Bundeskanzleramt

Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Erläuterungen zur Aufstellung von Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

Darstellung und Dokumentation mittels Bericht und Überprüfungsformular

NIS Fact Sheet 3/2021 – Version 1

Wien, März 2021

Inhalt

Einleitung

Sinn und Zweck

Das vorliegende Dokument dient zur näheren Erläuterung der Darstellung und Dokumentation von Überprüfungen mittels Bericht und Überprüfungsformular, um

a) **Betreiber wesentlicher Dienste** (BwD) bei der gesetzlichen Verpflichtung zur Aufstellung von Sicherheitsvorkehrungen gemäß § 17 Abs. 3 NISG sowie
b) **qualifizierte Stellen** (QuaSten) bei der Durchführung von Überprüfungen in diesem Zusammenhang zu unterstützen.

Eine einheitliche Form der Dokumentation und Darlegung anhand eines Berichts und Überprüfungsformulars ist entscheidend, um einen hohen Qualitätsstandard der durchgeführten Überprüfungen gewährleisten zu können. Zudem ermöglicht es die effiziente Nachvollziehbarkeit und Objektivierung der durchgeführten Prüfungshandlungen.

Aus Behördensicht sollte eine **Überprüfung** durch QuaSten bzw. die damit einhergehende Dokumentation jedenfalls folgende **übergeordneten Punkte** enthalten:

- Eine **Beobachtungsperiode** für Stichproben von mindestens einem Jahr
- Eine generelle **Übersicht der Systemlandschaft** für den betroffenen wesentlichen Dienst bzw. die betroffenen wesentlichen Dienste
- Eine Beschreibung des **Anwendungsbereichs** (Scopes) der Überprüfung
- **Informationen** zur **qualifizierten Stelle** und den eingesetzten **Prüfern**
- Eine **nachvollziehbare Darstellung** der geprüften **Kontrollen**, **Prüfungshandlungen, Prüfergebnisse**, **Stichproben** und zugeordneten geprüften **Systemkomponenten**

In Kapitel 1 und den dazugehörigen Unterkapiteln wird die Empfehlung aus Behördensicht zum Aufbau und Inhalt des **Berichts** dargestellt und näher erläutert. In diesem sind sowohl Stellungnahmen und Inhalte des BwD und der QuaSte notwendig.

In Kapitel 2 und den dazugehörigen Unterkapiteln werden das **Überprüfungsformular** als Formatvorlage für Überprüfungen von QuaSten sowie weitere Begrifflichkeiten erläutert.

Eine dementsprechend an die Behörde übermittelte Aufstellung von Sicherheitsvorkehrungen gemäß § 17 Abs. 3 NISG besteht somit aus zwei Teilen, dem Bericht und dem zugehörigen Überprüfungsformular.

Die Aufstellung von Sicherheitsvorkehrungen gemäß § 17 Abs. 3 NISG wird darüber hinaus sowohl durch einen oder mehrere zeichnungsberechtigte Vertreter des BwD als auch einen oder mehrere zeichnungsberechtigte Vertreter der QuaSte und den bzw. die eingesetzten Prüfer an entsprechender Stelle **unterfertigt**, bevor dieser zum Nachweis durch den BwD (vorzugsweise durch dessen Kontaktstelle) verschlüsselt an die zuständige Organisationseinheit des BMI **übermittelt** wird.

Bei Bedarf können Betreiber welche mehrere Dienste in unterschiedlichen Sektoren erbringen aus Gründen der Übersichtlichkeit auch ein Überprüfungsformular bzw. einen Prüfbericht pro Sektor oder Dienst einbringen.

Organisatorische Prüfung: Unter einer organisatorischen Prüfung wird seitens der Behörde ein kontrollbasierter Prüfansatz verstanden, welcher sich auf das interne Kontrollsystem, Prozesse, Vorgaben und Richtlinien des BwD stützt.

Technische Prüfung: Unter technischer Prüfung werden seitens der Behörde dezidiert technische, meist systembasierte, Prüfungshandlungen verstanden, welche ggf. in Verbindung mit einem technischen Werkzeug durchgeführt werden.

1 Aufbau und Inhalt des Berichts

Der Bericht besteht aus den folgenden fünf Abschnitten:

Tabelle 1: Berichtsaufbau und Verantwortlichkeiten

Nr.	Abschnitt	Verantwortlichkeit
1	Selbsteinschätzung und Bestätigung des BwD	BwD
2	Einschätzung und Bestätigung der QuaSte	QuaSte
3.1	Systembeschreibung	BwD
3.2	Prüfumfang	QuaSte
4	Prüfergebnisse	QuaSte
5	Stellungnahmen des BwD	BwD

1.1 Abschnitt 1 – Selbsteinschätzung und Bestätigung des BwD

Der BwD stellt im Rahmen von 1-2 Seiten die geforderte Umsetzung von Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG dar. Dies gibt Raum für eine Selbsteinschätzung bzw. -darstellung der Umsetzung (z.B. durch die Darstellung eingerichteter interner Kontrollmechanismen).

Der BwD bestätigt hier außerdem, dass die Angaben nach bestem Wissen und Gewissen gemacht wurden und die Darlegungen des Berichts sowohl in formaler (z.B. Prüfzeitraum, eingesetzte QuaSte etc.) als auch inhaltlicher Sicht (z.B. Anwendungsbereich, Prüfergebnisse, weitere Stellungnahmen seitens des BwD etc.) korrekt und umfassend sind.

Empfohlen wird an dieser Stelle zudem die Einholung einer Vollständigkeitserklärung seitens zeichnungsberechtigter Vertreter des BwD mit Bezug auf die getätigten Auskünfte und zur Verfügung gestellten Dokumente als Nachweis dieser.

1.2 Abschnitt 2 – Einschätzung und Bestätigung der QuaSte

In diesem Abschnitt stellt die QuaSte im Umfang von 1-2 Seiten ihr Prüfergebnis dar. Die zentral zu beantwortende Frage ist hier, ob alle geprüften Sicherheitsvorkehrungen entsprechend den Vorgaben des NISG umgesetzt sind oder inwieweit Einschränkungen bzw. Abweichungen im Rahmen der Überprüfung festgestellt wurden.

Die QuaSte bestätigt hier außerdem, dass die Angaben nach bestem Wissen und Gewissen gemacht wurden und die Darlegungen des Prüfberichts sowohl in formaler (z.B. Prüfzeitraum, eingesetzte Prüfer etc.) als auch inhaltlicher Sicht (z.B. Anwendungsbereich, Prüfergebnisse etc.) korrekt und umfassend sind.

1.3 Abschnitt 3 – Systembeschreibung und Prüfumfang

Abschnitt 3 setzt sich aus einer Systembeschreibung in Verbindung mit einer daran anschließenden Beschreibung des Prüfumfangs zusammen.

1.3.1 Systembeschreibung

Der BwD legt einen Überblick über die Systemumgebung (-landschaft) bzgl. des oder der von ihm betriebenen wesentlichen Dienste dar. Im Speziellen wird auf die Themen Services, Infrastruktur, Software, Personal, Prozesse und Daten im Rahmen des Anwendungsbereichs eingegangen. Des Weiteren werden hier relevante Aspekte des konkreten Anwendungsbereichs, des internen Kontrollsystems und der für die wesentlichen Dienste relevanten Risikoanalyse dargelegt.

Die Systembeschreibung dient als Anhaltspunkt und kurzer Überblick für die Behörde und umfasst 1-5 Seiten.

1.3.2 Prüfumfang

In diesem Abschnitt beschreibt die QuaSte den vereinbarten Prüfumfang im Hinblick auf die Systembeschreibung.

Die Darlegung des Prüfumfangs dient der Behörde als Grundlage für die Sichtung und Einordnung des dargelegten Berichts und umfasst 1-5 Seiten.

1.4 Abschnitt 4 – Prüfergebnisse

Dieser Abschnitt enthält die **Übersichtstabelle** (Tabellenblatt „Übersicht“) des **Überprüfungsformulars**.

Zudem bietet der Abschnitt 4 die Möglichkeit zur Dokumentation von etwaigen Abweichungen.

1.4.1 Übersichtstabelle:

Tabelle 2: Übersichtstabelle beispielhaft ohne Bewertung

Kategorie lt. NISV	**Nr.**	**Sicherheitsmaßnahme lt. NISV**	**Bewertung**
Governance und Risikomanagement	1.1	Risikoanalyse	
Governance und Risikomanagement	1.2	Sicherheitsrichtlinie	
Governance und Risikomanagement	1.3	Überprüfungsplan der Netz- und Informationssysteme	
Governance und Risikomanagement	1.4	Ressourcenmanagement	
Governance und Risikomanagement	1.5	Informationssicherheitsmanagementsystemprüfung	
Governance und Risikomanagement	1.6	Personalwesen	
Umgang mit Dienstleistern, Lieferanten und Dritten	2.1	Beziehungen mit Dienstleistern, Lieferanten und Dritten	
Umgang mit Dienstleistern, Lieferanten und Dritten	2.2	Leistungsvereinbarungen mit Dienstleistern und Lieferanten	
Sicherheitsarchitektur	3.1	Systemkonfiguration	
Sicherheitsarchitektur	3.2	Vermögenswerte	
Sicherheitsarchitektur	3.3	Netzwerksegmentierung	
Sicherheitsarchitektur	3.4	Netzwerksicherheit	

Kategorie lt. NISV	Nr.	Sicherheitsmaßnahme lt. NISV	Bewertung
Sicherheitsarchitektur	3.5	Kryptographie	
Systemadministration	4.1	Administrative Zugangsrechte	
Systemadministration	4.2	Systeme und Anwendungen zur Systemadministration	
Identifikations- und Zugriffsmanagement	5.1	Identifikation und Authentifikation	
Identifikations- und Zugriffsmanagement	5.2	Autorisierung	
Systemwartung und Betrieb	6.1	Systemwartung und Betrieb	
Systemwartung und Betrieb	6.2	Fernzugriff	
Physische Sicherheit	7.1	Physische Sicherheit	
Erkennung von Vorfällen	8.1	Erkennung	
Erkennung von Vorfällen	8.2	Protokollierung und Monitoring	
Erkennung von Vorfällen	8.3	Korrelation und Analyse	
Bewältigung von Vorfällen	9.1	Vorfallsreaktion	
Bewältigung von Vorfällen	9.2	Vorfallsmeldung	
Bewältigung von Vorfällen	9.3	Vorfallsanalyse	
Betriebskontinuität	10.1	Betriebskontinuitätsmanagement	
Betriebskontinuität	10.2	Notfallmanagement	
Krisenmanagement	11.1	Krisenmanagement	

1.4.2 Dokumentation von Abweichungen:

Tabelle 3 Tabelle zur Dokumentation von Abweichungen

Ref. / Sicherheitsmaßnahme / Kontrolle	Beschreibung der Kontrolle oder Prüfungshandlung	Beschreibung des Ergebnisses bzw. der Abweichung	Risikobeurteilung	Geplante Maßnahmen zur Behebung

1.5 Abschnitt 5 – Stellungnahmen des BwD

Der BwD ergänzt in diesem Abschnitt den Prüfbericht der QuaSte mit weiteren aus seiner Sicht relevanten Informationen, Stellungnahmen zu Einschränkungen und festgestellten Abweichungen bzgl. des in diesem Bericht und im Überprüfungsformular dargestellten Prüfergebnisses.

2 Überprüfungsformular

Die folgenden Beschreibungen beziehen sich auf das Überprüfungsformular „NIS-Ueberpruefungsformular_v*JJJJ*_#.xlsx“, welches berechtigten Unternehmen (beispielsweise BwD, QuaSten etc.) zur Verfügung gestellt wird.

In der Überprüfung gesichtete oder verwendete Dokumente zum **Nachweis** müssen initial **nicht** übermittelt werden. Im Sinne einer späteren Nachvollziehbarkeit der Überprüfung wird eine vollständige, unveränderte und verfügbare Dokumentation der im Laufe der Überprüfung gesichteten und verwendeten Dokumente zum Nachweis aus Behördensicht empfohlen. Dokumente zum Nachweis sollten zudem nachvollziehbar referenziert und den Prüfungshandlungen zugeordnet abgelegt werden. Hierzu wird auf die Spalte „Evidenzen / Ref.“ in den Tabellenblättern der einzelnen Sicherheitsvorkehrungen verwiesen.

Tabellenblatt „Generelle Angaben“

In diesem Tabellenblatt sind die Rahmenbedingungen der Überprüfung zu befüllen.

Als **Beobachtungsperiode** gilt der zwischen BwD und QuaSte vereinbarte Beobachtungszeitraum der Überprüfung aus dem z.B. Stichproben gezogen worden sind. Um eine seriöse Einschätzung der operativen Wirksamkeit der Maßnahmen treffen zu können, wird hierfür ein Zeitraum von zumindest einem Jahr empfohlen.

Tabellenblatt „Übersicht“

Das Tabellenblatt Übersicht befüllt sich automatisch, sobald Bewertungen unter den einzelnen Sicherheitsvorkehrungen (Tabellenblätter 1.1 bis 11.1) eingetragen worden sind. Es ist somit kein weiteres Befüllen notwendig.

Tabellenblatt „Systemkomponenten“

Dieses Tabellenblatt dient der Erfassung der verwendeten Systemkomponenten, genauer der Anführung von Art, Hersteller, Komponenten, Version und optionaler Beschreibung. Die in diesem Tabellenblatt eingetragenen Systemkomponenten werden in den Tabellenblättern der einzelnen Sicherheitsvorkehrungen verknüpft. Aus Gründen der Übersichtlichkeit

und besseren Nachvollziehbarkeit wird vor allem in der Spalte Art um die Verwendung einer einheitlichen Nomenklatur gebeten. (Beispiele: Access Point, Applikation, Betriebssystem, Datenbank, Firewall, ICS/SCADA, IDS/IPS, Policy, Prozess, Richtlinie, Router, Server-Service, SIEM, Switch, Virenscanner, Webapplikation, Webserver, Webservice, HMI, Fernwirksystem, Speichersystem, Alarmanlagen, Videoüberwachung, Zugangskontrollsysteme etc.)

Tabellenblätter der einzelnen Sicherheitsvorkehrungen „1.1“ bis „11.1“

Unter den Sicherheitsvorkehrungen wird um detaillierte Beschreibungen der einzelnen Kontrollen und Prüfungshandlungen ersucht.

Beschreibung:
Dieses Feld dient der Vornahme von kurzen und prägnanten Kontrollbeschreibungen (z.B. „Passwort- und Sicherheitseinstellungen sind angemessen gesetzt“ oder „Jährlich werden die Einstellungen vom Kontrollverantwortlichen auf Aktualität und Angemessenheit überprüft“)

Art:
Dieses Feld dient der Einordnung der überprüften Kontrollen/Maßnahmen. Als **manuell** werden manuell von Personen durchgeführte Kontrollen erachtet. Als **automatisch** werden Kontrollen und Maßnahmen erachtet, wenn Sie automatisch durch ein System und ohne manuellen Eingriff implementiert sind. **Semiautomatisiert** ist eine entsprechende Mischform beider Arten.

Standort:
Für Betreiber mit mehreren Standorten gibt es hier die Möglichkeit die Prüfungshandlungen einem entsprechenden Standort zuzuweisen.

Prüfer:
Dieses Feld dient der Deklarierung der Prüfer seitens der QuaSte.

Vorgehensweise:
Dieses Feld dient zur Bestimmung der angewandten IT Prüfungstechnik.

Befragung: Eine Befragung dient am besten zur anfänglichen Gewinnung eines Verständnisses von Prozessen und Kontrollen. Eine Befragung wird meist in Zusammenhang mit weiteren Prüftechniken angewendet, weshalb erweiterte Auswahlmöglichkeiten vorhanden

sind. („Befragung/Überprüfung“, „Befragung/Wiederausführung und „Befragung/Beobachtung“)

Überprüfung: Überprüfung bezieht sich auf die Untersuchung und Prüfung von Dokumenten und Stichproben, welche als Nachweis dienen. Eine Überprüfung kann sich mit einer Beobachtung überschneiden. Ein klassisches Beispiel ist die Einsichtnahme in Wartungsprotokolle bei der physischen Begehung von Rechenzentren. In Spezialfällen ist eine Einordnung auf Basis der Erfahrung des Prüfers zu treffen.

Beobachtung: Als Beobachtung werden Prüfungshandlungen definiert, in denen im Beisein des Prüfers entsprechende logische oder physische Sicherheitsmaßnahmen evaluiert werden. Hierzu zählen aber auch relevante Prozesse, welche im Zuge der Überprüfung vom Prüfer beobachtet und ggf. evaluiert werden.

Wiederausführung: Wiederausführung beschreibt eine erneute Ausführung von Prozessen im Beisein des Prüfers, um z.B. Kontrollen in einem automatisierten Prozess evaluieren zu können.

Werkzeug:
Dieses Feld dient der Auflistung von ggf. bei der Prüfungshandlung verwendeten technischen Hilfsmittel.

Überprüfungsart:
Unterscheidung zwischen organisatorischer und technischer Prüfung (siehe „Einleitung“)

Durchgeführte Prüfungshandlungen:
Dieses Feld dient der Auflistung der zu den Kontrollen gesetzten Prüfungshandlungen (z.B. Einsichtnahme in die Passwort- und Sicherheitseinstellungen und Evaluierung, ob selbige jährlich auf Aktualität und Angemessenheit überprüft wurden).

Kommentar zur Stichprobengröße:
Dieses Feld dient zur Darlegung von etwaig gezogenen Stichproben. Hier ist vor allem ein Augenmerk auf die Vollständigkeit und Richtigkeit der Grundgesamtheit zu legen. Auch die verwendeten Vorgaben/Richtlinien zur Ziehung von Stichproben können hier kurz erläutert werden.

Evidenzen / Ref.:

Dieses Feld bietet Platz für eine kurze Beschreibung und eine Referenz auf die verwendeten und abgelegten Dokumente zum Nachweis.

Feststellung der Ergebnisse:
Dieses Feld dient zur kompakten Beschreibung der Feststellungen.

Verbesserungsmöglichkeiten:
Hier können entsprechende Verbesserungsmöglichkeiten **optional** angeführt werden. Es sei darauf hingewiesen, dass bei einer als „effektiv" bewerteten Sicherheitsmaßnahme mit Verbesserungsmöglichkeiten eine entsprechende Beschreibung, warum die Maßnahme trotzdem als effektiv bewertet wurde, anzuführen ist.

Bewertung:
Als **effektiv** ist eine Sicherheitsmaßnahme zu bewerten, wenn die durchgeführten Prüfungshandlungen mit hinreichender Sicherheit eine Implementierung und operative Wirksamkeit der Kontrollen zur vollumfänglichen Abdeckung der Sicherheitsmaßnahme darlegen.

Als **teilweise effektiv** sind Sicherheitsvorkehrungen zu bewerten, bei denen nur eine teilweise Erfüllung oder Abdeckung der Sicherheitsvorkehrungen durch Kontrollen und interne Maßnahmen erreicht wird. Dies gilt auch wenn eine Kontrolle zwar implementiert, die operative Wirksamkeit aber nicht oder nur unvollständig nachgewiesen werden konnte.

Als **nicht effektiv** sind Sicherheitsvorkehrungen zu bewerten, die in überwiegendem Maße Kontrollschwächen und Abweichungen aufweisen.

Die Gesamtbewertung der jeweiligen Sicherheitsmaßnahme entspricht der niedrigsten Einzelbewertung einer Prüfungsmaßnahme bzw. Kontrolle. (Beispiel: Gibt es bei Sicherheitsmaßnahme 1.1 fünf „effektive" Prüfungsmaßnahmen bzw. Kontrollen und eine „teilweise effektive" ist die Gesamtbewertung „teilweise effektiv"**.**)

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: BMI/II/BVT/5.3-NIS und Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)
Wien, 2021. Stand: 1. März 2021

Abschließende Anmerkungen:
Es wird darauf hingewiesen, dass Änderungen vorbehalten sind.
Alle in diesem NIS Fact Sheet verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an nis@bvt.gv.at.