Browser in the Box
Wirksamer Schutz gegen Angriffe aus dem Internet

Sicheres Surfen im Web durch Trennung von Internet und Intranet

Schutz vor Schadcode, ZERO Day Exploits und APT

Die Verwendung des Internet ist aus dem heutigen Arbeitsalltag nicht mehr wegzudenken. Gleichzeitig wird der PC zur Verarbeitung von vertraulichen Unternehmensinformationen wie z.B. personenbezogenen oder betriebsinternen unternehmenskritischen Daten genutzt. Dem immensen Nutzen des Internet stehen seine sich fortwährend wandelnden Gefahren gegenüber. Die Browser-Entwicklung der letzten Jahre sowie Web 2.0 kann neben allen funktionalen Fortschritten vor allem auch als ein beständiger Wettlauf im Kampf gegen unterschiedliche Angriffsszenarien verstanden werden. Programmierschnittstellen wie JavaScript, Java, ActiveX oder VBScript erlauben auch den Zugriff auf den PC des Benutzers, etwa auf das Dateisystem. Trojaner und Viren können damit neue und mächtige Werkzeuge zum Zugriff auf vertrauliche Daten missbrauchen.

Neuer Lösungsansatz mit Browser in the Box

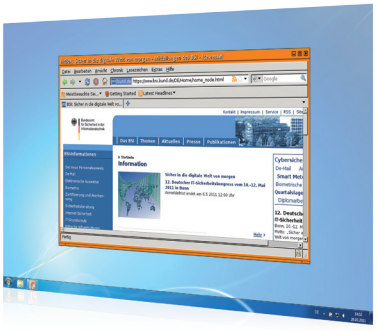
Die von Sirrix zunächst im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickelte Lösung „Browser in the Box“ stellt einen völlig neuen sicheren Ansatz für den Schutz gegen Angriffe aus dem Internet dar. Sie ermöglicht jedem Nutzer gefahrlos im Internet zu surfen und das – entgegen sonst üblicher Ratschläge – mit vollem Einsatz modernster und komfortabelster Webtechnologien. Auf Basis eines „Browser in the Box“ Konzeptes wird transparent für den Nutzer eine virtuelle Maschine mit gehärtetem Betriebssystem sowie einem darin gekapselten Webbrowser bereit-gestellt. 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. Mit diesem innovativen Konzept ist die Schutzwirkung auch gegen neuartige und unbekannte Angriffe stets gewährleistet. Die Schutzwirkung steht und fällt nicht mit der Erkennungsrate für Schadsoftware wie es beispielsweise bei Signatur oder verhaltensbasierten Ansätzen der Fall ist.

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 des Browsers (Favoriten etc.) 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. Zusätzlich zur Downloadkontrolle wird außerdem eine Kontrolle für den Upload von Dateien ins Internet wirksam und verhindert damit, dass kritische Daten durch einen ungewollten Upload in fremde Hände gelangen.

Mit dem so hergestellten Schutz des Basissystems vor Angriffen aus dem



ROHDE&SCHWARZ
Cybersecurity

Browser in the Box

Internet wird die Vertraulichkeit wichtiger Unternehmens- oder Behördendaten nicht schon bereits durch die bloße Bereitstellung eines Internetzugangs gefährdet.

„Browser in the Box“ ermöglicht so ein kosteneffektives sicheres Surfen ohne jede Komforteinschränkung. Der kostenträchtige und administrationsaufwendige Einsatz dedizierter Terminal- Server als Alternative für ein sicheres Surfen wird vermieden.

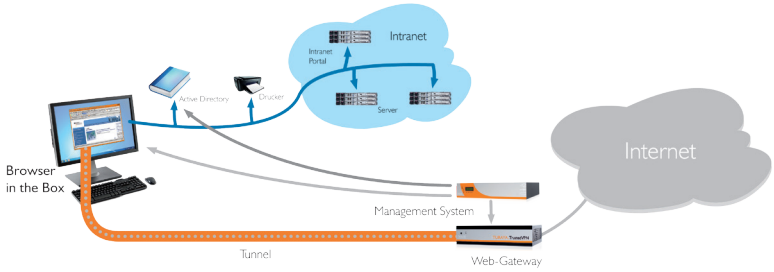
Performanceeinbußen sind bei den heutigen Rechnerarchitekturen ebenfalls nicht zu erwarten.

Mit diesem innovativen Konzept ist die Schutzwirkung auch gegen neuartige und unbekannte Angriffe wie z.B. ZERO Day Exploits oder Advanced Persistent Threats stets gewährleistet. Die Schutzwirkung steht und fällt nicht mit der Erkennungsrate für Schadsoftware wie es beispielsweise bei Signatur oder Verhaltensbasierten Ansätzen der Fall ist.

Browser in the Box Enterprise mit Verzeichnisdienst Unterstützung und zentralem Management

Für den professionellen Einsatz in zentral gemanagten IT-Umgebungen bietet Browser in the Box Enterprise ein zentrales Management. Es ermöglicht, auf einfache Weise Sicherheitsrichtlinien und Konfigurationen zu verwalten sowie die notwendigen Gast-Images zu generieren, zertifizieren und zu verteilen. Weiterhin wird ein Tunnel zwischen

„Browser in the Box“ und einem zentralen Internet-Gateway transparent integriert. Dieser sorgt dafür, dass eine zuverlässige Trennung zwischen Internet und Intranet stattfindet: Während die Anwendungen auf dem Client nur auf das interne Unternehmensnetz zugreifen können, wird „Browser in the Box“ nach außen getunnelt und kann somit als einzige Anwendung auf das Internet zugreifen – isoliert von den restlichen Clientanwendungen.



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, Windows 7, Windows 8
- Mitgelieferte Komponenten: VirtualBox, wahlweise Firefox oder Chrome

Sicherheit

- Browser läuft nur in getrennter virtueller Maschine mit eigenem Betriebssystem
- Internet-Downloads werden erst gescannt und dann bereitgestellt
- Sicheres Drucken von Internetseiten 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 persistentgespeichert werden und bleiben bei Reset erhalten

Komfort

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

Zentrales Management mit TrustedObjects Manager

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

Rohde & Schwarz Cybersecurity
Sirrix AG
Campus Gebäude D3 2
66123 Saarbrücken Germany

Phone +49 681 959 - 860
Fax +49 681 959 86 - 500

Email cybersecurity@rohde-schwarz.com

cybersecurity.rohde-schwarz.com