jusline®
»» Recht. Schnell

Sie können die QR Codes nützen um später wieder auf die neuste Version eines Gesetzestexts zu gelangen.

Anl. 1 NISV

NISV - Netz- und Informationssystemsicherheitsverordnung

Berücksichtigter Stand der Gesetzgebung:

Sicherheitsmaßnahmen

1.

Governance und Risikomanagement

1.1

Risikoanalyse:

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.

1.2

Sicherheitsrichtlinie:

Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.

1.3

Überprüfungsplan der Netz- und Informationssysteme:

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

1.4

Ressourcenmanagement:

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.

1.5

Informationssicherheitsmanagementsystemprüfung:

Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.

1.6

Personalwesen:

Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen.

2.

Umgang mit Dienstleistern, Lieferanten und Dritten

2.1

Beziehungen mit Dienstleistern, Lieferanten und Dritten:

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

2.2

Leistungsvereinbarungen mit Dienstleistern und Lieferanten:

Die Leistungsvereinbarungen mit Dienstleistern und Lieferanten sind periodisch zu überprüfen und zu überwachen.

3.

Sicherheitsarchitektur

3.1

Systemkonfiguration:

Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguratoin ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.

3.2

Vermögenswerte:

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

3.3

Netzwerksegmentierung:

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

3.4

Netzwerksicherheit:

Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.

3.5

Kryptographie:

Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.

4.

Systemadministration

4.1

Administrative Zugangsrechte:

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

4.2

Systeme und Anwendungen zur Systemadministration:

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

5.

Identitäts- und Zugriffsmanagement

5.1

Identifikation und Authentifikation:

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

5.2

Autorisierung:

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

6.

Systemwartung und Betrieb

6.1

Systemwartung und Betrieb:

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

6.2

Fernzugriff:

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.

7.

Physische Sicherheit

7.1

Physische Sicherheit:

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

8.

Erkennung von Vorfällen

8.1

Erkennung:

Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.

8.2

Protokollierung und Monitoring:

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

8.3

Korrelation und Analyse:

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

9.

Bewältigung von Vorfällen

9.1

Vorfallsreaktion:

Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.

9.2

Vorfallsmeldung:

Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.

9.3

Vorfallsanalyse:

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.

10.

Betriebskontinuität

10.1

Betriebskontinuitätsmanagement:

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

10.2

Notfallmanagement:

Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.

11.

Krisenmanagement

11.1

Krisenmanagement:

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

In Kraft seit 18.07.2019 bis 30.09.2026

© 2026 JUSLINE
JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.
www.jusline.at