Cyber-Security und Kartellrecht – aus Fehlern lernen

9. August 2019

Wettbewerbskommissarin Margrethe Vestager wandte sich kürzlich mit einer öffentlichkeitswirksamen Warnung an Automobilbauer, gegen die wegen Kartellabsprachen im Zusammenhang mit dem Abgas-Skandal ermittelt wird. Diese Warnung könnte auch für Unternehmen gelten, die im Bereich der Cyber-Security kooperieren wollen. Automobilbranche und Cyber-Security? Auf den ersten Blick mag es verblüffen, Parallelen zwischen einer der traditionsreichsten Industrien und dem vergleichsweise jungen und abstrakten Gebiet der Cyber-Security zu ziehen. Doch beide Bereiche stehen vor disruptiven technischen Herausforderungen, die Unternehmen nur gemeinsam bewältigen können. Aus den jüngsten Erfahrungen des Automobilsektors lassen sich hilfreiche Lehren auch über die Branche hinweg ziehen.

Cyber-Security: Nur gemeinsam stark?

Digitalisierung, das Internet of Things (IoT) und eine Vielzahl neuer digitaler Technologien bergen erhebliche Chancen für nahezu sämtliche Industrien, aber auch neue Herausforderungen im Bereich Cyber-Security. Die Kosten von Cyberangriffen für die Weltwirtschaft belaufen sich bereits heute auf jährlich rund EUR 400 Mrd. Während künftig zwar auch staatliche Interventionen und Standards eine Rolle spielen werden – etwa das geplante EU-weite Zertifizierungssystem für Cybersicherheit – tragen Wirtschaftsteilnehmer einen Großteil der Kosten für Cyber-Security selbst. Es liegt nahe, dass Unternehmen das Thema gemeinsam angehen, um die immensen Kosten für Cyber-Security auf viele Schultern zu verteilen. Auch die schiere Anzahl von Milliarden vernetzter digitaler Geräte innerhalb der EU machen eine Kooperation von Herstellern unumgänglich, um Sicherheit und Interoperabilität zu gewährleisten.

Die Notwendigkeit einer solchen Zusammenarbeit wird mehr und mehr erkannt: Partner aus Wirtschaft, Politik und Wissenschaft haben im Februar 2018 die Initiative „Charter of Trust“ ins Leben gerufen. Über die gesamte Wertschöpfungskette sollen Mindeststandards festgelegt und die gemeinsame Forschung im Bereich der Cyber-Security vorangetrieben werden. Auch das Unternehmen Huawei macht sich derzeit öffentlichkeitswirksam für gemeinsame Cyber-Security Standards im Telekommunikationsbereich stark. Und auf dem Internet Governance Forum Ende 2018 in Paris unter dem Motto „Internet of Trust“ griff zuletzt der französische Staatspräsident Emmanuel Macron die Notwendigkeit einer besseren Vernetzung aller Wirtschaftsteilnehmer im Kampf gegen Cyber Kriminalität auf: „[...] *we need to invent – innovate – new forms of multilateral cooperation that involve not only states, but also all of the stakeholders you represent.*“

Verstärkte Kooperationen im Bereich Cyber-Security sollen Informationsasymmetrien gegenüber Angreifern kompensieren und typische Angriffsmuster identifizieren. Dynamische Risiken wie Datendiebstahl, Phishing, Erpressung, Industriespionage und Sabotage erfordern oft gemeinsame Lösungen. Doch kann die Kooperation selbst zum Risiko werden?

Das mahnende Beispiel der Automobilbranche

Es lohnt ein vergleichender Blick auf die Automobilbranche, die seit längerem ebenfalls vor Herausforderungen steht, die sie nur kooperativ bewältigen kann. Vor allem steigende Umweltschutz-Standards erfordern neuartige Konzepte, die sich oft nur branchenweit umsetzen lassen. Wettbewerber haben hier schnell die Notwendigkeit von Kooperationen begriffen. Ihr Beispiel zeigt jedoch deutlich, dass Unternehmen sich bereits vor einer Zusammenarbeit die kartellrechtlichen Grenzen veranschaulichen sollten.

Kartellverfahren der jüngeren Vergangenheit verdeutlichen, dass gerade vermeintlich rein technische Kooperationen von Wettbewerbern das Risiko bergen, wettbewerbswidrige Absprachen zu begünstigen: Eine Vielzahl von Verfahren gegen Automobilzulieferer wurde schon mit Bußgeldern im dreistelligen Millionenbereich beendet. Aktuell wirft die Europäische Kommission namhaften deutschen Automobilherstellern vor, jahrelang gegen EU-Kartellrecht verstoßen zu haben. In einem als „Fünferkreis“ bezeichneten Arbeitskreis erörterten die Hersteller technische Themen wie gemeinsame Qualitätsanforderungen und Prüfverfahren sowie den Austausch technischer Expertise und die Bündelung von Entwicklungsanstrengungen im Bereich Fahrzeugsicherheit. Unter dem Stichwort Umweltschutz diskutierten die Hersteller außerdem, wie technische Lösungen zur Abgasreinigung implementiert werden könnten. Gerade Letzteres könnte ihnen nun zum Verhängnis werden.

Die Europäische Kommission wirft den Herstellern in einem laufenden Verfahren vor, gegen EU-Kartellrecht verstoßen zu haben. Sie sollen sich darauf verständigt haben, den Wettbewerb bei der Entwicklung von Technologien zur Reinigung der Emissionen von Diesel- und Benzin-Pkw einzuschränken. Nun wird geprüft, ob die mutmaßlichen Kartellanten Verbrauchern die Möglichkeit verwehrt haben, umweltfreundlichere Fahrzeuge zu kaufen, obwohl entsprechende Technologien längst verfügbar waren.

Wie führt der Bogen nun zurück auf Wettbewerber, die im Bereich Cyber-Security kooperieren wollen? Um nicht in den Verdacht einer Kartellabsprache zu geraten, sollten auch sie sich die eingangs zitierte Warnung von Margrethe Vestager zu Herzen nehmen: „Unternehmen können auf viele Arten zusammenarbeiten, um die Qualität ihrer Produkte zu verbessern. Die EU-Wettbewerbsvorschriften verbieten ihnen jedoch, Absprachen zu treffen, die genau das Gegenteil bewirken sollen, nämlich ihre Produkte nicht zu verbessern und bei der Qualität nicht miteinander in Wettbewerb zu treten.“

Cyber-Security-Entwicklung: Was es zu beachten gilt

Gemeinsame Forschung und Entwicklung kann effizienzsteigernd sein und wird deshalb kartellrechtlich privilegiert. Durch Kooperationen im Bereich Cyber-Security könnten Marktteilnehmer Synergieeffekte nutzen, Innovationskraft bündeln und die Marktreife neuer Lösungen schnell vorantreiben.

Beschränkt sich die Zusammenarbeit aber nicht auf die reine Forschung und Entwicklung neuer Sicherheitsprodukte, -standards oder -strategien, kann sie wettbewerbsrechtlich kritisch sein. Die Grenzen zwischen wettbewerbsfördernden Forschungs- und Entwicklungsvereinbarungen für völlig neue Produkte und ihre Nutzung zur kartellrechtswidrigen Verhaltensabstimmung oder zur Abschottung von Schlüsseltechnologien sind mitunter fließend.

In der Praxis erstrecken sich Kooperationen regelmäßig auf die Verwertung der Forschungsergebnisse durch gemeinsames Marketing, Lizensierung oder Produktion. Vor allem unter Wettbewerbern erfordert dies eine sorgfältige kartellrechtliche Prüfung. Welche Marktanteile halten die Kooperationspartner? Wem und zu welchen Konditionen wird Zugang zum gewonnenen Know-how gewährt? Ist eine eigene Parallelforschung erlaubt? Wird (potentieller) Wettbewerb beeinträchtigt? Ist gar eine unzulässige Marktverschließung zu befürchten? Oder stehen effizienzsteigernde Effekte im Vordergrund, die eine gemeinsame Forschung und Vermarktung ermöglichen?

Kooperationspartner sollten Forschungs- und Entwicklungsvorhaben schon im Vorfeld kartellrechtlich überprüfen. Auch sollten sie bereits vor Kooperationen robuste Compliance-Systeme etablieren. Nur so können sie sicherstellen, dass kartellrechtlich zulässige Zusammenarbeit nicht im Lauf der Zeit zu einer unzulässigen Verhaltensabstimmung wird.

Neue Technologien und Standards: Wie Unternehmen Fallstricke vermeiden

Bestenfalls führt eine kartellrechtlich zulässige Zusammenarbeit dann zu neuen Schlüsseltechnologien und innovativen technischen Standards für Cyber-Security. Das Beispiel der Automobilhersteller zeigt jedoch, dass auch hier große Risiken liegen. Werden Standards oder Schlüsseltechnologien branchenweit oder entlang der gesamten Wertschöpfungskette etabliert, ist trotz Innovationsgewinnen regelmäßig Vorsicht geboten.

Vereinheitlichte Sicherheitsstandard können etwa den Anreiz für Innovation und Weiterentwicklung hemmen. Eine marktweit etablierte Schlüsseltechnologie kann Entwicklern anderer Technologien den Zutritt zum Markt verwehren. Das Risiko einer solchen Marktverschließung steigt weiter, wenn technische Spezifizierungen vereinheitlicht werden, für die Patente oder sonstige geistige Eigentumsrechte

bestehen. Ohne Zugang zu den relevanten Technologien könnten Wettbewerber gänzlich vom Wettbewerb ausgeschlossen werden.

Wettbewerbsverstöße können in der Praxis am ehesten durch Transparenz vermieden werden. Auch sollten alle betroffenen Unternehmen die Möglichkeit erhalten, bereits bei der Festlegung eines Cyber-Security-Standards mitzuwirken und Alternativtechnologien vorzuschlagen. Wenn Wettbewerber nicht auf alternative Technologien ausweichen können, verlangt das Kartellrecht unter bestimmten Voraussetzungen, dass allen Marktteilnehmern gleichberechtigter Zugang zum Standard gewährt wird. Der Rechteinhaber muss sich dann verpflichten, die Sicherheitstechnologie zu fairen, zumutbaren und diskriminierungsfreien Bedingungen zu erteilen (sogenannte FRAND-Selbstverpflichtung). Auf diesem Weg können dritte Unternehmen Zugangsansprüche zu essentiellen Technologien auch gegen mächtigere Wettbewerber durchsetzen. Ob ein solcher Anspruch besteht, erfordert eine dezidierte Einzelfallprüfung. Erfasst der Zugangsanspruch überdies Datensammlungen – im Bereich Cyber-Security nicht ganz unwahrscheinlich –, müssen Unternehmen kartellrechtliche und datenschutzrechtliche Vorgaben in Einklang bringen.

Ausblick

Die Erfahrungen des Automobilsektors zeigen, wie wichtig es für Unternehmen ist, technische Kooperationen mit Wettbewerbern schon vorab gut vorzubereiten. Beim Kampf gegen Cyberbedrohungen sollten sie rechtliche Anforderungen immer im Blick behalten und neben ihrer Sicherheitsinfrastruktur kartellrechtliche Compliance-Strukturen sorgfältig überprüfen. Kooperationen bergen insofern eine Vielzahl kartellrechtlicher Herausforderungen – selbst wenn sie (vermeintlich) auf Innovationsgewinne ausgelegt sind. Zuletzt sollten Unternehmen auch die geplante 10. GWB-Novelle im Auge behalten, die kartellrechtliche Zugangsansprüche zu sicherheitsrelevanter Technologie weiter begünstigen und die kartellrechtliche Interventionsschwelle im Digitalbereich spürbar senken könnte.

BLOMSTEIN wird die weiteren Entwicklungen beobachten und darüber informieren. Wenn Sie Fragen zu den potenziellen Auswirkungen der Cyber-Security auf Ihr Unternehmen oder Ihre Branche haben, stehen Ihnen Dr. Anna Huttenlauch, Dr. Max Klasse und Philipp Trube jederzeit gern zur Verfügung.