Titel	**Trennung der Ausführungsumgebung internetgebundener Applikationen unter organisatorisch-funktionalen bzw. sicherheitstechnischen Überlegungen**	Schlüsselworte	ReCoBS, Remote Controlled Browser System, Internet, Terminalserver, CITRIX
Autor	Patrick Leibbrand / p.leibbrand@m-privacy.de	**Datum**	17.02.14
Redaktion	Patrick Leibbrand / p.leibbrand@m-privacy.de	**Version**	1.4 Final

1 Merkmale virtueller Ausführungsumgebungen

Interne Unternehmens- und Behördennetzwerke unterliegen einem steten Wandel. Immer häufiger werden Arbeitsumgebungen insbesondere für größere, homogene Nutzergruppen virtualisiert. Dies hat vor allem wirtschaftliche Gründe. Vorhandene oder zu beschaffende Hardware kann effizienter genutzt werden, zugleich lassen sich virtuelle Umgebungen besonders ressourceneffizient verwalten. Diese organisatorisch-funktionale Trennung spielt sich jedoch vollständig innerhalb des internen Unternehmens - bzw. Behördennetzwerks ab. **Eine Trennung unter Sicherheitsaspekten** im Sinne einer Abschirmung von den Gefahren aus dem Internet **erfolgt nicht.**

Im Gegenteil: Risiken beispielsweise infolge häufiger Sicherheitslücken in internetgebundenen Applikationen wirken sich in diesem Fall nicht nur auf einzelne Arbeitsplatzstationen aus. Sie gefährden vielmehr sämtliche Ressourcen der gesamten Topologie ausgehend von der zentralen Stelle eines Terminal- oder Hypervisor-Servers. Den Aspekten der IT-Sicherheit kommt vor diesem Hintergrund gerade in virtuellen Umgebungen besondere Bedeutung zu. Nur in vollem Bewusstsein um Eignung und Stärke ergriffener Schutzmaßnahmen lässt sich das hohe Wertschöpfungspotenzial einer virtuellen Arbeitsumgebung gefahrlos nutzen.

Klassische Virtualisierungslösungen innerhalb eines Unternehmens- bzw. Behördennetzwerks mit der Zielsetzung einer Rationalisierung sind konstruktiv bedingt grundsätzlich nicht als Sicherheitssysteme zum Schutz vor Gefahren aus dem Internet geeignet.

Sie wurden zu diesem Zweck unter Gesichtspunkten des Software Engineerings nicht entworfen und erfüllen die organisatorischen bzw. technischen Anforderungen an ein IT-Sicherheitssystem erwartungsgemäß nicht.

Insbesondere die Trennwirkung von der „Gefahrenquelle“ Internet, die Verwaltung von Berechtigungen für Applikationen und Benutzer sowie der Eigenschutz lassen bei nicht dediziert zu Sicherheitszwecken entworfenen Systemen zu wünschen übrig. Das trügerische Gefühl vermeintlicher Sicherheit bei Administratoren und Entscheidungsträgern ist in Anbetracht des weiter fortbestehenden Risikos als ebenso gefahrenträchtig einzustufen wie das mangelnde Schutzniveau an sich.

Ein zuverlässiger Schutz interner Netzwerke mitsamt der darin befindlichen virtuellen Arbeitsumgebungen ist nur durch eine **sicherheitszentrierte** Trennung der kompletten Infrastrukturen vom Internet zu bewerkstelligen. Dedizierte Remote-Controlled Browser Systems (ReCoBS) leisten diese Trennung. Sie ergänzen damit klassische Topologien (mit einzelnen Arbeitsplatzrechnern) ebenso wie virtualisierte Arbeitsumgebungen (z. B. via Terminalserver) um eine Sicherheitskomponente nach dem aktuellen Stand der IT-Sicherheitstechnik.

2 Konventionelle Terminalserver und ReCoB-Systeme

Konventionelle Virtualisierungslösungen sind als Schutzsysteme gegen Angriffe aus dem Internet nicht geeignet, da sie sich im internen Netzwerk befinden und ihre Trennwirkung nach außen zu schwach ist. Dieses Manko lässt sich bei kommerziell verfügbaren Anlagen nicht mit vertretbarem Aufwand kompensieren. Zugleich sind diese Infrastrukturen in höchstem Maße schutzbedürftig. Nachfolgende Tabelle verdeutlicht diesen Zusammenhang in einer Gegenüberstellung.

Eignung als Schutzsystem vor Angriffen aus dem Internet	
Ungeeignet	**Gut geeignet**
Klassischer Terminalserver, Virtualisierungslösung, Hypervisoren und entsprechende Server	**Professionelles, dediziertes Remote-Controlled Browser System (ReCoBS), z. B. TightGate™-Pro**
Sicherheitslevel abhängig vom zugrundeliegenden Betriebssystem; konventionell meist nur bedingt und mit hohem Aufwand absicherbar	Stark gehärtetes Serverbetriebssystem mit kernelseitig implementierten Sicherheitsfunktionen. Unabhängig von versorgten Plattformen
Grobmaschige Zugriffsrechtekontrolle ohne anwendungsspezifische Anpassung	Sehr feingranulare Zugriffsrechtekontrolle, vollständige Applikationskapselung durch individuell sicherheitszentriert erstelltes und gepflegtes Regelwerk
Funktionsreiches („zu mächtiges“) Übertragungsprotokoll zu den Arbeitsplatzrechnern (Klienten) bzw. zum Zugriff auf deren Ressourcen	Funktionsspezifisches Übertragungsprotokoll vermeidet Angriffsvektoren prophylaktisch, funktional auf Einsatzzweck optimiert
Sicherheitstechnisch einwandfreie Implementierung von Dateitransfer und Druckfunktionen schwierig	Drucken und Datentransfer nach dem „Schleusenprinzip“ gem. BSI-Schutzprofil
Instabilität und unerwünschte Seiteneffekte durch konzeptionell wenig erprobte Eigenentwicklungen	Ausgereiftes, praxisbewährtes System. Langzeitstabilität auch bei hoher Beanspruchung. Referenzinstallationen
Instabile, unbefriedigende oder fehlende Unterstützung von Multimediadaten und aktiven Inhalten	Störungsfreie Wiedergabe aller gängigen Multimediaformate. Sicherer Schutz vor Zero-Day-Exploits bei aktiven Inhalten
Hoher Konfigurations-, Wartungs- und Testaufwand bindet Ressourcen	Einfache, zentrale Installation; vorkonfiguriert, Softwarepflege komplett durch Hersteller

3 Optimale Ergänzung: professionelle ReCoB-Systeme

Das dedizierte ReCoB-System TightGate™-Pro arbeitet als der zu sichernden Infrastruktur vorgeschaltetes Schutzsystem. Die Funktionsweise unterscheidet sich grundsätzlich von reaktiven Maßnahmen wie Virenscanner oder Firewalls. TightGate™-Pro arbeitet nicht filternd, sondern präventiv abschirmend.

Es bewirkt die sicherheitszentrierte Trennung internetgebundener Applikationen von einem Terminalserver bzw. einer anderweitigen Arbeitsumgebung im internen Netzwerk. Andererseits schützt sich TightGate™-Pro autoaktiv vor Manipulationen der eigenen Systemumgebung durch das feingranulare Berechtigungssystem RSBAC[1] in Verbindung mit umfassender Betriebssystemhärtung nach dem aktuellen Stand der IT-Sicherheitstechnik.

1 RSBAC = Rule Set Based Access Control. Siehe auch www.rsbac.org

Folgende Eigenschaften zeichnen professionelle, dedizierte ReCoB-Systeme wie TightGate™-Pro aus:

1. **Physikalische Trennung** internetgebundener Applikationen vom internen Netz und damit auch von Terminalservern bzw. anderweitigen Virtualisierungslösungen.
2. **Keine Beschränkung auf den Webbrowser:** sichere Nutzung weiterer stark angriffsgefährdeter Applikationen wie etwa Adobe Reader ohne Gefährdung der virtualisierten Infrastruktur oder der Klientenrechner. Weitere Applikationen auf Kundenwunsch in die gekapselte Umgebung des vorgeschalteten Schutzsystems integrierbar.
3. **Generell keine Programmausführung mit Superuser-Privilegien:** Die wesentlichen Serverkomponenten von TightGate™-Pro zur Übertragung der Videoinhalte in das interne Netz arbeiten mit minimalen Rechten. Deren Berechtigungssphäre erlaubt weder eine Verwaltung des Systems noch den direkten Zugriff auf Ressourcen im internen Netzwerk (z. B. einen Terminalserver oder verbundene Klientenrechner).
4. **Schwachstelle Rechteverwaltung eliminiert:** Alle Applikationen auf TightGate™-Pro sind in jeweils eigenen Berechtigungssphären vollständig isoliert und verfügen nur über minimale Berechtigung zur Ressourcennutzung.
5. **Funktionsspezifisches Protokoll:** Verbindung zwischen ReCoBS-Server und Terminalserver ausschließlich über funktionsspezifisches VNC-Protokoll (Bilddatenübertragung, Maus- und Tastatursignale).
6. **Präventiver Schutz sensibler Daten** des internen Netzwerks einschließlich virtualisierter Arbeitsumgebungen und / oder der Klientenrechner vor unberechtigtem Zugriff, missbräuchlicher Nutzung (z. B. in sogenannten Botnetzen), Manipulation und Benutzerfehlverhalten. Fehlerträchtige Filterung oder andere Reaktivmaßnahmen sind nur noch flankierend erforderlich oder können entfallen. Hohe prophylaktische Wirksamkeit insbesondere gegen Zero-Day-Exploits in internetgebundenen Applikationen.
7. **Kein unberechtigter Datenabfluss in das Internet** („Data Leakage“) durch zuverlässige Trennung des internen Netzwerks von den internetgebundenen Applikationen auf dem vorgeschalteten Schutzsystem in Verbindung mit einer detaillierten Berechtigungsverwaltung. Keine unberechtigte Kontaktaufnahme interner Applikationen ins Internet (gilt insbesondere auch für auf anderen Wegen eingetragene Schadprogramme).
8. **Umfassender Eigenschutz des ReCoBS-Servers** durch systemeigenes, stark gehärtetes Serverbetriebssystem unabhängig von der sonstigen Sicherheitsarchitektur oder in Betrieb befindlicher Plattformen bzw. Anwendungen.
9. **Zentraler Übergangspunkt in das Internet**, dadurch kosteneffiziente Administration und zugleich umfassende Konfigurationsoptionen. Einbindung bestehender Verzeichnisdienste zur Benutzer- und Druckerverwaltung möglich. Plattformübergreifende Kompatibilität.
10. **Hohe Verfügbarkeit durch Clustersystem** mit automatischem Load Balancing und verteilter Datenhaltung.

4 Fazit

Keinesfalls darf davon ausgegangen werden, dass Terminalserver-Infrastrukturen oder Virtualisierungslösungen innerhalb interner Netzwerke per se bereits eine Sicherheitswirkung zum Schutz vor Angriffen aus dem Internet entfalten. **Dies können solche Systeme aus technischen Gründen nicht leisten, zumal sie einen integralen Bestandteil der zu schützenden, internen Infrastruktur darstellen!** Sie müssen entweder konventionell gesichert oder - weit zuverlässiger und ökonomischer - mit dedizierten ReCoB-Systemen wie TightGate™-Pro geschützt werden.

Die in vielen Fällen positive ökonomische Prognose einer virtualisierten Arbeitsumgebung lässt sich mit optimaler Systemsicherheit kombinieren, indem ein dediziertes ReCoB-System wie TightGate™-Pro zur Absicherung des Internetzugriffs eingesetzt wird. Professionelle ReCoB-Systeme führen zu einer sicherheitstechnischen Aufwertung bestehender oder einzurichtender Topologien. Dies gilt in dedizierten oder virtualisierten Netzen gleichermaßen.

5 Weiterführende Informationen

Nachfolgend sind Literaturhinweise (online und offline) im Hinblick auf die zugrunde liegende Technik sowie rechtlich-organisatorische Rahmenbedingungen gegeben. Erweiterte Informationen können jederzeit bei dem im Dokumentenkopf genannten redaktionellen Ansprechpartner abgerufen werden.

5.1 Informationen im Internet

- Homepage der m-privacy GmbH - www.m-privacy.de
- Informationen zu TightGate™-Pro - www.m-privacy.de/produkte/tightgate-pro
- Homepage des RSBAC-Projekts - www.rsbac.org

5.2 ReCoBS-Informationen des BSI

- **Kurzinformation ReCoBS** des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- **Schutzprofil „ReCoBS- Remote-Controlled Browser Systems“ (PP-0040)** des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

5.3 Unternehmensprofil

Die m-privacy GmbH mit Sitz in Berlin entwickelt seit dem Jahr 2002 innovative Client-Server-Lösungen zur hochsicheren Internetanbindung von Computerarbeitsplätzen mittels Remote-Controlled Browser Systems (ReCoBS) auf der Basis der TightGate™-Technologie. Diese verbindet das bewährte Konzept der „Administrativen Gewaltenteilung“ mit feingranularer Zugriffsrechtekontrolle über RSBAC (Rule Set Based Access Control) und einer umfassenden Härtung des Betriebssystems. TightGate™-Server der m-privacy GmbH werden deutschlandweit von Unternehmen sowie Bundes- und Landesbehörden zum Schutz ihrer Netzwerke verwendet. Die speziell für sensible Netzwerkumgebungen vorgesehenen Produkte wurden bereits mehrfach mit dem Datenschutz-Gütesiegel ausgezeichnet. Eine Zertifizierung des ReCoBS-Servers TightGate™-Pro (CC) Ver. 1.4 nach Common Criteria beim Bundesamt für Sicherheit in der Informationstechnik (BSI-DSZ-CC-0589) wird derzeit angestrebt.