Bundeskanzleramt

Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

NIS Fact Sheet 8/2019

Wien, August 2019

Inhalt

Einleitung

Hintergrund

Die 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-Richtlinie") zielt darauf ab, ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der EU zu erreichen.

Österreich setzt die NIS-Richtlinie mit dem am 28. Dezember 2018 kundgemachten Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) um.

Mit einer Verordnung zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV) legt der Bundesminister für EU, Kunst, Kultur und Medien, im Einvernehmen mit dem Bundesminister für Inneres, Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste fest.

Das vorliegende NIS Fact Sheet dient der näheren Erläuterung der in der Anlage 1 der NISV genannten Sicherheitsmaßnahmen, um Betreiber wesentlicher Dienste bei der Umsetzung der Vorgaben aus dem NISG und der NISV zu unterstützen. Diese werden den Beschreibungen jeweils vorangestellt, um den direkten Bezug zwischen NISV und dem vorliegenden NIS Fact Sheet zu ermöglichen.

Anwendbarkeit

Das NIS Fact Sheet hält sich weitgehend an die im Leitfaden der europäischen NIS-Kooperationsgruppe[1] formulierten Empfehlungen für Sicherheitsvorkehrungen, berücksichtigt aber auch nationale Besonderheiten und Erfahrungen aus den Sektorengesprächen.

[1] CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, abrufbar unter https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

Aus Sicht des Bundeskanzleramts und des Bundesministeriums für Inneres stellt dieses NIS Fact Sheet eine detailliertere Beschreibung der Sicherheitsmaßnahmen der NISV, die in ihrer Gesamtheit die Sicherheitsvorkehrungen bilden, dar.

Bei allen im NIS Fact Sheet beschriebenen Sicherheitsmaßnahmen ist bei der Umsetzung im Sinne des § 17 Abs. 1 NISG auf ein angemessenes Verhältnis zwischen dem feststellbaren Ausmaß einer Bedrohung und der wirtschaftlichen Belastung Wert zu legen. Wenn aus technischen oder betrieblichen Gründen die Umsetzung der die Sicherheitsmaßnahmen beschreibenden Ausführungen nicht gänzlich möglich ist, sind die dadurch bedingten Abweichungen bei der Umsetzung durch risikominimierende und/oder kompensierende Maßnahmen auszugleichen und dies entsprechend in den zu erbringenden Nachweisen (Prüfbericht) darzustellen und glaubhaft zu begründen.

1 Teil A: Governance und Ökosystem

1.1 Governance und Risikomanagement

1.1.1 Risikoanalyse

NIS-Verordnung:
Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.

Der Betreiber führt eine Risikoanalyse durch und aktualisiert sie regelmäßig. Die Analyse identifiziert jene Netz- und Informationssysteme, die der Betreiber für die Bereitstellung des wesentlichen Dienstes (oder der wesentlichen Dienste) nutzt, sowie die dazugehörigen Risiken. Die Risiken umfassen alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit der identifizierten Netz- und Informationssysteme haben, und die mit vernünftigem Aufwand feststellbar sind.

Diese Analyse bildet die Basis für die Fokussierung und Priorisierung von Sicherheitsmaßnahmen und -aktivtäten. Die Durchführung der Risikoanalyse beinhaltet die oben erwähnte laufende Aktualisierung im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP).

Bei der Aktualisierung der Analyse werden insbesondere neue Bedrohungen, der Effektivitätsverlust umgesetzter Maßnahmen sowie Änderungen der Risikosituation, beispielsweise durch Änderungen in der Systemarchitektur, berücksichtigt.

1.1.2 Sicherheitsrichtlinie

NIS-Verordnung:
Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.

Der Betreiber erstellt, pflegt und aktualisiert eine Sicherheitsrichtlinie, welche strategische Sicherheitsziele festlegt, das Risikomanagement beschreibt und auf alle relevanten weiteren spezifischen Sicherheitsvorgaben (Richtlinien, Guidelines etc.) verweist.

1.1.3 Überprüfungsplan der Netz- und Informationssysteme

NIS-Verordnung:
Die Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit ist zu planen und festzulegen.

Gemäß dem definierten Überprüfungsplan überprüft der Betreiber eigenständig die identifizierten Netz- und Informationssysteme.

Im Rahmen des Überprüfungsplans und in Abhängigkeit von der Risikoanalyse werden Überprüfungen der Netz- und Informationssysteme durchgeführt. Diese Prüfungen zielen darauf ab, die Anwendung, Wirksamkeit und Angemessenheit der definierten Sicherheitsmaßnahmen zu validieren.

Der Betreiber sorgt für eine Übersicht und eine laufend aktualisierte Dokumentation der durchgeführten Überprüfungen.

1.1.4 Ressourcenmanagement

NIS-Verordnung:
Alle Ressourcen, die erforderlich sind, um die Funktionsfähigkeit der Netz- und Informationssysteme zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und sicherzustellen.

Der Betreiber stellt die kurz-, mittel- und langfristige Verfügbarkeit aller für die Funktionsfähigkeit der Netz- und Informationssysteme erforderlichen personellen, finanziellen sowie technischen Ressourcen sicher.

1.1.5 Informationssicherheitsmanagementsystemprüfung

NIS-Verordnung:
Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.

Anhand einer Reihe von Indikatoren und Methoden evaluiert der Betreiber die Einhaltung seiner Sicherheitsrichtlinie. Indikatoren können sich beispielsweise auf die Angemessenheit und Effektivität des Risikomanagements des Betreibers, die Wartung und den Betrieb von Ressourcen unter sicheren Bedingungen, die Zugriffsrechte der Benutzer sowie die Authentifizierung des Zugriffs auf Ressourcen und die Ressourcenverwaltung beziehen.

1.1.6 Personalwesen

NIS-Verordnung:
Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen.

Der Betreiber stellt sicher, dass Mitarbeiter vertrauenswürdig und sich ihrer Verantwortung bewusst sind. Der Betreiber stellt des Weiteren sicher, dass Mitarbeiter für die ihnen zugewiesenen Rollen qualifiziert sind.

Für die Fort- und Weiterbildung in sicherheitsrelevanten Themengebieten gibt es ein entsprechendes Schulungs- bzw. Ausbildungsprogramm.

Eine Sensibilisierung in Sicherheitsfragen für alle Mitarbeiter sowie ein spezielles Sicherheitstrainingsprogramm für Mitarbeiter mit spezifischer Verantwortung für Netz- und Informationssysteme wird durchgeführt.

1.2 Umgang mit Dienstleistern, Lieferanten und Dritten

1.2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten

NIS-Verordnung:
Anforderungen an Dienstleister, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.

Der Betreiber erstellt ein Gesamtbild seines Ökosystems, einschließlich Dienstleister und Lieferanten mit vertraglichen Beziehungen sowie Dritter, insbesondere solcher, die Zugang zu den Netz- und Informationssystemen haben oder diese verwalten.

Der Zweck dieses Gesamtbilds ist es, Risiken und Abhängigkeiten, die sich aus den Beziehungen zu den Dienstleistern, Lieferanten und Dritten ergeben, zu identifizieren und zu bewerten. Um diese Bewertung durchzuführen, berücksichtigt der Verantwortliche zumindest die folgenden Fragestellungen:

Reife: Über welche technischen Fähigkeiten verfügen die Dienstleister, Lieferanten und Dritten in Bezug auf Cybersicherheit?

Vertrauen: Kann ich davon ausgehen, dass die Absichten des Dienstleisters, Lieferanten und Dritten mir gegenüber vertrauenswürdig und diese selbst zuverlässig sind?

Zugriffsebene: Welche Zugangsrechte haben die Dienstleister, Lieferanten und Dritten zu Netz- und Informationssystemen?

Abhängigkeit: Inwieweit ist die Beziehung zu Dienstleistern, Lieferanten und Dritten für die Tätigkeit entscheidend?

1.2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

NIS-Verordnung:
Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.

Der Betreiber legt eine Richtlinie für seine Beziehungen zu Dienstleitern und Lieferanten fest, um die identifizierten Risiken zu minimieren. Ein besonderer Fokus wird hierbei auf Schnittstellen zwischen deren Netz- und Informationssystemen und jenen des Betreibers gelegt.

Generell müssen für Netz- und Informationssysteme, die von Dienstleistern betrieben werden, Sicherheitsanforderungen identifiziert und definiert werden. Der Betreiber stellt durch Service Level Agreements (SLA) und/oder Prüfmechanismen sicher, dass seine Dienstleister und Lieferanten ebenfalls angemessene Sicherheitsmaßnahmen umsetzen, um den Sicherheitsanforderungen des Betreibers zu entsprechen.

Der Betreiber definiert mit seinen Dienstleistern und Lieferanten Reaktions- und Wiederherstellungsprozesse nach (Sicherheits-)Vorfällen und überprüft diese periodisch.

2 Teil B: Schutz

2.1 Sicherheitsarchitektur

2.1.1 Systemkonfiguration

NIS-Verordnung:
Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguration ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.

Der Betreiber verwendet nur Ressourcen (z.B. Dienste und Geräte), die für den Betrieb der Netz- und Informationssysteme notwendig sind.

Bei der Installation und im gesamten Lebenszyklus verfolgt der Betreiber einen Systemhärtungsansatz.

Zudem sorgt der Betreiber dafür, dass die Konfiguration aller relevanten Komponenten dokumentiert wird. Der Betreiber aktualisiert diese Dokumentation regelmäßig.

2.1.2 Vermögenswerte

NIS-Verordnung:
Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.

Der Betreiber erstellt ein geeignetes Konzept zur Verwaltung von Vermögenswerten (Assets) für die Identifizierung, Klassifizierung und Inventarisierung der IT-Prozesse, -Systeme, -Komponenten sowie Softwareplattformen/-Lizenzen und Applikationen. Im Inventar sind je Vermögenswert klare Rollen und Verantwortlichkeiten definiert und diese im Hinblick auf ihre Kritikalität klassifiziert.

Das Inventar unterstützt unter anderem das Ausrollen von Updates und Patches und ermöglicht gegebenenfalls eine Ermittlung, welche Komponenten von neuen Sicherheitsproblemen oder Schwachstellen betroffen sind.

2.1.3 Netzwerksegmentierung

NIS-Verordnung:
Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.

Der Betreiber trennt seine Systeme physisch oder logisch je nach Schutzbedarf und Klassifikation, um Auswirkungen von (Sicherheits-)Vorfällen innerhalb seiner Systeme einzudämmen.

Der Betreiber gestattet nur Verbindungen zwischen Systemen mit unterschiedlichem Schutzbedarf und unterschiedlicher Klassifikation, die für das Funktionieren der Netz- und Informationssysteme von signifikanter Bedeutung sind.

Für solche Schnittstellen (z.B. Schnittstellen zwischen den Netz- und Informationssysteme von Lieferanten und Kunden) dokumentiert der Betreiber angemessene Sicherheitsmechanismen und setzt diese um. Dies umfasst unter anderem Prozesse und Verfahren für einen sicheren Zugriff, Fernzugriff, Monitoring oder Datenaustausch.

2.1.4 Netzwerksicherheit

NIS-Verordnung:
Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.

Der Betreiber filtert den eingehenden und ausgehenden Netzwerkverkehr und begrenzt diesen auf das für das Funktionieren der Netz- und Informationssysteme unbedingt erforderliche Maß.

Der Betreiber filtert auch den Netzwerkverkehr innerhalb des Netzwerks und verbietet jeglichen Netzwerkverkehr, der für das Funktionieren seiner Systeme nicht erforderlich ist und potentielle Angriffe erleichtern kann.

Hierzu definiert und aktualisiert der Betreiber die Filterregeln regelmäßig nach Netzadresse, Portnummer, Protokoll usw.

2.1.5 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.

2.2 Systemadministration

2.2.1 Administrative Zugangsrechte

NIS-Verordnung:
Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.

Der Betreiber richtet – soweit dies vom System unterstützt wird – dedizierte und personalisierte Konten für die Administration ein, die zum Zweck der Installation, Konfiguration, Verwaltung, Wartung usw. verwendet werden dürfen. Diese Konten werden auf einer stets aktualisierten Liste dokumentiert und in einem regelmäßigen Review-Prozess überprüft, wobei eine solche Liste auch für nicht administrative Konten geführt wird.

Die erteilten administrativen Berechtigungen werden individualisiert auf den funktionalen und technischen Aufgabenbereich des jeweiligen administrativen Benutzerkontos beschränkt. Diese Benutzerkonten werden nur zum Zweck der Administration selbst und für die

Verbindung zu administrativen Systemen verwendet. Ein Einsatz für nicht administrative Tätigkeiten wird untersagt.

Bei der Vergabe von administrativen Konten werden Anforderungen der Pflichtentrennung berücksichtigt und administrative Tätigkeiten protokolliert.

2.2.2 Systeme und Anwendungen zur Systemadministration

NIS-Verordnung:
Systeme und Anwendungen zur Systemadministration sind ausschließlich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. Die Sicherheit dieser Systeme und Anwendungen ist zu gewährleisten.

Für die Durchführung von Administrationstätigkeiten werden nur Systeme eingesetzt, die der Betreiber oder Dienstleister für diesen Zweck vorgesehen hat. Hard- und Software, die für administrative Tätigkeiten verwendet werden, werden vom Betreiber oder gegebenenfalls vom Dienstleister, den der Betreiber zur Durchführung von administrativen Tätigkeiten autorisiert hat, verwaltet und sicher konfiguriert.

Administrative Systeme werden ausschließlich zur Durchführung von administrativen Tätigkeiten verwendet und nicht für andere Tätigkeiten genutzt. Insbesondere werden sie nicht für den Zugriff auf das Internet verwendet. Benutzer und Benutzerinnen verbinden sich keinesfalls über eine Softwareumgebung, die für andere Funktionen als die Administration eingesetzt wird, mit einem System, das für administrative Tätigkeiten verwendet wird.

Der Betreiber richtet ein dediziertes logisches oder physisches Netzwerk ein, um die administrativen Systeme mit den zu verwaltenden Systemen zu verbinden.

Für administrative Tätigkeiten werden sichere, den aktuellen Stand der Technik berücksichtigende Protokolle, Authentifizierungs- und Verschlüsselungsmechanismen eingesetzt.

2.3 Identitäts- und Zugriffsmanagement

2.3.1 Identifikation und Authentifikation

NIS-Verordnung:
Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten.

Zur Identifikation richtet der Betreiber entsprechend einem definierten und dokumentierten Verfahren eindeutige Konten für Benutzer oder für automatisierte Prozesse ein, die auf Netz- und Informationssysteme zugreifen müssen. Nicht genutzte oder nicht mehr benötigte Konten müssen deaktiviert werden. Hierzu wird ein regelmäßiger Überprüfungsprozess eingerichtet.

Für die Authentifikation schützt der Betreiber den Zugriff auf Ressourcen seines Netz- und Informationssystems durch Benutzer oder automatisierte Prozesse mit einem sicheren Authentifikationsmechanismus. Der Betreiber definiert die Regeln für die Verwaltung der Authentifizierungsdaten.

Wann immer es erforderlich ist, ändern die Benutzer ihre Authentifizierungsdaten entsprechend definierter Vorgaben regelmäßig. Insbesondere ändert der Betreiber vor Inbetriebnahme eines Systems die vom Hersteller/Lieferanten installierten Standard-Authentifizierungsdaten.

Der Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung wird vom Betreiber in seiner Architektur berücksichtigt und gezielt vorangetrieben.

2.3.2 Autorisierung

NIS-Verordnung:
Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.

Der Betreiber gewährt definierten Regeln folgend Benutzern oder automatisierten Prozessen nur dann Zugriffsrechte, wenn deren Zugriff für die Erfüllung von Aufgaben oder die Durch-

führung automatisierter Prozesse unbedingt erforderlich ist. Eine Vergabe von Zugriffsrechten erfolgt immer unter Anwendung des definierten Rechteanforderungsprozesses, in dem die Pflichtentrennung entsprechend berücksichtigt wird. Es werden Maßnahmen umgesetzt, um die Einhaltung des Grundsatzes „Need-to-know" bzw. des Minimalrechtsprinzips zu gewährleisten.

Der Betreiber überprüft diese Zugriffsrechte mindestens einmal jährlich, wobei er die Benutzerkonten, deren zugehörige Zugriffsrechte und die entsprechenden Systeme oder Funktionalitäten, auf die mit diesen Zugriffsrechten zugegriffen wird, überprüft.

Der Betreiber führt und aktualisiert eine Liste der privilegierten Konten (z.B. von administrativen Konten). Der Betreiber überprüft jede mögliche Änderung an einem privilegierten Benutzerkonto, um sicherzustellen, dass die Zugriffsrechte auf Systeme und Funktionalitäten dem Minimalrechtsprinzip entsprechen und für die Nutzung des Benutzerkontos angemessen sind.

2.4 Systemwartung und Betrieb

2.4.1 Systemwartung und Betrieb

NIS-Verordnung:
Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.

Der Betreiber definiert Verfahren und Bedingungen, unter denen die Sicherheit seiner Netz- und Informationssysteme im Betrieb sichergestellt ist. Unter anderem wird auch ein Verfahren definiert, um Informationen über Schwachstellen und zugehörige Patches, die Netz- und Informationssysteme betreffen, zu sammeln und davon abgeleitet entsprechende Schritte zu setzen.

Der Betreiber stellt sicher, dass die eingesetzten Systemversionen aus sicherheitstechnischer Sicht auf dem aktuellen Stand sind. Der Betreiber überprüft Herkunft und Integrität der jeweiligen Systemversion vor ihrer Installation beziehungsweise vor ihrer Aktualisierung und analysiert die technischen und betrieblichen Auswirkungen dieser Version auf das betreffende Netz- und Informationssystem.

Der Betreiber stellt sicher, dass Komponenten der Netz- und Informationssysteme regelmäßig entsprechend ihrer Wartungsintervalle gewartet werden und protokolliert die Durchführung.

2.4.2 Fernzugriff

NIS-Verordnung:
Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.

Der Betreiber etabliert Prozesse zur Verwaltung von Fernzugriffen. Insbesondere stellt er Techniken zur Verfügung, die Fernzugriffe auf Netz- und Informationssysteme nur nach dem Minimalrechtsprinzip autorisiert und zeitlich beschränkt ermöglichen.

Die Authentifizierung im Rahmen des Fernzugriffs wird mittels Zwei-Faktor-Authentifizierung umgesetzt. Jeglicher unautorisierte Zugriff wird unterbunden.

Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden. Alle Zugriffe externer Personen können nur unter Kontrolle der Systemverantwortlichen erfolgen.

2.5 Physische Sicherheit

2.5.1 Physische Sicherheit

NIS-Verordnung:
Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.

Der Betreiber verhindert unbefugten physischen Zugang zu, Zugriff auf, Beschädigung von und Eingriffe in Netz- und Informationssysteme.

Insbesondere erstellt der Betreiber ein physisches Sicherheitskonzept inklusive einer entsprechenden Definition unterschiedlicher Sicherheitszonen und definiert Verfahren für den sicheren Umgang mit Besuchern und betriebsfremdem Personal (wie etwa Wartungstechniker, Dienstleister, Lieferanten oder Dritte).

3 Teil C: Verteidigung

3.1 Erkennung von Vorfällen

3.1.1 Erkennung

NIS-Verordnung:
Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.

Der Betreiber richtet ein System zur Erkennung von sicherheitsrelevanten Ereignissen ein. Die hierzu im Netzwerk und auf Systemkomponenten eingerichtete Sensorik analysiert übertragene Daten, Datenströme, Protokolle sowie das Verhalten einzelner Systeme oder Komponenten selbst, um Ereignisse zu erkennen, welche die Sicherheit der Netz- und Informationssysteme beeinträchtigen können. Dieses System ist so einzurichten, dass es zumindest alle zwischen den Netz- und Informationssystemen des Betreibers und denen der Lieferanten und Dienstleister ausgetauschten Datenströme erfasst. Der Betreiber definiert Standardwerte für zulässige System- und Netzwerkoperationen und zu erwartende Datenflüsse und Aktivitäten.

3.1.2 Protokollierung und Monitoring

NIS-Verordnung:
Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.

Der Betreiber implementiert in seinen Netz- und Informationssystemen Mechanismen zu Protokollierung und Monitoring. Die Protokollierung umfasst u.a. die Anwendungsserver, System- und Netzwerkinfrastrukturserver, Sicherheitstechnologien und -systeme, Technik- und Wartungsstationen von Industriesystemen, Netzwerkausrüstungen und administrative Arbeitsstationen, die kritische Aktivitäten unterstützen. Der Betreiber erfasst im Protokollierungssystem Ereignisse mit Zeit- und Datumsstempel (unter Verwendung synchronisierter

Zeitquellen) und bewahrt die Informationen für einen definierten Zeitraum in zentralen Archiven auf.

3.1.3 Korrelation und Analyse

NIS-Verordnung:
Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.

Zur Korrelation und Analyse verwendet der Betreiber ein System, das sicherheitsrelevante Ereignisse zusammenfasst und auswertet, um Vorfälle zu erkennen.

Der Betreiber richtet ein spezielles Informationssystem für die Korrelation, Analyse und weitere Bearbeitung von Vorfällen ein. Der Betreiber berücksichtigt bei der Konzeption dieses Systems insbesondere die Vertraulichkeit der gespeicherten Daten.

3.2 Bewältigung von Vorfällen

3.2.1 Vorfallsreaktion

NIS-Verordnung:
Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.

Der Betreiber erstellt und implementiert Prozesse und Verfahren zur Reaktion auf Vorfälle, die das Funktionieren oder die Sicherheit eines Netz- und Informationssystems beeinträchtigen. Der Betreiber legt diesbezüglich klare Rollen und Verantwortlichkeiten fest. Die Prozesse und Verfahren werden regelmäßig aktualisiert und durch Tests bzw. Übungen überprüft.

Der Betreiber stellt sicher, dass forensisches Wissen und Kapazitäten entweder hausintern zur Verfügung stehen oder über einen Vertrag mit einem Dienstleister bei Bedarf abgerufen werden können.

Der Betreiber stellt sicher, dass Erkenntnisse und Lehren aus vorangegangenen Vorfällen in seine Prozesse und Verfahren einfließen (lessons learned).

3.2.2 Vorfallsmeldung

NIS-Verordnung:
Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.

Der Betreiber erstellt, implementiert und aktualisiert regelmäßig Prozesse und Verfahren zur internen und externen Meldung von Vorfällen.

Darüber hinaus entwickelt der Betreiber Prozesse und Verfahren, um bei Vorfällen bei Dienstleistern und Lieferanten umgehend von diesen informiert zu werden, sofern die Vorfälle für das Sicherheitsniveau oder die -situation des Betreibers relevant sein könnten.

3.2.3 Vorfallsanalyse

NIS-Verordnung:
Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.

Der Betreiber etabliert Prozesse und implementiert Verfahren, um die Analyse und Bewertung von erkannten und/oder vermuteten Vorfällen zu ermöglichen. Des Weiteren definiert der Betreiber Prozesse zur Sammlung und Bewertung analyserelevanter Informationen und erprobt diese.

4 Teil D – Resilienz

4.1 Betriebskontinuität

4.1.1 Betriebskontinuitätsmanagement

NIS-Verordnung:
Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.

Der Betreiber definiert Ziele und strategische Richtlinien für das Betriebskontinuitätsmanagement im Falle eines Sicherheitsvorfalls. Der Betreiber verantwortet den Aufbau eines leistungsfähigen Notfall- und Krisenmanagements zur systematischen Vorbereitung auf die Bewältigung von Sicherheitsvorfällen bzw. Schadereignissen, insbesondere der Wiederherstellung der Erbringung des wesentlichen Dienstes.

Als Grundlage des Notfall- und Krisenmanagements führt der Betreiber eine Business Impact Analyse seiner Netz- und Informationssysteme durch und aktualisiert diese regelmäßig.

4.1.2 Notfallmanagement

NIS-Verordnung:
Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.

Der Betreiber erstellt ein Notfallhandbuch und stellt sicher, dass die in diesem definierten Notfallprozesse dementsprechend durchgeführt werden. Der Betreiber stellt sicher, dass Erkenntnisse und Lehren aus früheren Sicherheitsvorfällen in die Notfallpläne einfließen.

Der Betreiber führt regelmäßige Notfallübungen durch, um die Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge zu prüfen.

4.2 Krisenmanagement

4.2.1 Krisenmanagement

NIS-Verordnung:
Rahmenbedingungen und Prozessabläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.

Der Betreiber definiert die Organisation und Verantwortlichkeiten für das Krisenmanagement bei Sicherheitsvorfällen, erstellt geeignete Alarmierungspläne und implementiert geeignete Prozesse und Verfahren zur Krisenbewältigung.

Der Betreiber stellt sicher, dass Aktivitäten im Rahmen des Krisenmanagements mit internen und externen Partnern (z.B. Internet Service Providern, CERT, Behörden, Systemintegratoren etc.) koordiniert werden.

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) und BMI/II/BVT/5.3-NIS
Wien, 2019
Stand: 26. August 2019

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@bka.gv.at und nis@bvt.gv.at.