Arbeitsgruppe Informationssicherheit

Beschluss Nr. 02/2014 vom 22. Mai 2014 – Handlungsempfehlungen und Umsetzungsplan zum verbesserten Einsatz von Verschlüsselungsverfahren

Die AG IS beschließt die in der Anlage aufgeführten Handlungsempfehlungen zum verbesserten Einsatz von Verschlüsselungsverfahren sowie den damit verbundenen Umsetzungsplan. Ziel ist eine deutliche Erhöhung der Informationssicherheit für die Webzugänge und den Datenaustausch im und zum SVN. Der AK ITEG wird um Zustimmung gebeten.

Begründung: Im Licht der NSA-Affäre besteht erhöhte Aufmerksamkeit in der Öffentlichkeit für veraltete Verschlüsselungslösungen, wie bereits z.B. das BSI selbst erfahren musste. In der Landesverwaltung Sachsen besteht hier derzeit noch erheblicher Handlungsbedarf, wie die vorliegende Erhebung des IST-Zustandes nachweist. Auf Basis der vorgeschlagenen, realistisch umsetzbaren Maßnahmen kann jedoch kurzfristig eine deutliche Verbesserung des Informationssicherheitsniveaus erreicht werden.

Beschluss 5/2014
Umlaufbeschluss vom 18. Juli 2014

1. Der AK ITEG begrüßt den Beschluss Nr. 02/2014 „Handlungsempfehlungen und Umsetzungsplan zum verbesserten Einsatz von Verschlüsselungsverfahren“ der AG IS vom 22. Mai 2014.

2. Die Mitglieder des AK ITEG wirken auf eine Ausführung der Handlungsempfehlungen und des Umsetzungsplans in ihrem Geschäftsbereich hin.

3. Das SMJus wird gebeten, die durchgängige Grundverschlüsselung der Leitungen im SVN mindestens als Option in die SVN 2.0-Ausschreibungsunterlagen aufzunehmen (anstelle der bisherigen Einzelfall-Lösung über den SVN-Warenkorb).

Anlage zum Beschluss Nr. 02/2014
der AG IS vom 22. Mai 2014

STAATSMINISTERIUM
DER JUSTIZ
UND FÜR EUROPA

Freistaat
SACHSEN

Kernteam Verschlüsselung

Handlungsempfehlungen

Handlungsempfehlungen

Themenfeld I: Sicherer Webzugang, Schwerpunkt HTTPS

- I.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
  - I.1.A - Zentrale Erfassung von Domains, Diensten und Zuständigkeiten
  - I.1.B - Definierte Prozesse zur Neubeauftragung, Aktualisierung und Abschaltung
- I.2 Strategische Verschlüsselungsempfehlungen
  - I.2.A - HTTPS-Verschlüsselung für alle Webseiten anbieten
  - I.2.B - mit HSTS die Nutzung von HTTPS erzwingen
  - I.2.C - mit Forward Secrecy die rückwirkende Entschlüsselung verhindern

Handlungsempfehlungen

Themenfeld I: Sicherer Webzugang, Schwerpunkt HTTPS

- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
  - I.3.A - Beseitigung von HTTPS-Zertifikatsfehlern (ungültig, abgelaufen, selbstsigniert) durch Einsatz von Zertifikaten der Sachsen Global CA
  - I.3.B - Zentrale Algorithmenunterstützung von TLS1.2, Abschaltung unsicherer Algorithmen wie RC4 und SSLv2
  - I.3.C - Härtung der HTTPS-Konfiguration zur Vermeidung von Angriffen wie Insecure Renegotiation, TLS-Compression, BEAST, CRIME und Heartbleed

Handlungsempfehlungen

Themenfeld II: Sicherer Datenaustausch im SVN

- II.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln
  - II.1.A - Grundverschlüsselung der Leitungen zwischen allen Behördenstandorten mindestens als Option in SVN 2.0-Ausschreibung aufnehmen
  - II.1.B - Aufnahme und Bewertung der Anforderungen an weitergehende Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung)
- II.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
  - II.2.A - Prüfung Aktualisierungsbedarf Hard- und Software im SVN bzgl. der Unterstützung moderner Verschlüsselungsverfahren
  - II.2.B - Ablösung unsicherer Verschlüsselungsalgorithmen im SVN (z.B. SHA-1 als Grundlage elektronischer Zertifikate der Landes-PKI)

Handlungsempfehlungen

Themenfeld II: Sicherer Datenaustausch im SVN

- II.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen
  - II.3.A - Flächendeckende Unterstützung von STARTTLS von und zu externen E-Mail-Partnern
  - II.3.B - Flächendeckende E-Mail-Verschlüsselung im SVN zwischen den Ressorts (Exchange-Konzept, Server-zu-Server Kommunikation)
  - II.3.C - Flächendeckende E-Mail-Verschlüsselung im SVN innerhalb der Behörden (Exchange-Konzept, hier: Outlook-Client-zu-Server Kommunikation)

Umsetzungsplan

Kurzfristige Maßnahmen (2. Quartal 2014)

*Alle dringlichen Maßnahmen, die sofort umgesetzt werden sollen, sind im Folgenden **fett gedruckt** hervorgehoben. Die anderen Maßnahmen sind noch näher zu untersetzen.*

- I.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
  - Das Kernteam legt einen entsprechenden Vorschlag vor.
- I.2 Strategische Verschlüsselungsempfehlungen
  - Die SVN-Leitstelle legt ein Angebot zu Kosten und Rahmenbedingungen zur zentralen Umstellung aller Webseiten der Landesverwaltung auf HTTPS vor.
- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
  - Das Kernteam legt eine Handlungsanleitung zur Umstellung auf Zertifikate der Sachsen Global CA und zur Beseitigung der vorhandenen Zertifikatsfehler für Systeme mit Apache und Microsoft IIS vor.

Umsetzungsplan

Kurzfristige Maßnahmen (2. Quartal 2014)

- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen (Fortsetzung)
  - **Alle Ressorts stellen die von ihnen betriebenen HTTPS-Seiten mit fehlerhaften Zertifikaten auf Zertifikate der Sachsen Global CA um, soweit möglich. Alle Zertifikatsfehler werden beseitigt.**
  - Das Kernteam erarbeitet auf Basis einer Erfassung der auf die Webseiten der Landesverwaltung zugreifenden Systeme eine Empfehlung der abzuschaltenden veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2. Nach **Beschluss durch die AG IS** erarbeitet das Kernteam eine entsprechende Handlungsanleitung zur Abschaltung veralteter Algorithmen für Systeme mit Apache und Microsoft IIS.
  - Analog zu den veralteten Algorithmen erarbeitet das Kernteam eine Empfehlung und - **nach Beschluss durch die AG IS** - eine Handlungsanleitung zur Härtung der HTTPS-Konfiguration.

Umsetzungsplan

Kurzfristige Maßnahmen (2. Quartal 2014)

- II.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln
  - **Die Grundverschlüsselung aller Leitungen wird vom SMJus mindestens als Option in SVN 2.0-Ausschreibungsunterlagen aufgenommen.**
- II.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
  - Das Kernteam erarbeitet auf Basis der auf die Landes-PKI zugreifenden Systeme eine Empfehlung der zu aktualisierenden Hard- und Software sowie zur Abschaltung unsicherer Verschlüsselungsalgorithmen.

Umsetzungsplan

Kurzfristige Maßnahmen (2. Quartal 2014)

- II.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen
  - Das Kernteam erstellt eine Handlungsanleitung für Outlook-Client-zu-Server-Verschlüsselung.
  - **Die Ressorts stellen flächendeckend auf verschlüsselte Exchange-Kommunikation um.**
  - **STARTTLS wird durchgängig umgesetzt, den Kommunen wird im Benehmen mit SAKD und KDN GmbH die Umsetzung empfohlen.**

Umsetzungsplan

Kurzfristige Maßnahmen (3. Quartal 2014)

- I.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
  - Prüfung des Vorschlags des Kernteams und **Beschluss der AG IS**.
- I.2 Strategische Verschlüsselungsempfehlungen
  - Prüfung des Angebots der SVN-Leitstelle zur flächendeckenden Umstellung auf HTTPS und **Beschluss der AG IS** zum weiteren Vorgehen.
  - Das Kernteam erarbeitet eine Empfehlung zur Umsetzung von HSTS und Forward Secrecy.
- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
  - Das Kernteam erarbeitet eine Empfehlung zur Umsetzung von TLS1.2.

Umsetzungsplan

Kurzfristige Maßnahmen (3. Quartal 2014)

- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen (Fortsetzung)
  - Die veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2 werden auf den zentralen Proxys (nach außen) abgeschaltet. Die HTTPS-Konfiguration wird gehärtet.
- II.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
  - Die Empfehlung des Kernteams der zu aktualisierenden Hard- und Software sowie zur Abschaltung unsicherer Verschlüsselungsalgorithmen wird geprüft. **Die AG IS fasst einen entsprechenden Beschluss**.

Umsetzungsplan

Mittelfristige Maßnahmen (4. Quartal 2014)

- I.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
  - Geregelte Prozesse zur Domainnamensverwaltung werden eingeführt.
- I.2 Strategische Verschlüsselungsempfehlungen
  - Prüfung der Empfehlung des Kernteams zur Umsetzung von HSTS und Forward Secrecy und **Beschluss der AG IS** zum weiteren Vorgehen.
  - Das Angebot zur flächendeckenden Umstellung auf HTTPS wird zentral (nach außen) umgesetzt.
- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
  - Prüfung der Empfehlung des Kernteams für die Unterstützung von TLS 1.2 und **Beschluss der AG IS** zum weiteren Vorgehen.

Umsetzungsplan

Mittelfristige Maßnahmen (4. Quartal 2014)

- I.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen (Fortsetzung)
  - Die veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2 werden auf den gehosteten Webseiten und auf allen HTTPS-Seiten der Ressorts abgeschaltet. Die HTTPS-Konfiguration wird gehärtet.
- II.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln
  - **Aufnahme und Bewertung der Anforderungen an weitergehende Verschlüsselungslösungen im SVN 2.0 durch das Kernteam mit den Ressorts.**
  - Die vom Kernteam vorgelegten Anforderungen an weitergehende Verschlüsselungslösungen werden geprüft und **von der AG IS beschlossen.** Anschließend nimmt das SMJus diese Anforderungen mindestens als Option in die SVN2.0-Ausschreibungsunterlagen auf.

Umsetzungsplan

Mittelfristige Maßnahmen (4. Quartal 2014)

- II.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
  - Die Ressorts aktualisieren veraltete, auf die Landes-PKI zugreifende Hard- und Software. Das SMJus schaltet die unsicheren Verschlüsselungsalgorithmen seitens der Landes-PKI ab.
- II.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen
  - **Alle Ressorts stellen flächendeckend auf verschlüsselte Kommunikation zwischen den Outlook-Clients und Exchange-Servern um.**

Umsetzungsplan

Mittel- und langfristige Maßnahmen

- I.2 Strategische Verschlüsselungsempfehlungen
  - Die flächendeckende Umstellung der gehosteten Webseiten sowie aller Internetseiten der Ressorts auf HTTPS wird im beschlossenen Umfang umgesetzt.
  - Das Kernteam erarbeitet eine Handlungsanleitung zur Umsetzung von HSTS und Forward Secrecy unter Apache und Microsoft IIS. Die Handlungsanleitung wird zunächst auf den zentralen Proxys und den gehosteten Webseiten, später auf allen HTTPS-Seiten der Ressorts umgesetzt.
  - TLS1.2 wird zunächst auf den zentralen Proxys und den gehosteten Webseiten, später auf allen HTTPS-Seiten der Ressorts umgesetzt.