Bundesamt
für Sicherheit in der
Informationstechnik

Remote-Controlled Browsers System (ReCoBS)

Grundlagen und Anforderungen

Version 2.0

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Remote-Controlled Browsers System (ReCoBS)

Grundlagen und Anforderungen

Version 2.0, Stand: 23.06.2006

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 1888-9582-0
E-Mail: bsi@bsi.bund.de
Internet: http://www.bsi.bund.de

© Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

Zusammenfassung

Unter einem Remote-Controlled Browsers System (ReCoBS) versteht das BSI den Web-Zugang mit Hilfe von speziell gesicherten Terminalserver-Systemen als modularen Bestandteil von Sicherheitsgateways. Dabei laufen die Browser nicht auf den Arbeitsplatz-PCs, sondern auf einem Terminalserver außerhalb des LAN und werden von den Arbeitsplätzen aus ferngesteuert. Im Browser auf dem Terminalserver werden alle Webinhalte ausgeführt, so dass bei Einhaltung entsprechender Sicherheitsanforderungen Aktive Inhalte nicht ins LAN gelangen können. Stattdessen werden grafische Informationen an die Arbeitsplätze übermittelt und dargestellt. Damit sind Ausführung und Darstellung Aktiver Inhalte voneinander getrennt.

Dieser Lösungsansatz ist eine unter verschiedenen Möglichkeiten zum Umgang mit Aktiven Inhalten auf der Anwenderseite. Im Vergleich zu anderen Ansätzen ermöglicht er sowohl eine bequeme als auch sichere Nutzung Aktiver Inhalte. Dabei ist „sicher“ in dem Sinne zu verstehen, dass die Daten im LAN geschützt werden, indem Aktive Inhalte die Arbeitsplatz-PCs und damit das LAN nicht erreichen. Die Aktiven Inhalte können auf dem Terminalserver technisch im gewünschten Funktionsumfang genutzt werden. Allerdings sollte auf einem Terminalserver mit WWW-Zugang keine Web-Nutzung mit sensitiven Inhalten erfolgen, da der Terminalserver den Gefahren Aktiver Inhalte weiterhin ausgesetzt ist. Aus diesem Grund ist ein ReCoB-System vor allem für die uneingeschränkte Recherche im WWW gedacht.

Die zur Realisierung eines ReCoB-Systems in Frage kommenden technischen Verfahren sollten nicht ohne geeignete Anpassungen als ReCoBS betrieben werden. Charakteristisch für ReCoBS sind gerade die aus Sicherheits- und Performanzgründen berücksichtigten technischen und organisatorischen Anforderungen. Im Vergleich zu anderen, weniger sicheren oder weniger bequemen Methoden für den Web-Zugang hat ReCoBS einen höheren Realisierungsaufwand. Daher richtet sich der Ansatz eher an Institutionen als an Privatanwender.

1 Ausgangslage, Problemstellung

Zur Gestaltung von Webseiten werden zunehmend Aktive Inhalte eingesetzt. Dabei handelt es sich um Programmcode, der zusammen mit dem HTML-Quellcode einer Webseite geladen und ohne Rückfragen auf dem Rechner des Web-Nutzers ausgeführt wird. Beispiele für Aktive Inhalte sind JavaScript, ActiveX-Controls, Flash-Dateien oder Java-Applets.

Aktive Inhalte dienen dem Zweck, anspruchsvolle Designvorstellungen und Interaktionsmöglichkeiten auf bequeme Weise zu realisieren, ohne dabei große Server- und Netzlasten zu erzeugen. Der Nachteil liegt in der Gefahr, zusammen mit dem HTML-Code auch Schaden verursachenden Code zu laden, der ohne weitere Barrieren oder Kontrollen ausgeführt wird. Die Gefahr besteht vor allem bei Webseiten aus nicht vertrauenswürdigen Netzen wie dem Internet. Dass es sich dabei nicht nur um eine theoretische Gefahr handelt, belegen zahlreiche dokumentierte Angriffe.

Am besten begegnet man dieser Gefahr durch Maßnahmen auf Seiten der Anbieter von Web-Inhalten. In der Regel kann auf Aktive Inhalte verzichtet werden, da sich die geforderte Funktionalität durch weniger gefährliche Techniken nahezu gleichwertig realisieren lässt. Für die Anbieterseite hätte der Verzicht auf Aktive Inhalte neben der Sicherheit ihrer Kunden auch den Vorteil, diejenigen Anwender zu erreichen, die Aktive Inhalte unterbinden. Entsprechende Appelle an die Anbieter verhallen aus unterschiedlichen Gründen dennoch meist unbeachtet.

Auf der Anwenderseite begegnet man dem Problem heutzutage entweder gar nicht oder dadurch, dass Aktive Inhalte herausgefiltert bzw. deaktiviert werden. Dies aber führt bei zunehmendem Einsatz von Aktiven Inhalten zur fortschreitenden Einschränkung der Web-Nutzung. Der sicherheitstechnisch ebenfalls empfohlene Einsatz dedizierter Internet-PCs (Stand-alone-PC) unterbricht den gewohnten Arbeitsablauf der Anwender und stößt daher auf geringe Akzeptanz.

Diese Ausgangslage führt zu dem grundlegenden Handlungsbedarf, dem Internet-Nutzer einerseits einen bequemen Web-Zugang in angemessenem Funktionsumfang zu ermöglichen und dabei andererseits ein möglichst hohes Sicherheitsniveau zu gewährleisten. Hierbei sollen insbesondere Anforderungen größerer Organisationseinheiten berücksichtigt werden.

2 Umgang mit Aktiven Inhalten auf der Anwenderseite

Unabhängig von den konkreten Anforderungen einzelner Anwender ist im Allgemeinen eine Lösung für den Web-Zugang gewünscht, die es erlaubt, Aktive Inhalte in vollem Funktionsumfang, bequem, sicher und kostengünstig zu nutzen. Dementsprechend ergeben sich vier relevante Beurteilungskriterien: Web-Funktionalität, Bedienungskomfort, Sicherheit und Realisierungsaufwand.

Erläuterung der vier Beurteilungskriterien:

a) Unter „Web-Funktionalität“ ist die technische Nutzbarkeit von Webseiten im Browser mit WWW-Zugang gemeint. Einerseits kann man grob davon ausgehen, dass bei einer Deaktivierung Aktiver Inhalte die Web-Funktionalität umso geringer ist, je mehr Aktive Inhalte von den Anbietern eingesetzt werden. Andererseits schränken Webseiten, die zwar Aktive

Inhalte einsetzen, sich aber auch bei deren Deaktivierung im Wesentlichen nutzen lassen (Webseiten der Risikoklasse 1[1]), die Web-Funktionalität nicht ein.

b) Mit „Bedienungskomfort“ ist die Bedienbarkeit des Browsers unabhängig von der Nutzbarkeit Aktiver Inhalte gemeint. Beispielsweise wird bewertet, ob man den Browser am eigenen Arbeitsplatz oder nur an einem speziellen „Surf-Arbeitsplatz“ nutzen kann. Aber auch die Nutzbarkeit der Druckfunktion oder der Zwischenablage kann eine Rolle spielen.

c) Bei der „Sicherheit“ geht es um das – durch Aktive Inhalte gefährdete – Sicherheitsniveau des zu schützenden Netzes und damit nicht um die Daten der Web-Anwendung. Die in Tabelle 1 verwendeten Sicherheitseinstufungen sollten nicht darüber hinwegtäuschen, dass die Methoden allenfalls für Netze geeignet sind, in denen unter Einhaltung entsprechender Sicherheitsmaßnahmen höchstens Informationen mit dem Geheimhaltungsgrad „VS – NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) verarbeitet werden dürfen. Als Ausnahme können bei Methoden mit separatem physischen „Surf-Netz“ in dem zu schützenden Netz unter Einhaltung weiterer Sicherheitsmaßnahmen auch Daten mit höherem Geheimhaltungsgrad verarbeitet werden. Eine weitergehende Beratung dazu bietet das BSI an.

d) Der „Realisierungsaufwand“ umfasst den materiellen und personellen Aufwand für Einrichtung und Unterhalt der jeweiligen Web-Zugangsmethode. Bei der Suche nach einer konkreten Lösung sollte allerdings auch der Aufwand im Schadensfall berücksichtigt werden. Er hängt vom individuellen Schutzbedarf ab und kann hier nicht pauschal berücksichtigt werden.

Die nachfolgende Übersicht vergleicht einige Methoden zum Umgang mit Aktiven Inhalten hinsichtlich der o. g. Kriterien. Es wird deutlich, dass

a) die gebräuchlichen Methoden zwar in einzelnen der ersten drei Kriterien gut abschneiden, aber nicht in allen dreien gleichzeitig,

b) sich einige Kriterien „gegenläufig“ verhalten, d.h. ein besonders gutes Abschneiden in einem oder mehreren Kriterien erfolgt stets zu Lasten eines anderen Kriteriums.

Die Einschätzungen hinsichtlich der Beurteilungskriterien können Tabelle 1 entnommen werden. Auf eine detaillierte Erläuterung der Einschätzungen wird hier verzichtet; die Übersicht soll lediglich Tendenzen verdeutlichen.

Nr.	Vorgehensweise, Methode	Einschätzung bzgl.			
		Web-Funktionalität	**Bedienungskomfort**	**Sicherheit**	**Realisierungsaufwand**
1	Ausführung aller Aktiven Inhalte im lokalen Browser, keine Schutzmaßnahmen.	uneingeschränkt	hoch	nicht vorhanden	minimal
2	Differenzierte Ausführung unterschiedlicher Aktiver Inhalte im lokalen	fast uneingeschränkt	hoch	sehr niedrig (variiert)	gering

[1] siehe E-Government-Handbuch des BSI, Modul „Sicherer Internet-Auftritt im E-Government“, S. 43, http://www.bsi.bund.de/fachthem/egov/download/4_IntAuf.pdf

	Browser, z. B. ActiveX deaktiviert, JavaScript zugelassen; kritische Browser-Konfigurationsmöglichkeiten für normale Benutzer gesperrt.	(variiert)			
3	Aktive Inhalte nur von vertrauenswürdigen Webseiten zugelassen, abgestützt auf Zonenmodell, ausgeführt im lokalen Browser, kritische Browser-Konfigurationsmöglichkeiten für normale Benutzer gesperrt; Problem: Zonenmodell kann z. B. durch Cross-Site-Scripting ausgehebelt werden.	eingeschränkt	hoch	niedrig	gering
4	Speziell gekapselter Browser auf dem Arbeitsplatz-PC, Aktive Inhalte aktiviert. (Beispiele: Changeroot-Umgebung für Linux, IE-Controller der c't [2])	uneingeschränkt	mittel	mittel	gering – mittel
5	Browser auf dem Arbeitsplatz-PC, zentrale selektive Filterung am Sicherheitsgateway – entsprechend der Gefährlichkeit des Code (semantische Analyse Aktiver Inhalte). Funktionalität und Sicherheit variieren diametral je nach Güte der selektiven Filterung.	eingeschränkt (variiert)	hoch	mittel (variiert)	mittel
6	Browser auf dem Arbeitsplatz-PC, alle Aktiven Inhalte werden zentral herausgefiltert oder dezentral deaktiviert, kein weiterer Web-Zugang.	deutlich eingeschränkt	hoch	sehr hoch [3]	mittel
7	Live-System, das direkt von einem Speichermedium (z. B. von CD) gebootet wird. Festplattenzugriff wirksam unterbunden.	uneingeschränkt	niedrig – mittel	mittel – hoch	mittel
8	Browser auf dediziertem Internet-PC jeweils für eine Arbeitsgruppe (Stand-alone-PC), physische Trennung vom Hausnetz, Aktive Inhalte für Stand-alone-PC freigeschaltet. Ggf. in Kombination mit Nr. 6.	uneingeschränkt	niedrig	sehr hoch	mittel
9	Dedizierter Internet-PC an jedem Arbeitsplatz, physische Trennung vom Hausnetz (d. h. zwei separate Netze und Rechner an jedem Arbeitsplatz), Aktive Inhalte im „physischen Surf-Netz“ freigeschaltet.	uneingeschränkt	mittel – hoch	sehr hoch	sehr hoch
10	Dedizierter Internet-PC an jedem Arbeitsplatz; Internet-PC und Arbeitsplatz-PC benutzen das gleiche physische Netz, Trennung der Datenströme z. B. durch ein VPN (virtuelles Surf-Netz).	uneingeschränkt	mittel – hoch	hoch	hoch – sehr hoch
11	Virtueller Rechner mit Internet-Browser auf jedem Arbeitsplatz-PC, Aktive Inhalte	unein-	hoch	hoch	sehr hoch

[2] c't-IE-Controller 2.0, www.heise.de/ct/ftp/projekte/iecontroller

[3] Diese Einschätzung bezieht sich nur auf die Gefahren Aktiver Inhalte und setzt voraus, dass eine vollständige Filterung gelingt.

	aktiviert. Arbeitsplatz-PC und virtueller Rechner benutzen das gleiche physische Netz, Trennung der Datenströme z. B. durch ein VPN (virtuelles Surf-Netz).	geschränkt			
12	ReCoBS: Web-Zugang mittels gesicherter Terminalserver (s. Abschnitt 3)	unein-geschränkt	hoch	sehr hoch	hoch

Tabelle 1: vergleichende Einschätzung der Methoden zum Umgang mit Aktiven Inhalte

Die Übersicht verdeutlicht, dass es eine Vielzahl von Methoden zum Umgang mit Aktiven Inhalten gibt. Aus sicherheitstechnischer Sicht sind nur wenige empfehlenswert. Welche Methode am besten geeignet ist, richtet sich nach den konkreten Anforderungen des jeweiligen Bedarfsträgers.

3 Lösungsansatz ReCoB-System

3.1 Funktionsweise

Ein Lösungsansatz für den Umgang mit Aktiven Inhalten auf der Anwenderseite besteht darin, die Ausführung und die Darstellung Aktiver Inhalte voneinander zu trennen, indem sie auf verschiedenen Rechnern realisiert werden. Hierzu wird der Web-Browser auf einem Terminalserver betrieben, der sich außerhalb der internen gesicherten Umgebung befindet (z. B. in der demilitarisierten Zone, DMZ). Die in den HTML-Quellcode eingebetteten und mit Hilfe von HTTP übertragenen Aktiven Inhalte werden im Browser auf dem Terminalserver ausgeführt; d. h. die ursprünglich im Code enthaltenen Informationen werden in grafische und akustische Informationen umgewandelt. Vom Terminalserver zu den Arbeitsplatzrechnern werden dann ausschließlich diese grafischen und akustischen Informationen mit Hilfe eines speziellen Terminalserver-Protokolls übertragen und am Arbeitsplatz-PC des Anwenders von einem entsprechenden Client dargestellt. Das Terminalserver-Protokoll gewährleistet darüber hinaus die Übertragung von Tastatureingaben und Mausbewegungen in umgekehrter Richtung, so dass die Browser von den Arbeitsplätzen aus ferngesteuert werden können.

Ein solches System wird im Folgenden **Remote-Controlled Browsers System (ReCoBS)** genannt. Ein ReCoB-System setzt sich im Wesentlichen aus „ReCoBS-Server“ und „ReCoBS-Clients“ zusammen. An die Stelle eines einzelnen ReCoBS-Servers kann natürlich auch ein Verbund von Servern treten, ggf. ergänzt um weitere Systeme, wie Load-Balancer, Verzeichnis-Server oder Log-Host (vgl. Topologie, Abschnitt 6).

Das Grundprinzip bei einem ReCoB-System besteht in dem Bruch der Informationsverarbeitung, bei dem die im HTML-Code (inkl. Aktiven Inhalten) enthaltenen Informationen in grafische Informationen umgewandelt werden. Der Sicherheitsgewinn für das LAN beruht im Wesentlichen auf diesem Bruch: Aufgrund der Trennung zwischen Ausführung und Darstellung Aktiver Inhalte erreichen nur die grafischen Informationen des Terminalservers die Arbeitsplatz-PCs und nicht die wesentlich gefährlicheren Aktiven Inhalte.

Charakteristisch für ReCoBS ist die gesamte Sicherheitskonzeption, bestehend aus diesem Grundprinzip und den flankierenden Maßnahmen zur Absicherung des Grundprinzips. Hierfür gibt es zwei „Linien der Verteidigung“: zum einen den Schutz des

ReCoBS-Servers gegenüber dem Internet und zum anderen den Schutz des Hausnetzes gegenüber einem eventuell kompromittierten ReCoBS-Server (vgl. Sicherheitskonzeption, Abschnitt 5).

Ähnliche Systeme, bei denen aus Sicherheitsgründen ein Bruch in der Informationsverarbeitung erfolgt, werden auch „grafische Firewall“ (engl. „graphical firewall“) genannt. Dieser Begriff soll hier aus zweierlei Gründen nicht verwendet werden: Zum einen ist ReCoBS modularer Bestandteil eines Sicherheitsgateways und dient der sicheren Behandlung von Aktiven Inhalten beim Surfen im Web. Es ist keine eigenständige Firewall. Zum anderen wird der Begriff „grafische Firewall“ auch für grafische Tools zur Firewall-Administration verwendet.

3.2 ReCoBS versus Terminalserver

Das grundlegende technische Prinzip eines ReCoB-Systems ist der indirekte Web-Zugang mit Hilfe von Terminalservern. Die Terminalserver-Technik wird seit Jahrzehnten gut beherrscht, und es gibt eine Fülle von kommerziellen und frei verfügbaren Produkten in diesem Bereich (vgl. potenzielle technische Systeme, Abschnitt 7). Dennoch lässt sich die Bereitstellung eines ReCoB-Systems nicht auf die Beschaffung und Integration eines beliebigen Terminalserver-Systems reduzieren. Ein ReCoB-System unterscheidet sich in drei wesentlichen Punkten von einem Terminalserver-System, wie es üblicherweise verwendet wird:

1. Die Performanz-Anforderungen sind bei ReCoBS in der Regel höher, da das Browsen eine grafisch anspruchsvolle Anwendung ist (z. B. durch Animationen) und der ReCoBS-Server (bzw. -Cluster) für alle Anwender einer Institution nur in der DMZ sinnvoll platziert werden kann.
2. Der ReCoBS-Server befindet sich im Vergleich zu den Clients in einem Netz mit niedrigerem Sicherheitsniveau. Üblicherweise werden Terminalserver in Netzen mit gleichem oder höherem Sicherheitsniveau betrieben. Aus diesem Grund können sie beispielsweise auch zur Administration der Clients verwendet werden, was bei ReCoBS zu gefährlich wäre.
3. ReCoBS wurde unter Sicherheitsaspekten optimiert. Demgegenüber zielt die Entwicklung von Terminalserver-Systemen eher auf die Erhöhung des Funktionsumfangs. Die Funktionalität üblicher Terminalserver-Protokolle (und auch der Client-Software) wurde mehr und mehr ausgedehnt, wodurch deren Missbrauchspotenzial gestiegen ist.

Dementsprechend sollte kein Terminalserver-System „von der Stange“ gewählt werden, um es unverändert als ReCoBS zu betreiben. Das ist vor allem auf Sicherheitsdefizite solcher Systeme zurückzuführen. Die ReCoBS-Sicherheitsanforderungen und -maßnahmen sind erforderlich, um eine hinreichende Absicherung typischer Einsatz-Szenarien zu gewährleisten. Die umfassende Sicherheitskonzeption ist charakteristisch für ReCoBS und unterscheidet es von einem normalen Terminalserver-System.

Die in Abschnitt 4 aufgeführten technischen Anforderungen an ReCoBS berücksichtigen die Unterschiede zu normalen Terminalserver-Systemen. Daher können sie auch als definierende Eigenschaften eines ReCoB-Systems interpretiert werden. Das gilt vor allem für die sicherheitstechnischen Anforderungen.

3.3 Vor- und Nachteile

ReCoBS erfüllt drei wesentliche Anforderungen an den Web-Zugang gleichzeitig:
Nutzung von Webseiten mit Aktiven Inhalten

- im gewünschten technischen Funktionsumfang
- bequem vom Arbeitsplatz aus und
- sicher für die Daten im LAN.

Der „gewünschte technische Funktionsumfang“ entspricht im Wesentlichen dem technisch möglichen Umfang. Ausgenommen sind jedoch einige besonders sicherheitskritische Funktionen, die mit Hilfe von ReCoBS auch technisch nicht nutzbar sein sollen. Dazu gehört etwa die automatische Softwareinstallation an den Arbeitsplätzen mit Hilfe Aktiver Inhalte.

Keine der verbreiteten Web-Zugangsmethoden erreicht in jedem der drei Kriterien Web-Funktionalität, Bedienungskomfort und Sicherheit ein so hohes Niveau wie ReCoBS. Die genannten Vorteile von ReCoBS erfordern einen gewissen Realisierungsaufwand. Web-Zugangsmethoden mit vergleichbaren Vorteilen dürften einen entsprechenden Aufwand voraussetzen. Bei den in Abschnitt 2 vorgestellten Methoden mit geringerem Realisierungsaufwand ist mindestens eines der Kriterien Web-Funktionalität, Bedienungskomfort oder Sicherheit wesentlich schwächer ausgeprägt als bei ReCoBS.

Aus betriebstechnischer Sicht kann es zu Performanz-Engpässen kommen, vor allem wenn das System viele bewegte Bilder verarbeiten soll. Ursache dafür ist die Informationsverarbeitung auf grafischer Ebene, die in der Regel mehr Ressourcen erfordert. Daher werden zahlreiche Anforderungen an die Ressourcenoptimierung gestellt, s. Abschnitt 4. Herausragendes Beispiel ist die Bandbreite; im ReCoBS-Backbone (s. Abb. 1, Abschnitt 6) kann je nach Einsatzbedingung eine Bandbreite im GBit/s-Bereich erforderlich sein. Zumindest beim ALG würden dadurch die Grenzen des zurzeit technisch Möglichen erreicht. Durch Optimierungsmaßnahmen reicht ggf. auch eine wesentlich geringere Bandbreite aus. Grundsätzlich gilt jedoch, dass sich mit hinreichend vielen bewegten Bildern (z. B. zahlreichen Videoströmen) und einer entsprechenden Anwenderzahl jedes ReCoBS „in die Knie zwingen“ lässt.

3.4 Grenzen von ReCoBS

ReCoBS schützt die Daten an den Arbeitsplätzen und damit auch im übrigen LAN vor den Gefahren Aktiver Inhalte. Nicht geschützt werden jedoch die beim Surfen mittels ReCoBS übertragenen Daten. Denn trotz zusätzlicher Sicherheitsmaßnahmen sind erfolgreiche Angriffe auf den ReCoBS-Server nicht auszuschließen, vor allem weil hier Aktive Inhalte ausgeführt werden. Solche Angriffe werden kurzzeitig in Kauf genommen („Opferrechner“). Das hat keine weitreichenden Folgen, solange sich auf dem ReCoBS-Server keine sensitiven Daten oder Anwendungen befinden. Es folgt allerdings, dass ReCoBS vor allem für die uneingeschränkte Recherche im WWW, nicht aber für die Nutzung sensitiver Web-Anwendungen gedacht ist (z. B. kein Zahlungsverkehr). Hierfür könnte ggf. ein dedizierter ReCoBS-Server eingesetzt werden, der nur mit vertrauenswürdigen Web-Servern kommunizieren darf; dabei sind weitere Sicherheitsmaßnahmen zu beachten.

Trotz des erheblichen Sicherheitsgewinns für das interne Netz gibt es natürlich auch bei ReCoBS ein verbleibendes Risiko. Kritisch wäre das Vordringen eines Angreifers ins LAN mit Hilfe von ReCoBS, nachdem der ReCoBS-Server übernommen wurde. Dieses Risiko ist abhängig vom Missbrauchspotenzial der grafischen Informationen und des verwendeten Terminalserver-Protokolls. Je kleiner der Funktionsumfang von Client-Software und Protokoll ist, umso leichter ist ein Missbrauchspotenzial zu beherrschen.

Das verbleibende Risiko ist bei Einhaltung der Sicherheitsanforderungen als vergleichsweise gering einzuschätzen (s. Abschnitt 5.12). In jedem Fall ist ein solches System zur Verarbeitung grafischer Daten wesentlich schwieriger für einen Angriff zu missbrauchen als Aktive Inhalte auf einem ungeschützten Browser am Arbeitsplatz-PC.

3.5 Empfehlungen

Ob ReCoBS die geeignete Lösung für den Web-Zugang ist, hängt von den konkreten Anforderungen auf der Anwenderseite ab. Sie sollten sich unter anderem aus folgenden Aspekten ergeben:

- Schutzbedarf der im internen Netz vorhandenen Daten
- Einsatzzweck
- technische Einsatzumgebung
- vorhandene Fachkompetenz
- personelle und materielle Ressourcen.

Da die Realisierung von ReCoBS einen gewissen Aufwand erfordert, richtet sich diese Lösung eher an Institutionen als an Privatanwender. Der Realisierungsaufwand kann unter anderem durch folgende Aspekte gerechtfertigt werden:

- Schutzbedarf der im internen Netz vorhandenen Daten
- zu erwartender Aufwand im Schadensfall
- Bedeutung der Web-Nutzung für die jeweilige Institution
- zunehmende Bedeutung des WWW als Einfallstor für Angreifer.

Auch wenn ReCoBS für hohen Schutzbedarf gedacht ist, sollte die Einführung eines solchen Systems nur bei solchen Netzen in Betracht gezogen werden, bei denen schon bisher auf die ein oder andere Art ein Internet-Zugang vertretbar war. Wird ein Netz, das bislang vollständig vom Internet getrennt war, ans Internet angeschlossen, kann auch ReCoBS nicht verhindern, dass das Sicherheitsniveau sinkt. Für Behörden gilt: In Netzen mit ReCoBS dürfen unter Einhaltung entsprechender Sicherheitsmaßnahmen allenfalls als VS-NfD eingestufte Informationen verarbeitet werden.

Für Netze, bei denen Aktive Inhalte aus unsicheren Quellen bis zu den Arbeitsplätzen gelangen, führt die Einführung von ReCoBS zu einem erheblichen Sicherheitsgewinn. Bei Netzen, die schon heute eine Web-Zugangsmethode auf hohem Sicherheitsniveau verwenden (vgl. Abschnitt 2), würde man ReCoBS eher aus Gründen der Web-Funktionalität oder Bedienbarkeit einführen. Hier wäre eine detaillierte Sicherheitsanalyse zur Abwägung erforderlich.

ReCoBS ist kein fertiges Produkt, sondern eine Konzeption für den Web-Zugang durch Anpassung entsprechender Standardprodukte. Die hier bereitgestellten Informationen sollten größere Institutionen oder IT-Systemhäuser (als Auftragnehmer) in die Lage versetzen, entsprechende Systeme zu realisieren. Das BSI plant, die Einführung von ReCoBS durch weitere Veröffentlichungen speziell zur Realisierung zu unterstützen.

4 Allgemeine technische Anforderungen

Die BSI-Anforderungen an ein ReCoB-System sind „allgemein“ in dem Sinne, dass sie nicht auf die Anforderungen eines speziellen Bedarfsträgers hin zugeschnitten sind. Vielmehr sollte ein am Markt etabliertes ReCoB-System die genannten Anforderungen erfüllen, um dann im Wesentlichen durch Konfiguration an den speziellen Bedarf einzelner Unternehmen oder Behörden angepasst werden zu können.

Die Anforderungen beziehen sich auf das Potenzial technischer Systeme und sind zunächst nicht zu verwechseln mit den Maßgaben einer Policy. Dementsprechend richten sich die Anforderungen zuerst an Hersteller und Entwickler. Selbstverständlich soll der Anforderungskatalog aber auch den IT-Verantwortlichen der Bedarfsträger als Vorlage dienen, um die konkreten Anforderungen der eigenen Institution zusammenzustellen bzw. zu ergänzen.

Die Anforderungen sind grob in betriebstechnische, anwendungstechnische und sicherheitstechnische untergliedert. Dabei sind die Grenzen fließend. Beispielsweise ist das Drucken zunächst eine anwendungstechnische Anforderung; bei einem ReCoB-System kommt der sicheren Implementierung des Druckens jedoch eine besondere Bedeutung zu, da der Druckauftrag über Netze mit unterschiedlichem Sicherheitsniveau hinweg bearbeitet werden muss.

Die folgende Tabelle gibt einen Überblick über alle Anforderungen. Sie werden im Anhang ausführlich erläutert.

Nr.	betriebstechnische Anforderungen
B 1	ReCoBS-Grundfunktionalität (vgl. Abschnitt 3.1)
B 2	hinreichende Performanz, unterstützt durch
B 2.1	Load-Balancing
B 2.2	zusätzliche Bandbreite und Bandbreitenoptimierung
B 2.3	automatisches Ausloggen bei Nicht-Nutzung
B 2.4	lastabhängige Ressourcenbereitstellung für die einzelnen Anwender
B 3	Variabilität, insbesondere durch
B 3.1	Skalierbarkeit
B 3.2	Plattformunabhängigkeit
B 3.3	Einsatzmöglichkeit für unterschiedliche Browser
B 3.4	flexible Konfigurierbarkeit der Anwenderaktivitäten auf dem Server
B 3.5	konzeptionelle Offenheit auch für andere Anwendungen
B 4	einheitliche, zentrale, umfassende und einfache Administration, ergänzt durch
B 4.1	Server-Fernadministration
B 4.2	zentrales Client-Management
B 4.3	Backup-Möglichkeit

Nr.	anwendungstechnische Anforderungen
(A 0)	Anwender-Grundanforderung (Verhalten wie lokale Anwendung erwünscht)
A 1	Drucken
A 2	Download
A 3	Webseiten-Speicherung
A 4	Copy and Paste
A 5	individuelle Benutzereinstellungen (z. B. Bookmarks, Oberflächengestaltung)
A 6	komfortable Bedienung
A 7	Sound-Unterstützung

Nr.	sicherheitstechnische Anforderungen
S 1	Serversicherheit, insbesondere
S 1.1	regelmäßiger System-Integritätscheck
S 1.2	regelmäßiger Reboot mit System-Bereinigung
S 1.3	Vertraulichkeit auf dem Server (u. a. durch Kapselung der Anwenderumgebungen)
S 1.4	sichere Fernadministration
S 1.5	keine kritischen Systemvorgänge auf dem Server (z. B. darf die Systemfunktionalität keine Verbindungsaufbauten von außen nach innen voraussetzen)
S 1.6	restriktiver Umgang mit ausführbaren Programmen
S 1.7	System-Härtung
S 1.8	Einschränkung der Anwender-Funktionen je nach konkretem Bedarf der Institution
S 1.9	Logging
S 2	Clientsicherheit, dazu gehört
S 2.1	Vertraulichkeit auf dem Client durch Deaktivierung typischer Funktionen von Terminalserver-Clients
S 2.2	Minimalität der Client-Software
S 3	Verbindungssicherheit zwischen Client und Server, insbesondere
S 3.1	Integrität (Authentizität)
S 3.2	Vertraulichkeit
S 3.3	minimales Terminalserver-Protokoll
S 4	sichere Implementierung aller Anforderungen unter Berücksichtigung ihres Zusammenwirkens
S 5	Umfeldsicherung durch das Sicherheitsgateway, insbesondere durch
S 5.1	Sicherheitsproxy für das Terminalserver-Protokoll, zumindest generischer Proxy
S 5.2	Web-Sicherheitsproxy
S 5.3	Paketfilter; innerer und äußerer Paketfilter des P-A-P-Aufbaus (ggf. ergänzt durch dedizierten Paketfilter zur Abgrenzung des Servers vom Sicherheitsgateway)

Tabelle 2: betriebs- (B), anwendungs- (A) und sicherheitstechnische (S) ReCoBS-Anforderungen

Ausführliche Erläuterung der

- betriebstechnischen Anforderungen: s. Anhang A
- anwendungstechnischen Anforderungen: s. Anhang B
- sicherheitstechnischen Anforderungen: s. Anhang C.

Das Zusammenwirken der sicherheitstechnischen Eigenschaften eines ReCoB-Systems wird im folgenden Abschnitt erläutert.

5 Elemente einer Sicherheitskonzeption

Auf Grund der unterschiedlichen Anforderungen der einzelnen Bedarfsträger kann hier kein einheitliches, allumfassendes Sicherheitskonzept für ein ReCoB-System aufgestellt werden. Stattdessen werden im Folgenden einige konzeptionelle Elemente zusammengestellt, mit denen sich jeder Bedarfsträger auseinandersetzen sollte.

5.1 Wesentliches Problem der Web-Nutzung

Neben dem aus dem Web angeforderten erwünschten Code kann Schaden verursachender Code – vor allem in Form von Aktiven Inhalten – heruntergeladen werden, der ohne weitere Kontrollen oder Barrieren auf dem Browser am Arbeitsplatz ausgeführt wird. Von dort kann das gesamte LAN angegriffen werden. Das Problem ist umso größer, je offener das externe Netz ist – am größten beim Internet.

5.2 Ziel

Vertraulichkeit, Integrität und Verfügbarkeit der Daten im LAN sollen gewährleistet werden.

5.3 Zweck eines ReCoB-Systems

Ein ReCoB-System soll die Nutzung von Webseiten mit Aktiven Inhalten

- im gewünschten technischen Funktionsumfang
- bequem vom Arbeitsplatz-PC aus und
- sicher (im Sinne der Zielsetzung)

gewährleisten.

ReCoBS dient im Rahmen eines Sicherheitsgateways dem Schutz von Netzen mit erhöhtem Sicherheitsbedarf (maximal VS-NfD). Durch den Einsatz von ReCoBS sollen die Daten innerhalb des LAN, nicht aber die bei der Nutzung von ReCoBS übertragenen Daten geschützt werden. Daher ist ReCoBS vor allem für die uneingeschränkte Recherche im WWW, nicht aber für die Nutzung sensitiver Web-Anwendungen gedacht.

5.4 Konzeptioneller Lösungsansatz und Funktionsweise

s. Abschnitt 3

5.5 Anforderungen für den konkreten Bedarf

s. Abschnitt 4. (Eine Anpassung an den konkreten Bedarf ist erforderlich.)

5.6 Kern der Sicherheitskonzeption

Die Sicherheit eines ReCoB-Systems beruht im Wesentlichen auf der Trennung zwischen Ausführung und Darstellung der Web-Inhalte. Dadurch gelangen anstelle von Aktiven Inhalten nur grafische Informationen ins LAN. Deren Missbrauchspotenzial ist wesentlich kleiner einzuschätzen als das der Aktiven Inhalte.

Damit die ReCoBS-Grundidee – also der Bruch in der Informationsverarbeitung – nicht umgangen wird, sind flankierende Schutzmaßnahmen erforderlich. Sie werden in den folgenden Abschnitten erläutert.

5.7 ReCoBS-Server als „Opferrechner“

Durch ReCoBS wird die Problematik der Aktiven Inhalte vom Arbeitsplatz-PC zu einem zentralen Server außerhalb des LAN verlagert. Der Sicherheitsgewinn liegt im Schutz des LAN. Prinzip bedingt verbleibt folgendes Problem: Da auf dem ReCoBS-Server Aktive Inhalte ausgeführt werden, können erfolgreiche Angriffe auf den Server nicht ausgeschlossen werden. Die Wahrscheinlichkeit für einen erfolgreichen Angriff ist wegen zusätzlicher Sicherheitsmaßnahmen zum Schutz des Servers kleiner im Vergleich zu der Situation, Aktive Inhalte bis zu den Arbeitsplätzen gelangen zu lassen. Der Server wird also nicht leichtfertig aufgegeben. Grundsätzlich muss jedoch davon ausgegangen werden, dass der ReCoBS-Server kompromittiert wird. Technische Maßnahmen sollen gewährleisten, dass eine Kompromittierung nur kurzzeitig in Kauf zu nehmen ist (s. 5.9). Damit eine solche vorübergehende „Opferung“ keine gravierenden Auswirkungen hat, müssen zwei wesentliche Voraussetzungen erfüllt sein:

1. Ein Angreifer auf dem ReCoBS-Server kann von dort nicht (oder nur mit unverhältnismäßig großem Aufwand) ins LAN vordringen (vgl. 5.6 in Verbindung mit 5.10).
2. Ein Angreifer findet auf dem ReCoBS-Server keine sensitiven Daten. Das wird durch die folgende organisatorische Grundregel gewährleistet.

5.8 Organisatorische Grundregel

Auf dem ReCoBS-Server, über den der WWW-Zugang ermöglicht wird, dürfen keinerlei sensitive Anwendungen betrieben oder sensitive Daten gespeichert werden. Beispielsweise sollte ReCoBS keinen Zugriff auf das **Intra**net erlauben.
Für die sensitiven Anwendungen einer Institution setzen die IT-Verantwortlichen diese Regel mit Hilfe der Gesamt-Sicherheitskonzeption durch. Sollte innerhalb einer Institution die private Nutzung von ReCoBS erlaubt sein, muss den Anwendern die Gefahr (z. B. fürs Online-Banking) verdeutlicht werden. Diese tragen das Risiko.
Für sensitive Web-Anwendungen kann ggf. ein dedizierter ReCoBS-Server eingesetzt werden, der nur mit vertrauenswürdigen Web-Servern kommunizieren darf. Dabei sind weitere Sicherheitsmaßnahmen zu beachten.

5.9 Schutz des ReCoBS-Servers gegenüber dem Internet („1. Verteidigungslinie“)

Das ReCoB-System ist Bestandteil des Sicherheitsgateway. Der ReCoBS-Server sollte in der demilitarisierten Zone platziert werden. Gegenüber dem Internet sollte er durch einen dynamischen Paketfilter und einen Web-Sicherheitsproxy (als Bestandteil des Application Level Gateways, ALG) geschützt werden. Der äußere Paketfilter soll gewährleisten, dass Verbindungsaufbauten

- nur von innen (ReCoBS-Server) nach außen (Internet) und
- nur für den für HTTP festgelegten Port erfolgen.

Der Web-Sicherheitsproxy soll die Einhaltung des HTTP-Protokolls gewährleisten.

Neben solchen, auf dedizierten Rechnern realisierten, Schutzmaßnahmen sind auf dem ReCoBS-Server weitere Maßnahmen erforderlich, die nachfolgend erläutert werden.

Der ReCoBS-Server soll gehärtet werden, d.h. alle Software, die nicht benötigt wird, soll nicht nur deaktiviert, sondern sogar deinstalliert werden. Das gilt insbesondere für die nicht erforderlichen Bestandteile des Betriebssystems und der Terminalserver-Software. Außerdem sollen alle Terminalserver-typischen Mechanismen, die das Ausspähen der regulären Benutzer unterstützen könnten, irreversibel deaktiviert werden – am besten, indem der Code entfernt wird. Dazu gehören Mechanismen, um das Fenster einer Sitzung auf mehreren Rechnern darzustellen (Spiegelung), wodurch bei üblichen Terminalserver-Anwendungen der Administrator beim Support unterstützt wird. Das Gleiche gilt für Client-seitige Mechanismen, mit denen Fenster (anderer Anwendungen) vom Server – aber auch von anderen Clients – aus ausgespäht werden könnten (z. B. sichere Konfiguration des X-Window-Systems).

Die folgenden Maßnahmen zum Schutz vor unberechtigtem Zugriff auf den Server werden nach unterschiedlichen „Nutzergruppen“ differenziert: Administratoren, reguläre Anwender, Hacker. Darin enthalten sind auch indirekte Zugriffsversuche mit Hilfe von Schadprogrammen.

Dem unberechtigten Zugriff durch Administratoren kann – wie üblich – durch organisatorische Maßnahmen begegnet werden, z. B. durch eine entsprechende Verpflichtung und die Kontrolle der Log-Dateien durch einen „Super-Administrator“.

Dem unberechtigten Zugriff durch einen regulären Benutzer soll im Wesentlichen durch folgende Maßnahmen begegnet werden:

- restriktive Rechtevergabe auf dem ReCoBS-Server
- Kapselung der Benutzerumgebungen (z. B. durch chroot-Umgebung oder durch unterschiedliche Verschlüsselung der Benutzerverzeichnisse).

Beim unberechtigten Zugriff durch Hacker sind wiederum zwei Fälle zu unterscheiden: Entweder erlangt der Hacker Root-Rechte oder nur die Rechte eines regulären ReCoBS-Anwenders, indem er dessen Browser und Benutzerumgebung kompromittiert (Weitere Fälle sind denkbar, in der Praxis dürften aber diese beiden Fälle entscheidend sein.). In dem zuletzt genannten Fall greifen die Maßnahmen, die schon reguläre Benutzer auf dem Server vom unberechtigten Zugriff abhielten. Die Kompromittierung des einzelnen Browsers und des einen(!) zugehörigen Benutzerbereichs wird Prinzip bedingt in Kauf genommen. Sie ist umso weniger gravierend, je weniger Rechte der reguläre Nutzer hat (z. B. Beschränkung auf die Speicherung der Browsereinstellungen und Bookmarks). Die Rechtevergabe sollte so restriktiv sein, dass die Kompromittierung mit Beendigung der Sitzung durch den regulären Benutzer ebenfalls beendet ist.

Für den Fall, dass der Hacker Root-Rechte auf dem ReCoBS-Server erlangt, sollen die in Abschnitt 5.10 genannten Schutzmaßnahmen den Übergriff aufs LAN verhindern.

Der Erkennung von unberechtigten Zugriffen auf den ReCoBS-Server dient das Logging auf einen dedizierten Log-Host. Darüber hinaus sollen die (regulären) Anwender ein ReCoB-System nicht zur Anonymisierung illegaler Web-Aktivitäten missbrauchen können. Die Log-Daten müssen eine Zuordnung zwischen den einzelnen Web-Anfragen des ReCoBS-Servers und den Anwendern erlauben. Solche Daten fallen auf dem Web-Proxy an, sofern sich die Browser dort anmelden müssen.

Sollte es zu einem erfolgreichen Angriff auf den ReCoBS-Server kommen, sollen die folgenden Maßnahmen zumindest gewährleisten, dass eine Kompromittierung allenfalls kurzzeitig in Kauf genommen werden muss:
Die Bereiche des ReCoBS-Servers, in denen keine Benutzereinstellungen oder -dateien gespeichert werden (statische Bereiche), sollen regelmäßig einem Integritätscheck unterzogen werden. Nicht vorhandene Integrität löst Alarm aus. Zusätzlich soll der Server regelmäßig von einem schreibgeschützten Medium aus gebootet und das System bereinigt werden. Für die dynamischen Bereiche, in denen Benutzereinstellungen und Bookmarks gespeichert werden, ist ein geeignetes Backup vorzusehen. Die in den meisten Fällen erforderliche Einrichtung eines Verbundes von ReCoBS-Servern unterstützt diese Maßnahmen, indem die statischen Bereiche auf den eigentlichen ReCoBS-Servern und die dynamischen auf einem Verzeichnis-Server realisiert werden (vgl. Topologie-Vorschläge, Abschnitt 6).

Die Nutzer sollten die Browser-Startseite nicht selbst wählen dürfen. Das kann durch Einschränkung des Browsers erfolgen. Zumindest soll beim regelmäßigen Reboot die Startseite auf eine harmlose Standardseite zurückgestellt werden. Auf diese Weise soll die dauerhafte Wahl einer Startseite verhindert werden, die

- große Server- und Netz-Ressourcen erfordert, z. B. weil sie bewegte Bilder enthält, oder
- einen Angriff auf den ReCoBS-Server ermöglicht, weil sie entsprechend präpariert wurde.

Im zuletzt genannten Fall könnte die – mittels regelmäßigem Reboot – erreichte System-Bereinigung ebenso regelmäßig wieder unterlaufen werden, falls die Kompromittierung durch den Integritätscheck nicht erkannt wird.

5.10 Schutz des LAN gegenüber dem ReCoBS-Server („2. Verteidigungslinie“)

Der entscheidende Sicherheitsaspekt eines ReCoB-Systems – also der Bruch in der Informationsverarbeitung (vgl. 3 und 5.6) – verhindert einen direkten Angriff aufs LAN über die Web-Schnittstelle. Aktive Inhalte erreichen nicht die Arbeitsplatz-PCs im LAN, sondern nur eine Benutzerumgebung auf dem ReCoBS-Server. Einerseits verursachen sie dort keine relevanten Schäden, andererseits ist das weitere Vordringen ins LAN sehr schwierig (vgl. 5.12). Sollte der ReCoBS-Server kompromittiert werden, sollen die folgenden Maßnahmen das LAN schützen:

- Auf dem ReCoBS-Server werden keine relevanten Daten gespeichert. Darüber hinaus sind dort keine kritischen Systemvorgänge implementiert, die dem Angreifer Zugriff auf das LAN gewähren könnten.
- Es sind ausschließlich hochspezialisierte, funktional eingeschränkte ReCoBS-Clients und Terminalserver-Protokolle zu verwenden, die neben der Darstellung bzw. dem Transport grafischer Informationen (inkl. Tastatureingaben und Mausbewegungen) keine weiteren Funktionen bieten, die ein Angreifer missbrauchen könnte.
- Die Einhaltung des Terminalserver-Protokolls soll nach Möglichkeit durch einen Sicherheitsproxy auf dem ALG gewährleistet werden. Dieser kann darüber hinaus verwendet werden, um ein funktional umfangreiches Terminalserver-Protokoll in seiner Funktion einzuschränken. Falls kein Sicherheitsproxy verfügbar ist, soll zumindest ein generischer Proxy eingesetzt werden. Außerdem kann es dann – abhän-

gig vom Schutzbedarf – notwendig sein, den ReCoBS-Client auf dem Arbeitsplatz-PC zusätzlich zu kapseln.

- Der innere Paketfilter zwischen ReCoBS-Server und LAN wacht darüber, dass Verbindungsaufbauten
  - nur von innen (LAN) nach außen (ReCoBS-Server) und
  - nur für den vorgesehenen Port erfolgen.
- Der ReCoBS-Server sollte durch einen Paketfilter vom ALG abgegrenzt werden, da ein Paketfilter in der Regel weniger Angriffsfläche bietet als ein ALG.

Die in diesem Abschnitt bislang beschriebenen Sicherheitsmaßnahmen sind bei den sicherheitstechnischen Systemanforderungen in Abschnitt 4 berücksichtigt.

5.11 Standardsicherheitsmaßnahmen

Darüber hinaus sind Standardsicherheitsmaßnahmen entsprechend dem IT-Grundschutz umzusetzen, auf die hier nicht weiter eingegangen wird (z. B. Zugangsschutz, Aktualität der Patches usw.).

5.12 Risikobewertung und verbleibendes Risiko

Zunächst sei noch einmal daran erinnert, dass Netze, die aus Sicherheitsgründen physisch vom Internet getrennt sind, nicht über ReCoBS mit dem Internet verbunden werden sollten. Andernfalls käme es zu einer deutlichen Absenkung des Sicherheitsniveaus. Die Risikobewertung von ReCoBS erfolgt daher im Vergleich zu zwei verbreiteten Fällen, den Web-Zugang für Arbeitsplatz-PC (APC) einzurichten.

1. Fall: Aktive Inhalte freigeschaltet
   Aktive Inhalte gelangen ins LAN bis zu den APC und werden dort ausgeführt. Das entspricht zunächst der Methode 1 in der Tabelle aus Abschnitt 2. Die Aussagen zu diesem Fall gelten jedoch mit leichten Abstrichen auch für die Methoden 2 bis 5.
   In diesem Fall würde die Einführung von ReCoBS zu einem Sicherheitsgewinn führen – und zwar um Größenordnungen; denn Aktive Inhalte im LAN verursachen alle bei ReCoBS verbleibenden Risiken und darüber hinaus zusätzliche, wesentlich größere Gefährdungen.
2. Fall: Aktive Inhalte gesperrt
   An den APC besteht Web-Zugang, allerdings ohne Aktive Inhalte. Sie werden am Sicherheitsgateway herausgefiltert. Stattdessen werden sie an Stand-alone-PCs genutzt, die physisch vom übrigen LAN getrennt sind (s. Methoden 6 und 8 der Tabelle in Abschnitt 2).
   Dieser Fall und ReCoBS bewegen sich auf einem vergleichbaren Sicherheitsniveau. Einerseits kann die Sicherheit etwas geschwächt werden, wenn man im Fall 2 ReCoBS einführt. Das zeigt die nachfolgende Betrachtung des verbleibenden Risikos bei ReCoBS. Andererseits kann es auch Situationen geben, in denen ReCoBS eine höhere Sicherheit bietet als die bloße Sperrung Aktiver Inhalte,
   - zum einen weil man in der Praxis nicht ganz sicher sein kann, ob die Filterung Aktiver Inhalte vollständig erfolgt und
   - zum anderen weil ReCoBS auch vor anderen Gefährdungen als Aktiven Inhalten schützt (Bsp.: WMF-Schwachstelle, CVE-2006-0020).

Auf Grund des vergleichbaren Sicherheitsniveaus würde man im zweiten Fall ReCoBS wegen des Bedienungskomforts bzw. der Web-Funktionalität einführen und nicht aus Sicherheitsgründen.

Während das Sicherheitsniveau bei freigeschalteten Aktiven Inhalten sehr niedrig ist, ist es sowohl im Fall gesperrter Aktiver Inhalte als auch bei ReCoBS sehr hoch. Der geringe Unterschied zwischen den Sicherheitsniveaus bei gesperrten Aktiven Inhalten und bei ReCoBS erfordert die genauere Betrachtung des verbleibenden Risikos bei ReCoBS.
Bei diesen Überlegungen sollte zusätzlich berücksichtigt werden, dass sich die Anwender bei einem unbequemen Web-Zugang möglicherweise eigene Wege schaffen, die dann die Sicherheit des LAN erheblich gefährden können.

Bei den verbleibenden Risiken eines ReCoB-Systems wird zwischen zwei Bereichen unterschieden:

1. Risiken, die bestehen, ohne dass ein Angreifer Zugriff auf den ReCoBS-Server erlangt hat:
   Ein ReCoB-System schützt beispielsweise nicht vor Web-Spoofing, DNS-Spoofing oder Cross-Site-Scripting.
   Bezüglich solcher Risiken sind die Sperrung Aktiver Inhalte und ReCoBS gleich sicher. Solche Risiken treten in gleicher Häufigkeit auch bei allen anderen Web-Zugangsmethoden auf – dann aber u. U. mit viel weitgehenderen Folgen.
2. Risiken, die bestehen, nachdem ein Angreifer Zugriff auf den ReCoBS-Server erlangt hat:
   Diese Risiken sind entscheidend für eine Abwägung zwischen ReCoBS und der Sperrung Aktiver Inhalte.

   a) Zunächst stellt sich die Frage nach dem Risiko für einen erfolgreichen Angriff auf den ReCoBS-Server. Dieses Risiko besteht, vor allem weil Aktive Inhalte auf dem ReCoBS-Server ausgeführt werden. Die unter 5.9 beschriebenen Maßnahmen sollen das Risiko minimieren.
      Angriffe mit Hilfe Aktiver Inhalte erreichen bei ReCoBS zunächst nur die Benutzerumgebung auf dem ReCoBS-Server. Schon wegen der Minimalitätsforderung ist die Erfolgswahrscheinlichkeit kleiner als bei Arbeitsplatz-PCs im Falle freigeschalteter Aktiver Inhalte. APC sind in der Regel das Gegenteil eines Minimalsystems. Die Kapselung der Benutzerumgebung ist die nächste, relativ hohe Hürde zur Übernahme des Servers. Dabei verringern laufende Integritätschecks die Wahrscheinlichkeit, unentdeckt zu bleiben.
      Solche Maßnahmen lassen sich Netzwerk-weit auf Client-Systemen nur schwer umsetzen. Insgesamt ist daher die Wahrscheinlichkeit für eine Übernahme des ReCoBS-Servers wesentlich kleiner als für die Übernahme eines beliebigen der APC bei freigeschalteten Aktiven Inhalten.
      (Anmerkung: Der erfolgreiche Angriff auf einen[!] APC im Falle freigeschalteter Aktiver Inhalte kann das entscheidende Ereignis für einen Angriff auf das LAN sein. Vor diesem Hintergrund wird das Single-Point-of-Failure-Risiko des ReCoBS-Servers [z. B. kurzzeitiger Ausfall des Web-Zugangs] bewusst in Kauf genommen. Es ist das kleinere Übel im Vergleich zum Risiko eines erfolgreichen LAN-Angriffs bei freigeschalteten Aktiven Inhalten. Mehr noch: Bei ReCoBS ermöglicht gerade die Konzentration der Web-Aktivitäten an diesem „Single Point“ die wirksame Kontrolle Aktiver Inhalte.)

Im Vergleich zu der Situation gesperrter Aktiver Inhalte kann die Wahrscheinlichkeit für einen erfolgreichen Angriff auf den ReCoBS-Server – je nach Anzahl und Absicherung der Stand-alone-PCs – sogar kleiner sein als die Wahrscheinlichkeit für einen erfolgreichen Angriff auf einen beliebigen der Stand-alone-PCs. Allerdings würde ein Angriff auf einen Stand-alone-PC das LAN weniger gefährden.

b) Ein Angreifer, dem die Übernahme des ReCoBS-Servers gelungen ist, kann Schaden beispielsweise folgender Art anrichten. Gefährdung der

- Integrität: Ein Angreifer kann angeforderte Webseiten fälschen und den regulären ReCoBS-Anwendern unterschieben. Diese Gefahr besteht ohnehin, ReCoBS bietet hier nur eine zusätzliche Möglichkeit.
- Authentizität: Ein Angreifer kann den WWW-Zugang für seine Zwecke missbrauchen – etwa um die eigene Identität zu verschleiern. Das ist relativ unwahrscheinlich, da es im Internet nicht nur wesentlich schlechter gesicherte Server als den ReCoBS-Server gibt, sondern sogar die Anonymisierung als Dienstleistung. Unter Umständen könnte es aber auch Absicht des Angreifers sein, die Institution durch missbräuchliche Web-Nutzung zu diskreditieren.
- Vertraulichkeit: Ein Angreifer kann jeglichen Datenverkehr ausspähen, der auf dem ReCoBS-Server anfällt, z. B. das Surf-Verhalten. Falls die Authentisierung auf dem ReCoBS-Server auf Passwörtern beruht, sollten sie sich daher signifikant von anderen Passwörtern unterscheiden.
  Bei Einhaltung der Organisatorischen Grundregel (s. 5.8) sollte kein relevanter Schaden entstehen.
- Verfügbarkeit: Ein Angreifer kann den Web-Zugang einschränken oder sogar verhindern. Letzteres würde allerdings sofort bemerkt werden, so dass entsprechende Gegenmaßnahmen ergriffen werden könnten. Zur Einschränkung würde beispielsweise auch die Installation von Dialern gehören. Dies wird u. U. nicht sofort entdeckt, was im Falle einer Standleitung oder Flatrate unbedeutend ist. Andernfalls wären Dialerschutzmaßnahmen außerhalb des ReCoBS-Servers erforderlich.

Solche Schäden werden bei ReCoBS kurzzeitig in Kauf genommen. Eine Kompromittierung sollte

- möglichst beim nächsten automatischen Integritätscheck erkannt (und danach behoben) werden,
- spätestens beim nächsten automatischen Reboot beseitigt sein. (Die Schwachstelle, die die Kompromittierung ermöglichte, ist dann allerdings noch nicht beseitigt.)

c) Über diese in Kauf zu nehmenden Risiken hinaus stellt sich die Frage nach dem Risiko für einen erfolgreichen Angriff auf die APC bzw. das LAN, nachdem der ReCoBS-Server übernommen worden ist. Die unter 5.10 beschriebenen Maßnahmen sollen dieses Risiko minimieren.
Hier sollte man zwei Fälle unterscheiden: Angriffe unter Ausnutzung des Terminalserver-Dienstes und Angriffe mit Hilfe sonstiger Dienste. Die Wahrscheinlichkeit für erfolgreiche Angriffe mit Hilfe sonstiger Dienste ist nicht höher als

bei Netzen mit physischer Anbindung zum Internet ohne ReCoBS. Es kommt auf die sorgfältige Konfiguration des Sicherheitsgateways an. Dem ReCoBS-Server dürfen keine sonstigen Dienste auf dem entsprechenden Interface angeboten werden. Erfolgreiche Angriffe auf die APC mit Hilfe des Terminalserver-Protokolls und der ReCoBS-Clients sind theoretisch denkbar. Solche Angriffe könnten ernsthafte Schäden verursachen, z. B. indem die Tastatureingaben anderer Anwendungen über ReCoBS ausgelesen werden. Dabei kommt der sorgfältigen Konfiguration von Clients, Paketfiltern und des ALG besondere Bedeutung zu. Bei Einhaltung der in den Abschnitten 4 und 5 beschriebenen Anforderungen und Maßnahmen sind solche Angriffe bislang nicht bekannt geworden.
Wie bereits erläutert sind derartige Angriffe umso unwahrscheinlicher, je geringer der Funktionsumfang des ReCoBS-Clients und des Terminalserver-Protokolls ist.

6 Topologie

Die nachfolgenden Diagramme zeigen zwei Topologie-Vorschläge für ein ReCoB-System.

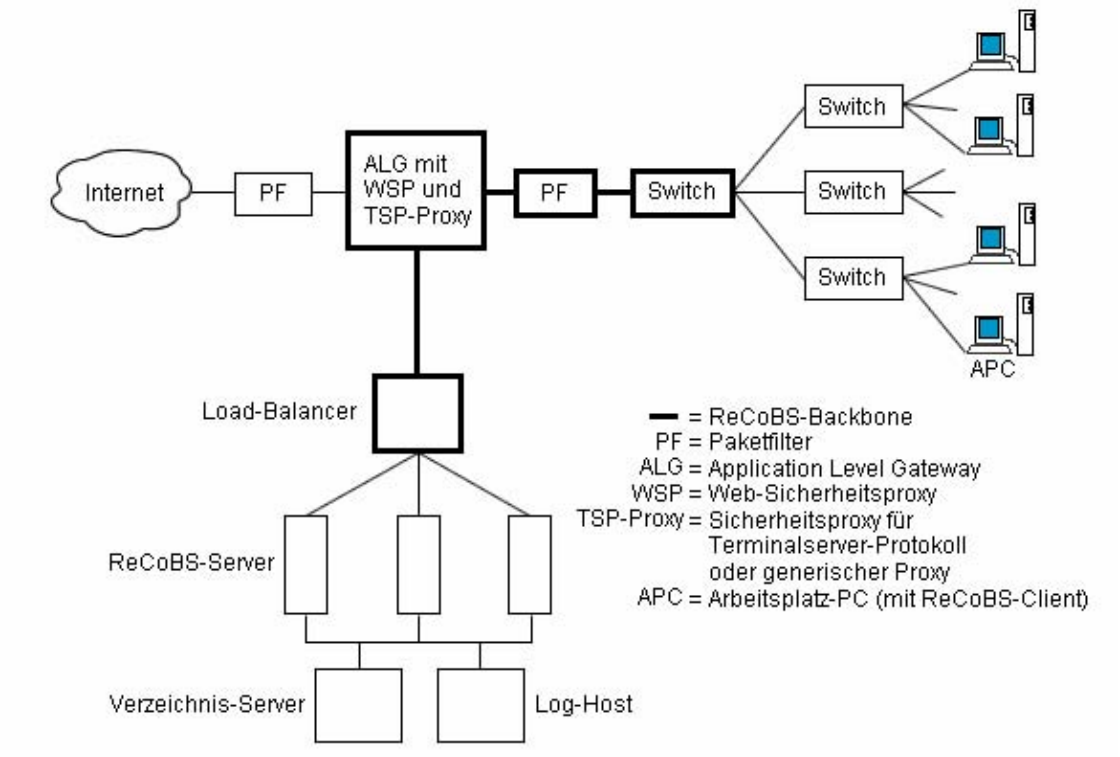

Abbildung 1: Topologie-Vorschlag 1 für ReCoBS, Anbindung des ReCoBS-Clusters am ALG

Dargestellt ist ein Sicherheitsgateway im empfehlenswerten P-A-P-Aufbau[4]. Das Sicherheitsgateway verbindet das vollständig geswitchte LAN mit dem Internet. Der ReCoBS-Verbund besteht aus dem Load-Balancer, den eigentlichen ReCoBS-Servern sowie Verzeichnis-Server und Log-Host. Der Verbund ist modularer Bestandteil des Sicherheitsgateways und befindet sich in einer DMZ, wobei der Load-Balancer an einem eigenen Interface des ALG angeschlossen ist. Im ReCoBS-Backbone (zwischen Load-Balancer und erstem Switch im LAN) kann eine Bandbreite im GBit/s-Bereich erforderlich sein. Zumindest beim ALG werden dadurch die Grenzen des zurzeit technisch Möglichen erreicht.

[4] P-A-P, d.h. Paketfilter – ALG – Paketfilter, siehe z. B. Bundesamt für Sicherheit in der Informationstechnik, „Konzeption von Sicherheitsgateways“, Bundesanzeiger-Verlag, 2005

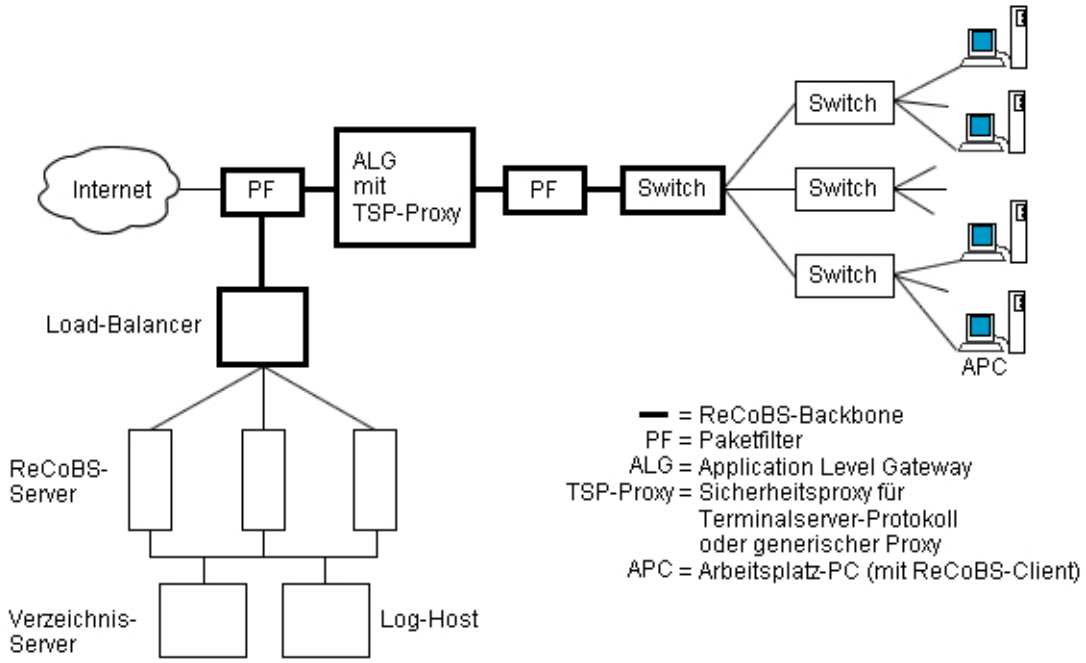

Abbildung 2: Topologie-Vorschlag 2 für ReCoBS, Anbindung des ReCoBS-Clusters am äußeren Paketfilter

Der zweite Vorschlag unterscheidet sich vom ersten durch die Anbindung des ReCoBS-Verbundes an den äußeren Paketfilter und durch das Fehlen des Web-Sicherheitsproxys.

Der Vorschlag hat gegenüber dem ersten folgende Vorteile:

- Ohne Web-Sicherheitsproxy wird das ALG hinsichtlich Performanz entlastet. Auch wenn der Web-Verkehr relativ zum Terminalserver-Verkehr klein ist, würde das ALG deutlich entlastet, da der Betrieb des Web-Proxys eine Vielzahl von Ressourcen verbrauchenden Prozess-Starts und -Stops erfordert.
- Bei Übernahme des ReCoBS-Verbundes durch einen Angreifer wird der Angriff auf das LAN erschwert,
  - da der benachbarte Paketfilter weniger Angriffsfläche bietet als das ALG (Die Praxis zeigt, dass ein ALG anfälliger für Fehlkonfiguration ist als ein Paketfilter und daher u. U. mehr Dienste am ReCoBS-Interface anbietet als erforderlich.)
  - da insgesamt mehr Stationen überwunden werden müssten, um ins LAN zu gelangen.

Andererseits kann der fehlende Web-Sicherheitsproxy bei speziellen Angriffen zu einem Sicherheitsproblem werden. Der Angriff auf den ReCoBS-Verbund wird gegenüber Vorschlag 1 erleichtert. Würde man den HTTP-Verkehr bei Vorschlag 2 über einen Web-Sicherheitsproxy auf dem ALG leiten, wäre der Performanz-Vorteil verschwunden.

Die Nachteile beider Vorschläge lassen sich natürlich durch die Einführung weiterer Geräte kompensieren:

- Bei Vorschlag 1 könnte man einen zusätzlichen Paketfilter zwischen ALG und Load-Balancer platzieren.
- Bei Vorschlag 2 wäre ein dedizierter Web-Sicherheitsproxy zwischen äußerem Paketfilter und Load-Balancer denkbar.

Das würde aber auch Komplexität und Aufwand erhöhen, so dass eine sorgfältige Abwägung erforderlich ist.

7 Potenzielle Technologie

Die folgende Auflistung zeigt eine Auswahl von technischen Systemen, die nach entsprechender Weiterentwicklung und Anpassung möglicherweise als ReCoBS betrieben werden könnten:

Ansatz	Beschreibung
„klassischer“ Terminalserver mit Software-Client auf dem Arbeitsplatz-PC	Die „klassischen“ Terminalserver bilden als eigenständiges Softwarepaket einen Aufsatz auf das zu Grunde liegende Betriebssystem. Die grafischen Ausgaben des Betriebssystems werden vom Terminalserver so aufbereitet, dass sie mit den meist proprietären Protokollen zum Arbeitsplatz-Rechner übertragen und dort von einem Client (dediziert oder als Browser-Plug-In) dargestellt werden können. Die Anwendung kann auf dem Terminalserver – ggf. auch auf einem dedizierten Applikations-Server – betrieben werden. Beispiele: Windows Terminal Services (Remote Desktop Protocol, RDP) Citrix MetaFrame (Independent Computing Architecture, ICA) GraphOn GO-Global (Rapid X Protocol, RXP) Tarantella (Adaptive Internet Protocol, AIP) Alle in den Beispielen genannten Protokolle basieren auf TCP/IP.
X-Window-System	Die Funktionalität, Grafikinformationen nicht nur lokal zu verarbeiten, sondern Netzwerk-weit zur Verfügung zu stellen, ist in Form des X-Window-Systems integraler Bestandteil jeder UNIX- bzw. Linux-Distribution. Auf dem Client (Arbeitsplatz-PC) läuft der X-Server, der die grafischen Informationen von einem X-Client entgegennimmt und weiterverarbeitet. Zur Übertragung zwischen X-Server und X-Client wird das auf TCP/IP aufsetzende X11-Protokoll verwendet. Im Falle von ReCoBS wäre der Browser auf dem ReCoBS-Server der X-Client. X-Server stehen auch für andere Betriebssysteme zur Verfügung – insbesondere für Windows –, so dass eine Migration der Arbeitsplätze in den meisten Fällen nicht erforderlich wäre.
VNC	Virtual Network Computing (VNC) ist ein Verfahren zur grafischen Fernbedienung. Es stützt sich auf VNC-Server und -Viewer. Diese kommunizieren mit Hilfe des Remote Framebuffer Protocol (RFB), das sich in der Regel auf TCP/IP abstützt. Die Kommunikation erfolgt auf der Ebene des Grafikspeichers und ist daher prinzipiell auf allen Betriebssystemen anwendbar. VNC-Server und -Viewer sind sowohl für UNIX/Linux als auch für Windows erhältlich. Im Gegensatz zum X-Server läuft der VNC-Server auf dem Rechner, auf dem sich die Anwendung befindet (hier also auf dem ReCoBS-Server). Ein VNC-Server unter UNIX/Linux übernimmt zusätzlich die Aufgabe des X-

Ansatz	Beschreibung
	Servers. Der VNC-Viewer hätte die Rolle des ReCoBS-Clients.
virtuelle Rechner	Von einem „virtuellen Rechner“ spricht man, falls das Betriebssystem nicht unmittelbar die zu Grunde liegende Hardware steuert. Stattdessen simuliert eine spezielle Software diesem „Gast“-Betriebssystem die Hardware-Schnittstellen eines normalen PC. Die Simulationssoftware setzt ihrerseits auf dem „Host“-Betriebssystem auf, das die Hardware direkt steuert. Auf diese Weise können auf einem (physischen) Rechner mehrere virtuelle Rechner realisiert werden. Ein solches System könnte als ReCoBS-Server dienen, indem die Browser auf den virtuellen Maschinen betrieben werden. Die Ausgaben der virtuellen Rechner werden mit Hilfe eines Terminalserver-Protokolls als virtuelle Konsolen auf die Arbeitsplatz-PCs übertragen. Die Rechte der Anwender auf den virtuellen Maschinen können je nach Anforderung des Bedarfsträgers deutlich eingeschränkt werden. Dieser Ansatz nimmt erhebliche Server-Ressourcen in Anspruch, da nicht nur einzelne Anwendungen, sondern ganze virtuelle Rechner auf dem Server betrieben werden. Er bietet aber u. U. ein höheres Sicherheitsniveau, da der Browser durch die virtuelle Maschine in natürlicher Weise gekapselt ist. Beispiel: VMware Server
Thin-Client-Technologie (kein eigenständiger Ansatz, sondern stets in Kombination mit der Server-Seite einer der o. g. Ansätze)	Im Gegensatz zu einem auch als „Fat Client“ bezeichneten PC versteht man unter einem „Thin Client“ einen Rechner ohne Festplatte und mit geringen Anforderungen an Prozessor und Arbeitsspeicher. Der Thin Client wird in der Regel von einer bootfähigen Netzwerkkarte aus gebootet. Anwendungen werden zentral bereitgestellt und ausgeführt – also im Gegensatz zu einem Netzwerk-Computer (NC) nicht vom zentralen Server geladen. Stattdessen übernimmt der Thin Client die Aufgabe eines Terminals, das die grafischen Ausgaben eines Terminalservers darstellt und Tastatur-/Mauseingaben an den Terminalserver übermittelt. Diese Funktionalität wird auch bei den oben beschriebenen Ansätzen verwendet; dort wird jedoch ein Fat Client eingesetzt, auf dem die entsprechenden Software-Clients laufen. Es gibt eine Reihe von Herstellern, die sich auf Thin-Client-Technologie spezialisiert haben. Im Open-Source-Bereich ist vor allem das Linux Terminal Server Project (LTSP) zu nennen. Die verschiedenen Thin-Client-Verfahren unterstützen mindestens eines der oben beschriebenen Terminalserver-Systeme. Zur Realisierung eines ReCoBS wäre der Einsatz von Thin Clients natürlich nur dann sinnvoll, falls bereits eine Thin-Client-Architektur existiert oder (aus anderen Gründen) neu eingerichtet wird. Andernfalls gäbe es an allen betroffenen Arbeitsplätzen zwei Rechner.

Wie bereits in Abschnitt 3 erläutert, unterscheidet sich ein ReCoB-System von einem Terminalserver-System, wie es üblicherweise verwendet wird. Dementsprechend ergab eine erste

Untersuchung des BSI, dass kein System „von der Stange“ gewählt werden sollte, um es unverändert als ReCoBS zu betreiben. Das ist vor allem auf Sicherheitsdefizite zurückzuführen. Die in den Abschnitten 4 und 5 behandelten sicherheitstechnischen Anforderungen und Maßnahmen sind erforderlich, um eine hinreichende Absicherung zu gewährleisten.

Anhang A: Betriebstechnische Anforderungen

Die betriebstechnischen Anforderungen beziehen sich auf die Installation und Administration eines ReCoB-Systems. Die damit verbundenen Funktionalitäten werden durch die Systemverantwortlichen gesteuert. Die Anwender sind davon mittelbar betroffen. Deren unmittelbare Anforderungen sind bei den „anwendungstechnischen Anforderungen“ zusammengefasst.

Die Erläuterungen sind teilweise mit Realisierungsvorschlägen und Beispielen für vergleichbare Problemstellungen versehen. Dadurch soll lediglich die Idee hinter einzelnen Anforderungen verdeutlicht werden. Die Vorschläge sind nicht verbindlich. Ziel sollten bessere Realisierungen sein.

Nr.	Anforderung	Beschreibung
B 1	ReCoBS-Grundfunktionalität	Der Web-Browser soll auf einem Terminalserver (ReCoBS-Server) außerhalb des LAN in einer gesicherten Umgebung (in der Regel die DMZ) betrieben werden. Es werden lediglich die grafischen (und ggf. akustischen) Informationen mit Hilfe eines Terminalserver-Protokolls an die Arbeitsplatz-PCs weitergeleitet und dort von einem ReCoBS-Client dargestellt. Tastatureingaben und Mausbewegungen werden in umgekehrter Richtung übertragen. Die Darstellung am ReCoBS-Client sollte so originalgetreu wie möglich sein. Dazu gehört beispielsweise eine ausreichende Farbtiefe.
B 2	Performanz	Die Akzeptanz eines ReCoB-Systems wird entscheidend von der Performanz des Systems im Vergleich zum lokal betriebenen Browser abhängen. In diesem Sinne soll das ReCoB-System ausreichend performant sein. Die Anforderung „Performanz“ wird in dieser Allgemeinheit aufgenommen, um alle Maßnahmen erfassen zu können, die die Performanz verbessern. Entscheidend – aber auch selbstverständlich – ist die angemessene Dimensionierung der einzusetzenden Hard- und Software – z. B. für die Terminalserver, den ReCoBS-Backbone (LAN-Anbindung des ReCoBS-Serververbundes) und die LAN-Topologie. Darüber hinaus wird nachfolgend eine Reihe einzelner Anforderungen gestellt (B 2.1 – B 2.4), die im Wesentlichen zum Ziel haben, die Performanz zu steigern. Da durch diese Einzelanforderungen keine Vollständigkeit erreicht wird, gibt es zusätzlich die globale Anforderung „Performanz“ an prominenter Stelle. Für 300 Anwender wird von folgenden Lastannahmen ausgegangen: • Alle 15 Sekunden wird eine Browser-Instanz auf dem ReCoBS-Server geöffnet. • Es sollen gleichzeitig bis zu 200 Browser-Instanzen geöffnet sein. • Pro Sekunde werden 4 Webseiten-Anfragen gestellt.
B 2.1	Load-	Zur Erhöhung der Performanz (und der Ausfallsicherheit) dürfte sich die Notwendigkeit ergeben, Server-Verbunde (Cluster) zu bilden, auf

Nr.	Anforderung	Beschreibung
	Balancing	denen ReCoBS-Server (Software) mit geeignetem Load-Balancing betrieben werden. Daher ist im Folgenden unter dem Begriff Terminalserver bzw. ReCoBS-Server stets auch ein solcher Cluster zu verstehen. Kriterien für ein anspruchsvolles Load-Balancing könnten z. B. sein: • CPU-Auslastung • Hauptspeicher-Auslastung • Festplatten-Zugriff • Anzahl der laufenden Anwendungen. Ein triviales Load-Balancing ist stets möglich. Denkbar sind z. B.: • Verteilung auf den Server-Verbund nach der Reihenfolge des Verbindungsaufbaus • feste Zuordnung der Anwender zu den Servern des Verbundes. Die Bildung eines Server-Verbundes ohne feste Zuordnung der Anwender auf die einzelnen Server erfordert die Verfügbarkeit der Anwenderprofile (z. B. Browsereinstellungen, Bookmarks etc.) auf allen Servern. Dabei könnten z. B. die folgenden Strategien verfolgt werden: • Bereithaltung aller Profile auf jedem Server mit entsprechendem Abgleich untereinander • Speicherung der Profile auf einem Verzeichnis-Server mit Verbindung zu allen ReCoBS-Servern. Aus sicherheitstechnischer Sicht darf dieser Verzeichnis-Server nicht mit dem zentralen Verzeichnis-Server des LAN identisch sein, da der ReCoBS-Server andernfalls verbindungsaufbauend auf letzteren zugreifen müsste (vgl. Anforderung „keine kritischen Systemvorgänge“).
B 2.2	zusätzliche Bandbreite	Die Bandbreite zur Übertragung der grafischen Informationen an die Arbeitsplätze soll so bemessen sein, dass auch kurze Filme und Animationen noch angemessen dargestellt werden können. Die zugehörigen Lastannahmen für typische Internet-Filme: 300 x 200 Pixel und 25 Bilder/sec. Es werden hier spezielle Probleme auftreten. Zum Beispiel stellen Animated Gifs in einer Endlosschleife für normale Browser kein Problem dar, bei einem ReCoB-System erzeugen sie hingegen erhebliche Netzlast. Das System sollte darüber hinaus „echte“ Videoströme angemessen behandeln können. Dabei ist klar, dass sich ein ReCoB-System mit hinreichend vielen bewegten Bildern stets „in die Knie“ zwingen lässt, so dass gewisse Obergrenzen akzeptiert werden müssen. Bevor eine (bandbreitensteigernde) Einschränkung der Darstellungsqualität (z. B. eine Reduktion der Farbtiefe) in Kauf genommen wird, sollen alle Möglichkeiten zur Bandbreitenoptimierung ausgeschöpft werden (z. B. Komprimierung, Codierung, Caching). Maßnahmen zur

Nr.	Anforderung	Beschreibung
		Komprimierung des Datenstroms können auf unterschiedlichen Ebenen der Protokollstruktur erfolgen. Die Behandlung „echter“ Videoströme erfolgt ggf. durch separate Verfahren.
B 2.3	automatisches Ausloggen	Ein Nutzer, der das System eine voreingestellte Zeit lang nicht benutzt hat, soll automatisch ausgeloggt und die zugehörige Browser-Instanz geschlossen werden können (Time-out). Das System sollte diese Zeit in Abhängigkeit von der Auslastung automatisch innerhalb gewisser Grenzen festlegen können. Zur Nutzung zählen auch (längere) Downloads und nicht nur Tastatur- und Mauseingaben.
B 2.4	lastabhängige Ressourcen-bereitstellung	Es soll möglich sein, die bereitgestellten System-Ressourcen (CPU, Hauptspeicher, Bandbreite, Anzahl der Browserinstanzen etc.) für den einzelnen Nutzer auf dem ReCoBS-Server in Abhängigkeit von den aktuellen Ressourcen-Anforderungen der übrigen Nutzer automatisiert einzuschränken. Ziel ist es, die gegenseitige Beeinträchtigung der eingeloggten Nutzer zu minimieren. Bezüglich dieser Anforderung sind auch spezielle Benutzerprofile denkbar, die mit unterschiedlicher Priorität behandelt werden. Vom Administrator fest eingestellte Werte werden nicht als optimale Lösung angesehen. Die Ressourcen-Zuweisung soll automatisiert erfolgen je nach Verfügbarkeit, die kontinuierlich (zumindest regelmäßig automatisch) gemessen wird.
B 3	Variabilität	Das ReCoB-System soll sich möglichst leicht an die unterschiedlichen Anforderungen verschiedener Bedarfsträger anpassen lassen. Durch diese allgemeine Anforderung sollen Hersteller und Entwickler aufgefordert werden, neben den im Anschluss aufgeführten Anforderungen B 3.1 – B 3.5 weitere zu identifizieren und zu realisieren, um die Einsatzmöglichkeiten zu erhöhen.
B 3.1	Skalierbarkeit	Das System muss leicht skalierbar sein, d.h. der Aufwand, um bis zu 1.500 Anwender zu versorgen, soll höchstens proportional zur Erhöhung der Anwenderzahl sein und sich im Wesentlichen auf die Ausweitung des Serververbundes beschränken. Darüber hinaus ist ein erhöhter Geräte-Einsatz (z. B. mehr Switche) hinnehmbar, eine neue Verkabelung nicht. Es wird ein sternförmiges Netz mit einer Bandbreite von 100 Mbit/s an den Arbeitsplatz-PC vorausgesetzt. Für den ReCoBS-Backbone (zwischen ReCoBS-Serververbund und erstem Switch im LAN) ist wahrscheinlich eine GBit/s-Verkabelung erforderlich. Ob eine solche Verkabelung auch zwischen der ersten und zweiten Switch-Ebene (zwischen ReCoBS-Servern und -Clients) erforderlich ist, hängt von der Gesamtzahl der Anwender ab.
B 3.2	Plattformun-abhängigkeit	ReCoBS-Server und -Clients sollen für möglichst viele Betriebssysteme zur Verfügung stehen – mindestens für Windows und Linux.

Nr.	Anforderung	Beschreibung
B 3.3	Browser-Vielfalt	Auf dem ReCoBS-Server sollen mehrere gängige Browser eingesetzt werden können, darunter möglichst viele der folgenden Menge: Internet Explorer, Netscape, Mozilla (Firefox), Opera, Konqueror. Alle Browser sollen Java-, JavaScript- und Flash-fähig sein. Welche Browser einsetzbar sind, ist vor allem vom verwendeten Betriebssystem auf dem ReCoBS-Server abhängig. Dieser Schwierigkeit kann man z. B. begegnen a) durch Software in Form von Emulatoren oder sogar virtuellen Maschinen, die den Betrieb von Anwendungen (hier: Browsern) ermöglichen, welche für ein anderes Betriebssystem gedacht sind, oder b) durch Hardware in Form einer Trennung der ReCoBS-Server-Plattform von der Anwendungs-Plattform mit logischer Integration verschiedener Anwendungs-Plattformen in das Gesamtsystem. Beide Wege bieten die Möglichkeit, a) den Browser unabhängig vom Betriebssystem des ReCoBS-Servers auswählen zu können; b) verschiedene Browser, die auf unterschiedlichen Plattformen laufen, nebeneinander innerhalb des gleichen ReCoB-Systems betreiben zu können. Die Softwarelösung zur Erhöhung der Browser-Vielfalt dürfte allerdings erhebliche Auswirkungen auf die Performanz haben.
B 3.4	flexible Konfigurierbarkeit	Das ReCoB-System soll so flexibel konfigurierbar sein, dass je nach Bedarf der Organisation • jedem Benutzer ein eigener Bereich auf dem Server-System zur Verfügung gestellt wird, in dem er ein eigenes Dateisystem einrichten kann und Installationsrechte für Programme des eigenen Gebrauchs erhält, oder • die Benutzer außer den „ReCoBS-Kernfunktionen“ keine weiteren Dienste auf dem Server in Anspruch nehmen können, d.h. den Benutzern bleibt jede Dateiablage und Installation mit Ausnahme der Browser-spezifischen Konfigurationen verwehrt, oder • eine Server-Konfiguration zwischen diesen beiden Extremen gewählt werden kann. Diese Funktionalität kann durch eine eigene Benutzer- und Rechteverwaltung des ReCoB-Systems oder aber durch das zugrunde liegende Betriebssystem realisiert werden. Am Beispiel dieser Anforderung wird noch einmal der Unterschied zwischen einer allgemeinen technischen Anforderung (im Sinne von Abschnitt 4) und einer (wahrscheinlichen) Policy deutlich. In den meisten Fällen wird die hier genannte Flexibilität auf dem ReCoBS-

Nr.	Anforderung	Beschreibung
		Server aus Sicherheitsgründen nicht erwünscht sein. Sie kann jedoch nicht für alle denkbaren Einsatz-Szenarien ausgeschlossen werden.
B 3.5	konzeptionelle Offenheit	Das ReCoB-System soll konzeptionell offen sein für andere Anwendungen neben dem Browser, z. B. für E-Mail-Programme. Diese Anforderung wird vorsorglich gestellt. Grundsätzlich gilt aber: Wird ReCoBS für den WWW-Zugang eingesetzt, so dürfen auf diesem Server keine sensitiven Anwendungen betrieben werden.
B 4	Administration/Betrieb	Das ReCoB-System wird in der Regel aus verschiedenen Hard- und Software-Komponenten unterschiedlicher Hersteller aufgebaut sein. Die Administration des Gesamtsystems soll • einheitlich (integriert) • zentral (für Server-Verbund und Clients) • umfassend und • einfach durchgeführt werden können. Zur Vollständigkeit der erforderlichen Maßnahmen wird die Anforderung in dieser Allgemeinheit aufgenommen. Insbesondere sollen die nachfolgenden Einzelanforderungen berücksichtigt werden.
B 4.1	Server-Fernadministration	Für den ReCoBS-Server soll die Möglichkeit zur Fernadministration bestehen. Zunächst ist hier an die Fernadministration direkt aus dem angeschlossenen LAN bzw. der entsprechenden DMZ gedacht. Auch die Fern-Administration soll umfassend, einheitlich und einfach erfolgen.
B 4.2	zentrales Client-Management	Das ReCoB-System soll ein zentrales Management der Clients unterstützen. Aus sicherheitstechnischen Gründen darf das Management der Clients nicht vom ReCoBS-Server aus erfolgen. Der Client-Rechner soll so konfiguriert werden können, dass er Updates nur von einem bestimmten Server entgegennimmt. Das darf nicht der ReCoBS-Server sein.
B 4.3	Backup	Das ReCoB-System soll Backups unterstützen. Einfachheit und Geschwindigkeit kommen dabei besondere Bedeutung zu. Möglicherweise ist es zweckmäßiger, anstelle einer ausgefeilten Backup-Strategie regelmäßig eine automatische Spiegelung der Server-Inhalte auf ein geeignetes Speichermedium vorzunehmen. Es stellt sich insbesondere die Frage, inwieweit das Backup im laufenden Betrieb oder nur bei angehaltenem System vorgenommen werden kann. Die Backup-Funktionalität muss nicht durch das ReCoB-System selbst, sondern kann auch durch das Betriebssystem oder andere Backup-Tools zur Verfügung gestellt werden.

Anhang B: Anwendungstechnische Anforderungen

Die anwendungstechnischen Anforderungen fassen die unmittelbaren Anforderungen der Anwender an ein ReCoB-System zusammen. Dabei handelt es sich um Funktionen, die direkt von den Anwendern bedient werden.

Mittelbare Anforderungen der Anwender (z. B. eine hinreichende Performanz) sind bei den betriebstechnischen Anforderungen aufgeführt.

Die Erläuterungen sind teilweise mit Realisierungsvorschlägen und Beispielen für vergleichbare Problemstellungen versehen. Dadurch soll lediglich die Idee hinter einzelnen Anforderungen verdeutlicht werden. Die Vorschläge sind nicht verbindlich. Ziel sollten bessere Realisierungen sein.

Nr.	Anforderung	Beschreibung
(A 0)	Anwender-Grundanforderung	Die Anwender erwarten von einem „Remote-Browser“, dass er sich wie ein lokaler Browser verhält. Zusammen mit dem herausragenden Aspekt der Sicherheit soll diese allgemeine Anforderung bei der Entwicklung eines ReCoB-Systems als Leitlinie dienen. Im Zweifelsfall hat allerdings die Sicherheit Vorrang, da einzig das angestrebte Sicherheitsniveau den vergleichsweise hohen Realisierungsaufwand für ein ReCoB-System rechtfertigt.
A 1	Drucken	Der Anwender soll Webseiten oder Teile davon ausdrucken können, wobei eine direkte Weiterleitung an den zuständigen Drucker ohne weiteres Zutun des Nutzers angestrebt werden soll (transparentes Drucken). Im Gegensatz zu klassischen Terminalserver-Implementierungen befindet sich der ReCoBS-Server im Vergleich zu den Clients in einem Netz mit niedrigerem Sicherheitsniveau. Daraus ergeben sich für das Drucken spezielle sicherheitstechnische Teilanforderungen, damit keine zusätzlichen Risiken entstehen: • Der ReCoBS-Server soll keine Verbindungen von außen nach innen aufbauen können – etwa um Druckaufträge ins LAN zu senden (vgl. Anforderung S 1.5). • Das Terminalserver-Protokoll und die ReCoBS-Clients sollen nicht zur Übertragung von Druckaufträgen verwendet werden können. Die Sicherheit bei ReCoBS beruht darauf, lediglich grafische Informationen mit möglichst funktionsarmen, d.h. schwierig anzugreifenden, Protokollen und Clients zu verarbeiten (vgl. Anforderung S 3.3). • Sicherheitsüberprüfungen der Druckaufträge sollen automatisiert durchgeführt werden können. Die abschließende Prüfung vor dem Eintritt ins LAN darf nicht auf dem ReCoBS-Server erfolgen (vgl. Anforderung S 1.5).

Nr.	Anforderung	Beschreibung
		Beispiele für eine sichere Implementierung des Druckens: 1. Zusammen mit dem Auftrag zum Drucken an den ReCoBS-Server wird ein Auftrag an einen Druckserver versandt, der eine Verbindung von innen nach außen zum ReCoBS-Server aufbaut, den Job abholt, auf Schadfunktionen prüft, in einen Druckjob wandelt und an den zuständigen Drucker weiterleitet. 2. Auf dem ReCoBS-Server wird der zu druckende Inhalt in ein PDF-Dokument, das keine Aktiven Inhalte enthält, konvertiert und dieses per E-Mail an den Anwender versandt. Die E-Mails werden vor dem Eintritt ins LAN an zentraler Stelle (außerhalb des ReCoBS-Servers, z. B. auf dem Sicherheitsgateway) auf Schadinhalte geprüft. Dadurch entstehen keine zusätzlichen Gefährdungen, sofern schon vorher E-Mails aus dem Internet intern verarbeitet worden sind. Entweder kann der Anwender nun über das Ausdrucken entscheiden, oder eine qualifizierte automatisierte Behandlung der so generierten Mails führt zum direkten Ausdruck auf dem zuständigen Drucker.
A 2	Download	Der Anwender soll die Möglichkeit haben, Dateien aus dem Internet herunterzuladen, um sie am Arbeitsplatz abspeichern zu können. Dabei soll eine Überprüfung auf Schadprogramme erfolgen. Der Vorgang soll für den Anwender transparent sein. Der Browser läuft auf dem ReCoBS-Server, so dass der Download bis zum Server wie gewohnt erfolgt. Entscheidende Bedeutung kommt dem automatischen Transfer der heruntergeladenen Datei zwischen ReCoBS-Server und Arbeitsplatz-PC zu. Insbesondere sind folgende sicherheitstechnische Teilanforderungen zu berücksichtigen: 1. Kein Verbindungsaufbau des ReCoBS-Servers von außen nach innen durch das Sicherheitsgateway (vgl. Anforderung S 1.5). 2. Insbesondere kein Zugriff des ReCoBS-Servers auf Laufwerke im LAN – etwa mit Hilfe von Drive Mapping bzw. Mounten. 3. Das Terminalserver-Protokoll (wie auch die Clients) sollte zum Dateitransfer nicht nur nicht verwendet werden, es sollte diese Funktion nicht bieten (vgl. Anforderung S 3.3). 4. Die – für die Sicherheit des LAN relevante – abschließende Prüfung auf Schadinhalte vor Eintritt einer Datei ins LAN darf nicht auf dem ReCoBS-Server erfolgen (vgl. Anforderung S 1.5). Darüber hinaus soll beachtet werden, dass Downloads umfangreich sein können. In diesem Fall wäre der Versand einer auf den ReCoBS-Server heruntergeladenen Datei per E-Mail an den ReCoBS-Anwender nicht der geeignete Weg. (Vgl. Realisierungsvorschlag 2 bei Anforderung A1.)
A 3	Webseiten-	Der Anwender soll die Möglichkeit haben, Webseiten am Arbeits-

Nr.	Anforderung	Beschreibung
	Speicherung	platz zu speichern, wobei eine automatisierte Konvertierung ins PDF-Format mit Auflistung der Links angestrebt werden sollte. Die Speicherung von Webseiten kann als eine spezielle Form des Downloads betrachtet werden, bei der der eigentliche Download (auf den ReCoBS-Server) bereits erfolgt ist, wenn sich der Anwender zur Speicherung am Arbeitsplatz entscheidet. Es gelten die gleichen sicherheitstechnischen Teilanforderungen für den Transfer zum Arbeitsplatz wie beim „normalen“ Download (vgl. A 2). Falls eine PDF-Konvertierung nicht erfolgen soll, ist eine Überprüfung auf Schadprogramme unerlässlich (vgl. A 2). Dieser Weg sollte jedoch die Ausnahme sein, da hierbei Aktive Inhalte ins LAN gelangen können. Außer dem vollständigen Herausfiltern Aktiver Inhalte gibt es keine wirksame und zuverlässige Methode, Aktive Inhalte auf Schadfunktionen zu prüfen. Gerade deshalb wird ein ReCoB-System benötigt. Falls die konkreten Anforderungen die Umwandlung einer HTML-Seite (oder ihrer Druckversion) ins PDF-Format zulassen, sollte die Umwandlung erfolgen, bevor die Aktiven Inhalte das LAN erreicht haben. Die Anforderung „Webseiten-Speicherung“ wird – wie viele andere in diesem Katalog auch – vorsorglich gestellt, ohne die konkreten Anforderungen zu kennen. In den meisten Fällen sollte der folgende Weg anwendungs- und sicherheitstechnisch gangbar sein: Umwandlung der Druckdarstellung einer Webseite in eine PDF-Datei mit einem geeigneten Konvertierungstool und Versand an den Anwender z. B. per E-Mail. Für besondere Bedarfsträger kann es auch notwendig sein, ein Screenshot-Tool einzusetzen, das die Webseite 1:1 archiviert. Danach kann die Archiv-Datei auf einem sicheren Weg ins LAN übertragen werden. Unter Umständen genügt auch ein lokaler Screenshot.
A 4	Copy and Paste	Der Anwender soll die Möglichkeit haben, die Funktionen „Copy and Paste“ in beide Richtungen zu verwenden, d. h. einerseits Inhalte einer Webseite zu kopieren und in andere Formate am Arbeitsplatz einzufügen und andererseits Inhalte am Arbeitsplatz zu kopieren (z. B. URLs) und in das Browserfenster einzubringen. „Inhalte“ können neben Text auch verschiedene Grafik-Formate sein. In den meisten Fällen wird es allerdings um Text gehen. Die Anforderung „Copy and Paste“ sicher zu implementieren (vgl. S 4), stellt eine besondere Herausforderung dar. Ursache ist, dass übliche Terminalserver-Implementierungen naheliegend die reguläre Zwischenablage am Arbeitsplatz-PC benutzen. Das hätte zur Folge, dass ein Angreifer, der den ReCoBS-Server übernommen hat, mit der regulären Funktionalität des ReCoB-Systems alle Zwischenablagen der verbundenen Arbeitsplatz-PC auslesen könnte. Auf diese Weise kann es zu einem erheblichen Abfluss sensitiver Informationen kom-

Nr.	Anforderung	Beschreibung
		men. Die beschriebene Gefährdung erscheint bei erster Betrachtung übertrieben; vergegenwärtigt man sich jedoch die intensive Nutzung der Zwischenablage im Rahmen moderner Büro-Anwendungen, so sollte sie nicht unterschätzt werden. Eine sichere Implementierung sollte zusätzliche, bewusste Anwender-Aktionen erfordern, um Inhalte von „innen“ nach „außen“ zu kopieren. Falls nur eine unsichere Realisierung zur Verfügung steht, sollte ggf. auf das „Copy and Paste“ verzichtet werden.
A 5	individuelle Benutzereinstellungen	Das ReCoB-System soll die Möglichkeit bieten, individuelle Benutzereinstellungen abzuspeichern und beim Aufruf durch den entsprechenden Benutzer zur Verfügung zu stellen. Dazu gehören: • die Einstellungen für die Oberflächengestaltung • die Verwaltung von Bookmarks/Favoriten • der Im- und Export von Bookmarks/Favoriten vom und zum Arbeitsplatz-PC. Dafür ist ein geeigneter sicherer Dateitransfer erforderlich. Netzwerkfreigaben, Drive Mapping und Mounten kommen nicht in Frage.
A 6	komfortable Bedienung	Es wird eine möglichst anwenderfreundliche Bedienung des Systems angestrebt, insbesondere sollen • der Start (etwa durch einen Doppelklick ggf. zusammen mit einer Passwortabfrage, möglichst keine weiteren Dialoge) und • die Bedienung des ReCoBS-Browsers sowie • die Größenveränderung und das Verschieben des ReCoBS-Browser-Fensters analog zu lokalen Anwendungen erfolgen können. Abgesehen von der möglichst uneingeschränkten Browser-Bedienung sollen sich die Einstellmöglichkeiten des Anwenders am ReCoBS-Client auf folgende Elemente beschränken: Start, Ende, Vergrößern, Verkleinern, Ändern der Fensterausmaße, Verschieben des Fensters. (Weitere ?) Der Anwender soll den Browser nicht schließen können, ohne dass sich auch das zugehörige Fenster schließt. Das Browser-Fenster sollte sich in den regulären Desktop des Arbeitsplatz-PC einfügen und keinen eigenen Desktop erfordern. Aus sicherheitstechnischen Gründen werden kleinere Verhaltensabweichungen des ReCoBS-Browsers von einem lokalen Browser in Kauf genommen. Beispielsweise könnte ein sicheres Drucken implementiert werden, indem die zu druckende Datei per E-Mail dem Anwender zugeschickt wird (vgl. A 1). Das ist aus Sicht der Bedienung ungewohnt, aber leicht und sicher zu implementieren; insbesondere erscheint es zumutbar.
A 7	Sound-	Es wird erwartet, dass der Übertragung akustischer Informationen

Nr.	Anforderung	Beschreibung
	Unterstützung	beim Web-Browsing eine immer größere Bedeutung zukommt. Daher soll ein ReCoB-System auch den Sound-Einsatz unterstützen. Bandbreitenproblemen kann eventuell durch eine Komprimierung mit entsprechenden Tonqualitätseinbußen begegnet werden. Sicherheitstechnische Teilanforderung: Sound sollte sich nur vom Server zum Client übertragen lassen, um ein Abhören der Arbeitsplätze zu verhindern. Das kann ggf. auch mit Hilfe eines Sicherheitsproxys durchgesetzt werden.

Anhang C: Sicherheitstechnische Anforderungen

Für Entwicklungsvorhaben in der IT fordert das BSI grundsätzlich, Sicherheit als gleichwertiges Leistungsziel neben Betrieb und Anwendung zu behandeln. Vor allem soll Sicherheit von Beginn an als integraler Bestandteil berücksichtigt und nicht erst am Schluss als Add-On künstlich „aufgepfropft“ werden. Bei einem ReCoB-System kommt der Sicherheit besondere Bedeutung zu, da ReCoBS gerade zum Ziel hat, bequem **und** sicher mit Aktiven Inhalten umgehen zu können. Aus diesem Grund wird ein vergleichsweise hoher Realisierungsaufwand in Kauf genommen. Durch ReCoBS dürfen keine zusätzlichen Sicherheitsrisiken entstehen. Das Sicherheitsniveau bei Verwendung eines ReCoB-Systems soll allenfalls unwesentlich niedriger sein als das Niveau eines LAN mit Internetanschluss und gesperrten Aktiven Inhalten. Dafür soll das Niveau wesentlich höher sein als bei jedem Verfahren, das Aktive Inhalte ins LAN bis zu den Arbeitsplätzen gelangen lässt.

Alle Sicherheitsmaßnahmen dienen dem eigentlichen Ziel, Vertraulichkeit, Integrität und Verfügbarkeit der Daten im LAN zu gewährleisten. Dies soll im Wesentlichen durch die ReCoBS-Grundidee, den Bruch in der Informationsverarbeitung, erreicht werden. Allerdings sind flankierende Sicherheitsmaßnahmen erforderlich, um ein Aushebeln des Grundprinzips zu verhindern. In diesem Sinne sind die unten aufgeführten Anforderungen zu verstehen. Die Auflistung beschränkt sich auf die ReCoBS-spezifischen Sicherheitsanforderungen. Darüber hinaus sind Standardsicherheitsanforderungen entsprechend dem IT-Grundschutz zu erfüllen, auf die hier nicht weiter eingegangen wird (z. B. Zugangsschutz, Aktualität der Patches usw.).

Durch weitere Aspekte (konkrete Anforderungen, erweiterte Einsatzszenarien, spezielle Realisierungen, neue Angriffsmethoden etc.) können sich zusätzliche sicherheitstechnische Anforderungen ergeben. Die nachfolgende Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit.

Hersteller, Entwickler und Bedarfsträger werden daher ausdrücklich aufgefordert, die hier zusammengestellten sicherheitstechnischen Anforderungen ggf. zu vervollständigen und an den konkreten Bedarfsfall anzupassen.

Die folgenden Anforderungen sind grob nach Server, Client, Verbindung und Umfeld untergliedert. Diese Strukturierung bezieht sich auf den logischen Ort, an dem die genannten Maßnahmen realisiert werden. Viele davon wirken sich aber auf das gesamte System aus.

Die Erläuterungen sind teilweise mit Realisierungsvorschlägen und Beispielen für vergleichbare Problemstellungen versehen. Dadurch soll lediglich die Idee hinter einzelnen Anforderungen verdeutlicht werden. Die Vorschläge sind nicht verbindlich. Ziel sollten bessere Realisierungen sein.

Nr.	Anforderung	Beschreibung
S 1	Server-sicherheit	Auf dem ReCoBS-Server sind geeignete Maßnahmen zu ergreifen, um Integrität, Vertraulichkeit und Verfügbarkeit der Daten auf dem Server – und damit letztlich der Daten im LAN – zu gewährleisten. Dazu gehören insbesondere die Anforderungen S 1.1 – S 1.9. Darüber hinaus soll die Vollständigkeit der Maßnahmen geprüft werden. Die vorgeschlagenen Maßnahmen sind teilweise restriktiv. Grund

Nr.	Anforderung	Beschreibung
		dafür ist die Netzwerktopologie und die Funktion des ReCoBS-Servers innerhalb des ReCoB-Systems: Bei klassischen Terminalserver-Implementierungen befindet sich der Server im Vergleich zu den Clients in einem Netz mit höherem oder gleichem Sicherheitsniveau. Der ReCoBS-Server befindet sich hingegen Prinzip bedingt in einem weniger sicheren Netz als die Clients. Auf dem Server werden Aktive Inhalte von beliebigen Webseiten ausgeführt. Daher muss mit erfolgreichen Angriffen auf den ReCoBS-Server gerechnet werden. Sie werden kurzzeitig in Kauf genommen („Opferrechner“). Sie dürfen keinen wesentlichen Schaden verursachen.
S 1.1	regelmäßiger System-Integritäts-check	Die Bereiche des ReCoBS-Servers, in denen keine Benutzereinstellungen oder -dateien gespeichert werden (statische Bereiche), sollen regelmäßig einem Integritätscheck unterzogen werden können (z. B. durch Tripwire, das von CD gestartet wird). Auch für die dynamischen Bereich, in denen Benutzereinstellungen gespeichert werden, sollte eine „Plausibilitätsprüfung“ möglich sein. Nach einer System-Bereinigung (vgl. S 1.2) soll gewährleistet werden können, dass ausschließlich „zulässige Typen“ von Benutzereinstellungen in den dynamischen Bereichen wiederhergestellt werden. Dies lässt sich umso leichter realisieren, je weniger Einstellmöglichkeiten die Benutzer haben (vgl. A 5).
S 1.2	regelmäßiger Reboot mit System-Bereinigung	Der ReCoBS-Server soll in regelmäßigen Abständen (z. B. täglich) automatisiert von einem schreibgeschützten System aus gebootet und bereinigt werden können. Unter „Bereinigung“ ist die Rücksetzung des Systems in einen als unkompromittiert definierten Ausgangszustand zu verstehen. Es soll sichergestellt werden, dass sich ein Angreifer auf dem System nicht permanent festsetzen kann. Erreicht werden kann dies beispielsweise, indem der Server von DVD gebootet und danach die Festplatte vollständig mit einem System-Image von der DVD überschrieben wird. Das „saubere“ System wird anschließend von der Festplatte gestartet. Auf diese Weise kann die Systemintegrität regelmäßig wiederhergestellt werden. Eine zuvor erfolgreiche Kompromittierung des Systems hätte ohne weitere Maßnahmen auch nach dem Reboot erneut Erfolg; sie wäre aber je nach Angriffsmethode und zusammen mit Anforderung S 1.6 für den Angreifer mit Aufwand verbunden. Es sollte möglich sein zu verhindern, dass die Anwender selbst eine Startseite für den ReCoBS-Browser festlegen. Zumindest soll beim regelmäßigen Reboot die Startseite auf eine harmlose Standard-Seite zurückgestellt werden können. Auf diese Weise wird gewährleistet, dass nicht dauerhaft eine Startseite gewählt ist, die • große Server- und Netz-Ressourcen erfordert, z. B. weil sie bewegte Bilder enthält, oder • einen Angriff auf den ReCoBS-Server ermöglicht, z. B. weil sie

Nr.	Anforderung	Beschreibung
		entsprechend präpariert wurde. Im zuletzt genannten Fall könnte die regelmäßige System-Bereinigung ebenso regelmäßig wieder unterlaufen werden, falls die Kompromittierung durch den Integritätscheck nicht erkannt wird. Eine wichtige Voraussetzung für die System-Bereinigung ist die klare Trennung von statischen und dynamischen Dateien. Vor allem Benutzereinstellungen sollen bei der Bereinigung nicht verloren gehen (vgl. A 5). Dazu können sie beispielsweise zwischengespeichert und zurückgespielt oder ständig außerhalb des ReCoBS-Servers gespeichert werden. Spätestens bei einer System-Bereinigung soll die Plausibilität der dynamischen Dateien überprüft werden (vgl. S 1.1). Als Alternative zum regelmäßigen Reboot kann möglicherweise auch regelmäßig ein partielles Recovery der statischen Speicherbereiche durchgeführt werden.
S 1.3	Vertraulichkeit auf dem Server	Die Aktivitäten eines ReCoBS-Nutzers auf dem Server könnten beobachtet werden. Mögliche Gegenmaßnahmen reichen von einer restriktiven Rechtevergabe über die Verschlüsselung des Dateisystems bis hin zur Verwendung von gekapselten Umgebungen, in denen der Benutzer nur seinen privaten Bereich des Dateisystems sehen kann (Bsp.: Chroot-Umgebungen in der Linux-Welt). Die Vertraulichkeit auf dem ReCoBS-Server, die durch Hacker, reguläre Anwender und den Administrator gefährdet sein kann, wird nicht nur durch die hier genannten Anforderungen, sondern durch das Zusammenwirken einer Reihe von Maßnahmen und Anforderungen gewährleistet. Dies darzustellen ist Aufgabe des Sicherheitskonzeptes.
S 1.4	sichere Fernadministration	Integrität und Vertraulichkeit einer Verbindung zur Fernadministration des ReCoBS-Servers sollen gewährleistet werden können. Die Verbindung zur Fernadministration hat einen höheren Schutzbedarf als normale ReCoBS-Verbindungen. Das gilt insbesondere, falls die Fernadministration nicht direkt aus dem LAN oder der DMZ, sondern über das Internet erfolgen soll.
S 1.5	keine kritischen Systemvorgänge	Auf dem ReCoBS-Server dürfen keine kritischen Systemvorgänge implementiert sein, insbesondere: • kein Verbindungsaufbau von außen nach innen (Auch nicht für Teilfunktionalitäten, vgl. Anforderungen A 1–3. Das System muss gewährleisten, dass Verbindungsaufbauten über das Sicherheitsgateway im Rahmen von ReCoBS-Aktivitäten stets von innen nach außen erfolgen. Die Durchsetzung dieser Anforderung sollte mindestens durch einen Paketfilter zwischen ReCoBS-Server und LAN erzwungen werden, vgl. S 5.3.) • keine abschließende Prüfung auf Schadinhalte beim Dateitransfer ins LAN (In jedem Fall muss eine solche Prüfung erfolgen; aller-

Nr.	Anforderung	Beschreibung
		dings darf die entscheidende dieser Prüfungen unmittelbar vor dem Eintritt der Dateien ins LAN nicht auf dem ReCoBS-Server durchgeführt werden. Möglicherweise ist es aus betriebstechnischer Sicht sinnvoll, dass eine zusätzliche Prüfung auch auf dem ReCoBS-Server erfolgt.) • keine Netzwerkfreigaben, kein Drive Mapping oder Mounten LAN-interner Ressourcen • keine Spiegelung von Sitzungen (Die Spiegelung ermöglicht die gleichzeitige Darstellung eines Terminalserver-Fensters auf einem weiteren Rechner und soll üblicherweise den Administrator beim Support unterstützen.) • keine zentralen Management-Funktionalitäten • keine Speicherung oder Verarbeitung kritischer Daten (Hier sind technische Daten gemeint und keine kritischen Anwenderdaten. Deren Speicherung muss durch die Policy verhindert werden.) • ... (viele weitere kritische Vorgänge unsicherer Server-Implementierungen sind denkbar).
S 1.6	restriktiver Umgang mit ausführbaren Programmen	Das System soll so konfigurierbar sein, dass von Medien, die zentral Benutzereinstellungen und -daten speichern, keine ausführbaren Programme auf den ReCoBS-Server geladen und dort ausgeführt werden können. Dies soll insbesondere gelten, wenn es möglich ist, ausführbare Programme zu speichern (vgl. Anf. B 3.4). In der UNIX-Welt lässt sich diese Anforderung durch „mounten ohne executable flag“ (noexec) erfüllen. Auf diese Weise soll verhindert werden, dass Aktive Inhalte Programme installieren und starten bzw. dass solche Programme (unbeabsichtigt) von den regulären Benutzern gestartet werden.
S 1.7	System-Härtung	Die Software auf dem ReCoBS-Server – insbesondere das Betriebssystem – soll gehärtet sein. Unter Härtung ist hier im Wesentlichen eine Beschränkung der installierten Software auf die erforderlichen Module zu verstehen (Minimalitätsanforderung).
S 1.8	Einschränkung von Anwender-Funktionen	Für die Anforderungen A 1 – A 4 soll gelten: 1. Die Funktionalitäten lassen sich deaktivieren. 2. Der Programmcode zur Realisierung dieser Funktionalitäten lässt sich entfernen, um das System zu härten. Dabei soll ein modularer Aufbau das rasche Entfernen des Codes gewährleisten.
S 1.9	Logging	Das ReCoB-System soll umfangreiche Möglichkeiten zum Logging bieten. Einerseits sollen auf diese Weise Hacker-Angriffe und Management-Aktivitäten nachvollzogen werden können. Andererseits soll auch die Möglichkeit bestehen, die Aktivitäten regulärer Anwender nachzuvollziehen – und zwar so weit, dass ReCoBS nicht zur Anonymisie-

Nr.	Anforderung	Beschreibung
		rung illegaler Web-Aktivitäten missbraucht werden kann. D. h., der vom Anwender gestartete Browser (z. B. identifiziert durch seine PID) soll den einzelnen Web-Anfragen des ReCoB-Systems zugeordnet werden können. Solche Daten fallen auf einem Web-Proxy an, sofern sich die ReCoBS-Browser dort anmelden müssen. Um Hacker-Angriffe nachvollziehen zu können, ist die Ausleitung der Log-Daten an einen dedizierten Log-Host erforderlich.
S 2	Client-sicherheit	Auf dem ReCoBS-Client sind geeignete Maßnahmen zu ergreifen, um Integrität, Vertraulichkeit und Verfügbarkeit der Daten auf dem Client und im LAN zu gewährleisten. Dazu gehören insbesondere die Anforderungen S 2.1 und S 2.2. Darüber hinaus soll die Vollständigkeit der Maßnahmen geprüft werden.
S 2.1	Vertraulichkeit auf dem Client	Ein ReCoBS-Client könnte das Ausspähen von Daten auf dem Client-System ermöglichen. Diese Möglichkeit könnte sich insbesondere bei Verwendung von X-Servern auf Client-Seite ergeben. Daher sollen alle regulären Funktionen, die das Ausspähen des Clients ermöglichen könnten, deaktiviert bzw. durch Code-Entfernung unterbunden werden. Hierbei handelt es sich um einen speziellen Aspekt, der für eine Reihe etablierter Terminalserver-Systeme typisch ist – ebenso wie die bei Anforderung S 1.5 unterbundene Spiegelung von Sitzungen auf dem ReCoBS-Server. Die Vertraulichkeit auf dem Client (wie auch Vertraulichkeit, Integrität und Verfügbarkeit der Daten im gesamten LAN) soll maßgeblich durch die ReCoBS-Grundidee, also den Bruch in der Informationsverarbeitung, und durch die flankierenden Maßnahmen gewährleistet werden.
S 2.2	Minimalität der Client-Software	Der ReCoBS-Client (hier ist die ReCoBS-Software gemeint, nicht der Client-Rechner oder sonstige Software auf dem Client) soll minimal sein in dem Sinne, dass sich die installierte Software auf die erforderlichen Module beschränkt.
S 3	Verbindungs-sicherheit	Die Verbindung zwischen ReCoBS-Server und -Client soll durch geeignete Maßnahmen geschützt werden, um Integrität, Vertraulichkeit und Verfügbarkeit der Daten im LAN zu gewährleisten. Dazu gehören insbesondere die Anforderungen S 3.1 – S 3.3. Darüber hinaus soll die Vollständigkeit der Maßnahmen geprüft werden.
S 3.1	Integrität (Authentizität)	Das ReCoB-System soll für die Verbindung zwischen Client und Server die Grundanforderung Integrität erfüllen können. Integrität wird normalerweise über kryptografische Prüfsummen gewährleistet. Diese Anforderung scheint hier jedoch übertrieben zu sein, da es zunächst um das Surfen im Internet geht. Man kann sich hier möglicherweise mit der Kombination von Authentifizierung und Ver-

Nr.	Anforderung	Beschreibung
		schlüsselung begnügen. Es zeichnet sich jedoch ab, dass ein ReCoB-System auch für sensitivere Anwendungen als das Surfen im Internet verwendet werden wird. Für solche Anwendungen müssten dedizierte Systeme bereitgestellt werden. Keinesfalls sollte eine sensitive Anwendung auf dem selben ReCoB-System realisiert werden, welches das Surfen auf beliebigen Webseiten ermöglicht. Bei dem zuletzt skizzierten Szenario wäre je nach Art der Anwendung ein Schutz der Integrität in vollem Umfang – also mittels kryptografischer Prüfsummen – unumgänglich.
S 3.2	Vertraulichkeit	Das ReCoB-System soll für die Verbindung zwischen Client und Server die Grundanforderung Vertraulichkeit erfüllen können. Dazu soll eine geeignete Verschlüsselung vorgesehen werden.
S 3.3	minimales Terminalserver-Protokoll	1. Das Terminalserver-Protokoll sollte nur die erforderlichen Funktionen umfassen (oder) 2. Die (technisch-funktionale) Unterstützung für das Terminalserver-Protokoll sollte sich auf die erforderlichen Funktionen einschränken lassen (oder) 3. Sollte das Protokoll mehr Funktionen beherrschen als die Übermittlung von Grafik-, Tastatur- und Maus-Informationen, so sollte es einen geeigneten Sicherheitsproxy geben, um alle anderen Funktionen im Bedarfsfall herausfiltern zu können (vgl. Anf. S 5.1). Das verbleibende Risiko eines ReCoB-Systems hängt u.a. vom Funktionsumfang des Terminalserver-Protokolls ab. Je spezialisierter und funktionsärmer es ist, umso weniger Angriffsfläche bietet es.
S 4	sichere Implementierung	Alle Anforderungen sollen so sicher implementiert werden, dass sie nur schwer für Angriffe missbraucht werden können. Durch das ReCoB-System dürfen keine neuen Sicherheitslücken entstehen. Diese Anforderung lässt sich global lediglich derart allgemein formulieren, da eine sichere Implementierung für die unterschiedlichen Anforderungen höchst unterschiedliche Konsequenzen hat. Ausdrücklich wird darauf hingewiesen, dass einzelne Sicherheitsanforderungen (z. B. S 1.5) weitreichende Auswirkungen auf die Realisierung anderer Anforderungen haben. Die globale Anforderung „sichere Implementierung“ soll den Aspekt der Sicherheit bei einem ReCoB-System unterstreichen. Einerseits soll bei der Entwicklung bzw. Systemintegration der Blick für das Detail (die einzelne Anforderung) geschärft werden. Andererseits soll das Augenmerk auf das Gesamtsystem gerichtet werden: Durch das Zusammenwirken der einzelnen Anforderungs-Implementierungen sollen keine neuen Gefahren entstehen. Eine Betrachtung verschiedener Terminalserver-Systeme am Markt hat gezeigt, dass

Nr.	Anforderung	Beschreibung
		• die Implementierung der Anforderungen bei den verschiedenen Systemen unterschiedlich sicher erfolgt, • es bei einzelnen Systemen für die gleiche Anforderung mehrere Realisierungsmöglichkeiten gibt, die unterschiedlich sicher sind.
S 5	Umfeld-sicherung	Zur Absicherung des ReCoB-Systems sollen im topologischen Umfeld geeignete Maßnahmen ergriffen werden. Dazu gehören mindestens die Nachfolgenden.
S 5.1	Sicherheits-proxy/ generischer Proxy	Die Einhaltung des Terminalserver-Protokolls bei der Kommunikation zwischen ReCoBS-Server und -Client soll durch einen geeigneten Sicherheitsproxy im Rahmen eines Application Level Gateways gewährleistet werden. Für einen performanten ReCoBS-Backbone (zwischen Server und erstem Switch im LAN) ist eine große Bandbreite erforderlich (Größenordnung: 100 MBit/s – 1 GBit/s bei den Lastannahmen aus B 2). Der Sicherheitsproxy muss entsprechend dimensioniert sein. Dabei könnten die Grenzen des zurzeit technisch Möglichen erreicht werden. Neben der Prüfung, ob das Protokoll eingehalten wird, kann der Sicherheitsproxy auch dem Zweck dienen, den Funktionsumfang des Protokolls wirksam einzuschränken, um die entsprechende Minimalitätsanforderung durchsetzen zu können (vgl. Anf. S 3.3). Falls kein Sicherheitsproxy existiert, soll zumindest ein generischer Proxy zwischen ReCoBS-Server und -Client eingesetzt werden, um die IP- und TCP-Header der ReCoBS-Datenpakete neu zu erzeugen. In diesem Fall sollte das Terminalserver-Protokoll darüber hinaus so beschaffen sein, dass seine Einhaltung möglichst leicht durch einen (ggf. noch zu entwickelnden) Sicherheitsproxy geprüft werden kann. Vertraulichkeit und Protokollanalyse sind konkurrierende Anforderungen in dem Sinne, dass eine Verschlüsselung die Analyse durch einen Proxy unmöglich macht, sofern sie nicht speziell für diesen Zweck unterbrochen wird. Zur Unterbrechung der Verschlüsselung wäre ein weiterer Proxy erforderlich. Falls kein Sicherheitsproxy für das Terminalserver-Protokoll existiert, kann es entsprechend dem Schutzbedarf erforderlich sein, zusätzlich den ReCoBS-Client auf dem Arbeitsplatz-PC zu kapseln.
S 5.2	Web-Sicherheits-proxy	Zwischen Internet und ReCoBS-Server soll ein Web-Proxy eingesetzt werden, um den HTTP-Verkehr überwachen zu können.
S 5.3	Paketfilter	Zur Absicherung des ReCoB-Systems sollen dynamische Paketfilter an mindestens zwei Positionen der Topologie eingesetzt werden: 1. zwischen Internet und ReCoBS-Server 2. zwischen ReCoBS-Server und LAN. Dort werden jeweils die Richtung des Verbindungsaufbaus („von

Nr.	Anforderung	Beschreibung
		innen nach außen“, vgl. Anf. S 1.5), die IP-Adressen und die Ports kontrolliert. Darüber hinaus wäre die Abgrenzung des ALG gegenüber dem ReCoBS-Server durch einen Paketfilter wünschenswert.