RICHTLINIE ZUR KOORDINIERTEN OFFENLEGUNG VON SCHWACHSTELLEN (COORDINATED VULNERABILITY DISCLOSURE POLICY)

in Ausführung der regulatorischen Anforderungen des
Cyber Resilience Act (CRA) der Europäischen Union

Präambel

In Erfüllung der regulatorischen Obliegenheiten sowie der gesetzlichen Sorgfaltspflichten gemäß den Bestimmungen des europäischen Cyber Resilience Act (CRA) konstituiert die vorliegende Richtlinie den formellen Rahmen zur geordneten Handhabung sicherheitsrelevanter Anomalien. Sie normiert das verbindliche Verfahren zur Meldung, Evaluierung und Remediation potenzieller Schwachstellen mit dem primären Schutzzweck der Aufrechterhaltung der Integrations- und Datensicherheit der Anwenderschaft.

§ 1 Sachlicher und räumlicher Anwendungsbereich

Die Dispositionen dieser Richtlinie entfalten vollumfängliche und ausnahmslose Rechtswirkung für jedwede softwarebasierten sowie softwaredefinierten Erzeugnisse. Dies umfasst subsumierend sämtliche reinen Softwareapplikationen als auch hardwaregebundene Systeme (T+A Produkte), insofern diese über integrierte Firmware- oder Softwarekomponenten verfügen und unter der administrativen oder urheberrechtlichen Verantwortlichkeit unseres Hauses entwickelt oder in den Verkehr gebracht werden.

§ 2 Form- und fristgebundene Übermittlung von Vulnerabilitätsanzeigen

Subjekte, seien es natürliche oder juristische Personen (im Folgenden: Melder), welche Kenntnis über eine sicherheitsrelevante Schwachstelle (Vulnerability) in den unter § 1 definierten Produkten erlangen, sind im Sinne der Schadensprävention angehalten, diese unverzüglich anzuzeigen. Um den formellen Anforderungen an eine prozesssichere und gerichtsfeste Dokumentation zu genügen, hat die Übermittlung der Anzeige zwingend und exklusiv über das auf der offiziellen Webpräsenz implementierte telemediale Meldeformular (E-Mail-Formular) zu erfolgen. Anderweitige Übermittlungswege begründen keinen Fristlauf und gelten als nicht formgerecht eingereicht.

§ 3 Materielle Anforderungen an die Vulnerabilitätsanzeige (Substantiierungspflicht)

Zur Gewährleistung einer sachgerechten, reproduzierbaren und prozessökonomischen Verifikation der gemeldeten Sachverhalte bedarf es der Übermittlung spezifizierter technischer Parameter. Unter Berücksichtigung der Dynamik asymmetrischer Bedrohungsszenarien wird auf eine statische Enumeration der erforderlichen Datensätze in diesem Dokument verzichtet. Stattdessen wird rechtsverbindlich auf die unter der URL **ta-hifi.de/cra** bereitgestellte Informationsmatrix verwiesen.

Die dortigen, tagesaktuell und bedarfsadjustiert gepflegten Spezifikationen gelten hiermit als integraler Bestandteil (per relationem) dieser Richtlinie.

§ 4 Internes Evaluierungs- und Mitigierungsverfahren

Der formgerechte Eingang einer jeden Anzeige initiiert ein vordefiniertes, mehrstufiges Prüfungsverfahren:

- **Klassifikation und Triage:** Initiale formelle und materielle Plausibilitätsprüfung zur Feststellung der Validität der Anzeige.
- **Interdisziplinäre Sachverhaltsaufklärung:** Tiefgehende forensische und systemische Analyse durch autorisierte Fachgremien. Hierbei ist die zwingende Partizipation der relevanten Fachabteilungen, namentlich der Entwicklung, der Produktion sowie der Fertigung, obligatorisch vorgeschrieben.
- **Remediation:** Nach positiver Verifikation der Vulnerabilität erfolgt die unverzügliche Einleitung von Maßnahmen zur Schadensabwehr (Mitigierung, Patch-Bereitstellung oder Firmware-Aktualisierung).

§ 5 Informationsaustausch und datenschutzrechtliche Bestimmungen

Die bilaterale Interaktion mit dem Melder unterliegt strikten Verhaltens- und Verschwiegenheitsmaßgaben:

- **Datenschutzrechtliche Konformität:** Die Verarbeitung jedweder personenbezogener Daten des Melders erfolgt unter strengster Wahrung der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO).
- **Grundsatz der Erforderlichkeit:** Etwaige Rückfragen seitens des Sicherheitsteams zur Sachverhaltsaufklärung oder Reproduzierbarkeit erfolgen unter Beachtung des Grundsatzes der Verhältnismäßigkeit und Bedarfsadäquanz über gesicherte und angemessene Kommunikationskanäle.

§ 6 Publizitätsbeschränkungen (Coordinated Vulnerability Disclosure)

Es gilt das unabdingbare Prinzip der koordinierten und sanktionierten Offenlegung. Dem Melder obliegt eine weitreichende Verschwiegenheitspflicht (Non-Disclosure). Es ist dem Melder untersagt, Details bezüglich der identifizierten Schwachstelle ganz oder teilweise ohne explizite, schriftlich erteilte Freigabe an Dritte oder die Öffentlichkeit zu kommunizieren. Eine Veröffentlichung darf frühestens zu jenem Zeitpunkt erfolgen, an dem der interne Analyse- und Remedian-Prozess vollumfänglich abgeschlossen ist und den betroffenen Endanwendern entsprechende Schutzmechanismen (Sicherheitsupdates) zur Verfügung stehen.

§ 7 Temporale Fristen und Modalitäten der Rückkopplung

Vorbehaltlich abweichender zwingender gesetzlicher Vorschriften gelten zur Sicherstellung der Compliance mit dem EU CRA folgende temporale Dispositionen:

- **Frist zur Erstreaktion:** Die formelle Bestätigung über den Eingang der Anzeige (Erstreaktion) erfolgt innerhalb eines Zeitfensters von maximal 30 Stunden ab Zugang der Meldung, gerechnet ausschließlich in Werktagen unter Zugrundelegung der Mitteleuropäischen Zeit (MEZ).
- **Interventions- und Meldepflichten:** Die weiterführende Untersuchung der Schwachstelle sowie die Erfüllung etwaiger Meldepflichten gegenüber staatlichen oder supranationalen Aufsichtsbehörden vollzieht sich strikt nach den gesetzlich normierten Fristen des EU CRA.
- **Substantiierte Rückmeldung (Feedback-Schleife):** In Abhängigkeit der prospektiven Schadensklasse und der systematischen Klassifizierung der Schwachstelle wird dem Melder spätestens nach Ablauf von 6 Wochen ab Eingangsbestätigung eine fundierte Stellungnahme hinsichtlich des weiteren prozeduralen Vorgehens übermittelt.