

DIN EN ISO/IEC 29147

ICS 35.030

**Informationstechnik –
Sicherheitstechniken –
Offenlegung von Schwachstellen (ISO/IEC 29147:2018);
Deutsche Fassung EN ISO/IEC 29147:2020**

Information technology –
Security techniques –
Vulnerability disclosure (ISO/IEC 29147:2018);
German version EN ISO/IEC 29147:2020

Technologies de l'information –
Techniques de sécurité –
Divulgateion de vulnérabilité (ISO/IEC 29147:2018);
Version allemande EN ISO/IEC 29147:2020

Gesamtumfang 46 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 29147:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 29147:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 8601	siehe	DIN ISO 8601
ISO/IEC 15408	siehe	DIN EN ISO/IEC 15408
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
ISO IEC 30111	siehe	DIN EN ISO/IEC 30111

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 15408*, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit*

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN EN ISO/IEC 30111, *Informationstechnik — IT-Sicherheitsverfahren — Prozesse für die Behandlung von Schwachstellen*

DIN ISO 8601, *Datenelemente und Austauschformate — Informationsaustausch — Darstellung von Datum und Uhrzeit*

* Es handelt sich hier um eine Normenreihe; dies wird in der Referenzfassung jedoch nicht aufgeführt.

Deutsche Fassung

Informationstechnik —
Sicherheitstechniken —
Offenlegung von Schwachstellen
(ISO/IEC 29147:2018)

Information technology —
Security techniques —
Vulnerability disclosure
(ISO/IEC 29147:2018)

Technologies de l'information —
Techniques de sécurité —
Divulgarion de vulnérabilité
(ISO/IEC 29147:2018)

Diese Europäische Norm wurde vom CEN am 3. Mai 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Abkürzungen	11
5 Konzepte	11
5.1 Allgemeines	11
5.2 Struktur dieses Dokuments	12
5.3 Zusammenhänge mit anderen Internationalen Normen	12
5.3.1 ISO/IEC 30111	12
5.3.2 ISO/IEC 27002	13
5.3.3 Normenreihe ISO/IEC 27034	14
5.3.4 ISO/IEC 27036-3	14
5.3.5 ISO/IEC 27017	14
5.3.6 Normenreihe ISO/IEC 27035	14
5.3.7 Sicherheitsbewertung, Prüfung und Spezifikation	14
5.4 Systeme, Komponenten und Dienstleistungen	14
5.4.1 Systeme	14
5.4.2 Komponenten	14
5.4.3 Produkte	15
5.4.4 Dienstleistungen	15
5.4.5 Schwachstelle	15
5.4.6 Wechselseitige Produktabhängigkeit	16
5.5 Rollen der Beteiligten	16
5.5.1 Allgemeines	16
5.5.2 Anwender	16
5.5.3 Anbieter	16
5.5.4 Berichtersteller	17
5.5.5 Koordinator	17
5.6 Zusammenfassung des Schwachstellenbehandlungsprozesses	18
5.6.1 Allgemeines	18
5.6.2 Vorbereitung	19
5.6.3 Empfang	19
5.6.4 Verifizierung	20
5.6.5 Entwickeln der Problembehebung	20
5.6.6 Freigabe	20
5.6.7 Nach der Freigabe	21
5.6.8 Sperrfrist	21
5.7 Informationsaustausch während der Offenlegung von Schwachstellen	21
5.8 Vertraulichkeit von ausgetauschten Informationen	22
5.8.1 Allgemeines	22
5.8.2 Sichere Kommunikationswege	22
5.9 Beratende Dokumente über Schwachstellen	23

5.10	Ausnutzung einer Schwachstelle	23
5.11	Schwachstellen und Risiko	23
6	Empfangen von Schwachstellenberichten	23
6.1	Allgemeines	23
6.2	Schwachstellenberichte	23
6.2.1	Allgemeines	23
6.2.2	Fähigkeit zum Empfangen von Berichten.....	24
6.2.3	Überwachung	24
6.2.4	Berichtsverfolgung	25
6.2.5	Bestätigung des Berichts	25
6.3	Erstbeurteilung	25
6.4	Weitere Untersuchungen.....	26
6.5	Fortlaufende Kommunikation	26
6.6	Beteiligung von Koordinatoren.....	26
6.7	Betriebssicherheit.....	27
7	Veröffentlichen von beratenden Dokumenten über Schwachstellen	27
7.1	Allgemeines	27
7.2	Beratendes Dokument.....	27
7.3	Zeitplan für die Veröffentlichung von beratenden Dokumenten	27
7.4	Elemente von beratenden Dokumenten	28
7.4.1	Allgemeines	28
7.4.2	Kennungen	29
7.4.3	Datum und Uhrzeit.....	29
7.4.4	Titel.....	29
7.4.5	Überblick	29
7.4.6	Betroffene Produkte.....	29
7.4.7	Vorgesehene Zielgruppe	30
7.4.8	Lokalisierung	30
7.4.9	Beschreibung	30
7.4.10	Auswirkung.....	30
7.4.11	Schweregrad.....	30
7.4.12	Problembehebung.....	31
7.4.13	Verweisungen	31
7.4.14	Anerkennung	31
7.4.15	Kontaktinformationen.....	31
7.4.16	Versionshistorie.....	31
7.4.17	Nutzungsbedingungen	31
7.5	Übermittlung des beratenden Dokuments	31
7.6	Format des beratenden Dokuments.....	32
7.7	Authentizität von beratenden Dokumenten	32
7.8	Problembehebungen.....	32
7.8.1	Allgemeines	32
7.8.2	Authentizität der Problembehebung	32
7.8.3	Durchführung von Problembehebungen.....	32
8	Koordination	33
8.1	Allgemeines	33
8.2	Anbieter mit verschiedenen Rollen	33
8.2.1	Allgemeines	33
8.2.2	Schwachstellenberichterstattung zwischen Anbietern.....	33
8.2.3	Berichten von Schwachstelleninformationen an andere Anbieter.....	34
9	Richtlinie über die Offenlegung von Schwachstellen	34
9.1	Allgemeines	34
9.2	Erforderliche Richtlinienenelemente.....	34
9.2.1	Allgemeines	34

9.2.2	Bevorzugte Kontaktaufnahmeverfahren.....	35
9.3	Empfohlene Richtlinien Elemente	35
9.3.1	Allgemeines	35
9.3.2	Inhalte des Schwachstellenberichts	35
9.3.3	Sichere Kommunikationsoptionen	35
9.3.4	Festlegen von Anforderungen an die Kommunikation.....	36
9.3.5	Anwendungsbereich.....	36
9.3.6	Veröffentlichung	36
9.3.7	Würdigung.....	36
9.4	Optionale Richtlinien Elemente	36
9.4.1	Allgemeines	36
9.4.2	Rechtliche Aspekte.....	36
9.4.3	Zeitplan für die Offenlegung.....	36
	Anhang A (informativ) Beispiele für Richtlinien über die Offenlegung von Schwachstellen.....	37
	Anhang B (informativ) In einem Bericht erforderliche Informationen	38
	Anhang C (informativ) Beispiele für beratende Dokumente.....	39
	Anhang D (informativ) Zusammenfassung der normativen Elemente.....	42
	Literaturhinweise.....	44

Europäisches Vorwort

Der Text von ISO/IEC 29147:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 29147:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2020, und etwaige entgegenstehende nationale Normen müssen bis November 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 29147:2018 wurde von CEN als EN ISO/IEC 29147:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 29147:2014), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- es wurden einige normative Festlegungen hinzugefügt (zusammengefasst in Anhang D);
- zahlreiche organisatorische und redaktionelle Änderungen wurden zur Verdeutlichung vorgenommen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Dieses Dokument soll zusammen mit ISO/IEC 30111 angewendet werden.

Einleitung

Im Kontext der Informationstechnik und Cybersicherheit ist eine Schwachstelle ein Verhalten oder eine Reihe von Bedingungen in einem System, einem Produkt, einer Komponente oder einer Dienstleistung, das bzw. die eine implizite oder explizite Sicherheitsrichtlinie verletzt. Eine Schwachstelle kann als Schwäche oder Gefährdung verstanden werden, die Auswirkungen auf die Sicherheit oder sicherheitstechnische Konsequenzen haben kann. Angreifer nutzen Schwachstellen aus, um die Vertraulichkeit, die Integrität, die Verfügbarkeit, den Betrieb oder einige andere Sicherheitsmerkmale zu gefährden.

Schwachstellen entstehen oftmals durch Fehler eines Programms oder Systems beim sicheren Umgang mit nicht vertrauenswürdigen oder unerwarteten Eingaben. Zu den Ursachen für Schwachstellen zählen Codierungs- oder Konfigurationsfehler, mangelhafte Design-Optionen und unsichere Protokoll- und Formatangaben.

Trotz des beträchtlichen Fortschritts bei der Verbesserung der Softwaresicherheit sind moderne Software und Systeme derart komplex, dass es nahezu unmöglich ist, sie ohne Schwachstellen herzustellen. Risikofaktoren von Schwachstellen sind:

- Einsatz und Abhängigkeit von Systemen, deren Schwachstellen bekannt sind;
- Fehlen von ausreichend Informationen über die Schwachstellen;
- Unwissenheit über bestehende Schwachstellen.

Dieses Dokument beschreibt die Offenlegung von Schwachstellen: Techniken und Richtlinien für Anbieter zum Empfangen von Schwachstellenberichten und zum Veröffentlichen von Informationen über die Problembehebung. Die Offenlegung von Schwachstellen ermöglicht sowohl die Behebung der Schwachstellen als auch bewusstere Risikoentscheidungen. Die Offenlegung von Schwachstellen ist ein kritisches Element für den Support, die Wartung und den Betrieb von Produkten bzw. Dienstleistungen, die aktiven Bedrohungen ausgesetzt sind. Dazu zählen praktisch alle Produkte bzw. Dienstleistungen, die offene Netzwerke wie das Internet nutzen. Die Fähigkeit zur Offenlegung von Schwachstellen ist ein wesentlicher Bestandteil der Entwicklung, des Erwerbs, des Betriebs und des Supports aller Produkte und Dienstleistungen. Der Betrieb ohne die Fähigkeit zur Offenlegung von Schwachstellen stellt für den Anwender ein erhöhtes Risiko dar.

Mit dem Ausdruck „Offenlegung von Schwachstellen“ werden sämtliche Tätigkeiten in Zusammenhang mit dem Empfangen von Schwachstellenberichten und dem Erteilen von Informationen über die Problembehebung beschrieben. Weitere Tätigkeiten wie das Untersuchen und Priorisieren von Berichten, das Entwickeln, Testen und Bereitstellen von Problemlösungen, und das Verbessern einer sicheren Entwicklung werden als „Behandeln von Schwachstellen“ bezeichnet und sind in ISO/IEC 30111 beschrieben. Der Begriff „Offenlegung“ wird auch im engeren Sinne verwendet, um den Vorgang zu bezeichnen, bei dem eine Partei erstmalig über eine Schwachstelle informiert wird (siehe 3.2).

Zu den obersten Zielen bei der Offenlegung von Schwachstellen gehören:

- Risikominderung durch Beheben von Schwachstellen und Informieren der Anwender;
- Minimieren von Schäden und Kosten in Zusammenhang mit der Offenlegung;
- Bereitstellen von ausreichend Informationen für die Anwender, um die durch Schwachstellen entstehenden Risiken zu bewerten;
- Festlegen der Erwartungshaltung, um die kooperative Interaktion und Koordination zwischen den Beteiligten zu erleichtern.

Ziel der in diesem Dokument beschriebenen Prozesse ist es, Risiken, Kosten und Schäden für alle Beteiligten auf ein Mindestmaß zu beschränken. Angesichts des Umfangs der gemeldeten Schwachstellen, des Fehlens exakter und vollständiger Informationen und anderer Faktoren ist es nicht möglich, einen einzigen feststehenden Prozess zu erarbeiten, der für jede auftretende Schwachstelle zutreffend ist.

Die normativen Elemente in diesem Dokument enthalten die Mindestanforderungen, mit denen die funktionale Fähigkeit zur Offenlegung von Schwachstellen geschaffen wird. Anbieter sollten die zusätzlichen informativen Leitlinien dieses Dokuments an ihre eigenen Bedürfnisse sowie an die Bedürfnisse der Anwender und anderer Beteiligter anpassen.

1 Anwendungsbereich

Dieses Dokument enthält Anforderungen und Empfehlungen für Anbieter zur Offenlegung von Schwachstellen in Produkten und Dienstleistungen. Die Offenlegung von Schwachstellen ermöglicht es den Anwendern, technische Schwachstellen nach ISO/IEC 27002:2013, 12.6.1 [1], zu handhaben. Durch die Offenlegung von Schwachstellen können Anwender ihre Systeme und Daten schützen, Abwehrmechanismen priorisieren und Risiken besser einschätzen. Ziel der Offenlegung von Schwachstellen ist es, das Risiko in Verbindung mit der Ausnutzung von Schwachstellen zu mindern. Eine koordinierte Offenlegung von Schwachstellen ist besonders wichtig, wenn mehrere Anbieter betroffen sind. Dieses Dokument enthält:

- Leitlinien für das Empfangen von Berichten über mögliche Schwachstellen;
- Leitlinien für das Offenlegen von Informationen über die Behebung von Schwachstellen;
- spezifische Begriffe für die Offenlegung von Schwachstellen;
- einen Überblick über die Konzepte der Offenlegung von Schwachstellen;
- Betrachtung von Techniken und Richtlinien für die Offenlegung von Schwachstellen;
- Beispiele für Techniken, Richtlinien (Anhang A) und für die Kommunikation (Anhang B).

Andere zugehörige Tätigkeiten, die zwischen dem Empfangen und dem Offenlegen von Schwachstellenberichten stattfinden, sind in ISO/IEC 30111 beschrieben.

Dieses Dokument gilt für Anbieter, die sich dazu entschieden haben, Schwachstellen offenzulegen, um das Risiko für die Anwender der von ihnen angebotenen Produkte und Dienstleistungen zu mindern.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

Schwachstelle

Funktionsverhalten eines Produkts oder einer Dienstleistung, das bzw. die eine implizite oder explizite Sicherheitsrichtlinie verletzt

Anmerkung 1 zum Begriff: In ISO/IEC 27002:2013, 12.6.1 [1] wird der Begriff „technische Schwachstelle“ verwendet, um zwischen dem allgemeineren risikobasierten Konzept einer Schwachstelle und dem in diesem Dokument verwendeten Begriff zu unterscheiden.

3.2

Offenlegung

erstes Bereitstellen von Informationen zu *Schwachstellen* (3.1) an eine Partei, von der angenommen wurde, dass sie vorher nicht über diese Informationen verfügte

3.3

Koordination

Reihe von Aktivitäten, einschließlich Identifizierung und Einbeziehung von interessierten Parteien, Vermittlung, Kommunikation und anderer Planungen zur Unterstützung der *Offenlegung* (3.2) von *Schwachstellen* (3.1)

Anmerkung 1 zum Begriff: Der Begriff „koordinierte Offenlegung von Schwachstellen“ wird angewendet, um einen Offenlegungsprozess zu bezeichnen, der Koordination umfasst.

3.4

Anbieter

Einzelperson oder Organisation, die für das Beheben von Schwachstellen verantwortlich ist

Anmerkung 1 zum Begriff: Ein Anbieter kann der Entwickler, Instandhalter, Hersteller, Produzent, Lieferant, Installateur oder Bereitsteller eines Produkts oder einer Dienstleistung sein.

3.5

Berichtersteller

Einzelperson oder Organisation, die einen *Anbieter* (3.4) oder *Koordinator* (3.6) über eine mögliche *Schwachstelle* (3.1) informiert

Anmerkung 1 zum Begriff: Es gibt keine besonderen Anforderungen, um als Berichtersteller zu fungieren. Berichtersteller können Einzelpersonen, Organisationen, Amateure oder Hobbyisten, Fachleute, Endanwender, Sicherheitsforschungsorganisationen, Anbieter, Regierungen oder Koordinatoren sein.

Anmerkung 2 zum Begriff: Der Begriff „Berichtersteller“ bedeutet nicht, dass es sich um eine einzigartige oder ursprüngliche Entdeckung oder Berichterstellung handelt.

Anmerkung 3 zum Begriff: Berichtersteller können als Forscher bezeichnet werden, unabhängig davon, ob der Berichtersteller explizit Sicherheits- oder Schwachstellenforschung durchführt. Historisch gesehen wird diese Rolle auch als „Entdecker“ bezeichnet.

3.6

Koordinator

Einzelperson oder Organisation, die die *Koordination* (3.3) übernimmt

3.7

Problembehebung

an einem Produkt oder einer Dienstleistung vorgenommene Veränderung, um eine *Schwachstelle* (3.1) zu beseitigen oder abzuschwächen

Anmerkung 1 zum Begriff: Eine Problembehebung erfolgt üblicherweise in Form eines Austauschs von Binärdateien, einer Änderung der Konfiguration oder eines Quellcode-Patches und einer Neukompilierung des Quellcodes. Zu den verschiedenen Begriffen, die für die „Problembehebung“ verwendet werden, gehören Patch, Fix, Update, Hotfix und Upgrade. Schadensminderungsmaßnahmen werden auch Übergangslösungen oder Gegenmaßnahmen genannt.

3.8

beratendes Dokument

Dokument oder Nachricht mit Informationen zu *Schwachstellen* (3.1), die dafür vorgesehen sind, das Risiko zu verringern

Anmerkung 1 zum Begriff: Ein beratendes Dokument ist dafür vorgesehen, Anwender und andere interessierte Parteien über eine Schwachstelle zu informieren, einschließlich, wenn möglich, wie anfällige Systeme identifiziert und Probleme behoben werden können.

4 Abkürzungen

COTS	handelsüblicher Artikel (en: common off-the-shelf)
CRM	Kundenbeziehungsmanagement (en: customer relationship management)
CSIRT	Reaktionsteam für Computersicherheitsvorfälle (en: computer security incident response team)
CVE	gemeinsame Schwachstellen und Gefahren (en: common vulnerabilities and exposures) [9]
CVRF	gemeinsames Format zur Schwachstellenberichterstattung (en: common vulnerability reporting format) [12] [13]
CVSS	gemeinsames Schwachstellenbewertungssystem (en: common vulnerability scoring system) [10]
CWE	gemeinsames Schwächeverzeichnis (en: common weakness enumeration) [11]
HTTP(S)	sicheres Hypertext-Übertragungsprotokoll (en: hypertext transfer protocol (secure))
IKT	Informations- und Kommunikationstechnologie
OpenPGP	open pretty good privacy
OWASP	open web application security project
PoC	Machbarkeitsnachweis (en: proof of concept)
PSIRT	Reaktionsteam für Produktsicherheitsvorfälle (en: product security incident response team)
S/MIME	secure multipurpose internet mail extensions
SQL	strukturierte Abfragesprache (en: structured query language)
TLS	Transportschichtsicherheit (en: transport layer security)

5 Konzepte

5.1 Allgemeines

Zweck dieses Abschnitts ist es, Hintergrundinformationen und Kontext für ein besseres Verständnis der Offenlegung von Schwachstellen zu liefern.

Die Offenlegung von Schwachstellen betrifft verschiedene Beteiligte mit unterschiedlichen Ansichten, Anreizen, Fähigkeiten und verfügbaren Informationen. Darüber hinaus kann die Kommunikation und die Prozesssynchronisation zwischen mehreren Beteiligten schnell kompliziert werden. In der Praxis kann die Offenlegung aufgrund vielfältiger unvorhergesehener Umstände von den in diesem Dokument beschriebenen Tätigkeiten abweichen.

5.2 Struktur dieses Dokuments

Dieses Dokument ist dafür vorgesehen, in seiner Gesamtheit gelesen zu werden, um als Eingabe für die Entwicklung oder Verbesserung von Richtlinien und Prozessen zur Offenlegung von Schwachstellen zu dienen. Die anderen Abschnitte dieses Dokuments sind wie folgt aufgebaut:

- Abschnitt 5: Konzepte;
- Abschnitt 6: Empfangen von Schwachstellenberichten;
- Abschnitt 7: Veröffentlichen von beratenden Dokumenten über Schwachstellen;
- Abschnitt 8: Koordination;
- Abschnitt 9: Richtlinie über die Offenlegung von Schwachstellen.

Die Struktur dieses Dokuments braucht nicht exakt in der vorstehend angegebenen Reihenfolge eingehalten zu werden. Zum Beispiel sollte ein Anbieter idealerweise zuerst eine Richtlinie entwickeln (Abschnitt 9), bevor er anfängt Berichte zu empfangen (Abschnitt 6).

Anhang D enthält eine Zusammenfassung aller normativen Elemente dieses Dokuments.

5.3 Zusammenhänge mit anderen Internationalen Normen

5.3.1 ISO/IEC 30111

ISO/IEC 30111 muss zusammen mit diesem Dokument angewendet werden. Der Zusammenhang zwischen den beiden Internationalen Normen wird in Bild 1 veranschaulicht.

Dieses Dokument enthält Leitlinien für Anbieter, die sie in ihre gewöhnlichen Geschäftsprozesse einbinden, wenn sie Berichte über mögliche Schwachstellen von externen Einzelpersonen oder Organisationen empfangen und wenn sie Informationen über das Beheben von Schwachstellen an die betroffenen Anwender herausgeben.

ISO/IEC 30111 enthält Leitlinien darüber, wie Berichte über mögliche Schwachstellen untersucht, verarbeitet und geklärt werden.

Während sich dieses Dokument mit der Schnittstelle zwischen Anbietern und Berichterstellern befasst, behandelt ISO/IEC 30111 die internen Prozesse des Anbieters einschließlich Sichtung, Untersuchung und Behebung von Schwachstellen, unabhängig davon, ob die Berichtsquelle außerhalb des Anbieters oder innerhalb des anbietereigenen Sicherheits-, Entwicklungs- oder Testteams liegt.