Coordinated Vulnerability Disclosure Policy (CVD-Policy)

der Firma

X2E GmbH

Version dieses Dokuments	1.0
Datum der letzten Änderung	10.09.2026
Autor	Danny Freier
Vertraulichkeitsstufe	ÖFFENTLICH

X2E GmbH
Große Ahlmühle 19
76865 Rohrbach

Tel.: +49 6349 99599 202
www.x2e.de

Änderungshistorie

Datum	Version	Erstellt durch	Beschreibung der Änderung
10.09.2026	1.0	Danny Freier	Initiales Dokument

Freigabe

Rolle	Funktion	Datum	Unterschrift
Erstellt	Informationssicherheitsverantwortlicher	10.09.2026	
Geprüft	Leitung IT-Administration	10.09.2026	
Freigegeben	Technischer Direktor	10.09.2026	

Inhalt

1. Zweck und Geltungsbereich

Die X2E GmbH („X2E“) nimmt die Sicherheit ihrer Produkte, Systeme und Infrastruktur ernst. Sicherheitsforschende, Kunden, Partner und andere Personen, die eine mögliche Sicherheitslücke entdecken, sollen diese auf einem klar definierten, sicheren und vertrauensvollen Weg an X2E melden können.

Diese Coordinated Vulnerability Disclosure Policy („CVD-Policy“) beschreibt,

- welche Schwachstellen über den CVD-Prozess gemeldet werden können,
- wie eine Meldung erfolgen soll,
- welche Verhaltensregeln für meldende Personen gelten,
- welche Zusicherungen X2E gegenüber meldenden Personen macht,
- innerhalb welcher Fristen X2E reagiert und
- wie eine Schwachstelle koordiniert behoben und gegebenenfalls veröffentlicht wird.

Die Policy gilt für Schwachstellen in Produkten mit digitalen Elementen, für die X2E als Hersteller oder Produktverantwortlicher verantwortlich ist, sowie für Schwachstellen in von X2E betriebenen IT-Systemen und Infrastrukturen.

Diese Policy wird mindestens einmal jährlich sowie zusätzlich bei wesentlichen rechtlichen, organisatorischen oder technischen Änderungen auf Aktualität und Angemessenheit überprüft.

2. Kontakt und Meldung einer Schwachstelle

X2E stellt unterschiedliche Kontaktwege für Schwachstellen in Produkten und für Schwachstellen in der eigenen IT-Infrastruktur bereit. Meldende Personen sollten nach Möglichkeit den für den jeweiligen Sachverhalt vorgesehenen Kontaktweg verwenden.

Eine Meldung über einen anderen der nachfolgend genannten Security-Kontaktwege wird dennoch bearbeitet und erforderlichenfalls intern an die zuständige Stelle weitergeleitet.

2.1 Schwachstellen in X2E-Produkten und zugehörigen Services

Schwachstellen in Produkten, Software, Firmware oder produktbezogenen Services, für die X2E verantwortlich ist, sollen an das Product Security Incident Response Team (PSIRT) gemeldet werden:

E-Mail: psirt@x2e.de

Das PSIRT ist insbesondere für die Entgegennahme, Bewertung, Koordination und Bearbeitung von Schwachstellen in X2E-Produkten und zugehörigen produktbezogenen Services zuständig.

2.2 Schwachstellen in der X2E-IT-Infrastruktur

Schwachstellen in der von X2E betriebenen Unternehmens- und IT-Infrastruktur sollen an das Computer Security Incident Response Team (CSIRT) gemeldet werden:

E-Mail: csirt@x2e.de

Hierzu zählen beispielsweise Schwachstellen in öffentlich erreichbaren IT-Systemen, Webanwendungen, Netzwerkdiensten oder sonstigen von X2E betriebenen IT-Komponenten, soweit diese nicht Bestandteil eines X2E-Produkts oder eines produktbezogenen Services sind.

Zum Umgang mit allgemeinen Informationssicherheitsvorfällen siehe Kapitel 2.5.

2.3 Telefonische Meldung

Für Schwachstellenmeldungen und Informationssicherheitsvorfälle steht ergänzend ein zentraler telefonischer Security-Kontakt zur Verfügung:

Telefon: +49 6349 99599 202

Die Telefonnummer kann sowohl für Schwachstellen in X2E-Produkten und der X2E-IT-Infrastruktur als auch für tatsächliche oder vermutete Informationssicherheitsvorfälle genutzt werden. Die Meldung wird anhand des geschilderten Sachverhalts intern der zuständigen Funktion – PSIRT, CSIRT oder Incident Response – zugeordnet.

Für die Übermittlung technischer Details, Dateien oder vertraulicher Informationen empfehlen wir grundsätzlich die Nutzung der jeweils zuständigen E-Mail-Adresse oder des Meldeformulars.

2.4 Anonyme Meldung

Schwachstellen können alternativ über das von X2E bereitgestellte Meldeformular übermittelt werden:

Anonymes Meldeformular: https://x2e.de/security/

Eine Meldung über das Meldeformular kann ohne Angabe personenbezogener Daten erfolgen.

Bei vollständig anonymen Meldungen ohne erreichbaren Rückkanal können keine individuellen Rückfragen oder persönlichen Statusinformationen übermittelt werden. Die Meldung wird dennoch nach denselben fachlichen Grundsätzen geprüft und bestmöglich bearbeitet.

Kann X2E anhand der Meldung nicht eindeutig feststellen, ob eine Produkt- oder Infrastruktur-Schwachstelle betroffen ist, erfolgt die interne Zuordnung durch X2E.

2.5 Abgrenzung zu Informationssicherheitsvorfällen

Diese CVD-Policy dient in erster Linie der Meldung und koordinierten Bearbeitung von **Schwachstellen** insbesondere in Bezug auf die eigenen Produkte.

Besteht hingegen der Verdacht, dass bereits ein Informationssicherheitsereignis oder Informationssicherheitsvorfall eingetreten ist oder aktuell stattfindet, soll der hierfür vorgesehene separate Meldeweg verwendet werden:

Informationssicherheitsvorfälle: incidentreport@x2e.de

Hierzu zählen beispielsweise Hinweise auf

- laufende oder bereits erfolgte Cyberangriffe,
- kompromittierte Benutzerkonten oder Zugangsdaten,
- Malware oder Ransomware,
- unberechtigte Zugriffe auf Systeme oder Daten,
- Datenabflüsse oder Datenlecks,
- Manipulation, Verlust oder unberechtigte Offenlegung von Informationen oder
- sonstige verdächtige Aktivitäten, die auf eine tatsächliche oder mögliche Beeinträchtigung der Informationssicherheit hindeuten.

Der Meldeweg für Informationssicherheitsvorfälle ist organisatorisch vom CVD-Meldeweg getrennt. Die Bearbeitung kann jedoch durch dieselben oder miteinander zusammenarbeitende Funktionen der X2E-Informationssicherheitsorganisation erfolgen.

Wird über einen CVD-Kontakt ein Informationssicherheitsvorfall gemeldet oder ergeben sich während der Bearbeitung einer Schwachstelle Hinweise auf eine tatsächliche Ausnutzung, überführt X2E den Sachverhalt zusätzlich in den hierfür vorgesehenen Incident-Response-Prozess.

Umgekehrt werden über den Incident-Meldeweg eingegangene Hinweise, die sich bei der Prüfung als CVD-relevante Schwachstellenmeldung herausstellen, an den zuständigen CVD-Prozess übergeben.

2.6 Inhalt einer Schwachstellenmeldung

Eine Schwachstellenmeldung sollte, soweit möglich, insbesondere folgende Informationen enthalten:

- das betroffene Produkt, System oder die betroffene Komponente einschließlich Version,
- eine Beschreibung der Schwachstelle und ihrer möglichen Auswirkungen,
- nachvollziehbare Schritte zur Reproduktion,
- gegebenenfalls einen Proof of Concept,
- Angaben zu bereits durchgeführten Tests,
- gegebenenfalls Vorschläge zur Behebung oder Risikominimierung sowie
- Kontaktdaten für Rückfragen, sofern die Meldung nicht anonym erfolgen soll.

Je vollständiger die bereitgestellten Informationen sind, desto schneller kann X2E die Schwachstelle nachvollziehen, bewerten und bearbeiten.

Statusanfragen zum Bearbeitungsstand sind ausdrücklich willkommen und können jederzeit über den für die jeweilige Meldung verwendeten Kontaktweg gestellt werden.

2.7 Vertrauliche Übermittlung

Schwachstelleninformationen können sicherheitskritische oder anderweitig vertrauliche Inhalte enthalten.

X2E empfiehlt daher, vertrauliche Informationen nach Möglichkeit **verschlüsselt und digital signiert** zu übermitteln.

Die öffentlichen Schlüssel und Informationen zu den unterstützten Verschlüsselungsverfahren werden über die zentrale X2E-Security-Seite bzw. die security.txt bereitgestellt:

PSIRT OpenPGP-Schlüssel: https://x2e.de/.well-known/pgp/psirt-x2e-de.asc

CSIRT OpenPGP-Schlüssel: https://x2e.de/.well-known/pgp/csirt-x2e-de.asc

3. Was ist eine gültige Schwachstellenmeldung?

Eine Meldung wird grundsätzlich im Rahmen dieses CVD-Prozesses behandelt, wenn

1. sie ein Produkt, eine Komponente, ein System oder eine Infrastruktur betrifft, für die X2E verantwortlich ist.[1]
2. die gemeldete Schwachstelle oder die wesentlichen dazugehörigen Informationen zum Zeitpunkt der Meldung noch nicht öffentlich bekannt sind und
3. die Meldung ausreichend Informationen enthält, um eine sachgerechte technische Bewertung zu ermöglichen.

Die Einordnung einer Schwachstelle als CVD-Fall bedeutet nicht automatisch, dass eine gesetzliche Meldepflicht nach Artikel 14 CRA besteht. Diese wird bei entsprechendem Produktbezug gesondert geprüft.

Ergebnisse ausschließlich automatisierter Schwachstellenscanner oder anderer automatisierter Tools gelten **ohne ergänzende technische Beschreibung und nachvollziehbare Dokumentation grundsätzlich nicht als gültige Schwachstellenmeldung**.

Bereits bekannte oder bereits behobene Schwachstellen können von X2E entgegengenommen und geprüft werden, müssen jedoch nicht als neuer CVD-Fall behandelt werden.

4. Erwartungen an meldende Personen

X2E bittet Sicherheitsforschende und andere meldende Personen um einen verantwortungsvollen und verhältnismäßigen Umgang mit entdeckten Schwachstellen.

Insbesondere erwarten wir, dass

- eine Schwachstelle nur in dem Umfang untersucht oder genutzt wird, der erforderlich ist, um ihre Existenz und mögliche Auswirkung nachzuweisen,
- keine vermeidbaren Schäden verursacht werden,
- keine Social-Engineering-, Phishing-, Spam-, Denial-of-Service-, Distributed-Denial-of-Service-, Brute-Force- oder vergleichbaren Angriffe gegen X2E oder Dritte durchgeführt werden,
- keine Daten Dritter absichtlich eingesehen, kopiert, verändert, gelöscht oder anderweitig manipuliert werden,
- keine dauerhafte Veränderung oder Beeinträchtigung von X2E-Systemen vorgenommen wird,
- keine Schadsoftware oder dauerhaften Zugänge eingerichtet werden,
- Schwachstellen und Exploits nicht vor Abschluss des koordinierten Offenlegungsprozesses an Dritte weitergegeben, verkauft oder öffentlich zugänglich gemacht werden und
- geltendes Recht eingehalten wird.

[1] Nicht umfasst sind grundsätzlich Schwachstellen in Systemen oder Diensten Dritter, die von X2E lediglich genutzt werden und für die X2E nicht verantwortlich ist.

Sollten während der Untersuchung unbeabsichtigt personenbezogene, vertrauliche oder anderweitig geschützte Informationen zugänglich werden, bitten wir darum, den Zugriff unverzüglich zu beenden, die betreffenden Informationen nicht weiterzuverwenden oder weiterzugeben und X2E darüber zu informieren.

Auch Meldungen von Personen, die einzelne Anforderungen dieses Verhaltenskodex nicht eingehalten haben, werden von X2E soweit möglich sachgerecht geprüft und im Interesse der Sicherheit bestmöglich bearbeitet. Die nachfolgend beschriebenen Zusicherungen können jedoch davon abhängen, dass die Voraussetzungen dieser Policy eingehalten wurden.

5. Unsere Zusicherungen gegenüber meldenden Personen

X2E verpflichtet sich zu einem fairen, professionellen und kooperativen Umgang mit Personen, die Sicherheitslücken im Rahmen dieser Policy melden.

5.1 Vertraulichkeit

X2E behandelt jede Meldung und die damit zusammenhängende Kommunikation **vertraulich, soweit dies gesetzlich zulässig ist**.

Informationen über eine Schwachstelle werden vor ihrer koordinierten Offenlegung nur den Personen und Stellen zugänglich gemacht, die sie zur Bewertung, Behebung, Koordination oder aufgrund gesetzlicher Verpflichtungen benötigen.

5.2 Schutz personenbezogener Daten

Personenbezogene Daten der meldenden Person werden **nicht ohne deren ausdrückliche Einwilligung an Dritte weitergegeben**, soweit X2E nicht aufgrund zwingender gesetzlicher Bestimmungen zu einer Weitergabe verpflichtet ist.

Die meldende Person entscheidet insbesondere selbst, ob ihr Name, Alias oder eine andere Zuordnung im Zusammenhang mit einer späteren Danksagung oder Veröffentlichung genannt werden darf.

5.3 Keine Verpflichtung zu einer Geheimhaltungsvereinbarung

X2E verlangt von meldenden Personen **keine Unterzeichnung einer Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA)** als Voraussetzung für die Meldung oder Bearbeitung einer Schwachstelle im Rahmen dieser Policy.

Die Regeln zur koordinierten Offenlegung ergeben sich aus dieser CVD-Policy und der laufenden Abstimmung zwischen X2E und der meldenden Person.

5.4 Keine Strafanzeige bei Einhaltung dieser Policy

X2E wird **keine Strafanzeige wegen der im Rahmen der Sicherheitsuntersuchung vorgenommenen Handlungen stellen**, sofern die meldende Person nach bestem Wissen und Gewissen im Einklang mit dieser Policy handelt, ihre Untersuchung auf das zur Feststellung und Dokumentation der Schwachstelle notwendige Maß beschränkt und keine erkennbare kriminelle Absicht verfolgt.

Diese Zusicherung gilt nicht für Handlungen, die erkennbar der Schädigung, Erpressung, Bereicherung, Sabotage, Ausspähung oder einem vergleichbaren kriminellen Zweck dienen.

Gesetzliche Verpflichtungen von X2E gegenüber Behörden bleiben unberührt.

5.5 Kontinuierlicher Ansprechpartner

X2E bleibt während des gesamten CVD-Prozesses für Rückfragen, technische Abstimmungen und Statusanfragen erreichbar.

Wir legen Wert auf einen respektvollen, sachlichen und transparenten Austausch. Dies erwarten wir gleichermaßen von allen Beteiligten.

5.6 Keine automatisierte Kommunikation als Ersatz für persönliche Rückmeldung

Automatisierte Eingangsbestätigungen können ergänzend eingesetzt werden. Sie ersetzen jedoch nicht die nachfolgend zugesagten persönlichen Rückmeldungen durch einen zuständigen Ansprechpartner.

6. Reaktions- und Bearbeitungszeiten

Für Meldungen im Rahmen dieser CVD-Policy gelten folgende maximale Reaktionszeiten.

Als **Arbeitstage** gelten Montag bis Freitag mit Ausnahme der gesetzlichen Feiertage am Hauptsitz der X2E GmbH.

Innerhalb von 5 Arbeitstagen

X2E gibt auf jede neue Schwachstellenmeldung sowie auf wesentliche Aktualisierungen einer bestehenden Meldung innerhalb von **fünf Arbeitstagen eine persönliche Rückmeldung**.

Eine ausschließlich automatisiert erzeugte Eingangsbestätigung erfüllt diese Verpflichtung nicht.

Bei vollständig anonymen Meldungen ohne erreichbaren Rückkanal entfällt diese Rückmeldung.

Innerhalb von 10 Arbeitstagen

Spätestens innerhalb von **zehn Arbeitstagen nach Eingang der Meldung** gibt X2E nach einer ersten Analyse eine detailliertere Rückmeldung.

Diese enthält, soweit zu diesem Zeitpunkt möglich,

- die Bestätigung der Schwachstelle,
- die begründete Zurückweisung der Meldung,
- konkrete technische Rückfragen oder
- eine Mitteilung, dass für die Prüfung zusätzliche Zeit erforderlich ist.

Ist eine abschließende Bewertung innerhalb von zehn Arbeitstagen nicht möglich, erläutert X2E den Grund für die weitere Prüfung und stellt **innerhalb weiterer zehn Arbeitstage ein erneutes Statusupdate** bereit.

Solange eine abschließende Bewertung aussteht, wird dieser regelmäßige Austausch angemessen fortgeführt.

Öffentliche Offenlegung innerhalb von 90 Tagen

Validierte und verifizierte Schwachstellen werden grundsätzlich **spätestens innerhalb von 90 Kalendertagen nach Eingang der Schwachstellenmeldung koordiniert öffentlich offengelegt**.

Ziel ist es, innerhalb dieses Zeitraums eine geeignete Behebung, Sicherheitsaktualisierung oder wirksame Gegenmaßnahme bereitzustellen und betroffene Nutzer angemessen zu informieren.

Ist eine Offenlegung innerhalb dieses Zeitraums aus sachlich begründeten Gründen nicht möglich oder würde sie ein erhebliches zusätzliches Sicherheitsrisiko verursachen, kann der Zeitraum **einmalig um bis zu weitere 90 Kalendertage verlängert werden**. Eine solche Verlängerung erfolgt in enger Abstimmung mit dem zuständigen nationalen CSIRT.

Eine weitere Verzögerung über diesen verlängerten Zeitraum hinaus erfolgt nur mit Zustimmung des zuständigen CSIRT.

X2E stimmt den konkreten Zeitpunkt und Inhalt einer Offenlegung nach Möglichkeit mit der meldenden Person sowie, soweit erforderlich, mit weiteren beteiligten Herstellern, Betreibern, CSIRTs oder zuständigen Behörden ab.

7. Koordinierte Offenlegung und EU Vulnerability Database

Nach erfolgreicher Validierung einer Schwachstelle koordiniert X2E deren Behebung und Offenlegung. Sobald für eine behobene Schwachstelle eine Sicherheitsaktualisierung bereitgestellt wurde, veröffentlicht X2E Informationen über die beseitigte Schwachstelle. Diese umfassen insbesondere eine Beschreibung der Schwachstelle, Angaben zur Identifikation der betroffenen Produkte bzw. Versionen, die Auswirkungen und den Schweregrad der Schwachstelle sowie klare und verständliche Informationen, die den Nutzern bei deren Behebung bzw. Risikominderung helfen.

Die Veröffentlichung kann insbesondere über Security Advisories, CVE-Informationen, Sicherheitshinweise oder andere geeignete Informationskanäle erfolgen.

In hinreichend begründeten Fällen kann X2E die Veröffentlichung von Informationen über eine bereits behobene Schwachstelle aufschieben, wenn die Sicherheitsrisiken einer sofortigen Veröffentlichung deren Nutzen überwiegen. Eine solche Verzögerung ist insbesondere möglich, um betroffenen Nutzern zunächst Gelegenheit zu geben, einen bereitgestellten Patch oder eine andere geeignete Korrekturmaßnahme anzuwenden.

Im Rahmen der europäischen Schwachstellenkoordination kann X2E in Abstimmung mit dem zuständigen nationalen CSIRT oder ENISA die Aufnahme bzw. Offenlegung einer behobenen Schwachstelle über die **European Vulnerability Database (EUVD)** veranlassen. Der CRA sieht vor, dass ENISA behobene Schwachstellen im Einvernehmen mit dem Hersteller in der Europäischen Schwachstellendatenbank offenlegen kann.

Die Veröffentlichung bzw. Koordination einer Schwachstelle über die EUVD **ersetzt keine gegebenenfalls bestehende gesetzliche Meldepflicht nach Artikel 14 des Cyber Resilience Act (CRA)**. CVD-Offenlegung und gesetzliche CRA-Meldung sind getrennte Prozesse und können parallel erforderlich sein.

8. Aktiv ausgenutzte Schwachstellen und gesetzliche CRA-Meldepflichten

Bei einer Schwachstelle, für die X2E Kenntnis von einer tatsächlichen aktiven Ausnutzung erlangt, sowie bei einem möglicherweise schwerwiegenden Sicherheitsvorfall mit Auswirkungen auf die Sicherheit eines X2E-Produkts mit digitalen Elementen wird der Sachverhalt unverzüglich priorisiert und intern als potenzieller CRA-Meldefall eskaliert.

Die gesetzlichen Meldepflichten nach Artikel 14 CRA gelten ab dem 11. September 2026. Die Meldungen erfolgen über die von ENISA betriebene Single Reporting Platform (SRP) gleichzeitig an das gemäß Artikel 14 CRA als Koordinator benannte CSIRT und an ENISA.

8.1 Aktiv ausgenutzte Schwachstelle

Bei einer aktiv ausgenutzten Schwachstelle in einem X2E-Produkt mit digitalen Elementen erfolgen insbesondere folgende Meldungen:

- unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, eine Frühwarnung; dabei werden gegebenenfalls die Mitgliedstaaten angegeben, in denen das betroffene Produkt nach Kenntnis von X2E bereitgestellt wurde,
- unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntniserlangung, eine weitergehende Schwachstellenmeldung mit den bis dahin verfügbaren allgemeinen Informationen zum betroffenen Produkt, zur Art der Ausnutzung und der Schwachstelle sowie zu bereits getroffenen und für Nutzer möglichen Korrektur- oder Risikominderungsmaßnahmen, und
- sofern die entsprechenden Informationen nicht bereits vorgelegt wurden, spätestens 14 Tage nachdem eine Korrektur- oder Risikominderungsmaßnahme verfügbar ist, ein Abschlussbericht. Dieser enthält mindestens eine Beschreibung der Schwachstelle einschließlich Schweregrad und Auswirkungen, soweit verfügbar Informationen zum böswilligen Akteur sowie Informationen über bereitgestellte Sicherheitsaktualisierungen oder andere Korrekturmaßnahmen.

8.2 Schwerwiegender Sicherheitsvorfall mit Auswirkungen auf die Produktsicherheit

Der CRA sieht neben aktiv ausgenutzten Schwachstellen eine eigenständige Meldepflicht für schwerwiegende Sicherheitsvorfälle mit Auswirkungen auf die Sicherheit eines Produkts mit digitalen Elementen vor.

Ein solcher Vorfall ist insbesondere dann zu prüfen, wenn er sich negativ auf die Fähigkeit des Produkts auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen zu schützen, oder wenn er zur Einführung oder Ausführung von Schadcode im Produkt bzw. in den Netz- und Informationssystemen eines Nutzers geführt hat oder führen kann.

Bei einem meldepflichtigen schwerwiegenden Sicherheitsvorfall erfolgen insbesondere:

- unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, eine Frühwarnung, die mindestens auch angibt, ob ein rechtswidriges oder böswilliges Handeln als Ursache vermutet wird,
- unverzüglich, spätestens innerhalb von 72 Stunden nach Kenntniserlangung, eine weitergehende Vorfallmeldung einschließlich der verfügbaren Informationen über Art und erste Bewertung des Vorfalls sowie getroffene und mögliche Risikominderungs- oder Korrekturmaßnahmen, und
- sofern die entsprechenden Informationen nicht bereits übermittelt wurden, innerhalb eines Monats nach der 72-Stunden-Meldung ein Abschlussbericht mit einer ausführlichen Beschreibung des Vorfalls einschließlich Schweregrad und Auswirkungen, der wahrscheinlichen Bedrohungsart bzw. Ursache sowie den ergriffenen und noch laufenden Abhilfemaßnahmen.

8.3 Information betroffener Nutzer

Nach Kenntniserlangung einer aktiv ausgenutzten Schwachstelle oder eines schwerwiegenden Sicherheitsvorfalls mit Auswirkungen auf die Sicherheit eines X2E-Produkts informiert X2E die betroffenen Nutzer und, soweit angemessen, weitere Nutzer über den Sachverhalt.

Soweit erforderlich, informiert X2E die Nutzer zugleich über verfügbare Risikominderungs- und Korrekturmaßnahmen, die sie ergreifen können, um die Auswirkungen der Schwachstelle oder des Sicherheitsvorfalls

zu reduzieren. Die Information kann, soweit angemessen, in einem strukturierten und maschinenlesbaren Format erfolgen.

Diese Nutzerinformation erfolgt unabhängig von der späteren koordinierten öffentlichen Offenlegung einer Schwachstelle.

8.4 Zuständiges nationales CSIRT und Meldeweg

Für X2E mit Hauptniederlassung in Deutschland ist im Rahmen der CRA-Meldeorganisation das hierfür als Koordinator benannte deutsche CSIRT maßgeblich; die gesetzliche Meldung erfolgt jedoch über die Single Reporting Platform an das zuständige koordinierende CSIRT und ENISA.

X2E übermittelt erforderliche Folgeinformationen, neue Erkenntnisse und Angaben zu Korrektur- und Risikominderungsmaßnahmen entsprechend den gesetzlichen Anforderungen und stimmt sich, soweit erforderlich, mit dem zuständigen koordinierenden CSIRT ab.

Die gesetzlichen CRA-Melde- und Informationspflichten bestehen unabhängig vom allgemeinen CVD-Prozess und dessen Reaktions- und Offenlegungsfristen.

9. Aktiv ausgenutzte Schwachstellen und Informationssicherheitsvorfälle

Ergeben sich Hinweise darauf, dass eine Schwachstelle tatsächlich ausgenutzt wird oder wurde, wird der Vorgang unverzüglich als potenzieller CRA-Meldefall nach Kapitel 8 behandelt. Zusätzlich wird geprüft, ob zugleich ein Informationssicherheitsereignis oder -vorfall vorliegt, der nach den internen Verfahren der X2E GmbH zu behandeln ist.

Eine aktive Ausnutzung einer Schwachstelle in einem X2E-Produkt bedeutet nicht automatisch, dass bei X2E selbst ein Informationssicherheitsvorfall vorliegt. Eine solche Ausnutzung kann beispielsweise ausschließlich ein bei einem Nutzer betriebenes X2E-Produkt betreffen.

Ein zusätzlicher Incident-Response-Prozess bei X2E ist insbesondere einzuleiten, wenn Hinweise auf eine Beeinträchtigung von X2E-Systemen, -Informationen oder -Prozessen bestehen. Hierzu können insbesondere zählen:

- eine tatsächliche Kompromittierung von X2E-Systemen oder X2E-Produkten,
- einen laufenden oder abgeschlossenen unberechtigten Zugriff,
- eine tatsächliche Ausleitung, Offenlegung oder Manipulation von Daten,
- kompromittierte Zugangsdaten,
- eine aktive Schadsoftware- oder Angriffskampagne oder
- sonstige Anzeichen einer aktiven Ausnutzung.

Liegt sowohl ein CVD-/CRA-relevanter Sachverhalt als auch ein Informationssicherheitsvorfall vor, werden CVD-/CRA-Prozess und Incident-Response-Prozess parallel durchgeführt und miteinander koordiniert.

9.1 Interne Eskalation

Bei Hinweisen auf eine aktive Ausnutzung erfolgt eine unverzügliche Eskalation an die für Incident Response und Informationssicherheit zuständigen Funktionen bei X2E.

Dabei werden insbesondere

- die Auswirkungen der Schwachstelle,
- Umfang und Zeitraum einer möglichen Ausnutzung,
- betroffene Produkte, Systeme, Daten und Nutzer,
- erforderliche Sofortmaßnahmen,
- Behebungs- und Mitigationsmaßnahmen sowie
- gegebenenfalls bestehende gesetzliche oder vertragliche Meldepflichten

bewertet.

Die weitere Bearbeitung und Dokumentation eines daraus resultierenden Informationssicherheitsvorfalls richtet sich ergänzend nach den hierfür geltenden internen Verfahren der X2E GmbH.

9.2 Gesetzliche Meldungen und zuständiges CSIRT

Soweit aufgrund einer aktiv ausgenutzten Schwachstelle gesetzliche Melde- oder Informationspflichten bestehen, nimmt X2E die erforderlichen Meldungen nach Artikel 14 CRA vor.

Das für Deutschland zuständige nationale CSIRT bzw. die zuständige nationale Cybersicherheitsbehörde (BSI) wird entsprechend den anwendbaren gesetzlichen Vorgaben eingebunden und über relevante neue Erkenntnisse, Gegenmaßnahmen und Zeitpläne informiert.

Weitere gesetzliche, regulatorische oder vertragliche Meldepflichten, beispielsweise nach Datenschutzrecht oder aufgrund kundenvertraglicher Anforderungen, werden unabhängig davon geprüft und gegebenenfalls parallel erfüllt.

9.3 Verhältnis zum separaten Incident-Meldeweg

Der öffentliche Meldeweg incidentreport@x2e.de dient der Meldung tatsächlicher oder vermuteter Informationssicherheitsereignisse und -vorfälle.

Er ist **kein Ersatz für die PSIRT- oder CSIRT-Kontakte zur Meldung noch nicht ausgenutzter Schwachstellen**.

Meldende Personen müssen eine bereits über PSIRT, CSIRT oder das anonyme Meldeformular übermittelte Schwachstelle nicht erneut an incidentreport@x2e.de melden, wenn sich während der Bearbeitung Hinweise auf eine aktive Ausnutzung ergeben. Die erforderliche interne Eskalation übernimmt in diesem Fall X2E.

Ebenso stellt X2E sicher, dass ein über incidentreport@x2e.de gemeldeter Sachverhalt dem PSIRT oder der Informationssicherheitsorganisation in ihrer CSIRT-Funktion zugeordnet wird, wenn sich bei der Prüfung herausstellt, dass eine Schwachstelle betroffen ist oder zusätzlich ein CVD-Prozess erforderlich wird.

10. Bewertung und Entscheidung nach dem Vier-Augen-Prinzip

Eine eingegangene Schwachstellenmeldung wird nicht allein deshalb beendet oder endgültig zurückgewiesen, weil eine einzelne mit der Bearbeitung betraute Person sie für unbegründet oder abgeschlossen hält.

Die endgültige Entscheidung,

- eine Schwachstelle als nicht valide zurückzuweisen,
- einen CVD-Vorgang ohne weitere Maßnahmen zu schließen oder
- einen validierten CVD-Vorgang als vollständig abgeschlossen zu betrachten,

erfolgt bei X2E nach einem **Vier-Augen-Prinzip** unter Beteiligung von mindestens zwei hierfür geeigneten Personen.

Dadurch sollen Fehlbewertungen vermieden und eine nachvollziehbare, konsistente Bearbeitung von Schwachstellenmeldungen sichergestellt werden.

11. Abschluss des CVD-Prozesses

Ein CVD-Vorgang gilt insbesondere dann als abgeschlossen, wenn einer der folgenden Fälle eingetreten ist:

1. **Unbegründete oder nicht reproduzierbare Meldung:**
   Die gemeldete Schwachstelle konnte nach angemessener Prüfung nicht bestätigt werden oder fällt nicht in den Geltungsbereich dieser Policy.
2. **Schwachstelle behoben und offengelegt:**
   Die Schwachstelle wurde validiert, angemessen behoben oder mitigiert und die erforderliche koordinierte Offenlegung wurde abgeschlossen.
3. **Keine weitere Mitwirkung der meldenden Person:**
   X2E benötigt für die weitere Bearbeitung Informationen oder eine Rückmeldung der meldenden Person und erhält trotz entsprechender Anfrage **30 Kalendertage lang keine Antwort**.

In diesem Fall kann der CVD-Vorgang administrativ geschlossen werden. Liegen X2E dennoch ausreichende Informationen zur Bewertung oder Behebung einer potenziell relevanten Schwachstelle vor, wird diese unabhängig von der fehlenden Rückmeldung angemessen weiterbearbeitet.

4. **Weitergabe an eine andere zuständige Stelle:**
   Es stellt sich heraus, dass X2E für die betroffene Komponente oder Infrastruktur nicht verantwortlich ist und der Vorgang nach Möglichkeit an die tatsächlich zuständige Stelle übergeben oder die meldende Person entsprechend informiert wurde.

Über den Abschluss und den Grund des Abschlusses informiert X2E die meldende Person, sofern ein Kommunikationskanal zur Verfügung steht.

12. Danksagung und Anerkennung

X2E schätzt die verantwortungsvolle Arbeit von Sicherheitsforschenden, die dazu beiträgt, die Sicherheit unserer Produkte und Systeme zu verbessern.

Auf Wunsch der meldenden Person kann X2E nach erfolgreichem Abschluss eines CVD-Prozesses deren **Namen oder Alias öffentlich würdigen**, beispielsweise auf einer Danksagungsseite.

Eine solche Veröffentlichung erfolgt ausschließlich mit ausdrücklicher Zustimmung der betroffenen Person.

Aus dieser allgemeinen CVD-Policy allein entsteht kein Anspruch auf eine finanzielle Vergütung.

13. Verhältnis zu gesetzlichen Verpflichtungen

Diese CVD-Policy soll eine vertrauensvolle und koordinierte Bearbeitung von Schwachstellen ermöglichen. Sie schränkt gesetzliche Pflichten von X2E, insbesondere gegenüber zuständigen Behörden, CSIRTs oder anderen gesetzlich vorgesehenen Stellen, nicht ein.

Der Cyber Resilience Act verpflichtet Hersteller unter anderem dazu, Verfahren für die Behandlung und koordinierte Offenlegung von Schwachstellen vorzuhalten. Die gesetzlichen Berichtspflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle nach Artikel 14 CRA gelten ab dem 11. September 2026; die wesentlichen übrigen CRA-Pflichten gelten grundsätzlich ab dem 11. Dezember 2027.

14. Änderungen dieser Policy

X2E überprüft diese CVD-Policy **mindestens einmal jährlich** auf Aktualität, Wirksamkeit und Übereinstimmung mit den geltenden rechtlichen und technischen Anforderungen.

Darüber hinaus wird die Policy überprüft, wenn

- sich relevante gesetzliche oder regulatorische Anforderungen ändern,
- sich die zuständigen Melde- oder Koordinierungsstellen oder Meldewege ändern,
- wesentliche Änderungen an den betroffenen Produkten, Systemen oder internen Prozessen vorgenommen werden oder
- Erkenntnisse aus bisherigen CVD-Verfahren eine Anpassung erforderlich machen.

Das **Datum der letzten Änderung** wird am Anfang dieser Policy deutlich sichtbar ausgewiesen.