Belgische Norm

ISO/IEC 27038:2014
EN ISO/IEC 27038:2016
NBN EN ISO/IEC 27038:2016

Informationstechnik - IT-Sicherheitsverfahren - Spezifikation für digitales Schwärzen (ISO/IEC 27038:2014)

Gültig ab 23-09-2016

ICS: 35.040

Bureau for Standarisation
Jozef II-straat 40 bus 6
1000 Brussel

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE69 6790 0009 5178
BIC Code PCHQBEBB

www.nbn.be

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27038

August 2016

ICS 35.040

Deutsche Fassung

Informationstechnik - IT-Sicherheitsverfahren - Spezifikation für digitales Schwärzen (ISO/IEC 27038:2014)

Information technology - Security techniques - Specification for digital redaction (ISO/IEC 27038:2014)

Technologies de l'information - Techniques de sécurité - Spécifications pour la rédaction numérique (ISO/IEC 27038:2014)

Diese Europäische Norm wurde vom CEN am 19. Juni 2016 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 Management-Zentrum des CEN-CENELEC 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, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Ref. Nr. EN ISO/IEC 27038:2016 D

Inhalt

Seite

Europäisches Vorwort

Der Text von ISO/IEC 27038:2014 wurde vom Technischen Komitee ISO/IEC JTC/TC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27038:2016 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2017, und etwaige entgegenstehende nationale Normen müssen bis Februar 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind 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 ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27038:2014 wurde vom CEN als EN ISO/IEC 27038:2016 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. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe von Technischen Komitees ist es Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm werden mindestens 75 % Zustimmung der Mitgliedsorganisationen benötigt.

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

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Einleitung

Manche Dokumente können Informationen enthalten, die einigen Personengruppen nicht offen zugänglich gemacht werden dürfen. Modifizierte Dokumente können für diese Personengruppen freigegeben werden, nachdem eine angemessene Bearbeitung des Originaldokuments erfolgt ist. Diese Bearbeitung kann das Entfernen von Abschnitten, Absätzen oder Sätzen betreffen, sofern erforderlich mit dem Hinweis, dass diese entfernt worden sind. Dieser Vorgang wird als „Schwärzen“ (en: redaction) des Dokuments bezeichnet.

Das digitale Schwärzen von Dokumenten ist ein relativ neuer Bereich des Dokumentenmanagements, der besondere Fragen und potentielle Risiken aufwirft. Wenn digitale Dokumente geschwärzt werden, dürfen die entfernten Informationen nicht wiederherstellbar sein. Demzufolge ist darauf zu achten, dass geschwärzte Informationen dauerhaft aus dem digitalen Dokument entfernt werden (z. B. reicht es nicht, sie in ausgeblendeten Teilen des Dokuments zu verstecken).

Diese Internationale Norm legt Methoden für das digitale Schwärzen von digitalen Dokumenten fest.

Schwärzen kann auch das Entfernen von Dokument-Metadaten sowie das Entfernen von Informationen (z. B. eines Bildes), die in das Dokument importiert wurden, umfassen.

Es kann die Möglichkeit bestehen, geschwärzte Informationen in einem geschwärzten digitalen Dokument anhand ihres Kontextes zu identifizieren. Beispielsweise kann die Länge des Ersatztextes für die geschwärzten Informationen auf die Länge der geschwärzten Informationen und demzufolge auf die Informationen selbst hinweisen. Diese Internationale Norm stellt zwei Kategorien des Schwärzens vor:

— EINFACHES Schwärzen, bei dem der Kontext nicht berücksichtigt wird;

— ERWEITERTES Schwärzen, bei dem der Kontext berücksichtigt wird.

Schwärzungsverfahren können zur Anonymisierung von Informationen in einem Dokument eingesetzt werden, z. B. durch das Entfernen von Namen in Sätzen. Sie können außerdem das Entfernen von Zahlen in Sätzen und deren Ersatz durch „XXX“ umfassen.

EN ISO/IEC 27038:2016 (D)

Informationstechnik — IT-Sicherheitsverfahren — Spezifikation für digitales Schwärzen

1 Anwendungsbereich

Diese Internationale Norm legt Merkmale von Techniken zum digitalen Schwärzen in digitalen Dokumenten fest. Diese Internationale Norm spezifiziert außerdem Anforderungen an Softwaretools zum Schwärzen und an Methoden, mit denen getestet wird, ob das digitale Schwärzen sicher abgeschlossen wurde.

Diese Internationale Norm umfasst nicht das Schwärzen von Daten aus Datenbanken.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

2.1
Anonymisierung
(en: anonymization)
Prozess, durch den personenbezogene Daten (PII, en: personally identifiable information) unwiderruflich so verändert werden, dass ein Betroffener (en: PII principal) nicht mehr direkt oder indirekt identifiziert werden kann, weder durch die verantwortliche Stelle (en: PII controller) allein noch in Zusammenarbeit mit jeder anderen Partei

[QUELLE: ISO/IEC 29100:2011, Begriff 2.2]

2.2
Dokument
(en: document)
aufgezeichnete Informationen, die als eine Einheit behandelt werden können

Anmerkung 1 zum Begriff: Dokumente können Text, Bilder, Video- und Audioinhalte, Metadaten und andere zugehörige Inhalte enthalten.

2.3
personenbezogene Daten
PII
(en: personally identifiable information)
sämtliche Informationen, die (a) verwendet werden können, um den Betroffenen, auf den sich solche Informationen beziehen, zu identifizieren, oder die (b) im direkten oder indirekten Zusammenhang mit dem Betroffenen stehen oder stehen könnten

Anmerkung 1 zum Begriff: Um festzustellen, ob ein Betroffener identifizierbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise vom Datenschutzvertreter, der im Besitz der Daten ist, oder von einer beliebigen anderen Partei verwendet werden können, um diese natürliche Person zu identifizieren.

[QUELLE: ISO/IEC 29100:2011, Begriff 2.9]

2.4
Schwärzen
(en: redaction)
dauerhaftes Entfernen von Informationen aus einem Dokument