaaten davon Ausnahmen genehmigen. Die Sanktionen der Cyberangriffs-Verordnung entsprechen ganz weitgehend den Sanktionen aus personenbezogenen Embargo-Verordnungen.8

1. Anknüpfungspunkt Vermögenswerte

Anknüpfungspunkt für die Sanktionierungen sind die Vermögenswerte der sanktionierten Personen oder Organisationen. Vermögenswert wird als Oberbegriff für wirtschaftliche Ressourcen und Gelder verwendet. Wirtschaftliche Ressourcen sind alle materiellen oder immateriellen, beweglichen oder unbeweglichen Vermögenswerte, bei denen es sich nicht um Gelder handele, die aber für den Erwerb von Geldern, Waren oder Dienstleistungen verwendet werden können (Art. 1 Abs. 8 lit. d) VO). Letztendlich werden danach alle Güter erfasst, die selbst wieder für den Erwerb von Finanzmitteln verwendet werden können, also einen Marktwert haben und handelbar sind.

Der Begriff der Gelder ist zwar im Verhältnis zu wirtschaftlichen Ressourcen spezieller, wird aber ebenfalls weit gefasst. Er umfasst neben Bargeld, Checks und Geldforderungen auch Einlagen bei Banken, Guthaben auf Konten, Zinserträge und Dividenden, jede Art von Wertpapieren, Obligationen sowie Kredite, Bürgschaften, Rechte auf Verrechnung, Vertragserfüllungsgarantien und andere finanzielle Ansprüche.

2. Gelistete Personen, Organisationen und Einrichtungen

Die Sanktionen richten sich gegen die in Anhang I der Verordnung gelisteten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die für (versuchte) Cyberangriffe verantwortlich sind. Auf die Liste aufgenommen werden können nach Art. 3 Abs. 3 VO darüber hinaus auch Personen, Organisationen und Einrichtungen, die finanzielle, technische oder materielle Unterstützung für Cyberangriffe leisten oder auf andere Weise daran beteiligt sind, also beispielsweise durch Planung, Vorbereitung, Unterstützung oder Ermutigung. Ausreichend ist schließlich auch, dass die gelisteten Personen/Organisationen mit den Genannten in Verbindung stehen. Wann eine solche Verbindung gegeben ist, wird nicht definiert. Klar ist aber, dass für den Nachweis einer solchen Verbindung die hohen Anforderungen der Rechtsprechung der europäischen Gerichte erfüllt sein müssen (siehe dazu sogleich). Der Ausdruck findet sich auch in neueren Sanktionsverordnung, z. B. betreffend restriktive Maßnahmen gegen Iran9 oder wegen der Lage in der Ukraine10; auch hier findet sich keine ausdrückliche Definition.

Es ist aber davon auszugehen, dass dieser Begriff weit zu verstehen ist und sich auf jede, auch nicht erst rechtliche oder institutionelle Verknüpfung zwischen zwei Personen bzw. Organisationen bezieht. Zum Teil wird nämlich in den Sanktionsverordnungen ausdrücklich auf Eigentum und Kontrolle abgestellt, wenn es auf rechtlich fundierte Verbindungen ankommen soll.11 Die Cyberangriffs-Verordnung hingegen lässt auch eine irgendwie geartete Verbindung ausreichen. Bislang ist die Liste der Cyberangriffs-Verordnung noch leer.

3. Einfrieren von Vermögenswerten

Erste Sanktion ist das Einfrieren von Vermögenswerten der gelisteten Personen oder Organisationen (Art. 3 Abs. 1 VO). Die Bundesbank kann von diesem Verfügungsverbot aber unter bestimmten Voraussetzungen eine Freigabe genehmigen.

a) Einfrieren

Sämtliche Gelder und wirtschaftlichen Ressourcen, die im Eigentum oder Besitz der gelisteten Personen bzw. Organisationen stehen oder von diesen gehalten oder kontrolliert werden, werden eingefroren. Gelder werden eingefroren, wenn jegliche Form des Transfers, der Verwendung oder des Zugangs zu ihnen oder ihres Einsatzes, wodurch das Volumen, die Höhe, die Belegenheit, das Eigentum, der Besitz oder die Zweckbestimmung verändert wird, verhindert wird. Jegliche Nutzungsmöglichkeit soll also ausgeschlossen werden. Da auch wirtschaftliche Ressourcen eingefroren werden sollen, dürfen diese darüber hinaus auch nicht für den Erwerb von Waren oder Dienstleistungen – was auch den Verkauf, das Vermieten oder das Verpfänden einschließt – genutzt werden. Diese Aufzählung ist im Rahmen der Verordnung nur beispielhaft.

b) Genehmigung bei Erfüllungsgeschäften

Die Bundesbank kann die Freigabe bestimmter Gelder oder wirtschaftlicher Ressourcen genehmigen, wenn sie Gegenstand einer schiedsgerichtlichen Entscheidung *vor* der Aufnahme der Person auf die Sanktionsliste oder Gegenstand einer gerichtlichen oder behördlichen Entscheidung, unabhängig vom Datum, sind. Die Vermögenswerte müssen zur Erfüllung der entsprechenden Forderung verwendet werden und dürfen nicht die gelistete Person bzw. Organisation begünstigen bzw. nicht im Widerspruch zur öffentlichen Ordnung des betreffenden Mitgliedstaates stehen (Art. 5 VO).

c) Altverträge

Gleiches gilt für Vermögenswerte, die auf Grundlage eines Vertrages oder einer vergleichbaren Verpflichtung zu leisten sind und dieser Vertrag vor dem Datum abgeschlossen wurde, an dem die Person/Organisation gelistet wurde (Art. 6 VO). In diesem Fall kann die Freigabe bestimmter Vermögenswerte genehmigt werden. Die Erfüllung von Altverträgen ist also weiterhin möglich.

4. Bereitstellungsverbot

Zweite Sanktion ist das Verbot, gelisteten Personen oder Organisationen Vermögenswerte unmittelbar oder mittelbar zur Verfügung zu stellen oder zugutekommen zu lassen (Art. 3 Abs. 2 VO).

a) Unmittelbar oder mittelbar zur Verfügung stellen

Es handelt sich um das klassische Bereitstellungsverbot, wonach den gelisteten Personen/Organisationen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt oder Zugutekommen dürfen.

Ein mittelbares Bereitstellen kann vorliegen, wenn die Vermögenswerte einem Unternehmen, das im Eigentum einer gelisteten Person

steht oder von dieser kontrolliert wird, zur Verfügung gestellt werden. Wann dies der Fall ist, hat der Rat der EU in der Aktualisierung seiner Leitlinien zur Umsetzung und Evaluierung restriktiver Maßnahmen (Sanktionen) im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik genauer definiert.12 So liegt Eigentum der gelisteten Person vor, wenn mehr als 50 Prozent der Eigentumsrechte in ihrem Besitz sind bzw. sie eine Mehrheitsbeteiligung hält. Die Frage, ob ein Unternehmen von einer gelisteten Person kontrolliert wird, ist deutlich komplexer. Dabei ist unter anderem zu prüfen, ob die gelistete Person allein oder über Vereinbarungen mit anderen Anteilseignern die Mehrheit der Stimmrechte hat oder bestimmenden Einfluss auf die Leitungs-, Verwaltungs- und Aufsichtsorgane des Unternehmens nehmen kann. Ist dies der Fall, so dürfen diesem Unternehmen grundsätzlich keine Gelder oder wirtschaftlichen Ressourcen zur Verfügung gestellt werden – denn dies würde als mittelbare Bereitstellung an die gelistete Person gelten.13

b) Beschränkungen des Umfangs

Das Bereitstellungsverbot hindert allerdings Banken nicht daran, Gelder die von Dritten auf das Konto einer gelisteten Person/Einrichtung überwiesen werden, gutzuschreiben. Die entsprechenden Beträge werden dann ebenfalls nach Art. 3 Abs. 1 VO eingefroren. Das Bereitstellungsverbot erstreckt sich unter gleichen Bedingungen ebenfalls nicht auf Zinsen oder Zahlungen aufgrund von Verträgen oder anderen Vereinbarungen, die vor dem Datum der Listung abgeschlossen wurden bzw. Zahlungen aufgrund von gerichtlichen oder behördlichen Entscheidungen (Art. 7 VO).

5. Genehmigungsmöglichkeit von Ausnahmen

Für bestimmte Vermögenswerte kann die Bundesbank die Freigabe vom Verfügungsverbot und vom Bereitstellungsverbot erteilen. Art. 4 VO listet vor allem Vermögenswerte auf, die auf dem Markt nicht als Finanzmittel dienen oder in Finanzmittel umgewandelt werden können. Diese Mittel dienen unter anderem zur

- Befriedigung der Grundbedürfnisse der gelisteten natürlichen Personen sowie unterhaltsberechtigter Familienangehöriger, z. B. für die Bezahlung von Nahrungsmitteln, Mieten, Medikamenten, Steuern, Versicherungen etc.;
- Bezahlung angemessener Honorare für rechtliche Dienstleistungen;
- Bezahlung von Gebühren oder Kosten der Verwahrung oder Verwaltung der eingefrorenen Vermögenswerte;
- Deckung außerordentlicher Ausgaben (Art. 4 VO).

6. Erfüllungsverbot

Ergänzt werden die Sanktionen durch ein Erfüllungsverbot: Gegenüber gelisteten bzw. in ihrem Namen handelnden Personen/Organisationen dürfen Ansprüche nicht erfüllt werden. Diese Ansprüche können sich aus Verträgen ergeben und umfassen auch Schadensersatzansprüche, andere Entschädigungsansprüche, aber auch Ansprüche auf Verlängerung oder Zahlung einer finanziellen Garantie in jeglicher Form; ausreichend ist, dass die Erfüllung dieser Ansprüche von den in der Verordnung

verhängten Maßnahmen unmittelbar oder mittelbar, ganz oder teilweise betroffen ist (Art. 11, Art. 1 Abs. 8 VO).

IV. Auswirkungen auf die unternehmerische Praxis

Wie alle Sanktionsregelungen hat auch die Cyberangriffs-Verordnung unmittelbar Auswirkungen auf das Compliance-Managementsystem in betroffenen Unternehmen. Neben den allgemeinen Anforderungen, die an ein solches System insbesondere im Bereich der Exportkontrolle gestellt werden,14 sind mit Blick auf die Cyberangriffe der Listenabgleich und spezielle Mitteilungspflichten hervorzuheben. Die Beachtung dieser Pflichten sollte im Unternehmen sichergestellt werden, da die drohenden Konsequenzen bei einem Verstoß empfindlich und weitreichend sein können.

1. Listenabgleich

Für Unternehmen ergibt sich aus der Cyberangriffs-Verordnung – wie bei allen vergleichbaren Sanktionsverordnungen – zunächst die Notwendigkeit, die gelisteten Personen/Organisationen in den Abgleich der Sanktionslisten einzubeziehen. Da diese Geschäftspartnerprüfung in der Regel elektronisch abläuft, wird zumindest zu prüfen sein, ob der jeweilige Anbieter auch die (zukünftig) im Rahmen der Cyberangriffs-Verordnung gelisteten Personen mitumfasst. Die anschließenden Prüfungs- und Entscheidungsprozesse des internen Compliance-Managementsystems des Unternehmens werden dann wie üblich ablaufen müssen.

2. Mitteilungspflichten

Darüber hinaus trifft Unternehmen auch eine generelle Mitteilungspflicht (Art. 8 VO): Danach müssen natürliche und juristische Personen, Organisationen und Einrichtungen alle Informationen, die die Anwendung dieser Verordnung erleichtern – z. B. Informationen über die eingefrorenen Konten und Beträge – unverzüglich der zuständigen Behörde des Mitgliedstaates übermitteln und mit dieser Behörde bei der Überprüfung der Informationen zusammenarbeiten.

3. Konsequenzen bei Verstoß

Ein Verstoß gegen die Verbote und Pflichten der Cyberangriffs-Verordnung ist als Straftat oder Ordnungswidrigkeit nach deutschem Recht sanktioniert und kann darüber hinaus für das Unternehmen weitergehende Nachteile mit sich bringen.

a) Straftaten und Ordnungswidrigkeiten

Nach deutschem Recht ist nach § 18 Abs. 1 Nr. 1 AWG die Einhaltung des Bereitstellungsverbots und des Verfügungsverbots über eingefrorene Gelder (Art. 3 Abs. 1, 2 VO) strafbewährt, und zwar mit einer Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Wird hiergegen fahrlässig verstoßen, kann ein Ordnungswidrigkeitentatbestand nach § 19 Abs. 1 AWG verwirklicht werden. Die Geldbuße kann dann bis zu 500.000 Euro betragen.

Ordnungswidrig handelt im Übrigen auch, wer eine Information nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt bzw. eine zuständige Behörde nicht oder nicht rechtzeitig unterrichtet; insoweit ist auch der Verstoß gegen die erwähnte Mitteilungspflicht nach Art. 8 VO sanktioniert.

Im Ordnungswidrigkeitenrecht ist darüber für den Bereich der Exportkontrolle auch die Aufsichtspflichtverletzung nach § 130 OWiG relevant. Danach können Inhaber eines Betriebs oder ihnen gleichgestellte Personen, wie z. B. Betriebsleiter oder Prokuristen mit einer Geldbuße belegt werden, wenn sie es fahrlässig oder vorsätzlich unterlassen haben, Maßnahmen zur Verhinderung betriebsbezogener

Verstöße zu ergreifen. Dazu kann es beispielsweise gehören, kein wirksames internes Kontroll- und Compliance-Managementprogramm installiert zu haben.

Darüber hinaus kann nach § 30 OWiG auch gegen das Unternehmen selbst eine empfindliche Geldbuße verhängt werden, wenn eine Leitungsperson eine Straftat oder Ordnungswidrigkeit begangen hat. Eine solche Ordnungswidrigkeit kann auch in einer Aufsichtspflichtverletzung nach § 130 OWiG bestehen. Die Unternehmensgeldbuße kann im Fall einer vorsätzlich begangenen Straftat bis zu 10 Mio. Euro betragen, bei fahrlässiger Begehung bis 5 Mio. Euro. Bei einer Ordnungswidrigkeit bestimmt sich das Höchstmaß der Geldbuße nach dem für die Ordnungswidrigkeit angedrohten Höchstmaß, kann sich allerdings verzehnfachen, wenn der Ordnungswidrigkeitentatbestand auf § 30 OWiG verweist (wie dies z. B. bei § 130 OWiG der Fall ist).

Darüber hinaus kann die Einziehung dessen, was durch oder für die Tat erlangt wurde, durch das Gericht angeordnet werden. Dies kann unter bestimmten Voraussetzungen die vollständigen Verkaufserlöse – und nicht nur den Gewinn – umfassen. Schließlich können sich für das Unternehmen bei einem Verstoß weitere Nachteile ergeben: So können Vereinfachungen im Zollrecht ausgesetzt oder widerrufen werden oder das Unternehmen wird – mit allen Konsequenzen für weitere Verwaltungsverfahren – in das Gewerbezentralregister eingetragen.15

b) Haftungsmaßstab und Haftungserleichterungen

Die Cyberangriffs-Verordnung sieht eine Haftungserleichterung vor, die sich vor allem auf mögliche Ersatzansprüche von Geschäftspartnern bei nichtzutreffender Berufung der Anwender auf die Beschränkungen der Verordnung bezieht. Die handelnden Personen können nämlich nicht in Anspruch genommen werden, wenn sie in gutem Glauben Gelder bzw. wirtschaftliche Ressourcen eingefroren oder nicht bereitgestellt haben (Art. 10 Abs. 1 VO). In diesem Fall können sie beispielsweise für eine fälschlicherweise erfolgte, verweigerte Vertragserfüllung nicht haftbar gemacht werden – auch wenn objektiv ein Grund zur Erfüllungsverweigerung gegenüber dem Geschäftspartner gar nicht vorgelegen hat. Dies gilt allerdings dann nicht, wenn das Einfrieren oder das Zurückhalten der Gelder bzw. wirtschaftlichen Ressourcen auf Fahrlässigkeit beruhte. Um also Ersatzansprüche durch Geschäftspartner zu vermeiden, ergibt sich die Notwendigkeit wirksamer betriebsinterner Vorkehrungen und Prozesse, um eine fahrlässig fälschliche Anwendung der Cyberangriffs-Verordnung zu vermeiden.

Eine ähnliche Haftungserleichterung gilt mit Blick auf die Verwirklichung der genannten Sanktionstatbestände: Die Anwender der Verordnung können für Handlungen nicht haftbar gemacht werden, wenn sie nicht wussten oder vernünftiger Weise nicht wissen konnten, dass sie gegen die Verordnung verstoßen (Art. 10 Abs. 2 VO). Dies bedeutet aber auch: Eine Haftung scheidet nur dann aus, wenn trotz Prüfung in der Regel im Rahmen des internen Compliance-Managementprogramms keine Anhaltspunkte dafür bestehen, dass beispielsweise Leistungen an einen Geschäftspartner mittelbar einer gelisteten Person oder Organisation zugutekommen.

V. Bewertung

Den vergleichsweise neuen Herausforderungen durch grenzüberschreitende Cyberangriffe begegnet die EU mit traditionellen Instrumentarien: Das Verbot, identifizierten Angreifern Vermögenswerte zur Verfügung zu stellen und das Einfrieren ihrer Vermögenswerte.

Ob diese Mittel allerdings geeignet sind, wird sich in Zukunft erst erweisen müssen. Zweifel daran sind berechtigt. Denn anders als bei den länderbezogenen Sanktionsverordnungen sind die zu sanktionierenden Personen, Einrichtungen und Organisationen im Bereich der Cyberangriffe nicht ohne Weiteres leicht auszumachen. Dies gilt umso mehr, als dass der Rat der EU die zu listenden Personen bzw. Organisationen nicht nur identifizieren muss, sondern dann auch eine Verbindung zum Cyberangriff nachweisen und bei der Aufnahme auf die Liste in Anhang I der Verordnung eine entsprechende Identifizierung und Begründung liefern muss. Dabei dürfte schon das Führen des entsprechenden Nachweises bei den naturgemäß verdeckt operierenden und alle technischen Möglichkeiten der Verschleierung nutzenden Organisationen sehr schwierig sein. Das zeigt nicht zuletzt die Verfolgung der eingangs erwähnten Cyberangriffe gegen den Deutschen Bundestag bzw. die WADA. Fünf Jahre haben die Ermittlungen gedauert, bevor im Mai 2020 ein Haftbefehl gegen einen mutmaßlichen russischen Geheimdienstagenten, der beim Militärgeheimdienst GRU der Hacker-Einheit APT28 angehören soll, ergehen konnte.

Die Aufnahme von Personen oder Organisationen in den Anhang der Verordnung muss den hohen formalen (und inhaltlichen) Anforderungen genügen, die die europäischen Gerichte in jüngerer Vergangenheit entwickelt und verschärft haben. So hat der Rat eine Pflicht zur Prüfung, er muss sich vergewissern, dass die Voraussetzungen einer Listung vorliegen. Darüber hinaus muss er die Aufnahme begründen, insbes. auch mit Blick auf die Wahrung der Verfahrens- und Grundrechte der Betroffenen.16 Diese hohen Anforderungen werden den Rat gerade im Bereich verdeckter Cyberangriffe vor große Herausforderungen stellen.

Ob die Verordnung deshalb tatsächlich zu einer wirksamen Sanktionierung erfolgter Angriffe und zu einer möglichen Abschreckung zukünftiger Angriffe wirkungsvoll beitragen kann, bleibt deshalb abzuwarten.

Autor

Dr. André Lippert, RA, Salary Partner bei Taylor Wessing in Berlin, berät im öffentlichen Wirtschaftsrecht in allen Fragen regulatorischer Compliance. Er unterstützt Unternehmen verschiedener Branchen bei der Einhaltung und Umsetzung aller regulatorischen Anforderungen, insbesondere im Umwelt-, Bau-, Planungs- und Produktrecht.

Fußnoten

1) Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (Cyberangriffs-Verordnung, Cyberangriffs-VO oder auch nur VO).

2)

BfV, Nachrichtendienstlich gesteuerte Cyberangriffe, Mai 2018.

3) Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2019, Oktober 2019.

4) Bundesministerium des Inneren, für Bau und Heimat, Referentenentwurf Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), 7. 5. 2020.

5) Bundesministerium des Inneren, für Bau und Heimat, Referentenentwurf Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), 7. 5. 2020.

6) Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union.

7) *Lippert*, BB 2019, 1538; *Lippert*, ZollProfi, Juni 2019, Seite 6.

8) Vgl. beispielsweise Art. 2 Verordnung (EU) 2018/1542 des Rates vom 15. Oktober 2018 über restriktive Maßnahmen gegen die Verbreitung und den Einsatz chemischer Waffen; Art. 2 Verordnung (EU) Nr. 208/2014 des Rates vom 5. März 2014 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in der Ukraine.

9) Verordnung (EU) Nr. 267/2012 des Rates vom 23. März 2012 über restriktive Maßnahmen gegen Iran.

10) Vgl. nur Verordnung (EG) Nr. 208/2014 des Rates vom 5. März 2014 (*) über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in der Ukraine.

11) Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus.

12) Rat der EU, Sanktionsleitlinien – Aktualisierung, 8. 12. 2017, 15598/17.

13) Dazu auch *Niestedt*/*Krause*, CB 2015, 152 ((153 f.).

14) Vgl. dazu nur BAFA, Firmeninterne Exportkontrolle, März 2018; *Wolffgang*/*Witte*, CB 2015, 138.

15) *Pfeil*/*Mertgen*, Compliance im Außenwirtschaftsrecht, 2016, Seite 202 ff.; *Niestedt*/*Krause*, CB 2015, 152 ((155).

16) EuGH, Urt. v. 26. 7. 2017 – C-599/14 P (ECLI:EU:C:2017:583); EuGH, Urt. v. 19. 12. 2018 – C-530/17 P – Azarov/Rat (ECLI:EU:C:2018:1031); *Egger*, EuZW 2019, 326.