SerNet

# CRA

# Cyber Resilience Act

Leander Sange, Dr. Johannes Loxen

SerNet GmbH, Göttingen – Berlin – San Francisco

# Übersicht

SerNet

- Einleitung
- Abgrenzung NIS2-Richtlinie
- CE-Kennzeichnung
- Produkte mit digitalen Elementen
- Unterstützungszeitraum
- Schritte zur Konformität
- Pflichten der Hersteller
- Sanktionen, Durchsetzung und Marktüberwachung
- Zeithorizont

# Einleitung

SerNet

- Der CRA stellt ein Mindestmaß an technischen und organisatorischen Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen
  → Produkte mit digitalen Elementen folgen den CE-Nachweisprozessen
- Produkte mit digitalen Elementen sind direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden und werden zudem an Kunden geliefert, z.B. „verinice.onprem“
- Zielgruppe: Hersteller, Importeure und Händler
- Der Hersteller garantiert die Cybersicherheit seiner Produkte über den gesamten Produktlebenszyklus und steht dafür in der Verantwortung
- Der Hersteller integriert die Cybersicherheitsanforderungen in die Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produktes mit digitalen Elementen

**Ziele der Verordnung**

- Erhöhung der Cybersicherheit
- Einheitlicher Rechtsrahmen
- Verbraucherschutz erhöhen
- Aktuelle Verordnungen ergänzen/vereinheitlichen

# Abgrenzung zur NIS2-Richtlinie

SerNet

**NIS2:**

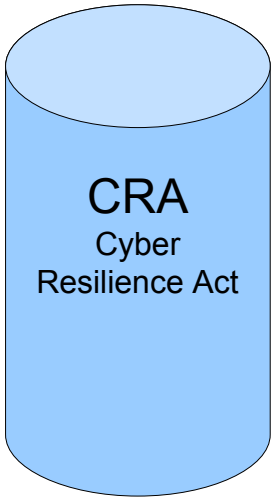
- Behandelt die Netzwerk- und Informationssicherheit innerhalb betroffener Unternehmen
- Betroffen sind mittlere und große Unternehmen aus definierten Branchen
- Ziele sind die Verbesserung der Cybersicherheit in kritischen Sektoren, Krisenreaktionsfähigkeit und Business Continuity
- SerNet ist betroffen
  → verinice.cloud

**Gemeinsamkeiten:**

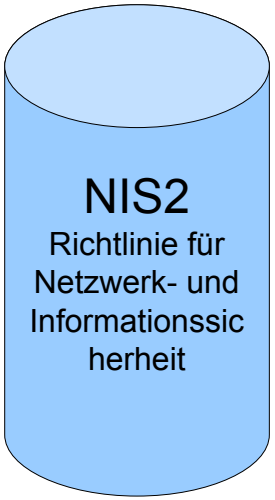
- Erhöhung der Cybersicherheit in der europäischen Union
- Festlegen von Cybersicherheitsanforderungen
- Einführung von Meldepflichten bei schwerwiegenden Sicherheitsvorfällen
- Einführung von Risikomanagementmaßnahmen
- Geldbußen/Sanktionen bei Nichteinhaltung

# Säulen zur Stärkung der Cybersicherheit in der europäischen Union

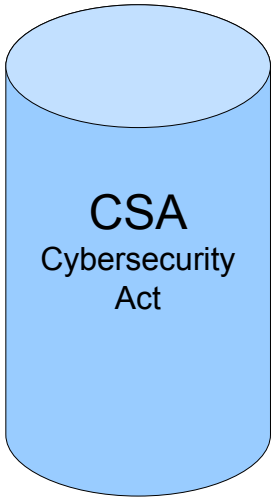
SerNet




Cybersicherheit von Produkten mit digitalen Elementen




Cybersicherheit in kritischer Infrastruktur und definierten Sektoren




Rahmenregelung für Cybersicherheits-Zertifizierungen

(CRA und NIS2 relevant)

# Was ist die CE-Kennzeichnung?[1]

CE[2]

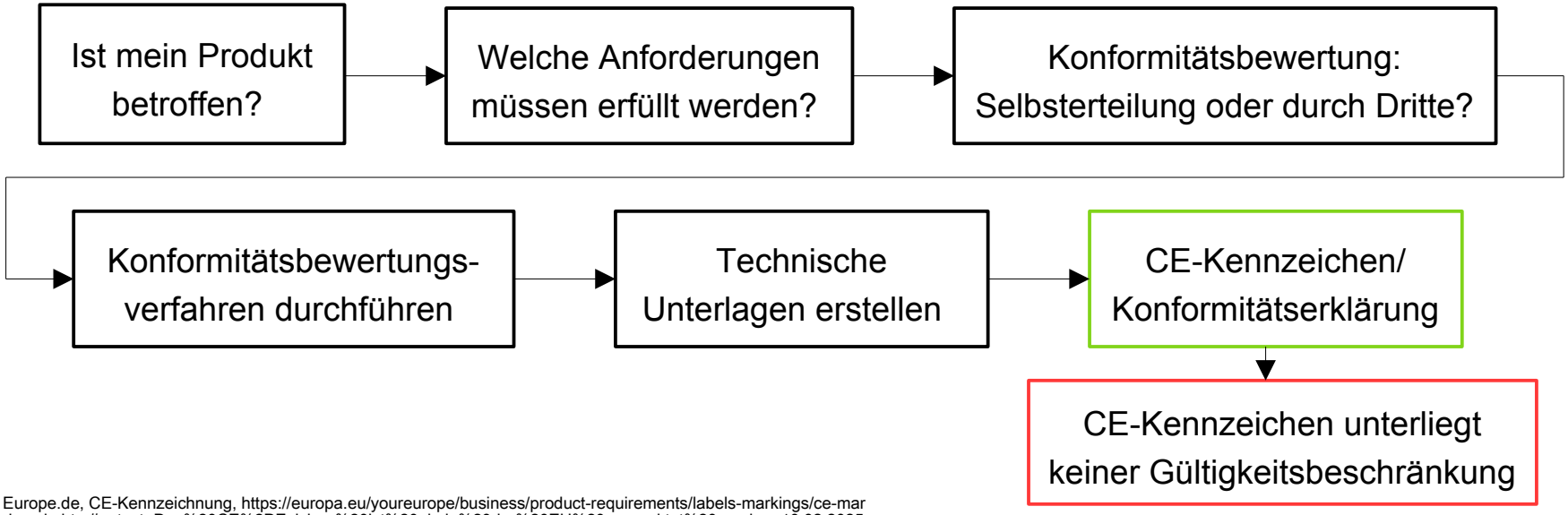
SerNet

- „Das CE-Kennzeichen ist ein Hinweis, dass ein Produkt vom Hersteller geprüft wurde und das es alle EU-weiten Anforderungen an Sicherheit, Gesundheitsschutz und Umweltschutz erfüllt.“

- Die CE-Kennzeichnung gilt für bestimmte Produkte
  → Maschinen, elektrische Betriebsmittel, Spielzeug

- Vermarktung auf dem EU-Markt nur mit CE-Kennzeichen zulässig

Verfahren der Konformitätserteilung:




[1] Your Europe.de, CE-Kennzeichnung, https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_de.htm#:~:text=Das%20CE%2DZeichen%20ist%20ein,in%20der%20EU%20vermarktet%20werden.,10.02.2025

[2] Deutsche Prüfservice GmbH, CE-Kennzeichen, https://deutsche-pruefservice.de/ce-konformitaetserklaerung-und-ce-siegel-die-7-wichtigsten-fragen-und-antworten#, 10.02.2025

# Erweiterung der CE-Kennzeichnung -was ist neu?

SerNet

- Die CE-Kennzeichnung wird auf **Produkte mit digitalen Elementen** erweitert
- Produkte mit digitalen Elementen müssen die grundlegenden Anforderungen an die **Cybersicherheit** erfüllen
- Der Hersteller unterstützt sein Produkt während des Produktlebenszyklus
  → z.B. Sicherheitsupdates
- Das CE-Kennzeichen wird gut sichtbar, leserlich und dauerhaft auf dem Produkt angebracht
  Falls direkte Kennzeichnung auf Produkt nicht möglich:
  → Verpackung und beigelegte Konformitätserklärung
  → bei Software in die Konformitätserklärung oder auf die begleitende Website

# Produkte mit digitalen Elementen

SerNet

Welche Anforderungen muss ein Produkt mit digitalen Elementen erfüllen?
→ Anhang I (Teil I + II) CRA

Anforderungen an die Cybersicherheit:

- keine **bekannten** **ausnutzbaren** Schwachstellen
- geeignete Kontrollmechanismen zum Schutz vor Zugriff durch Unbefugte
- Vertraulichkeit gespeicherter Daten schützen
- Verarbeitung personenbezogener Daten auf ein erforderliches Maß beschränken
- Möglichkeit bieten, Daten dauerhaft und einfach zu löschen

Anforderungen an die Behandlung von Schwachstellen:

- Schwachstellen ermitteln und dokumentieren
- Schwachstellen behandeln und beheben
- Sicherheit des Produkts regelmäßig testen und überprüfen
- Kontaktadresse für Schwachstellen-Meldungen zur Verfügung stellen

# Produkte mit digitalen Elementen -Kategorisierung

SerNet

- Produkte mit digitalen Elementen werden nach ihrem jeweiligen Cybersicherheitsrisiko unterschieden
- Die Unterscheidung beeinflusst die Cybersicherheitsanforderungen und das Konformitätsbewertungsverfahren

| Produkte mit digitalen Elementen | Wichtige Produkte mit digitalen Elementen → Klasse I und II (Anhang III) | Kritische Produkte mit digitalen Elementen (Anhang IV) |
|---|---|---|
| Beispiele: Vernetzter Kühlschrank, verinice.onprem | Beispiele Klasse I: Betriebssysteme, SAMBA+ Beispiele Klasse II: Firewall, IPS „Intrusion-Prevention-Systeme“ | Beispiele: Smart-Meter, Chipkartensysteme, Ausweis-App |

# Unterstützungszeitraum

SerNet

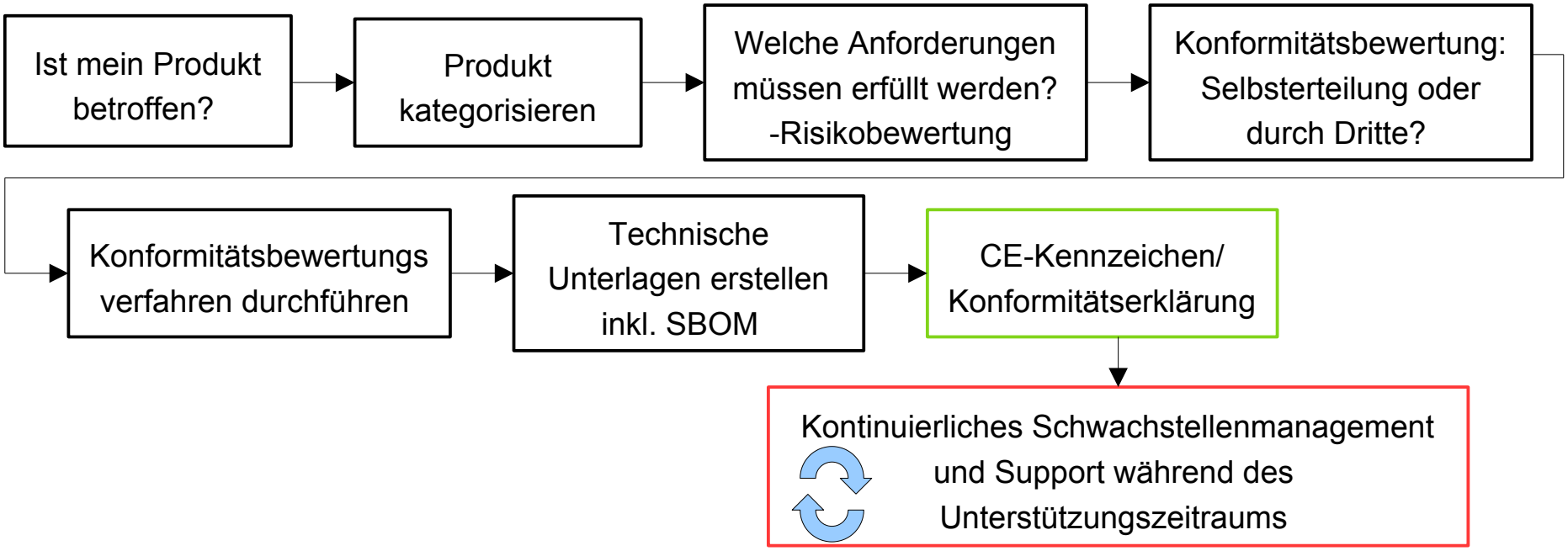
- Gewährleistung der Cybersicherheit eines Produktes m.d.E. über einen bestimmten Zeitraum
- Gibt die voraussichtliche Nutzungsdauer des Produktes wieder
- Mindestens fünf Jahre
  → oder voraussichtliche Nutzungsdauer
- Behandlung und Überwachung von Schwachstellen, sowie der Bereitstellung von Sicherheitsupdates
- Angabe der Dauer des Unterstützungszeitraums in:
  → technischer Dokumentation
  → Benutzerhandbuch/Verpackung
- Der Hersteller teilt das Ende des Unterstützungszeitraums seinen Nutzern/Kunden mit

# Schritte zur Konformität

SerNet

- Die Gewährleistung der Konformität ist kein einmaliger Vorgang. Sie ist ein laufender Prozess und wiederholt sich über den gesamten Unterstützungszeitraum
- Mit der Konformitätserklärung bestätigt der Hersteller die Erfüllung der Cybersicherheitsanforderungen und übernimmt die Verantwortung für die Cybersicherheit

Ablauf Konformitätserteilung:



# Produkte mit digitalen Elementen

SerNet

Unterschiede im Konformitätsbewertungsverfahren nach Produktkategorie:

| Produkte mit digitalen Elementen | Wichtige Produkte mit digitalen Elementen | Kritische Produkte mit digitalen Elementen |
|---|---|---|
| Konformitätsbewertung durch den Hersteller nach eigenem Verfahren/ Selbstprüfung | Klasse 1: Konformitätsbewertung eigenständig nach Normvorgabe oder durch notifizierte Stelle<br><br>Klasse 2: Konformitätsbewertung durch notifizierte Stelle | Konformitätsbewertung durch notifizierte Stelle |

# Pflichten der Hersteller

SerNet

Die Aufgaben der Hersteller werden unterschieden in:

Interne Aufgaben:

- Cybersicherheitsanforderungen in die Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase eines Produktes einbeziehen
  Beispiele:
  → Verschlüsselung gespeicherter Daten
  → Verbot schwacher Passwörter
- Cybersicherheitsrisiken bewerten und dokumentieren
  → Risikoanalyse durchführen
- Konformitätsbewertungsverfahren durchführen
- Technische Dokumentation erstellen
  → Risiken aufführen
  → SBOM erstellen
- CE-Kennzeichen anbringen
- Schwachstellenmanagement betreiben
  → Meldungen über einheitliche Meldeplattform
- Meldepflichten beachten

Externe Aufgaben:

- mit Marktüberwachungsbehörden zusammenarbeiten

Kundenbezug:

- Nutzer-Anleitung bereitstellen
- Unterstützungszeitraum festlegen und kommunizieren
- Konformitätserklärung ausstellen und unterzeichnen
- Sicherheitsupdates bereitstellen

# Meldepflichten der Hersteller

SerNet

Der Hersteller ist verpflichtet, jede aktiv ausgenutzte Schwachstelle, oder schwerwiegenden Sicherheitsvorfall einem als Koordinator benannten CSIRT und der ENISA über eine Meldeplattform zu melden

Aktiv ausgenutzte Schwachstelle:

Timeline:

- Innerhalb von 24 Stunden
  → Frühwarnung
- Innerhalb von 72 Stunden Meldung abgeben
  → Informationen über das betreffende Produkt
  → Art der Ausnutzung
  → ergriffene Korrektur und Risikominderungsmaßnahmen
  → Korrektur- und Abhilfemaßnahme für die Nutzer
- Innerhalb von 14 Tagen, nachdem eine Korrektur- oder Risikominderungsmaßnahme zur Verfügung steht
  → Abschlussbericht

Schwerwiegender Sicherheitsvorfall:

Timeline:

- Innerhalb von 24 Stunden
  → Frühwarnung
- Innerhalb von 72 Stunden Meldung abgeben
  → Informationen über die Art des Vorfalls
  → Bewertung des Sicherheitsvorfalls
  → ergriffene Korrektur und Risikominderungsmaßnahmen
  → Korrektur- und Abhilfemaßnahme die Nutzer ergreifen können
- Innerhalb von eines Monats, nach der Übermittlung der Meldung zum Sicherheitsvorfall
  → Abschlussbericht

# Sanktionen, Durchsetzung und Marktüberwachung

SerNet

Mögliche Geldbußen bei Verstößen:

Geldbußen bis 15 Mio. Euro oder bei Unternehmen bis 2,5% des Jahresumsatzes

- Nichteinhaltung der grundlegenden Cybersicherheitsanforderungen
- Verstoß gegen die Pflichten der Hersteller
- Verstoß gegen Meldepflichten

Geldbußen bis 10 Mio. Euro oder bei Unternehmen bis 2,0% des Jahresumsatzes
Verstöße gegen:

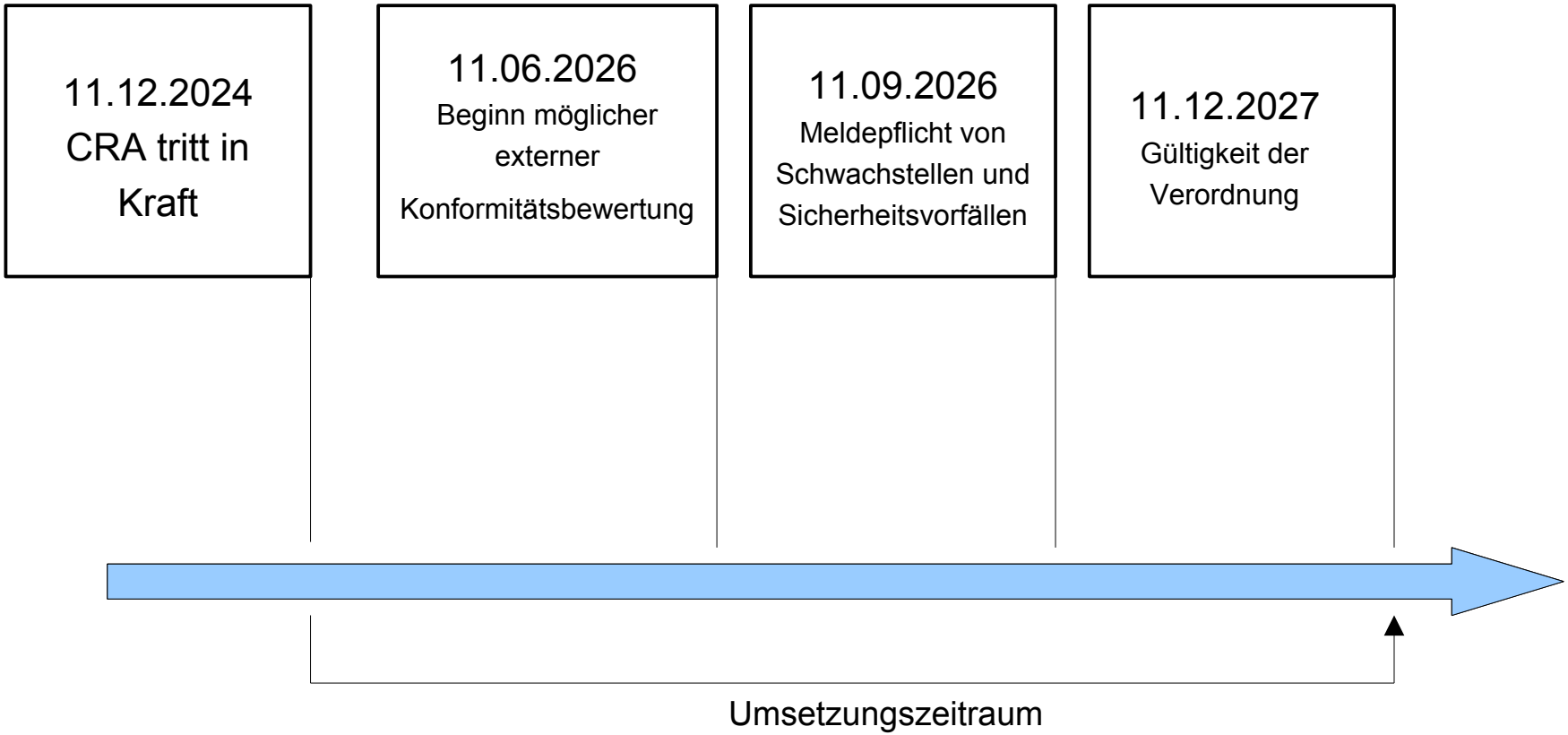
- Pflichten der Konformitätserklärung
- CE-Kennzeichnung
- technische Dokumentation
- Konformitätsbewertungsverfahren
- Zugang zu Daten und Dokumentationen für Marktüberwachungsbehörden

Geldbußen bis 5 Mio. Euro oder bei Unternehmen bis 1,0% des Jahresumsatzes

- Falsche, irreführende oder unvollständige Angaben gegenüber Marktüberwachungsbehörden und notifizierten Stellen

# Zeithorizont

SerNet



SerNet

# Vielen Dank für Eure Aufmerksamkeit!

Quelle:

VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 23. Oktober 2024
über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

# Kontakt

SerNet


## Dr. Johannes Loxen, jl@sernet.de

| | |
|---|---|
| **SerNet GmbH** | **SerNet, Inc.** |
| **Bahnhofsallee 1b** | **101 Montgomery St, #1900** |
| **37081 Göttingen** | **San Francisco CA 94104** |
| **tel +49 (551) 370000-0** | **+1 (415) 248-7818** |
| **http://www.sernet.de** | **http://www.sernet.com** |
| **kontakt@sernet.de** | **contact@sernet.com** |


© 2024, SerNet GmbH