



**„Cybersecurity wird jetzt
rechtliche Anforderung“**

Lange Zeit hing die Cybersecurity allein vom Engagement der Anwender und Hersteller ab und war kaum gesetzlich reguliert. Mit dem Cyber Resilience Act (CRA) soll das Recht jetzt zum Treiber der Security werden, wie Stefan Hessel, Anwalt für Cybersicherheit bei reuschlaw, im Interview klarstellt. Der Rechtsexperte erklärt außerdem, wie der CRA das IT-Sicherheitsniveau erhöht und was Unternehmen jetzt tun müssen.

Herr Hessel, in der industriellen Produktion wächst die Bedeutung der Cybersecurity stetig. Wie steht es um den juristischen Stellenwert der Informationssicherheit?

Ich bemerke eine ähnliche Entwicklung wie in der Industrie, wenn auch etwas zeitverzögert. Die Cybersicherheit hat juristisch sehr lange nur eine untergeordnete Rolle gespielt, weil es abgesehen vom Datenschutzrecht schlicht und einfach in der Breite keine gesetzlichen Anforderungen gab. Mit der stark ansteigenden Angriffsrate und den daraus resultierenden Auswirkungen auf die Industrie verändert sich das aber gerade stark und wir erleben eine Verdichtung des Cybersicherheitsrechts. Die Zeiten des sehr statischen Cybersicherheitsrechts mit nahezu keinerlei Regulierung sind definitiv vorbei.

Ein weiterer Baustein dieser Verdichtung ist der Cyber Resilience Act, der im September 2022 von der EU verabschiedet wurde. Was kommt da jetzt auf die Automatisierungsbranche zu?

Die EU reagiert mit dem Cyber Resilience Act auf die immer dynamischere Bedrohungslage, wie es im Amtsdeutsch heißt. Dahinter steckt im Grunde, dass sich Cyberangriffe nicht mehr nur noch auf Unternehmen richten, sondern vermehrt auch Produkte, die diese Firmen herstellen oder selbst einsetzen in den Fokus von Angreifern rücken. Dadurch, dass immer mehr Hardware selbst mit dem Internet verbunden ist oder zumindest über das World Wide Web erreichbar wird, entsteht eine neue Bedrohungslage. Und das nicht nur für kritische Infrastrukturen.

Sollte die Industrie das nicht schon längst bemerkt haben? Schließlich sind Cyberangriffe heutzutage keine Seltenheit mehr.

Das hat sie auch in jedem Fall bemerkt und viele haben daraus für ihre Produkte oder die von ihnen eingesetzten Assets auch entsprechende Vorkehrungen getroffen. Allerdings tun das nicht alle freiwillig, weshalb die europäische Gesetzgebung jetzt mit dem Cyber Resilience Act, kurz CRA, darauf reagiert.

Was erhofft sich die EU davon?

Sie will das Cybersicherheitsniveau in der Breite erhöhen, indem durch den CRA jedes Produkt mit digitalen Elementen bestimmte Security-Anforderungen erfüllen muss. Der CRA ergänzt damit die NIS-2-Richtlinie, die den cybersicheren Betrieb von IT-Systemen in Unternehmen reguliert. Damit gibt es jetzt eine Security-Baseline für die Unternehmens- und die Produktwelt.

Wie gravierend werden die Auswirkungen des CRA?

Fest steht, dass der CRA einen riesigen Effekt auf die Industrie haben wird, einfach weil der Spieß jetzt umgedreht wird und das Recht zum Treiber der Cybersicherheit wird. Bislang wurde Cybersicherheit etwas stiefmütterlich behandelt, weil es für die Kunden oder das Marketing nützlich war oder eben eigene Risiken ausgeschlossen werden sollten. Jetzt gilt: Wer Security nicht mitdenkt, wird schmerzhaft bestraft.

Was bedeutet das jetzt für die Hersteller und Betreiber?

Der CRA ist noch nicht beschlossen. Wir stecken noch mitten in den Trilogverhandlungen und nahezu täglich gibt es neue Änderungen. Was wir also aktuell mitbekommen ist mit Vorsicht zu genießen. Was jedoch schon spruchreif ist betrifft vor allem die Unterscheidung von kritischen und nicht-kritischen Produkten, die der CRA einführt. Diese Einteilung betrifft allerdings nicht die Anforderungen an die Produkte, denn die gelten gleichermaßen für alle, sondern ausschließlich die Konformitätserklärung, sprich die CE-Kennzeichnung. Bei nicht-kritischen Produkten kann ich sie als Hersteller selbst ausstellen, bei kritischen Assets der Klasse 1 braucht es dafür eine entsprechende Norm oder eine dritte Stelle, bei kritischen Produkten der Klasse 2 dann allerdings definitiv eine externe Prüfung. Das ist aus meiner Sicht auch sinnvoll, denn gerade wenn es um hochkritische Anwendungen geht, sollte die Security nicht allein dem Produkthersteller überlassen werden. Heiß diskutiert wird aktuell allerdings die Frage, wie Produkte in diese Kategorien eingeteilt werden sollen.

Warum?

Nun eine Festplatte z. B. ist an sich erst einmal ein nicht-kritisches Produkt, aber was passiert, wenn ich sie in kritischer Infrastruktur einbaue und nutze? Wird sie dann durch ihren Verwendungszweck zu einem kritischen Produkt? Die Einteilung ist hier noch nicht griffig und genau genug, was auch viele Industrieverbände kritisiert haben. Für Hersteller birgt das aktuell zusätzlich das Problem, dass sie antizipieren müssen, wofür ihr Produkt am Ende eingesetzt werden könnte. Aber wie bereits gesagt wird darüber rege diskutiert, so dass wir zukünftig mit mehr Trennschärfe rechnen können.

Die eben von Ihnen angesprochene dritte Stelle für die Konformitätsbewertung wird dann vermutlich an Dienstleister ausgegliedert?

Genau so wird es kommen, alles andere wäre auch nicht praktikabel. Die gängigen Zertifizierungs-Dienstleister werden sicherlich da alle ihren Namen in den Hut werfen und ihr Port-



Abbildung 1: Stefan Hessel ist Experte für cyberrechtliche Fragen.

folio ergänzen. In dem Kontext ist auch wichtig, dass wir Stand jetzt auch noch nicht wissen, welche Aufsichtsbehörde am Ende zuständig ist. Die Datenschutzaufsichtsbehörde wird es wohl nicht werden, so dass wahrscheinlich nur noch das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Bundesnetzagentur übrigbleiben. Denkbar wäre auch eine neue Behörde, was ich aber für unwahrscheinlich halte.

Wer auch immer am Ende dann die Zertifizierung übernimmt, muss dann aber auch die bereits eingesetzten Produkte nachträglich prüfen, oder?

Nein, denn der entscheidende Punkt ist die Bereitstellung am Markt. Also alles, was bereits vor der Einführung des CRA verkauft und in Betrieb genommen wurde, muss nicht nachträglich geprüft werden. Trotzdem gilt es zwei wichtige Aspekte zu beachten: Wenn keine Sicherheitsupdates für eingesetzte Geräte zur Verfügung stehen, kann dies aufgrund der NIS-2-Richtlinie zu einem Problem für den Betreiber werden, weil er sich um die dauerhafte Gewährleistung der Cybersicherheit kümmern muss. Außerdem können an sich cybersichere Geräte in unsicheren Umgebungen eingesetzt werden, was Hersteller in gewissem Umfang bei neuen Produkten, die dem CRA unterliegen, berücksichtigen müssen. Mittelbar hat der CRA jedoch nur indirekt Auswirkungen auf den Anlagenbestand.

Gängige Cybersicherheitsnormen wie die IEC 62443 zu erfüllen, reicht also künftig nicht aus, um auch hinsichtlich des CRA auf der rechtssicheren Seite zu stehen?

Natürlich deckt die IEC 62443 einige Aspekte ab, die auch der CRA in seinem Anforderungskatalog beschreibt. Jetzt

„Der CRA will das Cybersicherheitsniveau in der Breite erhöhen, indem jedes Produkt mit digitalen Elementen bestimmte Security-Anforderungen erfüllen muss.“

aber zu denken damit bereits auf der sicheren Seite zu sein, ist ein Trugschluss. Grundsätzlich darf man aber nie den Fehler machen, von der Norm zum Gesetz zu denken. Es ist nämlich genau andersherum: ein Gesetz wird durch Normen ausgefüllt. Das bedeutet, dass der CRA erst einmal Anforderungen aufstellt, die erfüllt werden müssen. Nicht alle davon werden von der aktuellen IEC 62443 abgedeckt. Sie wird z. B. nie dafür sorgen, dass es bei einer Anfrage einer Behörde einen Prozess gibt, wie die Unternehmens-IT zusammen mit der Rechtsabteilung darauf reagieren soll. Abgesehen davon kommt die Normung nicht mit den Umsetzungszeiträumen zurecht. Es ist also durchaus denkbar, dass es noch gar keine Norm gibt, die den CRA zu großen Teilen abdeckt, wenn er nach der Umsetzungszeit von vermutlich zwei Jahren anwendbar ist. Die Normung ist schlicht zu langsam oder der Umsetzungszeitraum zu knapp.

Was gilt es denn dann nun zu tun?

Die Unternehmen müssen erkennen, dass wir durch den CRA eine grundlegende Änderung der Rechtslage erleben. Cybersecurity wird zur rechtlichen Anforderung, unabhängig davon, ob ich Betreiber oder Hersteller bin. Deshalb wäre der erste Schritt aus meiner Sicht erst einmal zu schauen, inwiefern man von den Regelungen des CRA betroffen ist. Denn selbst wenn sich an den konkreten Details des CRA noch etwas verändert, werden die Anforderungen in jedem Fall Produkte mit digitalen Elementen betreffen. Sich zu fragen, ob die selbst produzierten oder eingesetzten Geräte unter diese Definition fallen, ist ein kluger erster Schritt.

Worauf müssen Anwender wie Betreiber noch achten?

Im Vordergrund sollten Aspekte wie z. B. die Updateability stehen. Wenn ein Sicherheitsproblem auftritt und der

„Unternehmen müssen erkennen, dass wir durch den CRA eine grundlegende Änderung der Rechtslage erleben. Cybersecurity wird zur rechtlichen Anforderung.“

Hersteller diese Lücke mit einem Update, over-the-air oder zum Download bereitgestellt, schließen kann, wird die Warnung der offiziellen Behörden weniger dramatisch ausfallen oder sogar vollständig überflüssig werden. Darüber hinaus kann es ratsam sein, sich mit den dafür notwendigen Abläufen und Organisationsstrukturen auseinanderzusetzen. Immer mehr Unternehmen beginnen außerdem damit, ihre Teams stärker interdisziplinär aufzustellen, um IT und OT aber auch die Rechtsabteilungen besser miteinander zu vernetzen.

Dahinter steht natürlich die Frage, ob in allen Abteilungen die entsprechenden Fachleute vorhanden sind.

Absolut und falls nicht, ob bis zum Ende der Umsetzungsfrist ausreichend Expertise aufgebaut werden kann. Was auch nicht schaden kann, ist sich jetzt schon mal mit den Aufsichtsbehörden zu vernetzen und sich darüber klarzuwerden, wie die Erwartungshaltungen aussehen. Auch der Kontakt zu Hochschulen und Forschungseinrichtungen kann lohnend sein, gerade wenn es um eventuelle Neu- oder Weiterentwicklungen von Produkten geht. Zu guter Letzt können auch Vertragsanpassungen mit Zulieferern notwendig sein, um z. B. Updatepflichten oder den Umgang mit Open Source Software rechtssicher zu regeln.

Wie viel Zeit bleibt dafür noch, sprich wie sieht die weitere Timeline des CRA aus?

Der Entwurf für den CRA wurde im September 2022 vorgelegt und aktuell laufen wie schon angesprochen die Trilogverhandlungen, in denen sich das EU-Parlament, die EU-Kommission und der Rat der Europäischen Union auf einen gemeinsamen Vorschlag einigen, der dann verabschiedet wird und in Kraft tritt. Natürlich wird es dann einen Umsetzungszeitraum von vermutlich zwei Jahren

geben, damit nicht von heute auf morgen alles umgeworfen werden muss. Der aus meiner Sicht früheste Zeitpunkt inklusive Umsetzungszeitraum wäre Mitte 2025. Es kann sich aber alles noch weiter in die Zukunft verschieben.

Scheitern kann der CRA aber nicht mehr?

Doch, natürlich ist auch das noch möglich, auch wenn ich das nicht für realistisch halte. Aber selbst wenn er scheitern würde, könnten die entwickelten Regelungen und Vorgaben dann in einer anderen Verordnung aufgenommen werden, die dann vielleicht einen anderen Namen hat. Die Marschroute für mehr Cybersicherheit in Europa steht fest.

Mal angenommen der CRA tritt 2025 in Kraft, wie könnten Verstöße dann geahndet werden?

Wie bei allen anderen Verordnungen zum Digitalrecht ist der Werkzeugkasten der Aufsichtsbehörden bei Verstößen relativ groß. Es ist die Verhängung von Bußgeldern möglich, wobei sich am Modell der DSGVO orientiert wird, was bedeutet, dass diese Strafzahlungen empfindlich hoch sein können. Die Aufsichtsbehörden haben im Einzelfall außerdem sehr weitreichende Untersuchungsbefugnisse und können z. B. entscheiden, dass Produkte nicht mehr zur Verfügung gestellt werden dürfen oder sogar zurückgerufen werden müssen. Darüber hinaus sind auch öffentliche Warnungen möglich. Das BSI hat die Befugnis, Produktwarnungen auszusprechen bereits und hat von dieser im Jahr 2022 bereits zweimal Gebrauch gemacht. Einmal war die die Sicherheitssoftware eines russischen Herstellers betroffen. Im anderen Fall stand ein smartes Türschloss im Mittelpunkt. Erste Präzedenzfälle sind also bereits vorhanden. In jedem Fall sollten Hersteller den CRA nicht auf die leichte Schulter nehmen und sich jetzt schon mit den Auswirkungen der Regelungen auf ihr Unternehmen beschäftigen.

ZUR PERSON

Stefan Hessel

Rechtsanwalt Stefan Hessel, LL.M. ist Salary Partner und Head of Digital Business bei reuschlaw in Saarbrücken. Er berät Unternehmen zu komplexen Fragestellungen in den Bereichen Datenschutz, Cybersicherheit und IT-Recht. Er ist zertifizierter Datenschutzbeauftragter (TÜV) und zertifizierter ISMS-Auditor nach ISO/IEC 27001 (ICO). Darüber hinaus ist er Lehrbeauftragter an der Deutschen Universität für Verwaltungswissenschaften Speyer und Autor zahlreicher Fachpublikationen.