Kunnus

WHITEPAPER · EU CYBER RESILIENCE ACT

Die Meldepflicht nach Artikel 14: Was bis zum 11. September 2026 stehen muss

Aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle: in 24 Stunden gemeldet, in 72 Stunden präzisiert, mit Abschlussbericht dokumentiert. Dieses Whitepaper macht aus jeder Pflicht eine konkrete Maßnahme, mit Fristen, Prozess-Landkarte und Checkliste.

- Auf dem Stand der Auslegungspraxis vom Juli 2026

HERAUSGEBER

Kunnus · Think Ahead Technologies GmbH

Stand

Juli 2026

INHALT

In diesem Whitepaper

01	Warum jetzt	Stichtage, Bußgelder, Bestandsprodukte
02	Zwei Auslöser, zwei Meldeketten	Was meldepflichtig ist und was nicht
03	Meldepflichtig oder nicht?	Der Entscheidungsbaum
04	Die Meldefristen	24 h · 72 h · 14 Tage / 1 Monat
05	Kenntnisnahme: Wann die Uhr startet	Neu präzisiert durch die Guidance
06	Vier strittige Grenzfälle	Altprodukte, Upstream, Nutzerinfo, Open Source
07	Die Prozess-Landkarte	Sechs Phasen vom Hinweis zur Meldung
08	Ein durchgespieltes Beispiel	IoT-Gateway, Dienstag 14:32 Uhr
09	Die Vorbereitung in vier Schritten	Checkliste und häufige Fragen
A	Anhang: Arbeitshilfen	Einstufung, Rollen, Meldeinhalte, Testlauf

AUF EINEN BLICK

11.09.2026
gilt die Meldepflicht, auch für Produkte, die heute schon auf dem Markt sind

24 h / 72 h
Frühwarnung und Detailmeldung, in Kalenderstunden, auch am Wochenende

15 Mio. €
oder 2,5 % des Weltumsatzes: Bußgeldrahmen bei Verstößen gegen Artikel 14

01

WARUM JETZT

Der erste harte CRA-Stichtag

Am 11. September 2026 wird Artikel 14 der Verordnung (EU) 2024/2847, des EU Cyber Resilience Act, verbindlich. Ab diesem Tag müssen Hersteller von Produkten mit digitalen Elementen aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle an das koordinierende CSIRT ihres Mitgliedstaats und an die ENISA melden. Die übrigen Herstellerpflichten, darunter Schwachstellenbehandlung, Security-Updates und CE-Konformität, folgen erst 15 Monate später.

Der Verordnungstext lässt an drei Stellen Interpretationsspielraum, an denen sich in der Praxis entscheidet, ob eine Meldung fristgerecht rausgeht: ab wann ein Hersteller als „kenntnisnehmend" gilt, was für Bestandsprodukte und abgekündigte Produkte gilt und wie Schwachstellen in Drittkomponenten zu behandeln sind. Dieses Whitepaper beantwortet diese Fragen auf dem Stand der aktuellen Auslegungspraxis der Kommission.

DIE CRA-ROADMAP

10.12.2024
CRA tritt in Kraft

27.07.2026
Kommissions-Guidance zum CRA

11.09.2026
Meldepflicht nach Art. 14 gilt für alle Produkte im CRA-Anwendungsbereich

11.12.2027
Volle Anwendbarkeit: Schwachstellenbehandlung, Anhang I, CE-Pflichten

SANKTIONSRAHMEN

Verstöße gegen die Meldepflicht liegen in der höchsten Sanktionsstufe des CRA: bis zu **15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes**, je nachdem, welcher Betrag höher ist.

REICHWEITE

Die Meldepflicht gilt **auch für Bestandsprodukte** (vor dem 11.12.2027 in Verkehr gebracht) und, anders als die Schwachstellenbehandlung, **auch nach dem Ende des Support-Zeitraums** weiter.

02

ZWEI AUSLÖSER, ZWEI MELDEKETTEN

Was Artikel 14 verlangt

ABS. 1–2

Aktiv ausgenutzte Schwachstellen

Sie stellen fest, dass eine Schwachstelle in Ihrem Produkt von Angreifern **tatsächlich ausgenutzt wird**. Eine veröffentlichte CVE allein löst die Frist nicht aus. Erst Ihre Kenntnis von der aktiven Ausnutzung startet die Uhr.

ABS. 3–5

Schwerwiegende Sicherheitsvorfälle

Ein Vorfall, der die Fähigkeit des Produkts beeinträchtigt, **Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit** sensibler Daten und Funktionen zu schützen. Ebenso ein Vorfall, der zu **bösartigem Code** im Produkt oder Nutzersystem geführt hat oder führen kann.

> Beide Ereignisse melden Sie **gleichzeitig** an das als Koordinator benannte CSIRT Ihres Mitgliedstaats und an die ENISA, über die Single Reporting Platform der ENISA nach Artikel 16. Sie soll zum 11. September 2026 betriebsbereit sein, mit Testphase davor. Nur in Ausnahmefällen melden Sie auf dem von Ihrem CSIRT bekanntgegebenen Weg — die Frist verlängert das nicht.

Was Artikel 14 nicht verlangt

Viele Hersteller überschätzen den Umfang der Meldepflicht deutlich. Nicht meldepflichtig sind:

- ✕ **Funde aus Vulnerability-Scannern.** Eine CVE in einer Dependency ist ein Fall fürs interne Schwachstellenmanagement.
- ✕ **Hinweise von Sicherheitsforschern.** Behandeln und beheben ja, meldepflichtig erst bei festgestellter aktiver Ausnutzung.
- ✕ **Veröffentlichte CVEs ohne Ausnutzung.** Auch bei CVSS 9.8, solange keine aktive Ausnutzung Ihres Produkts bekannt ist.
- ✕ **Pentest- und Audit-Ergebnisse.** Selbst gefundene Schwachstellen bleiben ein interner Vorgang.

Ein Sonderfall verdient Aufmerksamkeit: Belegt ein Forscher-Hinweis, dass bereits etwas passiert ist, etwa eingeschleuster Schadcode oder eine kompromittierte Build-Pipeline, dann handelt es sich um einen Sicherheitsvorfall nach Abs. 5 lit. b. Der ist auch ohne festgestellte aktive Ausnutzung meldepflichtig. Prüfen Sie eingehende Hinweise deshalb immer gegen beide Auslöser.

03

DER ENTSCHEIDUNGSBAUM

Meldepflichtig oder nicht?

Hinweis geht ein – Forscher, Kunde, Behörde, Medien, eigenes Team

Unverzügliche Erstprüfung – gegen beide Auslöser, mit Zeitstempel

KEIN AUSLÖSER ERFÜLLT

Keine Meldepflicht. Als normale Schwachstelle behandeln, Entscheidung dokumentieren. Eine freiwillige Meldung nach Art. 15 bleibt möglich.

AKTIVE AUSNUTZUNG VERIFIZIERT

Meldekette Schwachstelle: 24 h Frühwarnung, 72 h Detailmeldung, Abschlussbericht 14 Tage nach verfügbarem Fix.

SCHWERER VORFALL (ABS. 5) VERIFIZIERT

Meldekette Vorfall: 24 h Frühwarnung, 72 h Detailmeldung, Abschlussbericht binnen eines Monats.

DER HÄUFIGSTE GRENZFALL

Drittkomponenten: Eine aktiv ausgenutzte Schwachstelle aus einer integrierten Komponente ist meldepflichtig, sobald sie *in Ihrem Produkt* enthalten ist. Ist die Schwachstelle in Ihrem Produkt jedoch **nicht ausnutzbar**, etwa weil der verwundbare Code nicht erreichbar ist, oder **dort nicht ausgenutzt worden**, besteht für Sie keine Meldepflicht nach Art. 14 — so ausdrücklich das Kommissions-FAQ. Dokumentieren Sie diese Bewertung, die Nachweislast liegt bei Ihnen. Bestehen bleiben die Schwachstellenbehandlung nach Anhang I Teil II, das Upstream-Reporting nach Art. 13(6) und die Option der freiwilligen Meldung nach Art. 15.

Die Meldung wächst mit der Analyse

Niemand erwartet nach 24 Stunden eine fertige Forensik. Die Frühwarnung enthält bewusst nur begrenzte Angaben, und die Meldung wird fortlaufend aktualisiert, je weiter die interne Untersuchung kommt.

Freiwillige Meldung nach Art. 15

Schwachstellen und Vorfälle unterhalb der Schwelle können Sie jederzeit freiwillig an CSIRT und ENISA melden, etwa wenn Warnungen an andere Hersteller sinnvoll erscheinen. Eine Pflicht entsteht daraus nicht.

04

DIE MELDEFRISTEN

Drei Stufen im Überblick

0 → 24 h

Frühwarnung

Produkt, Titel; bei Schwachstellen Vertriebsländer, bei Vorfällen Verdacht auf böswillige Handlung

→ 72 h

Detailmeldung

Art der Schwachstelle bzw. des Vorfalls, erste Bewertung, ergriffene Maßnahmen, Workarounds für Nutzer

Fix entwickeln

Ohne gesetzliche Frist

Verfügbarkeit der Korrektur- oder Risikominderungsmaßnahme dokumentieren, denn sie startet die letzte Frist

14 T / 1 M

Abschlussbericht

Schwachstelle: 14 Tage nach verfügbarer Maßnahme · Vorfall: 1 Monat nach der 72-h-Meldung

STUFE	AKTIV AUSGENUTZTE SCHWACHSTELLE	SCHWERWIEGENDER VORFALL
Frühwarnung	binnen 24 Stunden nach Kenntnisnahme	binnen 24 Stunden nach Kenntnisnahme
Detailmeldung	binnen 72 Stunden nach Kenntnisnahme	binnen 72 Stunden nach Kenntnisnahme
Abschlussbericht	spätestens 14 Tage, nachdem eine Korrektur- oder Risikominderungsmaßnahme verfügbar ist	binnen eines Monats nach der 72-Stunden-Meldung

Kalenderstunden, keine Bürostunden. Die 24 und 72 Stunden laufen am Wochenende und an Feiertagen weiter. Wer Freitagabend verifiziert, meldet spätestens Samstagabend. Planen Sie Ihre Vertretungsregelung entsprechend.

Zwischenbericht auf Anfrage (Abs. 6)

Das CSIRT kann jederzeit Statusaktualisierungen anfordern. Wer ab der ersten Meldung eine Fall-Timeline pflegt, beantwortet solche Anfragen per Export statt per Rekonstruktion.

Formate im Blick behalten (Abs. 9–10)

Die Kommission präzisiert Meldeformate und -verfahren per Durchführungsrechtsakt. Welche Felder je Stufe verpflichtend sind, listet das ENISA-FAQ zur Single Reporting Platform; prüfen Sie Ihre Vorlagen dagegen quartalsweise.

05

KENNTNISNAHME

Wann die Uhr wirklich startet

Alle Fristen beginnen mit Ihrer Kenntnisnahme, und das ist nicht der Moment, in dem ein Hinweis im Posteingang landet. Kenntnisnahme setzt voraus, dass Sie nach einer Erstprüfung **mit hinreichender Sicherheit** davon ausgehen können, dass eine aktive Ausnutzung vorliegt oder ein schwerwiegender Vorfall die Sicherheit des Produkts beeinträchtigt hat. Dieser Maßstab ist kein CRA-Sonderweg: Er entspricht dem Kenntnisbegriff der NIS2-Durchführungsverordnung (EU) 2024/2690 und der Praxis zur Meldung von Datenschutzverletzungen unter der DSGVO. Wer dort schon Prozesse hat, kann sie hier weiterverwenden.

Kenntnisnahme heißt: Verifizierung mit hinreichender Sicherheit, nicht Posteingang. Die Prüfzeit dazwischen zählt nicht zur Frist, muss aber prompt beginnen und dokumentiert sein.

Aufschieben lässt sich die Erstprüfung nicht. Verlangt ist, jeden verdächtigen Hinweis **unverzüglich** zu bewerten, gleich ob er von einem Kunden, einem Sicherheitsforscher, einer Behörde oder aus den Medien kommt. Wer die Verifizierung verschleppt, verschiebt die Frist nicht, sondern riskiert den Vorwurf, zu spät Kenntnis genommen zu haben. Halten Sie deshalb fest, wann der Hinweis kam, wann die Prüfung begann und wann das Ergebnis feststand.

Keine Rückwirkung, mit einer wichtigen Ausnahme. Ausnutzungen, von denen Sie bereits vor dem 11. September 2026 Kenntnis hatten, müssen nicht rückwirkend gemeldet werden. Kannten Sie aber nur die Schwachstelle und nicht ihre Ausnutzung, und tritt die aktive Ausnutzung nach dem Stichtag ein oder wird Ihnen erst dann bekannt, ist sie regulär meldepflichtig.

06

GRENZFÄLLE

Vier Fälle, die in der Praxis strittig sind

Altprodukte und Support-Ende

Die Meldepflicht gilt ab dem 11.09.2026 für **alle** Produkte im CRA-Anwendungsbereich, auch für vor dem 11.12.2027 in Verkehr gebrachte. Sie endet auch nicht mit dem Support: Anders als die Schwachstellenbehandlung läuft sie nach dem Ende des Support-Zeitraums weiter. Nur die Pflichten aus Anhang I Teil II entfallen dann.

Upstream-Reporting (Art. 13(6))

Schwachstellen in integrierten Komponenten melden Sie an deren Hersteller oder Maintainer, aber nur für die **integrierte Version** und nur für Schwachstellen der Komponente selbst, nicht der Integration. Die Pflicht entfällt, wenn der Maintainer nachweislich informiert ist (vorher CVE-Datenbanken, Advisories und Issue-Tracker prüfen, um Duplikate zu vermeiden) oder wenn es keinen Maintainer mehr gibt.

Nutzerinformation nach Abs. 8

Betroffene Nutzer sind zu informieren, aber nicht zwingend öffentlich. Details dürfen **risikobasiert auf die Betroffenen beschränkt** bleiben, gerade bei Produkten in sensiblen Umgebungen, wo öffentliche Technikdetails weitere Angriffe erleichtern würden. Nach der Behebung kann eine breitere Offenlegung angemessen sein. Gefixte Schwachstellen sind nach Anhang I Teil II Nr. 4 mit dem Update offenzulegen.

Open-Source-Stewards (Art. 24)

Wie weit Art. 14 für FOSS-Stewards gilt, hängt von der Art ihres Supports ab. Wer **IT-Infrastruktur** bereitstellt, meldet schwere Vorfälle, die diese Infrastruktur betreffen. Wer **Engineering-Ressourcen** beisteuert, meldet aktiv ausgenutzte Schwachstellen und informiert gegebenenfalls Nutzer. Die Pflicht greift erst bei Kenntnis aktiver Ausnutzung, typischerweise über Reports von Herstellern, die die Komponente integriert haben.

> Keiner dieser vier Fälle verschärft die Meldepflicht, alle vier machen sie planbar. Wer Erstprüfung, Dokumentation und Zuständigkeiten ordentlich aufsetzt, hat sie zu seinen Gunsten geklärt.

07

DIE PROZESS-LANDKARTE

Vom Hinweis zur abgeschlossenen Meldung

Uhr läuft nicht

1 Eingang

Ein Hinweis trifft ein, ob von einem Forscher, einem Kunden, dem eigenen Team, einer Behörde oder aus den Medien, und landet im definierten Meldekanal. Eingang mit Zeitstempel dokumentieren.

Prüfpflicht

2 Erstprüfung, unverzüglich

Gegen beide Auslöser bewerten. Ist keiner erfüllt, besteht keine Meldepflicht; die Entscheidung wird dokumentiert. Wird verifiziert, ist der Zeitpunkt der Verifizierung die Kenntnisnahme. Jetzt startet die Uhr.

Stunde 0–24

3 Frühwarnung

Über die Single Reporting Platform an CSIRT und ENISA: Produkt, Titel, Vertriebsländer bzw. Verdacht auf böswillige Handlung. Mit vorbereiteter Vorlage ist das ein Ausfüllvorgang. Parallel laufen die technischen Sofortmaßnahmen.

Stunde 24–72

4 Detailmeldung

Analyse nachreichen: Art der Schwachstelle oder des Vorfalls, erste Bewertung, ergriffene Maßnahmen, Workarounds. Die Nutzerinformation nach Abs. 8 läuft parallel und beginnt bereits mit der Kenntnisnahme: bekannte betroffene Kunden unverzüglich direkt informieren, den breiteren Nutzerkreis per Advisory, sobald das ohne zusätzliches Risiko möglich ist.

Ohne Frist

5 Fix entwickeln

Patch oder Risikominderung entwickeln. Artikel 14 setzt hierfür keine Frist. Der Zeitpunkt, ab dem die Maßnahme verfügbar ist, startet aber die letzte Frist und gehört deshalb in die Fallakte.

14 T / 1 Monat

6 Abschlussbericht

Bei Schwachstellen spätestens 14 Tage nach Verfügbarkeit der Maßnahme, bei Vorfällen binnen eines Monats nach der 72-h-Meldung. Fall-Timeline und Security Advisory liefern den Inhalt, das Advisory bei Bedarf maschinenlesbar als CSAF.

Durchgehend, Phase 1 bis 6: dokumentieren. Jeder Schritt mit Zeitstempel in der Fall-Timeline. Zwischenbericht-Anfragen des CSIRT (Abs. 6) beantworten Sie dann per Export und können jederzeit belegen, wann Sie was wussten und getan haben.

08

EIN DURCHGESPIELTES BEISPIEL

Ernstfall beim IoT-Gateway-Hersteller

Ein fiktiver, aber realistischer Fall. So läuft die Kette ab, wenn die Vorbereitung aus Kapitel 09 erledigt ist:

Di, 14:32	Ein Sicherheitsforscher meldet über den Meldekanal eine Schwachstelle im Fernwartungsmodul, mit Proof-of-Concept, aber ohne Hinweis auf eine Ausnutzung. Eingang mit Zeitstempel erfasst.
Di, 15:05	Die Erstprüfung beginnt: Schwachstelle reproduzieren, Telemetrie und Kundenlogs gegen das Angriffsmuster prüfen. Prüfbeginn dokumentiert.
Di, 19:20	**Kenntnisnahme.** In den Logs zweier Kunden passt das Zugriffsmuster, die aktive Ausnutzung ist bestätigt. Die Uhr läuft, die Frühwarnung ist bis Mittwoch, 19:20 Uhr fällig.
Mi, 08:45	Die Frühwarnung geht über die Single Reporting Platform an CSIRT und ENISA, mit Produkt, Titel und Vertriebsländern aus der vorbereiteten Vorlage. Zehn Stunden Puffer bleiben ungenutzt, weil die Vorlage fertig war.
Do, 14:10	Die Detailmeldung geht raus, deutlich innerhalb der 72-Stunden-Frist: Art der Schwachstelle, erste Bewertung, ein Workaround (Fernwartungsmodul deaktivieren). Parallel werden die bekannten betroffenen Kunden direkt informiert.
Neun Tage später	Der Patch ist getestet und verfügbar. Der Zeitpunkt wird dokumentiert, ab jetzt läuft die 14-Tage-Frist für den Abschlussbericht.
Drei Tage danach	Abschlussbericht eingereicht, Security Advisory als CSAF veröffentlicht. Der Fall ist geschlossen, die komplette Timeline liegt mit Zeitstempeln vor.

> Zwischen Eingang und Fristbeginn liegen **knapp fünf Stunden dokumentierte Prüfzeit** — der Hinweis belegte die Ausnutzung zunächst nicht. Je klarer ein Hinweis sie schon belegt, desto kürzer ist dieser Spielraum: Prüfzeit verlängert die Frist nicht, sie muss unverzüglich beginnen und nachweisbar sein.

09

DIE VORBEREITUNG

Vier Schritte bis zum 11. September

- [ ] **1 · Meldekanal und Erstprüfung einrichten**
  Ein definierter Eingangskanal für alle Hinweise plus eine Klassifizierungsmatrix nach Abs. 5 mit Beispielen aus der eigenen Produktwelt. So entscheidet das Team in Minuten, ob ein Fall meldepflichtig ist. Der öffentliche Meldekanal wird formal erst ab Dezember 2027 Pflicht (Art. 13(17)); ohne ihn machen Sie sich das Leben aber unnötig schwer und müssen Hinweise im Ernstfall über verteilte Postfächer zusammensuchen.

- [ ] **2 · Zuständigkeit klären**
  Meldeverantwortlicher plus Vertretung benannt, zuständiges CSIRT dokumentiert. Maßgeblich ist der Mitgliedstaat der Hauptniederlassung, also dort, wo die Cybersicherheitsentscheidungen überwiegend fallen. Den Zugang zur Single Reporting Platform einrichten und in der Testphase vor dem Stichtag ausprobieren.

- [ ] **3 · Meldevorlagen bauen**
  Je eine Vorlage für die 24-Stunden-Frühwarnung, die 72-Stunden-Meldung, den Abschlussbericht und die Nutzerbenachrichtigung. Welche Felder je Stufe verpflichtend sind, listet das ENISA-FAQ zur Single Reporting Platform.

- [ ] **4 · Einmal durchspielen**
  Ein Tabletop-Durchlauf mit einer fiktiven Schwachstelle zeigt, wo die Kette hakt, solange es noch nichts kostet.

Der Aufwand liegt bei den meisten Herstellern im Bereich weniger Personentage. Die 24-Stunden-Frist wird erst dann zum Problem, wenn Abläufe, Zuständigkeiten und Vorlagen im Ernstfall zusammengesucht werden müssen.

A

ANHANG · ARBEITSHILFEN

Einstufung und Zuständigkeiten

KLASSIFIZIERUNGSMATRIX — SECHS TYPISCHE FÄLLE

SITUATION	EINSTUFUNG	KONSEQUENZ
Angreifer nutzen eine RCE-Lücke im Fernwartungsmodul nachweislich aus	**Aktiv ausgenutzte Schwachstelle**	Meldekette Schwachstelle, 24 h ab Kenntnisnahme
Ransomware verschlüsselt Gerätedaten bei mehreren Kunden	**Schwerer Vorfall (Abs. 5 lit. a)**	Meldekette Vorfall, 24 h ab Kenntnisnahme
Schadcode im signierten Update-Paket entdeckt, noch kein Angriff bekannt	**Schwerer Vorfall (Abs. 5 lit. b)**	Meldepflichtig auch ohne festgestellte Ausnutzung
CVE 9.8 in einer verwendeten Bibliothek, kein Exploit gegen Ihr Produkt bekannt	**Kein Auslöser**	Intern behandeln, ggf. Upstream nach Art. 13(6)
Pentest findet einen Auth-Bypass in der eigenen Firmware	**Kein Auslöser**	Interner Vorgang, Behebung nach Schwachstellenprozess
DDoS legt Ihre Unternehmenswebsite lahm, das Produkt ist nicht betroffen	**Kein Produktvorfall**	Nicht Art. 14; ggf. Meldepflichten nach NIS2 prüfen

ROLLEN IM ERNSTFALL — VORAB BENENNEN, NICHT IMPROVISIEREN

ROLLE	ENTSCHEIDET ÜBER	ERREICHBAR
Meldeverantwortlicher	Kenntnisnahme feststellen, Meldung freigeben und absenden	24/7, mit Vertretung
Technische Analyse	Reproduktion, Ausnutzungsnachweis, Workaround und Patch	Rufbereitschaft
Kundenkommunikation	Nutzerinformation nach Abs. 8, Advisory und Sprachregelung	Geschäftszeiten
Geschäftsführung	Eskalation, Rückruf oder Vertriebsstopp, externe Unterstützung	Eskalationsweg

A

Meldeinhalte und der Testlauf

MELDEINHALTE JE STUFE — ALS VORLAGENFELDER ÜBERNEHMEN

Frühwarnung (24 h)

Hersteller und Kontaktstelle · betroffenes Produkt mit Version · Schwachstelle oder Vorfall · bei Schwachstellen: EU-Vertriebsländer · bei Vorfällen: Verdacht auf böswillige Handlung, grenzüberschreitende Auswirkungen

Detailmeldung (72 h)

Art der Schwachstelle bzw. des Vorfalls · erste Einschätzung von Schweregrad und Auswirkungen · CVE-Kennung, falls vorhanden · ergriffene Korrektur- und Risikominderungsmaßnahmen · Workarounds für Nutzer

Abschlussbericht Schwachstelle (14 Tage nach Fix)

Beschreibung mit Schweregrad und Auswirkungen · Angaben zum Angreifer, soweit bekannt · verfügbares Update bzw. verfügbare Korrekturmaßnahme

Abschlussbericht Vorfall (1 Monat)

Detaillierte Beschreibung mit Schweregrad und Auswirkungen · Art der Bedrohung und mutmaßliche Ursache · ergriffene und laufende Abhilfemaßnahmen

TABLETOP-ÜBUNG IN 60 MINUTEN — ABLAUF FÜR DEN TESTLAUF

0–10 min	**Szenario einspielen.** Ein fiktiver Forscher-Hinweis samt Log-Auszug geht an den echten Meldekanal. Wer bemerkt ihn, und wie lange dauert es?
10–25 min	**Erstprüfung gegen die Matrix.** Das Team entscheidet mit der Klassifizierungsmatrix: aktive Ausnutzung, schwerer Vorfall oder keiner der beiden Auslöser? Entscheidung und Zeitstempel festhalten.
25–40 min	**Frühwarnung ausfüllen.** Vorlage mit echten Produktdaten befüllen, ohne abzusenden. Jedes Feld, das jemand nachrecherchieren muss, ist ein Fund.
40–50 min	**Nutzerinformation entwerfen.** Wer sind die betroffenen Kunden, über welchen Kanal erreichen Sie sie, und wer gibt den Text frei?
50–60 min	**Lücken protokollieren.** Jeder Fund wird Aufgabe mit Verantwortlichem und Termin. Erst dann war die Übung eine Übung und keine Diskussion.

HÄUFIGE FRAGEN

Kurz beantwortet

Muss ich jede CVE aus dem Scanner melden?

Nein. Meldepflichtig sind nur aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle nach Abs. 5. Scanner-Funde, CVEs ohne Ausnutzung und Pentest-Ergebnisse gehören ins interne Schwachstellenmanagement.

An wen melde ich?

Gleichzeitig an das koordinierende CSIRT des Mitgliedstaats Ihrer Hauptniederlassung und an die ENISA, über die Single Reporting Platform nach Art. 16.

Wir haben keine Niederlassung in der EU. Welches CSIRT ist zuständig?

Abs. 7 sieht eine Kaskade vor: der Mitgliedstaat des Bevollmächtigten, sonst des Einführers, sonst des Händlers, sonst der Staat, in dem die Nutzer sitzen. Einmal bestimmen, dokumentieren, fertig.

Wann startet die 24-Stunden-Frist?

Mit der verifizierten Kenntnisnahme, nicht mit dem Eingang eines Hinweises. Die Erstprüfung muss allerdings unverzüglich beginnen und dokumentiert sein.

Gilt das auch für alte, nicht mehr supportete Produkte?

Ja. Die Meldepflicht gilt für alle Produkte im CRA-Anwendungsbereich und läuft nach dem Ende des Support-Zeitraums weiter. Nur die Schwachstellenbehandlung endet mit dem Support.

Ist eine SBOM für die Meldung Pflicht?

Für Art. 14 nicht; Pflicht wird sie erst ab Dezember 2027 über Anhang I. Ohne sie lässt sich bei einer Komponenten-Schwachstelle aber kaum fristgerecht klären, welche Produkte betroffen sind.

IHR ANSPRECHPARTNER

Maximilian Heck
Head of Regulatory & Security

maximilian.heck@think-ahead.tech
+49 176 72001773 · linkedin.com/in/maximilian-heck

Quellen: Verordnung (EU) 2024/2847 (Cyber Resilience Act), Art. 13–16, 24, 64, 69, 71 · Kommissions-Guidance zur Anwendung des CRA, Juli 2026 · Durchführungsverordnung (EU) 2024/2690 (NIS2) · ENISA-FAQ zur Single Reporting Platform. Rechtsverbindlich ist allein der im Amtsblatt der EU veröffentlichte Wortlaut. Dieses Whitepaper stellt keine Rechtsberatung dar.