Sachstandsbericht

Erhebung des Umsetzungsstands zu den Anschlussbedingungen

18. August 2017, Version 1.0

1. Einleitung

Auf Basis von § 4 IT-Netz-Gesetz hat der IT-Planungsrat in seiner 16. Sitzung am 18. März 2015 die Anschlussbedingungen für das Verbindungsnetz mit verbindlicher Wirkung beschlossen (Entscheidung 2015/02). Die Ausarbeitung der Anschlussbedingungen war im Rahmen der Leitlinie für Informationssicherheit in der öffentlichen Verwaltung, die der IT-Planungsrat in seiner 10. Sitzung am 8. März 2013 beschloss, festgelegt worden. Die Anschlussbedingungen sind spätestens bis zum 31.12.2017 umzusetzen.

Gemäß Beschluss des IT-Planungsrats in seiner 20. Sitzung am 16. Juni 2016 wurde der Umsetzungsstand der Anschlussbedingungen zum 31.12.2016 erhoben. Damit sollte angesichts der stetig zunehmenden Bedrohung der Informationssicherheit ein aktueller Überblick über den Umsetzungsstand der Anschlussbedingungen gewonnen werden. Ferner sollten durch die Erhebung eventuelle Schwierigkeiten rechtzeitig vor Ablauf der Umsetzungsfrist identifiziert und ein Umgang damit abgestimmt werden.

In seiner 23. Sitzung am 22. Juni 2017 befasste sich der IT-Planungsrat erneut mit dem Thema, da der Rücklauf zur Rückgabefrist Ende Januar 2017 unzureichend war. Er beschloss

(Entscheidung 2017/24):

1. Der IT-Planungsrat bittet die Teilnehmer am Verbindungsnetz, den Bund bei der Erstellung des Berichtes gemäß dem Beschluss 2016/21 bis zum 30. Juni 2017 zu unterstützen.
2. Das Arbeitsgremium Verbindungsnetz und der Bund werden um Vorlage des Sachstandsberichts zur Herbstsitzung des IT-Planungsrats im Jahr 2017 gebeten.

Der hier vorliegende Sachstandsbericht wurde durch den Bund und das Arbeitsgremium Verbindungsnetz erstellt und fasst Verlauf und Ergebnis der Erhebung für den IT-Planungsrat zusammen.

2. Verlauf der Erhebung

Das Formular sollte laut Beschluss des IT-Planungsrats bis zum 31.01.2017 an die Koordinierungsstelle Verbindungsnetz beim Bundesverwaltungsamt übersandt werden.

Danach war eine Auswertung durch den Bund und das Arbeitsgremium Verbindungsnetz sowie eine Unterrichtung des IT-Planungsrats in der Sommersitzung des Jahres 2017 vorgesehen.

Nach Ablauf der Frist hatten jedoch nur ca. 50% der Verbindungsnetzteilnehmer geantwortet. Nach zweimaliger Erinnerung waren es ca. 60%. Auch zum 30.06.2017, nach erneuter Befassung des IT-Planungsrats, haben 19 von 92 Teilnehmern nicht geantwortet. Vier Teilnehmer haben um Fristverschiebung gebeten.

Eine Übersicht über die Rückmeldungen ist diesem Sachstandsbericht als Anlage angefügt.

3. Zusammenfassung der Auswertung

Wie oben dargestellt haben nur ca. 80% der angeschriebenen Teilnehmer die Erhebung beantwortet. Unter den Antworten finden sich wiederum zahlreiche Fälle, in denen die Umsetzung der Anschlussbedingungen in zentralen Punkten nicht erfolgt ist und auch nicht bis Ende 2017 geplant ist. Ein Teilnehmer hat nahezu alle Fragen mit „Nein“ beantwortet.

Einige Teilnehmer aus dem Kreis der Kommunen verwiesen auf die Stellungnahme der Vitako[1] zur Umsetzung der Anschlussbedingungen vom 12. Januar 2017. Diese Stellungnahme wird auf der Sitzung der AG InfoSic am 13./14.09.2017 erörtert.

4. Vorgehensvorschlag

Die Erhebung zeigt, dass das durch den IT-Planungsrat in seiner Entscheidung 2015/02 vorgegebene Ziel, die Umsetzung der Anschlussbedingungen bis zum 31.12.2017 voraussichtlich nicht erreicht wird.

Der Bund und das Arbeitsgremium Verbindungsnetz empfehlen daher dem IT-Planungsrat, die zeitnahe Beachtung der Anschlussbedingungen durchzusetzen. Im Einzelnen empfehlen sie:

- die Wiederholung der Abfrage zum Stichtag 1. Januar 2018 zu veranlassen
- die Beantwortung bis zum 31.03.2018 verbindlich einzufordern
- im Anschluss eine Arbeitsgruppe einzusetzen und diese mit der Auswertung der Ergebnisse sowie der Erarbeitung einer Empfehlung zum Umgang mit Abweichungen gemäß Ziffer 8. der Anschlussbedingungen bis zur Sommersitzung 2018 des IT-Planungsrats zu beauftragen.

[1] „Stellungnahme zur Umsetzung der Vorgaben nach den Anschlussbedingungen an das Verbindungsnetz für kommunale Anschlussnehmer“

5. Anhang: Antworten zu den Einzelfragen

Frage 1

„Wurden die beim Teilnehmer eingesetzten Infrastrukturen, die von dem in Kap. 3 der [AB][2] definierten Geltungsbereich umfasst sind, identifiziert und dokumentiert? (Im Folgenden: „konkreter Geltungsbereich")"

Ja:	53
Nein:	16
Indifferent:	3
Keine Antwort/Offen:	1

9 Teilnehmer, die mit „Nein" geantwortet haben, planen die Umsetzung der entsprechenden Forderung bis Ende 2017.

Frage 2

Werden im „konkreten Geltungsbereich" die BSI-Standards 100-1 bis 100-4 gemäß Kap. 3.2 der [L-IS][3] umgesetzt?

Ja:	27
Nein:	33
Indifferent:	12
Keine Antwort/Offen:	1

Insgesamt haben 15 Teilnehmer die genannten BSI-Standards teilweise eingeführt oder eine Einführung bis 2018 geplant.

Frage 3

Wurde für die Teile des „konkreten Geltungsbereichs" der Schutzbedarf gemäß BSI-Standards festgestellt und dabei berücksichtigt, dass für:

- das Sicherheits-Gateway am Übergangspunkt zum Verbindungsnetz,
- die Netzübergänge an andere Netze und

[2] Anschlussbedingungen

[3] Leitlinie für Informationssicherheit in der öffentlichen Verwaltung

- die dafür notwendigen Managementsysteme ein hoher Schutzbedarf durch [AB] festgelegt ist?

Ja: 43

Nein: 25

Indifferent: 5

9 Teilnehmer, die mit „Nein“ geantwortet haben, planen die Umsetzung der entsprechenden Forderung bis Ende 2017.

Frage 4

Erfolgt die Datenübertragung in den Teilen des „konkreten Geltungsbereichs“, für die gemäß Kap. 4 der [AB] der hohe Schutzbedarf festgestellt wurde bzw. festgelegt ist, verschlüsselt mit Produkten, die gem. § 37 Absatz 1 VSA des Bundes vom BSI zugelassen wurden?

Ja: 24

Nein: 40

Indifferent: 5

Keine Antwort/Offen: 4

Die 5 indifferenten Antworten sind eher als „nein“ zu werten.

Frage 5

"Wurde die Empfehlung umgesetzt, darüber hinaus die durchgängige Verschlüsselung durch BSI-zugelassene Kryptosysteme in allen Verwaltungsnetzen umzusetzen?“

Ja: 15

Nein: 56

Indifferent: 0

Keine Antwort/Offen: 2

Zahlreiche Teilnehmern, die hier mit „Nein“ antworteten, verwiesen direkt oder indirekt auf die Protokollnotiz zum Tagesordnungspunkt 5 („Anschlussbedinungen an das Verbindungsnetz“) der 16. Sitzung des IT-Planungsrats („Der Freistaat Thüringen geht davon aus, dass die Anschlussbedingungen Verbindungsnetz so zu verstehen sind, dass Datenströme mit hohem Schutzbedarf nur dann mittels der in Tz. 5.1 genannten Produkte zu verschlüsseln sind, wenn das Rechenzentrum aus mehreren Liegenschaften besteht, die nicht über ein eigenes Netz

miteinander verbunden sind und hierüber genannte Daten mit hohem Schutzbedarf übertragen werden.“)

Frage 6

"(Optional) Wenn die Frage zuvor mit Nein beantwortet wurde: Werden anderen Verfahren zur durchgängigen Verschlüsselung in den Verwaltungsnetzen im Sinne einer Basissicherheit eingesetzt?"

Ja:	18
Nein:	31
Indifferent:	4
Keine Antwort/Offen:	20

Frage 7

"Erfolgt am Übergang vom „konkreten Geltungsbereich“ zum Verbindungsnetz eine Trennung durch ein Sicherheits-Gateway (i.d.R. bestehend aus Application-Gateway und Paketfilter)?"

Ja:	66
Nein:	1
Indifferent:	5
Keine Antwort/Offen:	1

Frage 8

"Wird das in der Frage zuvor genannte Sicherheits-Gateway durch geschultes Personal betrieben?"

Ja:	71
Nein:	1
Indifferent:	0
Keine Antwort/Offen:	1

Frage 9

"Werden dabei Produkte mit nachgewiesenen Sicherheitsfunktionen im Rahmen einer BSI-Zertifizierung oder durch vom BSI anerkannte Zertifikate mit EAL4+ eingesetzt?"

Ja:	40
Nein:	25
Indifferent:	5
Keine Antwort/Offen:	3

Frage 10

"Wurde die Empfehlung umgesetzt, darüber hinaus alle anderen Sicherheits-Gateways zum „konkreten Geltungsbereich“ entsprechend auszulegen?"

Ja:	42
Nein:	27
Indifferent:	2
Keine Antwort/Offen:	2

Frage 11

"Werden im „konkreten Geltungsbereich“ folgende Maßnahmen zur Abwehr von Angriffen umgesetzt?

- Auswertung von Logdaten (mindestens an den Sicherheits-Gateways und Dienste-Servern)
- Einsatz von Angriffserkennungssystemen (z.B. IDS, SIEM,..),
- Einsatz von Systemen zur Abwehr von Schadprogrammen"

Ja:	43
Nein:	8
Indifferent:	22

Frage 12

"Wurde ein Konzept erstellt, das regelt, welche Logdaten an welchen Stellen im „konkreten Geltungsbereich“ erfasst werden müssen, um Angriffe erkennen zu können?

Sind dabei folgende Aspekte umfasst?

- Mindestens an Sicherheits-Gateways und Dienste-Server werden Logdaten erhoben.
- Die erfassten Logdaten werden zum Zweck der Angriffserkennung und -identifikation regelmäßig durch qualifiziertes Personal ausgewertet.
- Die nach rechtlichem Rahmen zulässigen Speicherfristen werden ausgeschöpft.

Wird das Konzept umgesetzt?"

Ja:	28
Nein:	35
Indifferent:	9
Keine Antwort/Offen:	1

Frage 13

"Besitzen alle Netzübergänge einen abhängig vom Schutzbedarf angemessenen Schutz vor Verfügbarkeitsangriffen (z.B. Distributed Denial of Service Angriffe)?"

Ja:	42
Nein:	26
Indifferent:	5

Frage 14

"Ist durch entsprechende IT-Sicherheitsmaßnahmen dafür gesorgt, dass Angriffe über indirekt angeschlossene Netze (z.B. das Internet) sich nicht auf Teile des „konkreten Geltungsbereichs“ auswirken?"

Ja:	65
Nein:	5
Indifferent:	1
Keine Antwort/Offen:	2

Frage 15

"Erfolgt das Einspielen von Sicherheitspatches umgehend im Rahmen definierter und dokumentierter Betriebs- und Änderungsprozesse?"

Ja:	59
Nein:	8
Indifferent:	6

Frage 16

"Ist der Teilnehmer in das Bund/Landes-ISMS gemäß Kapitel 3.4 der [L-IS] eingebunden? Sind insbesondere die Meldewege zwischen Teilnehmer und Bund/Landes-CERT festgelegt und dokumentiert?"

Ja:	26
Nein:	43
Indifferent:	2
Keine Antwort/Offen:	2

Das Ergebnis bestätigt die folgende Feststellung im Bericht zur Umsetzung der [L IS] an den IT-Planungsrat zur 20. Sitzung am 16.03.2016: „Die Einführung eines ISMS stellt aus Sicht der AG Informationssicherheit weiterhin mit Abstand die größte Bund/Länder-übergreifende IT-Herausforderung dar, bedingt durch die immer noch bestehende große Heterogenität in Bund und Ländern. Hinzu kommt ein weitreichender Interpretationsspieleraum beim Erreichungsgrad in Qualität und Quantität."

Frage 17

"Sind die Mindestanforderungen an ein Informationssicherheitsmanagementsystem (ISMS) gemäß Kap. 3.1 der [L IS] auch für den „konkreten Geltungsbereich" erfüllt?"

Ja:	42
Nein:	21
Indifferent:	8
Keine Antwort/Offen:	2

Frage 18

"Liegt ein BSI-Zertifikat für den „konkreten Geltungsbereich“ vor?"

Ja:	11
Nein:	61
Indifferent:	1

Da die Anschlussbedingungen in vielen Fällen gerade erst umgesetzt sind oder sich noch in der Umsetzung befinden, war eine hohe Anzahl negativer Antworten zu erwarten.

Frage 19

"Wenn die Frage zuvor mit Nein beantwortet wurde:

Kann (schon) eine unabhängige Auditierung, die die Einhaltung der Anschlussbedingungen bestätigt, nicht älter als 3 Jahre ist und deren Auditor über entsprechende Qualifikationen verfügt, nachgewiesen werden?"

Ja:	4
Nein:	57
Indifferent:	1
Keine Antwort/Offen:	11

Siehe Bemerkung zu Frage 18.

Frage 20

"Ist ein Prozess etabliert und dokumentiert, mit dem Abweichungen von Sicherheitsanforderungen in den Anschlussbedingungen dem IT-Planungsrat sowie dem Betreiber für das Verbindungsnetz bekanntgemacht werden?"

Ja:	10
Nein:	60
Indifferent:	0
Keine Antwort/Offen:	3