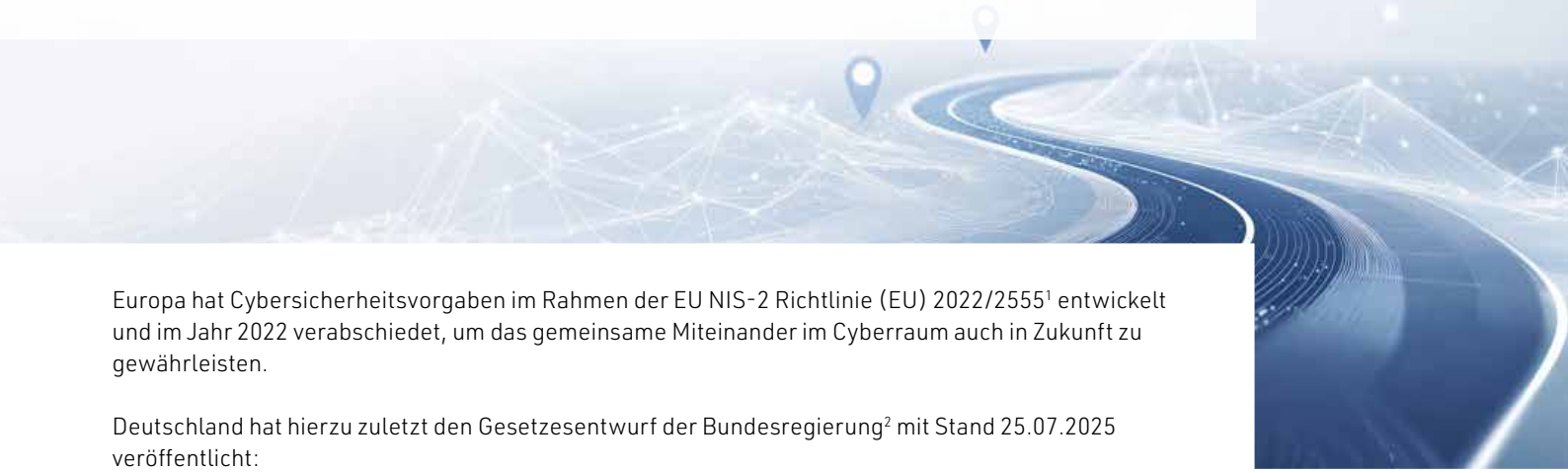
NIS2UMSUCG

Schulungspflicht für Geschäftsleitungen nach NIS-2



Europa hat Cybersicherheitsvorgaben im Rahmen der EU NIS-2 Richtlinie (EU) 2022/2555[1] entwickelt und im Jahr 2022 verabschiedet, um das gemeinsame Miteinander im Cyberraum auch in Zukunft zu gewährleisten.

Deutschland hat hierzu zuletzt den Gesetzesentwurf der Bundesregierung[2] mit Stand 25.07.2025 veröffentlicht:
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

In **NIS2UmsuCG § 38 Absatz (3)** wird dabei eine Schulungspflicht für Geschäftsleitungen von besonders wichtigen und wichtigen Einrichtungen vorgegeben, um den Anforderungen nach Satz (1) und (2) zur Umsetzungs- und Überwachungspflicht zu entsprechen.

SCHULUNGSPFLICHT FÜR GESCHÄFTSLEITUNGEN BESONDERS WICHTIGER UND WICHTIGER EINRICHTUNGEN

§ 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

(vgl. Seite 47 / 213)

In der **Gesetzesbegründung** wird dabei auf den Umfang und die Regelmäßigkeit näher eingegangen.

Hier wird dargelegt, dass eine Regelmäßigkeit durch Umsetzen einer entsprechenden Schulung gegeben ist, wenn diese alle drei Jahre angeboten wird.

ZU § 38 (UMSETZUNGS-, ÜBERWACHUNGS- UND SCHULUNGSPFLICHT FÜR GESCHÄFTSLEITUNGEN BESONDERS WICHTIGER UND WICHTIGER EINRICHTUNGEN)

*Absatz 3 dient der Umsetzung von Artikel 20 Absatz 2 der NIS-2-Richtlinie im Hinblick auf Geschäftsleitungen. Wichtige und besonders wichtige Einrichtungen werden aufgefordert, derartige Schulungen für alle Beschäftigten anzubieten. Als „regelmäßig" im Sinne dieser Vorschrift gelten Schulungen, die **mindestens alle drei Jahre** angeboten werden. Für Einrichtungen der Bundesverwaltung gilt abweichend § 43 Absatz 2.*

(vgl. Seite 175 / 213)

An der nachfolgenden Stelle wird durch die Berechnung der Veränderung des jährlichen Erfüllungsaufwands und der nachfolgenden Begründung der Kalkulation dargelegt, dass der Zeitaufwand zur Erfüllung der Anforderungen an

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[2] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

HISOLUTIONS

IHR ANSPRECHPARTNER

Manuel Atug
Principal

info@hisolutions.com
Fon +49 30 533 289 0

eine entsprechende Schulung mit einem Umfang von vier Stunden anzusetzen ist.

VORGABE 4.2.4 (WEITERE VORGABE): REGELMÄSSIGE SCHULUNGEN (BESONDERS WICHTIGE UND WICHTIGE EINRICHTUNGEN); § 38 ABSATZ 3 IN VERBINDUNG MIT § 28 BSIG-E

Veränderung des jährlichen Erfüllungsaufwands:

Fallzahl	*Zeitaufwand pro Fall (in Stunden)*
150.000	*4*
3.000.000	*1*

*Der Regelungsentwurf sieht vor, dass **Geschäftsleitende aller adressierten Einrichtungen regelmäßig Cybersicherheitsschulungen absolvieren müssen**; die übrigen Mitarbeitenden sollen regelmäßig an solchen Schulungen teilnehmen (vgl. § 38 Absatz 3 BISG-E).*

*Das Umsetzungsgesetz (vgl. Gesetzesbegründung) und die NIS-2-Richtlinie (vgl. Artikel 20 Absatz 2) machen hier nur allgemeine Forderungen von Schulungen zum Erwerb allgemeiner Kenntnisse und Fähigkeiten, um unter anderem Risiken im Bereich der Cybersicherheit zu erkennen und zu bewerten. So sollen die Schulungen zwar regelmäßig absolviert werden, eine konkrete Periodizität wird allerdings nicht vorgegeben. Zusätzlich ist unklar, **wer im Unternehmen konkret zu den Geschäftsleitenden zählt**. Schließlich ist nicht zu erkennen, wie umfangreich die speziellen Cybersicherheitsschulungen sein müssen. **Theoretisch können das Kurzschulungen von wenigen Stunden sein, oder aufgrund der komplexen Thematik mehrtägige Seminare.***

*Es wird geschätzt, dass jährlich rund 298.500 Geschäftsleitende Schulungen absolvieren. Dies liegt der freien Annahme zugrunde, dass einmal im Jahr zehn leitende Beschäftigte je Unternehmen an einer solchen Schulung teilnehmen (29.850 Unternehmen * 10). Es ist jedoch davon auszugehen, dass Unternehmen aus eigenem Interesse zum Teil bereits heute ihren führenden Mitarbeitenden Cybersicherheitsschulungen anbieten. Es wird daher angenommen, dass dies für 50 % der Unternehmen zutrifft, sodass davon auszugehen ist, dass sich für rund 150.000 leitende Beschäftigte eine Veränderung des Status quo ergibt.*

*Des Weiteren wird frei angenommen, dass es sich im Durchschnitt um eine **halbtägige Schulung** handelt (vier Stunden).*

*Hinsichtlich der **Schulung der Mitarbeitenden** wird angenommen, dass die Schulungen **weniger zeitaufwendig** sind, als die durch die Mitglieder der Leitungsorgane absolvierten.*

(vgl. Seite 125 ff. / 213)

INHALTE DER SCHULUNG FÜR GESCHÄFTSLEITUNGEN NACH NIS-2

In **NIS2UmsuCG § 38 Absatz (3)** wird eine Schulungspflicht für Geschäftsleitungen von besonders wichtigen und wichtigen Einrichtungen vorgegeben, um den Anforderungen nach Satz (1) und (2) zur Umsetzungs- und Überwachungspflicht zu entsprechen.

HISOLUTIONS INDIVIDUALISIERUNG DER SCHULUNG

HiSolutions berücksichtigt in der Individualisierung der Schulung weitere regulatorische Anforderungen aus dem jeweiligen Sektor bzw. der jeweiligen Branche in Abstimmung mit dem Bedarf der betroffenen Geschäftsleitung.

Für die Luftsicherheitsgesetzgebungen werden beispielsweise die Luftsicherheit und Flugsicherheit aufgrund der Anforderungen der DVO 2019/1583 (Cyberluftsicherheitsprogramm CLSP bzw. Luftsicherheit) und DelVO 2022/1645, sowie DelVO 2022/1645 (EASA PART IS bzw. Flugsicherheit) berücksichtigt. So wird im Rahmen der Einführung in das IS-Risikomanagement der Bezug zur Luftsicherheit und bei der Informationssicherheit der Bezug auf Luftsicherheit und Flugsicherheit abgebildet.

Nachfolgend werden die Inhalte, sowie Umfang, Aufbau und Struktur der Schulung dargelegt.

AUFBAU UND STRUKTURIERUNG DER SCHULUNG

Zeit	Inhalte
15 min	Begrüßung und Vorstellung
15 min	Einführung in das NIS2UmsuCG
15 min	Erklärung „besonders wichtige und wichtige Einrichtungen“
10 min	Pflichten der Geschäftsleitungen, Haftungs- und Bußgeldvorschriften im Kontext
10 min	Einführung IS-Risikomanagement
15 min	Identifikation von IS-Risiken
15 min	Analyse von IS-Risiken
15 min	Bewertung von IS-Risiken
15 min	Behandlung von IS-Risiken
15 min	Überwachung des IS-Risikomanagements
30 min	Umzusetzende Maßnahmen zur Behandlung von IS-Risiken um Kontext von NIS2UmsuCG § 30
30 min	Gesprächsgeführtes Üben von 2-3 Fallbeispielen zum Risikomanagement
30 min	Diskussion für inhaltliche Fragen
15 min	Verabschiedung und Feedback