ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Der EU Cyber Resilience Act: Empfehlung zur Umsetzung technischer Anforderungen

Steven Arzt
George Gkoktsis
Michael Kreutzer
Kirstin Scheel
Linda Schreiber

Version 1.0
Oktober 2024

EDITH GERMANY
Enabling Digital Innovation & Technology in Hesse

Der EU Cyber Resilience Act: Empfehlung zur Umsetzung technischer Anforderungen

Impressum

Kontakt
Nationales Forschungszentrum für
angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

Autoren

Steven Arzt
George Gkoktsis
Michael Kreutzer
Kirstin Scheel
Linda Schreiber

Förderhinweis

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) und des Hessischen Ministeriums für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.
Des Weiteren wurde die Erstellung unterstützt durch das BMBF-Projekt StartupSecure und von der Förderung des European Digital Innovation Hub EDITH vom European Commission's Digital Europe Programme.

Inhalt

Das Wichtigste im Überblick

Der **EU Cyber Resilience Act (CRA)** wurde im Oktober 2024 verabschiedet.[1] Nach einer Umsetzungsfrist von 21 bzw. 36 Monaten gelten dann **EU-weit einheitliche, branchen- und bereichsübergreifende Anforderungen für die Cybersicherheit von vernetzten Hard- und Softwareprodukten**. Dieser umfassende Regulierungsansatz des CRA wird viele Unternehmen erstmalig mit Vorschriften zur Cybersicherheit verpflichten, die durch die bisherigen produkt-, verbraucher- oder sektorspezifische Regelungen nicht erfasst sind.

Damit ihre Produkte weiterhin erfolgreich am Markt bestehen können und zukunftsfähig bleiben, sollten sich Hersteller von Produkten mit digitalen Elementen daher frühzeitig mit den Anforderungen des CRA befassen. Neben zusätzlichen Verpflichtungen bietet der CRA den Unternehmen jedoch auch einen Anlass und eine Chance zur Verbesserung bestehender und neuer Produkte sowie der zugehörigen internen Prozesse. So kann Cybersicherheit zum Qualitätsausweis der eigenen Produkte werden. Dies stärkt nicht nur das Vertrauen von Kunden, sondern verbessert auch die internationale Wettbewerbsfähigkeit. Der CRA wird voraussichtlich auch dazu führen, dass die Nachfrage nach Produkten mit transparenten Cybersicherheitseigenschaften verstärkt wird.

Die Vorschriften des CRA betreffen **Produkte, die im EU-Markt angeboten und vertrieben werden**. Die meisten Verpflichtungen adressieren die **Hersteller** dieser Produkte, unabhängig davon, ob diese selbst in der EU niedergelassen sind oder nicht. Um eine möglichst lückenlose Durchsetzung der CRA-Anforderungen sicherzustellen, werden neben Herstellern auch **weitere Akteure (sog. Einführer und Händler)** entlang der Lieferkette betroffener Produkte verpflichtet.

1 Dieses Whitepaper bezieht sich auf den Stand der CRA-Entwurfsversion vom 12.03.2024 (abrufbar unter: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.pdf).

Der CRA betrifft Produkte unabhängig davon, ob sie für **private Endnutzer oder für den Business-to-Business-Markt (B2B)** gedacht sind. **Auch Komponenten oder Bauteile**, die für die Integration in größere Produkte am Markt angeboten werden, sind vom CRA erfasst.

Die Anforderungen des CRA gelten für den **gesamten Lebenszyklus** eines betroffenen Produktes: Die Cybersicherheitsvorgaben des CRA müssen **ab der Konzeptionsphase und über einen Support-Zeitraum von mindestens fünf Jahren** erfüllt werden. Darüber hinaus orientiert sich der CRA an der voraussichtlichen Nutzungsdauer des Produkts.

Außerdem verpflichtet der CRA die Hersteller dazu, die Transparenz von Cybersicherheitseigenschaften zu verbessern, damit Nutzer die entsprechenden Produkte auch sicher verwenden können. Dies umfasst sowohl eine **Dokumentation der erwarteten Einsatzbedingungen** als auch eine **sichere Standardkonfiguration** des Produkts.

Der CRA schreibt zudem Prozesse für **eingehende Schwachstellenmeldungen sowie Sicherheitsvorfälle** vor. So soll es neben den eigenen Kunden z. B. auch unabhängigen Sicherheitsforschenden ermöglicht werden, Schwachstellen in den Produkten beim Hersteller zu melden. Entsprechende Meldungen sind vom Hersteller zu bearbeiten. Ebenfalls müssen Hersteller **Sicherheitsupdates** bereitstellen und die Nutzer über diese Updates informieren, wobei auch automatische Updates nicht nur vom Produkt unterstützt, sondern auch zur verpflichtenden Standardkonfiguration werden sollen.

Der CRA legt weitere **essenzielle Sicherheitsanforderungen** fest, die jedes Produkt mit digitalen Elementen erfüllen muss, insbesondere um die Vertraulichkeit, Integrität und Verfügbarkeit der Dienste und Daten sicherzustellen. Die übergreifende Verpflichtung der Hersteller besteht darin, **Produkte** an den Markt zu bringen, die ein **angemessenes Cybersicherheitsniveau gewährleisten**. Die Angemessenheit richtet sich dabei nach einem **Risikomodell**. Abhängig von der Produktkategorie durchlaufen sie zum Nachweis dieses Ziels ein definiertes **Konformitätsbewertungsverfahren**.

Neben der eigenen Implementierung ist die **Sicherheit der verwendeten Drittanbieterkomponenten** ein wesentlicher Bestandteil der Sicherheitsanforderungen des CRA. Hersteller müssen die verwendeten Komponenten kennen und eine **Software-Stückliste (SBOM)** führen. Wenn **Sicherheitslücken** in Drittsoftware bekannt werden, kann anhand

der Stücklisten festgestellt werden, ob Komponenten des Produkts diese Software ebenfalls enthalten und falls ja, folgt die Bewertung der **Auswirkungen der Lücken auf die Sicherheit des Produkts**.

Dieses Whitepaper richtet sich in erster Linie an Personen in herstellenden Unternehmen, die den Rahmen für die technische Entwicklung gestalten, also z. B. grundsätzlich an alle Verantwortlichen in der Produktentwicklung. Es adressiert auch Personen, die den Rahmen für Prozesse rund um die Produktentwicklung gestalten und verantworten, inklusive diejenigen, die in Prozesse für eingehende Schwachstellenmeldungen und Sicherheitsvorfälle nach dem Go-live involviert sind.

Dieses Whitepaper fokussiert die **technische Umsetzung** der Vorgaben des CRA und die damit verbundenen Prozesse. Ein weiteres Whitepaper mit einem Fokus auf die **rechtlichen Anforderungen** des CRA steht auf der Webseite von ATHENE ebenfalls zur Verfügung.

Der CRA reguliert umfassende technische Themenfelder. Aus diesem Grund kann dieses Whitepaper nur als Einstieg dienen. Für weitere Hilfestellungen und Unterstützung steht Ihnen ATHENE zur Verfügung: Als Nationales Forschungszentrum für angewandte Cybersicherheit unterstützt ATHENE Einrichtungen, die Fragen rund um den Themenkomplex CRA haben – beispielsweise durch Lunch Lectures. Die ATHENE-Forschenden werden die weitere Entwicklung beobachten und begleiten.

Die folgende ATHENE-Webseite enthält Veranstaltungen, Ansprechpartner und weitere Informationen zum CRA sowie ein Whitepaper mit Fokus auf die rechtlichen Anforderungen des CRA und die jeweils aktuelle Version dieses Whitepapers:
https://www.athene-center.de/cra

Gegenstand und Ziel des Whitepapers

Die technische Umsetzung von Anforderungen des CRA in herstellenden Unternehmen steht im Fokus dieses Whitepapers. Im Folgenden werden verschiedene Themen und Maßnahmen beleuchtet, die in Entwicklungs- und Pflegeprozessen sowie in den Organisationsabläufen zu beachten sind – bis hin zu Prozessen, die angepasst oder neu initiiert werden sollten.

Eine frühzeitige Auseinandersetzung mit diesen Anforderungen ist essenziell, um eine proaktive Planung der Ressourcen zu ermöglichen. Das Whitepaper bietet Hinweise für verschiedene horizontale und vertikale Zuständigkeiten im Unternehmen und gibt den Verantwortlichen die Möglichkeit, sich rechtzeitig und vorausschauend mit den Anforderungen und Empfehlungen auseinanderzusetzen.

Die verschiedenen Kapitel dieses Whitepapers können Personen mit unterschiedlichen Rollen und Verantwortlichkeiten im Unternehmen als Unterstützung dienen. Zur besseren Orientierung und Identifizierung, was die für Sie relevanten Kapitel sind, erfolgt im Folgenden eine kurze Übersicht zum Gegenstand der einzelnen Kapitel.

1. Bewertung von Cybersicherheitsrisiken als Grundlage der Umsetzung

Der CRA schreibt Herstellern vor, eine **Risikobewertung für die Cybersicherheit ihrer Produkte** durchzuführen, welche in allen Phasen des Produktlebenszyklus zu berücksichtigen ist, um Cybersicherheitsrisiken und Auswirkungen von Vorfällen zu minimieren. Diese Risikobewertung bildet auch die Grundlage für die Umsetzung der grundlegenden

Anforderungen an die Cybersicherheit. In diesem Kapitel wird das grundlegende Vorgehen einer solchen Risikoanalyse vorgestellt und skizziert.

2. TECHNIK: Produkte ohne bekannte ausnutzbare Schwachstellen und 3. TECHNIK: Software-Stückliste und 4. TECHNIK: Sicherheits- und Schwachstellentests

Der CRA liefert eine Liste mit grundlegenden **Anforderungen an die Cybersicherheit** von Produkten und an festzulegende Verfahren zur **Behandlung von Schwachstellen**, die von Herstellern umzusetzen sind. In diesen Kapiteln werden einzelne **technische Anforderungen** herausgegriffen, die eine Umsetzung am Produkt selbst erfordern. Dabei handelt es sich um die Anforderungen, das Produkt **ohne bekannte ausnutzbare Schwachstellen** auszuliefern, eine **Software-Stückliste (SBOM)** zu erstellen sowie **Sicherheits- und Schwachstellentests** durchzuführen. Zu diesen Anforderungen erfolgt eine Betrachtung des Zwecks sowie der Vorgaben aus dem CRA, zudem konkrete, praxisnahe Empfehlungen zur Umsetzung.

5. PROZESSE: Implementierung einer koordinierten Schwachstellenstrategie (CVD)

Dieses Kapitel behandelt eine Anforderung, die auf Prozessebene umzusetzen ist: Die Möglichkeit der **Meldung von Schwachstellen beim Hersteller** (Coordinated Vulnerability Disclosure) durch Externe.

6. KENNZEICHNUNG: CE-Kennzeichnung

Der CRA enthält die Vorgabe, dass Hersteller ein CE-Kennzeichen auf dem Produkt mit digitalen Elementen anbringen müssen, bevor sie es in den Verkehr bringen. Das Anbringen des CE-Kennzeichens ist sichtbarer Ausdruck der Konformität eines Produktes mit den Anforderungen des CRA. Dieses Kapitel gibt einen Überblick über formale Vorgaben des CRA von der Dokumentation zur Bewertung der Konformität bis hin zur Anbringung des CE-Kennzeichens.

Grundsätzlich folgen die Kapitel 2 bis 7 der gleichen Struktur und gliedern sich entlang der folgenden Fragen:

„Worum geht es?“ gibt eine kurze, allgemeinverständliche Themeneinführung;

„Was sagt der CRA?“ stellt die spezifischen rechtlichen Anforderungen dar, die sich aus dem CRA ergeben, und

„Was sind unsere Empfehlungen?“ präsentiert konkrete, praxisnahe Vorschläge und Empfehlungen zur Umsetzung der jeweiligen Anforderung.

Die Kapitel 1, 5 und 7 sind mit Blick auf die Umsetzung eher prozessorientiert.

Die Kapitel 2, 3 und 4 fokussieren sich eher auf technische Themen.

Kapitel 6 erläutert die CE-Kennzeichnung.

7. PROZESSE: Meldepflichten der Hersteller

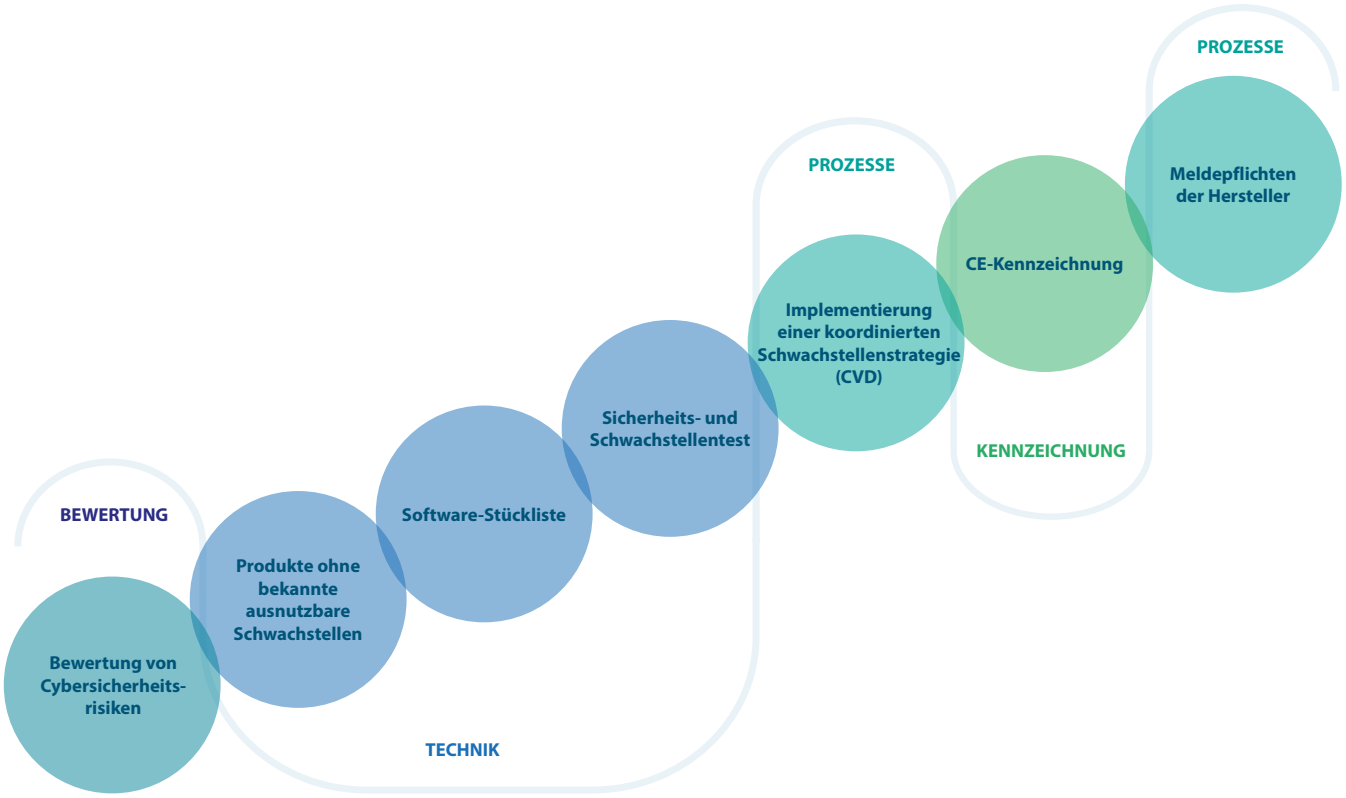
Ergänzend zum Kapitel 5 wird in diesem Kapitel eine weitere Anforderung auf Prozessebene betrachtet: die **Meldepflichten der Hersteller bei den zuständigen Behörden** im Falle von aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen mit Bezug zu ihren Produkten.

Bei der Erfüllung der Meldepflichten sind Fristen und verpflichtende Mindestangaben zu beachten.
Ausgehend von der grundlegenden Risikoanalyse in Kapitel 1 entwickeln sich die weiteren Themen; die Abfolge der Behandlung ist eine aus Erfahrungswissen gespeiste good practice, aber durch den CRA nicht vorgegeben.

Bei den in diesem Whitepaper vorgestellten **Empfehlungen** handelt es sich um **in der Praxis erprobte und bewährte Maßnahmen**, die ein Unternehmen und dessen Produkte grundsätzlich gut aufstellen und zukunftsfähig für Cybersicherheitsherausforderungen machen.

Mit der Verabschiedung des Cyber Resilience Acts ist die juristische Grundlage festgelegt. Doch auch nach der Verabschiedung sowie während der Umsetzungsphase und danach werden verschiedene **Konkretisierungen der Vorgaben des CRA durch nationale und europäische Behörden sowie ggf. auch die Rechtsprechung** zu treffen sein. Vor diesem Hintergrund sind die Darstellungen in diesem Whitepaper als **vorläufige Einschätzungen** zu sehen. Dementsprechend sind die gegebenen Empfehlungen also nicht dahingehend zu verstehen, dass sie abschließend sind und eine automatische Konformität mit dem CRA garantieren.

Zudem ist im Zusammenhang mit den Empfehlungen zu beachten, dass die konkrete Umsetzung des CRA und die Wahl der Mittel und Maßnahmen jeweils stark von der Art des Produktes, der Kritikalität sowie den assoziierten Risiken abhängt. Nicht jede Empfehlung wird für jedes Produkt zielführend oder erforderlich sein, es gibt **keine One-Size-Fits-All-Lösungen**.



Grafik 1: Die Bereiche zur Erfüllung der Anforderungen des CRA.

01 Bewertung von Cybersicherheits-risiken als Grundlage der CRA-Umsetzung

Worum geht es?

Informations- und Informationsmanagementsysteme werden zunehmend komplexer, die Bedrohungslandschaft ebenfalls. Gleichzeitig bedeutet die Innovationsgeschwindigkeit in der Informationstechnologie, dass die Vorhersage von IT-Sicherheitsrisiken über einen Zeitraum von mehreren Jahren, einschließlich aller Phasen des Produktlebenszyklus, eine nicht zu unterschätzende Aufgabe ist.

Aus diesen Gründen ist ein Verständnis des **grundlegenden Unsicherheitsfaktors „Risiko"** sowie seiner konzeptionellen Grenzen in Verbindung mit ggf. bereits bewährten Praktiken und Methoden, besonders mit Blick auf die Umsetzung der Vorgaben des CRA, von entscheidender Bedeutung: Andernfalls kann es zu einer **Unter- oder Überschätzung möglicher Bedrohungen** und der damit verbundenen Risiken kommen. Dies kann nicht nur dazu führen, dass anfällige/unsichere Produkte auf den EU-Markt gebracht werden, sondern auch zu einer Fehlbewertung der potenziellen Kosten für die Unternehmen im Schadensfall, was mikro- und makroökonomische Folgen nach sich ziehen würde. Ebenso kann es zu einer Fehlplanung der notwendigen Maßnahmen führen, indem entweder teure und unnötige Maßnahmen ergriffen werden, oder indem umgekehrt notwendige Maßnahmen unterbleiben.

Der entsprechende **Risiko-Management-Prozess** muss geplant und dokumentiert werden: Wie werden Risiken ermittelt, wie werden sie bewertet, behandelt – und anschließend überwacht. So gibt es z. B. etablierte

asset- oder szenariobasierte Ansätze zur Risikoermittlung, quantitative oder qualitative Risikobewertungsmethoden und unterschiedliche Methoden zur Risikoberechnung. Sind diese Schritte erfolgt und dokumentiert, ist eine kontinuierliche Überwachung der Risiken sowie eine laufende Berichterstattung über den Sicherheitsstatus der entsprechenden Produkte nötig. Da sich nicht jegliches Risiko komplett ausschließen lässt, braucht es zudem eine **Vorbereitung auf z. B. mögliche Vorfälle** und eine vorausschauende Entwicklung von Reaktionsstrategien im Rahmen eines **Notfallmanagements**.

Obwohl der Verwendungszweck eines Produkts mit digitalen Elementen zum Zeitpunkt der Zulassung genau beschrieben werden kann, ist die **vorhersehbare Verwendung des Produkts** innerhalb jahrelanger operativer Nutzung mit Unsicherheit behaftet. Die Entwurfsspezifikationen und die Entwicklung der Softwarefunktionen sind in den frühen Phasen des Lebenszyklus des Produkts (noch) nicht notwendigerweise umfassend bekannt. Wenn neue/weitere Funktionen z. B. als Software-Patch bereitgestellt werden, wird das Cybersicherheitsrisiko unbeständig.

Eine gewisse **strukturelle und technische Unsicherheit** des der Analyse zugrunde gelegten Bedrohungsmodells ist unvermeidlich und wird normalerweise bei der Risikobewertung berücksichtigt oder umgangen. Sie gewinnt aber an Bedeutung, wenn sie mit den anderen Unsicherheiten in Bezug auf die Art und den vorhersehbaren Gebrauch von Produkten mit digitalen Elementen zusammentrifft.

Der Risikobegriff folgt im Regelfall der Knight'schen Definition, d.h. das Risiko ist das Produkt aus der Eintrittswahrscheinlichkeit des Schadensereignisses und der Höhe des Schadens. In einigen Risikobewertungssystemen wird die Eintrittswahrscheinlichkeit des Schadens weiter aufgespalten in die Wahrscheinlichkeit, dass ein Angriff stattfindet, und die Wahrscheinlichkeit, dass der Angriff erfolgreich ist. In jedem Fall besteht die Herausforderung darin, die Zahlenwerte oder zumindest Kategorien (niedrig, mittel, hoch) adäquat zu schätzen.

Bei der Schadenshöhe ist das Vorgehen analog zu anderen Betriebsrisiken. Der entgangene Gewinn durch einen Tag Produktionsausfall (z. B. Nichtverfügbarkeit eines remote gesteuerten Schweißroboters) oder der Wert eines auf einer Fräse verarbeiteten CAD-Modells als Firmengeheimnis (Verlust der Vertraulichkeit) sind im Regelfall bekannt. Diese

Konsequenzen finden sich oftmals auch in Risikomodellen jenseits der IT, z. B. wenn besagter Roboter aufgrund eines Defekts ausfällt. In weniger eindeutigen Fällen sind zumindest grobe Richtwerte ableitbar.

Die Unsicherheit bzgl. der Eintrittswahrscheinlichkeit ist regelmäßig größer. Stehen Datenquellen (Richtwerte einer Branche, Daten von Versicherern, historische Daten des eigenen Unternehmens, usw.) zur Verfügung, bieten diese sich als Grundlage an. Ansonsten lässt sich im Regelfall eine kategorisierte Abschätzung (niedrig, mittel, hoch) treffen. Diese ist selbstredend von Unsicherheit geprägt und muss kontinuierlich auf Basis von z. B. Vorfällen im eigenen Unternehmen, aber auch mit vergleichbaren Produkten anderer Hersteller geprüft und ggf. angepasst werden.

Insgesamt ähnelt die Risikobetrachtung des CRA den bekannten Betrachtungen des Betriebsrisikos. Ob bspw. Ersatzteile für einen Roboter bevorratet werden müssen für den Fall einer technischen Störung folgt ähnlichen Mustern einer Kosten-/Risiko-Betrachtung. Die zu ergreifenden Maßnahmen müssen das Restrisiko auf ein vertretbares Maß reduzieren, das gemeinhin nicht null sein wird. Existierende Standards wie bspw. die ISO 27005 können als Grundlage für das eigene Risikomodell dienen.

In der Praxis gibt es für Informationstechnologien bestehende Ansätze und normierte Vorgehensweisen, die z. T. untereinander kompatibel sind. So hat z. B. die European Union Agency for Cybersecurity (ENISA) solche Rahmenwerke in einem Compendium gegenübergestellt, ihre Interoperabilität verglichen[2] und daraus ein „Interoperable EU Risk Management Framework“[3] sowie eine „Interoperable EU Risk Management Toolbox“[4] entwickelt. Diese können als Orientierung dienen und bei der Integration verschiedener Risiko-Management-Methoden im Umfeld einer Organisation oder organisationsübergreifend helfen. Hinzu kommt eine Handreichung spezifisch zu „Cyber Resilience Act Requirements Standards Mapping“[5], welche Standards konkret auf einzelne Anforderungen des CRA referenziert.

2 https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks, abgerufen am 15.10.2024.
3 https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework, abgerufen am 15.10.2024.
4 https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox, abgerufen am 15.10.2024.
5 https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping, abgerufen am 15.10.2024.

Sollten in einer Organisation bereits entsprechende anerkannte Methodiken im Einsatz und/oder Zertifizierungen vorhanden sein (wie z. B. nach der ISO/EC 27001 bzw. ISO/EC 27005 oder BSI-Standard[6] 200-2 bzw. 200-3 (IT-Grundschutz ISMS bzw. Risikomanagement)), welche sich bereits mit dem Thema befassen, so können diese womöglich für die spezifischen Pflichten, die der CRA fordert, angepasst werden.

Was sagt der CRA?

Eines der Ziele des CRA ist es, Verbraucher und Organisationen vor Cybersicherheitsrisiken zu schützen (Erwgr. 32 CRA).

Als Cybersicherheitsrisiko wird im CRA das **Potenzial für Verluste und Störungen**, die durch einen Sicherheitsvorfall verursacht werden, verstanden. Dieses ergibt sich aus dem Ausmaß eines Verlustes oder einer Störung sowie der Wahrscheinlichkeit des Eintretens eines Sicherheitsvorfalls (Art. 3 Nr. 37 CRA).

Gemäß Art. 13 Abs. 2 CRA haben Hersteller eine **Bewertung der Cybersicherheitsrisiken** durchzuführen, die ein Produkt mit digitalen Elementen birgt. Das Ergebnis ist bei der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase eines Produktes mit digitalen Elementen zu berücksichtigen, um Cybersicherheitsrisiken und Auswirkungen von Vorfällen zu minimieren. Diese Risikobewertung dient auch als Grundlage für die Umsetzung der wesentlichen Cybersicherheitsanforderungen aus Anhang I Teil I Abs. 2 CRA, welche im Anhang im Überblick dargestellt werden.

Die **Risikobewertung** umfasst gemäß Art. 13 Abs. 3 CRA mindestens eine Analyse von Cybersicherheitsrisiken auf der Grundlage

- der Zweckbestimmung,
- der vernünftigerweise vorhersehbaren Verwendung (z. B. die Betriebsumgebung oder zu schützende Vermögenswerte) sowie
- der voraussichtliche Nutzungsdauer

des Produktes mit digitalen Elementen.

6 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html, abgerufen am 15.10.2024.

Die **Risikobewertung ist zu dokumentieren** und gegebenenfalls während des Support-Zeitraums zu aktualisieren (Art. 13 Abs. 7 CRA). Eine **Aktualisierung** der Risikobewertung ist beispielsweise denkbar, wenn Produkte mit digitalen Elementen nachträglich physisch oder digital in einer Weise verändert werden, wie es in der ursprünglichen Risikobewertung nicht vorgesehen war. Dies gilt auch, wenn sich die Zweckbestimmung des Produktes ändert, wenn Softwareaktualisierungen mit nachteiligen Auswirkungen für das Cybersicherheitsrisiko durchgeführt wurden, die Angriffsfläche des jeweiligen Produktes durch das Hinzufügen neuer Funktionen vergrößert wurde oder sich die Art der Gefahr für das Produkt geändert hat, wie bei der Entdeckung neuer Schwachstellen (siehe Erwgr. 38 und 39 CRA).

Zudem ist anzugeben, ob und gegebenenfalls in welcher Weise die Sicherheitsanforderungen gemäß Anhang I Teil I Abs. 2 CRA auf das jeweilige Produkt mit digitalen Elementen anwendbar sind und wie diese gemäß den Ergebnissen der Risikobewertung umgesetzt werden (Art. 13 Abs. 3 CRA).

Was ist unsere Empfehlung?

Wie bereits angeklungen ist, fordert der CRA keine komplett neuartigen Methoden, sondern orientiert sich an **etablierten Vorgehensweisen des Risiko- und Notfallmanagements**. Mit welcher Methodik man sich genau den Themen Identifikation von Risiken, Bewertung von Risiken, Implementierung von Schutzmaßnahmen, Überwachung und Überprüfung, Notfallmanagement sowie Schulung und Sensibilisierung nähert, können Verantwortliche entscheiden bzw. im Rahmen vorhandener Dokumentationen und Zertifizierungen entsprechend anpassen – andere gesetzliche Vorgaben haben diesbezüglich ggf. bereits an anderen Stellen ähnliche interne Analysen veranlasst.

Neben internationalen Standards könnte sich in deutschen Unternehmen z. B. eine Einbettung im Rahmen der BSI-Grundschutz-Zertifizierung anbieten. Andere europäische Länder haben z. T. entsprechende Grundlagen (vgl. z. B. Österreichisches Informationssicherheitshandbuch[7] oder die niederländische „Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K analysis)“[8]). Im Sinne der Effizienz bietet es sich an, die Umsetzung von vornherein ins gesamte IT-Sicherheits- sowie Compliance-Management einzubinden, um Doppelarbeit zu vermeiden bzw. minimieren.

7 https://www.sicherheitshandbuch.gv.at/, abgerufen am 10.07.2024.
8 https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_dutch_ak_analysis.html, abgerufen am 10.07.2024.

02 TECHNIK: Produkte ohne bekannte ausnutzbare Schwachstellen

Worum geht es?

Eines der übergeordneten Ziele des CRA ist gemäß Erwgr. 2 CRA, dass Hard- und Softwareprodukte **mit weniger Schwachstellen in den Verkehr** gebracht werden. Ursachen von Schwachstellen können sowohl im eigenen Code als auch im Code der verwendeten **Drittanbieterkomponenten** (z. B. Bibliotheken) liegen. Die Empfehlungen in diesem Zusammenhang fokussieren sich auf letzteres.

In der Vergangenheit haben Lücken in verbreiteten Bibliotheken wie log4j dazu geführt, dass zahlreiche Produkte verwundbar waren, weil sie log4j verwendet haben. Da sich solche Lücken nie hundertprozentig vermeiden lassen, erfordert der CRA nun, dass Hersteller ihre verwendeten Komponenten kennen (mehr dazu im Kontext der Software Bill of Materials s. u.) und auf Sicherheitslücken überwachen. Werden Schwachstellen in diesen Komponenten bekannt, müssen Hersteller reagieren und ggf. ihr eigenes Produkt aktualisieren.

Im einfachsten Fall muss nur die verwendete Bibliothek gegen eine neuere Version ausgetauscht werden. In anderen Fällen erfordert dies auch Anpassungen an der eigenen Software.

Dabei ist zu bedenken, dass ein Produkt mit digitalen Elementen nicht nur aus Software bestehen muss. So kann in einem Smart TV z. B. auch ein in Hardware implementiertes Receiver-Modul einer Fremdfirma zugekauft und verbaut sein. Auch dieses Modul kann Schwachstellen beisteuern

und muss genauso behandelt werden wie eine in den eigenen Code einkompilierte oder auf dem eigenen Steuergerät installierte Software-Bibliothek.

Der CRA fokussiert sich auf **ausnutzbare Schwachstellen**. Dies bedeutet, dass Schwachstellen prinzipiell toleriert werden können, wenn sie im Kontext des Produkts nicht ausgenutzt werden können.

Was sagt der CRA?

Der CRA enthält verschiedene grundlegende Anforderungen, die sich auf von Herstellern festzulegende Verfahren und Maßnahmen zur Behandlung und Behandelbarkeit von Schwachstellen beziehen. Eine dieser Anforderungen ist gemäß Anhang I Teil I (2)(a) CRA, dass Produkte mit digitalen Elementen „ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden".

Für diese Anforderung ergibt sich die Ermittlung von für das jeweilige Produkt einschlägigen Risiken und Anforderungen ebenfalls aus der spezifischen Bewertung von Cybersicherheitsrisiken (siehe Kap. 2.).

In **Art. 3 Nr. 40 CRA** werden **Schwachstellen** als „Schwäche, Anfälligkeit oder Fehlfunktion eines Produkts mit digitalen Elementen, die bei einer Cyberbedrohung ausgenutzt werden" definiert. **Cyberbedrohungen sind dabei nach Art. 2 Nr. 8 des CSA** als mögliche Umstände, Ereignisse oder Handlungen zu verstehen, die Netz- und Informationssysteme, Nutzer dieser Systeme oder andere Personen schädigen, stören oder anderweitig beeinträchtigen könnten. Von Schwachstellen unterschieden werden nach Art. 3 Nr. 41 CRA **ausnutzbare Schwachstellen** als solche, die von einem Gegner unter praktischen Betriebsbedingungen wirksam genutzt werden können.

Bei der Beurteilung, ob eine Schwachstelle nicht nur ausnutzbar, sondern auch **bekannt** ist, soll auch die europäische Schwachstellendatendank unterstützen (Erwgr. 67 CRA). Diese soll künftig gemäß Art. 12 Abs. 2 NIS-2-Richtlinie durch die ENISA entwickelt und gepflegt werden und dazu dienen, dass Einrichtungen auf freiwilliger Basis öffentlich bekannte Schwachstellen in IKT-Produkten und IKT-Diensten offenlegen und registrieren, sowie sich hierzu informieren können. Dabei weist der EU-Gesetzgeber daraufhin, dass es

bereits jetzt ähnliche Register und Datenbanken gibt, die von Einrichtungen mit Sitz außerhalb der EU betrieben werden. Die ENISA hat hier den Auftrag, die Möglichkeit einer strukturierten Zusammenarbeit zu prüfen, um Doppelarbeit zu vermeiden (Erwgr. 63 NIS-2-Richtlinie).

Grundsätzlich ist es für den Umgang mit einer Schwachstelle unerheblich, ob diese in Open-Source-Komponenten oder in kommerziellen Komponenten identifiziert wurde.

Was ist unsere Empfehlung?

Empfehlung 1: Sorgsame Auswahl von Komponenten

Wir empfehlen, bereits bei der Auswahl der verwendeten Komponenten auf die Sicherheit dieser Komponenten zu achten. Gerade bei Open-Source-Komponenten sollte eine **Checkliste** angewendet werden, z. B. mit folgenden Leitfragen:

- Wird das Projekt immer noch **aktiv betreut**? Wann fand die letzte Codeänderung statt? Gibt es eine aktive Gemeinschaft (und nicht nur einzelne Beitragende) zum Projekt?
- Werden gemeldete oder gar öffentlich bekannte Sicherheitslücken **zeitnah geschlossen**?
- Gibt es Berichte, dass auf öffentlich bekannte Schwachstellen nicht in angemessener Zeit reagiert wurde?
- Wurden Schwachstellen in der Vergangenheit effektiv geschlossen oder waren mehrere Anläufe notwendig, bis die Lücke tatsächlich geschlossen wurde?
- Gibt es einen **Meldeprozess und Ansprechpartner** für Schwachstellenmeldungen? Wechseln diese Ansprechpartner häufig oder ist Kontinuität sichergestellt?

Lassen sich diese Fragen zufriedenstellend beantworten, kann das eigene Produkt durch Updates der verwendeten Komponenten abgesichert werden (mit Ausnahme von Zero-Day-Schwachstellen, die i. d. R. jedoch nicht als „bekannt" gelten, wenn sie vom Finder verantwortungsvoll gemeldet werden).

Lassen sich die Fragen nicht zufriedenstellend beantworten, besteht ein signifikantes Risiko, dass selbst die neueste Version bekannte Sicherheitslücken enthält. In diesem Fall wäre

der Hersteller verantwortlich, die Lücken selbst zu schließen. In der Praxis kann es sinnvoller sein, auf eine alternative Komponente auszuweichen.

Empfehlung 2: Verwendung aktueller Versionen

Wann immer eine neue Version eines Produkts herausgebracht wird, sollten die verwendeten Komponenten im Idealfall auf die jeweils neuesten verwendeten Versionen (nach ausführlichem, aus Effizienzgründen im Idealfall automatisiertem Test) aktualisiert werden, um das Risiko bekannter Schwachstellen durch veraltete Abhängigkeiten zu minimieren.

Empfehlung 3: Aktives Monitoring von Schwachstellen

Hersteller sollten ein **aktives Schwachstellen-Monitoring** auf den verwendeten Bibliotheken durchführen. So können öffentliche Repositories wie Maven Central bspw. mit Schwachstellenlisten wie Open Source Vulnerability Standard (OSV) abgeglichen werden, um verwundbare Komponenten und Versionen zu identifizieren.

Werden die Bibliotheken in einem unternehmensinternen Respository gespiegelt, lassen sich Prüfungen auch mit Reporting und ggf. sogar der Sperrung verwundbarer Komponenten verbinden. Letzteres stellt sicher, dass Software nicht mit verwundbaren Komponenten kompiliert werden kann, da der interne Spiegel solche Komponenten (Treffer in der Schwachstellenliste) nicht bereitstellt. Ebenso können automatisiert Warnungsmeldungen an Produktverantwortliche ausgelöst werden, wenn ein Buildprozess auf Komponenten mit bekannten Schwachstellen zugreift.

03 TECHNIK: Software-Stückliste

Worum geht es?

Eine **Software-Stückliste** (im Englischen oft als **"Software Bill of Materials"**, kurz **SBOM**, bezeichnet) ist eine Stückliste für Software. Sie gibt an, aus welchen Komponenten eine Software besteht. Die Stückliste kann unterschiedlichen Zwecken dienen. Sie ist nicht nur eine Anforderung des CRA und muss für eine etwaige Prüfung durch die Marktaufsichtsbehörde bereitgehalten werden, sondern ist auch ein wertvoller Datensatz für zahlreiche Prozesse im Unternehmen wie z. B. die Sicherstellung der Einhaltung der Lizenzen verwendeter Komponenten.

Viele Produkte mit digitalen Elementen basieren auf Open-Source-Komponenten. Diese stehen teilweise unter Lizenzen, die vorschreiben, dass die eigene Software, welche die Komponente verwendet, auch unter eine kompatible Lizenz gestellt werden muss ("Copyleft"). Für kommerzielle Geschäftsmodelle ist dies oftmals nicht gewünscht. Um das Risiko der unbeabsichtigten "Infektion" der eigenen Software mit einer solchen Lizenz zu reduzieren, muss jede verwendete Komponente mit ihrer jeweiligen Lizenz bekannt sein. Eine Software-Stückliste kann hierzu Auskunft geben.

Bei der Soft- und Hardwareentwicklung spielen **Komponenten von anderen Herstellern oder diverser Quellen und Bibliotheken** zudem eine sehr große Rolle für die Sicherheit des Produktes. Schwachstellen in populären Bibliotheken wie log4j haben gezeigt, welche Risiken Programmierfehler in Bibliotheken für eine Vielzahl von Produkten bedeuten können. Die Software-Stückliste ist ein essenzieller Baustein für das Management solcher Schwachstellen in verwendeten Bibliotheken. Aus der Stückliste geht hervor, welche Bibliothek in welcher Version genutzt wird. Bei Bekanntwerden einer Sicherheitslücke in einer Bibliothek, z. B. durch einen neuen CVE-Eintrag, kann diese Information gegen die

Stückliste abgeglichen werden, um zu erkennen, ob das eigene Produkt betroffen ist. Handelt es sich nur um eine Lücke in einer bestimmten ggf. veralteten Version, kann die Stückliste helfen zu erkennen, ob im Produkt vielleicht bereits eine neuere Version enthalten ist, welche die Schwachstelle nicht mehr enthält.

Neben Schwachstellen ist die Stückliste auch relevant, um nicht mehr weiter betreute Komponenten zu identifizieren. Komponenten erreichen ggf. ihr Lebensende, wenn kommerzielle Hersteller vom Markt verschwinden oder die Open-Source-Gemeinschaft sich anderen Projekten zuwendet. Da in einem solchen Fall keine Sicherheitsupdates mehr bereitgestellt werden und somit eine zeitnahe Behebung von Sicherheitslücken nicht mehr gewährleistet ist, stellen solche veralteten Komponenten ein Risiko dar. Mit der Stückliste können diese Komponenten identifiziert und für einen Austausch vorgesehen werden.

Die SBOM ist damit ein zentrales Thema der Software- und Lieferkettensicherheit, sowohl im Hinblick auf IT-Sicherheit als auch im Hinblick auf lizenzrechtliche Fragestellungen.

Was sagt der CRA?

Der CRA verpflichtet Hersteller unter Anhang I Teil II (1), eine „Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen“ zu erstellen, um Schwachstellen und Komponenten der Produkte mit digitalen Elementen zu ermitteln und dokumentieren. Grundsätzlich versteht der CRA eine Software-Stückliste gemäß Art. 3 Nr. 39 CRA als „formale Aufzeichnung der Einzelheiten und Lieferkettenbeziehungen der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind“.

Diese Stückliste ist **verpflichtender** Bestandteil der Technischen Dokumentation nach Art. 31, Anhang VII CRA für jedes Produkt mit digitalen Elementen und muss als solcher mindestens zehn Jahre für die Marktüberwachungsbehörde aufbewahrt werden (Art. 13 Abs. 13 CRA). Die Bereitstellung der SBOM für Nutzer ist für Hersteller **freiwillig** (Anhang II (9) CRA). Zudem soll es nach Art. 13 Abs. 25 CRA in Zukunft möglich sein, dass Informationen aus SBOMs anonymisiert und aggregiert verwendet werden, um EU-weite Bewertungen von Abhängigkeiten durchzuführen.

Das genaue Format und Elemente der SBOM kann später von der Europäischen Kommission im Wege von Durchführungsrechtsakten unter Berücksichtigung internationaler oder europäischer Standards festgelegt werden (Art. 13 Abs. 24 CRA).

Was ist unsere Empfehlung?

Empfehlung 1: Einbindung der SBOM in den Entwicklungsprozess

Um die Stückliste einerseits für die eigene Update-Strategie nutzbar zu machen und ihre Erstellung andererseits nicht zu einem zusätzlichen, manuell zu erstellenden Kostenfaktor werden zu lassen, empfiehlt sich eine **Einbindung der Stückliste in den Entwicklungsprozess**. Die Stückliste ist dabei genauso ein technisches Artefakt des Entwicklungsprozesses wie die kompilierte Software.

Bei der Softwareentwicklung überschneiden sich oftmals die Zuständigkeiten verschiedener Bereiche im Unternehmen. So wird der Code von der Entwicklungsabteilung geschrieben, während die Rechtsabteilung für Themen wie Lizenzverträge oder die Prüfung exportkontrollrechtlicher Vorschriften zuständig ist. Meist schlägt sich diese Trennung in unterschiedlichen Herangehensweisen, verwendeten Werkzeugen, usw. nieder. Die Stückliste ist jedoch, wie eingangs erläutert, ein übergreifender Aspekt. Sie muss aus Compliance-Gründen vorgehalten werden, dient der Entwicklungsabteilung zur Prüfung auf notwendige Aktualisierungen von Komponenten und ermöglicht der Rechtsabteilung, die Lizenzen der verwendeten Komponenten zu prüfen.

Wir empfehlen daher, einen **integrierten Prozess** zu wählen, der den Anforderungen aller betroffenen Stakeholder gerecht wird. Dabei beschränken wir uns auf die Dokumentation des Ist-Zustands der in einer Software verwendeten Komponenten. Etwaige Freigabeprozesse, ob eine bestimmte Komponente neu in die Software eingebracht werden darf, müssen separat behandelt werden.

Die Daten für die Erzeugung der Stückliste (Ist-Zustand) liegen in der Entwicklungsabteilung mindestens implizit vor. Andernfalls wäre es nicht möglich, die finale an den Kunden ausgelieferte oder auf dem Gerät installierte (z. B. Firmware

eines Smart TV) Software herzustellen. In modernen Entwicklungsprozessen mit automatisierten Test- und Erstellungsprozessen wird die Komposition des eigenen Codes mit den Bibliotheken auf Basis expliziter Beschreibungen automatisiert vorgenommen. Bei manuellen Integrationsprozessen besteht das Wissen organisatorisch im Integrationsprozess, da das finale Produkt offensichtlich funktionsfähig ist und somit nicht an übersehenen Abhängigkeiten scheitert.

Somit existiert de facto – ungeachtet des konkreten Datenformats – bereits eine Stückliste, auf die aufgebaut werden kann. Von einer separaten Pflege einer Stückliste als neue Compliance-Dokumentation in Parallelstrukturen raten wir daher ab. Wir sehen die **Entwicklungsabteilung als Eigner der Stückliste** im Sinne von "Code Ownership" und damit in der Verantwortung, die Stückliste mit den technischen Mitteln des Software-Engineering herzustellen und aktuell zu halten, genauso wie die finale integrierte Software selbst hergestellt und aktuell gehalten wird. Die **anderen Stakeholder**, z. B. für eine Lizenzprüfung, sehen wir als Konsumenten der Stückliste.

Empfehlung 2: Abhängigkeiten vollautomatisch erfassen

Mit einem modernen Entwicklungsprozess kann der Aufwand zur Erstellung der Stückliste minimiert werden, indem sich die automatisch erstellte Stückliste und die Erzeugung des Softwareprodukts aus derselben Datenquelle speisen. Gleichzeitig ist die Stückliste immer aktuell und wird mit jedem Erstellvorgang (z. B. Nightly Build) neu erzeugt.

Moderne Entwicklungsprozesse basieren oft auf **deklarativen Abhängigkeiten**. So wird bei Java bspw. nicht mehr mit einzelnen JAR-Dateien für abhängige Komponenten gearbeitet. Stattdessen wird in Build-Systemen wie Maven oder Gradle spezifiziert, welche Komponenten in welcher Version eingebunden werden sollen. Maven bzw. Gradle übernehmen die Bereitstellung der entsprechenden Dateien aus zentralen Repositories wie bspw. Maven Central oder einem firmeneigenen Spiegeldienst, der wiederum auf diesen öffentlichen Repositories basiert. Ähnliche Konzepte existieren für andere Plattformen, z. B. wenn MS Build mit NuGet für die Erstellung von .net-Anwendungen eingesetzt wird. In jedem Fall existiert eine maschinenlesbare Spezifikation mindestens der unmittelbaren Abhängigkeiten, welche ausreichend ist, um die Anforderungen des CRA zu erfüllen.

Die Spezifikationsdateien von Maven, Grade, NuGet, usw. lassen sich als Teil des Kompilierungsvorgangs auslesen und **z. B. in einer CSV-Datei pro Produkt** zusammenfassen oder in eine Datenbank schreiben. Zwar wird die EU-Kommission im CRA ermächtigt, ein einheitliches Zielformat festzulegen, dieses existiert jedoch bisher nicht. Daher ist der Hersteller in der Wahl des Formats derzeit noch frei, solange es üblich und maschinenlesbar ist. Sind diese Voraussetzungen erfüllt, sollte es später auch nicht schwerfallen, die Daten automatisiert in das EU-Format zu überführen, sobald (und falls) es definiert werden sollte.

Daneben bieten sich auch die verschiedenen Industriestandards wie CycloneDX an, die von Unternehmen und Organisationen wie der OWASP unterstützt werden. Der Vorteil solcher Standards besteht in der breiten Werkzeugunterstützung. So lassen sich Maven-Spezifikationen bspw. automatisiert mittels eines Maven-Plugins in eine CycloneDX-Spezifikation übersetzen, wobei neben den unmittelbaren Abhängigkeiten auch die transitiven Abhängigkeiten aufgelöst werden. Dabei macht sich das Werkzeug zunutze, dass Maven-Spezifikationen auf Bibliotheken verweisen, die wiederum eigene Maven-Spezifikationen besitzen und damit auch wieder ihre Abhängigkeiten angeben.

Je nach **Anforderungen der weiteren Stakeholder**, z. B. für die Prüfung der Lizenzen der verwendeten Komponenten, muss die Stückliste ggf. noch um weitere Daten angereichert werden. Bei dieser Anreicherung stehen nicht die Anforderungen des CRA im Vordergrund, sondern die Nutzung der ohnehin vorgeschriebenen Stückliste zur Vereinfachung der Prozesse im Unternehmen. Im Beispiel von Java-basierter Software mit Maven als Buildsystem können die Lizenzen bereits Teil der Maven-Spezifikation sein. Dadurch entfällt der zusätzliche Schritt für die Anreicherung mit weiteren Daten in diesem Kontext zumindest für solche Bibliotheken, die die optionale Lizenzangabe in ihrer Maven-Spezifikation enthalten.

Empfehlung 3: Nutzung der Stückliste für Schwachstellenscans

Die erzeugte Stückliste sollte als **Teil des automatisierten Erstellungsprozesses** direkt für einen **Abgleich mit bekannten Schwachstellen** genutzt werden können. Ist bekannt, welche Komponenten verwendet werden und in welchen Komponenten Sicherheitslücken öffentlich bekannt sind

(CVE-Liste), lassen sich diese beiden Listen abgleichen, um potenzielle „geerbte" Sicherheitslücken im eigenen Produkt zu identifizieren.

Diese Sicherheitsprüfung kann wie ein funktionaler Test gehandhabt werden. Eine identifizierte verwundbare Abhängigkeit entspricht dabei einem fehlgeschlagenen Testfall. Diese Analogie ist bei der Aufnahme neuer Komponenten trivial. Es ist bereits jetzt üblich, dass bei jeder vorgeschlagenen Codeänderung (GIT Merge Request) die Software automatisiert gebaut und getestet wird. Die Codeänderung kann nur übernommen werden, wenn diese Schritte erfolgreich durchlaufen werden. Integriert man den Abgleich der – durch die neu aufgenommene Komponente erweiterten – Stückliste, kann die Änderung nur übernommen werden, wenn für diese neue Komponente keine bekannten Schwachstellen existieren.

Im Gegensatz zu funktionalen Fehlern kann sich der Sicherheitszustand eines Produkts allerdings auch ohne eigene Codeänderungen über die Zeit verändern, z. B. wenn Sicherheitslücken in den verwendeten Komponenten gefunden werden. Daher sollte, auch wenn keine erneute Erstellung der Software ausgelöst wurde, regelmäßig ein Abgleich der neuesten Stückliste mit einer aktuellen Schwachstellenliste erfolgen, z. B. als zeitgesteuerter Auftrag einmal täglich. Werden bei einer solchen Prüfung Schwachstellen erkannt, sollten diese analog zu einer Meldung im Rahmen des CVD-Prozesses (siehe Kapitel 5) betrachtet werden.

Empfehlung 4: Erfassung aller verwendeten Komponenten in der SBOM – pro Risikobewertung und pro Unterstützung der Schwachstellenprozesse

Die SBOM sollte alle verwendeten Komponenten enthalten. Auch wenn der CRA bspw. nur vorschreibt, direkte Abhängigkeiten zu erfassen, empfiehlt sich auch die **Berücksichtigung transitiver Abhängigkeiten**. So wird eine verwundbare Komponente evtl. vom eigenen Produkt direkt gar nicht eingesetzt, sondern von einer anderen verwendeten Komponente. Dennoch kann die Sicherheitslücke im Kontext des Produkts ausnutzbar sein, unabhängig von der Anzahl der Indirektionen der Abhängigkeit.

Verwendete Komponenten werden nicht immer durch statische Verlinkung mit der eigenen Software verbunden. Bei

Exkurs

Eine Herausforderung ergibt sich bei der **Zuordnung der CVE-Einträge zur Stückliste**. Oftmals referenziert die CVE (oder NVD) ein Produkt, nicht aber die präzise betroffene Komponente. So besteht log4j bspw. aus einer Vielzahl einzelner Bibliotheken, von denen nicht alle in jede Software eingebunden werden. Selbst wenn man hier eine Überabschätzung trifft und alle Teile der betroffenen Bibliothek (log4j im Beispiel) als potenziell verwundbar annimmt, bleibt das Problem, dass Komponenten auf der technischen Ebene (z. B. in Maven) einer anderen Nomenklatur folgen als die CVE-Datenbank. Letztere verwendet CPE (Common Platform Enumeration), die jedoch im Open-Source-Ökosystem für Bibliotheken kaum Beachtung findet. Eine direkte automatisierte Zuordnung ist nicht präzise möglich.

Es gibt jedoch Werkzeuge, die mittels Textanalyse und Heuristiken versuchen, diese Beziehung herzustellen. Verschiedene Anbieter pflegen darüber hinaus solche Zuordnungen per Hand und stellen entsprechende Datenbanken bereit, oftmals zusammen mit Werkzeugen, die z. B. Maven-Spezifikationen gegen die Datenbank prüfen. Zudem wird derzeit versucht, OSV (Open Source Vulnerability Standard) als neuen Standard zu etablieren. Die OSV-Datenbank speist sich als Aggregator aus bestehenden Datenbanken im OSV-Format, z. B. Github Advisories. Mit diesen Angeboten lässt sich der Abgleich in der Praxis bereits jetzt durchführen.

dynamischer Verlinkung werden z. B. DLL-Dateien für Windows oder SO-Dateien für Linux mit der eigenen Software ausgeliefert und zur Laufzeit geladen. Dennoch handelt es sich um verwendete Komponenten, die Teil der Software-Stückliste werden sollten. Auch bei Komponenten, die vom eigenen Installationsprogramm zwingend zusammen mit der eigenen Software installiert werden, z. B. Laufzeitbibliotheken, kann davon ausgegangen werden, dass sie in den Verantwortungsbereich des Softwareherstellers fallen. Da beim Bekanntwerden von Sicherheitslücken hier Maßnahmen (z. B. Updates) erforderlich sind, wird die Empfehlung gegeben, sie als integrale Bestandteile für die einschlägigen Prozessen von vornherein ebenfalls zu erfassen.

Neben den – direkt oder transitiv – mit der Software ausgelieferten Abhängigkeiten bestehen auch Abhängigkeiten zur Ausführungsumgebung. Verwendet eine Software bspw. eine kryptografische Bibliothek, die Teil des Betriebssystems ist, handelt es sich dabei nicht um einen Bestandteil der eigenen Anwendung und diese muss entsprechend CRA nicht in die SBOM aufgenommen werden. Die Aktualisierung der Bibliothek erfolgt in diesem Fall direkt über das Betriebssystem. Dennoch ist die **Kenntnis der Abhängigkeit** relevant, da der Softwarehersteller weiterhin beim Bekanntwerden von Sicherheitslücken in der Bibliothek in der Lage sein muss, eine Risikoabschätzung zu treffen. So hängt der zu befürchtende Schaden von den zu verschlüsselnden Daten ab und kann nicht abschließend alleinstehend für die Bibliothek bewertet werden. Diese Empfehlung greift die **Risikosichtweise von Bewertungssystemen** wie z. B. dem Common Vulnerability Scoring System (CVSS) auf: Ausgehend von einem "Base Score" sollte – abhängig von der Einsatzumgebung – der dann aussagekräftigere "Environment Score" zur Anwendung kommen.

04 TECHNIK: Sicherheits- und Schwachstellentests

Worum geht es?

Auch bei sorgfältiger Konzeption und Implementierung von Produkten können Schwachstellen nicht ausgeschlossen werden. Im Rahmen **der Konformitätsbewertung** kommt dem **Test des finalen Produkts auf Sicherheitslücken** eine essenzielle Bedeutung zu. So wird praktisch überprüft, ob es einem Tester, der ähnlich zu einem Angreifer vorgeht, möglich ist, die Sicherheit des Produkts zu kompromittieren. Der Test umfasst dabei das gesamte Produkt aus Sicht eines Nutzers bzw. Angreifers, unabhängig davon, welcher Teil der Funktionalität von eigenen Komponenten oder von Drittanbieterkomponenten bereitgestellt wird.

Die Verpflichtung für Tests endet nicht damit, dass das Produkt an den Markt gebracht wird. Stattdessen müssen die Tests regelmäßig wiederholt werden, um der Entwicklung neuer Angriffstechniken und -Werkzeuge Rechnung zu tragen. Das schließt auch die mögliche Ausnutzung zwischenzeitlich bekanntgewordener Sicherheitslücken in Drittanbieterkomponenten ein.

Was sagt der CRA?

Hersteller müssen gemäß Anhang I Teil II (3) CRA die Sicherheit eines „Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen“. Diese Anforderung gilt gemäß Art. 13 Abs. 8 CRA während der erwarteten Produktlebensdauer und dem Unterstützungszeitraum des jeweiligen Produkts.

Was ist unsere Empfehlung?

Empfehlung 1: Integration von Tests in den Entwicklungsprozess

Tests sollten nicht erst nach Abschluss aller Implementierungstätigkeiten, sondern soweit möglich bereits während der Implementierung durchgeführt werden. Welche Tests möglich sind, hängt vom Implementierungsfortschritt und den Kosten / dem Zeitaufwand sowie dem Automatisierungsgrad der Tests ab. Wir empfehlen folgendes Schema:

- **Einfache Prüfungen**, z. B. zu Programmierrichtlinien innerhalb der Entwicklungsumgebung direkt beim Schreiben des Quellcodes
- **Automatisches Codescanning** bei jeder Änderung am Code, z. B. bei jedem Merge Request im Versionskontrollsystem
- Bei großen Systemen mit einer Vielzahl an Diensten: **Penetrationstest** nach **Fertigstellung** eigenständig nutzbarer Dienste
- **Penetrationstest** auf dem Gesamtsystem nach der **Integration**

Dieses Schema zur Integration von Tests in den Entwicklungsprozess **ersetzt keine** regelmäßig wiederkehrenden Penetrationstests. Ein abgewandeltes Schema kann auch bei größeren Änderungen an der Software angewendet werden. Bei kleineren Änderungen wie Patches ist der Penetrationstest entbehrlich, da gerade bei sicherheitsrelevanten Patches die Auslieferung des Patches nicht verzögert werden sollte. Rein automatisierte Prozesse wie z. B. statische Codeanalyse sollten auch bei kleinen Änderungen durchgeführt werden.

Empfehlung 2: Integration automatisierter Tests

Um den manuellen Aufwand für die wiederkehrenden Sicherheitstests zu reduzieren, sollten automatisierte Testverfahren eingesetzt werden. Hierdurch können Fehler frühzeitig erkannt werden, wodurch kostenintensive manuelle Penetrationstests weniger verbleibende Fehler finden und somit seltener wiederholt werden müssen, bis ein angemessenes Sicherheitsniveau nachgewiesen werden kann.

Je nach verwendeter Programmiersprache und Umgebung sind verschiedene Testverfahren sinnvoll. Ist der Kompilierprozess eher einfach (z. B. homogener Maven-Build) mit einer begrenzten Auswahl an Programmiersprachen (z. B. gesamter Code in Java) können Quellcodescanner, die in den Buildprozess integriert werden, eine angemessene Wahl sein. Soll eine Integration in den Buildprozess aufgrund der damit verbundenen Komplexität vermieden werden, kann ein Binärscanner verwendet werden, welcher die finale ausführbare Datei inspiziert. Binärscanner bieten zudem den Vorteil, dass sie auch Drittanbieterkomponenten, die im Binärcode (z. B. als JAR-Datei) eingebunden werden, zusammen mit der Anwendung analysieren.

Insbesondere bei Anwendungen, die in nativen Programmiersprachen mit einem nicht verwalteten Speichermodell wie bspw. C/C++ entwickelt werden, kann **Fuzzing als automatisches Testverfahren** sinnvoll sein. Fuzzing zeigt gute Ergebnisse bei der Erkennung von Speicherfehlern in der Verarbeitung binärer Eingabedaten in Native Code. Dieses Vorgehen ist nicht auf Dateien beschränkt. Fuzzing kann auch auf Netzwerkpakete oder von Hardware-Schnittstellen erhaltene Daten angewendet werden. Fuzzing-Techniken für höhere Abstraktionsebenen wie bspw. die REST-Schnittstellen in Webanwendungen sind Gegenstand aktueller Forschung und dürften in absehbarer Zeit Einzug in die industrielle Verwendung finden. Generell zu beachten ist, dass Fuzzing-Startdaten, sogenannte Seeds, notwendig sind, von denen ausgehend die Testeingaben an die Zielanwendung erzeugt werden. Stehen Testfälle zur Verfügung, können Fuzzing-Seeds daraus abgeleitet werden.

Bei Produkten, die aus kompletten IT-Systemen bestehen, z. B. Industriemaschinen mit verschiedenen PCs, PLCs, Switches, usw. im Produkt, kann ein **breiterer Ansatz der Automatisierung** sinnvoll sein. Hier empfehlen sich Werkzeuge des automatisierten Scanning und Exploiting. Hierbei ist zu beachten, dass diese Werkzeuge i. d. R. nur Konfigurationsfehler finden (z. B. in den Einstellungen des Betriebssystems oder von Systemdiensten), aber keine bisher unbekannten Sicherheitslücken in der verwendeten eigenen oder fremden Software.

Empfehlung 3: Wechsel der externen Tester

Um eine möglichst umfassende und unabhängige Überprüfung der IT-Sicherheit zu gewährleisten, ist es ratsam, für die Penetrationstests **regelmäßig die externen Tester zu wechseln**. Dies hat mehrere Vorteile:

Ein neuer Tester kann:
- mit einem frischen Blick auf das System möglicherweise Schwachstellen entdecken, die dem vorherigen Tester entgangen sind.
- andere Methoden, Werkzeuge oder Erfahrungen einbringen, die die Qualität und Abdeckung der Tests erhöhen.
- eine höhere Objektivität und Unvoreingenommenheit garantieren, da er nicht von Vorannahmen beeinflusst ist, die er aus Interaktionen mit dem Entwicklungsteam oder aus der Analyse vorheriger Programmversionen kennt.
- die interne Sicherheitskultur stärken, indem er neue Erkenntnisse, Best Practices oder Empfehlungen vermittelt.

Um einen optimalen Nutzen aus dem Wechsel der externen Tester zu ziehen, sollte dieser jedoch nicht zu häufig oder zu selten erfolgen. **Zu häufige Wechsel** können zu einer mangelnden Kontinuität, einem Verlust von Know-how oder einer geringeren Vertrauensbildung führen. **Zu seltene Wechsel** können zu einer Routine, einer Abhängigkeit oder einer Blindheit für bestimmte Risiken führen. Eine mögliche Faustregel ist, alle zwei bis drei Jahre den externen Tester zu wechseln, je nach Art, Umfang und Komplexität des Systems. Zudem sollte der Wechsel transparent und nachvollziehbar gestaltet werden, um mögliche Interessenkonflikte oder Qualitätsmängel zu vermeiden.

05 PROZESSE: Implementierung einer koordinierten Schwachstellenstrategie (CVD)

Worum geht es?

Ein **CVD-Prozess (Coordinated Vulnerability Disclosure)** ist ein standardisierter Ablauf, um die **Meldung von Sicherheitslücken** in digitalen Produkten zu ermöglichen. Hierbei handelt es sich um eine Anforderung, die zunächst auf Prozessebene umzusetzen ist. Der Prozess basiert auf der Zusammenarbeit zwischen den Herstellern der Produkte und den Personen oder Organisationen, die die Schwachstellen entdecken und melden, die regelmäßig externe Personen sind. Die gemeldeten Schwachstellen sind wertvolle Informationen, um die Sicherheit von Produkten zu verbessern.

Neben der **Annahme von Meldungen** muss der Prozess dafür Sorge tragen, dass die **Meldungen geprüft, in ihrem Schweregrad bewertet und den verantwortlichen Entwicklungsteams bereitgestellt** werden. Die Ursache der Sicherheitslücke kann auch in einer verwendeten Komponente eines Drittanbieters oder einer Open-Source-Komponente liegen. In diesem Fall liegt die Einbindung des Dritten ebenfalls in der Verantwortung des Herstellers. Der Hersteller ist dafür verantwortlich, die Meldungen zu verarbeiten. Es ist nicht die Aufgabe des Meldenden, die Ursache des Fehlers zu identifizieren oder den Bericht an den passenden Zulieferer zu senden.

Ist die Schwachstelle bekannt, muss sie behoben werden. Anschließend muss Kunden das Update bereitgestellt werden. In diesem Bereich unterscheiden sich die notwendigen Aktivitäten nicht von der Nachbereitung eines z. B. vom Hersteller selbst beauftragten Penetrationstests.

Was sagt der CRA?

Der CRA legt fest, dass beliebige Dritte solche Meldungen vornehmen können, auch ohne vom Hersteller mit einer Untersuchung beauftragt zu sein. Unter dem CRA müssen Hersteller von Produkten mit digitalen Elementen nach Anhang 1 Teil II (5) CRA künftig „eine **Strategie für die koordinierte Offenlegung von Schwachstellen** aufstellen und umsetzen". Eine zentrale Kontaktstelle, über die Schwachstellen gemeldet werden können sowie über die das Konzept für die koordinierte Offenlegung zu finden ist, ist als Bestandteil den Informationen und Anleitungen für Nutzer nach Anhang II Nummer 2 CRA beizufügen.

Entsprechende von internen oder externen Quellen gemeldete potenzielle Schwachstellen sind von Herstellern gemäß Art. 13 Abs. 8 CRA zu bearbeiten und zu beheben.

Eine Meldung kann entweder direkt an den jeweiligen Hersteller erfolgen oder indirekt und bei Bedarf anonym über einen sog. Koordinator (Erwgr. 77 CRA). Die EU-Mitgliedstaaten sind durch Art. 12 Abs. 1 NIS-2-Richtlinie dazu verpflichtet ein nationales Computer Security Incident Response Team (CSIRT) als Koordinator für koordinierte Offenlegungen von Schwachstellen zu benennen. Für Deutschland ist geplant, dass diese Rolle das Bundesamt für Sicherheit in der Informationstechnik (BSI) wahrnimmt.[9] Die Koordinatoren können bei Bedarf als vertrauenswürdiger Vermittler zwischen der meldenden Person und den Herstellern eingeschaltet werden und dabei unterstützen, betreffende Einrichtungen zu ermitteln und zu kontaktieren. Sie können auch helfen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen (Art. 12 Abs. 1 lit. a-c NIS-2-Richtlinie).

In Erwgr. 77 CRA wird ausgeführt, dass das Konzept für die koordinierte Offenlegung von Schwachstellen einen **strukturierten Meldeprozess** vorsehen sollte, der die Diagnose und Behebung von Schwachstellen erlaubt, bevor detaillierte Informationen zur Schwachstelle an die Öffentlichkeit gegeben werden. Weiterhin sollen Hersteller erwägen, diese Konzepte in einem maschinenlesbaren Format zu veröffentlichen sowie angesichts der hohen Schwarzmarktpreise für

9 siehe § 5 Abs.1 des Referentenentwurfs des Bundesministeriums des Innern und für Heimat vom 03.07.2023 für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz.

Schwachstellen, Anreize für das Melden beim Hersteller durch Anerkennungen oder Belohnungen (bspw. **„Bug-Bounty-Programme“**) zu schaffen.

Was ist unsere Empfehlung?

Empfehlung 1: Auswahl geeigneter Meldewege

Der CRA lässt die Ausgestaltung der Meldewege für Schwachstellen offen, solange sie die **Mindestanforderungen wie bspw. die Vertraulichkeit der gemeldeten Schwachstellen** sicherstellen. Je nach Anzahl der verwendeten Komponenten, bieten sich unterschiedliche Ansätze an:

- **Mailadresse mit PGP-Key auf der Webseite (https):** Gibt es nur wenige Produkte und sind nur wenige Meldungen zu erwarten, sticht dieser Ansatz durch die geringen Kosten zur Einrichtung des Meldeverfahrens hervor. Es sollte eine Funktionsadresse (z. B. security@firma.de) verwendet werden, die an mehrere Personen verteilt, um auch bei Abwesenheiten (Krankheit, Urlaub, usw.) eine zeitnahe Bearbeitung der Meldungen sicherzustellen. Um die Kommunikation mit dem Einreicher und die interne Koordination zu vereinfachen, kann ein Ticketsystem genutzt werden. Der Nachteil dieses Ansatzes besteht darin, dass neue Meldende ggf. nicht unmittelbar alle benötigten Informationen bereitstellen, da Mails im Gegensatz zu einem Onlineformular unstrukturiert sind.
- **Onlineformular:** Auf einer Webseite (https) können mittels Onlineformular alle benötigten Informationen zur Schwachstelle abgefragt werden. Dies vermeidet, dass Meldende Informationen vergessen, die ihnen eigentlich vorliegen. Gleichzeitig darf ein Formular nicht durch Pflichtfelder dazu verwendet werden, Meldende zur Analyse der Schwachstelle zu verpflichten. Anders ausgedrückt muss die Schwachstellenmeldung auch angenommen werden, wenn nicht alle Detailinformationen (z. B. die für die Schwachstelle ursächliche interne Komponente) vorliegen.
- **Anbieter:** Der Prozess zur Schwachstellenmeldung kann an einen externen Anbieter ausgelagert werden. Solche Anbieter existieren bereits und führen bspw. Bug-Bounty-Programme für Firmen durch. In diesen Programmen werden externe Sicherheitsforscher über die Ausschreibung von Gratifikationen dazu motiviert,

nach Schwachstellen in Produkten der teilnehmenden Firmen zu suchen und an die Firmen über das Portal des Anbieters melden. Der Leistungsumfang dieser Anbieter variiert je nach Anbieter und gebuchtem Modell. So kann der Anbieter bspw. die Vorkontrolle der Meldungen übernehmen oder das Programm bewerben, um Sicherheitsforscher zur Meldung von Lücken zu gewinnen. Auch eine reine Meldeinfrastruktur ohne Bug-Bounty-Programm ist denkbar. Der CRA erfordert nicht zwingend die Bereitstellung von Prämien. In jedem Fall verbleibt die Verantwortung für die technische Prüfung und Behebung der gemeldeten Lücken beim Hersteller.

Empfehlung 2: Teilnahme an Bug-Bounty-Programmen

Auch wenn es für die Erfüllung der Pflichten aus dem CRA nicht zwingend erforderlich ist, empfehlen wir, den CRA als Motivation zu verstehen, Sicherheit proaktiv zu behandeln und dies gegenüber Kunden und Öffentlichkeit zu kommunizieren. Mit der Teilnahme an einem Bug-Bounty-Programm kann ein Hersteller hervorheben, **aktiv Informationen zu Schwachstellen einzuwerben**, um seine Produkte zu verbessern. Hierdurch kann aus einer reaktiven Bearbeitung von Schwachstellenmeldungen, wie sie verpflichtend ist, eine **proaktive Suche** nach Verbesserungspotenzial werden, was den hohen Stellenwert der Cybersicherheit beim Hersteller – auch gegenüber seinen Kunden – belegt.

Die ausgeschriebenen Prämien sollten sich dabei an der Kritikalität der gemeldeten Schwachstellen orientieren. Prämien müssen nicht rein monetär sein, sondern können z. B. auch die öffentliche Anerkennung der Meldenden (z. B. in Form einer „Hall of Fame“) einschließen. Solche Ansätze motivieren erfolgreiche Meldende, auch in Zukunft nach Schwachstellen in den Produkten dieses Herstellers zu suchen und diese zu melden.

Empfehlung 3: Schwachstellenmeldungen als Vorteil betrachten

Durch eine aktive Kommunikation kann auch der Blick von Kunden auf Schwachstellen verändert werden. Statt Schwachstellen als Qualitätsmängel zu sehen, kann der aktive Umgang mit Lücken als Bestreben zur ständigen Verbesserung des Produkts dargestellt werden. Große Softwarehersteller bestreiten diesen Weg bereits. Wichtig hierfür ist, die Kommunikation auszugestalten und selbstständig Informationen bereitzustellen, statt auf Anfragen von Kunden und Presse zu warten.

06 KENNZEICHNUNG: CE-Kennzeichnung

Worum geht es?

Grundsätzlich wird beim CRA mit den **Vorgaben zur Konformitätsbewertung und CE-Kennzeichnung** auf bestehende Mechanismen zurückgegriffen. Diese Mechanismen sind Teil des „New Legislative Frameworks" (NLF) und werden von vielen anderen EU-Rechtsvorschriften genutzt, die Anforderungen an die Sicherheit sowie den Gesundheits- oder Umweltschutz von bestimmten Produkten stellen.

Was sagt der CRA?

Bevor Hersteller ein Produkt mit digitalen Elementen in Verkehr bringen, müssen sie nach Art. 13 Abs. 12, Art. 30 CRA eine CE-Kennzeichnung am Produkt anbringen. Die Anbringung des CE-Kennzeichens ist ein abschließender Schritt und **sichtbarer Ausdruck des Ergebnisses eines Prozesses**, welcher die **Konformität eines Produktes mit den Anforderungen des CRA** nachweist.

Hat ein Hersteller für ein Produkt mit digitalen Elementen alle Anforderungen nach Anhang I CRA umgesetzt und eine technische Dokumentation nach Art. 31 CRA erstellt, führt er eine Konformitätsbewertung nach einem von ihm gewählten Verfahren durch, um festzustellen, ob eben diese Anforderungen erfüllt sind (Art. 32 Abs. 1 CRA). Für den Nachweis der Konformität gibt es verschiedene formalisierte Verfahren, die in Art. 32 Abs. 1 lit. a-d und Anhang VIII CRA gelistet sind, und entweder durch den Hersteller selbst oder durch eine externe sog. notifizierte Stelle durchgeführt werden. Welche Verfahren für ein jeweiliges Produkt zur Verfügung stehen, richtet sich danach, ob dieses als wichtiges oder kritisches Produkt mit digitalen Elementen nach Art. 7 und 8, Anhang III und IV CRA einzuordnen ist, und ergibt sich aus Art. 32 Abs. 2-4 CRA.

Wird mit einem entsprechenden Konformitätsbewertungsverfahren nachgewiesen, dass ein Produkt die Anforderungen des CRA erfüllt, stellen Hersteller eine EU-Konformitätserklärung aus und bringen die CE-Kennzeichnung an. Die **EU-Konformitätserklärung** hat in ihrem Aufbau dem Muster in Anhang V sowie den Vorgaben aus Art. 28 CRA zu entsprechen. Mit der Ausstellung übernimmt der Hersteller nach Art. 28 Abs. 4 CRA die Verantwortung für die Konformität des Produktes.

Die CE-Kennzeichnung ist nach Art. 30 Abs. 1 CRA gut sichtbar, leserlich und dauerhaft auf dem Produkt mit digitalen Elementen anzubringen. Falls dies am jeweiligen Produkt nicht möglich ist, wird die CE-Kennzeichnung auf der Verpackung und der beigefügten EU-Konformitätserklärung angebracht. Bei Software wird das CE-Kennzeichen entweder auf der EU-Konformitätserklärung oder auf einer produktbegleitenden Webseite angebracht, wobei diese für Verbraucher leicht und direkt zugänglich zu sein hat.

Nach Art. 29 CRA gelten für die CE-Kennzeichnung die allgemeinen Grundsätze nach Art. 30 der Verordnung (EG) Nr. 765/2008. Hier werden u.a. missbräuchliche Formen der CE-Kennzeichen Verwendung aufgeführt sowie in Anhang II eine technische Zeichnung des Schriftbildes des CE-Kennzeichens geliefert.

Für ein Produkt mit digitalen Elementen können neben dem CRA auch **weitere Harmonisierungsvorschriften der Union** einschlägig sein und ein entsprechendes Konformitätsbewertungsverfahren erfordern. In diesen Fällen sollte eine EU-Konformitätserklärung über die Übereinstimmung mit allen einschlägigen Vorschriften abgegeben werden (Anhang V Nr. 5 CRA). Die Anbringung der CE-Kennzeichnung ist in diesen Fällen nach Art. 30 Abs. 5 CRA Ausdruck dessen, dass ein Produkt alle einschlägigen Harmonisierungsvorschriften erfüllt.

Wurde die CE-Kennzeichnung unter Nichteinhaltung der Vorgaben des Art. 28 und 30 CRA oder gar nicht angebracht, kann eine **Marktüberwachungsbehörde** nach Art. 58 Abs. 1 lit. a und b CRA den betroffenen Hersteller auffordern, diese Nichtkonformität zu beheben. Geschieht dies nicht, kann die Bereitstellung des Produktes gemäß Art. 58 Abs. 2 CRA durch den betreffenden Mitgliedstaat eingeschränkt oder untersagt werden oder das Produkt zurückgerufen oder vom Markt genommen werden. Verstöße in diesem Bereich können nach Art. 64 Abs. 3 CRA mit Geldbußen von bis zu

10.000.000 Euro oder von bis zu 2 Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist, belegt werden.

Was ist unsere Empfehlung?

Hersteller sollten sich bereits frühzeitig mit den Anforderungen des CRA auseinandersetzen. Das CE-Kennzeichen darf nur angebracht werden, wenn die entsprechenden Voraussetzungen erfüllt sind. Hersteller sollten also ermitteln, ob ihr Produkt wichtig oder kritisch im Sinne des CRA ist, welches Konformitätsbewertungsverfahren zum Einsatz kommen soll, ggf. auf welche Standards aufgebaut werden soll und welche externen notifizierten Stellen zur Konformitätsbewertung zum Einsatz kommen sollen. Hierbei ist zu bedenken, dass auch Bestandsprodukte betroffen sind, wenn für neue Produkte oder Versionen auf diesen aufgebaut wird.

Ganz praktisch ist die Frage zu klären, wo das CE-Kennzeichen angebracht werden soll, wenn es sich z. B. um eine ausschließlich zum Download angebotene Software handelt.

07 PROZESSE: Meldepflichten der Hersteller

Worum geht es?

Der CRA führt **Meldepflichten für Hersteller** ein, wenn Schwachstellen oder Sicherheitsvorfälle bekannt werden. Von einem Vorfall spricht man bspw. bei einem erfolgreichen Angriff auf die für den Betrieb eines Produkts erforderlichen Cloud-Dienste.

Die Meldungen werden in einer neu zu schaffenden einheitlichen Meldeplattform für jedes Mitgliedsland sowie für die EU gesammelt. Hierdurch ergibt sich sowohl auf Ebene des jeweiligen Mitgliedstaats als auch auf Ebene der EU ein Lagebild, welche Schwachstellen bzw. Vorfälle gerade „aktiv" sind und wie deren Status ist. Sind z. B. zahlreiche Firmen in ganz Europa von einer Schwachstelle betroffen, welchen Angreifern die Ausführung beliebigen Codes ermöglicht, ergibt sich ein anders Lagebild, als wenn nur einzelne Firmen betroffen sind oder ein Angreifer nur die Leistungsfähigkeit der Systeme geringfügig beeinträchtigen kann. Mit den Meldungen nach dem CRA können Behörden genauer planen und agieren. In der Vergangenheit lagen solche Informationen nur bei CERTs bzw. CERT-Verbünden großer Firmen vor, die ihre jeweils eingesetzten Produkte überwachen. Der CRA verschiebt die **Verantwortung zur Bereitstellung dieser Daten zum Hersteller** und ermöglicht den behördlichen Zugang zu diesen Daten.

Die Meldepflichten sind die Richtschnur, welche Informationen ein Hersteller binnen welcher Frist ermittelt haben sollte, um angemessen mit einer Sicherheitslücke oder einem Vorfall umzugehen. Hierdurch wird ein **Zeitplan** definiert, der eine angemessene Behebung sicherstellen soll. Wichtig ist, dass sich notwendige Aktionen nicht auf das Bereitstellen eines Patches beschränken. So müssen Hersteller, insbesondere

wenn ein Patch nicht unmittelbar bereitsteht, Möglichkeiten zur anderweitigen Reduzierung des Risikos bereitstellen, z. B., indem Nutzern empfohlen wird, bestimmte Funktionen (temporär) zu deaktivieren.

Was sagt der CRA?

Der CRA sieht in Art. 14 im Falle von **aktiv ausgenutzten** Schwachstellen sowie **schwerwiegenden Vorfällen**, die sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirken, **Meldepflichten** für Hersteller vor.

Aktiv ausgenutzte Schwachstellen sind gemäß Art. 3 Nr. 42 CRA solche Schwachstellen, zu denen „verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat". Hierbei handelt es sich um Fälle, in denen ein Hersteller feststellt, dass ein böswilliger Akteur einen Fehler in einem vom Hersteller bereitgestellten Produkt ausnutzt und diese Sicherheitsverletzung Auswirkungen auf Nutzer oder andere Personen hat (Erwgr. 69 CRA).

Sicherheitsvorfälle meinen grundsätzlich nach Art. 6 Nr. 6 NIS-2-Richlinie „ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt". Ein **Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts** mit digitalen Elementen umfasst nach Art. 3 Nr. 44 CRA solche Vorfälle, die sich negativ auf die Fähigkeit eines Produktes mit digitalen Elementen auswirken oder auswirken können, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen. Als **schwerwiegend** ist ein solcher Vorfall gemäß Art. 14 Abs. 5 CRA anzusehen, wenn sich diese negativen Auswirkungen auf die Fähigkeiten zum Schutz sensibler oder wichtiger Daten oder Funktionen beziehen, oder wenn der Vorfall zur Einführung oder Ausführung eines böswilligen Codes im jeweiligen Produkt mit digitalen Elementen selbst oder im Netzwerk und Informationssystem eines Nutzers dieses Produkts geführt hat oder führen kann.

Liegen diese Voraussetzungen bei einer Schwachstelle oder einem Sicherheitsvorfall vor, ist dies durch den Hersteller nach Art. 14 Abs. 1 und 3 CRA gleichzeitig an das als

Koordinator benannte CSIRT und die Agentur der Europäischen Union für Cybersicherheit (ENISA) zu melden. Bei dem als Koordinator benannten CSIRT handelt es sich nach Art. 3 Nr. 51 CRA um jeden Koordinator, der nach Art. 12 Abs. 1 NIS-2-Richtlinie in jedem Mitgliedstaat der EU zu benennen ist, also für Deutschland planmäßig dem BSI. Grundsätzlich hat der Hersteller an das CSIRT zu melden, was in dem Mitgliedstaat benannt wurde, in dem der Hersteller seine Hauptniederlassung hat.[10] Die Meldung an das als Koordinator benannte CSIRT und die ENISA durch den Hersteller soll zentral über eine **einheitliche Meldeplattform** erfolgen, die von der ENISA einzurichten ist und welche nationale Endpunkte für die elektronische Meldung an die zuständigen CSIRTs enthalten soll (Art. 16 Abs. 1 CRA).

Die Meldung von aktiv ausgenutzten Schwachstellen (Art. 14 Abs. 2 CRA) und schwerwiegenden Sicherheitsausfällen mit Auswirkungen auf die Sicherheit von Produkten (Art. 14 Abs. 4 CRA) erfolgt nach Kenntniserlangung durch den Hersteller in einem **dreistufigen Verfahren**, welches hier zusammenfassend dargestellt wird:

- Unverzüglich, innerhalb von **24 Stunden** nach Kenntniserlangung durch den Hersteller (Art. 14 Abs. 2 lit. a, Abs. 4 lit. a CRA): **Frühwarnung** über Sicherheitsvorfall oder Schwachstelle unter Angabe betroffener Mitgliedstaaten. Im Falle von ausgenutzten Schwachstellen ggf. die Angabe eines Verdachtes, ob der Vorfall auf böswillige oder rechtswidrige Handlungen zurückzuführen ist.
- Unverzüglich, innerhalb von **72 Stunden**, sofern Informationen nicht bereits zuvor übermittelt wurden (Art. 14 Abs. 2 lit. b, Abs. 4 lit. b CRA): Allgemeine Informationen, bspw. zu Art des Vorfalls/der Schwachstelle, Korrektur- oder Risikominderungsmaßnahmen, die ergriffen wurden oder durch Nutzer ergriffen werden können, sowie wie sensibel der Hersteller den Inhalt der Meldung einschätzt.
- **Abschlussbericht**, sofern Informationen nicht bereits übermittelt wurden (Art. 14 Abs. 2 lit. c, Abs. 4 lit. c CRA), bei **Sicherheitsvorfällen** innerhalb **eines Monats** nach Meldung innerhalb der 72-Stunden-Frist, bei **Schwachstellen** innerhalb von **14 Tagen** nachdem eine Korrektur- oder Risikominderungsmaßnahme zur Verfügung steht. Enthält u. a. Beschreibung des Vorfalls/der

10 Art. 14 Abs. 7 CRA enthält Vorgaben zur Bestimmung des zuständigen CSIRTs, insbesondere im Falle von Herstellern, die keine Hauptniederlassung innerhalb der EU haben.

Schwachstelle, Schweregrad, Auswirkungen, Abgaben zu Art der Bedrohung, Ursache, ggf. ausnutzendem Akteur, Angaben zu Abhilfe- und Korrekturmaßnahmen

Was ist unsere Empfehlung?

Empfehlung 1: Monitoring für Vorfälle definieren

Bietet ein Hersteller z. B. Produkte mit Cloud-Diensten an, d.h. wenn Teile der Datenverarbeitung des Produkts entfernt erfolgen, sollte der Hersteller ein **Monitoring für seine Cloud-Dienste** etablieren, um potenziell sicherheitsrelevante Anomalien frühzeitig zu erkennen. Anomalien können bspw. ein besonders hoher Ressourcenverbrauch (Rechenzeit, Arbeitsspeicher, Festplattenplatz) oder ungewöhnliche Zugriffsmuster sein. Eine Prüfung der Anomalie kann diese anschließend als Fehlalarm verwerfen oder als sicherheitskritisches Ereignis bestätigen. Auch die Einschätzung, ob es sich um einen schwerwiegenden Vorfall handelt, ergibt sich aus der Analyse der Anomalie.

Beispielsweise kann ein deutlich erhöhtes Übertragungsvolumen auf dem Netzwerk darauf hindeuten, dass in größerem Umfang Daten ausgeleitet werden. Eine erhöhte Nutzung der CPU bei gleichzeitig ungewöhnlich hoher Festplattenaktivität kann auf einen Ransomware-Angriff mit Verschlüsselung von Daten hindeuten.

Das Monitoring muss dabei proaktiv eingerichtet werden, um Daten im Normalbetrieb sammeln zu können. Nur so lassen sich Abweichungen vom Normalbetrieb erkennen.

Sind konkrete Sicherheitslücken bekannt, die sowohl das beim Kunden eingesetzte Produkt als auch dessen Cloud-Komponenten betreffen, empfiehlt es sich, das Monitoring mit Mustern zu versehen, die auf Versuche zur Ausnutzung der Lücke hindeuten. So können bspw. bestimmte Angriffsmuster im Netzwerkverkehr erkannt werden. Eine solche Maßnahme ist jedoch nur dann sinnvoll, wenn es noch weitere nicht gepatchte Systeme (z. B. beim Kunden) gibt, da andernfalls nach dem Patchen des Cloud-Systems nicht mehr vom Ausnutzen der Lücke gesprochen werden kann, sondern lediglich von Fehlversuchen der Angreifer.

Empfehlung 2: Betrieb von Honeypots

Hersteller können eigene Produkte als Endnutzer im Internet betreiben bzw. solche Geräte simulieren. Dabei sollte eine Überwachung der Produkte auf auffälliges Verhalten erfolgen. In jedem Fall sollten diese Honeypots für Außenstehende nicht von tatsächlichen Produkten beim Kunden zu unterscheiden sein. Angreifer, die nach verwundbaren Geräten suchen, werden dadurch mit hoher Wahrscheinlichkeit auch die präparierten Systeme des Herstellers angreifen. Hierdurch kann nicht nur beobachtet werden, welche bereits bekannten Lücken aktiv ausgenutzt werden, sondern es können ggf. auch Angriffe erkannt werden, die noch nicht bekannte Lücken ausnutzen. Diese Informationen über sogenannte **Zero-Day-Lücken** sollten beim Hersteller im normalen Schwachstellenmeldeprozess behandelt werden, analog zu den Ergebnissen beauftragter Penetrationstest oder externer Meldungen.

Empfehlung 3: Monitoring des Graumarkts

Als Hersteller von größeren oder kritischen Komponenten kann es sinnvoll sein, den Graumarkt (Handel mit Schwachstellen) zu beobachten oder entsprechende Informationsdienste zu nutzen. Ändern sich Preise oder entsteht dort signifikant Aktivität, sollte besonders geprüft werden, ob bei den Produkten, die der Hersteller beobachten kann, ungewöhnliche Aktivitäten auftreten. Wurde zuvor eine Schwachstelle bekannt, ist davon auszugehen, dass für diese ggf. Exploits verkauft werden, was für eine aktiv ausgenutzt Schwachstelle spricht. Diese Empfehlung ist aufgrund der benötigten Strukturen nicht für alle Produkte und Hersteller einschlägig.

Ausblick: Den CRA als Chance nutzen

Cybersicherheit ist gleichermaßen ein **Governance- wie IT-Thema**. Die IT-Abteilung allein wird der Komplexität der CRA-Umsetzung nicht gerecht werden können – Management Attention ist notwendig, ebenso wie eine abteilungs- und ebenenübergreifende **Sensibilisierung und Zusammenarbeit**.[11]

Die Anforderungen des CRA sind nur ein Puzzlestein in den bestehenden und derzeit in Arbeit befindlichen **gesetzlichen Rahmenbedingungen**, die bei der Entwicklung und Nutzung von IT-Systemen in Unternehmen beachtet werden müssen. Am bekanntesten ist vermutlich die **Datenschutz-Grundverordnung (DSGVO)**, in Kraft getreten 2018, welche über die technischen Maßnahmen hinaus regulatorische Auswirkungen auf die organisatorischen Regelungen einer Organisation hat. Mit der neugefassten **NIS-2-Richtlinie** werden entsprechende Verpflichtungen zu Cybersicherheit für Betreiber kritischer Infrastrukturen deutlich weiter gefasst als bisher, sodass wesentlich mehr Unternehmen sich diesen Anforderungen stellen müssen. Zudem gibt es **spezifische Regulierungen** anderer, teilweise bezüglich Cybersicherheit kritischer Bereiche und Branchen, die konkrete Vorgaben machen (z. B. auf EU-Ebene der Digital Operational Resilience Act (DORA), die Payment Services Directive 2 (PSD2), Electronic Identification, Authentication, and Trust Services (eIDAS) Regulation u. a.).

Grundsätzlich wird die Einhaltung von gesetzlichen Bestimmungen und unternehmensinternen Richtlinien durch Unternehmen als Compliance beschrieben.[12] Ein

11 Kreutzer, M., Scheel, K.: Smart Governance for Cybersecurity, in: ERCIM News, 2021, S. 6–7.
12 Deutscher Corporate Governance Kodex in der Fassung vom 24. Juni 2014 (4.1.3).

Compliance-Management-System beschreibt die Gesamtheit der Grundsätze, Maßnahmen und Prozesse einer Organisation zur Einhaltung von gesetzlichen Bestimmungen und organisationsinternen Richtlinien sowie zur Vermeidung von Regelverstößen.[13] Die Einrichtung eines Compliance-Management-Systems ist nicht explizit gesetzlich geregelt. In Deutschland ist die grundsätzliche Pflicht zur **Sorgfalt bei der Geschäftsführung** in §§ 93 Abs.1 AktG, 43 Abs. 1 GmbHG verankert. § 91 Abs. 2 AktG legt (mit Ausstrahlwirkung für andere Unternehmensformen) die **Pflicht des Vorstands** fest, geeignete Maßnahmen zu treffen und insbesondere Überwachungssysteme einzurichten, die den Fortbestand von unternehmensgefährdenden Entwicklungen früh erkennen.[14] Hierunter ist eine allgemeine Legalitätspflicht zu verstehen, dafür Sorge zu tragen, dass ein Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße erfolgen. Hieraus wird in der Rechtsprechung die Verpflichtung zur Schaffung eines funktionierenden Compliance-Systems abgeleitet.[15]

Neben den im CRA vorgesehenen umfassenden **Dokumentations- und Nachweispflichten** sind auf solche Weise sämtliche rechtlichen Verpflichtungen systematisch zu erfassen, denen eine Organisation unterliegt, beispielsweise aus dem Bereich Datenschutz.[16] Es ist daher sinnvoll, diese nicht getrennt voneinander zu betrachten, sondern übergreifend.

Neue Regulierungen stellen zudem immer eine Möglichkeit zur Weiterentwicklung dar, da sie Unternehmen dazu veranlassen (um nicht zu sagen zwingen) können, Geschäftspraktiken zu überdenken und anzupassen. Dies kann zu **mehr Effizienz, Transparenz und Nachhaltigkeit** beitragen, was langfristig zu Wettbewerbsvorteilen und einem besseren Ruf führen kann. Die DSGVO ist hierfür ein Beispiel, welche inzwischen weltweit quasi als „Goldstandard"[17] gilt und vielerorts nationale Bemühungen ähnlicher Art angestoßen hat. Durch die Einhaltung der DSGVO können Unternehmen einen besseren Umgang mit personenbezogenen Daten

13 IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980).
14 Schmidt-Versteyl, S.: Cybersecurity als Unternehmensleitungsaufgabe – Neue Aspekte der Organhaftung, in: Cybersecurity als Unternehmensleitungsaufgabe, S. 45–62.
15 LG München I, NZG 2014 345, 346ff..
16 Katko, Checklisten zur DSGVO, § 2 Accountability, Rn. 107.
17 Vgl. https://www.heise.de/hintergrund/Missing-Link-5-Jahre-DSGVO-Die-gezielte-Panikmache-hat-sich-gelegt-9059939.html?seite=all, Abruf am 12.03.2024.

gewährleisten und das Risiko von Datenschutzverletzungen und damit verbundenen rechtlichen Konsequenzen minimieren. Die Verpflichtung zur Einführung eines Datenschutz-Management-Systems kann bei der Umsetzung des CRA im Unternehmen Vorbild sein und ggf. sogar im Rahmen des Compliance-Managements helfen.

Auch die konkret im Zuge der DSGVO umgesetzten Maßnahmen lassen sich ggf. erweitern oder als Bausteine für den CRA wiederverwenden. Muss bspw. die Vertraulichkeit der im Produkt gespeicherten oder verarbeiteten Daten sichergestellt werden, kann man dies als Generalisierung der DSGVO-Anforderung zum Schutz der Vertraulichkeit personenbezogener Daten verstehen. Selbstredend eröffnet der CRA auch **neue Handlungsfelder**, die kein Äquivalent in der DSGVO besitzen. Dennoch sollte der CRA nicht als komplett eigenständiges Handlungsfeld im Sinne eines „Compliance-Stückwerks" verstanden werden.

Daher bietet es sich für Unternehmen an, auf ein **integriertes Risiko- und Compliance-Management sowie integrierte Entwicklungsprozesse** zu setzen, in denen Datenschutz und Cyber Resilience, aber auch andere aufstrebende Themen wie Nachhaltigkeit Bausteine in einem gemeinsamen Rahmenwerk bilden. Eine isolierte Betrachtung jedes Anforderungsgebiets trägt der Vielzahl an Erwartungen nicht ausreichend Rechnung und führt zu doppelten Aufwänden oder gar widersprüchlichen Anforderungen an das Produkt. Hierbei ist zu bedenken, dass Produkte oftmals **nicht allein für den europäischen Markt** entwickelt werden, sondern gleichermaßen z. B. die Anforderungen der Executive Order 14028 in den USA abdecken müssen, wenn das Produkt an die einschlägigen Kunden verkauft werden soll. Es ist zu erwarten, dass andere Staaten in Zukunft ebenfalls Regulatorik zur Cybersicherheit verabschieden werden. Nur ein integrierter Prozess bietet die Chance, ein in allen Zielmärkten rechtssicheres Produkt an den Markt zu bringen.

Dieses Whitepaper zielt mit seinen Empfehlungen zum CRA nicht nur darauf ab, die Compliance im Blick zu haben, sondern die **Umsetzung auch als Chance** für weitere Ziele innerhalb und außerhalb der Cybersicherheit zu nutzen. Neue Regulierungen können auch neue Märkte und Geschäftsmöglichkeiten schaffen, wenn Unternehmen innovative Lösungen entwickeln, um den neuen Anforderungen gerecht zu werden.

Dabei muss auch immer bedacht werden, dass Compliance für wirtschaftliche Akteure kein Selbstzweck ist. Neben der

Compliance muss der Prozess sicherstellen, dass ein **wirtschaftlich erfolgreiches Produkt** hergestellt wird, das die Bedürfnisse der Kunden befriedigt, sowohl hinsichtlich der Funktionalität als auch hinsichtlich des Preises und der Qualität. Auch diese Betrachtung spricht für integrierte Prozesse von der Erhebung der Anforderungen über die Entwicklung und Implementierung des Produkts bis hin zu den finalen Tests.

Es empfiehlt sich also nicht nur für strenger regulierte Organisationen der kritischen Infrastruktur, IT-Sicherheit in ein **Compliance-Management** aufzunehmen. Neben rechtlichen Auswirkungen darf nicht vergessen werden, welche betrieblichen und damit auch finanziellen Auswirkungen Cybervorfälle auf eine Organisation haben (siehe auch Infobox zum Return on Security Investment (RoSI), S. 52). Es gibt inzwischen eine Reihe von Unternehmen, die aufgrund eines solchen Vorfalls insolvent wurden.

Wie in allen anderen Bereichen gilt, dass zu einem erfolgreichen Management Messbarkeit gehört, weshalb zum einen bestimmte Kenngrößen, zum anderen interne und ggf. auch externe Audits eingeführt werden sollten. Wo sich entsprechende Messgrößen ableiten lassen, liegt die Integration ins Reporting nahe.

Sauber aufgestellte und dokumentierte **Cybersicherheitsprozesse und -verfahren** können dagegen sogar Versicherungsprämien senken.[18,19] Ganz zu schweigen von möglichem Reputationsverlust und den damit einhergehenden finanziellen Risiken. Unter diesem Blickwinkel sollte Cybersicherheit also integraler Teil des **betrieblichen Risiko- sowie Kontinuitätsmanagement** sein.[20]

18 Alspach, K.: Need cyber insurance? Get ready to show your data, in: Protocol, August 2022, https://www.protocol.com/enterprise/cyber-insurance-google-microsoft-aws.

19 Camillo, M.: Cyber risk and the changing role of insurance, in: Journal of Cyber Policy, 2017, S. 53–63.

20 Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-4 BCM, Business Continuity Management https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD_2_0.pdf?__blob=publicationFile&v=5.

Exkurs

Eine kurze Einführung in den Return on Security Investment

Während die Rendite von Investitionen in die Cybersicherheit üblicherweise mit der Methode **Return on Security Investment (RoSI)** berechnet wird, wurden auch schon andere Ansätze vorgesc hlagen, wie zum Beispiel der von Microsoft vorgeschlagene „Return on Mitigation".

Mithilfe einfacher Arithmetik und einigen weiteren Konzepten der Finanztheorie werden wir den **Wettbewerbsvorteil** veranschaulichen, den die Einhaltung des CRA bietet, und diese mit der RoSI-Metrik in Verbindung setzen.

Die grundsätzliche Berechnung erfolgt gemäß:

ROI= (Revenue-Investment)/Investment*100

Für RoSI sind speziell die folgenden Faktoren relevant:

- Single Loss Expectancy (SLE): Die geschätzten Verluste, die durch einen einzelnen Cyber-Sicherheitsvorfall verursacht werden,
- Annual Rate of Occurrence (ARO): Die erwartete Häufigkeit von Cyber-Sicherheitsvorfällen, die zu SLE-Verlusten führen,
- Annual Loss Expectation (ALE): Das Produkt aus SLE und ARO, das die erwarteten Verluste durch Cyber-Sicherheitsvorfälle darstellt,
- Mitigation Effectiveness (ME): Die Reduktion von ARO aufgrund angewendeter Minderung,
- Investment, oder Kosten der Kontrollen: Die Gesamtsumme der jährlichen Kosten zur Implementierung der Cyber-Sicherheitskontrollen, die die Minderungseffektivität gewährleisten.
- Es ist gängige Praxis, RoSI dann mit der folgenden Formel zu berechnen:

RoSI= ((SLE*ARO)*(ME)-Investment)/Investment

Der erste Term des Bruchs hat die Form (SLE*ARO)*(ME), was die jährlichen Einsparungen durch die Reduktion der Verluste aufgrund von Cyber-Sicherheitsvorfällen darstellt, die hier als Einnahmen interpretiert werden. Der RoSI-Index wird jedoch normalerweise mit den Renditen der Investitionen in die Sicherheit des Unternehmens selbst in Verbindung gebracht und gilt nicht unbedingt im Kontext des CRA,

da das Cyber-Sicherheitsrisiko und die damit verbundenen Verluste den Kunden oder Verbraucher betreffen und nicht das Unternehmen.

Um dieses Hindernis zu umgehen, werden wir einen weiteren Begriff aus der Finanztheorie einführen, nämlich den risikoadjustierten Umsatz (RAR). Er wird in den meisten Modellen mit der folgenden Formel berechnet:

RAR=Revenue*(1-Risk Adjustment Factor)

Für die Einnahmen können wir den erwarteten Verkaufsumsatz eines Produkts mal der Anzahl der verkauften Produkte einsetzen. Für den zweiten Term können wir die Risikodarstellungen der erwarteten Nutzenformeln verwenden, die wir in Kapitel 2 eingeführt haben. Zwischen den beiden untersuchten Fällen, d.h. vor und nach der Einhaltung des CRA, nimmt der Risikoadjustierungsfaktor (RAF) die Form an:

RAF=1-(Risk´-Risk)/(Risk´)

Je höher das Risiko, desto kleiner der RAR. Lassen Sie uns die Konzepte RAF und RAR anhand der Fälle U0 und U1 aus Kapitel 2 veranschaulichen. Wir kommen zu folgendem Ergebnis:

Risk = p2*L + p3*C = 0,2*800-0,1*200 = 140

Risk´= p2´*L´+p3*C = 0,1*1000 – 0,1*200 = 80

RAF = 1- 0,428= 0,572

Basierend auf diesen Berechnungen können wir feststellen, dass die nicht geminderten Risiken eines Produkts, das nicht mit dem CRA übereinstimmt, folgende sind:

RAR = Revenue* (1-RAF) = 0,428*Revenue

Wenn wir nun den RoSI-Index neu formulieren, um der Differenz zwischen den erwarteten gesteigerten Einnahmen aufgrund der Minderung des Cyber-Sicherheitsrisikos für die Produkte, die mit der CRA übereinstimmen, zu entsprechen, kommen wir zu:

RoSI= (Revenue*(RAF´-RAF)-CRA_Cost)/(CRA_Cost)

Unter dieser Formulierung wird die **Rendite der Sicherheitsinvestition** mit den Auswirkungen der Cybersicherheit und deren Auftretenswahrscheinlichkeit, die im RAF-Faktor enthalten sind, in Verbindung gebracht, beinhaltet aber auch positive Externalitäten, die die ursprüngliche Formulierung nicht ausgleichen kann.

Das ursprüngliche Dilemma, ob man **über die Einhaltung des CRA hinaus in die Cybersicherheit investieren** oder in zusätzliche Funktionalitäten für das Produkt mit digitalen Elementen investieren sollte, nimmt nun eine andere Gestalt an. Nehmen wir zum Beispiel zwei verschiedene Produkte an, die genau den gleichen erwarteten Nutzen für den Kunden haben, sich jedoch in der Größe ihrer jeweiligen Cybersicherheitsrisiken unterscheiden. Damit diese Bedingung zutrifft, muss der erwartete Ertrag des zweiten Produkts größer sein als der des ersten. Allerdings wird der RAR-Wert größer sein, sodass die erwarteten Einnahmen im Vergleich zum ersten Produkt geringer ausfallen werden. Infolgedessen gelten die Bedingungen für einen Wettbewerbsvorteil. Wenn man die oben genannten Projektionen sowie die sekundären Effekte, wie das Vertrauen in das Unternehmen, die Wertwahrnehmung der Produkte aufgrund der erhöhten Sicherheit und den allgemeinen Ruf des Unternehmens berücksichtigt, werden die Vorteile deutlich. Das liegt daran, dass der erwartete Nutzen des Produkts höher ist.

Zusammenfassend lässt sich sagen, dass selbst wenn die genaue Quantifizierung der Eintrittswahrscheinlichkeit eines Cybersicherheitsvorfalls schwierig ist, die finanziellen Dynamiken, die mit der Einhaltung des CRA verbunden sind, eher auf eine Chance als auf eine Belastung hindeuten.

Anhang: Die „grundlegenden Anforderungen“ an die Cybersicherheit im Überblick

Die konkreten technischen und prozessualen Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen sind zentral in **Anhang I des CRA** gelistet. Die Anforderungen sind technologieneutral formuliert und sollen sicherstellen, dass Cybersicherheit in der gesamten Lieferkette von Produkten mit digitalen Elementen berücksichtigt wird (Erwgr. 8 und 10 CRA). Sofern bestimme Anforderungen aus Anhang I auf ein Produkt **nicht anwendbar** sind, muss der Hersteller dies begründen und dokumentieren (Art. 13 Abs. 4 CRA).

Die „grundlegenden Anforderungen“ gliedern sich in **Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen** (Anhang I Teil I CRA) sowie **Anforderungen an die Behandlung von Schwachstellen** (Anhang I Teil II CRA).

Nachfolgend werden alle Anforderungen kurz im Überblick dargestellt und erklärend eingeordnet. Anforderungen, die im Whitepaper im Detail dargestellt werden, sind in der nachfolgenden Übersicht entsprechend verlinkt.

Anhang I Teil I: Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

Angemessenes Cybersicherheitsniveau: Grundsätzlich sind Produkte mit digitalen Elementen so zu konzipieren, entwickeln und herzustellen, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

Auf Grundlage der **Bewertung der Cybersicherheitsrisiken** sind soweit zutreffend folgende Anforderungen umzusetzen:

Ohne bekannte ausnutzbare Schwachstellen: Diese Anforderung kann sich auf den eigenen Code sowie auf die verwendeten Drittanbieterkomponenten (kommerziell und Open Source) beziehen.

Sichere Standardkonfiguration: Produkte sollten grundsätzlich mit einer sicheren Konfiguration ausgeliefert werden und dürfen kein reduziertes Sicherheitsniveau in Kauf nehmen, um der Bequemlichkeit des Nutzers oder einer schnelleren Vermarktung zu dienen. Zudem muss das Produkt auf diese Standardeinstellungen zurückgesetzt werden können, einschließlich der Löschung der Nutzerdaten.

Schutz vor unbefugtem Zugriff: Bspw. durch angemessene Authentifizierungsmechanismen, die sich nach dem Schutzbedarf der Produktfunktionen und der vom Produkt verarbeiteten Daten richten.

Schutz der Vertraulichkeit: Alle Daten, ob personenbezogen oder nicht, müssen vor unbefugter Einsichtnahme geschützt werden. Dies betrifft neben der Speicherung auch die Übermittlung und Verwendung der Daten.

Schutz der Integrität: Alle Daten, ob personenbezogen oder nicht, müssen vor unbefugter Veränderung geschützt werden. Dies gilt ebenso für Programme und Konfigurationen, solange die Änderungen nicht vom legitimen Nutzer autorisiert sind.

Datenminimierung: Betrifft unter dem CRA alle Daten, nicht nur personenbezogene. Dies kann bspw. dadurch erreicht werden, dass optionale Funktionen nur auf expliziten Nutzerwunsch aktiviert werden.

Schutz der Verfügbarkeit: Das Produkt sollte Basisfunktionalitäten auch bei Angriffen aufrechterhalten. Zudem sind Maßnahmen zur Eindämmung von DoS-Angriffen erforderlich, damit diese nicht auf verbundene Geräte übergreifen.

Minimierung von negativen Auswirkungen auf die Verfügbarkeit: Diese Anforderung befasst sich mit dem Schutz anderer Geräte innerhalb eines Netzwerkes, die über ein verwundbares Produkt angegriffen werden können. Es empfiehlt sich, diese Anforderung als grundsätzliche Betrachtung von Sicherheit in der Tiefe (Security in Depth) zu verstehen.

Reduzierung von Angriffsflächen: Sicherheitsrelevante Dienste, die nicht zwingend erforderlich sind, sollten standardmäßig abgeschaltet sein.

Verringerung der Auswirkungen eines Vorfalls: Diese Anforderung bezieht sich bspw. auf die Möglichkeiten eines Angreifers, das Produkt zu kompromittieren, nachdem er bereits eine initiale Schwachstelle ausgenutzt hat.

Sicherheitsmonitoring: Das Produkt muss seinen Zustand überwachen und protokollieren. Hieraus lassen sich Angriffe und andere Sicherheitsereignisse nachvollziehen.

Möglichkeiten zum Update zur Behebung von Schwachstellen: Es muss möglich sein, Sicherheitslücken mittels Patches zu schließen, wobei ein spezieller Fokus auf der automatischen Aktualisierung des Produkts liegt.

Teil II: Anforderungen an die Behandlung von Schwachstellen

Dokumentation von Komponenten und Schwachstellen, u.a. durch Erstellung einer Software Bill of Materials (SBOM): Schwachstellen entstehen nicht nur durch den eigenen Code, sondern auch durch verwendete Bibliotheken. Daher ist ein Überblick über die verwendeten Komponenten und ein Monitoring ihrer Schwachstellen unerlässlich.

Schwachstellenbehandlung, u. a. durch Bereitstellung von Sicherheitsupdates: Werden Schwachstellen im Produkt erkannt (unabhängig davon, ob sie durch eigenen Code oder durch verwendete Bibliotheken verursacht werden), müssen diese behoben werden. Im Regelfall geschieht dies durch Bereitstellung von Softwareupdates.

Sicherheitsüberprüfungen und -tests: Sicherheitslücken können nur behoben werden, wenn sie bekannt sind. Daher sind regelmäßige Tests durchzuführen, um Lücken zu identifizieren.

Bereitstellung von Informationen über beseitigte Schwachstellen: Sobald ein Sicherheitsupdate bereitsteht, müssen Nutzer über die behobenen Lücken und deren Auswirkungen informiert werden, einschließlich ggf. notwendiger weitere Aktivitäten des Nutzers (z. B. Anpassungen der Konfiguration).

Strategie zur koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure (CVD)): Hersteller müssen einen Prozess anbieten, mit dem Dritte (nicht zwingend nur eigene Kunden) Sicherheitslücken in den Produkten melden können. Diese Berichte müssen geprüft und die entsprechenden Lücken behoben werden.

Maßnahmen zum Informationsaustausch zu Schwachstellen, u. a. Kontaktadresse für Meldungen: Als konkrete Maßnahme für CVD muss eine Kontaktadresse für Schwachstellenmeldungen eingerichtet werden. Zudem müssen Informationen in das Unternehmen fließen können, z. B. wenn Schwachstellen in verwendeten Komponenten veröffentlicht werden.

Mechanismen zur Verbreitung von Updates: Patches für Sicherheitslücken müssen den Kunden so bereitgestellt werden können, dass der Updateprozess selbst keine neuen Sicherheitslücken erzeugt. Gleichzeitig muss der Prozess hinreichend schnell sein, um Lücken in der Praxis zeitnah zu schließen, i. d. R. durch automatisierte Updates. Diese Anforderung bezieht sich auf die Infrastruktur für die Bereitstellung der Updates.

Bereitstellung von Sicherheitsupdates: Diese Anforderung bezieht sich auf die tatsächliche Bereitstellung der Updates. Updates müssen kostenlos sein, unverzüglich bereitgestellt und dokumentiert werden (z. B. falls der Nutzer noch weitere Aktivitäten ergreifen muss). Letztlich darf ein Sicherheitsupdate den Kunden auch nicht dazu zwingen, neue Hardware zu kaufen.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit