pribizz Consulting

Cyber Resilience Act (CRA)

Über mich

pribizz consulting GmbH

Ing. Mag. Jürgen Hutsteiner, CIPP/E

Datenschutz- und Informationssicherheitsexperte

Künstliche Intelligenz, Prozessoptimierung und strategische Beratung

Über 8 Jahre Erfahrung in den Bereichen Datenschutz und Informationssicherheit

ISO 27001 und ISO 9001 Auditor

Mitglied des Führungsteams der IT-Security Expertsgroup Oberösterreich

EU-Richtlinien und Verordnungen

DSGVO

DORA

KI-Verordnung

NIS 2

Cybersecurity Act

Cyber Resilience Act (CRA)

Smarte Geräte

über 3 Millionen Apps

über 80 Apps...
befinden sich auf unserem Handy

Cybercrime

Über 90 Android-Apps betroffen: Sicherheitsforscher warnen vor Trojanern

Anbieter prominenter KI-Plattform bestätigt Cyberangriff

Tiktok bestätigt Cyberangriff auf bekannte Accounts

CYBERANGRIFF AUF TRACKER-HERSTELLER

Hacker greift Kundendaten von Tile ab

Stadt in England kann nach Cyberangriff die Lichter nicht mehr abdrehen

Cyberangriff auf Zuger Krypto-Börse Lykke: 22 Millionen Dollar gestohlen

Hacker erbeuten Daten von 560 Millionen Kunden von Ticketmaster

IT-Sicherheit BSI-Report 2023

BSI-Report 2023:

- 250.000 neue Schadprogramm-Varianten pro Tag
- 66% der Spam-Mails waren Cyberangriffe
- 84% aller betrügerischen E-Mails waren Phishing E-Mails
- 2.000+ Schwachstellen in Softwareprodukten (15% davon kritisch) durchschnittlich pro Monat (Zuwachs von 24%)

BSI = Bundesamt für Sicherheit und Informationstechnik Deutschland

Cyber Resilience Act (CRA)

Abgrenzung

DSGVO	NIS 2	DORA	CRA
EU-Verordnung	EU-Richtlinie	EU-Verordnung	EU-Verordnung
Alle Unternehmen	Unternehmen kritischer Sektoren	Finanzunternehmen, IKT-Dienstleister	Unternehmen, die Produkte mit digitalen Elementen herstellen oder vertreiben
Schutz von personenbezogenen Daten	Schutz der Netzwerk- und Informationssysteme	Schutz der digitalen Systeme des Finanzsektors	Cybersicherheit von Produkten mit digitalen Elementen
Unternehmensweite Maßnahmen	Unternehmensweite Maßnahmen	Unternehmensweite Maßnahmen	Produktspezifische Maßnahmen

Was regelt der CRA?

- Mindestanforderungen hinsichtlich Cybersicherheit in der Konzeptionierung, Entwicklung und Herstellung
- Durchführung von Risikoanalysen hinsichtlich Cybersicherheit
- Erstellung der technischen Dokumentation
- Sicherstellung der Cybersicherheit bei Komponenten von Dritten

Was regelt der CRA?

Etablierung eines umfangreichen Schwachstellenmanagements

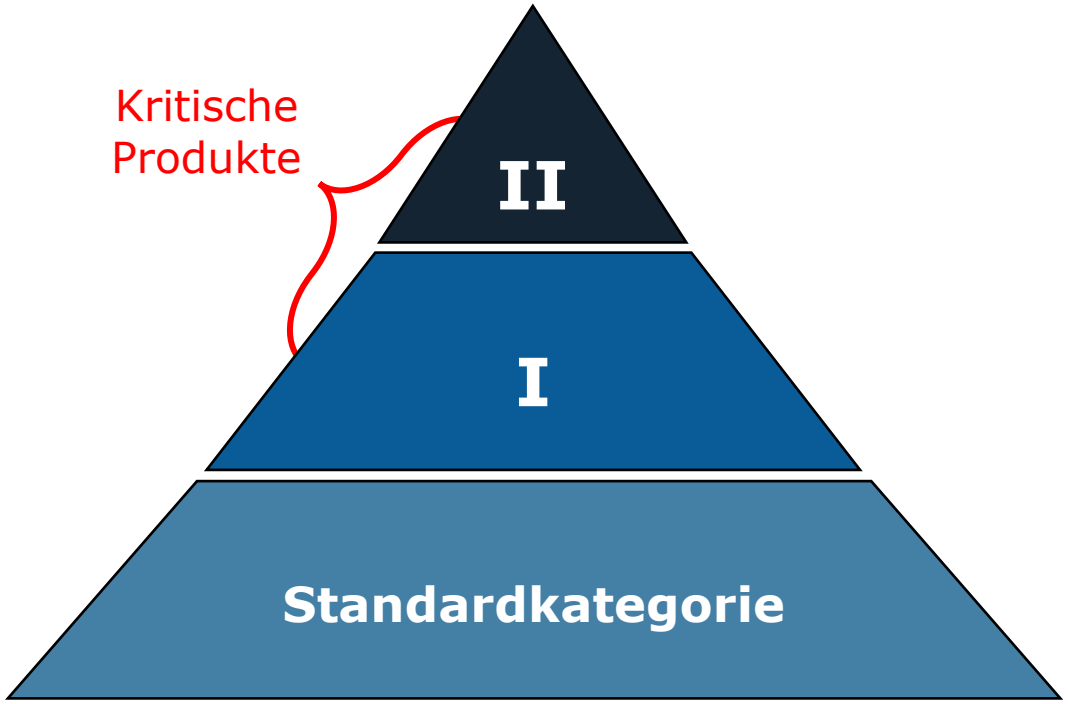
Durchführung des Konformitätsbewertungsverfahrens

Umsetzung der Transparenz- und Informationspflichten

Kennzeichnung der Produkte

Meldepflichten

Klassifikation von Produkten



Betroffene Unternehmen

Hersteller

Unternehmen, die Produkte konzipiert, entwickelt oder herstellt oder dies durch jemand anderes im eigenen Namen durchführen lassen

Einführer

Unternehmen, die Nicht-EU-Produkte innerhalb der EU in Verkehr bringen

Händler

Unternehmen in der Lieferkette, die Produkte ohne Änderung ihrer Eigenschaften bereitstellen

Sonderregeln

- Einführer und Händler unterliegen den Pflichten der Hersteller, wenn sie das Produkt unter eigenem Namen bzw. Marke verkaufen

- Einführer, Händler und sonstige Unternehmen unterliegen den Pflichten der Hersteller, wenn sie wesentliche Änderungen an einem bereits in Verkehr gebrachten Produkt vornehmen

Cybersicherheit in der Entwicklung

Anforderungen an digitale Produkte

Angemessenes Cybersicherheitsniveau ohne bekannte Schwachstellen	Aufzeichnungen, Überwachungen und Protokolle
Schutz der Integrität	Komponentenliste
Schutz der Vertraulichkeit	Standardkonfiguration und Zurücksetzbarkeit
Schutz der Verfügbarkeit	

Schwachstellenmanagement

Meldepflichten

Meldepflichten	Hersteller	Einführer	Händler
Einstellung des Betriebes: Meldung an Marktüberwachungsbehörde und falls möglich Information an die Nutzer	ja	Alternativ	Alternativ
Aktiv ausgenutzte Schwachstelle: Meldung an ENISA innerhalb 24h	ja	nein	nein
Feststellung Schwachstelle: Meldung an Hersteller	ja	ja	ja
Feststellung Schwachstelle mit erheblichem Cybersicherheitsrisiko: Meldung an Marktüberwachungsbehörde	nein	ja	ja
Sicherheitsvorfall: Meldung an ENISA innerhalb 24h und Nutzer	ja	nein	nein
Vermutung der Nichtkonformität mit erheblichem Cybersicherheitsrisiko: Meldung an Hersteller und an Marktüberwachungsbehörde	nein	ja	ja

ENISA: Agentur der Europäischen Union für Cybersicherheit
Marktüberwachungsbehörde: nationale Behörde

Bereitstellung von Informationen

1) Name, Anschrift, E-Mailadresse von Hersteller und Kontaktstelle für Meldung von Cybersicherheitslücken
2) Identifikationsnummer des Produktes und Komponentenliste
3) Informationen über Hauptfunktion, bereitgestelltes Sicherheitsumfeld und der Sicherheitseigenschaften
4) Alle bekannten und vorhersehbaren Umstände, die zu erheblichen Cybersicherheitsrisiken führen können
5) Informationen über Sicherheitsunterstützung und Sicherheitsaktualisierung
6) Maßnahmen, die notwendig sind, um eine sichere Verwendung zu gewährleisten
7) Information über die sicherheitsrelevanten Auswirkungen bei Änderungen am Produkt
8) Anleitung zur Installation von sicherheitsrelevanten Aktualisierungen
9) Anleitung zur sicheren Außerbetriebnahme und Datenlöschung

Technische Dokumentation

Allgemeine Beschreibung des Produktes

inkl. Zweckbestimmung, Softwareversionen, Fotografien und Abbildungen der Hardwarekomponenten, Informationen und Anleitungen für die Nutzer

Beschreibung der Konzeption, Entwicklung und Herstellung des Produkts und der Verfahren zur Behandlung von Schwachstellen

inkl. Zeichnungen, Systemarchitektur aller Komponenten, Komponentenliste, Konzept für die koordinierte Offenlegung von Schwachstellen, Beschreibung der gewählten technischen Lösungen für die sichere Verbreitung von Aktualisierungen und vollständiger Informationen und Spezifikationen bezüglich der Herstellungs- und Überwachungsprozesse des Produkts

Bewertung der Cybersicherheitsrisiken

Berichte über die Tests und Prüfungen

Fristen und Konsequenzen

12/23 politische Einigung

03/24 Gesetzesbeschluss

??/24 Inkrafttreten

unmittelbar innerhalb der EU anwendbar → 21 Monate, um Meldeprozesse zu etablieren → 36 Monate, um CRA vollständig zu erfüllen

Einhaltung der CRA-Anforderungen notwendig für EU-Marktzugang

Herstellerpflichten

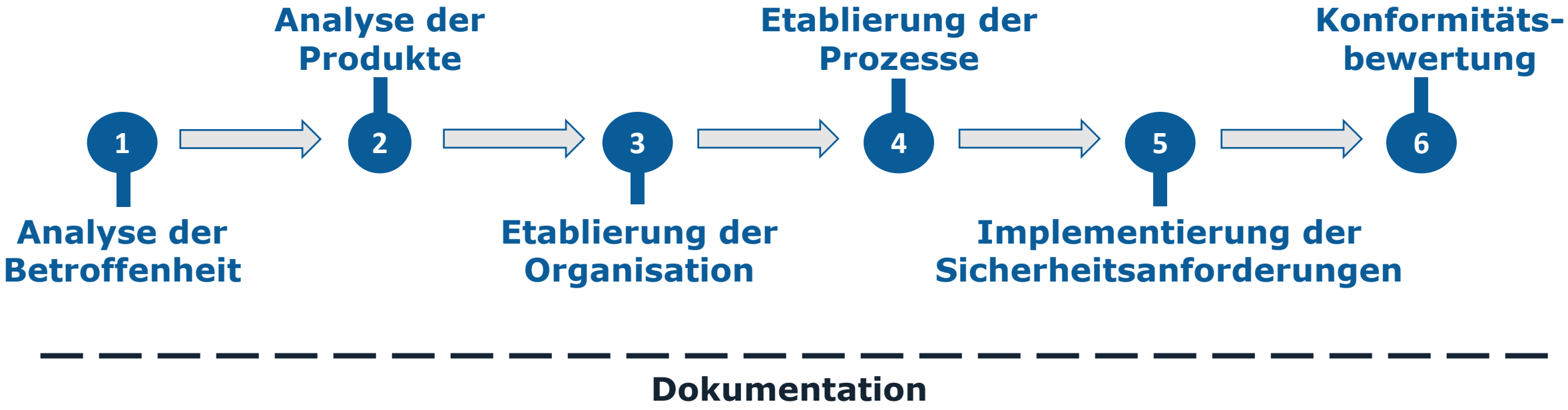
bis zu 15 Mio / 2,5% des weltweiten Jahresumsatzes

Andere Pflichten

bis zu 10 Mio / 2% des weltweiten Jahresumsatzes

Verwaltungs-strafen

Notwendige Schritte für Unternehmen



Diskussions- und Fragerunde

pribizz Consulting

Ing. Mag. Jürgen Hutsteiner, CIPP/E
Inhaber, Geschäftsführer
jh@pribizz.at
+43 676 51 66 51 8

pribizz consulting GmbH
Weberberg 13
4076 St. Marienkirchen an der Polsenz
www.pribizz.at