MMR FOKUS

Dennis-Kenji Kipker **Massiver Ausbau der EU-Cyber-Sicherheitskapazitäten – Jahresansprache 2017 des EU-Kommissionspräsidenten Juncker und Veröffentlichung der neuen europäischen Cyber-Sicherheitsstrategie** MMR-Aktuell 2017, 394677

Im Rahmen seiner Jahresansprache an das *EU-Parlament* widmete sich der EU-Kommissionspräsident, *Jean-Claude Juncker*, in besonderem Maße dem Thema Cybersicherheit. Ziel sei es laut *Juncker* nicht nur, die bisherige europäische Cyber-Sicherheitspolitik, die in wesentlichen Teilen auf der Cyber-Sicherheitsstrategie von 2013 basiert, zu erneuern, sondern ebenso den digitalen Binnenmarkt vor Cyberbedrohungen zu schützen.

Insbesondere hob der *Kommissionspräsident* hervor, dass Cyberangriffe in den Mitgliedstaaten eine größere Bedrohung für die Demokratie und die Wirtschaft darstellten, als dies für konventionelle Angriffsmittel der Fall sei. Dementsprechend und gerade auch auf Grund der Cyberangriffe in Europa im Jahr 2017 wie „WannaCry" und „Petya" sei es erforderlich, auf politischer Ebene rasch zu handeln. So hätten Statistiken gezeigt, dass es zurzeit mehr als 4.000 Vorfälle von Ransomware-Angriffen pro Tag gebe, und 80% der in der EU angesiedelten Unternehmen hätten im Jahr 2016 zumindest einen Cyber-Sicherheitsvorfall zu verzeichnen gehabt. Dies mache mehr als deutlich, dass niemand gegen Cyberangriffe immun sei, so *Juncker*.

Nachdem Kritiker noch im Sommer 2017 angenommen hatten, dass die lang angekündigte Novellierung der Cyber-Sicherheitsstrategie der EU sicher noch auf sich warten lassen würde, wurden unmittelbar an die Rede des *Kommissionspräsidenten* anknüpfend gleich mehrere Dokumente von Seiten der *EU-Kommission* veröffentlicht, hierunter ein Vorschlag zur Umstrukturierung der europäischen IT-Sicherheitsbehörde *ENISA*, ein Plan zur europaweiten Zertifizierung des IT-Sicherheitslevels von Soft- und Hardware sowie die Neufassung der mittlerweile in die Jahre gekommenen Cyber-Sicherheitsstrategie der EU.

Umfassende Umstrukturierung der ENISA

Die Umstrukturierung der *ENISA* wird voraussichtlich umfassend sein: So soll nicht nur das derzeitige Personal von 84 auf 124 Mitarbeiter aufgestockt werden, auch wird die auf Kreta ansässige Behörde in Zukunft EU-weit die Kommunikation zwischen den Mitgliedstaaten koordinieren, sollte es zu einem länderübergreifenden IT-Sicherheitsvorfall kommen. Diese EU-Strategie ist nur konsequent, denn infolge der mitgliedstaatlichen Umsetzung der Netz- und InformationssicherheitsRL (NIS-RL) der EU sind die EU-Staaten schon jetzt verpflichtet, speziell auf die Cybersicherheit bezogene Informations- und Kommunikationskanäle in Richtung der EU offen zu halten. Im Einzelnen zu klären sein wird aber noch, in welchem Umfang und von welcher Art die Informationen sein werden, die im europäischen Datenaustausch stehen. Hierin liegt auch ein besonderes Problem der Wahl des Rechtsetzungsinstruments der europäischen Richtlinie, das den Mitgliedstaaten einen eigenen Entscheidungsspielraum bei der Umsetzung der EU-Anforderungen einräumt. Schon bei der NIS-RL waren sich die Mitgliedstaaten im Gesetzgebungsverfahren uneinig, was zu einer erheblichen Ausdehnung des Legislativprozesses führte. Für den nun beabsichtigten erweiterten Informationsaustausch mit der *ENISA* ist Ähnliches zu befürchten.

Neue europäische IT-Sicherheitszertifizierung

Über den länderübergreifenden Informationsaustausch hinaus wird die *ENISA* in Zukunft auch dafür zuständig sein, die neue europäische IT-Sicherheitszertifizierung zu koordinieren und zu prüfen. In einem ersten Schritt wird es notwendig sein, Zertifizierungsregeln zu erarbeiten, die eine staatenübergreifende Zustimmung genießen. Diese werden im Anschluss durch die *Kommission* verabschiedet. Die Schaffung einer EU-weiten Sicherheitszertifizierung ist nicht nur unter IT-Security-Gesichtspunkten vorteilhaft, sondern würde auch dazu beitragen, den europäischen Binnenmarkt weiter zu öffnen, indem Firmen, die z.B. in Deutschland eine zertifizierte IT-Anlage betreiben, mit vergleichbaren Anforderungen ein System auch in Frankreich oder Spanien einsetzen könnten. Dies kann im Zweifelsfall zu erheblichen Kosteneinsparungen führen, so z.B. im Bereich der Smart Meter, wo für eine Zertifizierung im deutschen Raum zurzeit mehr als € 1 Mio. für das betroffene Unternehmen veranschlagt werden kann, wohingegen eine vergleichbare Zertifizierung in Frankreich zu in etwa einem Zehntel dieser Summe möglich ist.

Obgleich die EU-weite Vereinheitlichung von Sicherheitsstandards zunächst nur Vorteile zu bringen scheint, so sind damit auch Risiken verbunden, die mit denen des Gesetzgebungsprozesses zur NIS-RL vergleichbar sind: Wo Deutschland sehr hohe Maßstäbe anlegt, weil hierzulande bereits seit Jahren Cybersicherheit auf behördlicher Seite, insbesondere durch das *BSI* betrieben wird, verfügen manch andere Mitgliedstaaten kaum über vergleichbare Regelungs- und Behördenstrukturen. Die politische Herausforde-

rung wird es sein, auch hier ein gesundes Mittelmaß zu finden, um die europäische Cybersicherheits-Zertifizierung nicht auf einen allgemein so niedrigen Standard zu senken, dass Sicherheitslücken als Politikum bewusst in Kauf genommen werden. Zumindest für die NIS-RL ist dieser europaweite Kompromiss jedoch gut gelungen. Soweit die Zertifizierungsrichtlinien von Seiten der *ENISA* erarbeitet wurden, können Unternehmen eine entsprechende Anerkennung beantragen. Erteilt wird die Zertifizierung für die Dauer von maximal fünf Jahren und verfügt über eine EU-weite Gültigkeit.

Überarbeitete EU-Cyber-Sicherheitsstrategie

Nachdem die *Bundesregierung* bereits Ende 2016 ihre neue Cyber-Sicherheitsstrategie veröffentlichte, zieht die EU nun nach und schlägt mit ihrem neuen Papier verschiedene Maßnahmen vor, die die Mitgliedstaaten auf die veränderte Cyber-Sicherheitslage der Zukunft vorbereiten sollen. Zuvorderst thematisiert werden Abwehrstrategien für großflächig angelegte Angriffe im digitalen Raum, die gleichzeitig verschiedene Mitgliedstaaten betreffen. Hier wird die *ENISA* mit ihrer neuen Funktion als zentrale Koordinierungsstelle einen erheblichen Beitrag leisten, um effektive Schutzmaßnahmen zu ergreifen; auch ist hier vorgesehen, weitere EU-Behörden einzubeziehen. Darüber hinaus wird die *ENISA* regelmäßige IT-Sicherheitsübungen vorsehen, um die mitgliedstaatliche Koordinations- und Abwehrbereitschaft zu überprüfen. Hauptziel der neuen EU-Cyber-Sicherheitsstrategie ist es, in Zukunft nicht mehr einen reaktiven, sondern vielmehr einen proaktiven Ansatz zur Cybersicherheit zu verfolgen, sodass Behörden und Unternehmen schon im Vorfeld entsprechende Schutz- und Abwehrmaßnahmen ergreifen können. Hierzu gehört auch die Forschung im Bereich der IT-Sicherheit. Um die *ENISA* sowie die Mitgliedstaaten mit entsprechenden Informationen zu versorgen, soll deshalb ein Kompetenzzentrum zur Cybersicherheit gegründet werden, das die europäische Forschung in diesem Bereich wohl ab dem Jahr 2018 leiten wird.

Cybersicherheit ja – aber um jeden Preis?

Der europäische Ansatz zur Neuregulierung der EU-weiten Cybersicherheit kommt nicht überraschend: Schon seit Langem war in entsprechenden Kreisen bekannt, dass die EU eine Novellierung ihrer IT-Sicherheitsstrategie plant; darüber hinaus haben die IT-Sicherheitsvorfälle 2017 gezeigt, dass das Niveau der bisher ergriffenen Sicherheitsmaßnahmen noch nicht ausreichend sein kann. Durchaus überraschend ist jedoch der Umfang und die Geschwindigkeit, mit welcher die Europäische Union den Ausbau ihrer IT-Sicherheitskompetenz plant und vorantreibt: War es im Jahr 2016 die NIS-RL als vornehmlich auf die Mitgliedstaaten bezogener Ansatz, so ist es in 2017 die umfassende Umstrukturierung der europäischen Cyber-Sicherheitskompetenz. So begrüßenswert die neuen Vorschläge und das schnelle Handeln der *EU-Kommission* dabei zunächst auch sein mögen, so sollte zugleich nicht vergessen werden, dass die europäische Regulierung der IT-Sicherheit auch nach über einem Jahr seit dem Inkrafttreten der NIS-RL noch ein „heißes Pflaster" ist, denn noch immer herrscht in vielen Mitgliedstaaten ein faktisch ungleiches IT-Sicherheitsniveau. Da es für den Erfolg der neuen Kommissionspläne in einem erheblichen Maße auch auf die Akzeptanz und Mitarbeit der EU-Staaten hinsichtlich der zu ergreifenden Maßnahmen ankommt, sollte hier deshalb nicht überstürzt gehandelt werden – und erst recht nicht deshalb, um einen bloßen politischen Willen in einer schwierigen Zeit zu manifestieren. Die bisher ergriffenen und auch die neuen Regulierungsansätze gesamteuropäischer Cybersicherheit sind sicher gut geeignet, um mittelfristig das IT-Sicherheitsniveau flächendeckend zu verbessern – um jeden Preis aber sollte eine schnelle Realisierung vom Reißbrett nicht geschehen, denn dies würde nur mehr schaden als tatsächlich nützen.

■ Vgl. auch *Kipker/Stelter*, MMR-Aktuell 2017, 394832; *Kipker*, MMR-Aktuell 2017, 389121; *ders.*, MMR 2017, 143; *ders.*, ZD-Aktuell 2016, 05363; MMR-Aktuell 2017, 394324; *Roth*, ZD 2015, 17; ZD-Aktuell 2017, 05783 und *Rockstroh/Kunkel*, MMR 2017, 77.

Dr. Dennis-Kenji Kipker
ist Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, Projektmanager beim Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V. in Frankfurt/M., Abteilung CERT@VDE, und Mitglied des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.