Zahnloser Tiger oder tonnenschwerer Mühlstein

Die Working Group Cyber and Data der European Digital SME Alliance informiert über den anstehenden Cyber Reslience Act (CRA).

Brüssel. Ein neues Gesetz der EU sorgt derzeit für Kontroversen: der Cyber Resilience Act, kurz CRA. Am 15. Februar berichtete im Rahmen der Arbeitsgruppe Cyber and Data der European Digital SME Alliance Mitverfasser Benjamin Bögel, Policy Officer on Cybersecurity bei der Europäischen Kommission, über den Stand der Lage. Und löste damit eine lebhafte Diskussion aus. Der Bundesverband IT-Mittelstand mit Patrick Häuser (BITMi-Hauptstadtbüro), Rasmus Keller, RK IP Law, Stephan Schwichtenberg, pi-lar GmbH und Matthias Kampmann, IT-Sicherheitscluster e. V., waren dabei und vertraten dort die Interessen ihres Dachverbands und ihrer organisierten Mitgliedsunternehmen.

Was angesichts von Milliarden Euro an jährlichen finanziellen Schäden (Quelle: **https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/)** durch Cybercrime alleine in Deutschland als sinnvolles Vorhaben erscheint, könnte sich als ein Instrument symbolischer Rechtsetzung entpuppen. Dass das Gesetz kommt, steht außer Frage, und auch die Timeline steht weitgehend. Benjamin Bögel beschrieb das Vorhaben als zielgerichtet zugeschnitten auf die Sicherheit von Hardware- und Software-Produkten, also Waren mit "digital Elements". Betroffen sind sämtliche Produkte dieser Art im Markt der EU, ganz gleich, ob sie aus dem Nicht-EU-Ausland stammen oder in der EU produziert worden sind. Ziel ist eine EU-weite, rechtliche Einheitlichkeit noch bevor es Standards gibt. Darauf einstellen müssen sich aber nicht nur Produzenten bzw. Hersteller, sondern auch Importeure und (Groß-)Händler. Wer verkauft, muss wissen, dass er nur dann Produkte verkaufen kann, wenn sie rechtskonform gemäß CRA sind.

Darunter fallen alle erdenklichen Softwareprodukte oder Software in Kombination mit Hardware, die auf einem internetfähigen Device ausgeführt werden können. Folglich müssen selbst einfachste Desktopanwendungen die CRA-Anforderungen einhalten, etwa Texteditoren oder Grafiktools – und zwar unabhängig von den Sicherheitsklassen. Damit werden Prüf-, Dokumentations-, Gestaltungs- und Leistungspflichten für Softwarehersteller begründet. Die Standards werden dann von den europäischen Standardisierern CEN/CENELEC gesetzt. Anbieter müssen dabei eine Konformitätsprüfung durchlaufen. Ferner wird es eine Meldeverpflichtung geben. Schwachstellen, für die es bereits einen Exploit gibt, müssen selbstständig in definierten Fristen angezeigt werden. Vorbild für das Gesetz ist das CE-Zeichen, das auf jedem ordentlichen Elektrogerät zu finden ist. Adressiert sind bei diesem Siegel Produktsicherheit sowie Umwelt- und Gesundheitsschutz. Mit dem CRA ergibt sich dann eine Erweiterung auf Cybersecurity**,** um Schwachstellen in Produkten konsequent und zielgerichtet zu erfassen und Cybercrimeschäden zu verhindern.

Hinsichtlich Hardware sind beispielsweise Laptops, Smart Appliances, CPUs, Router oder Firewalls betroffen. Mit Blick auf die Software fallen Betriebssysteme, aber auch Games oder Apps für Smartphones oder Tablets darunter. Wesentlich, und das hat die Problematik rund um Log4J mehr als deutlich gezeigt, ist die Zielrichtung, Programmbibliotheken ebenfalls

unter den Schirm der betroffenen Produkte zu nehmen. Ziele des Gesetzes sind nicht reine Dienstleistungen, aber Software, die im Kontext von und für Services programmiert wird.

Das Gesetz gilt nicht für Hobbyprojekte oder komplett nichtkommerzielle Software und Dienste (SaaS). Ebenfalls ausgeschlossen sind Produkte aus dem Bereich Automotive, Avionik oder Waffenindustrie. Generell kann man sagen, dass bestehende Regulierungen auch in der nationalen Gesetzgebung priorisiert sind. Der CRA ist bei vorhandener Deckung durch andere Gesetze dann erst einmal in der zweiten Reihe.

Eine wichtige Frage, die jeden Unternehmer interessieren wird: Wie steht es um den Nachweis von Konformität und wie hoch ist der Aufwand? Dies geschieht mittels „Self Assessment“. Und wie in vielen Gesetzgebungsvorhaben besitzt auch der CRA unterschiedliche Risikoklassen, die unterschiedliche Anforderungen an die Unternehmen stellen. Schwergewichte sind etwa Betriebssysteme, Anti-Virus-Software, Router und Firewalls. Eine Klasse höher noch rangieren kritische Produkte, etwa Smart Cards, Secure Elements, also physische Komponenten in elektronischen Geräten, die gemäß BSI-Definition "sensible Daten und Anwendungen sicher aufbewahren und schützen" sollen.

In seiner letzten Ausprägung hat der Entwurf vor allem freie und quelloffene Software ins Visier genommen. Weil Open Source keine Blackbox sei, seien hier keine besonderen Maßnahmen an Transparenz notwendig. Der CRA wird allgemein als das EU-Vorhaben mit der größten Berücksichtigung von Open Source überhaupt eingeschätzt. Daher geht die Einschätzung nicht fehl, dass die Regulierung auf Open Source zugeschnitten wurde. Contributer in andere Projekte sind im Übrigen nicht betroffen. Nur selbstständige Vorhaben fallen in den Rahmen des CRA. Ein neues Konzept ist der "Steward" im Kontext von Open Source. Damit sind etwa Vereine, Verbände oder Stiftungen gemeint, die selbst keine Software produzieren, sondern Support bereitstellen und qualitätssichernde Tätigkeiten ausüben. Für derartige Organisationen gelten weniger strenge Richtlinien.

Diese auch als Bevorzugung lesbare Behandlung von Open Source-Software ist Grund genug, aufmerksam zu sein. Es bleiben nämlich aus der Sicht der KMU und des BITMi eine Reihe offener Fragen: Werden der risikobasierte Ansatz und eine vereinfachte technische Dokumentation nicht dennoch KMU schlichtweg überfordern, wenn sie strenger bemessen werden als etwa die "Stewards"? Dies gerade auch hinsichtlich weiterer Regulierungsvorhaben, die im Konzert miteinander einen an sich löblichen Schutzschirm aufspannen, aber eben auch den Aufwand vervielfachen. Kann also das Konformitätsassessment mit angemessenen und verhältnismäßigen Gebühren und ebensolchen Prozessen erzielt werden? Und wie sieht es aus mit den Strafen: Hier ist zwar die Größe des Unternehmens der ausschlaggebende Faktor, etwa hinsichtlich Meldepflichten. Aber kaskadieren dann nicht die Anzeigen?

Es wird zu prüfen sein, ob der CRA nicht zu einem ökonomischen Desaster für KMU führt und das Gegenteil dessen hervorbringt, was beabsichtigt ist: Sicherheit, Produktstabilität und Planbarkeit. Zudem muss auch die Durchsetzung gegenüber Konzernen und Nicht-EU-Unternehmen gewährleistet sein, damit der CRA nicht als zahnloser Tiger auf den Weg gebracht wird. Das alles hängt natürlich auch von unterstützenden Maßnahmen für KMU ab: Hilfen, harmonisierte Standards, nationale Maßnahmen, ein CSIRT-Helpdesk und Fördermittel etwa aus dem gigantischen Programm Digital Europe sollen auf den Weg gebracht werden. Ohne derartige Hilfen wird es wahrscheinlich nicht gehen. Angesichts der gewaltigen Schadenssumme sind diese Ausgaben hoffentlich verkraftbar und vertretbar.

Eine zeitlich exakt abgestimmte Route kann derzeit noch nicht angegeben werden. In der 2. Hälfte 2024 fällt der Startschuss. Dann gibt es eine dreijährige Übergangsphase, die in der zweiten Hälfte 2027 beendet sein soll. Dazwischen müssen alle unterstützenden Plattformen und Hilfstools aufgesetzt sein. Der Übergang kommt also nicht als Schock. Und sowohl die Instanzen der EU als auch die KMU sind in der Pflicht zur Umsetzung.