DIN EN ISO/IEC 30121

DIN

ICS 35.080 Einsprüche bis 2016-04-26

Entwurf

Informationstechnik – Leitfaden für die Betriebsführung digitaler Forensik (ISO/IEC 30121:2015); Deutsche und Englische Fassung FprEN ISO/IEC 30121:2016

Information technology –
Governance of digital forensic risk framework (ISO/IEC 30121:2015);
German and English version FprEN ISO/IEC 30121:2016

Technologies de l'information –
Gouvernance du cadre de risque forensique numérique (ISO/IEC 30121:2015);
Version allemande et anglaise FprEN ISO/IEC 30121:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-02-26 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 24 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

Nationales Vorwort

ISO/IEC 30121:2015 wurde vom Technischen Komitee ISO/IEC JTC 1/SC 40 „IT Service Management and IT Governance“ erarbeitet. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 30121:2015 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 30121:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitsausschuss NA 043-01-40 AA „IT-Servicemanagement und IT-Betriebsführung“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der FprEN ISO/IEC 30121 beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

– Entwurf –

CEN/TC

Datum: 2016-01

FprEN ISO/IEC 30121:2016

CEN/TC

Sekretariat:

Informationstechnik — Leitfaden für die Betriebsführung digitaler Forensik (ISO/IEC 30121:2015)

Technologies de l'information — Gouvernance du cadre de risque forensique numérique (ISO/IEC 30121:2015)

Information technology — Governance of digital forensic risk framework (ISO/IEC 30121:2015)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: formelle Abstimmung
Dokument-Sprache: D

STD Version 2.7g

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

Inhalt

Seite

Europäisches Vorwort ... **3**

Vorwort ... **4**

Einleitung ... **5**

1 Anwendungsbereich ... **6**

2 Normative Verweisungen ... **6**

3 Begriffe ... **6**

4 Grundsätze ... **7**
4.1 Verantwortung ... **7**
4.2 Strategie ... **7**
4.3 Anschaffung ... **7**
4.4 Leistung ... **7**
4.5 Konformität ... **7**
4.6 Menschliches Verhalten ... **7**

5 Rahmenwerk ... **7**
5.1 Mandat der interessierten Partei ... **7**
5.2 Einrichtung ... **7**
5.3 Bewerten ... **8**
5.4 Leiten ... **8**
5.5 Überwachen ... **8**

6 Prozesse ... **8**
6.1 Archivierungsstrategie ... **8**
6.2 Auffindungsstrategie ... **8**
6.3 Offenlegungsstrategie ... **8**
6.4 Strategie zur digitalen forensischen Fähigkeit ... **8**
6.5 Strategie zur risikobezogenen Übereinstimmung ... **9**

7 Metriken ... **9**
7.1 Allgemeines ... **9**
7.2 Zielindikatoren ... **9**
7.3 Leistungskennzahlen ... **9**
7.4 Unternehmensindikatoren ... **9**

Anhang A (informativ) **Überblick über die Internationale Norm** ... **10**

Literaturhinweise ... **11**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

Europäisches Vorwort

Dieses Dokument (FprEN ISO /IEC 30121:2015) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 40 „IT Service Management and IT Governance“ erarbeitet.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 30121:2015 wurde vom CEN als FprEN ISO/IEC 30121:2016 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

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.

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 ist 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 empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: Foreword — Supplementary information.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, Information technology, Subcommittee SC 40, IT Service Management and IT Governance.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

Einleitung

Organisationen jeder Art sehen sich sowohl internen als auch externen Faktoren und Einflüssen gegenüber, die zum Eintreten von Gerichtsverfahren führen und Anforderungen an die Informationstechnik (IT) und zugehörige Informationssysteme (IS) stellen können, digitale Beweise offenzulegen. Das Eintreten eines Gerichtsverfahrens kann Folge eines unbestimmten, ungeplanten oder unerwarteten Ereignisses sein oder es kann als ein geplantes Vorgehen gegen Angestellte, Wettbewerber oder Dienstleistungserbringer eintreten. Ob ein Risiko signifikant ist oder nicht, wird vom Risikoniveau und der Risikoeinstellung der Organisation abhängig sein. Ihre Risikoeinstellung spiegelt sich in ihren Risikokriterien wider. Da es nahezu sicher ist, dass digitale Beweise gefunden und daher Gegenstand rechtlich begründeter Offenlegung sein werden, sollten Organisationen die Fähigkeit planen und entwickeln, mit derartigen Gerichtsverfahren umzugehen, bevor sie eintreten.

Die Internationale Norm behandelt die besonnene strategische Vorbereitung einer Organisation auf digitale Nachforschungen. Forensische Bereitschaft stellt sicher, dass eine Organisation die geeignete und relevante strategische Vorbereitung getroffen hat, um mögliche Vorgänge von beweiskräftiger Art aufzunehmen. Verfahren könnten als Folge von unvermeidbaren Sicherheitsverstößen, Betrug und Behauptungen, die auf das Ansehen zielen, auftreten. In jeder Situation sollte die IT strategisch eingesetzt werden, um die Wirksamkeit der Verfügbarkeit, Zugänglichkeit und Kosteneffizienz der Beweise zu maximieren.

Es liegt in der Verantwortung des Leitungsgremiums, die strategische Ausrichtung in allen organisationsrelevanten Fragen vorzugeben. Das Leitungsgremium besitzt Kenntnis von den bewährten Vorgehensweisen, die einen allgemeinen Leitfaden in Fragen von Sicherheit und Übereinstimmung (en: certainty and compliance) bereitstellen. Diese Grundsätze können von legalen Mandaten, Normen oder gesellschaftlichen und kulturellen Notwendigkeiten herrühren. Die Grundsätze in dieser Internationalen Norm entstammen ISO/IEC 38500 für den Leitfaden für bewährte Praktiken bei der Führung (Governance) in der Informationstechnik (Abschnitt 4).

Die Grundsätze erfordern eine Umsetzung. Die Ziele des Leitungsgremiums sind die Bewertung von Vorschlägen und Plänen, die Überwachung der Leistung und Konformität und die Ausrichtung von Strategien und Politiken. Die interessierten Parteien einer Organisation können das Mandat zur Führung erteilen und das Leitungsgremium ist der endgültige Risikoeigner. Ein Rahmenwerk für die Steuerung des digitalen forensischen Risikos wird durch die Risikoeigner festgelegt, die geeignete Maßnahmen ergreifen, um die strategische Ausrichtung der Organisation sicherzustellen. Daher ist das strategische Ziel die Umsetzung der Grundsätze und die Sicherstellung einer geeigneten Vorbereitung auf eine digitale Nachforschung (Abschnitt 5).

Das Rahmenwerk erfordert strategische Prozesse, um leitenden Angestellten und Mitgliedern der obersten Leitung eine Ausrichtung zu vermitteln. Die strategischen Prozesse werden ausgewählt, um einen geeigneten Anwendungsbereich sicherzustellen und umfassen vorwiegend Archivierung, Auffindung, Offenlegung, Fähigkeit und Übereinstimmung mit Risikokriterien (Abschnitt 6).

Die aus den Prinzipien abgeleiteten Ziele sind durch Zielindikatoren (KGI, en: Key Goal Indicator) messbar, die aus den Strategien abgeleiteten strategischen Ziele sind durch Leistungskennzahlen (KPI, en: Key Performance Indicator) messbar und die Abweichung der Werte zwischen KGI und KPI ist ein Hinweis auf die Unternehmensleistung einer Organisation (KBI) (Abschnitt 7).

Diese Internationale Norm sollte in Verbindung mit dem Vokabular in ISO Guide 73:2009; ISO/IEC 35802, *Information technology — Governance of IT framework and model*; und ISO/IEC 38500, *Information technology — Governance of IT for the organization*, angewendet werden

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03

1 Anwendungsbereich

Diese Internationale Norm bietet einen Leitfaden für Leitungsgremien von Organisationen (einschließlich der Inhaber, Vorstände, Direktoren, Partner, leitende Angestellte, oder ähnliches) um die Organisation für digitale Nachforschungen vorzubereiten. Diese Internationale Norm gilt für die Entwicklung der strategischen Prozesse (und Entscheidungen) im Zusammenhang mit der Rückhaltung, Verfügbarkeit, Zugriff und Kosteneffizienz von digitalen Beweisen. Diese Internationale Norm gilt für alle Arten und Größen von Organisationen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. 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 38500, *Information technology — Governance of IT for the organization*

ISO Guide 73:2009, *Risk management — Vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 38500, ISO Guide 73:2009 und die folgenden Begriffe.

3.1
digitaler Beweis
Informationen oder Daten, die in binärer Form gespeichert oder übermittelt werden, und die als Beweise verwendet werden können

[QUELLE: ISO/IEC 27037:2012, 3.5]

3.2
Leitungsgremium
Person oder Personengruppe, die gegenüber den interessierten Parteien für die Leistung und Konformität der Organisation verantwortlich ist

[QUELLE: ISO/IEC TR 38502:2014, 2.9]

3.3
digitale Forensik
wissenschaftliche Aufgaben, Techniken und Praktiken, die bei der Untersuchung gespeicherter oder übermittelter binärer Informationen oder Daten zu rechtlichen Zwecken angewendet werden

3.4
strategisches Risiko
Wirkung von Unsicherheit auf Ziele

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 30121:2016-03