Browser in the Box TS

Wirksamer Schutz vor Schadcode und Exploits beim Surfen im Web

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 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. Insbesondere gegen Angriffe, die Schwachstellen im Browser oder Betriebssystem ausnutzen greifen bisherige Techniken wie Anti-Virus Software nicht mehr. Sogenannte Zero-Day Exploits ermöglichen dabei Angreifern auch bei regelmäßig gepatchten Systemen ein erfolgreiches Eindringen. Der Schaden für Unternehmen und Behörden entsteht dabei nicht nur bei zielgerichteten Angriffen: Durch den hohen Anteil infizierter Server im Web, ist das Infektionsrisiko bei einfachem Websurfen bereits groß genug um erhebliche Kosten zu verursachen:

Beispielsweise durch das regelmäßige Neuaufsetzen von Client-Rechnern nach einer Infektion.

Innovativer Lösungsansatz mit Browser in the Box

Die von Sirrix zunächst im Auftrag des BSI für die Bundesbehörden entwickelte virtuelle Surfumgebung „Browser in the Box“ ermöglicht den Nutzern ein freies und gefahrenloses Surfen im Internet. Das pro-aktive, Security-by Design Konzept schafft damit Sicherheit – auch gegen bisher unbekannte Schwachstellen und Malware.

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 Exploits und Malware

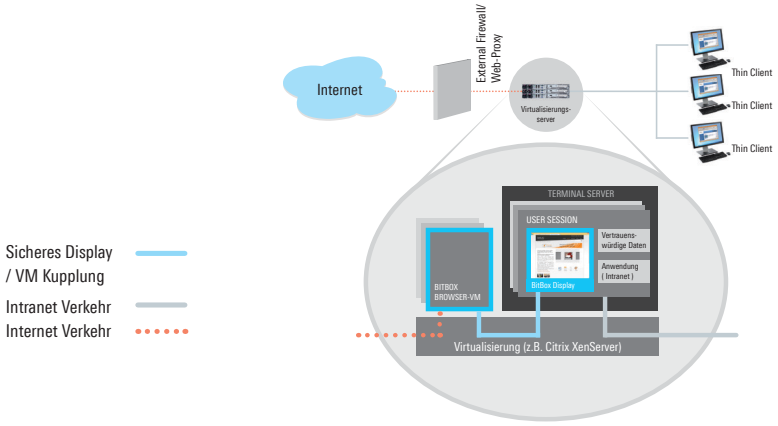
Im Unterschied zur einfachen Sandboxing-Methode von Standardbrowsern isoliert die Separierung eines ganzen Gastbetriebssystems alle Aktivitäten des Browsers vollständig vom Basisbetriebssystem. Lediglich ein

Browser in the Box TS

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 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 und ohne Performanceeinbußen.

Browser in the Box für Terminal Server

Das bewährte Browser in the Box Konzept steht auch für zentrale virtualisierte Infrastrukturen mit Terminal Servern und Thin Clients zur Verfügung. In Terminal Server Infrastrukturen, läuft ein Windows Server in einer virtualisierten Umgebung wie sie Citrix, VMware, oder Microsoft bereitstellen. Dieser Windows Server stellt jedem Benutzer eine Desktop-Session bereit, welche auf dem Thin-Client lediglich angezeigt wird. Bei Browser in the Box für Terminal Server läuft der Browser nicht in der Desktop-Session des Windows Server sondern in einer separaten virtuellen Maschine. Lediglich die Anzeige des Browsers wird in die Desktop-Session übertragen und dargestellt. Damit wird eine zuverlässige Trennung von Intranet-Netzwerken und dem Internet ermöglicht. Diese flexible Architektur bindet Browser in the Box für Terminal Server in bestehende virtuelle Infrastrukturen ein. Der administrationsaufwendige und ohnehin nicht angemessen sichere Einsatz dedizierter Terminal-Server als Surf-Alternative wird vermieden. Mit dem zentralen Managementsystem wird auf einfache Weise ermöglicht, Sicherheitsrichtlinien und Konfigurationen zu verwalten sowie die notwendigen Gast-Images zu generieren, zertifizieren und zu verteilen.



Features

Basiseigenschaften

- Einsetzbar für Windows Server 2008 / 2012 / 2012 R2 in Citrix Infrastruktur

Sicherheit

- Browser läuft vollständig getrennt in virtueller Maschine mit eigenem Betriebssystem
- Heruntergeladene Daten werden erst sicherheitsgeprüft 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 gespeichert werden und bleiben bei Reset erhalten
- Trennung von Intranet und Internet

Komfort

- Transparente Nutzung ohne Unterschied zu normalem, direktem Browserbetrieb
- Einfache Installation
- Komfortables Managementsystem für Sicherheitsrichtlinien, Konfigurationen und Images
- Active Directory Integration

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 89 4129-0
cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

3607571931

3607.5719.31 01.00 PDP 1 de July 2016