Arbeitsgruppe Informationssicherheit

Beschluss Nr. 03/2014 vom 26. September 2014 – Abschaltung veralteter Verschlüsselungsalgorithmen und Härtung der HTTPS-Konfiguration

Die AG IS beschließt die in der Anlage aufgeführten Handlungsempfehlungen zur Abschaltung veralteter Verschlüsselungsalgorithmen wie RC4 oder SSL v2 und zur Härtung der HTTPS-Konfiguration. Ziel ist die weitere Verbesserung der Sicherheit der Internetseiten und -dienste der Landesverwaltung. Der AK ITEG wird um Zustimmung gebeten.

Beschluss 6/2014

63. Sitzung des AK ITEG am 14. Oktober 2014

1. Der AK ITEG begrüßt den Beschluss Nr. 03/2014 „Abschaltung veralteter Verschlüsselungs-algorithmen und Härtung der HTTPS-Konfiguration“ der AG IS vom 26. September 2014.

2. Die Mitglieder des AK ITEG wirken auf eine Umsetzung der von der AG IS beschlossenen Maßnahmen in ihrem Geschäftsbereich hin.

Beschluss 7/2014

Umlaufbeschluss vom 15. Dezember 2014

1. Der AK ITEG beschließt die sofortige Abschaltung des stark unsicheren Verschlüsselungsalgorithmus SSL v3 auf allen Internetseiten und -diensten der Landesverwaltung.

2. Die Mitglieder des AK ITEG wirken auf eine Umsetzung der sofortigen Abschaltung von SSL v3 in ihrem Geschäftsbereich hin.

STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Empfehlung zur Abschaltung veralteter Verschlüsselungsalgorithmen wie RC4 oder SSLv2 und zur Härtung der HTTPS-Konfiguration

- Empfehlung zur Abschaltung veralteter
- Verschlüsselungsalgorithmen wie RC4 oder SSL v2
- und zur Härtung der HTTPS-Konfiguration

Dokumentenkontrolle:

Versionskontrolle:

Version	Datum	Kommentar
V1.0 final	26.09.2014	Beschlussfassung AG IS
V2.0	15.12.2014	Aktualisierte und überarbeitete Fassung zur Veröffentlichung

Inhaltsverzeichnis

1. Vorbetrachtung

Der Freistaat Sachsen betreibt eine Vielzahl von Internetseiten und -diensten innerhalb und auch außerhalb des SVN. Mit Stand von April 2014 waren über 1.000 solche Angebote der Landesverwaltung Sachsen aus dem Internet erreichbar. Über ein Drittel der Seiten und Dienste sind dabei mit HTTPS verschlüsselt.

Um die Sicherheit dieser HTTPS-Seiten weiter zu optimieren, wurden vom Kernteam Verschlüsselung in einem ersten Schritt Handlungsempfehlungen zur Behebung der Zertifikatsfehler als wichtigste Verbesserungsmaßnahme vorgelegt. Diese Empfehlungen wurden von AG IS und AK ITEG als verbindlich bestätigt. Entsprechende Handlungsanleitungen für mit Microsoft IIS oder Apache betriebene Webserver sowie ressortspezifische Übersichten der betroffenen Webseiten und -dienste wurden den Ressorts inzwischen bereitgestellt.

Als zweiter Schritt wurde die weitere Verbesserung der HTTPS-Konfiguration begonnen. Mit dem vorliegenden Dokument werden die von AG IS und AK ITEG ebenfalls bereits als verbindlich bestätigten Empfehlungen des Kernteams Verschlüsselung zur Abschaltung veralteter Verschlüsselungsalgorithmen wie RC4 oder SSL v2 (Maßnahme I.3.B der Handlungsempfehlungen) und zur Härtung der HTTPS-Konfiguration gegen bekannte Angriffe auf das HTTPS-Protokoll (Maßnahme 1.3.C) vorgestellt.

2. Technische und organisatorische Umsetzung in Sachsen

2.1. Ist-Stand

Die Konfiguration der HTTPS-Seiten und -dienste des Freistaates Sachsen ist sehr heterogen, da viele Serverstandorte und -betreiber existieren. Wichtige Vorgaben zum Betrieb sind hier die Richtlinien »Sicherheitsleitfaden für den Betrieb von Webservern im Bereich des Infohighways Sachsen« und »Sicherheitsrichtlinie für Internetanwendungen der Ressorts im InfoHighway Landesverwaltung Sachsen«.

Derzeit läuft in den Ressorts die von AG IS und AK ITEG beschlossene Beseitigung der Zertifikatsfehler als wichtigste Verbesserungsmaßnahme für die Sicherheit der HTTPS-Seiten der Landesverwaltung. Zur weiteren Optimierung der Sicherheit der Seiten wurde die Umsetzung der im folgenden Kapitel näher beschriebenen und ebenfalls von AG IS und AK ITEG verbindlich beschlossenen Maßnahmen begonnen.

2.2. Soll-Stand

Zur weiteren Verbesserung der Sicherheit der HTTPS-Seiten der Landesverwaltung sollen flächendeckend veraltete und unsicher gewordene Verschlüsselungsalgorithmen und -protokolle abgeschaltet und die HTTPS-Konfiguration gegen bekannte Angriffsmöglichkeiten gehärtet werden. Browser und Webserver unterstützen oft eine Vielzahl unterschiedlicher Verschlüsselungsalgorithmen und -protokolle. Je nach Konfiguration der von der Gegenseite verwendeten Software bzw. Softwareversion wird beim Aufbau der Verbindung die jeweils am besten passende Algorithmenkombination ausgehandelt. Die Software der von der Landesverwaltung angebotenen Webserver sollte deshalb so konfiguriert werden, dass sie immer nur ausreichend sichere Verbindungen zulässt. Im Ernstfall führt das zu der Ablehnung von Verbindungsanfragen von Clients, die ausschließlich veraltete und unsichere Verschlüsselungsalgorithmen unterstützen. Dieses Szenario ist jedoch sehr unwahrscheinlich und wird nur selten tatsächlich eintreten, da alle gängigen Browser die aktuellen Verschlüsselungsstandards unterstützen. Bei einem Test der Umstellung eines großen Serverbereichs im SVN auf die aktuellsten Algorithmen traten selbst bei Clients mit dem veralteten System Windows XP keine derartigen Kompatibilitätsprobleme auf.

Folgende Einzelmaßnahmen müssen umgesetzt werden, um die mit dem Beschluss der Handlungsempfehlungen Verschlüsselung durch AG IS und AK ITEG angestrebten Sicherheitsziele für die Internetseiten und -dienste der Landesverwaltung zu erreichen:

Sofortige Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v2

Das 1994 und damit nur ein Jahr nach der Veröffentlichung der ersten Webseite im Internet eingeführte Verschlüsselungsprotokoll SSL (Version 2) ist aufgrund seines hohen Alters und zahlreicher kritischer Sicherheitslücken den heutigen Sicherheitsanforderungen nicht mehr gewachsen. Seit März 2011 ist die Verwendung des Protokolls SSL v2 laut einer Richtlinie der IETF untersagt (*http://tools.ietf.org/html/rfc6176*). Auch das BSI untersagt in seiner Technischen Richtlinie TR-02102-2 die Nutzung von SSL v2 (*https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile*).

AG IS und AK ITEG haben deshalb beschlossen, SSL v2 auf allen Internetseiten und -diensten der Landesverwaltung sofort abzuschalten und mit entsprechend anfragenden Clients höherwertige Verschlüsselungsalgorithmen auszuhandeln.

Sofortige Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v3

SSL (Version 3) ist ebenfalls ein sehr alter Verschlüsselungsstandard aus dem Jahr 1995, der aber auch auf den Webseiten der Landesverwaltung noch weit verbreitet ist. In SSL v3 sind zwar die kritischsten Sicherheitslücken von SSL v2 beseitigt, dennoch entspricht auch SSL v3 nicht mehr den heutigen Sicherheitsanforderungen. So ist SSL v3 z. B. gegen die BEAST-Attacke nicht geschützt, während das aktuelle Protokoll TLS ab Version 1.1 entsprechende Schutzmaßnahmen vorsieht. Auch Forward Secrecy und andere Schutzmaßnahmen funktionieren unter SSL v3 nicht oder nur eingeschränkt.

Das BSI schreibt deshalb in seiner Technischen Richtlinie TR-02102-2 vor, dass SSL v3 nicht mehr eingesetzt werden darf. Schließlich wurde im Herbst des Jahres 2014 eine schwere Sicherheitslücke (»POODLE«) in SSL v3 bekannt, in deren Folge das über 15 Jahre alte SSL v3 allgemein als endgültig gebrochen angesehen wird. Zahlreiche große Internetdienste (z. B. Apple, PayPal, GMX) schalteten nach Bekanntwerden der Sicherheitslücke das bis dahin vor allem aus Kompatibilitätsgründen oft noch unterstützte SSL v3 ab. Auch die großen Browserhersteller kündigten an, die Unterstützung für SSL v3 aus ihren Produkten zu entfernen und haben das teilweise bereits umgesetzt (z.B. Firefox).

In Verschärfung der ursprünglichen Empfehlung aus der AG IS, SSL v3 mittelfristig bis Ende des Jahres 2015 abzuschalten, beschloss der AK ITEG deshalb die sofortige Abschaltung des stark unsicheren Verschlüsselungsalgorithmus SSL v3 auf allen Internetseiten und -diensten der Landesverwaltung.

Kurzfristige Abschaltung des unsicheren Verschlüsselungsalgorithmus RC4 bis Ende 2014

RC4 als derzeit noch weit verbreiteter Verschlüsselungsstandard wurde 1987 erstmalig veröffentlicht. Spätestens mit dem Bekanntwerden einer realistischen Angriffsmöglichkeit auf den Algorithmus im Jahr 2013 gilt RC4 als unsicher. Im Zuge der NSA-Affäre gab es zusätzlich mehrere Presseberichte, die nahelegten, dass die NSA mit RC4 verschlüsselte Datenströme in Echtzeit brechen und damit im Klartext mitlesen kann. Im Ergebnis empfehlen praktisch alle öffentlichen Sicherheitseinrichtungen, RC4 nicht mehr einzusetzen. So sagt das BSI in seiner Technischen Richtlinie TR-02102-2: *»Der Verschlüsselungsalgorithmus RC4 weist (...) erhebliche Sicherheitsschwächen auf und darf nicht mehr eingesetzt werden.«* Auch die europäische Sicherheitsbehörde ENISA warnt vor dem Einsatz von RC4 und empfiehlt einen Wechsel auf aktuellere Algorithmen.

AG IS und AK ITEG haben deshalb beschlossen, RC4 auf allen Internetseiten und -diensten der Landesverwaltung kurzfristig bis Ende 2014 abzuschalten.

Kurzfristige Absicherung der Neuaushandlung von HTTPS-Verbindungen bis Ende 2014

Unter dem Stichwort »Secure Renegotiation« sind verschiedene Maßnahmen zur Absicherung der Neuaushandlung von HTTPS-Verbindungen notwendig. Anderenfalls kann es zu Man-in-the-middle-Attacken kommen, bei denen ein Angreifer eigene Daten in die sichere Verbindung einschleusen kann. Außerdem sind wirkungsvolle dDoS-Attacken möglich (siehe z. B. *http://netsense.ch/blog/ssl-tls-renegotiation-dos-beheben/*). Das BSI sagt in seiner Technischen Richtlinie TR-02102-2 dazu: *»Session Renegotiation darf nur auf Basis von [RFC5746] verwendet werden. Durch den Client initiierte Renegotiation sollte vom Server abgelehnt werden.«*

AG IS und AK ITEG haben deshalb beschlossen, die Neuaushandlung von HTTPS-Verbindungen bis Ende 2014 entsprechend abzusichern, d. h. nur serverbasierte Neuaushandlungen zuzulassen und nur RFC5746-konforme Webserver-Softwareversionen einzusetzen (Liste der kompatiblen Versionen siehe z. B. *http://www.digicert.com/news/2011-06-03-ssl-renego.htm*).

Kurzfristige Deaktivierung der Option SSL/TLS-Datenkompression bis Ende 2014

2012 wurde eine Angriffsmöglichkeit auf das HTTPS-Protokoll unter dem Namen CRIME bekannt, die auf der Ausnutzung von Effekten der Datenkompression auf anschließend verschlüsselte Daten beruhte. Als Gegenmaßnahme soll die TLS-Datenkompression deaktiviert werden. Negative Auswirkungen sind dadurch nicht zu befürchten, auch da es sich um eine sehr selten genutzte Option handelt. Das BSI sagt in seiner Technischen Richtlinie TR-02102-2: *»TLS bietet die Möglichkeit, die übertragenen Daten vor der Verschlüsselung zu komprimieren. Dies führt zu der Möglichkeit eines Seitenkanalangriffes auf die Verschlüsselung über die Länge der verschlüsselten Daten (siehe [CRIME]). Um dies zu verhindern, muss sichergestellt werden, dass alle Daten eines Datenpakets von dem korrekten und legitimen Verbindungspartner stammen und keine Plaintext-Injection durch einen Angreifer möglich ist. Kann dies nicht sichergestellt werden, so darf die TLS-Datenkompression nicht verwendet werden.«*

AG IS und AK ITEG haben deshalb beschlossen, die Option »SSL/TLS Compression« ohne Einschränkung auf allen Internetseiten und -diensten der Landesverwaltung bis Ende 2014 abzuschalten.

Mittelfristige Absicherung gegen die BEAST-Attacke bis Ende 2015

Die unter dem Namen BEAST-Attacke seit 2004 bekannte Schwachstelle im HTTPS-Protokoll wurde 2006 mit der Version 1.1 des SSL-Nachfolgers TLS serverseitig geschlossen. Auch die meisten Clients sind inzwischen gegen den Angriff geschützt. Da aber die meisten Webserver auch noch die bereits vor 2004 erschienenen und damit verwundbaren Protokolle SSL v2, SSL v3 und TLS 1.0 unterstützen, besteht die Gefährdung durch BEAST weiterhin. Mit sofortigen Abschaltung von SSL v2 und SSL v3 wird jedoch die Gefährdung für Internetseiten und -dienste der Landesverwaltung weiterhin sinken, auch da sich die schon jetzt geringe Anzahl der angreifbaren, veralteten Clients bis dahin weiter verringern wird.

AG IS und AK ITEG haben zur Absicherung gegen die BEAST-Attacke eine mittelfristige Prüfung der Abschaltung von TLS 1.0 (und eine entsprechende Aktivierung von TLS 1.1 und TLS 1.2) bis Ende 2015 beschlossen.

3. Zusammenfassung

Zusammenfassend haben AG IS und AK ITEG folgende sechs wichtige Teilmaßnahmen beschlossen, um die Sicherheit der HTTPS-Seiten der Landesverwaltung weiter zu verbessern:

- Sofortmaßnahmen:
  - Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v2
  - Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v3
- Kurzfristige Maßnahmen bis Ende des Jahres 2014:
  - Abschaltung des unsicheren Verschlüsselungsalgorithmus RC4
  - Absicherung der Neuaushandlung von HTTPS-Verbindungen (Secure Renegotiation)
  - Deaktivierung der Option SSL/TLS-Datenkompression (Absicherung gegen CRIME-Attacke)
- Mittelfristige Maßnahmen bis Ende des Jahres 2015:
  - Prüfung der Abschaltung von TLS 1.0 (Absicherung gegen BEAST-Attacke)

Zur Verifizierung der Wirksamkeit dieser Maßnahmen sollte nach der Umsetzung ein erneuter Test aller HTTPS-Seiten der Landesverwaltung mit dem SSL-Servertest von Qualys (*https://www.ssllabs.com/ssltest*, **Häkchen bei der Schaltfläche »Do not show the results on the boards« setzen**) erfolgen.

Zusätzlich zu diesen Maßnahmen wird auf die weiterführenden Empfehlungen des BSI in seiner Technischen Richtlinie TR-02102-2 verwiesen (*https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile*).
Insbesondere die detaillierten Ausführungen zu den empfohlenen Cipher-Suites in Kapitel 3.3 der Richtlinie werden zur Beachtung und Umsetzung empfohlen.

Eine weitere wichtige Quelle zur sicheren Konfiguration von HTTPS-Seiten findet sich im Dokument »SSL/TLS Deployment Best Practices« der Firma Qualys (*https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf*). Auch diese Hinweise werden ausdrücklich zur Umsetzung empfohlen.

Die bekanntesten Angriffsmöglichkeiten auf das HTTPS-Protokoll sind in folgendem Dokument noch einmal gut zusammengefasst und beschrieben: *https://www.isecpartners.com/media/106031/ssl_attacks_survey.pdf*

Schließlich wird noch auf die Empfehlungen der europäischen Sicherheitsbehörde ENISA zu Algorithmen und Schlüssellängen verwiesen (*http://www.heise.de/security/artikel/ENISA-Empfehlungen-zu-Krypto-Verfahren-2043356.html* und *http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport*).

Herausgeber & Redaktion
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Straße 4
01097 Dresden

Verteilerhinweis

Diese Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Information der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme des Herausgebers zu Gunsten einzelner politischer Gruppen verstanden werden könnte.

Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist. Erlaubt ist jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.