Webinar

IHK Spezial

Cyber Resilience Act

IHK Schwaben

Format	Thema
Webinar 16.10.2024	LiveHacking: Angriff der Maschinen - Künstliche Intelligenz verleiht Cyberkriminellen „Superkräfte“
Webinar: 17.10.2024,	Die neuen gesetzlichen Vorgaben im IT-Sicherheitsrecht - NIS-2-Richtlinie und NIS2UmsuCG
Webinar: 22.10.2024	Cybersicherheit in der Gesundheits- und Sozialbranche
Webinar: 28.10.2024	hack me if you can
Webinar: 04.11.2024	Cyber Resilience Act verstehen und umsetzen: Gesetzliche Vorgaben und praktische Handlungsempfehlungen
Vor Ort: 07.11.2024	Gipfel der BIHK-Reihe zur IT-Sicherheit in Weilheim
Webinar: 12.11.2024	Die ISO 27001 als Asset für Ihr Unternehmen
Webinar: 14.11.2024	Aktueller Handlungsbedarf bei der E-Mail-Sicherheit
Webinar: 18.11.2024	Chancen & Risiken von KI-Sprachmodellen - Einführung in In-Context Learning & Prompt Injection
Webinar: 27.11.2024	NIS2: Was kommt auf die Unternehmen zu?
Vor Ort: 02.12.2024	Abschluss der BIHK-Reihe zur IT-Sicherheit in Ingolstadt

Warum braucht es den Cyber Resiliance Act?

Steigende Zahl von Cyberangriffen

Der Gesamtschaden beträgt 178,6 Milliarden Euro

Zwei Drittel der Unternehmen sehen sich durch Cyberangriffe in ihrer Existenz bedroht

Fehlende klare Standards zur Gewährleistung der Cybersicherheit

Notwendigkeit einer stärkeren gesetzlichen Grundlage, um Cybersicherheit verpflichtend zu machen

Quelle: Bitkom Research, 2024

Gesetzliche Vorgaben und praktische Handlungsempfehlungen

- Einführung in den Cyber Resilience Act (CRA)
- Welche Unternehmen sind betroffen?
- Welche Pflichten lassen sich daraus ab?
- Wie kann mein Unternehmen diese Pflichten praktisch umsetzen?

Julian Modi
Fachanwalt für IT-Recht
Sonntag & Partner

Prof. Dr.-Ing. Dominik Merli
Professor für IT-Sicherheit & Leiter Institut für innovative Sicherheit
Technische Hochschule Augsburg

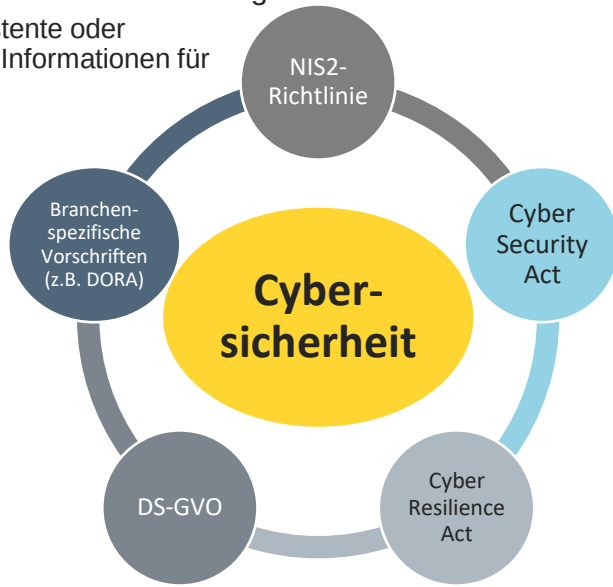
Julian M. Modi, LL.M.

- Partner | Rechtsanwalt
  Master of Laws (LL.M.)
  Fachanwalt für IT-Recht
  Fachanwalt für Urheber- und Medienrecht
- Sonntag & Partner Partnerschaftsgesellschaft mbB, Schertlinstr.23, 86159 Augsburg

- Tätigkeitsschwerpunkte
  - Gewerblicher Rechtsschutz/Geistiges Eigentum
  - IT-Recht
- Lehrbeauftragter der Hochschule Augsburg sowie der Universität Augsburg
- Dozent der IHK Ulm zum Datenschutzrecht und Online-Marketing

Cybersicherheit-Regularien

- Steigende Angriffe auf die Cybersicherheit machen gesetzgeberisches Handeln notwendig!
  - Hintergrund der Cyberangriffe sind unter anderem Schwachstellen, inkonsistente oder unzureichende Bereitstellung von Sicherheitsupdates sowie unzureichende Informationen für Benutzer
- Vielzahl von europäischen Sicherheitsregelungen
  - Digital Services Act
  - Digital Markets Act
  - Data Act
  - AI Act
  - Data Governance Act
  - ePrivacy-Verordnung
  - NIS-2-Richtlinie
  - Cyber Security Act
  - DSGVO
- Regelungen sind häufig sektorspezifisch und führen zu einer komplexen rechtlichen Landschaft



Einführung in den Cyber Resilience Act

- Seit Ende 2022 im Europäischen Parlament behandelt
- Verabschiedung des CRA vom Europäischen Parlament am 12.03.2024 und am 10.10.2024 im Rat der Europäischen Union
- CRA stellt eine europäische Verordnung dar und entfaltet daher **unmittelbare Geltung**
  - nationaler Umsetzungsrechtsakt nicht erforderlich

Was regelt der CRA?

- Verordnung für Produkte mit digitalen Elementen, welche horizontale Cybersicherheitsanforderungen setzt
- Festlegung europaweit verbindlicher Anforderungen an die IT-Sicherheit
  - Weniger Schwachstellen bei Produkte, die auf den EU-Markt gebracht warden
  - Verantwortlichkeit von Herstellern für die IT-Sicherheit während des Lebenszyklusses des Produkts
  - Transparenz über die Sicherheit von Hard- und Softwareprodukten
  - Höhere Sicherheit von Nutzern
  - Dadurch Harmonisierung und Verbesserung des Sicherheitsniveaus in den Mitgliedstaaten
- Verpflichtende Cybersecurity-Risk-Assessments für Hersteller und Distributeure
- Komplementäre Regelungen zur NIS2-Richtlinie sowie dem Cyber-Security-Act

CRA-Anwendungsbereich

Persönlicher Anwendungsbereich

- Alle Unternehmen, die Produkte mit digitalen Elementen herstellen oder anbieten (z. B. Hersteller, Importeure, Händler)

Örtlicher Anwendungsbereich

- Alle innerhalb des Unionsmarkts in den Verkehr gebrachte Produkte

Sachlicher Anwendungsbereich

- Ausgangspunkt sind „Produkte mit digitalen Elementen (PmdE)“
  - beabsichtigte und vernünftigerweise vorhersehbare Nutzung hat eine direkte oder indirekte Datenverbindung zu einem anderen Gerät oder Netzwerk
  - auch Software- und Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen („non-embedded“)
  - Software- oder Hardwareprodukte sowie mit ihnen verbundene Cloudlösungen, aber auch separat in Verkehr gebrachte Software- und Hardwarekomponenten.

CRA-Anwendungsbereich

Unterteilung von PmdE anhand des Risikograds:

- *Einfache* PmdE
  - Auffangtatbestand
- *Wichtige* PmdE (Anhang III)
  - *für die Cybersicherheit anderer Produkte, Netze oder Dienste von entscheidender Bedeutung oder*
  - *Wichtige Funktion, bei deren Ausfall ein erhebliches Risiko nachteiliger Auswirkungen besteht*
- *Kritische* PmdE (Anhang IV)

Standartprodukte
Standartkategorie
Selbstbewertung
Kriterien: entfällt

Wichtige Produkte	
Klasse I	**Klasse II**
Standartbewertung oder Bewertung durch Dritte	• Bewertung durch Dritte
Kriterien: • Funktionalität • Beabsichtigte Verwendung • Andere Kriterien (z.B. Ausmaß der Auswirkungen)	

CRA-Anwendungsbereich

Wichtige PmdE gem. Anhang III des CRA-E
Klasse I (Auszug)
• Identitätsmanagementsysteme • Passwort-Manager • Antivirensoftware • Netzverwaltungssysteme • ***Infrastruktur für öffentliche Schlüssel und Software für die Ausstellung digitaler Zertifikate*** • Physische ***und virtuelle*** Netzwerkschnittstellen • Betriebssysteme • Mikroprozessoren mit sicherheitsrelevanten Funktionalitäten
Klasse II
• Hypervisoren und Container-Laufzeitsysteme, die die virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen • Firewalls, Systeme zur Erkennung und Verhinderung von Eindringlingen • ***Manipulationssichere*** Mikroprozessoren • ***Manipulationssichere Mikrocontroller***

Pflichtenkatalog für betroffene Unternehmen

Der CRA legt den Betroffenen Unternehmen einen umfangreichen Pflichtenkatalog auf, der die Cybersicherheit eines Produkts über seinen kompletten Lebenszyklus gewährleisten soll

- **Security by Design:** einen sicheren Produkt- und Entwicklungslebenszyklus, der Cybersicherheit im gesamten Lebenszyklus berücksichtigt
- kontinuierliches Schwachstellen-Management: **Erstellung einer umfangreichen Risikoanalyse**
  - Dokumentation von Cybersicherheitsrisiken
  - Meldung aktiv ausgenutzter Schwachstellen und Zwischenfälle
- sicheres Software-Update-Management
  - Dauerhafter Support
  - Sicherheitsaktualisierungen und Patches für die voraussichtliche Nutzungsdauer des Produkts eine sicherheitsbezogene Dokumentation mit klaren und verständlichen Anweisungen
- Vorgaben zur Konformitätsbewertung bzw. der Produktkonformität und der Risikobewertung

Sanktionsregime

- Mitgliedstaaten legen die Sanktionen fest, die bei einem Verstoß gegen diese Verordnung zu verhängen sind
- Möglichkeit der Verhängung von Bußgeldern
  - Von bis zu 5 000 000 EUR bis zu 15 000 000 EUR oder von 1% bis zu 2,5 % des weltweiten Jahresumsatzes eines Unternehmens
  - Entscheidend ist, welcher Betrag höher ist

Vielen Dank für Ihre Aufmerksamkeit!

www.sonntag-partner.de

AUGSBURG	+49 821 570 58-0
MÜNCHEN	+49 89 255 44 34-0
ULM	+49 731 379 58-0
NÜRNBERG	+49 911 815 11-0

Sonntag & Partner
Partnerschaftsgesellschaft mbB
Wirtschaftsprüfer, Steuerberater, Rechtsanwälte

SONNTAG
Wirtschaftsprüfung. Steuer. Recht.

PROF. DR. DOMINIK MERLI

Professor für IT-Sicherheit @ THA

- **Praktiker**
  - Praxiserfahrung @ Fraunhofer und Siemens CT
  - Seit 2017 mehr als 50 Kooperationsprojekte mit Unternehmen
- **Forscher**
  - Institutsleiter THA_innos und Forschungsteam aus 6 Doktoranden
- **Autor**
  - Buch „Engineering Secure Devices“ (No Starch Press, Juni 2024)

VERANTWORTUNG

Wer hat den Product-Security-Hut auf?

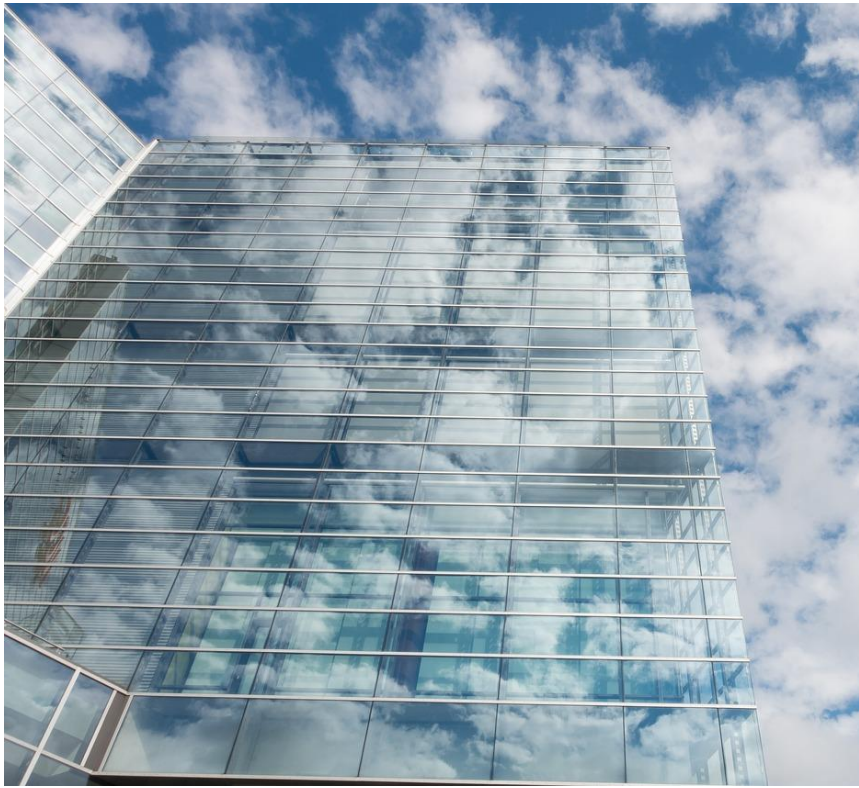
- **Management-Commitment**
  - Finanzielle und personelle Ressourcen
- **Ansprechpartner für Kundinnen und Kunden**
  - Typischerweise viel Gesprächsbedarf
- **Koordination unternehmensweiter Prozesse**
  - Compliance, Schwachstellenmanagement, etc.

BEDROHUNGEN UND RISIKEN

Was wäre wenn … ?

- **Bedrohungsanalyse**
  - Systemverständnis aus Cybersicherheitsperspektive
  - Schutzbedarf, Angreifermodell, typische Angriffe, etc.
- **Risikobestimmung**
  - Eintrittswahrscheinlichkeit und Auswirkungen
- **Priorisierung**
  - Risikobasierte Entscheidung für Schutzmaßnahmen

TRANSPARENZ



Wissen Sie was alles in Ihrem Produkt steckt?

- **Software-Bill-of-Materials (SBOM)**
  - Einheitliche „Liste“ für Softwarekomponenten
- **Third-Party Komponenten**
  - Anforderungen an externe Komponenten? Vertrauen?
- **Chance: Ausmisten!**
  - Transparenz kann viele positive Effekte haben!

SCHWACHSTELLENMANAGEMENT

Wie gehen Sie mit Sicherheitslücken um?

- **Klare Kontaktmöglichkeiten**
  - Website, E-Mail-Adresse, Informationen zum Prozess
- **Monitoring von Third-Party Komponenten**
  - Neue Schwachstellen in der Supply Chain?
- **Prozess und Ressourcen**
  - Bewertung, Entwicklung, Kommunikation, Verteilung

FAZIT

Erste, pragmatische Schritte in Richtung CRA

- Klären Sie die Verantwortlichkeiten.
- Analysieren Sie die Cyber Risiken Ihrer Produkte.
- Schaffen Sie Transparenz bzgl. Produktkomponenten.
- Etablieren Sie ein Schwachstellenmanagement.

Unsere nächsten Webinare im Themenfeld Digitalisierung und KI

Der Cyber Resilience Act in der industriellen Praxis

14.11.2024 | 10.00 bis 11.00 Uhr

- Warum benötigen wir cybersichere Produkte?
- Der CRA im Überblick
- Welche Pflichten lassen sich aus dem CRA für mein Industrieunternehmen ableiten?
- Wie können Hersteller diese Pflichten praktisch umsetzen?

Bernd Gehring
Area Manager Industrial Security
ditis Systeme, Heidenheim

Chancen & Risiken von KI-Sprachmodellen - Einführung in In-Context Learning & Prompt Injection

18.11.2024 | 14.00 bis 15.00 Uhr

- Einführung in das Thema KI-Sprachmodelle
- Welche Chancen bietet das In-Context Learning von KI-Sprachmodellen?
- Welche Risiken birgt Prompt Injection?
- Welche Handlungsempfehlungen gibt es, um die Chancen von KI-Sprachmodellen zu nutzen und sich vor Risiken zu schützen?

Michael Lauter
Team Lead DevOps & AI
soffico GmbH

Kommen Sie bei Fragen gerne auf uns zu!

Dr. Vanessa Steinherr

Projektmanagerin Digitale Innovation
und Künstliche Intelligenz

vanessa.steinherr@schwaben.ihk.de

0821/3162-230

04.11.2024

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter
ihk.de/schwaben/ihkspezial

IHK Schwaben