Deutsche Stiftung für Recht und Informatik

Meldepflichten des Cyber Resilience Acts

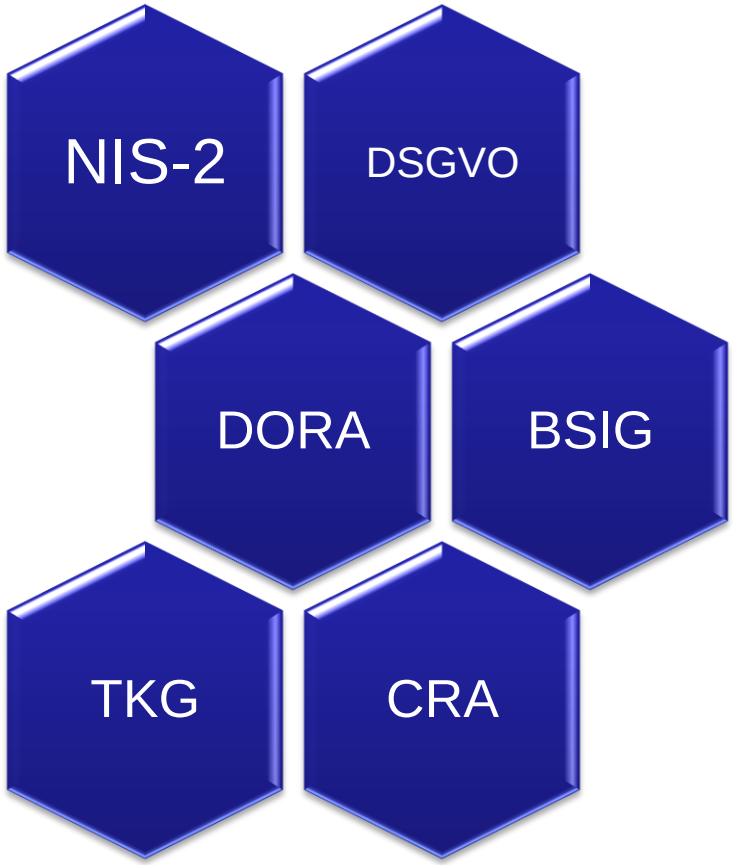
Dipl.- Jur. Alexander Erdelt, LL.M.
Mainova AG

Herbstakademie 2024

Agenda

1. Meldepflichten im IT-Sicherheitsrecht
2. Meldepflichten nach Art. 14 CRA
3. Informationspflichten gegenüber Nutzern und Verwaltern quelloffener Software
4. Sanktionen bei Nichteinhalten
5. Freiwillige Meldungen nach Art. 15 CRA
6. Schwachstellendatenbank; Meldeplattform
7. Vergleichbarkeit des Meldesystems des CRA mit denjenigen der NIS-2-RL und demjenigen der DSGVO
8. Fazit und Ausblick

Meldepflichten im IT-Sicherheitsrecht



Überblick: Meldepflichten des CRA

- Art. 14 Abs. 1 S. 1 CRA
- Art. 14 Abs. 3 CRA
- Art. 15 Abs. 1 CRA (freiwillige Meldung)
- Art. 15 Abs. 2 CRA (freiwillige Meldung)

Meldepflicht nach Art. 14 Abs. 1 CRA *

Artikel 14

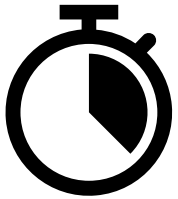
Meldepflichten der Hersteller

(1) Ein Hersteller meldet ▌ jede aktiv ausgenutzte Schwachstelle, die in dem Produkt mit digitalen Elementen enthalten ist ***und von der er Kenntnis erlangt, gleichzeitig dem gemäß Absatz 7 als Koordinator benannten CSIRT und der ENISA. Der Hersteller meldet diese aktiv ausgenutzte Schwachstelle über die gemäß Artikel 16 eingerichtete einheitliche Meldeplattform.***

*Quelle: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.html

Meldepflicht nach Art. 14 Abs. 1 CRA

- Meldung einer **aktiv ausgenutzten Schwachstelle**
- Abgestuftes Meldesystem:



  - Frühwarnung: unverzüglich, jedenfalls innerhalb von 24 Stunden, Art. 14 Abs. 2 a) CRA
  - Meldung innerhalb von 72 Stunden, Art. 14 Abs. 2 b) CRA
  - Meldung innerhalb von 14 Tagen, Art. 14 Abs. 2 c)

- Jeweils ab Kenntniserlangung

Aktiv ausgenutzte Schwachstelle

Art. 3 Nr. 42 CRA:

„eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat“

ErwGr. 69 S. 1 CRA konkretisierend zu „aktiv ausgenutzten Schwachstellen“:

- „Böswilliger Akteur“ nutzt Fehler in einem Produkt mit digitalen Elementen
- Begriff „Böswilliger Akteur“ nicht im CRA definiert, wohl z. B.: Hacker
- Dadurch wird ein Schaden für den Nutzer oder eine andere natürliche Person verursacht
- Schwächen in den Identifizierungs- und Authentifizierungsfunktionen eines Produktes, ErwGr. 69 S. 2 CRA

Meldepflicht nach Art. 14 Abs. 3 CRA

Ein Hersteller meldet ▌ jeden ***schwerwiegenden*** Vorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt ***und von der er Kenntnis erlangt, gleichzeitig dem gemäß Absatz 7 als Koordinator benannten CSIRT und der ENISA. Der Hersteller meldet diesen Vorfall über die gemäß Artikel 16 eingerichtete einheitliche Meldeplattform.***

Meldepflicht nach Art. 14 Abs. 3 CRA

- Meldung eines **schwerwiegenden** Sicherheitsvorfalles
- „Sicherheitsvorfall“, Art. 3 Nr. 43 CRA
- Verweis auf Art. 6 Abs. 6 NIS-2-RL (RL (EU) 2022/2555))
  - Art. 6 Nr. 6 NIS-2 RL: Sicherheitsvorfall“ [ist] 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;
- „Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen“, Art. 3 Nr. 44 CRA
  - einen Sicherheitsvorfall, der sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen;

Schwerwiegender Vorfall

- Art. 14 Abs. 5 a) CRA:

  schwerwiegender Vorfall

  negative Auswirkung auf Fähigkeit des PmdE: Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von sensiblen Daten oder Funktionen

- Art. 14 Abs. 5 b) CRA:

  hat zu Einführung oder

  Ausführung eines böswilligen Codes in einem PmdE oder im Netzwerk und Informationssystem

  bei einem Nutzer geführt oder dazu führen kann

Adressaten der Meldung nach Art. 14 Abs. 1 und 3 CRA

Informationspflichten gegenüber Nutzern und Verwaltern quelloffener Software

- Information des Herstellers gegenüber **Nutzern**, Art. 14 Abs. 8 CRA
- über: aktiv ausgenutzte Schachstelle
- über: schwerwiegenden Vorfall
- zudem: Mitteilung von Risikominderungsmaßnahmen oder Korrekturmaßnahmen
- Information des Herstellers gegenüber **Verwaltern quelloffener Software** (Art. 3 Nr. 14 CRA)
- Verweis in Art. 24 Abs. 3 S. 2 CRA auf Pflichten in Art. 14 Abs. 3 und 8 CRA
- Die Pflichten sind gegenüber denjenigen der Hersteller deutlich reduziert

Sanktionen bei Nichtbeachten der Meldepflichten des CRA

- Geldbußen, Art. 64 Abs. 2 CRA
- Bis zu 15 Mio. EUR oder bis zu 2,5 % des weltweiten Jahresumsatzes bei Verstoß z. B. gegen Art. 14 CRA (wenn Adressat ein Unternehmen ist)
- Je nachdem welcher Betrag höher ist
- Anknüpfen an Bußgeldmodell der DSGVO, wenn auch nicht unbedingt einfach zu übernehmen
- Ausnahmen bei Kleinstunternehmen, Kleinunternehmen oder Verwaltern quelloffener Software, sofern die in Art. 14 Abs. 2 lit. a oder Abs. 4 lit. b CRA genannten Fristen der Meldepflichten nicht eingehalten wurden

Meldung nach Art. 15 Abs. 1 CRA

- Meldung von **Schwachstellen** und **Cyberbedrohungen**
- „Cyberbedrohung“, Art. 3 Nr. 46 CRA: *„Cyberbedrohung“ ist eine Cyberbedrohung gemäß der Begriffsbestimmung in Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 (Cybersecurity Act)*
- **Art. 2 Nr. 8 (EU) 2019/881:**

  „Cyberbedrohung“ bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte“
- Es kann, muss aber nicht gemeldet werden
- Neben **Herstellern** auch
- **Natürliche** und **juristische** Personen
- Insb. **Verwalter quelloffener** Software gem. Art. 24 Abs. 1 CRA sollen freiwillige Meldungen tätigen

Meldung nach Art. 15 Abs. 2 CRA

- Meldung eines jeden Vorfalles, der sich auf die Sicherheit des Produktes mit digitalen Elementen auswirkt

- Auch: Beinahe-Vorfälle, Art. 3 Nr. 45 CRA - Verweis auf Art. 6 Nr. 5 NIS-2-RL:

> „“Beinahe-Vorfall“ [ist] 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 haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist.“

- Erweiterung von „Meldepflichten“ auf weniger schwerwiegende Vorfälle

Kritik am Meldesystem des CRA

- Zu kurze Frist zur Abgabe einer Meldung nach Art. 14 Abs. 1 S. 1 CRA
- Prozesse und technische Umsetzung, z. B. mittels Schnittstellenkonzepts
- An ENISA und CSIRT ist zu melden
- Informationen könnten Hacker für weitere Angriffe genutzt werden
- Kein Eigeninteresse der Hersteller an der Meldung von Schwachstellen wegen Reputationsschäden?
- Aber: Anreize bereits in der Herstellung cybersicheres Produkt zu erhalten

Schwachstellendatenbank

- Europäische Schwachstellendatenbank, Art. 17 Abs. 5 CRA
- Gemeldete Schwachstellen nach Art. 14 Abs. 1 CRA und Art. 15 Abs. 1 CRA
- Einrichtung nach Art. 12 Abs. 2 NIS-2-RL
- Informationen zu Schwachstellen betroffener Produkte
- Sammlung von Informationen über Möglichkeiten zu Gegenmaßnahmen und Behebung der Schwachstellen unter Verantwortung der ENISA

Meldeplattform

- Meldeplattform für Meldungen nach Art. 14 Abs. 1 und 3 CRA sowie nach Art. 15 Abs. 1 und 2 CRA
- ENISA ist für Einrichtung und den Betrieb verantwortlich
- Art. 16 Abs. 1 S. 1 und 2 CRA
- Vgl. auch softwarebasierte Meldewesensysteme, auch auf Seiten der Aufsicht

EU CyCLONe*

- ENISA kann EU CyCLONe Informationen übermitteln, die nach Art. 14 Abs. 1 und 3 CRA sowie Art. 15 Abs. 1 und 2 CRA gemeldet wurden, Art. 17 Abs. 1 CRA
- Verbindungsorganisation gem. Art. 16 NIS-2-RL eingerichtet
- Bei massiven Cybersicherheitsvorfällen angezeigt
- Koordiniertes Vorgehen soll ermöglicht werden
- Technische Analysen des CSRIT-Netzwerkes kann ENISA in Erwägung ziehen
- Information der Öffentlichkeit über schwerwiegenden Sicherheitsvorfall möglich, Art. 17 Abs. 2 CRA

*European cyber crisis liaison organisation network; Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen; Bild: pixabay.com

Vergleich des Meldesystems des CRA mit NIS-2-RL

- Abgestuftes Meldesystem
- Dreistufiges Meldepflichtsystem bei der Meldung eines erheblichen Sicherheitsvorfalles
- Angabe ob krimineller Hintergrund vorliegen könnte oder grenzübergreifende Auswirkungen
- Abschlussbericht ein Monat nach Kenntniserlangung des Sicherheitsvorfalles (CRA: 14 Tage)

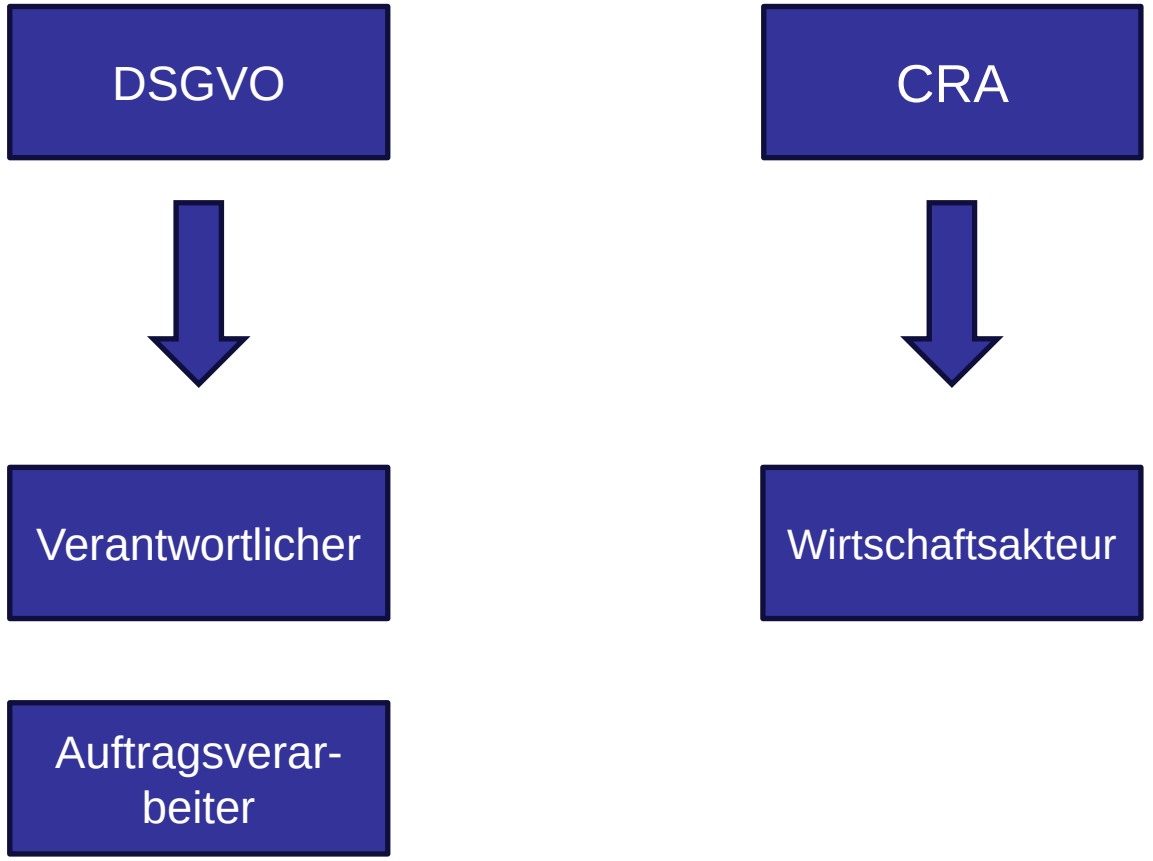
Vergleich des Meldesystems des CRA mit der DSGVO

- Meldung von Datenpannen gem. Art. 33 Abs. 1 S. 1 DSGVO
- Unverzüglich, möglichst innerhalb von 72 h
- Beschreibung und Art der verletzten personenbezogenen Daten
- Beschreibung der Folgen und der Maßnahmen, die ergriffen wurden
- Adressaten der Meldung

- DSGVO: Verantwortlicher (Art. 4 Nr. 7 DSGVO),
- Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO)
- CRA: Wirtschaftsakteure, Art. 3 Nr. 12 CRA wie z. B. Hersteller

- Bußgeldpraxis **DSGVO:** Übertragbarkeit auf den **CRA**? offen, da noch nicht geklärt ist, welche Behörde zuständig sein wird.

Adressaten der Meldungen



Fazit und Ausblick

- Neue spezifische Melde- und Informationspflichten durch den CRA
- Hinzutreten zu bereits bekannten Meldepflichten aus dem IT-Sicherheitsrecht, z. B. aus der NIS-2-RL
- Neben der Update-Pflicht und Dokumentationspflicht ergänzende Instrumente des CRA und damit des Cybersicherheitsrechtes, um PmdE cybersicherer zu machen.
- Meldepflichten sorgen für mehr Transparenz
- Komplexität der Meldeverfahren steigt: Meldungen u. U. an mehrere Behörden erforderlich
- Einheitliche Meldeplattform, die es noch gilt zu etablieren, soll Überblick verschaffen über relevante Meldungen und diese in hoher Qualität und zeitgerecht abzugeben
- Hersteller von PmdE müssen entsprechende Meldeprozesse etablieren und diese zeitnah umzusetzen.
- Anlaufstellen für Meldepflichten auf nationaler Ebene sinnvoll vgl. ErwGr. 73 S. 1 CRA „Hilfestellung“ – „Empfehlung“ der Einrichtung von zentralen Anlaufstellen – ist zu begrüßen

Bild rechts, Quelle: pixabay.com

Vielen Dank!

Dipl.-Jur. Alexander Erdelt, LL.M.

Mainova AG

a.erdelt@mainova.de

www.mainova.de