cryptas

we protect identities.

NIS2 – Was ist zu tun?

Konkrete Anforderungen an Betroffene

27.7.2023

Author: DI (FH) Stefan Bumerl
stefan.bumerl@cryptas.com

Document Version: 1.0
Creation Date: 7/2023

+Update BSI-Gesetz

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

About CRYPTAS

SPECIALIST FOR PKI, STRONG AUTHENTICATION, ENCRYPTION, LAWFUL SIGNATURES AND DIGITAL IDENTITIES

Own solutions around Digital Signatures, Virtual Smart Card, clientless Smart Card access, Self-Service Processes, PKI, OCSP++...

CONSULTING, DEVELOPMENT, INTEGRATION, SERVICES

Topics: eSignature, Smart Cards, PKI, FIM, Key Management, HSM, Encryption...

WIEN, GRAZ, DÜSSELDORF, HENGELO AND STOCKHOLM

Successful in crypto-business since 2003; main markets D/A/CH, Typical Project Size: 1.000 to 300.000 Users

> 50.000 CUSTOMERS / ~100 COUNTRIES /

Verticals: banking, insurance, energy provider, health, industry, government...

eIDAS TRUST CENTER

Qualified Trust Center with focus on Qualified Onboarding, eIDAS Online Contracting, Video-Legitimation, eIDAS Remote Services

Millions Transactions per Day

Thousands Enrollments per Day

> 4 Millions qualified certificates issued to 163 nationalities

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

Wer ist betroffen?

Behörden nominieren auf Basis Risiko-Analyse

NIS2 - Annex 1	NIS2 - Annex 2	RCE
Energie	Post und Kurier	Energie
Gesundheit	Entsorgung	Gesundheit
Transport	Chemikalien	Transport
Banken und Finanz	Ernährung	Banken und Finanz
Wasser und Abwasser	Herstellende Industrie	Wasser und Abwasser
Digitale Infrastruktur	Digitale Dienste	Digitale Infrastruktur
ICT Service Provider	Forschung	Ernährung
Öffentliche Verwaltung		Öffentliche Verwaltung
Raumfahrt		Raumfahrt

EU KMU-Regeln

- Mittlere: >50 MA oder >10M€ Umsatz/Bilanz
- Große: >250 MA oder >50M€ Umsatz bzw. 43M€ Bilanz

Sonderfälle!

- Unabhängig von Größe laut Definition NIS2
- Monopole, grenzüberschreitend, kritisch...

Sektor	groß	mittel	klein
Annex 1	wesentlich	wichtig	
Annex 2	wichtig	wichtig	

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

Scope und Ziele der NIS2-Richtlinie

"In dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll"

Policies	Kryptografie
Effektivität	Zugangskontrolle
All-Risk-Ansatz	Multi-Faktor-Auth.
Training	Verschlüsselung
Supply Chain	Personal
Incident Management	Business Continuity
Asset Management	Bewältigung

! ACHTUNG !

„Alle Netz- und Informationssysteme, die für den Betrieb oder für die Erbringung der Dienste benutzt werden."

Scope ist gesamte Organisation

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

NIS2 (EU 2022/2555) Richtlinie - Inhalt

+ Kapitelüberisicht

I. ALLGEMEINE BESTIMMUNGEN
II. KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT
III. ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE
IV. RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT
V. ZUSTÄNDIGKEIT UND REGISTRIERUNG
VI. INFORMATIONSAUSTAUSCH
VII. AUFSICHT UND DURCHSETZUNG
VIII. DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE
IX. SCHLUSSBESTIMMUNGEN

+ Anhänge

I. SEKTOREN MIT HOHER KRITIKALITÄT ("Wesentliche Dienste" / "Essential")
II. SONSTIGE KRITISCHE SEKTOREN ("Wichtige Dienste" / "Important")
III. ENTSPRECHUNGSTABELLE

Pflicht für Mitgliedstaaten:
Einrichten von Anlaufstellen, CSIRT...

Pflicht für Betroffene:
Cybersicherheitsrisikomanagement

Pflichten zum Austausch von
Cybersicherheitsinformationen

Pflicht für Mitgliedstaaten:
Aufsichts- und Durchsetzungspflichten

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Artikel 21: Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity (Backup-Mangement, Notfall- und Krisenmangement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen
- Cyberhygiene and Schulungen
- Verfahren zur Bewertung der Wirksamkeit
- Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Zugriffskontrolle
- Multi-Faktor-Authentifizierung, gesicherte Kommunikationswege

Organizational Measures

Management systems like ISMS and BCMS

Technological Measures

Implementing "State of the Art" mechanisms

Attack detection

Utilizing SIEM or CSIRT/SOC

→ Niveau: "Stand der Technik" und ggf. einschlägige Standards

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

EU

Artikel 24: Europäischen Schemata für die Sicherheitszertifizierung

- Option für verpflichteten Einsatz von speziellen
  - IKT-Produkten
  - IKT-Diensten
  - IKT Prozesse

  durch Mitgliedstaaten oder Kommission falls unzureichendes Niveau der Cybersicherheit festgestellt wird

- ENISA (EU) 2019/881 bildet hier eine Basis (vgl. eIDAS)

- „Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen“

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Technikklausel „Stand der Technik"

- Generell:
  Die Anforderungsschwelle des Standes der Technik gilt als erreicht, wenn das tatsächlich gesetzte Verhalten fortschrittlich ist, auf einschlägigen wissenschaftlichen Erkenntnissen beruht, und seine Funktionstüchtigkeit erprobt und erwiesen ist."

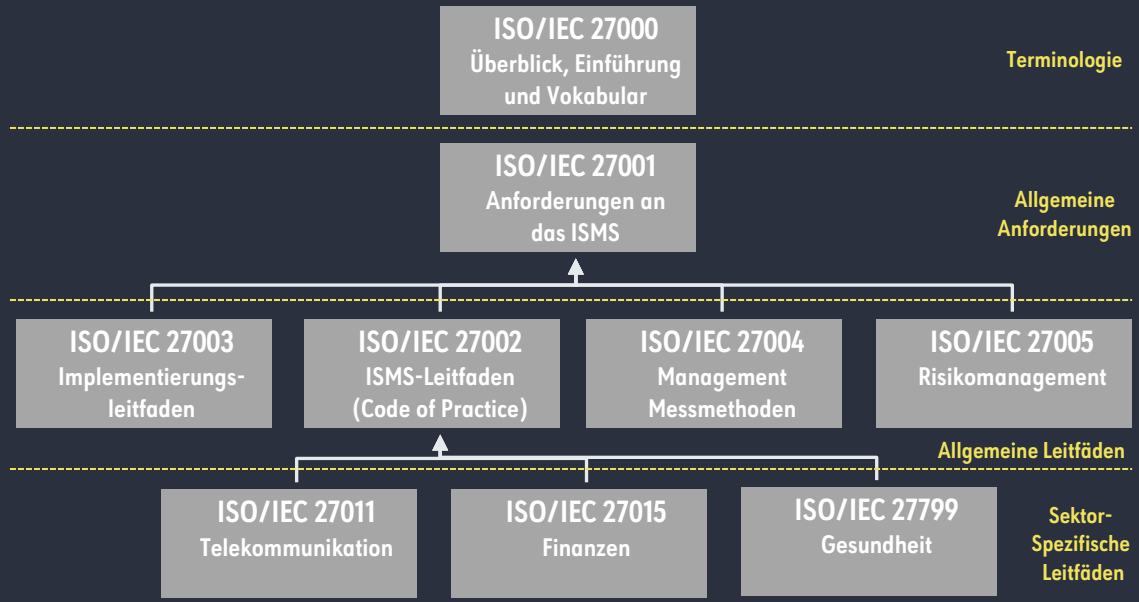
- Fortschrittlichkeit:
  - macht den Vergleich mit alternativen Verhaltensweisen notwendig
  - ... wenn das damit verfolgte Ziel im konkreten Fall besser erreicht werden kann...
  - Verhältnismäßigkeit ist zu berücksichtigen

- ISO 27000 – Reihe als Stand der Technik anerkannt

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

ISO 27000-Reihe als Grundlage



Unterstützende Normen

ISO/IEC 27010 Inter-sector Communication	ISO/IEC 27014 Governance Framework
ISO/IEC 27031 Business Continuity	ISO/IEC 27032 Cyber Security
ISO/IEC 27033 Network Security	ISO/IEC 27034 Application Security
ISO/IEC 27035 Security Incident Management	ISO/IEC 27036 Outsourcing
ISO/IEC 27037 Digital Evidence	ISO/IEC 27099 PKI Trust Services

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

BSI – Gesetz: §2 Begriffsbestimmungen

36. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

    a) in informationstechnischen Systemen, Komponenten oder Prozessen oder

    b) bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen;

37. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

BSI – Gesetz: §3 Aufgaben des Bundesamtes

14. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf;

26. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;

27. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände;

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

BSI – Gesetz: §30 Risikomanagementaufgaben

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe der Einrichtung oder des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

BSI – Gesetz: §30 Risikomanagementaufgaben

(4) Maßnahmen nach Absatz 1 müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die informationstechnischen Systeme, Komponenten und Prozesse und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,

2. Bewältigung von Sicherheitsvorfällen,

3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,

4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,

5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

BSI – Gesetz: §30 Risikomanagementaufgaben

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,

7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,

8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,

9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,

10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

BSI – Gesetz: §30 Risikomanagementaufgaben

(8) Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 berücksichtigt die Einrichtung oder der Betreiber die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.

(12) Besonders wichtige Einrichtungen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Diese müssen Durchführungsrechtsakte der Europäischen Kommission so berücksichtigen, dass sie nicht im Widerspruch zu den dort genannten Anforderungen stehen sowie darin enthaltende Vorgaben nicht unterschritten werden. Das Bundesamt stellt auf Antrag fest, ob diese branchenspezifisch und geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

BSI – Gesetz: §38 Pflichten für Geschäftsleiter

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.

(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Satz 1 gilt nicht für Geschäftsleiter besonders wichtiger Einrichtungen des Teilsektors Zentralregierung des Sektors öffentliche Verwaltung.

(3) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(4) Die Geschäftsleiter von besonders wichtigen Einrichtungen und wichtigen Einrichtungen müssen und deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Ausblick: Praktische Empfehlungen

	User	Device	Service	Software	Data
Authenticity	MFA	Certificates	Certificates	Code Signing	Dig Signatur
Integrity	Onboarding	Cert Mgmt.	Cert Mgmt.	Code Signing	Dig Signatur
Confidentiality	Certificates	Certificates	Certificates	Encryption	Encryption
Accountability	Cred Mgmt.	Cert Mgmt.	Cert Mgmt.	Cert Mgmt.	Cert Mgmt.
Availability	Decoupling	Validation	Validation	X	Backup

→ (Qualified) Trust Service – PKI als zentrale Basis!

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

infinigate
spark your growth

pwc

THALES
Building a future we can all trust

Fragen

?

cryptas
we protect identities.

infinigate
spark your growth

pwc

THALES
Building a future we can all trust

Vielen Dank für Ihre Teilnahme!

Für weitere Fragen oder Anregungen stehen gerne zur Verfügung:

Mareike Gehrmann / Infinigate :	mareike.gehrmann@infinigate.de
Mailin von Knobelsdorff / PwC:	mailin.von.knobelsdorff@pwc.com
Andre Glenzer / PwC:	andre.glenzer@pwc.com
Stefan Bumerl / CRYPTAS:	stefan.bumerl@cryptas.com
Karl Heinz Mayer / CRYPTAS:	karl-heinz.mayer@cryptas.com

Nächstes Webinar: 10.08.2023, 11:00:

Stand der Technik und praktische Umsetzung der NIS-2 Erfordernisse

https://attendee.gotowebinar.com/register/5634539611113943 91