



m-privacy GmbH  
Werner-Voß-Damm 62  
12101 Berlin  
Tel. +49-30-24 34 23 34  
Fax +49-30-99 29 68 56  
info@m-privacy.de  
www.m-privacy.de

## Pressemitteilung

BSI-Zertifikat für sicheren Browser

## TightGate-Pro CC erhält deutsches IT-Sicherheitszertifikat nach Common Criteria

*Berlin, 15.02.2016 - Das neue Jahr fängt gut an für Internetnutzer in sicherheitskritischen Umgebungen: Das dedizierte Remote-Controlled Browser System (ReCoBS) TightGate-Pro CC der Berliner m-privacy GmbH wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) offiziell nach Common Criteria (CC) auf der Stufe EAL3+ zertifiziert. TightGate-Pro wird weltweit zur risikoarmen Internetnutzung in sicherheitskritischen Umgebungen eingesetzt, wo beispielsweise Firewalls allein nicht ausreichen.*

Mit Brief und Siegel: TightGate-Pro ist der sichere Webbrowser! Das Remote-Controlled Browser System (ReCoBS) der Client-Server-Lösung begegnet Angriffsszenarien aus dem Internet vorbeugend. Mit der Zertifizierung von TightGate-Pro CC gemäß Common Criteria haben Kunden die Gewissheit einer funktionalen, sicheren und unabhängig geprüften Lösung auf höchstem Niveau. Das für den Einsatz in Umgebungen mit normalem bis sehr hohem Schutzbedarf konzipierte System isoliert die Gefahren des Internets weitaus besser als lokale Virtualisierungslösungen oder nicht als Schutzsystem vorgesehene Terminalserver-Infrastrukturen.

Insbesondere im öffentlichen Bereich, jedoch zunehmend auch im Finanzwesen, der Energiewirtschaft und zahlreichen Industriebetrieben ist ein vom BSI vergebenes Sicherheitszertifikat eine zentrale Anforderung an IT-Sicherheitsprodukte im Vorfeld der Beschaffung. Markus Senbert, Channel Account Manager des auf IT-Sicherheit spezialisierten Distributors sysob, betont den deutlichen Mehrwert aus Anwendersicht: „Das Zertifikat erspart die aufwendige Evaluierung auf Behörden- oder Unternehmensseite und gewährleistet definierte Produktsicherheit entsprechend internationaler Standards.“

Die Common Criteria for Information Technology Security Evaluation, kurz Common Criteria oder CC, sind der weltweite Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten. Die Zertifizierung von TightGate-Pro erfolgte gemäß den strengen Vorgaben des vom BSI entwickelten ReCoBS-Schutzprofils auf der Stufe EAL3+, die für Systeme dieser Art der höchsten Prüftiefe entspricht. Entwicklungsleiter Dr. Amon Ott bringt es auf den Punkt: „Zusammen mit dem präventiven Funktionsprinzip der konsequenten Trennung kann TightGate-Pro in Abhängigkeit vom Einsatzszenario auch IT-Sicherheitsprodukten mit nominell höherem EAL sicherheitstechnisch deutlich überlegen sein.“

Die Sicherheit eines dedizierten ReCoBS wie TightGate-Pro resultiert vor allem aus der starken Trennwirkung: Der Browser des Arbeitsplatzrechners kommuniziert zu keinem Zeitpunkt direkt mit dem Internet. Stattdessen übernimmt die dem internen Netzwerk vorgelagerte Appliance TightGate-Pro die Ausführung des Browsers. Das abgesetzte System ruft die angeforderten Web-Inhalte ab und leitet dem Computer des Anwenders nur die Bildschirmausgabe über ein funktionsspezifisches Protokoll zu. Auch aktive Inhalte wie beispielsweise Adobe Flash sind gefahrlos nutzbar. Für den Anwender unterscheiden sich Bedienung und Funktionsumfang nur wenig verglichen mit dem lokal installierten Webbrowser - bei erheblich gesteigerter Sicherheit.

#### **Die m-privacy GmbH**

mit Sitz in Berlin entwickelt innovative Client-Server-Lösungen zur sicheren Internetanbindung von Computerarbeitsplätzen auf Basis der TightGate-Technik. Darüber hinaus stellen wir ein umfangreiches Dienstleistungsportfolio zur IT-Sicherheit und zum betrieblichen Datenschutz für professionelle Anwender bereit. Die TightGate-Technik verbindet das bewährte Konzept der „Administrativen Gewaltenteilung“ mit RSBAC (Rule Set Based Access Control) und einer umfassenden Härtung des Betriebssystems.

#### **Die sysob IT-Distribution GmbH & Co. KG**

ist ein renommierter Value-Added-Distributor (VAD), der sich auf den Vertrieb von zukunftsweisenden IT-Security- und Wireless LAN-Lösungen spezialisiert hat. Unter dem Motto „innovativ, kompetent, vertrauensvoll“ greift der VAD auf ein Netzwerk von Partnern in Deutschland, Österreich und der Schweiz zurück. Einen zusätzlichen Mehrwert für den Channel bietet sysob mit dem Service-Konzept „Total Solution Provider“. Darüber hinaus forciert sysob als moderner Distributor das Managed Security Service Provider(MSSP)- bzw. Managed Backup-Konzept: Durch Nutzung der sysob-eigenen Infrastruktur und eines in Deutschland betriebenen Rechenzentrums können Partner eigene Cloud-Lösungen für deren Kunden hosten sowie Teststellungen und MSSP-Sonderkonditionen inklusive Finanzierungsmodellen anbieten. Nicht zuletzt ist der speziell gegründete Unternehmensbereich „sysob IT-Service u. Support“ für die technische Beratung, Unterstützung und Schulung der Reseller zuständig. sysob verfügt über ein breites Sortiment an praxiserprobten Produkten von kompetenten Herstellern. Weitere Informationen unter: [www.sysob.com](http://www.sysob.com).

**m-privacy GmbH**  
Werner-Voß-Damm 62  
12101 Berlin

Fon: +49 30 24342334  
Fax: +49 30 99296856

[info@m-privacy.de](mailto:info@m-privacy.de)  
[www.m-privacy.de](http://www.m-privacy.de)  
[www.tightgate.de](http://www.tightgate.de)

**sysob IT-Distribution GmbH & Co. KG**  
Kirchplatz 1  
93489 Schorndorf

Markus Senbert  
Fon: +49 (94 67) 74 06 124  
Fax: +49 (94 67) 74 06 290

[msenbert@sysob.com](mailto:msenbert@sysob.com)  
[www.sysob.com](http://www.sysob.com)

### **Hintergrund: Angriffe über Internetbrowser**

Professionelle Anwender sind sich des Risikos bewusst: Viele Attacken auf Rechner und Netzwerke nutzen gezielt allgegenwärtige Sicherheitslücken in verbreiteten Internetbrowsern. Zuverlässiger Schutz vor solchen Attacken ist schwierig. Webbrowser sind komplexe Programme, die kaum fehlerfrei zu entwickeln sind. Konventionelle Betriebssysteme verfügen überdies nur über eine recht grobmaschige Zugriffsrechtekontrolle. Sie räumen Applikationen oft deutlich mehr Berechtigungen ein als nötig. Wirkungsvolle Kapselung einer gefährdeten Software ist so kaum möglich. Auch filternde Schutzsysteme wie Firewalls oder Intrusion Detection Systems (IDS) gelangen im Hinblick auf Erkennungsrate und Fehlalarmresistenz schnell an ihre Grenzen. Das Schutzniveau in sicherheitskritischen Umgebungen bleibt daher oft hinter den Anforderungen zurück, sobald Internetzugang am Arbeitsplatz vorgesehen ist.

### **Zuverlässiger Schutz durch Trennung**

Zielführender ist der Ansatz des ferngesteuerten Webbrowsers, der mit TightGate-Pro implementiert und nunmehr durch das BSI zertifiziert wurde. Der Browser des Anwenders ist hierbei nicht direkt mit dem Internet verbunden. Stattdessen wird ein marktüblicher Browser auf einem dedizierten Server in einer abgesetzten, stark gehärteten Systemumgebung ausgeführt. Diese liegt bewusst außerhalb des internen Klientennetzwerks, um den direkten Durchgriff aus dem Internet auf die interne Unternehmens-IT präventiv zu vermeiden. Lediglich die Bildschirmausgabe wird über ein funktionspezifisches Protokoll verschlüsselt an den Klientenrechner übertragen, dort dekodiert und dargestellt. Umgekehrt kann der Browser vom Arbeitsplatz durch den Benutzer wie gewohnt per Maus und Tastatur bedient – lies: ferngesteuert – werden.

### **Abstand schafft Sicherheit**

Diese technische Abbildung des „Abstandsprinzips“ verbannt potenzielle Angreifer präventiv aus internen Netzwerken und verhindert darüber hinaus ungewollten Datenabfluss in das Internet. Zugleich ist die vollfunktionale Nutzung des Internets von jedem Arbeitsplatz aus möglich. Auf aktive Inhalte, Multimedia oder Adobe Flash muss unter Sicherheitsaspekten nicht verzichtet werden. Das funktionspezifische Protokoll zwischen dem abgesetzten ReCoBS-Server und dem Klienten sowie die starke Härtung des Serverbetriebssystems sorgen für Trennwirkung von der „Gefahrenquelle Internet“. Ein ReCoBS gehört damit technisch bedingt zu den wirkungsvollsten Schutzmaßnahmen gegen Angriffe aus dem Internet über den Webbrowser.

TightGate-Pro wird weltweit auf einigen 10.000 Arbeitsplätzen verwendet und ist aufgrund seiner ausgefeilten Systemarchitektur sowohl für kleinere, als auch für sehr große Infrastrukturen geeignet. Für mobile Rechner steht eine virtualisierte Version zur Verfügung, die einen Basisschutz vor Angriffen über den Internetbrowser bietet.