Browser
in the Box

Die virtuelle Umgebung für gesichertes und komfortables Surfen

Die Verwendung des Internet ist aus dem heutigen Arbeitsalltag – alleine schon zur Informationsgewinnung – kaum mehr wegzudenken. Gleichzeitig wird der PC zur Verarbeitung von vertraulichen Informationen verwendet, seien dies personenbezogene oder betriebsinterne, unternehmenskritische Daten. Dem immensen Nutzen des Internet stehen seine sich fortwährend wandelnden Gefahren gegenüber. Die Browser-Entwicklung der letzten Jahre kann neben allen funktionalen und Komfortfortschritten vor allem auch als ein beständiger Wettlauf im Kampf gegen unterschiedliche Angriffsszenarien verstanden werden.

Spätestens seit das Internet mit „Web 2.0“ aktiv wurde, ist die Gefahren - Nutzen Balance verloren gegangen. „Aktive Inhalte“ sind aus heutigen Webseiten nicht mehr wegzudenken, moderne Webseiten sind von vollwertigen nativen Anwendungen kaum noch zu unterscheiden. Programmierschnittstellen wie JavaScript, Java, ActiveX oder VBScript erlauben auch den Zugriff auf den PC des Benutzers, etwa auf das Dateisystem oder eine angeschlossene Webcam. Trojaner und Viren können damit diese neuen mächtigen Werkzeuge zum Zugriff auf vertrauliche Daten missbrauchen.

Unternehmen und Behörden stehen heute vor dem Dilemma, die Internetnutzung (auf unterschiedlichste Weisen) deutlich einzuschränken oder einen Weg zu finden, mit der Gefährdung zu leben.

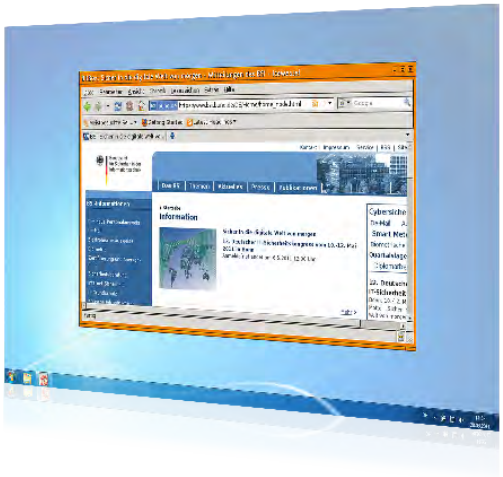
Einzelplatzversion frei erhältlich für Privatleute

Die von Sirrix zunächst im Auftrag des BSI für die Bundesbehörden entwickelte virtuelle Surfumgebung „Browser in the Box“ steht nun allgemein zur Verfügung und ermöglicht jedem Nutzer gefahrenlos im Internet zu surfen und das alles – entgegen sonst üblicher Ratschläge – mit vollem Einsatz modernster und komfortabelster Webtechnologien.

Auf Basis eines „Browser in the Box“ Konzeptes wird in einer für den Nutzer transparenten Weise eine virtuelle Maschine mit reduziertem Betriebssystem sowie einem darin gekapselten Webbrowser bereitgestellt. Schadsoftware kann daher nicht in das Basisbetriebssystem eindringen und ein eventueller Schaden an der separierten virtuellen Maschine wird bei jedem Browserstart durch Rückkehr auf einen zertifizierten Ausgangszustand beseitigt.

Schutz gegen Malware und Datenverlust

Im Unterschied zur einfachen Sandboxing-Methode von Standardbrowsern isoliert die Separierung eines ganzen Gastbetriebssystems alle Aktivitäten des Browsers vollständig vom Basisbetriebssystem. Lediglich ein gemeinsamer Ordner ist im Basisbetriebssystem für ein gesondertes Nutzerkonto zugreifbar. Hier werden alle persistenten Konfigurationsdaten (Favoriten etc.) des Browsers gespeichert. Auch alle aus dem Internet heruntergeladenen Dateien werden zunächst hier abgelegt bevor sie nach einem Malware-Scan dem Benutzer in seinem üblichen Download-Verzeichnis zur Verfügung gestellt werden. Neben dem so hergestellten weitgehenden Schutz des Basissystems vor Angriffen aus dem Internet wird außerdem ein Upload von Dateien ins Internet wirksam verhindert und damit die Vertraulichkeit wichtiger Unternehmens- oder Behördendaten nicht schon bereits durch die Bereitstellung eines Internetzugangs gefährdet. „Browser in the Box“ ermöglicht so ein kosteneffektives sorgenfreies Surfen ohne jede Komforteinschränkung. Der kostenträchtige und administrationsaufwendige Einsatz dedizierter Terminal-Server als Alternative für ein sicheres Surfen wird vermieden. Performanceeinbußen sind bei den heutigen Rechnerarchitekturen ebenfalls nicht zu erwarten.

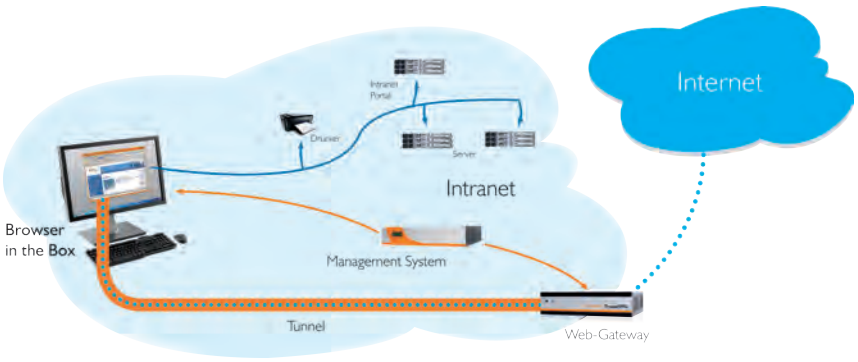


Sirrix AG
security technologies

Sirrix AG
Im Stadtwald D3 2
66123 Saarbrücken
Germany
+49 681 / 95986-0
+49 681 / 95986-500
info@sirrix.com
www.sirrix.com

Erweiterte Version zentral administrierbar

Für den professionellen Einsatz in zentral gemanagten IT-Umgebungen ist die erweiterte Variante eine ideale Lösung. Dabei wird ein Tunnel zwischen dem „Browser in the Box"-Browser und einem zentralen Internet-Gateway transparent integriert, der dafür sorgt, dass eine zuverlässige Trennung zwischen Internet und Intranet stattfindet: Während die Anwendungen auf dem Client nur auf das interne Unternehmensnetz zugreifen können, wird der „Browser in the Box" -Browser nach außen getunnelt und kann somit als einzige Anwendung auf das Internet zugreifen – isoliert von den restlichen Clientanwendungen. Weiterhin wird ein zentrales Managementsystem bereitgestellt, das auf einfache Weise ermöglicht, Sicherheitsrichtlinien und Konfigurationen zu verwalten sowie die notwendigen Gast-Images zu generieren, zertifizieren und zu verteilen.



Der Arbeitsplatz mit seinem Basisbetriebssystem wird in der erweiterten Version von „Browser in the Box" vollständig vom Internet abgekoppelt. Nur die virtuelle Maschine mit dem gekapselten Browser hat eine getunnelte Verbindung zum Internet.

Features

Basiseigenschaften

- Einsetzbar für Windows XP, Vista und Windows 7 sowie Linux Debian, (K)Ubuntu, OpenSUSE und Gentoo
- Mitgelieferte Komponenten: VirtualBox, gehärtetes Linux Debian 6 und Firefox

Komfort

- Transparente Nutzung ohne Unterschied zu normalem, direktem Browserbetrieb
- Einfache Installation ohne Knowhow-Anforderungen

Sicherheit

- Browser läuft nur in getrennter virtueller Maschine mit eigenem Betriebssystem
- Heruntergeladene Daten werden erst gescannt und dann bereitgestellt
- Sicheres Drucken von Seiten aus dem „Browser in the Box" -Browser über Client
- Sicheres Cut & Paste, einstellbar über Policy
- Hochladen von Dateien wird optional verhindert
- Reset zu zertifiziertem Startimage bei Neustart des Browsers
- Konfigurationsdaten des Browsers können persistent

Erweiterte Version

- Komfortables Managementsystem für Sicherheitsrichtlinien, Konfigurationen und Images
- Active Directory Integration
- Trennung von Intranet und Internet mittels Tunnel zwischen „Browser in the Box" Browser und Internet-Gateway