STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

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

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

Dokumentenkontrolle:

Versionskontrolle:

Version	Datum	Kommentar
V1.0	12.09.2014	Erarbeitung durch Kernteam Verschlüsselung der AG IS
V2.0	16.12.2014	Aktualisierte und überarbeitete Fassung zur Veröffentlichung

Inhaltsverzeichnis

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 solcher 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 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 Systemregistrierung des Webservers, welche entsprechend vorab gesichert werden sollte. Die Änderungen können entweder per Hand über regedit.exe, per Gruppenrichtlinie oder toolgestützt z. B. über das kostenlose Programm IIS Crypto der Firma Nartac vorgenommen werden. Eine Konfiguration über den Microsoft IIS Manager (Version 2008 R2) ist leider nicht möglich.

Empfohlen wird, die Einstellungen über das kostenfreie und weitestgehend selbsterklärende Tool IIS Crypto der Firma Nartac (*https://www.nartac.com/Products/IISCrypto/Default.aspx*) vorzunehmen. Durch die Anwendung der Konfigurationsvorlage »Best Practices« aus dem Tool heraus wird eine bewährte Kombination von Einstellungen auf den Webserver angewandt. Diese Kombination enthält alle in dieser Handlungsanleitung empfohlenen Konfigurationseinstellungen für die Maßnahmen »Abschaltung SSL v2 und RC4«. Zusätzlich zu der Vorlage „Best Practices“ muss nur noch der Algorithmus RC4 128/128 und die Cipher Suite TLS_RSA_WITH_RC4_128_SHA deaktiviert werden, um die Vorgaben der AG IS und des AK ITEG zur Abschaltung von RC4 zu erfüllen. Weiterhin wird empfohlen, den Hashalgorithmus MD5 aus Sicherheitsgründen zu deaktivieren. Die Abschaltung von SSL v3 und die bis 2015 zu prüfende Abschaltung von TLS 1.0 kann ebenfalls mit dem Tool IIS Crypto vorgenommen werden. Die Konfigurationsmaßnahmen für die Absicherung der Neuaushandlung von HTTPS-Verbindungen und für die Abschaltung der SSL/TLS-Datenkompression müssen manuell über die Systemregistrierung erfolgen, da diese Einstellungen nicht vom Tool II Crypto unterstützt werden.

Nach dem Ändern der HTTPS-Konfiguration ist ein Neustart des Webservers 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.

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 Microsoft IIS 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). Neben der Abschaltung von SSL v2 sind auch die vergleichbar veralteten und unsicheren Protokolle PCT 1.0 und Multi-Protocol Unified Hello zu deaktivieren, falls diese noch aktiv sein sollten.

Es wird empfohlen, die Abschaltung von SSL v2 sowie PCT 1.0 und Multi-Protocol Unified Hello über das Tool IIS Crypto der Firma Nartac vorzunehmen. Dazu kann die Konfigurationsvorlage „Best Practices“ aus dem Tool heraus verwendet werden. Weitere Maßnahmen sind nicht notwendig.

Grundsätzlich erfolgt die Abschaltung von SSL v2 über das Setzen der entsprechenden Werte im Registrierungszweig SCHANNEL (Secure Channel) in der Systemregistrierung des Webservers. Unter Microsoft IIS (Version 2008 R2) findet sich dieser Zweig unter *HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL*. Im Unterzweig *SCHANNEL\Protocols* werden die Einstellungen zu allen HTTPS-Protokolle abgelegt. Dies sind folgende:

- Multi-Protocol Unified Hello
- PCT 1.0
- SSL 2.0
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

Für die Konfiguration dieser Protokolle muss ein entsprechender Zweig mit einem Schlüssel (Unterzweig) »*Server*« vorhanden sein oder angelegt werden (also für SSL v2 der Zweig *SCHANNEL\Protocols\SSL 2.0\Server*), in dem die Einstellungen zur Behandlung von externen Clients eingehenden HTTPS-Anfragen abgelegt werden. Im Schlüssel *Server* gibt es zwei Einträge des Typs DWORD, mit denen das Verhalten des Webservers für das jeweilige Protokoll festgelegt wird: *Enabled* und *DisabledByDefault*. Um ein Protokoll abzuschalten, muss der vorhandene oder neu angelegte Eintrag »*Enabled*« auf 0 (dword:00000000) sowie der Eintrag »*DisabledByDefault*« auf 1 (dword:00000001) gesetzt werden. Je nach Version des Webservers reicht oft einer der beiden Einträge, sicherheitshalber sollten jedoch immer beide Einträge gesetzt werden.

Zusammengefasst sind für die serverseitige Deaktivierung von SSL v2 folgende Registrierungseinträge erforderlich:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Server]
"Enabled" = DWORD: 00000000
"DisabledByDefault" = DWORD: 00000001
```

Mit den obenstehenden Einträgen wird das Protokoll SSL v2 für ein- und ausgehende HTTPS-Verbindungen auf dem Webserver deaktiviert. Analog sind die Protokolle Multi-Protocol Unified Hello und PCT 1.0 zu deaktivieren. Diese Protokolle sind zwar auf aktuellen Webservern meist nicht mehr vorhanden, sollten aber dennoch sicherheitshalber in der Registrierung immer deaktiviert werden.

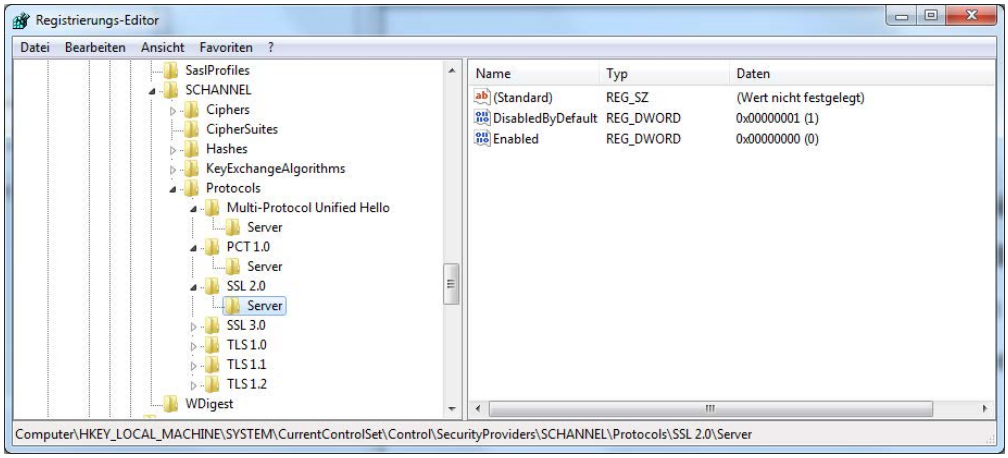


Abbildung 1: Deaktiviertes serverseitiges SSL v2 im Registrierungszweig SCHANNEL\Protocols

Im Zuge der Deaktivierung der veralteten Protokolle SSL v2, PCT 1.0 und Multi-Protocol Unified Hello sollte die Unterstützung für TLS 1.1 und TLS 1.2 aktiviert werden. Beide TLS-Versionen werden z. B. von Microsoft IIS (Version 2008 R2) unterstützt, sind aber standardmäßig deaktiviert. In den entsprechenden Unterzweigen *Client* und *Server* des jeweiligen Protokollzweigs sind die Einträge »*Enabled*« auf ffffffff und »*DisabledByDefault*« auf 0 zu setzen.

Eine bequeme Möglichkeit zum Setzen aller dieser Einstellungen bietet das kostenfreie und weitestgehend selbsterklärende Tool IIS Crypto der Firma Nartac (*https://www.nartac.com/Products/IISCrypto/Default.aspx*). In diesem Tool kann z. B. SSL v2 (wie die anderen unsicheren Protokolle) mit einem einfachen Mausklick deaktiviert werden. Auf dem gleichen Weg können TLS 1.1 und 1.2 mit einem Doppelklick aktiviert werden. Die grau hinterlegten Einstellungen entsprechen der unveränderten Standardeinstellung des Webservers.

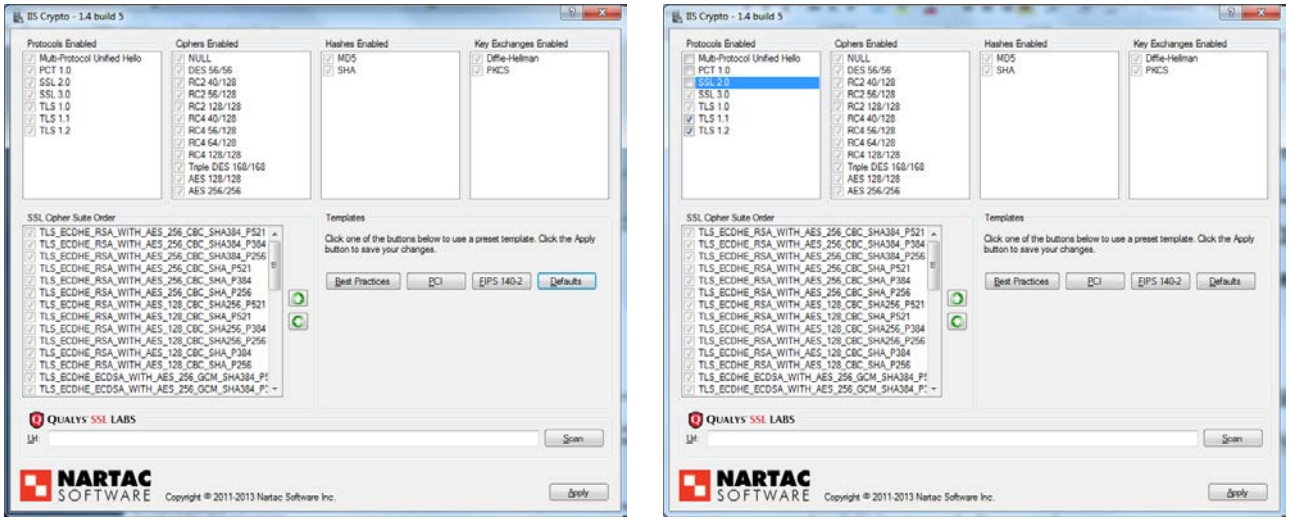


Abbildung 2: Tool IIS Crypto von Nartac (links nach Start, rechts empfohlene Mindesteinstellungen)

Das Tool IIS Crypto setzt alle notwendigen Einstellungen für die serverseitige Deaktivierung von SSL v2. Sollte der Webserver selbst auch als Client agieren (z. B. wenn der Server als Proxy arbeitet), sind die gleichlautenden Eintragungen im Zweig *SCANNEL/Protocols/SSL 2.0/Client* entsprechend manuell zu ergänzen.

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

Es wird empfohlen, die Abschaltung von SSL v3 über das Tool IIS Crypto der Firma Nartac vorzunehmen. Dazu kann die Konfigurationsvorlage »Best Practices« aus dem Tool heraus verwendet werden. Weitere Maßnahmen sind nicht notwendig.

Analog zur bereits beschriebenen Abschaltung von SSL v2 hat die server- und ggf. auch clientseitige Deaktivierung der Nutzung von SSL v3 direkt über die Systemregistrierung oder toolgestützt z. B. über IIS Crypto erfolgen. Im Ergebnis müssen im Zweig *SCHANNEL\Protocols\SSL 3.0\Server* folgende Einträge des Typs DWORD vorhanden sein:

- der Eintrag *Enabled* mit dem Wert 0 (dword:00000000) sowie
- der Eintrag *DisabledByDefault* mit dem Wert 1 (dword:00000001).

Gleichzeitig sollte jedoch sichergestellt sein, dass mindestens das Protokoll TLS 1.0, besser jedoch auch TLS 1.1 und TLS 1.2 aktiviert sind (Enabled = ffffffff, DisabledByDefault = 0).

Mit diesen Einträgen wird das 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 verschlüsselten 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).

Es wird empfohlen, die Abschaltung von RC4 sowie DES, RC2 und NULL über das Tool IIS Crypto der Firma Nartac vorzunehmen. Dazu kann die Konfigurationsvorlage »Best Practices« aus dem Tool heraus verwendet werden. Zusätzlich zu der Vorlage »Best Practices« muss der Algorithmus RC4 128/128 und die entsprechende Cipher Suite TLS_RSA_WITH_RC4_128_SHA deaktiviert werden. Auch der Hashalgorithmus MD5 sollte deaktiviert werden. Weitere Maßnahmen sind nicht notwendig.

Die unter Microsoft IIS (Version 2008 R2) notwendigen Einstellungen zur Deaktivierung von RC4 erfolgen analog zu der Deaktivierung von SSL v2 über das Setzen der entsprechenden Werte im Registrierungszweig SCHANNEL (Secure Channel) in der Systemregistrierung des Webservers, hier im Unterzweig *HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers*.

In diesem Zweig werden die Einstellungen zu allen Verschlüsselungsalgorithmen abgelegt. Das sind folgende:

- NULL
- DES 56/56
- RC2 40/128, 56/128 und 128/128
- RC4 40/128, 56/128, 64/128 und 128/128
- Triple DES 168/168
- AES 128/128 und 256/256

Die Zahlen hinter den Algorithmen stehen für die jeweiligen Schlüssellängen. Für jede dieser Kombinationen muss ein entsprechender Zweig vorhanden sein oder angelegt werden (z. B. für RC4 128/128 der Zweig *SCHANNEL\Ciphers\RC4 128/128*).
In diesen Zweigen ist ein Eintrag bei *Enabled* mit dem Typ DWORD anzulegen, dadurch wird das Verhalten des Webservers für den jeweiligen Algorithmus festgelegt: Ist der Wert des Eintrags 0 (dword:00000000) ist der jeweilige Algorithmus deaktiviert, ist der Wert ffffffff (dword:ffffffff) wird der Algorithmus eingesetzt.
Zusammengefasst sind für die Deaktivierung von RC4 folgende Registrierungseinträge erforderlich:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Ciphers]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Ciphers\RC4 40/128]
"Enabled" = DWORD: 00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\ Ciphers\RC4 56/128]
"Enabled" = DWORD: 00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Ciphers\RC4 64/128]
"Enabled" = DWORD: 00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\ Ciphers\RC4 128/128]
"Enabled" = DWORD: 00000000
```

Mit den obenstehenden Einträgen wird der Verschlüsselungsalgorithmus RC4 für ein- und ausgehende HTTPS-Verbindungen auf dem Webserver deaktiviert. Analog sind die Verschlüsselungsalgorithmen NULL, DES (nicht Triple DES) und RC2 zu deaktivieren. Diese Algorithmen sind zwar auf aktuellen Webservern teilweise nicht mehr vorhanden, sollten aber dennoch sicherheitshalber in der Registrierung immer deaktiviert werden.

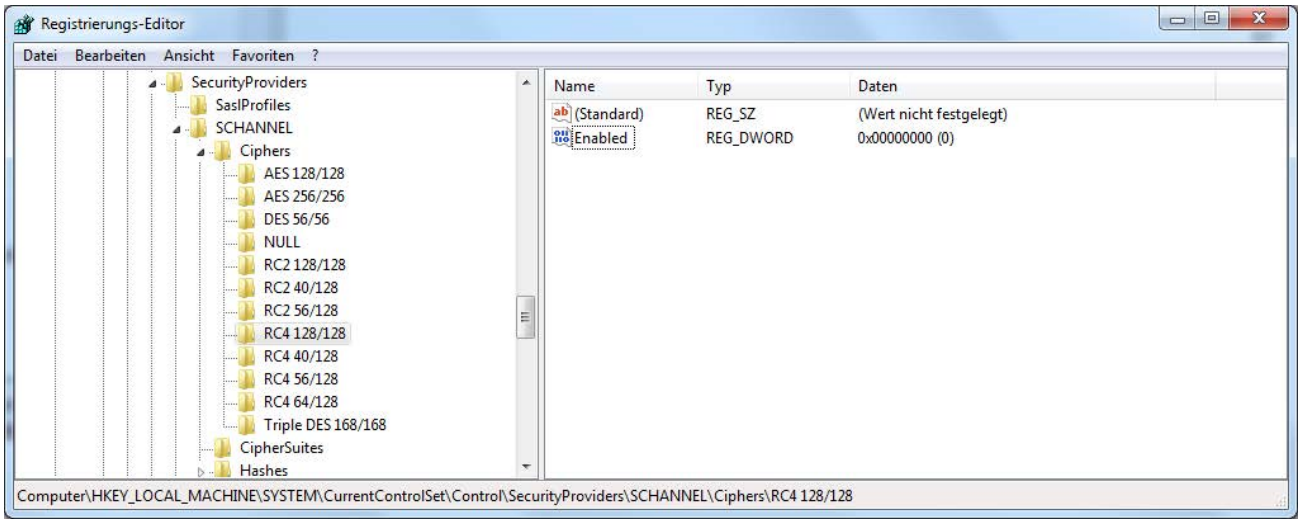


Abbildung 3: Deaktiviertes RC4 128/128 im Registrierungszweig SCHANNEL\Ciphers

Im Unterschied zu den nach Client und Server unterschiedenen Einstellungen zu den HTTPS-Protokollen wirken die Einstellungen zu den Verschlüsselungsalgorithmen (und auch zu Hashalgorithmen) immer übergreifend für den gesamten Webserver und sofort ohne Neustart des Systems.

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 (z. B. MD5) sowie die verwendeten Schlüsselaustauschverfahren wie (z. B. Diffie-Hellman) Beachtung finden. Die Kombination dieser vier Faktoren:

- Protokoll,
- Verschlüsselungsalgorithmus,
- Hashalgorithmus sowie
- Schlüsselaustauschverfahren

ergeben 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 Microsoft IIS über die Systemregistrierung ist nicht trivial, da es eine große - und je nach Serverversion unterschiedliche - Anzahl von unterstützten Cipher Suites gibt (*http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757%28v=vs.85%29.aspx*). Für die Konfiguration von Auswahl und Priorisierung gibt es zwei verschiedene Registrierungsschlüssel: der erste Schlüssel *HKLM\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002* enthält die Liste der vom Webserver zu verwendenden Cipher Suites, während der zweite Schlüssel *HKLM\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002* bestimmt, in welcher Reihenfolge die Suites anzuwenden sind.

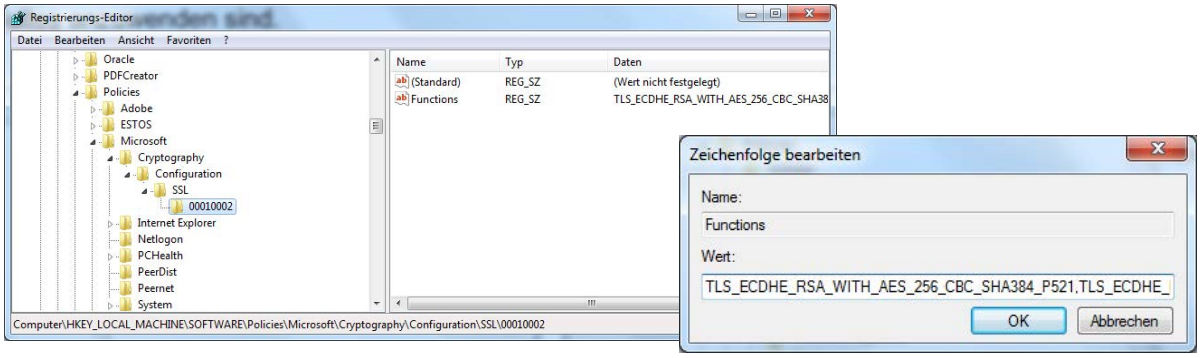


Abbildung 4: Registrierungsschlüssel für die Reihenfolge der Cipher Suites

Für Microsoft IIS (Version 2008 R2) wird folgende Reihenfolge der Cipher Suites empfohlen:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

Diese Auflistung setzt sich aus allen von Microsoft IIS (Version 2008 R2) unterstützten Cipher Suites zusammen, mit Ausnahme der folgenden Cipher Suites:

```
TLS_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_RC4_128_MD5,
SSL_CK_RC4_128_WITH_MD5,
SSL_CK_DES_192_EDE3_CBC_WITH_MD5,
TLS_RSA_WITH_NULL_SHA256,
TLS_RSA_WITH_NULL_SHA
```

Diese Suites nutzen unsichere Protokolle oder Algorithmen (z. B. RC4) und sollen nicht mehr verwendet werden. Die obere Liste kann als Vorlage für den entsprechenden Eintrag in der Systemregistrierung genutzt werden (vorher alle Leerzeichen entfernen). **Fett gedruckt dargestellt sind diejenigen Cipher Suites, die vom BSI in der Richtlinie TR-02102-2 als langfristig sicher eingeschätzt sind.**

Mit dem SChannel-Patch MS14-066 (KB2992611) wurden von Microsoft am 11. November 2014 die folgenden vier neuen Ciphersuites ausgeliefert:

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256
```

Diese Ciphersuites werden vom BSI in der Richtlinie TR-02102-2 als langfristig sicher eingeschätzt. Aufgrund von teilweise auftretenden Client-Verbindungsproblemen wurden die vier neuen Ciphersuites jedoch am 18. November 2014 in einem Update des Patches wieder aus der Liste der Standard-Suites entfernt.

Es gibt auch die Möglichkeit, die Reihenfolge der Cipher Suites über eine Gruppenrichtlinie festzulegen. Dafür sind folgende Schritte einzuhalten:

1. Aufrufen des Editors für Gruppenrichtlinien, z. B. durch Eingabe von »gpedit.msc« in der Kommandozeile
2. Auswahl »Computerkonfiguration -> Administrative Vorlagen -> Netzwerk -> SSL-Konfigurations-einstellungen«
3. Option »*Richtlinieneinstellungen bearbeiten*« auswählen

Das weitere Vorgehen wird dann in dem Fenster »*Reihenfolge der Verschlüsselungssammlungen*« angezeigt (auf rechter Seite ganz nach unten scrollen). Kurz zusammengefasst sind die Option »Aktiviert« oben links zu wählen und anschließend die Liste der Cipher Suites (siehe letzte Seite) in das Feld *SSL-Verschlüsselungssammlungen* zu kopieren (vorher Leerzeichen entfernen).

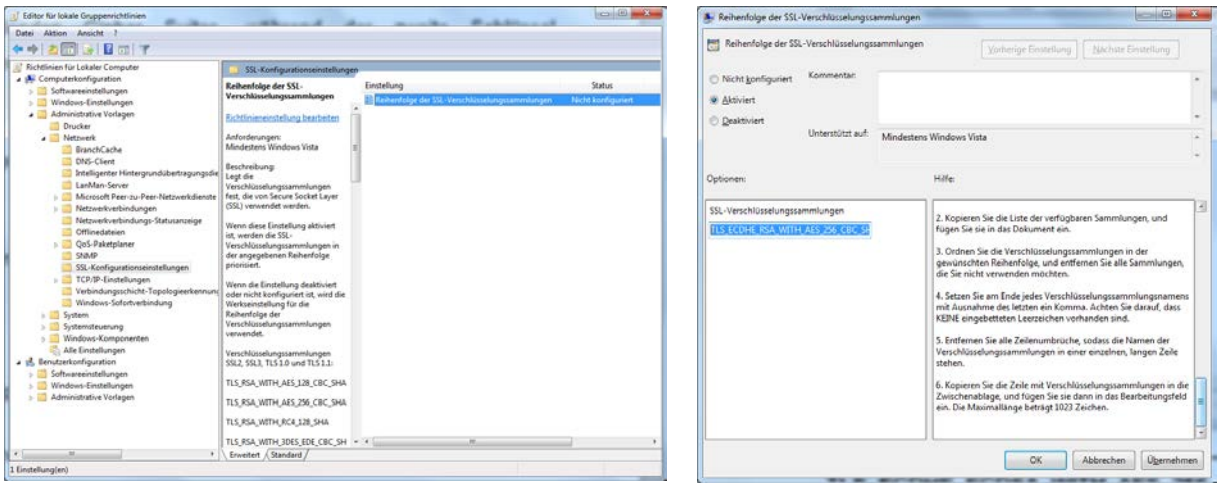


Abbildung 5: Gruppenrichtlinie für die Reihenfolge der Cipher Suites

Eine einfache Alternative ist das Tool IIS Crypto der Firma Nartac. Mit der empfohlenen Anwendung der Konfigurationsvorlage »Best Practices« aus dem Tool heraus wird eine bewährte Kombination von Einstellungen auf den Webserver angewandt. Diese Kombination enthält auch eine praxiserprobte Auswahl und Priorisierung von Cipher Suites. **Insbesondere sind in dieser Kombination auch alle von Microsoft IIS (Version 2008 R2) unterstützten, sicheren Cipher Suites enthalten.**

Zusätzlich zu der Vorlage »Best Practices« muss der Algorithmus *RC4 128/128* und die entsprechende Cipher Suite *TLS_RSA_WITH_RC4_128_SHA* deaktiviert werden, um die Vorgaben der AG IS und des AK ITEG zur Abschaltung von RC4 zu erfüllen. Weiterhin sollte auch der Hashalgorithmus MD5 aus Sicherheitsgründen deaktiviert werden.

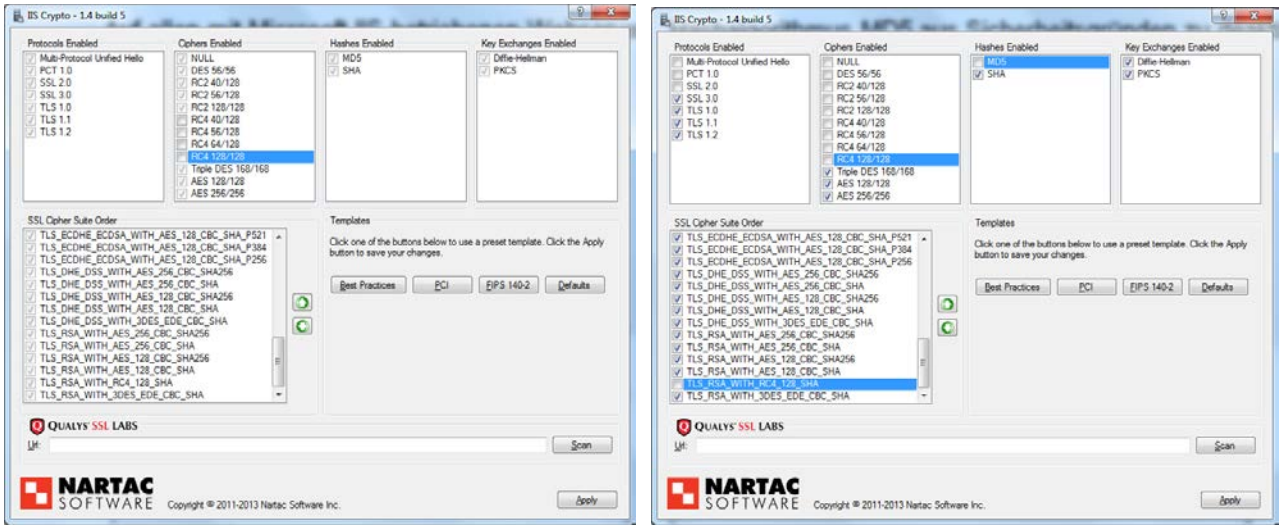


Abbildung 5: Tool IIS Crypto von Nartac (links nur RC4 deaktiviert, rechts empfohlene Einstellungen)

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 des Jahres 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. Ein entsprechender Patch für Microsoft IIS (*http://support.microsoft.com/kb/980436*) ermöglicht es, das Verhalten des Webservers konform zu RFC5746 zu konfigurieren, schaltet diese Option jedoch nicht standardmäßig ein. Die entsprechenden Registrierungseinträge finden sich im Zweig *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL*. Hier ist ein neuer Eintrag des Typs DWORD mit dem Namen *AllowInsecureRenegoClients* und dem Wert 0 (dword:00000000) anzulegen. Durch diesen Eintrag wird der Strict-Modus von SCHANNEL eingeschaltet, der eine unsichere Neuaushandlung mit nicht RFC5746-konformen Gegenstellen unterbindet. Ein weiterer Eintrag des Typs DWORD mit dem Namen *DisableRenegoOnServer* verhindert zusätzlich eine clientbasierte Neuaushandlung und darauf basierende dDoS-Angriffe (siehe z. B. *http://netsense.ch/blog/ssl-tls-renegotiation-dos-beheben/*).

Zusammengefasst sind für die serverseitige Absicherung der Neuaushandlung von HTTPS-Verbindungen folgende Registrierungseinträge erforderlich:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel]
"AllowInsecureRenegoClients" = DWORD: 00000000
"DisableRenegoOnServer" = DWORD: 00000001
```

Wenn der Webserver auch HTTPS-Verbindungen zu anderen Servern aufbaut (z. B. beim Einsatz als Proxy-Server), sollten zusätzlich im Systemregistrierungszweig *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL* noch zwei weitere Einträge des Typs DWORD mit den Namen *AllowInsecureRenegoServers* (Wert 0 bzw. dword:00000000) sowie *DisableRenegoOnClient* (Wert 1 bzw. dword:00000001) angelegt werden.

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 neben der Option SSL/TLS Compression zusätzlich auch die eher selten eingesetzte Methode SPDY Compression mit abzuschalten, falls diese aktiv sein sollte.

Microsoft unterstützt jedoch weder clientseitig im Internet Explorer noch serverseitig in IIS die Komprimierungsmethode SSL/TLS Compression, so dass Webserver unter Microsoft IIS - anders als z. B. unter Apache - nicht von der CRIME-Attacke gefährdet sind. Auch die Methode SPDY Compression wird von Microsoft IIS (alle Versionen) zumindest derzeit nicht unterstützt, da seitens Microsoft bisher nur der Internet Explorer 11 das SPDY-Protokoll unterstützt. **Für Betreiber von Webservern unter Microsoft IIS besteht hier deshalb derzeit kein Handlungsbedarf.**

Im Umfeld der CRIME-Attacke sollte jedoch beachtet werden, dass seit 2013 ein weiterentwickelter Angriff unter dem Namen BREACH bekannt ist, der auch die weit verbreitete und in Microsoft IIS eingesetzte Komprimierungsmethode *HTTP Compression* betrifft. Wie diese konfiguriert wird, ist z. B. in folgendem Beitrag beschrieben: *http://fullsocrates.wordpress.com/2012/07/31/enabling-http-compression-to-save-network-cost-in-iis7-x-23/*. Ein Schutz durch Abschaltung der betroffenen Komprimierung lässt sich hier nicht so einfach wie bei der CRIME-Attacke umsetzen, da die Performance und Bandbreitenausnutzung zu stark leiden würde. 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 sofortiger 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 des Jahres 2015 zu prüfen.

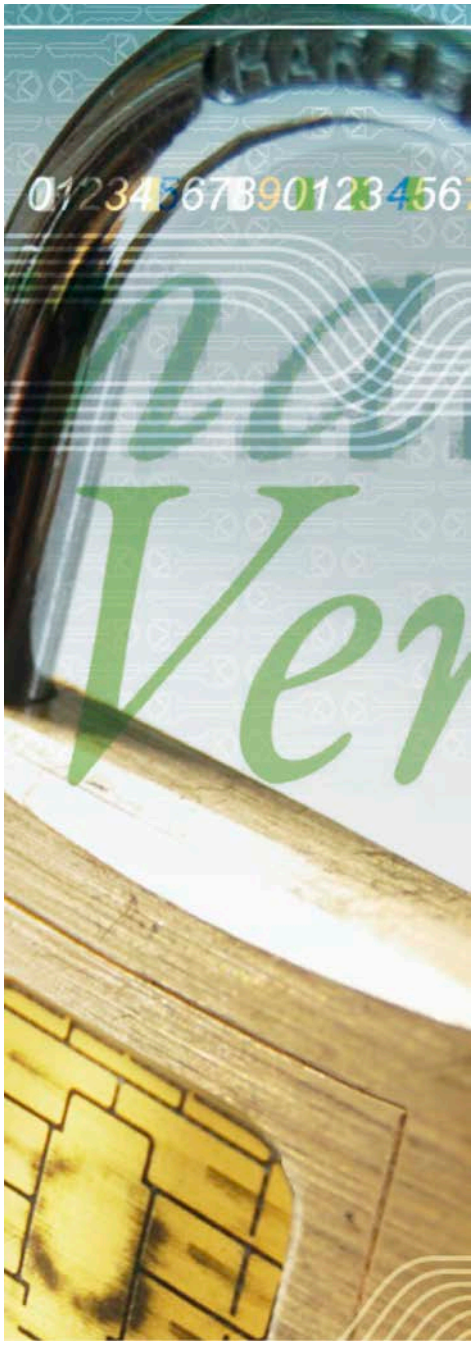
Es wird empfohlen, die Abschaltung von TLS 1.0 über das Tool IIS Crypto der Firma Nartac vorzunehmen. Dazu kann die Konfigurationsvorlage »Best Practices« aus dem Tool heraus verwendet werden. Weitere Maßnahmen sind nicht notwendig.

Analog zur Abschaltung von SSL v3 kann die server- clientseitige Deaktivierung der Nutzung von TLS 1.0 direkt über die Systemregistrierung oder toolgestützt z. B. über IIS Crypto erfolgen. Im Ergebnis müssen im Zweig *SCHANNEL\Protocols\TLS 1.0\Server* folgende Einträge des Typs DWORD vorhanden sein:

- der Eintrag *Enabled* mit dem Wert 0 (dword:00000000) sowie
- der Eintrag *DisabledByDefault* mit dem Wert 1 (dword:00000001).

Gleichzeitig ist sicherzustellen, dass mindestens das Protokoll TLS 1.1, besser jedoch auch TLS 1.2 aktiviert ist (*Enabled* = ffffffff, *DisabledByDefault* = 0).

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.