DIN EN ISO/IEC 30111

DIN

ICS 35.030

Informationstechnik – IT-Sicherheitsverfahren – Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019); Deutsche Fassung EN ISO/IEC 30111:2020

Information technology –
Security techniques –
Vulnerability handling processes (ISO/IEC 30111:2019);
German version EN ISO/IEC 30111:2020

Technologies de l'information –
Techniques de sécurité –
Processus de traitement de la vulnérabilité (ISO/IEC 30111:2019);
Version allemande EN ISO/IEC 30111:2020

Gesamtumfang 21 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 30111:2020-07

Nationales Vorwort

Der Text von ISO/IEC 30111:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 30111:2020 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 internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 15408-3	siehe	DIN EN ISO/IEC 15408-3
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000

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 15408-3, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3: Komponenten zur Sicherheitskontrolle*

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

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 30111:2020-07

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 30111

Mai 2020

ICS 35.030

Deutsche Fassung

Informationstechnik — IT-Sicherheitsverfahren — Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019)

Information technology — Security techniques — Vulnerability handling processes (ISO/IEC 30111:2019)

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (ISO/IEC 30111:2019)

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 30111:2020-07

Inhalt

Seite

Europäisches Vorwort ... 3
Vorwort ... 4
Einleitung ... 5
1 Anwendungsbereich ... 6
2 Normative Verweisungen ... 6
3 Begriffe ... 6
4 Abkürzungen ... 6
5 Beziehungen zu anderen Internationalen Normen ... 6
5.1 ISO/IEC 29147 ... 6
5.2 ISO/IEC 27034 (alle Teile) ... 7
5.3 ISO/IEC 27036-3 ... 7
5.4 ISO/IEC 15408-3 ... 8
6 Richtlinie und organisatorisches Rahmenwerk ... 8
6.1 Allgemeines ... 8
6.2 Führung ... 8
6.2.1 Führung und Verpflichtung ... 8
6.2.2 Richtlinie ... 9
6.2.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse ... 9
6.3 Entwicklung der Schwachstellenbehandlungsrichtlinie ... 9
6.4 Entwicklung eines organisatorischen Rahmenwerks ... 10
6.5 CSIRT oder PSIRT des Lieferanten ... 10
6.5.1 Allgemeines ... 10
6.5.2 Auftrag des PSIRT ... 10
6.5.3 Verantwortlichkeiten des PSIRT ... 10
6.5.4 Fähigkeiten von Mitarbeitern ... 12
6.6 Verantwortlichkeiten des Produkt-Geschäftsbereichs ... 12
6.7 Verantwortlichkeiten des Kundendienstes und der Öffentlichkeitsarbeit ... 13
6.8 Rechtsberatung ... 13
7 Prozess für die Behandlung von Schwachstellen ... 13
7.1 Schwachstellenbehandlungsphasen ... 13
7.1.1 Allgemeines ... 13
7.1.2 Vorbereitung ... 14
7.1.3 Eingang ... 14
7.1.4 Verifizierung ... 15
7.1.5 Entwicklung von Abhilfemaßnahmen ... 16
7.1.6 Veröffentlichung ... 17
7.1.7 Nachveröffentlichung ... 17
7.2 Prozessüberwachung ... 17
7.3 Vertraulichkeit der Informationen über die Schwachstelle ... 18
8 Betrachtung der Lieferkette ... 18
Literaturhinweise ... 19

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 30111:2020-07

Europäisches Vorwort

Der Text von ISO/IEC 30111:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 30111:2020 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 30111:2019 wurde von CEN als EN ISO/IEC 30111:2020 ohne irgendeine Abänderung genehmigt.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 30111:2020-07

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) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe http://patents.iec.ch).

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 Technischen Komitee ISO/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *Information security, cybersecurity and privacy protection,* erarbeitet.

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.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 30111:2013), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— einige der normativen Bestimmungen wurden überarbeitet oder hinzugefügt (in Anhang A zusammengefasst);

— organisatorische und redaktionelle Änderungen wurden zur besseren Verständlichkeit sowie zur Harmonisierung mit ISO/IEC 29147:2018 vorgenommen.

Dieses Dokument ist für die Verwendung im Zusammenhang mit ISO/IEC 29147 vorgesehen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 30111:2020-07

Einleitung

In diesem Dokument werden Prozesse für Anbieter für die Bearbeitung von Meldungen über potentielle Schwachstellen bei Produkten und Dienstleistungen beschrieben.

Die Zielgruppe dieses Dokuments besteht unter anderem aus Entwicklern, Lieferanten, Evaluatoren und Anwendern von Produkten und Dienstleistungen der Informationstechnologie. Die folgenden Zielgruppen können dieses Dokument verwenden:

— Entwickler und Lieferanten bei der Reaktion auf Meldungen über tatsächliche oder potentielle Schwachstellen;

— Evaluatoren bei der Bewertung der Sicherheitszusagen, die die Bearbeitungsprozesse der Lieferanten und Entwickler bei Schwachstellen bieten; und

— Anwender bei der Formulierung von Beschaffungsanforderungen an Entwickler, Lieferanten und Integratoren.

Dieses Dokument ist ein Bestandteil von ISO/IEC 29147 zum Empfangszeitpunkt von Meldungen über potentielle Schwachstellen und zum Zeitpunkt der Verteilung von Abhilfemaßnahmen für Schwachstellen (siehe 5.1).

Beziehungen zu anderen Normen sind in Abschnitt 5 aufgeführt.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 30111:2020-07