Kooperationsgruppe „Informationssicherheit des IT-PLR“

Leitlinie für die Informationssicherheit

in der öffentlichen Verwaltung

- Umsetzungsplan -

Stand 19.02.2013

Version 1.6 (10. IT-Planungsrat Beschluss 2013/01)

Inhaltsverzeichnis

0 Allgemeines 3

1 Informationssicherheitsmanagement 3

2 Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung..... 5

3 Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren 5

4 Gemeinsame Abwehr von IT–Angriffen..... 5

5 Standardisierung und Produktsicherheit 6

0 Allgemeines

Ab Inkrafttreten dieser Leitlinie

1. Überführung der Kooperationsgruppe in eine ständige Arbeitsgruppe Informationssicherheit des IT-PLR. Die Arbeitsgruppe setzt sich aus den benannten Vertretern der Mitglieder zusammen und erarbeitet gemeinsam Vorschläge zur Weiterentwicklung der Leitlinie und sowie einen jährlichen Bericht zur Erfolgskontrolle für den IT-PLR. Sie dient außerdem dem regelmäßigen Austausch zu Themen der Informationssicherheit unterhalb des IT-PLR. Die Arbeitsgruppe berücksichtigt die Standardisierungsagenda des IT-PLR und kooperiert mit dem BSI bzgl. Standards für Informationssicherheit.

   [**KOSTEN**: Keine zusätzlichen Kosten erwartet]

2. Der erreichte Stand der Umsetzung des vorliegenden Umsetzungsplans ist jährlich intern zu evaluieren und im Rahmen der Erfolgskontrolle dem IT-PLR vorzulegen. Etwaige Vorschläge für eine Anpassung oder Fortschreibung des Umsetzungsplans werden durch die Arbeitsgruppe aus 1. vorbereitet und bedürfen einer Freigabe durch den IT-PLR.
   [**KOSTEN**: Keine zusätzlichen Kosten erwartet]

1 Informationssicherheitsmanagement

Innerhalb 5 Jahre nach Inkrafttreten dieser Leitlinie:

Einführung von ISMS und Vereinheitlichung in folgender Priorität (Umsetzungsstand wird im Rahmen der jährlichen Erfolgskontrolle erfasst und an den IT-PLR berichtet – s. o. Punkte 1, 2):

3. Benennung der Landes-/Bundes-IT-Sicherheitsbeauftragten
4. Benennung der IT-Sicherheitsbeauftragten für die wesentlichen Behörden
   [**KOSTEN**: 1 VZÄ für den jeweiligen Landes-/Bundes-IT-Sicherheitsbeauftragten. Restlicher Bedarf abhängig von Anzahl, Größe und Komplexität der Behörden]
5. Verabschiedung der jeweiligen verbindlichen Leitlinie für die Informationssicherheit

[**KOSTEN**: Für Verabschiedung keine zusätzlichen Kosten erwartet. Umsetzungskosten abhängig von der konkreten Ausgangslage im jeweiligen Zuständigkeitsbereich.]

6. Einführung eines ISMS auf Basis ISO 27001 oder IT-Grundschutz. Hierzu gehören insb. :
    a. IT-Sicherheitskonzepte werden erstellt
    b. Abläufe bei IT-Sicherheitsvorfällen sind festgelegt und dokumentiert
    c. Prozesse eingerichtet, mit denen Umsetzung, Wirksamkeit und Beachtung der Sicherheitsmaßnahmen regelmäßig kontrolliert und die Einleitung ggf. erforderlicher Maßnahmen (z. B. Fortschreibung Sicherheitskonzepte) gewährleistet wird
    d. Anforderungsgerechte, einheitliche Fortbildung der IT-Sicherheitsbeauftragten

    [**KOSTEN**: Abhängig von der konkreten Ausgangslage im jeweiligen Zuständigkeitsbereich. Diskutiert wurde ein prozentualer Ansatz in Abhängigkeit von IT-Ausgaben. Ansatz wurde verworfen, da IT-Ausgaben oft in Haushaltstiteln „versteckt" sind und die tatsächlichen Kosten von zahlreichen weiteren individuellen Faktoren (z.B. den Organisationsstrukturen, der Komplexität IT-Landschaft, dem individuellen Schutzbedarf oder den unterstützten Fachaufgaben) abhängig sind.]
7. Vereinheitlichung der ISMS orientiert an IT-Grundschutz

    [**KOSTEN**: Konkrete Kosten abhängig von der individuellen Ausgangslage im jeweiligen Zuständigkeitsbereich.]

Sonstige Daueraufgaben

8. Jahrestagung der IT-Sicherheitsbeauftragten zum gegenseitigen Erfahrungsaustausch (Verantwortung für Organisation wechselt mit Vorsitz im IT-Planungsrat)

    [**KOSTEN**: Erwartete Kosten von ca. 10.000 € für Durchführung einer Jahrestagung.]
9. Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit.

    [**KOSTEN**: Abhängig von Anzahl der Beschäftigten und deren jeweiligen konkreten Aufgaben sowie bereits erfolgten Informationen, Weiterbildungen und Sensibilisierungen]

2 Absicherung der Netzinfrastrukturen der öffentlichen Verwaltung

Innerhalb 1 Jahr nach Inkrafttreten dieser Leitlinie

10. Verabschiedung der Anschlussbedingungen durch Bund und Länder gemeinsam im Koordinierungsgremium für das Verbindungsnetz (IT-PLR) gemäß §4 IT-NetzG unter Beachtung der vereinbarten Rahmenbedingungen und Ziele (s. Hauptdokument Kapitel 3.2). Der Bund wird dem Koordinierungsgremium (IT-PLR) einen Vorschlag für die Anschlussbedingungen vorlegen.

    [**KOSTEN**: Für Verabschiedung keine zusätzlichen Kosten erwartet. Kosten für Umsetzung der Anschlussbedingungen (z.B. Anwendung BSI-Standards) abhängig von der konkreten Ausgangslage im jeweiligen Netz.]

3 Einheitliche Sicherheitsstandards für Ebenen-übergreifende IT-Verfahren

Ab Inkrafttreten dieser Leitlinie

11. Bei der Planung und Anpassung Ebenen-übergreifender IT-Verfahren ist der IT-Grundschutz nach BSI anzuwenden.

    [**KOSTEN**: Kosten abhängig vom konkreten IT-Verfahren. Aus Sicht der Länder ggf. prozentual von den Gesamtkosten des Verfahrens abschätzbar. Konkrete Erfahrungswerte liegen jedoch (auch im BSI) nicht vor.]

Innerhalb 1 Jahr nach Inkrafttreten dieser Leitlinie

12. Erfassung und Beschreibung der im jeweiligen Bereich betriebenen Ebenen-übergreifenden IT-Verfahren, insbesondere der kritischen Ebenen-übergreifenden IT-Verfahren.

    [**KOSTEN**: Keine zusätzlichen Kosten erwartet]

4 Gemeinsame Abwehr von IT–Angriffen

Innerhalb 1 Jahr nach Inkrafttreten dieser Leitlinie

13. Beginn des Aufbaus der Landes-CERTS

[**KOSTEN**: Kosten für Aufbau der Landes-CERTs: ca. 100 T€ pro VZÄ.. Weitere Erfahrungswerte: NI: ca. 500 T€ bei 5 VZÄ, NW: ca. 625 T€ bei 6 VZÄ]

14. Verabschiedung der Geschäftsordnung für den VerwaltungsCERT-Verbund unter Beachtung der vereinbarten Rahmenbedingungen und Ziele (s. Hauptdokument Kapitel 3.4).

    [**KOSTEN**: Keine zusätzlichen Kosten erwartet. Kosten für Umsetzung abhängig von der konkreten Ausgangslage im jeweiligen CERT]

15. Gewährleistung der Erreichbarkeit von für IT-Krisen relevanten Stellen und Benennung von entsprechenden Ansprechstellen für die IT-Krisenreaktion zur Warnung, Alarmierung und Krisenreaktion. Dies betrifft Organisationen auf ministerieller Ebene, in den Kopfstellen und CERTs, bei den Betreibern der Verwaltungsnetze und von IT-Dienstleistungen sowie in den relevanten Behörden und Einrichtungen. Hierfür sind die für IT-Krisen relevanten Stellen zu identifizieren. Diese müssen mit den notwendigen Kompetenzen und Ressourcen ausgestattet sein, im IT-Krisenfall geeignet reagieren zu können. Zudem sind die für die IT-Sicherheit in Verwaltungsnetzen zuständigen Stellen geeignet in die Prozesse des VerwaltungsCERT-Verbunds einzubinden. Kurzfristig ist insb. der Kontakt zu den Kopfstellen herzustellen, um die Weitergabe von Material zu gewährleisten.

    [**KOSTEN**: Keine zusätzlichen Kosten erwartet]

Innerhalb 3 Jahre nach Inkrafttreten dieser Leitlinie

16. Aufbau Landes-CERTS abgeschlossen

    [**KOSTEN**: Kosten für Aufbau der Landes-CERTs: ca. 100 T€ pro VZÄ. Weitere Erfahrungswerte: NI: ca. 500 T€ bei 5 VZÄ, NW: ca. 625 T€ bei 6 VZÄ]

5 Standardisierung und Produktsicherheit

Innerhalb 2 Jahre nach Inkrafttreten dieser Leitlinie

17. Erarbeitung eines Konzeptes für die regelmäßige Bedarfsermittlung und gemeinsame Festlegung von Mindestsicherheitsanforderungen für sichere Produkte, Systeme und Verfahren notwendig mit dem Ziel, gemeinsame Basiskomponenten einzusetzen. [**KOSTEN**: Keine zusätzlichen Kosten erwartet]