

<b>Titel</b>	<b>Vergleich eines ReCoB-Systems nach der TightGate™-Technologie mit klassischen, X-Server-basierten Terminalserver-Architekturen</b>	<b>Schlüsselworte</b>	ReCoBS, Remote Controlled Browser System, Internet, X-Server, Terminalserver, Internet, Intranet, RSBAC, Rule Set Based Access Control, Administrative Gewaltenteilung
<b>Autoren</b>	Holger Maczkowsky / h.maczkowsky@m-privacy.de Patrick Leibbrand / p.leibbrand@m-privacy.de	<b>Datum</b>	22.12.11
<b>Redaktion</b>	Patrick Leibbrand / p.leibbrand@m-privacy.de	<b>Version</b>	1.4 Final

## Inhalt

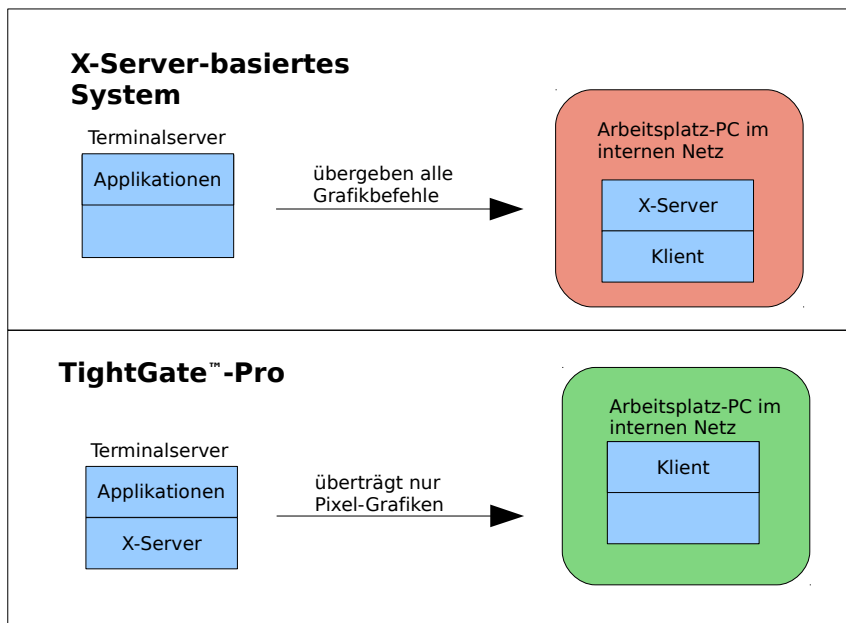
0 Einleitung und Begriffsdefinition.....	1
1 Ausführungsumgebung .....	2
1.1 Klassischer X-Server.....	2
1.2 X-Server bei TightGate™-Pro.....	2
2 Angriffsszenarien.....	3
2.1 Erste Stufe: Terminalserver.....	3
2.2 Zweite Stufe: X-Server.....	3
3 Sicherheit durch professionelle ReCoB-Systeme.....	3
4 Terminalserver mit Eigenmitteln.....	4
5 Anhang.....	6
5.1 Informationen im Internet.....	6
5.2 ReCoBS-Informationen des BSI.....	6
6 Unternehmensprofil.....	6

## 0 Einleitung und Begriffsdefinition

Moderne Systemumgebungen mit konventionellem Aufbau umfassen zahlreiche internetgebundene Applikationen. Internetbrowser oder E-Mail-Programme setzen eine Verbindung in das Internet zur einwandfreien Funktion zwingend voraus. Nicht zuletzt durch die grobmaschige Berechtigungskontrolle der meisten klassischen Betriebssysteme resultiert aus internetgebundenen Applikationen prinzipiell ein hohes Sicherheitsrisiko für die Systemumgebung sowie das angeschlossene Netzwerk. Grundsätzlich bieten X-Server-basierte Lösungen eine Möglichkeit zur Trennung von Applikationen und Systemumgebungen. Abhängig von der jeweiligen Implementierung dieses Grundkonzepts kann das erzielte Schutzniveau jedoch sehr unterschiedlich sein.

Um zu verstehen, weswegen ein ReCoB-System<sup>1</sup> wie TightGate™-Pro der klassischen X-Server-Lösung sicherheitstechnisch grundsätzlich überlegen ist, ist zunächst ein genauerer Blick auf die Architektur der einzelnen Systeme notwendig. Nachfolgend ist hierzu eine schematische Übersicht gegeben.

<sup>1</sup> ReCoB-System / ReCoBS: Remote Controlled Browser System - System mit ferngesteuertem Internetbrowser zur Trennung von internetgebundenen Applikationen von der Systemumgebung der Arbeitsplatzrechner

**Terminalserver:**

Server, auf den die Applikationen zur Ausführung gebracht werden

**X-Server:**

Server, der die Informationen, welche von den Applikationen bereit gestellt werden, in eine Bildschirmausgabe umwandelt

**Klient:**

Applikation, die sich mit dem X-Server verbindet und von diesem alle Informationen zur Grafikausgabe übernimmt

**Arbeitsplatz-PC:**

Arbeitsplatzcomputer im internen Netz

## 1 Ausführungsumgebung

### 1.1 Klassischer X-Server

Der X-Server ist im klassischen System ein Programm, welches mit Administrationsrechten (Root-Rechten unter UNIX) läuft. Das Programm hat vollen Zugriff auf alle I/O-Ports des Computers und kann diesen vollständig kontrollieren.

Wie die Grafik zeigt, läuft im klassischen System der X-Server ebenfalls auf dem Arbeitsplatz-PC im internen Netzwerk und nicht auf dem entfernten Terminal-Server, der auch außerhalb einer Firmeninfrastruktur angesiedelt werden könnte. In der Folge werden sämtliche Informationen zur Bild-erzeugung (unabhängig davon, ob sie von lokalen Programmen oder den Anwendungen des Terminal-servers selbst stammen) direkt an den X-Server auf dem Arbeitsplatz-PC übergeben und erst dort in die eigentliche Bildausgabe gewandelt. Bedingt durch das notwendige, vergleichsweise funktionsreiche Protokoll ergibt sich keine effektive Trennung der netzwerktechnisch gekoppelten Systemumgebungen. Je „mächtiger“ das verwendete Protokoll ist, desto mehr Angriffsvarianten sind denkbar.

### 1.2 X-Server bei TightGate™-Pro

Bei TightGate™-Pro ist der X-Server serverseitig und nicht auf dem Arbeitsplatz-PC integriert und bewirkt eine wesentlich weitergehende Trennung der Systemumgebungen. Die Kommunikation erfolgt über das funktionsspezifische und damit anderweitig maximal eingeschränkte VNC-Protokoll. Es werden vom ReCoBS-Server TightGate™-Pro zum Arbeitsplatz-PC (Klient) die abschließend aufbereiteten Grafikinformatoren (ähnlich eines Videodatenstroms) übergeben, die nachfolgend nur noch zur Anzeige gelangen. Darüber hinaus läuft der X-Server des ReCoB-Systems TightGate™-Pro nicht mit Administrationsrechten. Stattdessen wird eine eigene Berechtigungssphäre mit speziell definierten und anhand einer Positivliste stark beschränkten Rechten geschaffen. Ein Angriff auf den X-Server kann auf diese Weise den Arbeitsplatzrechner im internen Netzwerk aus technischer Sicht kaum noch erreichen.

## 2 Angriffsszenarien

Ein Angreifer muss zunächst den Terminalserver überwinden, um Zugriff auf den X-Server des Arbeitsplatz-PCs zu bekommen. Der X-Server in klassischen Systemen läuft mit Administrationsrechten auf dem Arbeitsplatz-PC.

### 2.1 Erste Stufe: Terminalserver

Um den Terminalserver zu überwinden, muss ein Angreifer im einfachsten Fall lediglich eine Sicherheitslücke in einer installierten Applikation nutzen, um sich Systemrechte (root-Berechtigung) zu verschaffen. Da der Terminalserver Internetdienste für die Rechner im internen Netzwerk bereitstellen soll, gerät in diesem Zusammenhang vor allem der Internetbrowser ins Blickfeld. Als Standardsoftware ist dieser aufgrund hoher Funktionalität (insbesondere durch Multimediaerweiterungen, Flash- und Viewer-Plug-ins) ein lohnendes Ziel für Angriffe. Anleitungen, wie solche Lücken auszunutzen sind („Exploits“), lassen sich leicht eruieren und sind teilweise mit einfachen Mitteln nachvollziehbar.

Die Gefahr eines erfolgreichen Angriffs auf einen Webbrowser für ein klassisches Computersystem ist recht hoch. Wird eine beliebige Komponente des Browsers kompromittiert, erlangt der Angreifer häufig die Berechtigungen des am System angemeldeten Benutzers. Ein klassischer Terminalserver ist hinsichtlich eines Angriffs über den Browser keine nennenswerte Hürde<sup>2</sup>. Zugleich ist dessen Absicherung („Härtung“) bei gängigen Betriebssystemen technisch nur eingeschränkt möglich.

### 2.2 Zweite Stufe: X-Server

Hat ein Angreifer die Rechte eines Benutzers auf dem Terminalserver erlangt, kann er zur zweiten Stufe des Angriffs übergehen. Er muss nun eine Sicherheitslücke des X-Servers auf dem Arbeitsplatzrechner ausnutzen, um Vollzugriff zu erhalten.

Günstig für den Angreifer ist, dass der X-Server im klassischen System mit Administrationsrechten läuft. Ein erfolgreicher Angriff auf den X-Server ist fast immer gleichbedeutend mit der Erlangung des Administratorstatus' auf dem Arbeitsplatz-PC. Eine solche Attacke fällt leicht: Fortlaufend werden Security-Bulletins herausgegeben, die teils gravierende Sicherheitslücken detailliert beschreiben.

Verfügt ein Angreifer über administrativen Zugriff auf einen Arbeitsplatzrechner, so kann er unter der Kennung eines jeden Benutzers dieses Arbeitsplatzes auf alle zur Verfügung stehenden Ressourcen des gesamten Netzwerks zugreifen und Daten ausspähen, manipulieren oder stehlen.

## 3 Sicherheit durch professionelle ReCoB-Systeme

Das ReCoB-System TightGate™-Pro ist konzeptionell so gestaltet, dass die Sicherheit der Arbeitsplatzrechner im internen Netzwerk nicht von der eingesetzten Standardsoftware auf einem Terminalserver abhängt. TightGate™-Pro arbeitet im Gegensatz zu klassischen Maßnahmen als vorgeschaltetes Schutzsystem. Es sorgt einerseits mit einer physikalischen Trennung internetgebundener Applikationen von internen Systemkomponenten präventiv für eine sichere Übertragung in das interne Netzwerk. Übergriffe aus dem Internet auf das interne Netzwerk und die darin befindlichen Rechner sind technisch so gut wie ausgeschlossen. Andererseits schützt sich TightGate™-Pro autoaktiv vor Manipulationen der eigenen Systemumgebung durch das feingranulare Berechtigungssystem RSBAC<sup>3</sup> in Verbindung mit umfassender Betriebssystemhärtung nach dem aktuellen Stand der IT-Sicherheitstechnik.

<sup>2</sup> Zur ausführlichen Darstellung dieses Zusammenhangs siehe auch <http://www.m-privacy.de/unternehmen/kompetenzen/rsbac2/>

<sup>3</sup> RSBAC = Rule Set Based Access Control. Siehe auch [www.rsbac.org](http://www.rsbac.org)

Folgende Schutzmechanismen sind im ReCoB-System TightGate™-Pro implementiert:

1. Tatsächliche Trennung des X-Servers vom Arbeitsplatz-PC, verbunden mit Beschränkung der Rechte des X-Servers. Ein erfolgreicher Angriff über den X-Server kann bei TightGate™-Pro in sehr seltenen Fällen Auswirkungen auf die Benutzerumgebung auf dem ReCoBS haben, jedoch niemals auf den Arbeitsplatz-PC.
2. Der X-Server von TightGate™-Pro arbeitet ohne Administrationsrechte. Die Berechtigungssphäre des X-Servers erlaubt weder die Verwaltung des Systems noch direkten Zugriff auf die Arbeitsplatzrechner im internen Netzwerk.
3. Alle Applikationen auf TightGate™-Pro sind in jeweils eigenen Berechtigungssphären vollständig isoliert. Durch Kapselung der einzelnen Programme wird es für einen Angreifer nahezu unmöglich, die Kontrolle über das vorgeschaltete Schutzsystem zu übernehmen. Zusätzlich wird bei TightGate™-Pro die Verbindung zur Übermittlung der Bildschirmausgabe nur vom Arbeitsplatzrechner zum ReCoB-Server aufgebaut. Der umgekehrte Verbindungsweg ist im Gegensatz zur klassischen Terminalserver-Topologie nicht möglich und kann demzufolge auch nicht zweckentfremdet werden.

## 4 Terminalserver mit Eigenmitteln

In der Praxis sind leistungsfähige, sichere und benutzerfreundliche ReCoB-Systeme implementierungstechnisch eine anspruchsvolle Aufgabe. Sie eignen sich nicht als firmeninternes Entwicklungsprojekt für Systemadministratoren oder Netzwerkspezialisten.

Vorgeschaltete Schutzsysteme nach der ReCoB-Spezifikation des Bundesamtes für Sicherheit in der Informationstechnik (BSI) können mit konventionellen Entwicklungswerkzeugen und auf Basis frei verfügbarer Softwarekomponenten erstellt werden. Nachfolgender Überblick zeigt jedoch, dass es im Zuge der Projektierung eine Reihe technischer und organisatorischer Rahmenbedingungen zu beachten gilt. Die Beschaffung eines kommerziell verfügbaren und ausgereiften ReCoB-Systems wie TightGate™-Pro nebst situationsbezogener Dienstleistungspakete ist daher unter technischen wie auch betriebswirtschaftlichen Gesichtspunkten in der Regel die empfehlenswerte Alternative. Dies gilt insbesondere in Bereichen mit normalem bis hohem Schutzbedarf.

- Professionelle ReCoB-Systeme schützen die Rechner im internen Netzwerk präventiv und prinzipbedingt vor Angriffen aus dem Internet. Grundsätzlich sind sie unter Sicherheitsaspekten nicht zwingend auf häufige Aktualisierungen angewiesen, im Gegensatz zu konventionellen Terminalserversystemen oder lokal installierter Schutzsoftware. Veränderungen am vorgeschalteten Schutzsystem können jedoch erforderlich werden, um zusätzliche Funktionalität zu integrieren und mit den Sicherheitsmerkmalen in Einklang zu bringen. Angesichts der rasanten Entwicklung der Internettechnologie ist dies eine immerwährende Aufgabe, die im Rahmen eines Servicevertrags geregelt werden sollte. In Eigenregie von Firmen und Behörden erstellte Lösungen können unter diesem Aspekt erhebliche Entwicklungs- und Administrationskräfte binden, die für unternehmensspezifische Belange fehlen.
- Bedingt durch die vollständige Isolation der internetgebundenen Applikationen vom Arbeitsplatzrechner sind direkte Downloads (Datenabruf aus dem Internet) in das interne Netzwerk ausgeschlossen. Gleiches gilt für eine direkte Wiedergabe von multimedialen Inhalten aus dem Internet an den Arbeitsplatzcomputern. Derlei Aktivitäten sollten dennoch durch das ReCoB-System sicher ermöglicht und benutzerfreundlich gehandhabt werden. Andernfalls stehen Akzeptanz und Produktiveignung der betreffenden Infrastruktur infrage. Häufig bestehen auch anwenderseitig weitergehende Anforderungen hinsichtlich der Einrichtungen zum Dateitransfer. Spezielle Zugriffsregelungen, Dateitypfilterung oder ein umfassender Schutz vor unkontrolliertem Datenabfluss in das Internet („Data Leakage“) sind hierbei zu nennen. Sicherheitstechnisch beanstandungsfreie, funktionale und performante Lösungen bedingen bei unternehmensinterner Erstellung hohen Entwicklungs-, Konfigurations- und Qualitätssicherungsaufwand. Diese umfassenden Leistungen erbringen bei Beschaffung kommerziell verfügbarer Systeme spezialisierte Anbieter. Zugleich ist konstant hohes Schutzniveau auf dem Stand der Technik sichergestellt.

- Die Druckausgabe von Internetinhalten auf den Arbeitsplatzrechnern im internen Netzwerk muss sicherheitstechnisch und funktional einwandfrei implementiert sein, um den Schutz durch den ReCoB-Server nicht durch einen weiteren Angriffsvektor zu konterkarieren. Der TightGate™-Printserver bindet sowohl Netzwerkdrucker als auch an Arbeitsplatzrechnern angeschlossene Drucker ohne eigene Druckdatenaufbereitung (GDI-Drucker) sicher in das Gesamtsystem ein. Ressourcenaufwändige Eigenentwicklungen oder Konfigurationsarbeiten sind nicht notwendig.
- Im professionellen Umfeld eingesetzte IT-Systeme unterliegen jenseits ihrer technischen Funktionalität einer Reihe administrativer, organisatorischer und rechtlicher Rahmenbedingungen. Diese erschließen sich auch versierten Softwareentwicklern und Systemadministratoren nicht immer vollständig. Datenschutzrechtliche Vorgaben, Verpflichtung zur Speicherung und Aufbewahrung sowie vorgeschriebene Revisionssicherheit automatisch erstellter Protokolle sind Aspekte, die zusätzlich zum IT-Sicherheitsgedanken in die Entwicklung professionell genutzter ReCoB-Systeme einfließen müssen. Kommerziell verfügbare und zertifizierte Lösungen verbinden branchenübliche Funktionen mit der notwendigen Rechtssicherheit und entlasten technisches sowie administratives Personal firmenseitig von komplexen juristischen Fragestellungen.
- Betreiber komplex ausgebauter, umfangreicher Infrastrukturen setzen häufig auf IT-Eigenentwicklungen. Doch der Vorteil technologischer Autarkie wird durch den Nachteil hoher finanzieller und organisatorischer Aufwendungen neutralisiert, zumal ausgereifte Lösungen auf der Basis offener Standards und frei verfügbarer Softwarekomponenten erhältlich sind. Gut dokumentierte, benutzerfreundliche MOTS-Systeme<sup>4</sup> können fakultativ durch eigene Mitarbeiter oder externe Dienstleister gepflegt werden, ohne dass hoher Einarbeitungsaufwand oder gar temporäre Ausfälle zu befürchten wären. Selbst die anbieterunabhängige Weiterentwicklung solcher Lösungen ist leichter möglich als bei vollproprietären Lösungen oder mangelhaft dokumentierten Eigenentwicklungen.

Zusammenfassend spricht einiges dafür, die Implementierung von ReCoB-Systemen entsprechend spezialisierten Entwicklungsorganisationen zu überlassen und im Bedarfsfall auf deren Produkte zurückzugreifen. Sie gewährleisten maximal mögliches Schutzniveau, berücksichtigen juristische und organisatorische Aspekte des Anwenderunternehmens und bieten Investitionssicherheit auf einem technologisch rasch voranschreitenden Gebiet.

---

<sup>4</sup> MOTS = Modifiable, off-the-shelf; für anwenderspezifische Belange anpassbares, kommerziell verfügbares Serienprodukt.

## 5 Anhang

Nachfolgend sind Literaturhinweise (online und offline) im Hinblick auf die zugrundeliegende Technologie 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](http://www.m-privacy.de)
- Informationen zu TightGate™-Pro - [www.m-privacy.de/produkte/tightgate-pro](http://www.m-privacy.de/produkte/tightgate-pro)
- Informationen zur TightGate™-Technologie - [www.m-privacy.de/unternehmen/technologie](http://www.m-privacy.de/unternehmen/technologie)
- Informationen zu Rule Set Based Access Control (RSBAC) - [www.mprivacy.de/unternehmen/technologie/rsbac](http://www.mprivacy.de/unternehmen/technologie/rsbac)
- Homepage des RSBAC-Projekts - [www.rsbac.org](http://www.rsbac.org)

### 5.2 ReCoBS-Informationen des BSI

- **Kurzinformation ReCoBS** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [https://www.bsi.bund.de/clin\\_183/ContentBSI/Themen/Internet\\_Sicherheit/Gefahrenungen/Aktiv\\_einhalte/schutzmoeglichkeiten/recobs/kurzinformation.html](https://www.bsi.bund.de/clin_183/ContentBSI/Themen/Internet_Sicherheit/Gefahrenungen/Aktiv_einhalte/schutzmoeglichkeiten/recobs/kurzinformation.html)

## 6 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 Netzwerkimgebungen 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.