

# DIN EN ISO/IEC 29147:2020-08 (D)

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

---

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 Richtlinienelemente .....	34
9.2.1	Allgemeines.....	34
9.2.2	Bevorzugte Kontaktaufnahmeverfahren.....	35

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