Titel	**Professionelle Angriffsprävention durch ReCoB-Systeme**	Schlüsselworte	ReCoBS, Remote Controlled Browser System, TightGate-Pro
Autor	Patrick Leibbrand / p.leibbrand@m-privacy.de	Datum	20.02.17
Redaktion	Patrick Leibbrand / p.leibbrand@m-privacy.de	Version	1.6

0 Ausgangssituation

Täglich werden Arbeitsplatzrechner in Unternehmen aller Art weltweit Ziel von Angriffen aus dem Internet - trotz Schutzmaßnahmen wie Firewalls, Virenscannern und Intrusion Detection Systems. Mit teils enormem administrativem Aufwand versucht man gerade in Bereichen mit erhöhtem Sicherheitsbedarf, ein notwendiges Schutzniveau aufrecht zu erhalten.

Dennoch attackieren Angreifer aus dem Internet gezielt Arbeitsplatzrechner im internen Netzwerk von Firmen und Behörden, oft unter Ausnutzung von Sicherheitslücken der darauf installierten Programme. Industriespionage, unberechtigter Abfluss sensibler Interna zu unbefugten Dritten und massive Beeinträchtigung des Systembetriebs durch Manipulation von Daten und Programmen sind die unmittelbaren Folgen.

1 Gefahr durch Internetzugriff

Moderne Computerarbeitsplätze erfordern in der Regel Internetzugriff. Viele Informationen sind in der gebotenen Aktualität und Detailliertheit nur online verfügbar, zudem werden Geschäftsstellen und Unternehmensbereiche immer stärker vernetzt. Die auf Arbeitsplatzrechnern installierten Anwenderprogramme greifen in vielen Fällen funktionsbedingt und weitgehend unbehelligt von konventionellen Schutzmaßnahmen auf das Internet zu. Dies betrifft vor allem Webbrowser, jedoch auch E-Mail-Programme, PDF-Viewer oder Multimediaapplikationen.

Sicherheitslücken werden mit zunehmender Funktionenvielfalt und Komplexität der Anwendungen wahrscheinlicher. Jede Schwachstelle birgt das Potenzial eines Angriffs auf den betreffenden Rechner und das interne Netzwerk mit unter Umständen weitreichenden Konsequenzen. Zugleich erlaubt es die Architektur gängiger Betriebssysteme nur eingeschränkt, Auswirkungen von Sicherheitslücken installierter Programme zu neutralisieren, etwa durch ein hinreichend engmaschiges Berechtigungskonzept. Daraus folgt, dass sich interne Rechner und Netzwerke mittels konventioneller Verfahren nicht effektiv gegen Angriffe aus dem Internet schützen lassen.

Kommt ein Verzicht auf den Internetzugriff aus organisatorischen Gründen nicht infrage, wird bisher in besonders schutzbedürftigen Infrastrukturen auf vollständig separate Netzwerke zurückgegriffen. Letztere erfordern jedoch organisatorisch und materiell einen hohen Aufwand.

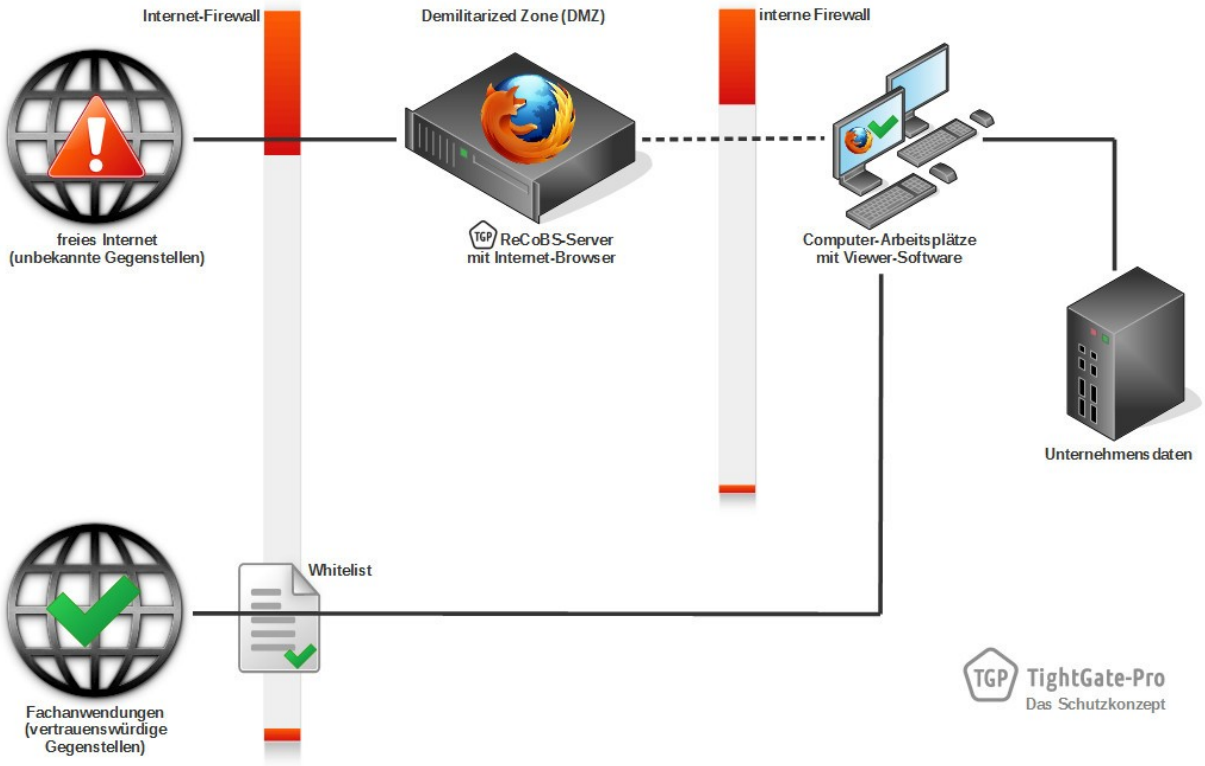
2 Angriffsprävention durch ReCoBS

Starken Schutz gegen Angriffe aus dem Internet über Sicherheitslücken in Anwenderprogrammen bieten sogenannte Remote-Controlled Browser Systems (ReCoBS). Auch hier handelt es sich de facto um eine physische Trennung der Netzwerke. Aufwand und Kosten sind jedoch im Vergleich zu bisherigen Ansätzen stark vermindert, und dies bei zugleich weitaus besserer Bedienbarkeit.

Ein ReCoBS isoliert potenziell gefährdete Applikationen vom Arbeitsplatzrechner bzw. dessen Netzwerk und verhindert damit Übergriffe aus dem Internet auf interne Daten und Systeme. Internetbrowser, E-Mail-Programm und weitere Anwendungen wie beispielsweise Adobe Reader werden dabei auf einem getrennten, dem Unternehmensnetzwerk vorgelagerten Schutzsystem ausgeführt. Lediglich die Bildschirmausgabe wird über ein funktionsspezifisches Protokoll an die Arbeitsplatzstation geliefert. Maus- sowie Tastatursignale werden in umgekehrter Richtung an das ReCoBS übermittelt. Internetge-

bundene Applikationen, allen voran der Webbrowser, können ferngesteuert ohne Gefährdung interner Infrastrukturen genutzt werden.

Neben dem Schutz vor einer Manipulation der Rechner und Netzwerkkomponenten wird auch unberechtigtem Datenabfluss in das Internet zuverlässig vorgebeugt. Moderne ReCoB-Systeme sind unkompliziert in professionelle Unternehmensinfrastrukturen integrierbar und entfalten ihre Schutzfunktion nach initialer Konfiguration transparent und technisch unabhängig von anderweitigen Maßnahmen.



Die Grafik illustriert den prinzipiellen Aufbau des Gesamtsystems. Die Arbeitsplatzrechner werden über einen Paketfilter, der nur die notwendigen Pakete des ReCoBS passieren lässt, mit der Bildschirmausgabe der Applikationen versorgt, die wiederum auf dem vorgelagerten Server ausgeführt werden. Das ReCoB-System wird vorzugsweise hinter der ersten Firewall des Firmennetzwerks in der Demilitarisierten Zone (DMZ) installiert. Fachanwendungen, die als vertrauenswürdige Gegenstellen fungieren, können nach Freigabe weiterhin mit dem lokal installierten Webbrowser genutzt werden.

3 Das ReCoB-System TightGate-Pro

Leistungsfähige ReCoB-Systeme, die den strengen Kriterien des ReCoBS-Schutzprofils des BSI (PP-0040) entsprechen, entwickelt die Berliner m-privacy GmbH mit den Serverprodukten der TightGate-Produktlinie. TightGate-Pro ermöglicht die Versorgung von Rechnerarbeitsplätzen mit vollfunktionalem Internetzugriff ohne Risiko eines An- oder Übergriffs auf das interne Netzwerk.

TightGate-Pro der m-privacy GmbH werden von Unternehmen sowie Bundes- und Landesbehörden zum Schutz ihrer Arbeitsplatzrechner und Netzwerke verwendet.

TightGate-Pro (CC) Ver. 1.4 ist nach Common Criteria EAL 3+ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-DSZ-CC-0589) zertifiziert.

Vorteile einer ReCoBS-Lösung mit TightGate-Pro:

- Zuverlässiger Schutz interner Infrastrukturen vor Angriffen aus dem Internet
- Verhinderung von Datenabfluss und Betriebsspionage
- Gefahrlose Internetnutzung, auch aktiver Inhalte
- Präventives Schutzkonzept statt reaktiver Filterung
- Geringer Wartungsaufwand, zentrale Verwaltung
- Hohe Benutzerfreundlichkeit
- Geringer Schulungsaufwand, hohe Nutzerakzeptanz

4 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.

4.1 Informationen im Internet

- Homepage der m-privacy GmbH – www.m-privacy.de
- Abstand schafft Sicherheit – TightGate-Pro im Detail (Videokanal)
- Boxen-Stopp – TightGate-Pro und Browser in The Box (Video)
- Informationen zu TightGate-Pro – www.m-privacy.de/tightgate-pro
- Homepage des RSBAC-Projekts – www.rsbac.org

4.2 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 Unternehmensprofil

Die m-privacy GmbH mit Sitz in Berlin entwickelt seit dem Jahr 2002 innovative Client-Server-Lösungen zur sicheren Internetanbindung von Computerarbeitsplätzen mittels Remote-Controlled Browser Systems (ReCoBS) auf der Basis der TightGate-Technik. 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 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.