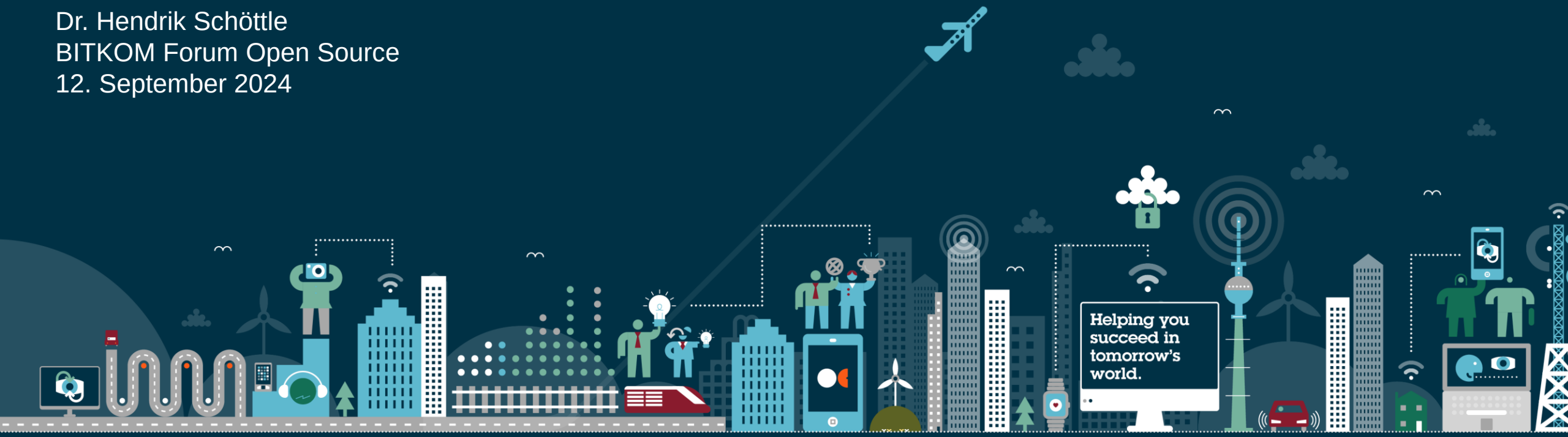
Von kybernetischer Resilienz, Verwaltern quelloffener EDV-Programme und gesetzlichen Neuregelungen

Was der Cyber Resilience Act für Unternehmen, OSS Stewards und Communities bedeutet

Dr. Hendrik Schöttle
BITKOM Forum Open Source
12. September 2024



NEWS

Pwnie Awards

Crowdstrike erhält Award für "Most Epic Fail"

Mo 12.08.2024 - 12:43 Uhr
von Gayathri Albert und jor

Nach der globalen IT-Panne hat Crowdstrike den Award für den "Most Epic Fail" an der Sicherheitskonferenz Def Con entgegengenommen. Der Präsident von Crowdstrike, Michael Sentonas, nahm den Schmähpreis persönlich an.

Reorganisation der Regionen
Update: Christoph Kaelin verlässt Extreme Networks
20.08.2024 - 11:26 Uhr

Fachbeitrag von Aveniq
Cybersecurity und unternehmerische Nachhaltigkeit: Eine neue Perspektive
19.08.2024 - 07:00 Uhr

Konfigurationsfehler
Datenleck bei Flightaware gibt jahrelang Nutzerdaten preis

Die xz-Hintertür: Das verborgene Oster-Drama der IT

Mit einer Hintertür in einer unbekannten Kompressionsbibliothek hätten Unbekannte beinahe große Teile des Internets übernehmen können. Leider kein Scherz.

(Bild: BeeBright / Shutterstock.com)

02.04.2024, 17:10 Uhr Lesezeit: 8 Min. | Security

Regulatorische Anforderungen/Standards | Überblick

Aktuelle Gesetzgebungsinitiativen im Bereich IT-Sicherheit:

- **Cyber Resilience Act (CRA):** Ziel ist Gewährleistung der IT-Sicherheit. **Stand:** Verabschiedung des finalen Entwurfs durch das EU-Parlament am 12. März 2024, Verkündung steht noch aus. Umsetzungszeitraum der Mitgliedstaaten: 36 Monate nach Inkrafttreten. Meldepflichten werden allerdings schon 21 Monate nach Inkrafttreten wirksam.

- **Network and Information Systems Directive (NIS-2):** Ziel ist ebenfalls Gewährleistung der IT-Sicherheit, adressiert werden aber nur Betreiber kritischer Infrastrukturen. **Stand:** In Kraft, Umsetzung in den Mitgliedstaaten bis zum 17. Oktober 2024, in Deutschland finaler Regierungsentwurf des NIS-2UmsuCG am 22. Juli 2024 vom BMI veröffentlicht.

- **Product Liability Directive (PLD):** Neuregulierung der Produkthaftung; Aufnahme von Software. **Stand**: Verabschiedung des finalen Entwurfs durch das EU-Parlament am 12. März 2024, formelle Bestätigung durch den Rat steht noch aus. Umsetzungszeitraum der Mitgliedstaaten: 24 Monate nach Inkrafttreten.

- **Technische Richtlinie TR-03183 (BSI-Techn RL):** Cyber-Resilienz-Anforderungen an Hersteller und Produkte – Version 1.0 vom 12. Juli 2023

- **Executive Order 14028** der US-Regierung und hierzu **Mindestanforderungen** an die SBOM der National Telecommunications and Information Administration (NTIA)

Cyber Sticker (10 Stk.)
Ab €2,50

Cyber Klebeband
€10

Cyber Absperrband
€10

Cyber Becher
€5

IM ANGEBOT

Cyber Starterpaket
~~€30,50~~ €25

Cyber-Produkte für eine sichere und moderne Technologie-Zukunft!

Erleben Sie die Zukunft der Technologie mit unseren Cyber-Produkten. Ob Sicherheitslösungen für Ihre Daten, moderne Geräte für eine effizientere Arbeit oder innovative Gadgets für den Alltag - wir bieten Ihnen alles, was Sie für eine sichere und moderne Zukunft brauchen. Unsere Cyber-Produkte werden von führenden Experten entwickelt und bieten Ihnen höchste Qualität und Zuverlässigkeit.

Mit unseren Produkten können Sie sicher sein, dass Sie immer auf dem neuesten Stand der Technologie sind. Erleben Sie eine sichere und moderne Zukunft und bestellen Sie jetzt Ihre Cyber-Produkte bei uns. Entdecken Sie die Zukunft der Technologie! Cyber all the Things!

Cyber Resilience Act | Regulatorische Anforderungen/Standards

- **An wen richtet sich der CRA?**
  - CRA enthält Regelungen für „*Produkte mit digitalen Elementen*“ (Art. 3 Nr. 1 CRA)
  - Relevanz für verschiedene „Wirtschaftsakteure“ (Art. 3 Nr. 12 CRA), und zwar für:
    - **Hersteller,** insb. Pflichten Art. 13 ff. CRA; Inverkehrbringen der Produkte
    - **Bevollmächtigte der Hersteller,** Art. 18 CRA; nicht alle Pflichten übertragbar
    - **Einführer,** insb. Pflichten nach Art. 19 CRA; Einführen der Produkte
    - **Händler,** insb. Pflichten nach Art. 20 CRA; Bereitstellen der Produkte auf dem Markt
    - **Quasi-Hersteller,** Art. 22 CRA; jeden, der Änderungen am Produkt vornimmt, treffen die Pflichten des Herstellers bei *„wesentlicher Produktänderung“*
  - **OSS-Stewards** (Art. 3 Nr. 14 CRA), insb. Pflichten nach Art. 24 CRA; *Entwicklung und Dokumentation von Cybersicherheitsstrategien*

Cyber Resilience Act | Regulatorische Anforderungen/Standards

Anforderungen (siehe Annex I „**essential cybersecurity and vulnerability handling requirements**“):

- Erstellen einer **Software-Stückliste** (SBOM) gem. EG 78, Anhang I, 2. (1).
- Durchführung und regelmäßige Überprüfung eines Assessments des „**Cybersicherheitsrisikos**“, Art. 13 Abs. 3 CRA, Aufnahme eines solchen in die technische Dokumentation, Art. 13 Abs. 4
- Konformitätsbewertungsverfahren und Erstellen einer „**Konformitätserklärung**“, Art. 13 Abs. 12, 28 Abs. 1 CRA und Anhang IV
- **CE-Kennzeichnung** der Produkte, Art. 13 Abs. 12, 30 Abs. 1 CRA
- **Updatepflichten** für die erwartete Lebensdauer des Produkts mit digitalen Elementen, unklare Regelung, die fünf Jahre offenbar als groben Rahmen vorsieht (es kann auch weniger als fünf Jahre sein, Beweislast dann wohl beim Hersteller, Art. 13 Abs. 8 CRA)
- Umfangreiche **Meldepflichten** für Softwarehersteller nach Art. 14 CRA
  - bei einer aktiv ausgenutzten Schwachstelle spätestens innerhalb von 24 Stunden an **ENISA** (European Network and Information Security Agency) (Art. 14 Abs. 1 CRA) über eine einheitliche **Meldeplattform** (Art. 16 CRA)
  - **Information der Nutzer** über die aktiv ausgenutzte Schwachstelle sowie über von diesen Nutzern zu ergreifende Maßnahmen (Art. 14 Abs. 8 CRA)
  - Upstream an Entwickler von Drittkomponenten (Art. 13 Abs. 6)

Cyber Resilience Act | Sachlicher Anwendungsbereich

- Anwendung auf Produkte mit **digitalen Elementen** (Art. 3 Nr. 1 CRA), als „Software- oder Hardwareprodukt **und** dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden“

- eine Datenfernverarbeitungslösung (Art. 3 Nr. 2 CRA) ist eine „entfernt stattfindende Datenverarbeitung […] ohne die das Produkt […] eine seiner Funktionen nicht erfüllen könnte“

  - Datenfernverarbeitungslösung ist also Voraussetzung für die Anwendbarkeit des CRA

  - hiervon erfasst sein dürfte **jede Schnittstelle, die zwei entfernte Geräte miteinander verbindet;** es sei denn, es handelt sich um eine „Einwegschnittstelle“

  - nicht direkt geregelt, wie es sich mit Schnittstellen verhält, die zwar vorhanden sind, aber für die Funktionalität des Produkts nicht benötigt werden (z.B. WLAN-Adapter oder LAN-Schnittstelle)

  - Anwendungsbereich daher möglicherweise weit zu verstehen, da fehlender Zweck einer dennoch vorhandenen Schnittstelle potenziellen Angreifern egal sein dürfte

Cyber Resilience Act | Regulatorische Anforderungen/Standards

- CRA ordnet Produkte in 4 **Sicherheitskategorien** ein:
  - (einfache) Produkte mit digitalen Elementen
  - wichtige Produkte mit digitalen Elementen
    - Klasse I
    - Klasse II
  - kritische Produkte mit digitalen Elementen
- Nach Art. 32 CRA muss für jedes Produkt eine **Bewertung durchgeführt werden, ob die grundlegenden Anforderungen des Anhangs I eingehalten werden**
- Bewertung erfolgt durch Hersteller selbst, anhand von „*harmonisierten Normen*“ oder durch unabhängige Dritte, je nach Kategorie

Cyber Resilience Act | Regulatorische Anforderungen/Standards

- **Sanktionsregime** vergleichbar mit dem der DSGVO:
  - Verstoß gegen grundlegende Sicherheitsanforderungen: max. 15 Mio. EUR oder bis zu 2,5 % des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr (Art. 64 Abs. 2)
  - Verstoß gegen übrige Sicherheitsanforderungen: max. 10 Mio. EUR bzw. 2 % (Art. 64 Abs. 3)
  - Unrichtige, unvollständige oder irreführende Meldungen gegenüber Behörden: max. 5 Mio. EUR bzw. 1% (Art. 64 Abs. 4)

Cyber Resilience Act | Räumlicher Anwendungsbereich

- Alle innerhalb des Unionsmarktes in Verkehr gebrachten Produkte mit digitalen Elementen, ungeachtet des Herstellungsorts
- Wenn außerhalb der Union hergestellt, ist der CRA anwendbar auf diejenigen, die das Produkt auf dem Unionsmarkt in den Verkehr bringen
- Adressaten der Norm müssen sicherstellen, dass beim Import von Produkten schon bei der Herstellung und über den Lebenszyklus der Produkte die Pflichten eingehalten werden

Cyber Resilience Act | Wichtigste Pflichten

- **Länge des Unterstützungszeitraums**
  - Mindestens fünf Jahre (Art. 13 Abs. 8 CRA), es sei denn, das Produkt ist weniger als fünf Jahre in Betrieb, dann voraussichtliche Nutzungsdauer
  - Ggf. sinnvolle Anknüpfung an Zeitraum, in dem etwaige Gewährleistungsansprüche geltend gemacht werden können
- **Sicherheits-Risikobewertung**
  - Bewertung muss sich auf die gesamte Produktlebensdauer erstrecken (Art. 13 Abs. 2 bis 4 CRA), d.h. alles von der Planungs- bis zur Wartungsphase
  - Sicherheitsbewertung geknüpft an den Unterstützungszeitraum
- Zudem Empfehlung, Source Code nach End of Life zu veröffentlichen, EG 62.

Cyber Resilience Act | Wichtigste Pflichten

- **Meldepflichten nach Art. 14 – Fristen**
  - Unterscheidung zwischen aktiv ausgenutzter Schwachstelle und schwerwiegendem Vorfall
  - **Innerhalb von 24 Std**. **„Frühwarnung“** an CSIRT und ENISA (Art. 14 Abs. 2 a) bzw. Abs. 4 a)) ab Kenntnisnahme von der aktiv ausgenutzten Schwachstelle/des schwerwiegenden Vorfalls
  - **Innerhalb von 72 Std. Abgabe einer „vollständigen“ Meldung** an CSIRT und ENISA (Art. 14 Abs. 2 b) bzw. Abs. 4 b)), die u.a. allgemeine Informationen über das Produkt, die Art der Ausnutzung der Schwachstelle und ergriffene Korrektur- und Risikominderungs- bzw. Abhilfemaßnahmen benennt
  - **Innerhalb von 14 Tagen oder einem Monat Erstellung eines Abschlussberichts**: 14 Tage bei aktiv ausgenutzter Schwachstelle (Art. 14 Abs. 2 c)), ein Monat bei schwerwiegendem Vorfall (Art. 14 Abs. 4 c)) der die Schwachstelle sowie deren Auswirkungen und Informationen enthalten muss über die Angreifer, soweit bekannt, sowie Informationen über Updates und Patches, die zur Verfügung gestellt wurden
  - Fristen allesamt extrem kurz bemessen

Cyber Resilience Act | Wichtigste Pflichten

- **Meldepflichten nach Art. 14 – Was ist eine „aktiv ausgenutzte Schwachstelle“?**
  - Art. 3 Nr. 42 CRA verlangt, dass „*ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat*“
  - Ausnutzung nur beim Hersteller oder genügt gerade auch eine „allgemeine“ Ausnutzung?
  - Abstellen auf Ausnutzungs**möglichkeit** im konkreten Fall erscheint sinnvoll
- **Meldepflichten nach Art. 14 – Was ist ein „schwerwiegender Sicherheitsvorfall“?**
  - Voraussetzungen bereits erfüllt, wenn Vorfall sich „*negativ auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit auswirkt oder […] zur Ausführung von Schadcode geführt hat oder […] führen kann*“ (Art. 19 Abs. 5 CRA)

Cyber Resilience Act | Wichtigste Pflichten

- **Meldepflichten nach Art. 14 – Wer ist neben den Behörden sonst noch Adressat?**
  - ***downstream* Information** der betroffenen Nutzer über die aktiv ausgenutzte Schwachstelle sowie über von diesen Nutzern zu ergreifende Maßnahmen (Art. 14 Abs. 8 CRA)
  - ***upstream* Information** der Maintainer von (auch fremder) OSS (Art. 14 Abs. 7 CRA)
    - kein konkreter Weg vorgeschrieben
    - Meldepflicht besteht auch dann, wenn Upstream die Schwachstelle bereits bekannt ist
    - Maintainer von (OSS-)Projekten dürften schnell in (hundert)tausenden Meldungen ertrinken
    - Risiko, dass einfach per E-Mail gemeldet wird – und dass Maintainer dadurch handlungsunfähig sind, weil sie gerade dann, wenn eine Sicherheitslücke zu patchen ist, erst einmal mit ihrem E-Mail-Provider eine Quota-Erhöhung verhandeln müssen, um überhaupt wieder erreichbar zu sein.
    - Einzige Hoffnung: Änderung Non-Compliance der Verpflichteten...

Cyber Resilience Act | Bereichsausnahme für OSS

Genese des CRA im Hinblick auf Open-Source-Software

- Erweiterung des ursprünglich geplanten Anwendungsbereichs von iOT auf Softwarelösungen allgemein versetzte die OSS-Community in Aufruhr
- OSS wird in weiten Teilen von Unternehmen mit kommerziellen Interessen entwickelt – aber mit einem ganz anderen wirtschaftlichen Setup als kommerzielle Softwareanbieter
- OSS-Foundations hätten möglicherweise vollständig dem CRA unterlegen
- Gesetzgeber hingegen schien ursprünglich von Garagenbastlern und Wochenend-Hobbyentwicklern als Standardfall auszugehen
- Einwände der Community wurden gehört und haben zu weitreichenden Anpassungen im Gesetzestext geführt. Leider damit auch zur Divergenz von der PLD (dort ursprünglich identisch geregelt)

Cyber Resilience Act | Bereichsausnahme für OSS

Der Open-Source Software Steward

- Verwalter quelloffener Software (Open-Source Software Stewards) unterliegen nach Art. 24 nur wenigen Pflichten des CRA.
- Voraussetzungen:
    - Sie sind „Verwalter quelloffener Software“ nach Art. 3 Nr. 14
    - Die Definition quelloffener Software (Art. 3 Nr. 48) ist erfüllt

Cyber Resilience Act | Bereichsausnahme für OSS

Art. 3, Nr. 48

„freie und quelloffene Software“ eine Software, deren Quellcode offen geteilt wird und die im Rahmen einer kostenlosen Open-Source-Lizenz zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen

- Source-Code-Verfügbarkeit erforderlich? Oder auch BSD und MIT erfasst?
- *„**kostenlosen** Open-Source-Lizenz“*? Nicht definiert.
- Im Englischen: “free and open-source license”
- gemeint ist wohl eher “free as in freedom, not as in free beer” (https://www.gnu.org/philosophy/free-sw.html.en) – also “frei” und nicht “kostenlos”

Cyber Resilience Act | Open-Source Software Steward

Art. 3, Nr. 14 – Begriffsdefinition des Open-Source Software Stewards (OSSS)

‘Verwalter quelloffener Software‘ ist eine juristische Person, bei der es sich nicht um den Hersteller handelt, die […] die Entwicklung spezifischer Produkte […], die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Vermarktbarkeit dieser Produkte sicherstellt;

- Zweck, systematisch Support auf nachhaltiger Basis zu liefern
- OSS wird entwickelt
- für kommerzielle Zwecke anderer Akteure bestimmt
- Was ist systematischer Support? Was ist eine nachhaltige Basis?

- Konsequenz:
  - „Verpflichteter light“ neben den Herstellern ohne eigenes Interesse an der Vermarktung der OSS
  - Bußgelder greifen nicht, vgl. Art. 64 Nr. 10 b)

Cyber Resilience Act | Open-Source Software Steward

- Abgrenzung bei kleineren Organisationen wohl nach dem Tätigkeitsschwerpunkt
- Auch hier schlägt das Kriterium der „Datenfernverarbeitung“ zu Buche
- Wenn bloß Produkt entwickelt wird, das lediglich bestimmte Teilaufgaben erledigt und keinerlei Netzwerkschnittstelle benötigt, dürfte eine Anwendbarkeit des CRA ausscheiden

Cyber Resilience Act | Open-Source Software Steward | Pflichten

Art. 24

- Erstellung von Cybersecurity Policies und Übermittlung derselben an die Marktüberwachungsbehörde auf deren „begründetes Verlangen“
- Förderung
  - der Entwicklung eines sicheren Produkts
  - der freiwilligen Meldung von Sicherheitslücken
  - des Informationsaustauschs über aufgedeckte Schwachstellen innerhalb der OSS-Community
- Zusammenarbeit mit den Marktüberwachungsbehörden, um Cybersicherheitsrisiken von OSS zu mindern
- Meldung von aktiv ausgenutzten Schwachstellen an die ENISA über die Meldeplattform, soweit OSSS an der Entwicklung der Produkte (durch OSS oder anderweitig) beteiligt sind
- „Detailgrad“ der Meldung abhängig davon, ob es sich um einen schwerwiegenden Vorfall handelt, der Netz- und Informationssysteme beeinträchtigt, die von den OSSS für die Entwicklung solcher Produkte bereitgestellt werden

Cyber Resilience Act | Open-Source Software Steward | Pflichten

Art. 64 Nr. 10 b)

Abweichend von den Absätzen 3 bis 10 gelten die in diesen Absätzen genannten Geldbußen nicht für

[…]

*b) Verwalter quelloffener Software bei **jedem** Verstoß gegen diese Verordnung.“*

- Keine Strafen, wenn OSSS ihre Pflichten nicht erfüllen

Cyber Resilience Act | Open-Source Software Steward | Fazit

- Bislang eher weiche Regelungen für OSSS – Cybersecurity Policy erstellen und ggf. offenlegen
- IT-Sicherheit und Meldungen von Sicherheitslücken fördern
- Abgrenzungsfragen:
  - Wann bin ich OSSS?
  - Was ist systematischer Support auf nachhaltiger Basis im Sinne des Art. 3 Nr. 14? Foundation ja, Einzelentwickler, der regelmäßig released auch?
  - Was ist mit Dual-Licensing-Modellen? Commercial Edition = product with digital elements. Community Edition wohl nicht.
  - Kann dann das Unternehmen, das dual lizenziert, gleichzeitig OSSS und Manufacturer sein? Art. 3 Nr. 14: OSSS ist „*eine juristische Person, bei der es sich nicht um einen Hersteller handelt* “ → wohl eher nicht.

Regulatorische Anforderungen/Standards | Technische Richtlinie

Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte, Teil 2: SBOM
(July 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=3)

- Beschreibt die Anforderungen an eine SBOM, wie sie im aktuellen Entwurf des CRA gefordert wird
- Definiert SBOM (dt. Software-Stückliste/ -Teileliste) als: *„eine maschinenverarbeitbare Datei, die Details und Lieferkettenverhältnisse der in einer Software genutzten Komponenten enthält.“* (Seite 6)
- Ziel: Überprüfung, *„ob ein Produkt potenziell von einer Schwachstelle betroffen ist, indem dessen Komponentenliste mit den in den Schwachstelleninformationen aufgeführten Software-Komponenten abgeglichen wird.“* (Seite 4), enthält selbst aber keine Informationen zu Schwachstellen (Seite 6)
- Muss für jede Softwareversion neu erzeugt werden (Seite 6)
- Und in folgenden Formaten vorliegen:
  - CycloneDX in der Version 1.4 oder höher
  - SPDX in der Version 2.3 oder höher

Regulatorische Anforderungen/Standards | Executive Order

Software Bill of Materials („**SBOM**“): Darstellung von Informationen der Software Supply Chain – quasi eine maschinenlesbare Inventur

Ziel: Transparenz und Erkennen von potenziellen Sicherheitslücken und rechtlichen Risiken

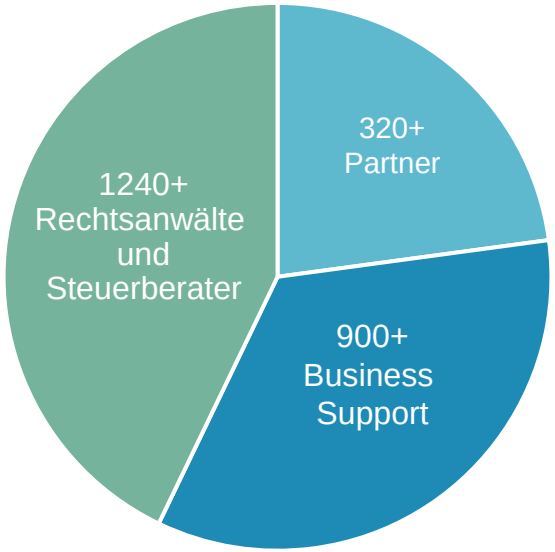
Hintergrund: Erfolgreicher Hack von kritischer Infrastruktur in den USA

- **Executive Order 14028 der US-Regierung**
  (Mai 2021, www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom)
  - Verlangt Mitlieferung von SBOM bei Produktlieferungen an US-Behörden
  - Definiert SBOM in Sec 10 (j) als: *“a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. […]”*
  - Herausforderung: Unternehmen müssen Informationen übermitteln, die meist bislang gar nicht erhoben werden

Osborne Clarke International

2,480

Mitarbeiter



25

internationalen Standorten*

Europa

Belgien: Brüssel
Deutschland: Berlin, Hamburg, Köln, München
Frankreich: Paris
Italien: Busto Arsizio, Mailand, Rom
Niederlande: Amsterdam
Polen: Warschau
Schweden: Stockholm
Spanien: Barcelona, Madrid, Saragossa
Vereinigtes Königreich: Bristol, London, Reading

USA

New York, San Francisco

Asien

China: Shanghai
Indien*: Bangalore, Mumbai, Neu-Delhi
Singapur

*Dienstleistungen in Indien werden von einer Partnerfirma angeboten

Kontakt

Dr. Hendrik Schöttle
Partner, Fachanwalt für IT-Recht
Germany

+49 89 5434 8046
hendrik.schoettle@osborneclarke.com

„Hat sich im Bereich Open Source einen Spitzennamen gemacht“

Wettbewerber, JUVE-Handbuch 2023/2024

Dr. Hendrik Schöttle berät im IT- und Datenschutzrecht.

Hendrik wurde 2023 vom Handelsblatt und von Best Lawyers zum Anwalt des Jahres für IT-Recht in Bayern gekürt. Er wurde in den letzten Jahren wiederholt sowohl vom Handelsblatt und von Best Lawyers als auch von der Wirtschaftswoche, von Legal 500 und vom Kanzleimonitor als einer der besten Anwälte bzw. als mehrfach empfohlener Anwalt im IT-Recht genannt. Das JUVE-Handbuch 2023/2024 empfiehlt ihn als Spitzenname im Bereich Open Source.

Er hat langjährige Erfahrung bei der Beratung, Vertragsgestaltung und Verhandlung von komplexen IT-Projekten. Seine Schwerpunkte sind IoT, Digitalisierung und Cloud Computing. Er berät zu Software-Lizenzmodellen, insbesondere zu Open-Source-Software, und im Datenschutzrecht. Zu seinen Mandanten gehören international tätige Technologiekonzerne sowie namhafte IT- und E-Business-Unternehmen.

Hendrik Schöttle arbeitet seit 2005 als Rechtsanwalt, seit 2007 im Münchner Büro von Osborne Clarke. Er war mehrfach im Rahmen von Secondments in Rechtsabteilungen von IT-Unternehmen tätig. Zudem hat er mehrere Jahre als Software-Entwickler am Institut für Rechtsinformatik der Universität des Saarlandes gearbeitet. Seine praktische Erfahrung und sein technisches Know-how kommen seinen Mandanten bei der technologienahen Beratung zugute.

Er ist Autor zahlreicher Veröffentlichungen, Mitautor mehrerer Handbücher und Kommentare, unter anderem des Beck’schen Handbuchs IT- und Datenschutzrecht und des juris Praxiskommentars zum BGB.

Hendrik Schöttle ist Dozent der Deutschen Anwaltakademie für den Fachanwaltslehrgang IT-Recht und hält regelmäßig Vorträge zu Themen des IT-Rechts.

Er ist Mitglied im Vorstand des Arbeitskreises Open Source des BITKOM, Mitglied des Ausschusses Datenschutzrecht der Bundesrechtsanwaltskammer (BRAK), der Arbeitsgemeinschaft Informationstechnologie im Deutschen Anwaltverein (DAV) und der Deutschen Gesellschaft für Recht und Informatik (DGRI).