Das Ende von SSL 3.0 / TLS 1.0 – alles wird unsicher? – oder das BEAST erwacht

Seit einigen Tagen (theoretisch ja schon seit laengerer Zeit) kursieren Geruechte, das im Internet fast ausschliesslich verwendete SSL 3.0 / TLS 1.0 Protokoll zu „Hacken“. Jetzt ist es wohl das erste mal ernster geworden:
Quelle: TLS 1.0 (SSL Cookies) Hacking in 10 Minuten:
http://www.heise.de/newsticker/meldung/Tool-soll-SSL-Cookies-in-zehn-Minuten-knacken-1346257.html
Weitere Informationen zur “block-wise chosen-plaintext Attacke”:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.61.5887&rep=rep1&type=pdf

Auf diese Meldungen erreichten uns auch einige Kundenanfragen, wie mit der Problematik grundsaetzlich im Bereich Forefront TMG umzugehen sei. Ob TMG nun die hoeheren TLS-Versionen beherrscht und falls ja ob man diese auch einstellen soll. Dazu einen allgemeinen Ueberblick der Cipher Suiten in Forefront TMG:
https://www.carbonwind.net/blog/post/SSLTLS-usage-within-Forefront-TMG-2010.aspx

Webseiten, welche TLS 1.1 oder hoeher unterstuetzen:
http://blog.ivanristic.com/2011/09/ssl-survey-protocol-support.html

Wie man die Cipher Suiten in Windows einstellt:
„Alte“ OS: http://support.microsoft.com/kb/245030/en-us
„Neue“ OS: http://technet.microsoft.com/en-us/library/cc766285(WS.10).aspx

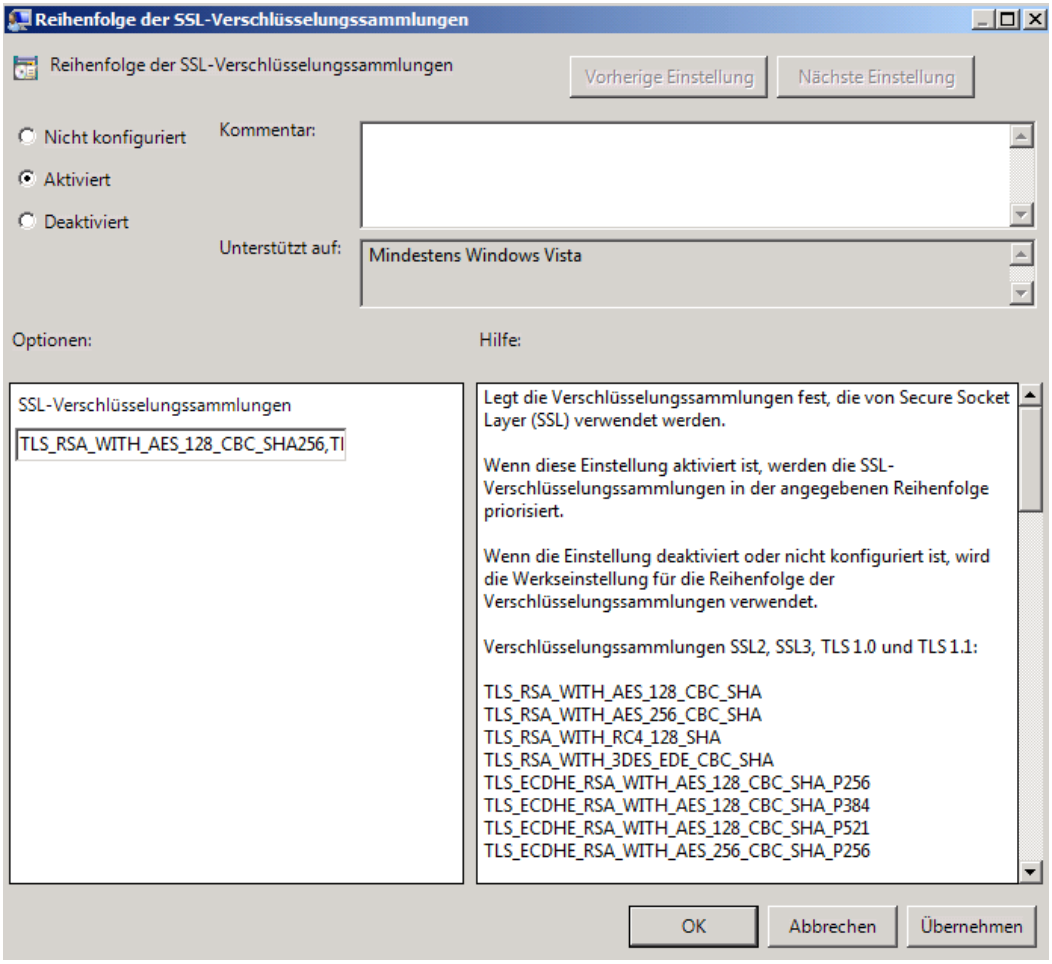
Nach diesen zahlreichen Informationen ueber die generelle Funktionsweise, die Frage, wie kann man sich mit Forefront TMG gegen moegliche zukuenftige Exploits schuetzen?:

Die Loesung?:

Da die Crypto Funktionen alle ueber die CAPI (Crypto API – Schannel) von Windows gehandelt werden, durchlaufen alle Verschluesselungs-Operationen das Crypto Subsystem von Windows. Somit bedient sich auch Forefront TMG dieser Funktionen und kann per Regkey oder GPO so konfiguriert werden, dass nur bestimmte Cipher Suites akzeptiert werden. TLS 1.0 kann auf diese Weise komplett deaktiviert werden. Das Hauptproblem werden allerdings die Anwendungen und Browser sein, welche keine Verbindung mehr mit einem Webserver/Weblistener aufbauen koennen, wenn ein Server nur noch TLS 1.1 oder hoeher unterstuetzt. Die potentielle Gefaehrdung des TLS 1.0 Protokolls durch Exploits steht somit im Gegensatz zu den Clienteinstellungen der jeweiligen zugreifenden Systeme.
Das Publishen interner Ressourcen via Forefront TMG (Exchange-Webclients, MOSS, Dynamics) kann in bestimmten Umgebungen sicherlich durch Administratoren gesteuert werden, so es sich um Corporate-Clients handelt. Schwieriger koennte aber z.B. der Bereich „Pushmail“ mit einem Wildwuchs von Endgeraeten (Smartphones) darstellen.
Für die Umstellung auf hoehere TLS-Versionen werden keine neuen Zertifikate benötigt. Ebenfalls sind keine CNG (Cryptograhic Next Generation)-Zertifikate

erforderlich, die aber momentan eh nicht von Forefront TMG unterstuetzt werden:
Quelle: http://technet.microsoft.com/de-de/library/ee796231.aspx

Wie man die Cipher Suites per Gruppenrichtlinie einstellen kann:



Deaktivieren einiger Cipher Suites per Registrierungseditor:
http://support.microsoft.com/kb/187498

Wie kann man sich noch schuetzen, außer TLS 1.1 oder hoeher am Webserver einzustellen:
http://www.heise.de/ct/meldung/Erste-Loesungen-fuer-SSL-TLS-Schwachstelle-1349687.html
(Hinweis: RC4 einsetzen 😃)

UPDATE: Von Microsoft gibt es zwischenzeitlich auch einen Security Bulletin:
http://technet.microsoft.com/en-us/security/advisory/2588513

Fazit: Forefront TMG unterstuetzt TLS 1.1 oder hoeher, weil das darunterliegende OS die Funktion mitbringt (Schannel). Ob nach der Umstellung alle Clients die angebotenen via Forefront TMG veroeffentlichten Services nach wie vor nutzen koennen ist momentan eher fraglich, da die breite Unterstuetzung im Wunderbaren Weltweiten Wildwuchs (WWW) (noch) nicht gegeben ist.