RECHT.NRW
Landesrecht Nordrhein-Westfalen

Ministerium des Innern
des Landes Nordrhein-Westfalen

Ministerialblatt für das Land Nordrhein-Westfalen

Ausgabe: MBl. NRW. 2000 Nr. 12
Veröffentlichungsdatum: 25.01.2000
Seite: 152

I

Festlegung von Sicherheitsmaßnahmen zur Internetnutzung und sonstiger Kommunikation mit Stellen außerhalb der Landesverwaltung - Sicherheitskonzept Kommunikation NRW -

I.

20025

**Festlegung von Sicherheitsmaßnahmen zur Internetnutzung
und sonstiger Kommunikation mit Stellen
außerhalb der Landesverwaltung
- Sicherheitskonzept Kommunikation NRW -**

RdErl. d. Innenministeriums v. 25.1.2000 –

V B 2/201.1-6

Aufgrund des §11 ADV-Organisationsgesetz – ADVG NW – in der Fassung der Bekanntmachung vom 9.Januar 1985 (GV.NRW. S.41/SGV. NRW. 2006) wird das vorliegende Sicherheitskonzept Kommunikation erlassen:

1
Allgemeines

1.1
Zweck

Mit dem Sicherheitskonzept sollen eine gesicherte Internetnutzung ermöglicht und die Mindestanforderungen hinsichtlich Sicherheit bei der Kommunikation mit anderen Stellen der öffentlichen Verwaltung festgelegt werden.

1.2
Anwendungsbereich

Das Sicherheitskonzept ist von den Behörden und Einrichtungen des Landes, die

- ihren Mitarbeiterinnen und Mitarbeitern eine Nutzung des Internet ermöglichen wollen oder

- informationstechnische Verfahren planen, die eine Kommunikation mit Stellen außerhalb der Landesverwaltung NRW vorsehen

anzuwenden.

1.3
Netzübergänge

Die Kopfstelle des Landesverwaltungsnetzes (LVN) stellt Netzübergänge zum Internet sowie zum bundesweiten Netz für öffentliche Verwaltungen (TESTA) bereit. Bei der Fernwartung sind die in der Anlage beigefügten Sicherheitsregelungen für die externe Fernwartung in der Landesverwaltung, bei der Telearbeit mit mittlerem Schutzbedarf die Regelungen des IT-Grundschutzhandbuchs (vgl. RdErl. d. Ministeriums für Inneres und Justiz zugleich im Namen des Ministerpräsidenten und aller Landesministerien vom 22.8.1998 "IT-Grundschutzhandbuch" – SMBl. NRW. 20025) zugrundezulegen. Zugriffe auf externe Datenbanken sind im Einzelfall zu regeln.

1.4
Ergänzende Sicherheitsmaßnahmen

Die im vorliegenden Sicherheitskonzept dargestellten Sicherheitsmechanismen stellen lediglich die Mindestanforderungen an Sicherheit dar. In der Regel wird es notwendig sein, dass der Aufgabenträger oder die ansonsten zuständige Behörde oder Einrichtung ergänzende Sicherheitsmaßnahmen vorsieht, um die Vertraulichkeit, Authentizität und Integrität der Datenübertragung sowie den Schutz der eigenen lokalen Systeme und Netze zu gewährleisten.

1.5
Sondernetze

Der Betreiber eines Sondernetzes übernimmt für sein Netz und im Rahmen seiner fachlichen Zuständigkeit die Aufgaben und Pflichten, die ansonsten vom Landesamt für Datenverarbeitung und Statistik (LDS) gemäß dieser Vorschrift zu erfüllen sind.

2
Internetnutzung

2.1
Firewall

Der Übergang zwischen dem LVN und dem Internet ist vom LDS unter Verwendung einer hochsicheren und von einer anerkannten Zertifizierungsinstanz in der Europäischen Union zu zertifizierenden Firewall zu sichern. Die Firewall ist im Rechenzentrum zu installieren und den dort geltenden Sicherheitsmaßnahmen zu unterwerfen. Das LDS wird Dienstanweisungen für die mit der Administration der Firewall betrauten Mitarbeiterinnen und Mitarbeiter erstellen, die dem besonderen Sicherheitsbedarf in angemessener Weise Rechnung tragen. Die Firewall darf funktional nur erweitert werden, wenn durch den Einsatz der notwendigen Produkte die Zertifizierung nicht gefährdet ist.

2.2
Elektronische Post (Sicherheitsklasse 1)

2.2.1
Dienste

In der Sicherheitsklasse 1 steht der Dienst "Elektronische Post" zur Nutzung zur Verfügung. Er erlaubt es, aus dem LVN heraus auf elektronischem Wege Post ins Internet zu versenden und auch von dort zu empfangen. Bezüglich der erreichbaren Teilnehmer im Internet gibt es keine Einschränkungen.

2.2.2
Zentrale Sicherheitsmaßnahmen

Die vom Internet empfangene elektronische Post ist durch das LDS im Rahmen der technischen und rechtlichen Möglichkeiten auf Viren zu prüfen. Wird ein Virus festgestellt, ist die elektronische Post auszusondern, zu archivieren und der Empfänger über den Vorgang zu informieren.

2.2.3
Lokale Sicherheitsmaßnahmen

Die jeweilige Behörde oder Einrichtung sollte zusätzliche Virenprüfungen vornehmen, da in zahlreichen Fällen eine zentrale Erkennung von Viren nicht möglich ist. Vertraulichkeit, Authentizität und Integrität können durch Verwendung der digitalen Signatur und Verschlüsselung erreicht werden.

2.2.4
Auftragsverfahren

Der Dienst "Elektronische Post" ist frei zugänglich. Eine gesonderte Beauftragung des LDS ist nicht erforderlich.

2.3
Internet und Foren (Sicherheitsklasse 2)

2.3.1
Dienste

In der Sicherheitsklasse 2 stehen die Dienste

- Nutzung des Internet (http)

- Nutzung von Dateiarchiven mit Hilfe eines Internet-Browsers (Anonyme Dateiübertragung über http)

- Teilnahme an offiziellen Internet-Diskussionsforen (nntp)

zur Verfügung.

2.3.2
Zentrale Sicherheitsmaßnahmen

Um die Sicherheit der genannten Dienste zu gewährleisten ist durch das LDS sicherzustellen, dass

- nur zugelassenen Behörden und Einrichtungen die Nutzung des angeforderten Dienstes möglich ist (auf Basis der IP-Adresse des Dienstevermittlers),

- nur der http- bzw. der nntp-Dienst verfügbar ist,

- ein Zugriff aus dem Internet auf das LVN nicht möglich ist.

2.3.3
Lokale Sicherheitsmaßnahmen

Von der jeweiligen Behörde oder Einrichtung sind Zugangs- bzw. Nutzungsregelungen festzulegen und auf dem lokalen Dienstevermittler (http- bzw. nntp-Proxy) umzusetzen.

2.3.4
Auftragsverfahren

Zur Nutzung der Dienste ist es notwendig, dass

- die jeweilige Behörde das LDS schriftlich mit der Freischaltung des Internet bzw. der Diskussionsforen beauftragt,

- noch nicht zur Verfügung stehende Diskussionsforen beim LDS schriftlich beauftragt werden. Für die Nutzung kostenpflichtiger Diskussionsforen sind entsprechende Kostenregelungen mit dem LDS zu treffen.

2.3.5
Technische Voraussetzungen

Zur Nutzung der Dienste ist von der Behörde oder Einrichtungen ein entsprechender Dienstevermittler (http- bzw. nntp-Proxy) einzurichten und zu betreiben.

2.4
Dateiübertragung und Fernzugriff (Sicherheitsklasse 3)

2.4.1
Dienste

In der Sicherheitsklasse 3 stehen die Dienste

- Dateiübertragung (ftp) und

- Fernzugriff (telnet)

zur Nutzung zur Verfügung.

In Erweiterung der Sicherheitsklasse 2 erlaubt es der Dateitransfer in dieser Klasse auch solche Dateiarchive bzw. Server zu nutzen, die eine Authentifizierung des Nutzers z.B. in Form eines Passwortes erwarten.

2.4.2
Zentrale Sicherheitsmaßnahmen

Eine Freigabe der beauftragten Dienste erfolgt ausschließlich personenbezogen. Zur Freigabe der Dienste wird dem jeweiligen Nutzer vom LDS das zur Authentifizierung gegenüber der Firewall notwendige Passwort mitgeteilt. Die beauftragten Dienste können nur von den Systemen der jeweiligen Behörde oder Einrichtung aus genutzt werden.

Am Internetübergang wird mit Hilfe einer Passwortabfrage sichergestellt, dass ausschließlich die vom LDS autorisierten Personen die für sie beauftragten Dienste nutzen können.

Ein Zugriff aus dem Internet auf Systeme im LVN ist nicht zulässig.

2.4.3
Lokale Sicherheitsmaßnahmen

Durch die Behörde oder Einrichtungen sind organisatorische Rahmenbedingungen zur Nutzung der Dienste festzulegen.

2.4.4
Auftragsverfahren

Zur Nutzung der Dienste ist es notwendig, dass das LDS schriftlich mit der Freischaltung von Nutzern beauftragt wird.

2.4.5
Technische Voraussetzungen

Um die Dienste dieser Sicherheitsklasse nutzen zu können ist durch die Behörde bzw. Einrichtung sicherzustellen, dass alle betroffenen Systeme innerhalb des lokalen Netzes

- namentlich durch einen einzurichtenden DNS-Dienst der Behörde aufgelöst werden können und

- von der Firewall aus zu erreichen sind.

2.5
Internetzugriff auf isolierte System im LDS
(Sicherheitsklasse 4**)**

2.5.1
Dienste

In Erweiterung der vorhergehenden Sicherheitsklassen ermöglicht die Sicherheitsklasse 4 den Zugang aus dem Internet auf isolierte Systeme im LDS. Zu den isolierten Systemen zählen Systeme, die

- außer der Verbindung ins Internet keine weiteren Anbindungen zu Netzen oder Systemen der Landesverwaltung haben (sog. "Stand-alone" Systeme),

- auf Grund von systemtechnischen Eigenschaften ebenfalls als Stand-alone Systeme betrachtet werden können. Diese Eigenschaft ist durch ein Zertifikat einer anerkannten europäischen Zertifizierungsinstanz für das jeweilige System vor Inbetriebnahme nachzuweisen.

Hinsichtlich der auf isolierten Systemen nutzbaren Dienste gibt es keine Einschränkungen.

2.5.2
Zentrale Sicherheitsmaßnahmen

Für isolierte Systeme sind keine weiteren Sicherheitsmaßnahmen notwendig.

2.5.3
Auftragsverfahren

Über die beabsichtigte Realisierung von Verfahren gemäß der Sicherheitsklasse 4 ist das LDS rechtzeitig zu unterrichten.

3
Kommunikation mit anderen Stellen der öffentlichen Verwaltung

3.1
Anbindung an das LVN

Die Anbindung von Kommunikationspartnern anderer öffentlicher Verwaltungen an das LVN erfolgt grundsätzlich über TESTA.

Soweit das Internet für die Kommunikation genutzt werden soll, gelten die Bestimmungen gemäß Nr. 2.

In Ausnahmefällen kann der Zugang für einen Übergangszeitraum auch unter Nutzung anderer Kommunikationsverbindungen erfolgen, soweit eine eindeutige Identifizierung des jeweils zugelassenen Kommunikationspartners gewährleistet werden kann. Dabei sind die vom LDS verwalteten IP-Adressbereiche zu verwenden.

3.2
Dienste

Die notwendigen Dienste sind verfahrensspezifisch festzulegen, wobei vorrangig die Dienste einzusetzen sind, die auch im Internet allgemein verwendet werden.

3.3
Zentrale Sicherheitsmaßnahmen

Das LDS hat sicherzustellen, dass

- die Kopfstelle des Kommunikationspartners (auf Basis der IP-Adresse) eindeutig identifiziert wird, und

- nur Verbindungen zu den am Verfahren beteiligten Systemen innerhalb der Landesverwaltung aufgebaut werden können.

3.4
Sonstige Sicherheitsmaßnahmen

Die für das Verfahren notwendigen sonstigen Sicherheitsmaßnahmen sind entsprechend den IT-Richtlinien - RdErl. des Innenministers v. 15.7.1996 (SMBl. NRW. 20025) - durch den Aufgabenträger festzulegen. Im Rahmen des verfahrensspezifischen Sicherheitskonzepts sind die geeigneten und notwendigen Maßnahmen, beispielsweise

- zur Authentifizierung der berechtigten Nutzer,

- zur Wahrung der Integrität der Daten oder

- zur Beschränkung des Zugriffs auf die zulässigen Systeme und Daten

festzulegen.

3.5
Auftragsverfahren

Die zuständige oberste Landesbehörde beauftragt in Abstimmung mit dem Innenministerium das LDS mit der Einrichtung der notwendigen Kommunikationsverbindungen und -dienste.

4
Verhalten im Schadensfall

4.1
Zentrale Maßnahmen

Bei festgestellten erheblichen Sicherheitsverletzungen am Internetübergang, an den Zugangspunkten im LVN oder sonstigen Bereichen wird der betroffene Bereich geschlossen bzw. das betroffene Kommunikationsverfahren durch das LDS unterbrochen. Das LDS hat in diesem Fall unverzüglich die notwendigen und geeigneten Maßnahmen zur Schadensbegrenzung und –be-

hebung zu treffen. Über die festgestellten Sicherheitsverletzungen ist das Innenministerium sowie ggf. der Aufgabenträger zu informieren.

4.2
Lokale Maßnahmen

Alle Mitarbeiterinnen und Mitarbeiter der Landesverwaltung haben den jeweiligen Netzbetreiber unverzüglich über festgestellte Sicherheitsverletzungen in Kenntnis zu setzen. Der Netzbetreiber hat in diesen Fällen unverzüglich die notwendigen und geeigneten Maßnahmen zur Schadensbegrenzung und -behebung zu treffen.

5
Protokollierungen

5.1
Zweck

Das LDS protokolliert anfallende Daten zum Zweck

- der Fehleranalyse und –beseitigung,

- der Bedarfsanalyse sowie

- zum Nachweis gefährdender Aktivitäten.

5.2
Internetnutzung

5.2.1
Sicherheitsklasse 1

In der Sicherheitsklasse 1 werden am Internetübergang für den Dienst "Elektronische Post" die folgenden Daten protokolliert:

- Quelladresse

- Zieladresse

- Zeitpunkt der Verschickung

- Größe der übermittelten Post.

Die protokollierten Verkehrsdaten sind über einen Zeitraum von einem Monat aufzubewahren und anschließend vollständig zu löschen.

5.2.2
Sicherheitsklasse 2

Bei der Nutzung der Dienste dieser Sicherheitsklasse werden durch das LDS, im Gegensatz zu den anderen Sicherheitsklassen, keine personenbezogenen Daten erhoben, da in den protokol-

lierten Verkehrsdaten lediglich ein Bezug auf die abrufende Behörde existiert (IP-Adresse des Dienstevermittlers).

Die protokollierten Verkehrsdaten sind über einen Zeitraum von sechs Monaten aufzubewahren und anschließend vollständig zu löschen.

5.2.3
Sicherheitsklasse 3

In der Sicherheitsklasse 3 werden für den Dienst "Dateiübertragung" folgende personenbezogene Verkehrsdaten protokolliert:

- Alias des Nutzers (Pseudonym)

- Adresse und Name des Startsystems

- Adresse und Name des Zielsystems

- Uhrzeit des Verbindungsauf- und -abbaus

- Benutzte Dienste

- Übertragenes Datenvolumen

- Passwörter des Zielsystems.

Neben den genannten Daten wird für den Dienst "Fernzugriff" der vollständige Sitzungsinhalt protokolliert.

Die Verkehrsdaten sind über einen Zeitraum von sechs Monaten aufzubewahren und anschließend vollständig zu löschen.

Eine Zuordnung des in den Protokolldateien benutzten Alias zu der zugehörigen natürlichen Person darf nur mit Hilfe einer im LDS unter Verschluss zu haltenden Tabelle möglich sein. Eine Auswertung der so personifizierten Daten durch das LDS ist nur nach schriftlichem Auftrag der jeweiligen Behörde oder Einrichtung statthaft; das Ergebnis ist vertraulich zu behandeln und darf ausschließlich dem Auftraggeber zur Verfügung gestellt werden.

5.2.4
Sicherheitsklasse 4

In der Sicherheitsklasse 4 sind durch den Betreiber des jeweiligen Systems Regelungen zu den Protokollierungen festzulegen.

5.3
Kommunikation mit anderen Stellen der öffentlichen Verwaltung

Bei der Kommunikation von Stellen anderer öffentlicher Verwaltungen mit Teilnehmern des LVN findet im LDS eine Protokollierung nur statt wenn

- diese bereits im verfahrensspezifischen Sicherheitskonzept des Aufgabenträgers vorgesehen ist oder

- das LDS einen schriftlichen Auftrag des jeweiligen Aufgabenträgers erhält.

Anlage

Sicherheitsregelungen für die externe Fernwartung in der Landesverwaltung

Die nachfolgenden Sicherheitsregelungen ergänzen die Maßnahmeempfehlungen für den mittleren Schutzbedarf des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik. Die Anwendung des IT-Grundschutzhandbuches ist mit RdErl. des Ministeriums für Inneres und Justiz vom 22.08.1998 (SMBl. NRW. 20025) empfohlen worden.

Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Sollte sich nach Prüfung des Aufgabenträgers ergeben, dass auf eine externe Fernwartung nicht verzichtet werden kann, so sind die Gründe aktenkundig zu machen.

Zusätzliche Sicherungsmaßnahmen:

1.
Aufbau der Verbindung

Der Aufbau der Verbindung für eine externe Fernwartung sollte immer vom lokalen IT-System initiiert werden. Davon kann aus technischen, wirtschaftlichen oder organisatorischen Gründen abgesehen werden, wenn die Behörde vor dem Aufbau der Verbindung ihr Einverständnis erteilt hat. Hierzu muss von der Behörde eine verantwortliche Person benannt werden.

2.
Authentifizierung

Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Hierzu sollten Einmalpaßwörter verwendet werden, die am Ende der Sitzung vom Systemverwalter zurückgesetzt werden. Der Behörde ist freigestellt, weitere Authentifizierungsmechanismen einzusetzen.

3.
Protokollierung

Alle Tätigkeiten bei der Durchführung der externen Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden. Im Einvernehmen mit der Behörde kann auch eine zentrale Protokollierung vorgenommen werden, z.B. im betreuenden Rechenzentrum.

4.
Einschränkung der Rechte des Wartungspersonals

Das Wartungspersonal sollte nicht die vollen Administrationsrechte besitzen. Falls in besonderen Fällen darauf nicht verzichtet werden kann, hat der Systemverwalter vor Ort den Ablauf der Fernwartung über die gesamte Dauer mitzuverfolgen.

5.
Personenbezogene Daten
Datenverarbeitungssysteme sind grundsätzlich so zu gestalten, dass bei ihrer Wartung nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht gewährleistet ist, hat die Daten verarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.

6.
Benutzerkennung für das Wartungspersonal

Für das Wartungspersonal ist auf dem IT-System eine eigene Benutzerkennung einzurichten unter der alle Wartungsarbeiten durchgeführt werden.

7.
Zwangslogout

Wird die Verbindung zur Fernwartungsstelle unterbrochen, so muss der Zugriff auf das System durch einen Zwangslogout beendet werden.

8.
Abbruch der Fernwartung

Es muss jederzeit die Möglichkeit geben, die Fernwartung von Seiten der Mitarbeiter der Behörde abzubrechen.

9.
Daten oder Programme des Wartungspersonals

Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so dürfen diese nur unter besonderer Kennung des Wartungspersonals in einem eigenen Verzeichnis abgelegt werden.

In Ergänzung zu den vorstehenden Sicherheitsregelungen sind für die Fernwartung vertragliche Regelungen, insbesondere hinsichtlich der Geheimhaltung der Daten sowie der Pflichten und Kompetenzen des externen Wartungspersonals zu treffen sowie auf die vorliegenden Sicherheitsregelungen Bezug zu nehmen. Der Vertrag ist mit den von der Fernwartung betroffenen Ressorts sowie dem Netzbetreiber abzustimmen.

MBl. NRW 2000 S. 152