CoreTec

Netz- und Informationssystem-sicherheitsgesetz (NISG)

Prüfungsgrundlagen

- Richtlinie (EU) 2016/1148
  des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
- NIS-Gesetz
  Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)
- NIS-Verordnung
  Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV)
- Verordnung über qualifizierte Stellen
  Verordnung des Bundesministers für Inneres zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV)

- NIS Fact Sheets
- NIS Fact Sheet 3/2021 – Version 2
  Erläuterungen zur Aufstellung von Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste
- NIS Fact Sheet 9/2022
  Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste
- NIS Fact Sheet 7/2019 – Version 2
  Qualifizierte Stellen

Quelle: nis.gv.at

Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Kategorien und Sicherheitsmaßnahmen der NISV

1. Governance und Risikomanagement
2. Umgang mit Dienstleistern, Lieferanten und Dritten
3. Sicherheitsarchitektur
4. Systemadministration
5. Identitäts- und Zugriffsmanagement
6. Systemwartung und Betrieb
7. Physische Sicherheit
8. Erkennung von Vorfällen
9. Bewältigung von Vorfällen
10. Betriebskontinuität
11. Krisenmanagement

3 Sicherheitsarchitektur

3.5 Kryptographie

NIS-Verordnung: Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen

Der Betreiber legt Richtlinien und Verfahren für den Einsatz von Kryptographie und Schlüsselmanagement fest, um deren angemessene und wirksame Verwendung zum Schutz der Vertraulichkeit, Authentizität und/oder Integrität von Informationen und Systemen in seinen Netz- und Informationssystemen sicherzustellen *(Fact Sheet 09/2022)*

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Kryptographie
- ISO/IEC 27002:2022: 8.1 Einsatz von Kryptographie
- IEC 62443 2-1: Protection of Data
- CIS CSC v8.0: Data Protection, Application Software Security

NIS Überprüfungsformular

TLP/Klassifizierung:	Amber
Kategorie lt. NISV	Sicherheitsarchitektur
Sicherheitsmaßnahme lt. NISV	Kryptographie
Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.	
Verwendete Werkzeuge gem. § 2 Z 10 QuaSteV getrennt mit ";"	
Geprüfte Systemkomponenten ID aus "Systemkomponenten" - getrennt mit ";"	
Aggregierte Effektivitätsbewertung der	keine Bewertungen
Gefährdungsbewertung	

Prüfgegenstand	Prüfungshandlung							Ergebnis / Findings	
Beschreibung	Standort	Prüfer	Vorgehensweise	Überprüfungsart	Durchgeführte Prüfungshandlungen	Evidenzen / Ref.	Feststellungen	Effektivitätsbewertung	Verbesserungsmöglichkeit(en)
TLP/Klassifizierung:	Amber								

Dokumentinformation | Generelle Angaben | Übersicht | Systemkomponenten | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 | 2.1 | 2.2 | 3.1 | 3.2 | 3.3 | 3.4 | 3.5 | 4.1 | 4.2 | 5.1 | 5.2 | 6.1 | 6.2 | 7.1 | 8.1 | 8.2 | 8.3 | 9. ... +

3.5 Kryptographie

TLP/Klassifizierung:	**Amber**
Kategorie lt. NISV	**Sicherheitsarchitektur**
Sicherheitsmaßnahme lt. NISV	**Kryptographie**
Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.	
Verwendete Werkzeuge gem. § 2 Z 10 QuaSteV getrennt mit ";"	Technisches Werkzeug oder Hilfsmittel;
Geprüfte Systemkomponenten ID aus "Systemkomponenten" - getrennt mit ";"	1;2
Aggregierte Effektivitätsbewertung der	nicht effektiv
Gefährdungsbewertung	sehr hoch

Prüfgegenstand	**Prüfungshandlung**							**Ergebnis / Findings**	
Beschreibung	**Standort**	**Prüfer**	**Vorgehensweise**	**Überprüfungsart**	**Durchgeführte Prüfungshandlungen**	**Evidenzen / Ref.**	**Feststellungen**	**Effektivitätsbewertung**	**Verbesserungsmöglichkeit(en)**
Der Betreiber legt Richtlinien und Verfahren für den Einsatz von Kryptographie und Schlüsselmanagement fest, um deren angemessene und wirksame Verwendung zum Schutz der Vertraulichkeit, Authentizität und/oder Integrität von Informationen und Systemen in seinen Netz- und Informationssystemen sicherzustellen.	Wien	A1	Befragung/Überprüfung	org./tech.	Prüfung der organisatorischen Vorgaben sowie Kontrolle der umgesetzten Maßnahmen. Die Vorgaben entsprechen dem Stand der Technik.	RL Kryptografie Auszug Konf. PKI Screenshot1.png	Die Konfiguration sowie die Umsetzung der organisatorischen Vorgaben aus der Richtlinie wurde nur teilweise und mangelhaft umgesetzt.	nicht effektiv	Die Umsetzung der RL ist zeitnahe entsprechend der darin angeführten Vorgaben durchuführen

Berichterstellung

NIS-2

- In Kraft getreten am 16.1.2023
- Umzusetzen in nationales Recht bis 17.Oktober 2024
- Voraussichtlich ab 18. Oktober 2024 für Unternehmen gültig

Wesentliche Einrichtungen:	Wichtige Einrichtungen:
•Energie •Verkehr •Bankwesen •Finanzmarktinfrastrukturen •Gesundheitswesen •Trinkwasser •Abwasser •Digitale Infrastruktur •Verwaltung von IKT-Diensten B2B •öffentliche Verwaltung •Weltraum	•Post- und Kurierdienste •Abfallbewirtschaftung •Chemie •Lebensmittel •verarbeitendes/herstellendes Gewerbe •Anbieter digitaler Dienste •Forschung (fakultativ)

NIS-2 kleine Unternehmen

- Kleine Unternehmen, d.h. Unternehmen, die weniger als 50 Mitarbeiter:innen beschäftigen und die entweder einen Jahresumsatz von höchstens 10 Mio. Euro erzielen oder deren Jahresbilanzsumme sich auf höchstens 10 Mio. Euro beläuft, fallen nicht unter NIS2.
- Dabei gibt es jedoch Ausnahmen - folgende Unternehmen fallen unabhängig von ihrer Größe in den Anwendungsbereich:
  - Vertrauensdiensteanbieter
  - Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
  - TLD-Namenregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern
  - Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.
- Zusätzlich müssen auch Dienstleister und Lieferanten von betroffenen Unternehmen Sicherheitsvorkehrungen einhalten
- Bei Nichterfüllung: EUR 10Mio oder 2% Gesamtjahresumsatz bei wesentlichen Einrichtungen
- EUR 7 Mio oder 1,4% Gesamtjahresumsatz bei wichtigen Einrichtungen
- Leitungsorgane haften für Verstöße wenn essenzielle Risikoabwägungen vernachlässigt oder ignoriert wurden

Quelle: WKO

Maßnahmen zur Umsetzung

- Betrieb eines Informationssicherheits-Managementsystems (ISMS)
  - z.B. auf Basis einer ISO/IEC27001
- Reifegradanalyse (Überprüfung nach NIS-Kriterien mit Ergebnisbericht und Maßnahmenvorschlägen zur Erhöhung des Reifegrads)

Rückfragen

Helmut Fidi MSc, CoreTEC IT Security Solutions GmbH
Ernst-Melchior-Gasse 24/DG, 1020 Wien
+43 1 503 72 73 0
hf@coretec.at