NIS2 DEEP DIVE: ANFORDERUNGEN AN WICHTIGE UND BESONDERS WICHTIGE EINRICHTUNGEN SOWIE BETREIBER KRITISCHER ANLAGEN

BAIT 1
(MaRisk AT 7.2, AT 4.2)
IT-Strategie

BAIT 2
(MaRisk AT 7.2, AT 4.3, AT 5)
IT-Governance

BAIT 3
(MaRisk AT 7.2, AT 4.4)
Informationsrisikomanagement

BAIT 4
(MaRisk AT 7.2, AT 7.1, AT 4.4)
Informationssicherheitsmanagement

BAIT 5
(MaRisk AT 7.2)
Operative Informationssicherheit

BAIT 6
(MaRisk AT 7.2, AT 4.3)
Identitäts- und Rechtemanagement

BAIT 7
(MaRisk AT 7.2, AT 8.2)
IT-Projekte und Anwendungen

BAIT 8
(MaRisk AT 7.2)
IT-Betrieb

BAIT 9
(MaRisk AT 9)
(IT-) Auslagerungen und (IT-) Fremdbezug

BAIT 10
(MaRisk AT 9)
(IT) Notfallmanagement

Domain 01
ICT strategy management

Domain 02
IT governance management & Internal controls system

#	NIS2-Anforderung	NIS2-Referenz
02-01	Sicherstellung der Einrichtung von technischen und organisatorischen Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.	§30 Abs. 1 NIS2
02-02	Sicherstellung von technisch-organisatorischen Maßnahmen, die den Stand der Technik einhalten und die die einschlägigen europäischen und internationalen Normen berücksichtigen	§33 Abs. 2 NIS2
02-03	Geschäftsleitungen sind verpflichtet, die Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.	§38 Abs. 1 NIS2

Domain 03
Internal audit and compliance management

#	NIS2-Anforderung	NIS2-Referenz
03-01	Bestimmung der NIS2-Relevanzgemäß §28 und Registrierung des Unternehmens als besonders wichtige oder wichtige Einrichtung oder als Domain-Name-Registry-Dienstleistanbieter	§33 Abs. 1 NIS2
03-02	Übermittlung der Pflichtangaben durch Betreiber kritischer Anlagen gemäß §33 Abs. 2 NIS2	§33 Abs. 2 NIS2
03-03	Regelmäßige Überprüfung und ggf. Neuübermittlung der Einstufungskriterien und Angaben	§33 Abs. 5 NIS2
03-04	Sicherstellung, das nach § 58 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwendet werden, wenn diese über eine Cybersicherheitszertifizierung	§30 Abs. 6 NIS2
03.05	Vorschlag von branchenspezifischen Sicherheitsstandards zur Gewährleistung der Anforderungen	§30 Abs. 8 & 9 NIS2
03-06	Betreiber kritischer Anlagen müssen ggf. Auch aufwendigere technisch-organisatorische Maßnahmen umsetzen	§31 Abs. 1 NIS 2
03-07	Auf Anweisung des BSI sind Empfänger von Diensten über Sicherheitsvorfälle und ggf. Abhilfemaßnahmen zu unterrichten	§35 Abs. 1 & 2 NIS 2
03-08	Betreiber kritischer Anlagen übermitteln dem BSI die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das BSI kann die Vorlage eines geeigneten Mängelbeseitigungsplanes und die Beseitigung der Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen	§39 Abs. 1 NIS 2
03-09	Betreiber kritischer Anlagen haben den erstmaligen Einsatz kritischer Komponenten dem BSI vor ihrem Einsatz anzuzeigen.	§42 Abs. 1 NIS 2

Domain 04
ICT asset & architecture management

Domain 05
ICT risk management

#	NIS2-Anforderung	NIS2-Referenz
05-01	Konzepte in Bezug auf die Risikoanalyse	§30 Abs. 2 Ziffer 1 NIS2
05-02	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-maßnahmen im Bereich der Sicherheit in der Informationstechnik	§30 Abs. 2 Ziffer 6 NIS2
05-03	Die Geschäftsleitungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagement-praktiken im Bereich der Sicherheit in der Informations-technik und die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste zu erwerben.	§38 Abs. 3 NIS2

Domain 06
Information security & human resource (security) management

#	NIS2-Anforderung	NIS2-Referenz
06-01	Konzepte in Bezug auf die Sicherheit in der Informationstechnik	§30 Abs. 2 Ziffer 1 NIS2
06-02	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik	§30 Abs. 2 Ziffer 7 NIS2
06-03	Maßnahmen zur Sicherheit des Personals	§30 Abs. 2 Ziffer 9 NIS2

Domain 07
IT configuration management

Domain 08
Cryptography, Certificates & Key Management

#	NIS2-Anforderung	NIS2-Referenz
08-01	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,	§30 Abs. 2 Ziffer 8 NIS2

Domain 09
Secure network & infrastructure management

Domain 10
Backup

#	NIS2-Anforderung	NIS2-Referenz
10-01	Maßnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall	§30 Abs. 2 Ziffer 3 NIS2

Domain 11
Security testing

#	NIS2-Anforderung	NIS2-Referenz
	Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach § 30 Absatz und § 31 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Das BSI kann die Vorlage eines geeigneten Mängelbeseitigungsplanes und die Beseitigung der Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen	§39 Abs. 1 NIS2

Domain 12
Threat-led penetration testing

Domain 13
Logging

Domain 14
Data and ICT system security

#	NIS2-Anforderung	NIS2-Referenz
	Verwendung von Lösungen zur gesicherten Sprach-, Video- und Textkommunikation	§30 Abs. 2 Ziffer 10 NIS2

Domain 15
Physical and environmental security

Domain 16
Vulnerability & patch management

#	NIS2-Anforderung	NIS2-Referenz
06-01	Sicherheitsmaßnahmen zum Management und Offenlegung von Schwachstellen	§30 Abs. 2 Ziffer 5 NIS2

Domain 17
Identity and access management

#	NIS2-Anforderung	NIS2-Referenz
06-01	Konzepte für die Zugriffskontrolle	§30 Abs. 2 Ziffer 9 NIS2
	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung,	§30 Abs. 2 Ziffer 10 NIS2

Domain 18
ICT change management

Domain 19
IT project & project portfolio management

Domain 20
Acquisition, development and maintenance of ICT systems and EUA/IDP

#	NIS2-Anforderung	NIS2-Referenz
06-01	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen,	§30 Abs. 2 Ziffer 5 NIS2

Domain 21
ICT incident management

#	NIS2-Anforderung	NIS2-Referenz
10-01	Maßnahmen zur Bewältigung von Sicherheitsvorfällen	§30 Abs. 2 Ziffer 2 NIS2
	Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vor zusehen. Dabei soll der Stand der Technik eingehalten werden.	§31 Abs. 2 NIS2
	Übermittlung von frühen Erstmeldungen, Meldungen, ggf. Zwischenmeldungen oder Fortschrittsmeldungen und Abschlussmeldungen zu erheblichen Sicherheitsvorfällen an die Meldestelle	§32 Abs. 1 NIS2

Domain 22
Monitoring, Availability, Capacity & Performance Management

#	NIS2-Anforderung	NIS2-Referenz
10-01	Maßnahmen für das Management von Anlagen	§30 Abs. 2 Ziffer 9 NIS2

Domain 23
ICT outsourcing & third-party risk management

#	NIS2-Anforderung	NIS2-Referenz
23-01	Maßnahmen zur Sicherheit der Lieferkette	§30 Abs. 2 Ziffer 4 NIS2

Domain 24
Subcontracting management

#	NIS2-Anforderung	NIS2-Referenz
24-01	Maßnahmen zur Sicherheit der Lieferkette **einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleanbietern**	§30 Abs. 2 Ziffer 4 NIS2

Domain 25
ICT provider & service level management

Domain 26
ICT business continuity management

#	NIS2-Anforderung	NIS2-Referenz
10-01	Maßnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	§30 Abs. 2 Ziffer 3 NIS2
	Gegebenenfalls Verwendung von gesicherten Notfallkommunikationssysteme innerhalb der Einrichtung	§30 Abs. 2 Ziffer 10 NIS2

© Copyright 2024 | Dr. Marlen Hofmann| Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt. Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.