Empfehlung zur Konfiguration von TLS

Version 1.0

Nach aktuellen Statistiken von Mozilla[1] und Qualys[2] werden zwischen 93,1% und 94,7% aller https-Verbindungen mit TLS 1.2 aufgebaut. TLS 1.0 und 1.1 werden bei weniger als 1,5% der Verbindungen genutzt. Vor diesem Hintergrund und wegen der massiven Unsicherheiten in diesen veralteten Protokollen werden die führenden Browserhersteller die Unterstützung von TLS 1.0 und TLS 1.1 zeitnah abschalten. Web-Seiten, die dann kein TLS 1.2 anbieten, können nicht mehr mit diesen Browsern abgerufen werden.

Aus Sicherheitsgründen ist der Einsatz veralteter Browser, um weiterhin TLS 1.0 und 1.1 nutzen zu können, nicht sinnvoll.

Microsoft unterstützt im Rahmen des Angebots Office 365 bereits seit dem 31.10.2018 TLS 1.0 und TLS 1.1 nicht mehr.[3]

Der Standard der Kreditkarten-Industrie PCI DSS verbietet seit 20.6.2018 TLS 1.0.[4]

Die Zeitpläne der Browserhersteller zur Deaktivierung von TLS 1.0 und TLS 1.1 sind wie folgt:

- Google ab Chrome 81 (ca. März 2020) deaktiviert[5]
- Mozilla Firefox ab März 2020 deaktiviert[1]
- Apple Safari ab März 2020 deaktiviert[6]
- Microsoft IE 11 und Edge in der erste Hälfte 2020 deaktiviert[7]

Daraus ergeben sich folgende dringende Konfigurationsempfehlungen:

- SSL v2 abschalten[8]
- SSL v3 abschalten[9]
- TLS v1.0 abschalten[10]
- TLS v1.1 abschalten[10]
- TLS v1.2 aktiviert
- TLS v1.3 aktiviert, wenn technisch möglich
- SHA/SHA-1 in TLS 1.2 deaktivieren[10]

[1] https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/ (abgerufen 28.2.2019)

[2] https://www.ssllabs.com/ssl-pulse/ (abgerufen 28.2.2019)

[3] https://support.microsoft.com/en-us/help/4057306/preparing-for-tls-1-2-in-office-365

[4] https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

[5] https://security.googleblog.com/2018/10/modernizing-transport-security.html

[6] https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/

[7] https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/

[8] seit 2011 „deprecated (prohibited)“ (RFC 6176)

[9] seit 2012 „deprecated“ (RFC 7568)

[10] https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Bei der Konfiguration der Krypto-Suiten unter TLS 1.2 sind die Empfehlungen für eine striktere Konfiguration (Anhang 1) und eine etwas offenere Konfiguration (Anlage 2) möglichst zu beachten. Die Auswahl der empfohlenen Krypto-Suiten ergibt sich aus Empfehlungen der ENISA[11], des BSI[12], der Mozilla Foundation[13] und der sog. Suite B[14] der NSA.

Bei den Webservern der Einrichtungen (aktueller Apache bzw. Microsoft IIS oder vergleichbarer Server) ist eine entsprechende Konfiguration problemlos möglich. Kritisch werden jedoch proprietäre Workflow-Systeme, Zeiterfassungs-Systeme, SAP-Systeme, embedded Web-Server in Geräten wie Firewalls, Router, Switches etc., da hier Abhängigkeiten von Firmwaren existieren. Soweit die erforderliche Konfiguration nicht möglich ist, wird der Zugriff über einen reverse Proxy empfohlen. Dabei ist darauf zu achten, dass das Netzwerksegment zwischen reverse Proxy und Web-Server geschützt ist. Bei einem entsprechenden hohen Schutz des Netzes zwischen reverse Proxy und Web-Server kann u.U. in diesem Segment auf Verschlüsselung verzichtet werden.

Sobald Anmeldungen mit Benutzername und Passwort über verschlüsselte https-Verbindungen laufen oder auf personenbezogene Daten zugegriffen wird, muss nach Art. 32 DSGVO bei den technischen Maßnahmen der Stand der Technik eingehalten werden. Dies gilt auch für Web-Angebote bei denen personenbezogene Daten, z.B. in Kontaktformulare, Registrierungen, eingeben werden. Bei Verschlüsslungsverfahren vor TLS 1.2 ist die Einhaltung des Stands der Technik nicht mehr der Fall.

Bezüglich der praktischen Konfiguration für die Webserver Apache, lighttpd, nginx, Cherokee und MS IIS wird auf die Anleitung „Applied Crypto Hardening: bettercrypto.org“[15] verwiesen.

[11] https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report/at_download/fullReport

[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;

[13] https://wiki.mozilla.org/Security/Server_Side_TLS

[14] https://tools.ietf.org/html/rfc6460

[15] https://bettercrypto.org

Anhang 1

Die Empfehlung dieses Anhangs basiert auf BSI TR 2102-2 Tabelle 1, der Mozilla Empfehlung „Modern Compatibilty" & „Intermediate Compatibilty" (ohne SSLv3 und ohne Keyexchange mit RSA), den Empfehlungen von Enisa und der Suite B der NSA.

Empfohlen für alle Dienste mit Login für Beschäftigte und Studierende; Zugriff auf personenbezogen Daten; Eingabemasken für personenbezogene Daten; Own-/Nextcloud oder ähnliche Dienste.

(Tabellenreihenfolge ohne Performance Optimierung)

Code	IANA Namen	OpenSSL Namen
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
0x00,0x6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
0x00,0x9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
0x00,0x9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
0xC0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
0xC0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
0xC0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
0xC0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
0xC0,0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
0xC0,0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
0xC0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256
0x00,0x6A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256
0x00,0xA2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256
0x00,0xA3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384
0xCC,0xA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305
0xCC,0xA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305

Eine etwas striktere Empfehlung wäre die Mozilla-Empfehlung „Modern Compatibilty". Die Einhaltung kann dann recht einfach mit dem Skript „analyse.py" aus dem Paket cipherscan[16] überprüft werden.

[16] https://github.com/mozilla/cipherscan

Anhang 2

Ergänzt die Empfehlungen aus Anhang 1 um die Empfehlungen aus BSI TR 2102-2 Tabelle 2 und Tabelle 3.

Empfohlen für alle sonstigen verschlüsselten Web-Dienste.

(Tabellenreihenfolge ohne Performance Optimierung)

Code	IANA Namen	OpenSSL Namen
0x00,0x3E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	
0x00,0x3F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	
0x00,0xA0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	
0x00,0xA1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	
0x00,0xA4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	
0x00,0xA5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	
0xC0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	
0xC0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	
0xC0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	
0xC0,0x2A	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	
0xC0,0x2D	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	
0xC0,0x2E	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	
0xC0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	
0xC0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	
0x00,0xAA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	DHE-PSK-AES128-GCM-SHA256
0x00,0xAB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	DHE-PSK-AES256-GCM-SHA384
0x00,0xAC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	RSA-PSK-AES128-GCM-SHA256
0x00,0xAD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	RSA-PSK-AES256-GCM-SHA384
0x00,0xB2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	DHE-PSK-AES128-CBC-SHA256
0x00,0xB3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	DHE-PSK-AES256-CBC-SHA384
0x00,0xB6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	RSA-PSK-AES128-CBC-SHA256
0x00,0xB7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	RSA-PSK-AES256-CBC-SHA384
0xC0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	ECDHE-PSK-AES128-CBC-SHA256
0xC0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	ECDHE-PSK-AES256-CBC-SHA384
0xC0,0xA6	TLS_DHE_PSK_WITH_AES_128_CCM	DHE-PSK-AES128-CCM
0xC0,0xA7	TLS_DHE_PSK_WITH_AES_256_CCM	DHE-PSK-AES256-CCM
0xD0,0x01	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	
0xD0,0x02	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	
0xD0,0x05	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	