# Cyber Resilience Act – Podcast-Transkript

Deutsche Originalaufnahme · deutsche Lesefassung · 26:05

Redaktionell geglättete Lesefassung des deutschen Gesprächs mit Zeitmarken. Die fachliche Einordnung ergänzt einzelne verkürzte Aussagen im Originalton.

## Fachliche Einordnung zum Gespräch

Stand der fachlichen Einordnung: 15. November 2026.

Support und Updates. Der Unterstützungszeitraum beträgt grundsätzlich mindestens fünf Jahre. Bei voraussichtlich kürzerer Nutzung darf er der erwarteten Nutzungsdauer entsprechen. Automatische Sicherheitsupdates sind vorgesehen, soweit dies anwendbar ist.

Software-Stückliste. Sie muss mindestens die Abhängigkeiten der obersten Ebene erfassen. Aus der Dokumentationspflicht folgt kein pauschaler Anspruch aller Käufer auf Herausgabe der vollständigen SBOM.

Meldungen. Artikel 14 gilt seit dem 11. September 2026. Hersteller müssen bei aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen grundsätzlich binnen 24 Stunden ab Kenntnis frühwarnen und binnen 72 Stunden nachmelden. Für den Abschlussbericht gelten je nach Fall unterschiedliche Fristen.

Produkthaftung. (EU) 2024/2853 ist eine Richtlinie. Ein fehlendes Update kann für die Fehlerhaftigkeit relevant sein. Ein ersatzfähiger Schaden und der ursächliche Zusammenhang müssen ebenfalls vorliegen. Schäden an ausschließlich beruflich genutzten Sachen und Daten sind von dieser Richtlinie ausgenommen.

CE-Kennzeichnung. Nach Artikel 30 Absatz 4 CRA folgt die Kennnummer der notifizierten Stelle auf das CE-Zeichen, wenn diese Stelle am Verfahren der umfassenden Qualitätssicherung nach Modul H beteiligt ist.

(EU) 2024/2847 · (EU) 2024/2853 · Meldepflichten zum CRA

## Das vernetzte Babyphone und der Geltungsbereich

**00:00** Also, stell dir mal vor, du kaufst dir ein nagelneues Auto, ne? Ja, okay. Ein schickes neues Auto. Genau. Du fährst vom Hof des Händlers, beschleunigst auf der Autobahn, so auf 130 km/h und plötzlich stellst du fest, dass der Hersteller einfach mal die Bremsen vergessen hat. Das wäre suboptimal, ja. Absolut. Also rufst du beim Kundenservice an, völlig panisch und die sagen dir ganz entspannt, „Oh, sorry, die Bremsbeläge, die müssen Sie sich selbst aus dem Internet herunterladen und irgendwie einbauen. Viel Glück dabei.“ Das klingt komplett absurd. Richtig. Da würde jeder sofort klagen. Richtig.

**00:34** Aber in der digitalen Welt, da kaufst du quasi jeden Tag smarte Türschlösser, Babyphone oder WLAN-Router, bei denen exakt das passiert. Ja, leider. Man kauft ein

unfertiges Produkt. Genau. Ein unfertiges, unsicheres Produkt und du als Käufer trägst das komplette Risiko. Zumindest bis heute. Denn die EU, die drückt da jetzt den großen Notstoppschalter. Und zwar mit einer Wucht, die man sich kaum vorstellen kann. Das wird die gesamte globale Tech-Industrie also wirklich erschüttern. Gut gesagt.

**01:06** Und damit ein herzliches Willkommen zu unserer heutigen Tiefenanalyse. Schön, dass du als unser geschätzter dritter Teilnehmer im Raum wieder dabei bist. Schön, dass du zuhörst. Wir schauen uns heute nämlich etwas an, das auf den ersten Blick, naja, nach trockener Brüsseler Bürokratie klingt. Ist es aber nicht. Nee, überhaupt nicht. Es ist in Wahrheit ein absolutes regulatorisches Erdbeben. Wir reden über die neue EU-Verordnung (EU) 2024/2847. Besser bekannt als der EU Cyber Resilience Act oder kurz der CRA. Genau. Und unsere Quellen heute, die bestehen wirklich ausschließlich aus dem originalen Rechtstext der EU. Aber keine Panik, wir übersetzen das Ganze für dich. Also lass uns das mal entpacken.

**01:47** Ja, lass uns da direkt reingehen. Um das greifbar zu machen, habe ich mir gedacht, wir erfinden heute mal ein Produkt, an dem wir das Gesetz so ein bisschen durchspielen. Nennen wir es das Smart Baby 3000. Das Smart Baby 3000, gefällt mir. Was kann das? Das ist ein hochmodernes mit dem WLAN verbundenes Babyphone mit HD-Kamera, Cloud-App für dein Smartphone, allem drum und dran. Wie ändert dieser CRA jetzt das Leben von genau diesem Gerät? Also, um das zu verstehen, müssen wir uns zuerst diesen neuen Anwendungsbereich anschauen.

**02:19** Der CRA gilt nämlich für alle, und das ist jetzt ein Zitat, Produkte mit digitalen Elementen. Das klingt extrem weit gefasst. Ist es auch. Der Text definiert das so, dass es um Produkte geht, deren Zweck eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Das heißt, unser Smart Baby 3000 fällt da voll rein. Zu 100 Prozent, weil es eben Hardware und Software kombiniert und funktional vernetzt ist. Ausgenommen sind eigentlich nur Bereiche, die ohnehin schon extrem strenge Spezialgesetze haben. Also sowas wie Medizinprodukte oder Flugzeuge. Genau, Autos, Luftfahrt, Medizin, da gibt es schon krasse Regeln.

**02:57** Okay, aber warte mal. Das Babyphone selbst, das steht ja bei mir physisch im Kinderzimmer. Aber was ist denn mit der App und der Cloud? Das ist eine sehr gute Frage. Weil das Videosignal läuft ja oft über irgendeinen Server in Übersee. Reguliert die EU jetzt nur das Plastikgehäuse und den Chip oder fällt diese Cloud auch drunter?

**03:17** Das ist eine fantastische Unterscheidung. Also grundsätzlich reguliert der CRA Produkte, keine reinen Dienstleistungen. Aber, und das ist echt ein riesiges Aber, diese Datenfernverarbeitung, also die Cloud, fällt dann unter den CRA, wenn das Produkt ohne sie seine Funktion gar nicht erfüllen könnte. Ah, okay. Wenn dein Smart Baby 3000 ohne die Schnittstelle auf dem Hersteller-Server gar kein Bild auf dein Handy zaubern kann, dann ist diese Cloud-Komponente juristisch gesehen Teil des regulierten Produkts. Krass. Der Hersteller kann also nicht einfach sagen, unser Gerät ist sicher, nur der Server da drüben wurde leider gehackt. Exakt, das zählt nicht mehr. Er haftet für das Gesamtkonstrukt.

## Sichere Voreinstellungen und Verantwortung in der Lieferkette

**03:54** Das leuchtet ein. Aber was verlangt die EU jetzt konkret? Darf der das Ding einfach so auf den Markt werfen und später, keine Ahnung, wenn da Hacker gruselige Stimmen ins Kinderzimmer rufen, einfach einen Patch nachreichen? Eben nicht mehr. Das ist vorbei. Das Herzstück der Verordnung, das ist das Prinzip Security by Design und by Default. Also Sicherheit ab Werk. Ja, genau. Bisher war Sicherheit oft so ein nachträglicher Gedanke. Weißt du, wie ein Pflaster, das man auf eine offene Wunde klebt. Ja, also nach dem Motto, wir patchen das schon noch. Richtig. Und der Gesetzgeber zwingt die Hersteller nun, Produkte komplett ohne bekannte ausnutzbare Schwachstellen auf den Markt zu bringen. Das ist eine Pflicht ab dem Reißbrett. Wow.

**04:33** Dazu gehört auch Datenminimierung. Das Babyphone darf also nicht heimlich irgendwelche Metadaten für Werbezwecke sammeln, wenn das für die Funktion gar nicht nötig ist. Sehr beruhigend für ein Babyphone, muss ich sagen. Ja, oder? Und das Wichtigste. Schutz vor unbefugtem Zugriff als absolute Standardeinstellung. Das heißt, diese ganzen berüchtigten Standardpasswörter, du weißt schon, „Admin123“ oder einfach „0000“, die früher millionenfach fest einprogrammiert waren, die sind dann illegal. Absolut illegal. Jedes Gerät muss individuelle Zugangsdaten haben. Oder es muss dich beim ersten Einschalten zwingen, ein wirklich sicheres Passwort zu vergeben. Endlich.

**05:13** Ja, und was hier faszinierend ist, ist eigentlich der ökonomische Aspekt dahinter. Die EU greift hier ein, um ein ganz klassisches Marktversagen zu korrigieren. Wie meinst du das? Informationsasymmetrie. Genau. Du als normaler Nutzer, du kannst doch die Sicherheit von so einem komplexen Smart-Home-Teil gar nicht beurteilen. Nee, absolut nicht. Das sieht halt schick aus und funktioniert. Richtig. Aber ob der Code im Hintergrund aussieht wie ein Schweizer Käse, das siehst du nicht. Der Hersteller weiß das natürlich. Aber der hatte bisher einfach null finanziellen Anreiz, Geld in diese unsichtbare Sicherheit zu stecken. Klar, weil Gehäusedesign sich besser verkauft als Codequalität. Genau so ist es. Und der CRA, der verschiebt diese ökonomische Last jetzt radikal zum Hersteller.

**05:54** Gut, also der Hersteller, der das Ding baut, muss investieren. Aber jetzt mal ehrlich, so ein Babyphone wird ja in der Regel irgendwo in Asien produziert. Meistens ja. Dann wird das von so einer kleinen Importfirma nach Europa gebracht und liegt am Ende hier im großen Elektronikmarkt im Regal. Wenn jetzt der Hersteller in Asien sagt, „EU-Regeln interessieren mich nicht“. Was dann? Sind die Händler hier in Europa dann fein raus? Nein, überhaupt nicht. Die EU hat da echt aus vergangenen Regulierungen gelernt. Die spannt jetzt die komplette Lieferkette mit ein. Also auch den Elektronikmarkt um die Ecke.

**06:27** Ja, Einführer und Händler in der EU sind voll mit in der Haftung. Wenn du als großer Markt containerweise diese billigen Smart-Home-Gadgets aus Übersee kaufst, darfst du die nur vertreiben, wenn das CE-Kennzeichen dran ist und die IT-Sicherheit nachweislich stimmt. Das heißt, der Händler muss das quasi kontrollieren. Genau. Wenn ein Händler auch nur den bloßen Grund zur Annahme hat, dass dieses Smart Baby 3000

ein Risiko ist, darf er das gar nicht erst ins Regal stellen. Er muss es blockieren und sofort die Behörden informieren.

## Open Source und kommerzielle Nutzung

**06:55** Okay, da muss ich jetzt aber echt mal reingrätschen. Weil das klingt in der Theorie ja super, aber das kollidiert doch massiv mit der Realität der Software-Entwicklung, oder? Inwiefern? Ja, fast jedes moderne kommerzielle Produkt besteht heute aus Open-Source-Komponenten. Der Hersteller von meinem Smart Baby 3000, der schreibt das Betriebssystem ja nicht komplett neu. Das stimmt. Der schnappt sich einfach ein freies Linux, klatscht eine Open-Source-Kamerabibliothek von GitHub drauf und fertig ist das Ding. Wenn dieser freie Code, der ja von Freiwilligen geschrieben wurde, jetzt unsicher ist, wer haftet dann?

**07:26** Ich sehe, worauf du hinaus willst. Weil das klingt so, als würde dieses Gesetz die komplette freie Entwicklerszene einfach abwürgen. Wenn ich jetzt am Wochenende in meinem Keller ein cooles Smart-Home-Plugin programmiere und setze da einen kleinen Patreon-Link für Kaffeekassenspenden auf meine Seite, bin ich dann plötzlich auf Millionen verklagbar, wenn mein Code gehackt wird? Weil, ganz ehrlich, wenn ja, nehme ich meinen Code heute noch offline. OK, OK. Atme erst mal tief durch. Du kannst deinen Code ganz beruhigt online lassen. Puh, ein Glück. Aber du sprichst da was an. Das war tatsächlich die allergrößte Panik in der Open-Source-Community, als die ersten Entwürfe rauskamen. Ja, völlig verständlich. Total.

**08:03** Aber wenn wir tief in den Text schauen, so Erwägungsgründe 17 bis 19, da sehen wir, wie extrem elegant der Gesetzgeber das gelöst hat. Der CRA trennt nämlich scharf zwischen der Entwicklungsphase und der kommerziellen Lieferphase. OK, was heißt das genau? Freie und quelloffene Software, also FOSS, fällt nur dann unter diese strengen Pflichten, wenn sie im Rahmen einer kommerziellen Geschäftstätigkeit bereitgestellt wird. Und mein Patreon-Button für den Kaffee? Das ist keine kommerzielle Tätigkeit. Spenden ohne Gewinnabsicht gelten explizit als Ausnahme im Gesetz. Sehr gut.

**08:38** Kommerziell wird es wirklich erst, wenn du die Software aktiv monetarisierst oder wenn du zum Beispiel technischen Support gegen Geld anbietest. Oder und das ist jetzt der entscheidende Punkt für Unternehmen, wenn du als große Firma diesen kostenlosen Hobbycode nimmst und ihn gewinnbringend in deinen kommerziellen Router oder dein Babyphone einbaust. Dann und nur dann wirst du als Hersteller dieses Endprodukts voll haftbar für die Sicherheit von all diesen Open-Source-Bausteinen. Das ist ja genial. Das heißt, der Hersteller vom Smart Baby 3000 kann sich nicht mehr rausreden nach dem Motto, wir können nix dafür, die freie Kamerabibliothek hatte halt den Bug. Ganz genau. Er verdient Geld mit dem Gesamtpaket. Also muss er auch garantieren, dass die kostenlosen Teile, die er da reingeworfen hat, sicher sind. Das schützt die Innovation der kleinen Entwickler, nimmt aber die Big-Tech-Firmen in die Pflicht. Ziemlich smart.

**09:31** Aber warte mal, was ist mit so richtig großen Open-Source-Stiftungen? Du meinst was wie die Apache Foundation? Ja, genau. Die stellen ja Software her, die gefühlt das halbe Internet betreibt. Aber die machen das oft als Non-Profit. Dafür führt der Gesetzgeber eine brandneue Rolle ein, die sogenannten Verwalter quelloffener

Software. Okay, das klingt sehr förmlich. Ist es auch. Das sind juristische Personen, die Open Source systematisch und nachhaltig unterstützen, aber eben nicht wie so klassische Hersteller fertige Produkte verkaufen. Und warum eine eigene Rolle für die?

**10:09** Weil die EU schon verstanden hat. Wenn wir jetzt eine Apache-Stiftung mit Millionenstrafen überziehen, dann bricht das Internet morgen zusammen. Deshalb bekommen diese Verwalter vereinfachte Pflichten. Also ein bisschen Welpenschutz. So ähnlich. Sie müssen eine dokumentierte Cybersicherheitsstrategie haben und professionell mit Schwachstellen umgehen. Das ist klar. Aber sie dürfen zum Beispiel kein CE-Kennzeichen anbringen und der Text schützt sie explizit vor harten Bußgeldern. Man will sie ja nicht in den Ruin treiben. Okay, das ergibt Sinn. Wir haben jetzt also das Design und diese ganze Entwicklungsphase geklärt.

## Updates, Unterstützungszeitraum und Software-Stückliste

**10:44** Aber lass uns mal in die Zeit nach dem Kauf springen. Gerne, die Nutzungsphase. Genau. Ich nutze mein Smart Baby 3000 jetzt seit drei Jahren. Plötzlich findet irgendein IT-Sicherheitsforscher eine massive Lücke in genau dieser Kamerabibliothek. Der klassische Fall. Bisher hat der Hersteller da oft gesagt, das Modell ist alt. Kauf dir halt das neue Smart Baby 4000. Wie regelt der CRA denn jetzt Updates? Und hier, hier wird das Gesetz richtig schmerzhaft für viele Hersteller. Der CRA fordert nämlich einen garantierten Unterstützungszeitraum.

**11:17** Unterstützungszeitraum. Ja, das ist die Phase, in der Sicherheitsupdates bereitgestellt werden müssen. Und dieser Zeitraum muss der voraussichtlichen Nutzungsdauer des Produkts entsprechen. Aber er beträgt grundsätzlich mindestens fünf Jahre. Fünf Jahre? Wow. Das ist in der Tech-Welt ja eine halbe Ewigkeit. Ja, Ausnahmen gibt es echt nur, wenn die Lebensdauer des Produkts von Natur aus viel kürzer ist. Also zum Beispiel bei so einer temporären App für ein Event oder so. Aber bei einem physischen Gerät reden wir wirklich in der Regel von mindestens fünf Jahren.

**11:48** Und müssen diese Updates automatisch kommen oder muss ich als Nutzer da ständig in irgendwelchen kryptischen Menüs herumsuchen und auf „Update suchen“ klicken? Das ist der nächste große Schritt. Der Gesetzgeber verlangt, dass Produkte so gestaltet sind, dass Sicherheitsupdates als Standardeinstellung automatisch heruntergeladen und installiert werden. Yes. Du bekommst natürlich einen simplen Opt-Out-Mechanismus, falls du das aus irgendeinem Grund wirklich nicht willst. Aber Standard ist automatisch. Und noch faszinierender ist eine weitere Vorgabe. Funktionsupdates sollen künftig von Sicherheitsupdates getrennt werden. Oh, danke, liebe EU. Das bedeutet, ich werde nicht mehr gezwungen, so ein komplett neues speicherfressendes Interface-Redesign der App zu installieren, nur um eine winzige Sicherheitslücke zu schließen. Exakt. Die Sicherheitsarchitektur wird entkoppelt. Das ist super nutzerfreundlich.

**12:36** Aber jetzt kommt die eigentliche Herkulesaufgabe für die Hersteller. Welche? Na ja, woher weiß der Hersteller des Smart Baby 3000 nach drei Jahren überhaupt noch, dass exakt diese angreifbare, drei Jahre alte Open-Source-Bibliothek tief unten in

seinem Code versteckt ist? Da kommt dieses Akronym ins Spiel, über das in der IT-Industrie gerade alle schwitzen, richtig, dieses SBOM. Ganz genau SBOM. Das steht für Software Bill of Materials. Auf Deutsch sagt man Software-Stückliste. Der CRA verpflichtet die Hersteller, eine maschinenlesbare Liste von allen Komponenten, Bibliotheken und Abhängigkeiten zu erstellen und aktuell zu halten, die in ihrem Produkt stecken.

**13:16** Wenn wir das mal auf den Alltag übertragen. Das ist im Grunde wie die Zutatenliste auf einer Lebensmittelverpackung, oder? Genau, so kann man das sehen. Also wenn jemand eine Erdnussallergie hat, dann dreht er die Packung um und schaut, sind da Erdnüsse drin. Wenn jetzt eine Schwachstelle in einem bestimmten Stück Code auftaucht, schaut der Hersteller in seine SBOM-Zutatenliste und sieht sofort, oh Mist, in unserem Babyphone steckt dieses verwundbare Stück Code. Wir müssen sofort patchen. Das ist eine Super-Analogie. Aber stell dir vor, diese Zutatenliste hat hunderttausende Einträge und einige Zutaten bestehen wiederum aus dutzenden Unterzutaten von Lieferanten, die du gar nicht persönlich kennst. Okay, das klingt nach einem Albtraum.

**13:55** Ist es. Aber wenn wir das mit dem Gesamtbild verknüpfen, dann verstehen wir, warum die SBOM so revolutionär ist. Erinnerst du dich an Log4j? Oh Gott ja. Das war so eine winzige Protokollierungsbibliothek in Java, die quasi überall verbaut war. Als da eine Schwachstelle gefunden wurde, herrschte absolute Panik weltweit. Große Konzerne haben Wochen gebraucht, um überhaupt mal herauszufinden, in welchen ihrer eigenen Systeme Log4j eigentlich lief. Ein gigantischer Schmetterlingseffekt. Richtig. Und mit einer SBOM scannst du deine Stücklisten einfach automatisiert durch und weißt in Sekundenbruchteilen, welche deiner Produkte betroffen sind. Es ist zwar logistisch extrem hart, das jetzt für alten Code aufzubauen, aber für die Zukunft ist es einfach essenziell.

## Produktrisiko, Konformität und CE-Kennzeichnung

**14:35** Wow, okay. Also wir haben jetzt sicheres Design, fünf Jahre automatische Updates und eine lückenlose Zutatenliste. Aber wer kontrolliert das alles? Vertraut die EU einfach darauf, dass die Hersteller das schon irgendwie richtig machen? Ändert sich da was auf der Verpackung von meinem Babyphone? Das sichtbare Siegel auf der Verpackung bleibt weiterhin die CE-Kennzeichnung. Aber ihre Bedeutung ändert sich jetzt dramatisch. Inwiefern? Bisher stand das CE-Zeichen bei vielen smarten Geräten oft nur für elektrische Sicherheit. Also, dass das Netzteil nicht anfängt zu brennen oder für irgendwelche Funkstandards. Ab jetzt steht das CE-Zeichen zwingend auch für IT-Sicherheit nach diesem CRA. Und wer prüft das?

**15:17** Das hängt von der Risikoklasse ab. Bei sogenannten Standardprodukten mit geringem Risiko darf der Hersteller die Konformität in einem internen Kontrollverfahren noch selbst bewerten und dokumentieren. Aber mein Smart Baby 3000 hat eine Kamera, die direkt in mein Kinderzimmer filmt. Das kann kein Standardrisiko sein, oder? Völlig richtig. Solche Produkte fallen in die Kategorie der wichtigen Produkte mit digitalen Elementen. Und die sind nochmal unterteilt in Klasse 1 und Klasse 2. Okay, was ist Klasse 1? Klasse 1 umfasst Dinge wie intelligente Haushaltsgeräte mit

Sicherheitsfunktionen, Babyphones, vernetztes Spielzeug oder auch Passwortmanager. Wenn ein Hersteller hier nicht strikt nach harmonisierten EU-Normen arbeitet, dann muss zwingend eine unabhängige Prüfstelle ran.

**15:59** Und woran erkenne ich das als Käufer? Dann steht direkt neben dem CE-Zeichen auch die vierstellige Kennnummer von dieser Prüfstelle. Verstehe. Und Klasse 2? Das sind noch sensiblere Dinge. Firewalls, Container-Runtimesysteme oder manipulationssichere Mikroprozessoren. Da ist eine externe Prüfung durch Dritte immer Pflicht. Ohne Ausnahme. Heftig. Aber in dem Gesetzestext war doch noch von einer Kategorie für kritische Produkte die Rede. Was ist das denn dann, wenn Firewalls schon Klasse 2 sind?

**16:31** Das sind die wirklich zentralen Nervensysteme unserer gesamten Infrastruktur. Hast du ein Beispiel? Denk an Smart-Meter-Gateways, die unsere Stromnetze steuern. Oder Hardware-Sicherheitsmodule, die Kryptoschlüssel für große Banken verwalten. Hier geht die EU komplett aufs Ganze. Die EU-Kommission kann hier im Wege delegierter Rechtsakte sogar zwingend verlangen, dass diese Produkte ein europäisches Cyber-Sicherheitszertifikat erlangen müssen. Bevor sie überhaupt verkauft werden dürfen. Genau. Und zwar mindestens der Stufe Mittel oder Hoch. Vorher geht das gar nicht erst auf den Markt. Das wird den Markt echt komplett umkrempeln. Als Nutzer achte ich dann im Laden ja nicht mehr nur auf die Megapixel der Kamera, sondern auch auf die Zertifizierung und die Update-Laufzeit auf der Packung. Ganz genau.

## Meldepflichten und Informationsaustausch

**17:14** Aber, und das ist jetzt mein nächster großer Kritikpunkt, wo ich beim Lesen echt gestolpert bin. Schieß los. Was passiert im Krisenfall? Weil selbst mit SBOMs und unabhängigen Prüfstellen, wird es natürlich Hacks geben. Hacker sind kreativ. Natürlich. Hundertprozentige Sicherheit gibt es nicht. Eben. Und da habe ich im Text etwas gelesen zu Meldefristen. 24 Stunden. Ja, die 24-Stunden-Regel. Stell dir das mal vor. Wenn bei mir im Unternehmen eine aktiv ausgenutzte Schwachstelle auftaucht. Dann brennen bei mir wörtlich die Server. Die IT-Abteilung ist im absoluten Panikmodus. Wir versuchen verzweifelt, Systeme vom Netz zu nehmen.

**17:53** Und in genau dieser Situation verlangt die EU von mir, dass ich mich an den Schreibtisch setze und innerhalb von 24 Stunden irgendwelche Formulare ausfülle? Das ist exakt der Moment, in dem viele Unternehmensführungen Schnappatmungen bekommen haben. Ja, zu Recht. Aber schauen wir uns den Prozess mal genauer an, okay? Bei einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall musst du eine sogenannte Frühwarnung abgeben. Und ja, unverzüglich, spätestens nach 24 Stunden. An wen denn überhaupt? Das geht an eine zentrale, einheitliche Meldeplattform der EU-Cybersicherheitsagentur ENISA. Und diese Plattform verteilt die Meldung dann an das national zuständige Computer Security Incident Response Team. Also an das CSIRT deines Landes.

**18:36** Aber das ist doch Wahnsinn. Denk das doch mal zu Ende. Ich melde eine massive, komplett ungepatchte Lücke an eine EU-Datenbank. Wenn diese Datenbank gehackt wird. Oder wenn ein Mitarbeiter da plaudert. Dann hat man gerade eine

perfekte, detaillierte Bauanleitung geliefert, wie sie in mein System kommen. Und ich habe zu dem Zeitpunkt noch nicht mal einen Patch fertig. Das verschlimmert das Problem doch extrem. Ich verstehe dich da total. Das ist eine sehr legitime Angst.

**19:03** Aber auch das hat die EU durchdacht. Es geht hier gar nicht darum, Schwachstellen sofort in die ganze Welt zu posaunen. Der Gesetzgeber hat da sehr strikte Regeln für die Informationsweitergabe eingebaut. Wie sehen die aus? Aus Cybersicherheitsgründen kann die Weitergabe deiner Meldung aufgeschoben oder sogar komplett anonymisiert werden. Also, die halten das geheim? Genau. Das zuständige CSIRT kann entscheiden, hey, wenn wir diese Info jetzt an andere Staaten weitergeben, provozieren wir eine Katastrophe. Wir halten die Information unter Verschluss, bis der Hersteller den Patch ausgeliefert hat. Ah, okay. Und erst spätestens 14 Tage nach Bereitstellung von diesem Fix musst du als Hersteller dann einen detaillierten Abschlussbericht nachreichen. Vorher bleibt das oft sehr abgeschirmt.

**19:45** Sie bauen also eine Art Quarantäne für die Informationen ein. Aber mal ganz ehrlich, warum dann diese extreme Eile? Warum muss ich mich in den ersten 24 Stunden so stressen, wenn die das dann ohnehin erstmal unter Verschluss halten? Wegen des europäischen Binnenmarkts und des sogenannten Blast Radius. Blast Radius. Also der Zerstörungsradius. Exakt. Ja, der Zerstörungsradius eines Hacks. Ein brennender Server bei einem Hersteller in Frankreich ist heute vielleicht nur ein lokales Problem für ihn. Aber morgen früh ist das ein systemisches Sicherheitsproblem für vernetzte Krankenhäuser in Deutschland und für Stromnetze in Italien.

**20:20** Okay, das macht Sinn. Durch diese 24-Stunden-Frühwarnung wissen die nationalen Abwehrzentren sofort, Achtung, da rollt eine Welle auf uns zu. Sie können dann kritische Infrastrukturen warnen, spezifischen Datenverkehr blockieren und Netzwerke abdichten, und zwar noch bevor der Hackerangriff sich flächendeckend ausbreitet. Okay, da muss ich zugeben, das ergibt absolut Sinn. Das ist wie so ein Frühwarnsystem für Tsunamis. Genau das ist es. Aber was, wenn man sich als Unternehmen einfach nicht an diese 24 Stunden hält oder wenn man generell schummelt und gar kein sicheres Design baut, was sind da die Sanktionen? Wahrscheinlich nicht nur ein böser Brief aus Brüssel, oder?

## Marktaufsicht und Anwendungstermine

**20:55** Ganz und gar nicht. Die Marktüberwachungsbehörden bekommen richtig Zähne. Sie können Produkte europaweit zurückrufen lassen und das bedeutet einen massiven Imageschaden und immense Kosten für die Firma. Und Geldstrafen? Ja. Sie können drastische Geldbußen verhängen. Die bewegen sich im zweistelligen Millionenbereich oder orientieren sich an einem prozentualen Anteil des weltweiten Jahresumsatzes. Je nachdem, was höher ist. Das tut weh.

**21:23** Aber, und das ist wichtig, um auf die Verhältnismäßigkeit zurückzukommen, um Startups und winzige Betriebe nicht wegen eines rein formalen Fehlers sofort zu vernichten, gibt es Ausnahmen. Zum Glück. Ja, gegen Kleinst- und Kleinunternehmen werden keine Geldbußen verhängt, wenn sie nur diese extrem knappe 24-Stunden-Frist verpassen. Vorausgesetzt, sie arbeiten ansonsten kooperativ mit den Behörden

zusammen. Ein bisschen Gnade vor Recht für die Kleinen. Das ist fair. Wie viel Zeit bleibt der Industrie denn jetzt eigentlich noch, um ihre alten Gewohnheiten über Bord zu werfen? Wann wird dieser Sheriff in diesem digitalen Wilden Westen aktiv?

**21:58** Der Zeitplan ist echt straff, aber er ist gestaffelt. Die allgemeine Gültigkeit des CRA beginnt am 11. Dezember 2027. Das ist der Tag, an dem das neue CE-Kennzeichen und die Designpflichten endgültig greifen. Aber Vorsicht, die Pflichten zur Meldung von Schwachstellen und Vorfällen, also diese 24-Stunden-Regel, genau die über die wir gerade so intensiv gesprochen haben, die startet bereits über ein Jahr früher, nämlich schon am 11. September 2026. Ab da tickt die Uhr im Krisenfall.

**22:28** Wahnsinn. Lass uns das kurz mal alles zusammenfassen, weil das war jetzt super viel Input. Also, der Wilde Westen der unsicheren IoT-Geräte und der ganzen lückenhaften Software, der bekommt endlich ein strenges Regelwerk. Von der einfachen Smart-Home-Kamera über den Passwort-Manager bis hin tief rein in die Mikroprozessoren, Sicherheit ist künftig eine gesetzliche Pflicht ab Werk. Richtig. Fünf Jahre garantierte Updates werden die absolute Norm. Hersteller müssen über so eine SBOM exakt wissen, welche digitalen Zutaten in ihren Produkten stecken. Wer Open Source kommerziell nutzt, der haftet dafür. Und wer gehackt wird, der muss das in einem hochsicheren System innerhalb von 24 Stunden melden. Präzise auf den Punkt gebracht.

**23:09** Es ist wirklich ein gigantischer Schritt. Wer künftig auf diesem lukrativen EU-Markt verkaufen will, der muss sich anpassen. Völlig egal, ob die Firma in München, im Silicon Valley oder in Shenzhen sitzt. Und das ist auch mein wichtigster Hinweis an dich, wenn du uns gerade zuhörst. Wenn du in Zukunft eine Software kaufst, sei es für dein Zuhause, wenn du im Büro eine neue IT-Lösung ausrollst. Frag den Verkäufer proaktiv nach der SBOM. Und frag ganz gezielt nach dem garantierten Ende des Supportzeitraums. Sehr guter Tipp. Du hast ab dem Geltungsbeginn des CRA ein gesetzliches Recht auf diese Antworten. Du kaufst ab dann nicht mehr die digitale Katze im Sack. Absolut. Du erwirbst ein Produkt, für das der Hersteller wirklich umfassend Rechenschaft ablegen muss.

## Produkthaftung und Schlussgedanke

**23:54** Und während wir heute so viel über Bußgelder und Verstöße gesprochen haben, mir ist beim erneuten Lesen des Textes noch etwas aufgefallen. Oh, was denn? Das ist mir vorhin fast entgangen, aber es ist eigentlich der ultimative Hammer. Wenn wir in den Erwägungsgrund 31 schauen, gibt es da einen echt winzigen, unscheinbaren Querverweis. Ich ahne, worauf du hinaus willst. Da steht, dass der Cyber Resilience Act Hand in Hand mit der neuen EU-Produkthaftungsrichtlinie funktioniert. Der Verordnung 2024/2853. Oh, ja, die Produkthaftungsrichtlinie.

**24:30** Das ist die juristische Abrissbirne, die das Ganze auf ein völlig neues Level hebt. Lass dir das mal auf der Zunge zergehen. Diese Richtlinie führt für Software das Prinzip der verschuldensunabhängigen Haftung ein. Das ist gewaltig. Das bedeutet ganz konkret, wenn ein Hersteller dir kein rechtzeitiges Sicherheitsupdate liefert, was nach dem CRA jetzt ja seine verfluchte gesetzliche Pflicht ist und dir als Nutzer entsteht

dadurch ein Schaden. Dein Firmennetzwerk wird durch genau diese Lücke lahmgelegt oder deine Kontodaten werden aus dem Babyphone gestohlen. Dann könntest du diesen Hersteller direkt auf Schadensersatz verklagen.

**25:05** Richtig. Unabhängig davon, ob der Hersteller den Hack direkt verursacht hat. Allein das fehlende Update reicht für die Haftung aus. Wir reden hier nicht mehr nur über Bußgelder an den Staat, wir reden über zivilrechtliche Millionenklagen von Nutzern. Da dämmert mir gerade etwas. Wird die bloße Angst vor massiven Schadensersatzklagen, der Tech-Industrie endlich dieses alte Silicon Valley-Motto „Move fast and break things“ austreiben?

**25:31** Das ist eine brillante Schlussfolgerung. Denn genau das ist die Konsequenz aus dem Ganzen. „Move fast and break things“ funktioniert nur, solange man für das, was kaputt geht, nicht bezahlen muss. Und das ändert sich jetzt für immer. Eine völlig neue Zeitrechnung für Software, würde ich sagen. Denk mal darüber nach, wenn du heute Abend dein nächstes Update auf dem Handy installierst. Bisher war Cybersicherheit ja oft eher so eine Glaubensfrage. Mit dem Cyber Resilience Act haben wir nun endlich den Versuch, Sicherheit sichtbar, messbar und vor allem einklagbar zu machen. Das war unsere tiefe Analyse für heute. Bleibt neugierig.