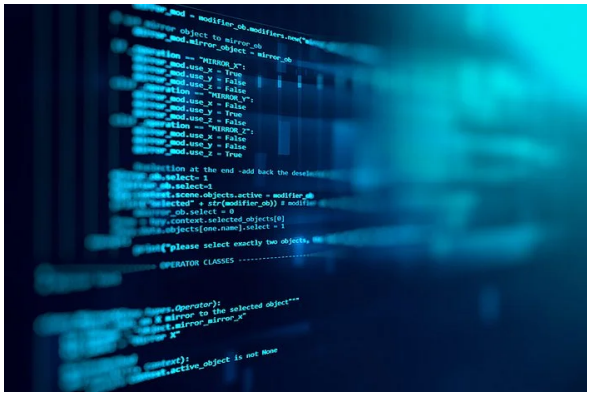
FACHBEITRAG | Update Datenschutz Nr. 48

Der Cybersecurity Act – Wohin steuert Europa in Fragen der Cybersicherheit?

Dr. Hans Markus Wulf



14.12.2018 – I. Einleitung

Laut einer Studie der Bitkom aus September 2018 ist der deutschen Industrie in den vergangenen beiden Jahren durch Cyberangriffe ein Gesamtschaden von 43 Milliarden Euro entstanden. Sieben von zehn Industrieunternehmen sind in diesem Zeitraum Opfer entsprechender Angriffe geworden. Auf EU-Ebene wurde zuletzt verstärkt darüber diskutiert, wie man dieser aufziehenden Gefahr begegnen kann.

Am 10.12.2018 haben sich nun das Europäische Parlament, der Europäische Rat und die Europäische Kommission politisch über einen Rechtsakt zur Cybersicherheit geeinigt. Die Verordnung über die EU-Cybersicherheitsagentur (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cyberrisiken von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“) wird im Wesentlichen von zwei Gedanken getragen:

- Die EU-Sicherheitsagentur (ENISA – Agentur der Europäischen Union für Netz- und Informationssicherheit) erhält ein nunmehr dauerhaftes und stärkeres (über das Jahr 2020 hinausgeltendes) Mandat zwecks Unterstützung der Mitgliedsstaaten im Umgang mit Cyberangriffen.
- Es wird eine gemeinschaftsrechtlich geltende Cybersicherheitszertifizierung (europäischer Zertifizierungsrahmen) von Produkten, Verfahren und Diensten geschaffen.

Nachfolgend soll ein Überblick zu den wesentlichen Inhalten der Verordnung gegeben werden, ergänzt um aktuelle Informationen zur neuen Agentur für Cybersicherheit.

II. Wesentliche Inhalte der Verordnung

1. Konformitätsbewertung (EU-Zertifizierungsrahmen)

Die Verordnung sieht zunächst eine sogenannte „Konformitätsbewertung“ vor, also einen EU-weit geltenden europäischen Zertifizierungsrahmen für die Cybersicherheit von Produkten, Diensten und Verfahren, ähnlich der ISO/IEC 17000:2004. Dem EU-Bürger ist dieses Verfahren von definierten Mindeststandards und deren Überprüfung bereits aus den Bereichen der allgemeinen Produktsicherheit bekannt. Die Verordnung richtet sich mit der angedachten Konformitätsbewertung im Kern ebenfalls auf die Harmonisierung von Sicherheitsstandards. Ziel ist insoweit die Überprüfbarkeit der Einhaltung von festgelegten Cybersicherheitsmerkmalen bezogen auf Produkte, Dienste und Verfahren durch die zuständige Stelle.

2. Mindestsicherheitsstandards bzw. Leitlinienkompetenz der ENISA

Der ENISA fällt nunmehr die wichtige Rolle zu, Leitlinien zur Sicherung eines Mindeststandards für Im- und Exporte von IT-Produkten über die europäische Grenze aufzustellen. In dieser Leitlinienkompetenz ähnelt ENISA dann dem BSI (§ 8 Abs. 1 BSIG) mit dem wesentlichen Unterschied, dass die Adressaten nicht nur Stellen des Bundes, sondern auch Unternehmen sind. Dabei soll das Vertrauen der EU-Bürger in IT-Produkte dieser Unternehmen durch eine ganze Reihe von Maßnahmen gefestigt werden. So müssen bspw. die Hersteller dieser IT-Produkte schriftliche Erklärungen dahingehend abgeben, dass

- weder Hardware noch Software bekannten Sicherheitslücken enthalten,
- es zu keinem Einsatz von unveränderbaren bzw. unverschlüsselbaren Passwörtern bzw. Zugangsdaten kommt, die einem authentifizierten Sicherheitsupdate entzogen sind,
- bei dem betroffenen Gerät eine angemessene Rangfolge von Abhilfemaßnahmen vorgesehen ist und
- die Unterstützung bzw. der Support für den Endkunden zu einem individuell mitgeteilten Zeitpunkt endet.

Untrennbar mit dieser Aufstellung von Mindeststandards durch die ENISA ist die stetige Implementierung der Sicherheitsaspekte bei Schaffung von Software (Security by Design) und dem damit korrelierenden technischen Datenschutz (Privacy by Design) verbunden. Nicht zuletzt deshalb sollen sämtliche IT-Sicherheitsanforderungen des nunmehr europäischen Zertifizierungssystems während der verschiedenen Phasen von der

Markteinführung eines IT-Produkts bis hin zu dessen Herausnahme vom Markt (sog. Produkt- bzw. Dienstlebenszyklus) durch die jeweils eingebundenen Akteure umgesetzt werden. Festzuhalten bleibt, dass es sich bei der Verordnung um die erste Binnenmarktvorschrift handelt, die die Sicherheit von vernetzten Produkten mithilfe solcher Zertifikate steigern wird.

Als wichtig wird auch der richtige Umgang mit Backdoors in IKT-Produkten eingestuft. Als Backdoor bezeichnet man denjenigen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. Um diese Umgehungstatbestände zu verhindern, soll ENISA durch eine Kompetenzerweiterung mit nationalen Zertifizierungsbehörden zusammenarbeiten und entlang der fünf Kernprinzipien (d.h. geringstes Privileg, Mikro-Segmentierung, Verschlüsselung, Multi-Faktor-Authentifizierung und Patching) Cyberhygiene- Verfahren entwickeln, um mögliche Schwachstellen zu schließen.

3. Unterschiedliche IT-Sicherheitsstufen für IKT-Produkte

Getragen von dem Gedanken, die unterschiedlichen Anforderungen durch internationale und nationale IT-Sicherheitszertifizierungen aufzuheben, soll die ENISA homogene Sicherheitsstufen für IKT-Produkte und -Dienste schaffen. Für die jeweilige Cybersicherheitszertifizierung wird dann das einzelne IKT-Produkt bzw. der -Dienst einer dieser Sicherheitsstufen zugeordnet. Dies impliziert die mögliche Umgruppierung bzw. Umbenennung bisheriger Stufen. Künftig sollen drei Sicherheitsstufen Anwendung finden:

- Erste Stufe: Funktional sicher, impliziert ein angemessenes Maß an Vertrauen in die IT-Sicherheit (niedrigstes Sicherheitsniveau)
- Zweite Stufe: Im Wesentlichen sicher, meint ein mittleres Maß an Vertrauen
- Dritte Stufe: Äußerst sicher, impliziert ein erhöhtes Maß an Vertrauen in die Sicherheit (höchstes Sicherheitsniveau)

Eine weitergehende Ausdifferenzierung der Sicherheitsstufen, ähnlich der DIN 66 33 99 mit ihren sieben Sicherheitsstufen, ist denkbar.

Die ENISA wird schließlich Checklisten führen und öffentlich zur Verfügung stellen, um das Cyberrisiko des jeweiligen IKT-Produkts und -Dienstes vorab einschätzen zu können.

4. Priority-List: IKT-Produkte und -Dienste werden künftig von ENISA priorisiert

Der ENISA soll aufgrund ihrer künftig immer zentraler werdenden Funktion die Aufgabe zukommen, die Cybersicherheitszertifizierung für IKT-Produkte und -Dienste in Form einer fortwährend aktualisierten Liste zu priorisieren (Priority-List). Aus dieser soll ersichtlich werden, welches Produkt bzw. welche Dienstleistung auf einer Skala der Notwendigkeit ganz oben steht. Dabei arbeitet die ENISA mit der ständigen Dialoggruppe der Interessenvertreter und der Europäischen Gruppe für Cybersicherheitszertifizierung (die wiederum aus den nationalen Zertifizierungsbehörden besteht) und sonstigen Stellen zusammen.

5. Der Schulterschluss: ENISA bezieht künftig den Datenschutz (EU-DSGVO) ein

Bis dato wurden Cybersicherheit und Datenschutz überwiegend getrennt voneinander betrachtet. Um dieser Praxis entgegenzuwirken, wird zunächst das Mandat der ENISA auch auf die Entwicklung und Umsetzung des europäischen Datenschutzes ausgedehnt. Ziel ist es, dass ENISA die europäische Datenschutzbehörde bei deren Leitlinienerstellung berät, insbesondere im technischen Bereich. Denn diese Leitlinien regeln die notwendige Nutzung von personenbezogenen Daten zu IT-Sicherheitszwecken und damit einen Kernbereich, den es fortan vor dem Hintergrund eines gemeinsamen Ziels besser abzustimmen gilt. Deshalb soll die ENISA neben Daten zu Cybersicherheits-Attacken auch Daten zu den Datenschutzverletzungen bündeln und künftig zu beiden Themen Empfehlungen abgeben. Da Sicherheitsvorfälle in der IT nicht nur aus Machine-to-Machine-Kommunikation (M2M) herrühren, sondern ebenso denkbar ihren Ursprung in einer Datenschutzverletzung nach der DSGVO haben, werden künftig auch große Datenpannen (sog. Data Breaches) auf einem eigenen europäischen Portal der ENISA protokolliert.

III. Deutsche Unabhängigkeit: Agentur für Cybersicherheit in Vorbereitung

Vor dem Hintergrund der weltweit zunehmenden Bedrohungslage durch Cyberangriffe auf Staaten und deren Infrastrukturen (etwa durch digitale Konfliktszenarien wie hybride Kriegsführung, Cyber-Spionage oder Cyber-Kriminalität) und losgelöst vom europäischen Cybersecurity Act, hat die Bundesregierung dem Sicherheitsbedürfnis der Infrastruktur Deutschlands durch die Gründung einer Agentur für Cybersicherheit Rechnung getragen.

Die neu geschaffene Agentur für Innovation in der Cybersicherheit wird ihre Arbeit mit Beginn des Jahres 2019 aufnehmen und dabei innerhalb der nächsten fünf Jahre auf ein (Forschungs-)Budget von immerhin € 200 Mio. zugreifen können. Wo der Sitz dieser noch 2018 in der Rechtsform einer GmbH zu gründenden Agentur mit einer Zielgröße von 100 Mitarbeitern letztlich sein wird, ist noch offen).

Das Arbeitsziel der Agentur wird es sein, Cybersicherheits- und Schlüsseltechnologien der Inneren und äußeren Sicherheit mit hohem Innovationspotential zu ermitteln und zu unterstützen. An Technologien, die der inneren und äußeren Sicherheit dienen, hat der Bund ein hohes Interesse und so verwundert es nicht, dass das ganze Projekt der Agentur für Cybersicherheit ressortübergreifend geprägt ist, insbesondere durch das Bundesministerium für Verteidigung und das Bundesministerium des Inneren

IV. Die deutsche Antwort auf eine Cyber-Attacke: Gedanken zum Hack-Back

Schließlich wird derzeit auf Bundesebene diskutiert, ob es nicht der „technologischen Waffengleichheit“ entsprechen würde, wenn man zum Gegenangriff auf einen Eindringling im Datennetz ausholen könnte und dies auch rechtlich dürfte. Diese Form des Gegenschlags wird unter Fachleuten „Hack-Back“ genannt. Technisch sind sowohl Bundeswehr als auch BND hierzu in der Lage. Derzeit fehlen allerdings für einen

solchen Gegenschlag noch die Exekutivbefugnisse. Die Bundesregierung prüft daher aktuell Möglichkeiten, derartige Rechtsgrundlagen zu schaffen.

V. Fazit

Der neue EU-Cybersecurity-Act, also die Verordnung über die EU-Cybersicherheitsagentur (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cyberrisiken von Informations- und Kommunikationstechnik, ist ein richtiger Schritt zur effektiven Abwehr von Cyberangriffen. Insbesondere Hersteller von IT-Produkten werden sich dem Thema nähern müssen, denn zukünftig gilt für bestimmte Bereiche eine Zertifizierungspflicht. Diesbezüglich bietet der neue Zertifizierungsrahmen insbesondere für kleine und mittlere Unternehmen (KMU) Vorteile, denn zukünftig wird die Einholung von nationalen Einzel-Zertifikaten obsolet, es gibt dann ein EU-weiteres Zertifizierungssystem.

Für den EU-Bürger bedeutet die Verordnung, dass sie ihren täglich genutzten Geräten mehr Vertrauen können, da es künftig eine Auswahl an Produkten geben wird, deren Cybersicherheit EU-zertifiziert wurde.
Unternehmen, die bereits vor Inkrafttreten des EU-Cybersecurity-Act ihre eigene IT-Sicherheit im Betrieb erhöhen möchten, könnten folgende Maßnahmen in Erwägung ziehen:

- Nutzen Sie Security Awareness Trainings mit dem Ziel der Sensibilisierung Ihrer Mitarbeiter für das Thema „Computersicherheit“ und proben Sie Ablaufpläne zum Deaktivieren von Zugangsberechtigungen
- Räumen Sie Mitarbeitern, Führungskräften und der Geschäftsleitung selbst nur Zugriffe auf das Nötigste ein, denn jeder dauerhafte Zugriff ist im Umkehrschluss ein Sicherheitsrisiko im Falle eines Angriffs auf den Zugriffsberechtigten
- Führen Sie die Trennung von Netzen ein, d.h. Sachbearbeiter und Produktionsmaschinen sollten nicht im gleichen Netz sein. Es empfiehlt sich zu separieren, soweit es geht
- Klären Sie ab, wie Ihre Firewall konfiguriert wurde. Für Internetzugriffe sollte sie auf „streng“ gesetzt werden, denn normale Nutzer müssen z.B. keine ausführbaren Dateien herunterladen können
- Minimieren Sie die externen Zugänge bzw. schaffen Sie eine starke Authentifizierung (bspw. 2-Faktor-Authentifizierung)
- Nutzen Sie APT Technologien (d.h. Daten werden in einer Sandbox zur Analyse ausgeführt)
- Nutzen Sie IDS-Systeme, d.h. Angriffsmuster werden erkannt und zeitlich befristet ausgesperrt
- Führen Sie Geolocation ein, d.h. lassen Sie Verbindungen aus Netzen anderer Länder nicht zu, mit denen Sie auch keine Handelsbeziehungen pflegen; beachten Sie hierbei jedoch die neue EU-Geoblocking-Verordnung
- Betreiben Sie Monitoring, also die Überwachung von Vorgängen. Erfolglose Login-Versuche deuten beispielsweise auf einen gerade stattfindenden oder stattgefundenen Cyber-Angriff hin.
- Nutzen Sie Endpoint Detection and Response Methoden (EDR).

Wir danken Herrn RA Sebastian B. Jürgensen für die Mitarbeit an diesem Beitrag. Er ist Syndikusanwalt einer mittelständischen Unternehmensgruppe in Hamburg.

Ansprechpartner

Dr. Hans Markus Wulf
PARTNER

Inhalte online lesen und teilen

Auf unserer Website veröffentlichen wir regelmäßig Inhalte zu den aktuellen Rechtsthemen. Scannen Sie den QR-Code um diesen Beitrag online zu öffnen.