m-privacy White Paper

Titel	**TightGate-Pro und der Mindeststandard für sichere Web-Browser des BSI**	**Schlüsselwörter**	TightGate-Pro, ReCoBS, BSI, Bundesamt für Sicherheit in der Informationstechnik, web-Browser, Webbrowser, Mozilla, Firefox, Google, Chrome
Autor	Patrick Leibbrand {p.leibbrand@m-privacy.de}	**Datum**	10.04.18
		Version	1.0

Inhalt

0 Einführung

Im März des Jahres 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den „Mindeststandard des BSI für sichere Web-Browser“ veröffentlicht. Hierin wurden die weit verbreiteten Webbrowser Mozilla Firefox, Google Chrome und Microsoft Edge unter sicherheitstechnischen Aspekte verglichen und Empfehlungen zur sicheren Konfiguration der Applikationen gegeben.

0.1 Betrachtungsgegenstand des Mindeststandards

Der Mindeststandard des BSI bezieht sich explizit auf lokal installierte Webbrowser, die unmittelbar auf einem Arbeitsplatzrechner (APC) ausgeführt werden und von dort aus auf das Internet zugreifen können. Dies impliziert eine Verbindung des internen Netzes, in dem sich der APC befindet, mit dem Internet. Der Mindeststandard des BSI führt zahlreiche Bedrohungen auf, die über den Webbrowser aus dem Internet auf den APC und das diesem umgebende Netzwerk sowie die darin erreichbaren Ressourcen einwirken können. Zugleich ist der Webbrowser aufgrund softwarearchitektonischer Gegebenheiten als vergleichsweise leicht kompromittierbar durch Standardverfahren für Angriffe auf IT-Systeme anzusehen.

0.2 Risiken lokal installierter Webbrowser

Beides führt einerseits zu begründeten Sicherheitsanforderungen hinsichtlich der funktionalen Aspekte der Applikation und der organisatorischen Gegebenheiten zum Zeitpunkt der Entwicklung und der Softwarepflege. Andererseits führt das BSI detaillierte Empfehlungen zur sicheren Auswahl und Konfiguration lokal installierter Webbrowser an. Im Abschnitt 3.2 des Mindeststandards weist das BSI im Rahmen der spezifischen Risikobetrachtung dennoch eindringlich auf ein nicht zu vernachlässigendes Restrisiko hin. Es besteht beim Betrieb auch eines korrekt entwickelten, gepflegten und konfigurierten Webbrowsers weiterhin, sofern dieser lokal installiert ist. Dieses Restrisiko kann je nach anzustrebendem Schutzniveau der Zielinfrastruktur in manchen Fällen tragbar sein. Bei erhöhtem Schutzbedarf kann es nach Aussage des BSI notwendig sein, Maßnahmen zu ergreifen, die dieses Restrisiko zusätzlich minimieren.

1 TightGate-Pro für erhöhten Schutzbedarf

Der Mindeststandard gilt daher nach Angabe des BSI nur für normalen Schutzbedarf gemäß IT-Grundschutz. Für darüber hinausgehenden Schutzbedarf empfiehlt das BSI erweiterte Lösungen wie beispielsweise Remote-Controlled-Browser-Umgebungen. Das dedizierte Remote-Controlled Browser System (ReCoBS) TightGate-Pro arbeitet nach dem empfohlenen Prinzip des ferngesteuerten Webbrowsers. Es erfüllt vollumfänglich das BSI-Schutzprofil BSI-PP-0040 und ist in einer gemäß Common Criteria auf dem Schutzlevel EAL 3+ zertifizierten Version erhältlich.

1.1 Kapselung von Standard-Browsern

TightGate-Pro positioniert sich sicherheitstechnisch erheblich über dem Mindeststandard und ermöglicht die sichere Internetnutzung über einen Standard-Webbrowser auch in Umgebungen mit erhöhtem Schutzbedarf. TightGate-Pro implementiert wahlweise die Webbrowser Mozilla Firefox und / oder alternativ den Webbrowser Google Chrome. Beide Produkte erfüllen hinsichtlich ihrer grundlegenden Eigenschaften nach Analyse des BSI die meisten sicherheitsbezogenen Anforderungen a priori. Weiterhin erfolgt bei TightGate-Pro die Isolierung des Browsers auf einem dedizierten Serverrechner mit weitreichend gehärtetem Betriebssystem, das zusätzlich über eine kernelseitig implementierte, hochgradig feingranulare Zugriffsrechtekontrolle mittes Rule-Set Based Access Control (RSBAC) verfügt. Damit ist eine bestmögliche Kapselung des Browsers auch gegen das unterliegende Serverbetriebssystem gegeben, womit ausgewiesen hohe Resistenz gegen Angriffe aus dem Internet und maximaler Eigenschutz des ReCoBS-Servers einhergehen.

1.2 Trennung vom internen Netzwerk

TightGate-Pro wird stets außerhalb eines schutzbedürftigen internen Netzwerks (beispielsweise in einer Demilitarisierten Zone, DMZ) betrieben und von diesem durch Paketfilter getrennt. Die Verbindung zu den APC im internen Netzwerk erfolgt über ein funktionsspezifisches Protokoll, das nur Bildschirminformationen framebasiert überträgt. Selbst im Falle einer Kompromittierung des TightGate-Servers ist die Übertragung von Angriffsaktivitäten in das interne Netzwerk praktisch ausgeschlossen.

1.3 Sichere Grundkonfiguration, Konfigurations- und Administrationsschutz

TightGate-Pro wird werkkseitig in einer sicheren und datenschutzfreundlichen Grundkonfiguration ausgeliefert. Alle wesentlichen Einstellungen des Systems, insbesondere solche mit Sicherheitsrelevanz, sind nur serverseitig möglich. Benutzer können auf sicherheitsbezogene Systemeinstellungen von TightGate-Pro grundsätzlich keinen Einfluss nehmen. Alle benutzerseitig zugänglichen Einstelloptionen betreffen lediglich funktionale Aspekte und schwächen weder Trennwirkung noch Eigenschutz von TightGate-Pro. Die administrativen Aufgaben sind auf mehrere nach Verantwortungsbereich getrennte Administrationsrollen mit dedizierten Zugängen delegiert. Die vollständige Kontrolle eines TightGate-Pro-Systems über nur ein Administratorenkonto ist dabei nicht möglich. Das Sicherheitskonzept der „Administrativen Gewaltenteilung“ (Rollentrennung, Segregation of Duties) erfordert stets das Zusammenwirken mehrerer Verwaltungsrollen. Hierdurch können organisatorische Gegebenheiten leicht auf TightGate-Pro übertragen werden, zudem verringert sich die Gefahr einer umfassenden Kompromittierung im Fall des Verlustes administrativer Zugangsdaten.

2 Risikominimierung durch TightGate-Pro

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgewiesenen Restrisiken beim Betrieb eines empfohlenen und korrekt konfigurierten lokal installierten Webbrowsers werden mit TightGate-Pro weitgehend neutralisiert. Interne Ressourcen sind für Angreifer aus dem Internet bei Nutzung des Webbrowsers über TightGate-Pro in keinem Fall zugänglich. Benutzer haben auf sicherheitsrelevante Einstellungen keinen Zugriff. Zugleich können die seitens des BSI ausgegebenen Sicherheitsempfehlungen zum Betrieb von Webbrowsern mit TightGate-Pro ohne Verminderung des Schutzniveaus vereinfacht umgesetzt werden, was den administrativen Aufwand in sicherheitskritischen Umgebungen vermindert.

2.1 Wirksamkeit gegen Advanced Persistent Threats (APT)

Schließlich positioniert sich TightGate-Pro als explizit zu IT-Sicherheitszwecken konzipiertes und zertifiziertes Schutzsystem in technischer Hinsicht auch deutlich über den ebenfalls im Mindeststandard des BSI erwähnten Virtualisierungslösungen. Letztere wurden hinsichtlich ihrer Softwarearchitektur bisweilen nicht durchgehend als Schutzsystem entworfen, implementieren weniger weitgehende Sicherheitsmaßnahmen im Serverbetriebssystem oder nutzen zu funktionsreiche Übertragungsprotokolle. Die resultierenden, grundsätzlichen Unzulänglichkeiten manifestieren sich in folgenschweren Sicherheitslücken wie der jüngst bekannt gewordenen „Spectre“-Schwachstelle. TightGate-Pro ist bezüglich derlei Angriffsvektoren systembedingt weit weniger empfindlich als Client-Server-Lösungen mit konventioneller Systemarchitektur und nimmt daher auch unter den Remote-Controlled Browser Systems sicherheitstechnisch eine Sonderstellung ein.

3 Weiterführende Informationen

- **Mindeststandard des BSI für sichere Web-Browser**
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/Sichere_Web-Browser/Sichere_Web-Browser_node.html
  Detaillierte Informationen und Dateidownloads
- **Internetpräsenz der m-privacy GmbH**
  https://www.m-privacy.de

4 Unternehmensprofil

Die m-privacy GmbH mit Sitz in Berlin entwickelt TightGate-Pro, eine Client-Server-Lösung zur sicheren Internetanbindung von Computerarbeitsplätzen nach dem Prinzip des ferngesteuerten Webbrowsers. TightGate-Pro ist auch in einer BSI-zertifizierten Version erhältlich und erreicht die Schutzstufe EAL3+. Darüber hinaus stellt das Unternehmen ein umfangreiches Dienstleistungsportfolio zur IT-Sicherheit und zum Datenschutz für professionelle Anwender bereit.