STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Handlungsanleitung zur Abschaltung veralteter Verschlüsselungsalgorithmen wie RC4 oder SSLv2 und zur Härtung der HTTPS-Konfiguration unter **Apache**

- Handlungsanleitung zur Abschaltung veralteter
- Verschlüsselungsalgorithmen wie RC4 oder SSLv2
- und zur Härtung der HTTPS-Konfiguration
- unter Apache

Dokumentenkontrolle:

Versionskontrolle:

Version	Datum	Kommentar
V1.0	19.12.2014	Neu erstellte Fassung zur Veröffentlichung

Inhaltsverzeichnis

1. Grundlagen 2

2. Maßnahmen zur Optimierung der HTTPS-Konfiguration 3

2.1. Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v2 4
2.2. Abschaltung des stark unsicheren Verschlüsselungsprotokolls SSL v3 5
2.3. Abschaltung des unsicheren Verschlüsselungsalgorithmus RC4 6
2.4. Absicherung der Neuaushandlung von HTTPS-Verbindungen (Secure Renegotiation) 8
2.5. Deaktivierung der Option SSL/TLS-Datenkompression (Absicherung gegen CRIME-Attacke) 9
2.6. Prüfung der Abschaltung von TLS 1.0 (Absicherung gegen BEAST-Attacke) 9

1. Grundlagen

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, wurde seitens der AG IS und des AK ITEG in einem ersten Schritt die Behebung der Zertifikatsfehler als wichtigste Verbesserungsmaßnahme festgelegt. Entsprechende Handlungsanleitungen für mit Microsoft IIS oder Apache betriebene Webserver sowie ressortspezifische Übersichten der betroffenen Webseiten und -dienste wurden den Ressorts bereitgestellt. Als zweiter von der AG IS und dem AK ITEG beschlossener Schritt hat nun die weitere Verbesserung der HTTPS-Konfiguration begonnen. Die dazu notwendigen Maßnahmen zur Abschaltung veralteter Verschlüsselungsalgorithmen wie RC4 oder SSLv2 und zur Härtung der HTTPS-Konfiguration gegen bekannte Angriffe auf das HTTPS-Protokoll werden in der vorliegenden Handlungsanleitung beschrieben. Eine ressortspezifische Übersicht der von den einzelnen Maßnahmen betroffenen Webseiten liegt den Ressorts bereits vor.

Den aktuellen Stand der Sicherheit der HTTPS-Konfiguration Ihrer Webseite können Sie jederzeit über einen kostenlosen SSL-Server-Test der Firma Qualys unter *https://www.ssllabs.com/ssltest* **(Achtung: Häkchen bei Option »Do not show the results on the boards« setzen)** prüfen.

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

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

Eine Übersicht der Angriffsmöglichkeiten auf das HTTPS-Protokoll und der Verwundbarkeit verschiedener Software und Algorithmen finden sich unter *http://en.wikipedia.org/wiki/Transport_Layer_Security* und *https://www.isecpartners.com/media/106031/ssl_attacks_survey.pdf*.

Abschließend 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*.

Für Fragen und Ergänzungsvorschläge zu dieser Handlungsanleitung können Sie sich per E-Mail an den Beauftragten für Informationssicherheit des Landes unter *bfis-land@smi.sachsen.de* wenden.

2. Maßnahmen zur Optimierung der HTTPS-Konfiguration

Alle im vorliegenden Dokument beschriebenen Maßnahmen erfordern Änderungen an der Systemkonfiguration des Webservers, welche entsprechend vorab gesichert werden sollte. Die Änderungen können per Hand oder mit ggf. vorhandenen Managementwerkzeugen vorgenommen werden.

Üblicherweise werden Webserver auf Unix-Betriebssystemen mit der Software Apache httpd und OpenSSL betrieben. Viele der aktuellen HTTPS-Sicherheitsfunktionen sind nur in jüngeren Versionen dieser Programme verfügbar. So wurde beispielsweise die Unterstützung eines sicheren Forward Secrecy-Schlüsselaustauschs erst mit Apache Version 2.4.8 eingeführt. OpenSSL unterstützt viele wichtige Features erst mit der Version 1.0.1j. **Falls möglich sollte man den Einsatz alter Apache-Versionen (2.2, 2.0) oder alter OpenSSL-Versionen (0.9.8, 1.0.0) deshalb vermeiden und stattdessen auf die jeweils aktuellsten Versionen setzen.**

Eine besondere Schwierigkeit bei der Erstellung dieser Handlungsanleitung war, dass es zahlreiche verschiedene Unix-Betriebssysteme gibt, unter denen jeweils systemspezifische Konfigurationsbedingungen gelten. Das erstreckt sich vom Ort und Aufbau der Konfigurationsdateien bis hin zur anzuwendenden Syntax der entsprechenden Befehle. Die Handlungsanleitung bietet deshalb nur einen allgemeinen Überblick. Weitere Hinweise zur Konfiguration der einzelnen Optionen finden sich in der Betriebssystembeschreibung des jeweiligen Servers und in den entsprechenden Nutzerforen. Grundsätzlich befinden sich die entsprechenden Konfigurationsdateien für die HTTPS-Optionen bei den verschiedenen Unix-Betriebssystemen an folgenden Stellen:

```
RedHat/CentOS:          /etc/httpd/conf.d/ssl.conf
Debian/Ubuntu:          /etc/apache2/mods-available/ssl.conf
SuSE:                   /etc/apache2/ssl-global.conf
```

Eine Übersicht über weitere Unix-Betriebssysteme und Speicherorte findet sich z. B. unter *http://wiki.apache.org/httpd/DistrosDefaultLayout*. Alternativ können die Dateien z. B. mit dem Befehl `grep` gesucht werden. Die grundlegende Konfiguration einer HTTPS-Seite unter Apache ist z. B. unter *https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html* kurz beschrieben und sieht (je nach System) so aus:

```
LoadModule ssl_module modules/mod_ssl.so
Listen 443
<VirtualHost *:443>
    ServerName www.beispiel.sachsen.de
    SSLEngine on
    SSLCertificateFile /path/to/www.beispiel.sachsen.de.cert
    SSLCertificateKeyFile /path/to/www.beispiel.sachsen.de.key
</VirtualHost>
```

Diese HTTPS-Konfigurationsdatei ist um die verschiedenen Optionen zur Abschaltung veralteter Verschlüsselungsalgorithmen und zur Härtung der HTTPS-Konfiguration zu ergänzen. Nach dem Ändern der HTTPS-Konfigurationsdatei ist ein Neustart des Webservers z. B. über den Befehl `service apache2 restart` bzw. `service httpd restart` notwendig, um die Änderungen wirksam werden zu lassen. Anschließend sollte die neue Konfiguration z. B. über den SSL Servertest von Qualys gegengetestet werden, um die Wirksamkeit der Maßnahmen zu prüfen. Werden dabei z. B. abgeschaltete Verschlüsselungsprotokolle dennoch als aktiv angezeigt, sollte noch einmal eingehend geprüft werden, ob alle betreffenden Konfigurationsdateien geändert wurden. Hier kann eine Suche nach der jeweiligen Konfigurationsoption in allen Dateien im Verzeichnis des Webservers helfen.

2.1. 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 SSLv2 (*https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile*).

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

Auf allen mit Apache betriebenen Webservern sind in diesem Rahmen verschiedene Einstellungen zu prüfen und umzusetzen. Ziel ist die Deaktivierung der Nutzung von SSL v2 sowohl auf Client- als auch auf Serverseite (für aus- und eingehende HTTPS-Verbindungen aus Sicht des Webservers). Grundsätzlich erfolgt die Abschaltung von SSL v2 über das Setzen der entsprechenden Werte in der jeweiligen Konfigurationsdatei, unter RedHat also beispielsweise in der Datei `ssl.conf`.

In dieser Datei ist die Zeile `SSLProtocol All -SSLv2` hinzuzufügen, um das Verschlüsselungsprotokoll SSL v2 abzuschalten (wenn dieses standardmäßig nicht bereits deaktiviert ist). Anschließend ist der Webserver neu zu starten.

Mit den obenstehenden Einträgen wird das stark unsichere Protokoll SSL v2 für ein- und ausgehende HTTPS-Verbindungen auf dem Webserver deaktiviert.

2.2. 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 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 2015 abzuschalten, beschloss der AK ITEG deshalb die sofortige Abschaltung des stark unsicheren Verschlüsselungsalgorithmus SSL v3 auf allen Internetseiten und -diensten der Landesverwaltung.

Analog zur bereits beschriebenen Abschaltung von SSL v2 ist die serverseitige Deaktivierung der Nutzung von SSL v3 direkt in der jeweiligen Konfigurationsdatei, unter RedHat also beispielsweise in der Datei `ssl.conf`, vorzunehmen. In dieser Datei ist die Zeile `SSLProtocol All -SSLv2 -SSLv3` hinzuzufügen, um das Verschlüsselungsprotokoll SSL v3 abzuschalten (SSLv2 sollte in jedem Fall mit deaktiviert werden, falls nicht bereits erfolgt). Anschließend ist der Webserver neu zu starten.

Mit den obenstehenden Einträgen wird das stark unsichere Protokoll SSL v3 für ein- und ausgehende HTTPS-Verbindungen auf dem Webserver deaktiviert.

2.3. Abschaltung des unsicheren Verschlüsselungsalgorithmus RC4

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. Zusätzlich empfiehlt auch Microsoft, RC4 nicht mehr einzusetzen und kündigt eine entsprechende Umstellung seiner Produkte an (*http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx*).

Laut Beschluss von AG IS und AK ITEG ist RC4 deshalb auf allen Internetseiten und -diensten der Landesverwaltung kurzfristig bis Ende 2014 abzuschalten.

Neben der Abschaltung von RC4 sind auch die vergleichbar veralteten und unsicheren Verschlüsselungsalgorithmen DES (nicht Triple DES) und RC2 mit zu deaktivieren, falls diese noch aktiv sein sollten. Außerdem sollte sichergestellt werden, dass die Daten in keinem Fall unverschlüsselt übertragen werden (Abschaltung Verschlüsselungsoption NULL).

Im Rahmen der Deaktivierung der unsicheren Verschlüsselungsalgorithmen wie RC4 und der vorherigen Abschaltung der stark unsicheren Protokolle wie SSL v2 und SSL v3 sollten auch noch die verwendeten Hash-Algorithmen wie MD5 sowie die verwendeten Schlüsselaustauschverfahren wie Diffie-Hellman Beachtung finden. Die Kombination dieser vier Faktoren

- Protokoll,
- Verschlüsselungsalgorithmus und
- Hashalgorithmus sowie
- Schlüsselaustauschverfahren

ergibt zusammen die sogenannten Cipher Suites. Jeder Webserver unterstützt zahlreiche Cipher Suites, um kompatibel zu möglichst vielen verschiedenen anfragenden Clients zu sein.

Die von AG IS und AK ITEG beschlossene Abschaltung unsicherer Verschlüsselungsalgorithmen und Protokolle schränkt die Anzahl der unterstützten Cipher Suites ein. Im Ernstfall führt das zu der Ablehnung von Verbindungsanfragen von Clients, die ausschließlich veraltete und unsichere Cipher Suites 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 Cipher Suites traten selbst bei Clients mit dem veralteten System Windows XP keine derartigen Kompatibilitätsprobleme auf.

Bei der Aushandlung der zu verwendenden Cipher Suites zwischen Client und Server kommt es auch auf die Priorisierung der jeweiligen Suites seitens der Beteiligten an. Webserver sollten also so konfiguriert werden, dass besonders sichere Cipher Suites am höchsten priorisiert sind.

Für eine Auswahl von sicheren Cipher Suites werden die detaillierten Ausführungen in Kapitel 3.3 der Richtlinie TR02102-2 des BSI zur Beachtung und Umsetzung empfohlen: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf?__blob=publicationFile* .

Die Auswahl und Priorisierung der Cipher Suites in Apache ist nicht trivial, da es eine große - und je nach Serverversion unterschiedliche - Anzahl von unterstützten Cipher Suites gibt. Apache nutzt dabei normalerweise die von OpenSSL angebotenen Cipher Suites. Eine nähere Dokumentation dieser findet sich unter *http://www.openssl.org/docs/apps/ciphers.html* .

Die Konfiguration von Auswahl und Priorisierung erfolgt zusammen mit der Abschaltung der unsicheren Verschlüsselungsalgorithmen über zwei Zeilen in der entsprechenden HTTPS-Konfigurationsdatei (in RedHat z. B. `ssl.conf`):

1. Die Vorgabe, welche Verschlüsselung verwendet werden soll, sollte durch den Server statt wie normalerweise durch den Client erfolgen:

```
SSLHonorCipherOrder On
```

2. Mit folgenden Optionen werden unsichere Cipher Suites blockiert:

```
SSLCipherSuite HIGH:MEDIUM:!LOW:!aNULL:!eNULL:!EXPORT:!DES:!DSS:!MD5:!PSK:
!SEED:!IDEA:!SRP:!RC2:!RC4@STRENGTH
```

Achtung: die ebenfalls möglichen Optionen »`!SSLv2`« und »`!SSLv3` in der Zeile `SSLCipherSuites` schalten auch die Unterstützung von TLS1.0 und TLS 1.1 mit ab. Die Deaktivierung von SSLv2 und SSLv3 sollte deshalb ausschließlich über die Option `SSLProtocol` erfolgen.

Die Option »`!eNULL`« schaltet alle Cipher Suites ohne Verschlüsselung ab, die Option »`!aNULL`« alle ohne Authentisierung; »`@STRENGTH`« sortiert die restlichen Cipher Suites nach Stärke (Schlüssellänge). Die Option »`!RC4`« schaltet den stark unsicheren Verschlüsselungsalgorithmus RC4 und alle darauf basierenden Cipher Suites ab. Eine einzelne Auflistung und Priorisierung der zu unterstützenden Cipher Suites wäre ebenfalls möglich, ist jedoch stark von der verwendeten Software und deren Version abhängig. Die Anzeige der unterstützten Cipher Suites (und auch der Auswirkung der gewählten Optionen zur Auswahl dieser) kann z. B. über den folgenden Befehl erfolgen (hier für die Stärke der Cipher Suites):

```
openssl ciphers 'HIGH:MEDIUM:!LOW'
```

Mit den obenstehenden Einträgen wird (nach einem Neustart des Webservers) der unsichere Verschlüsselungsalgorithmus RC4 sowie die veralteten Verschlüsselungsalgorithmen NULL, DES (nicht Triple DES) und RC2 für ein- und ausgehende HTTPS-Verbindungen auf dem Webserver deaktiviert. Außerdem wird eine sichere Auswahl und Priorisierung der Cipher Suites erreicht.

2.4. Absicherung der Neuaushandlung von HTTPS-Verbindungen (Secure Renegotiation)

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. 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.«*

Die AG IS und der AK ITEG haben festgelegt, dass die Neuaushandlung von HTTPS-Verbindungen bis Ende 2014 entsprechend abzusichern ist. Das heißt, es sind nur serverbasierte Neuaushandlungen zuzulassen und nur RFC5746-konforme Webserver-Softwareversionen einzusetzen.

In der Richtlinie RFC5746 (*http://tools.ietf.org/html/rfc5746*) werden der Hintergrund der Schwachstelle bei der Neuaushandlung von HTTPS-Verbindungen sowie die entsprechenden Gegenmaßnahmen beschrieben. Dazu wird insbesondere eine neue Erweiterung (TLS-Renegotiation Indication Extension) definiert, die eine sichere Neuaushandlung der Verbindungen ermöglicht.

In Apache (mod_ssl) kann die unsichere Neuaushandlung der Verbindungen über die Option `SSLInsecureRenegotiation off` in der HTTPS-Konfigurationsdatei deaktiviert werden. Parallel dazu sollte geprüft werden, ob ein Update auf eine aktuellere Version von Apache und OpenSSL möglich ist.

Eine weitere Gefährdung ist die clientbasierte Neuaushandlung und darauf basierende dDoS-Angriffe (siehe z. B. *http://netsense.ch/blog/ssl-tls-renegotiation-dos-beheben/*).

2.5. Deaktivierung der Option SSL/TLS-Datenkompression (Absicherung gegen CRIME-Attacke)

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 sich darauf verständigt, dass die Option »SSL/TLS Compression« ohne Einschränkung auf allen Internetseiten und -diensten der Landesverwaltung bis Ende 2014 abzuschalten ist.

Das Ziel dieser Vorgabe ist die Verhinderung der Verwundbarkeit von HTTPS-Verbindungen durch die sogenannte CRIME-Attacke. Dazu ist unter Apache folgende Zeile in die HTTPS-Konfigurationsdatei aufzunehmen und der Webserver anschließend neu zu starten:

```
SSLCompression off
```

Im Umfeld der CRIME-Attacke sollte auch beachtet werden, dass seit 2013 ein weiterentwickelter Angriff unter dem Namen BREACH bekannt ist, der auch die weit verbreitete Komprimierungsmethode »*HTTP Compression«* betrifft. Ein Schutz durch Abschaltung der betroffenen Komprimierung lässt sich hier nicht so einfach wie bei der CRIME-Attacke umsetzen. Weitere Betrachtungen zum Thema und empfohlene Maßnahmen finden sich z. B. hier: *https://community.qualys.com/blogs/securitylabs/2013/08/07/defending-against-the-breach-attack*.

2.6. Prüfung der Abschaltung von TLS 1.0 (Absicherung gegen BEAST-Attacke)

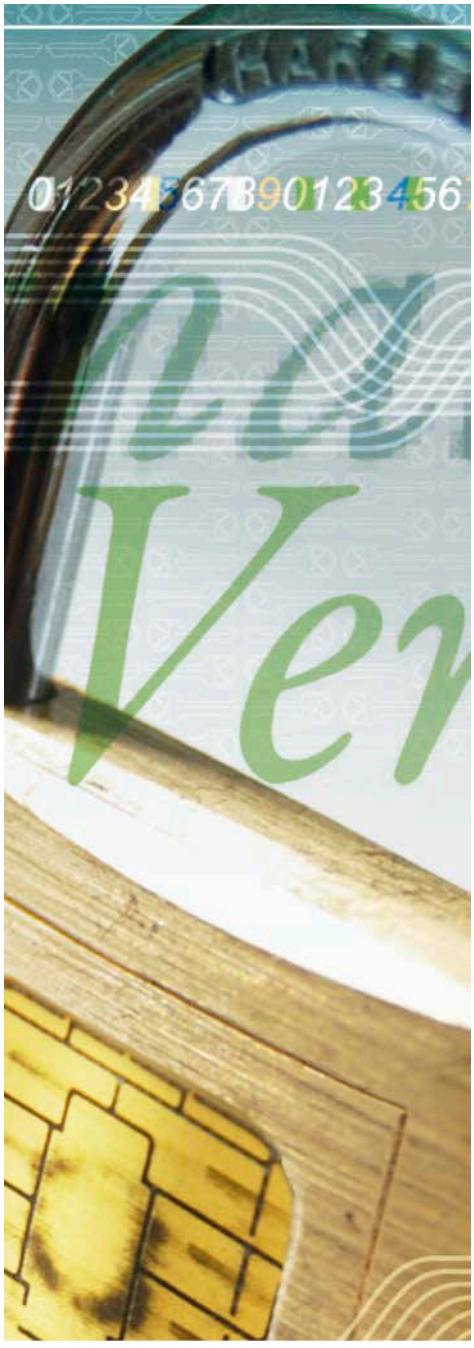
Die unter dem Namen BEAST-Attacke seit 2004 bekannte Schwachstelle im HTTPS-Protokoll wurde 2006 mit der Version 1.1 des SSL-Nachfolgers TLS serverseitig geschlossen. Auch die meisten Clients sind inzwischen gegen den Angriff geschützt. Da aber die meisten Webserver auch noch die bereits vor 2004 erschienenen 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, weil veralteten Clients bis dahin weiter verringern wird.

Laut Beschluss von AG IS und AK ITEG ist zur Absicherung gegen die BEAST-Attacke eine Abschaltung von TLS 1.0 bis Ende 2015 zu prüfen.

Analog zur Abschaltung von SSL v3 kann die serverseitige Deaktivierung von TLS 1.0 wieder über die HTTPS-Konfigurationsdatei erfolgen. In diesem Rahmen sollte die Unterstützung für TLS 1.1 und TLS 1.2 explizit mit aktiviert werden.

```
SSLProtocol -SSLv2 -SSLv3 -TLSv1 +TLSv1.1 +TLSv1.2
```

Mit diesen Einträgen kann das Protokoll TLS 1.0 für eingehende HTTPS-Verbindungen auf dem Webserver deaktiviert werden.



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.