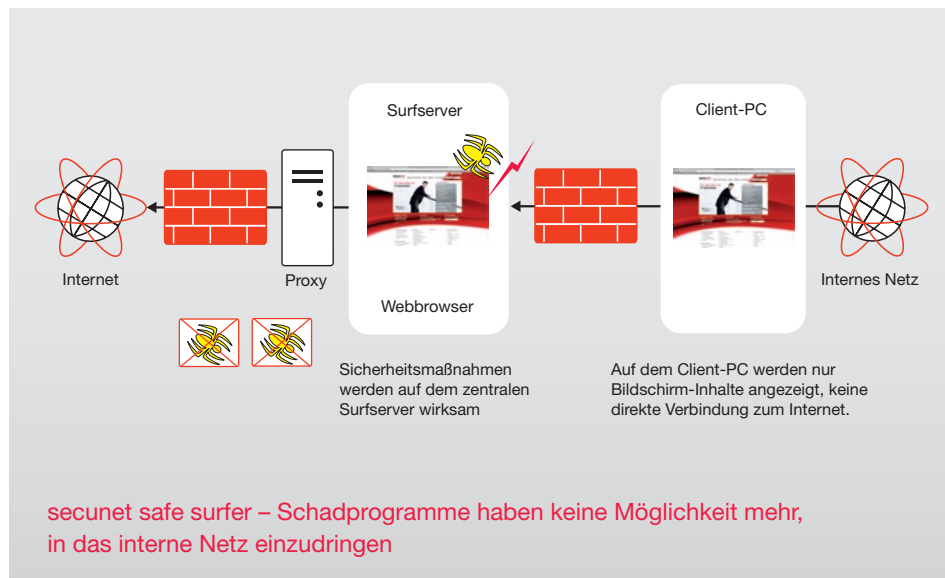


Sicherer Schutz vor Schadprogrammen



Ihre Vorteile:

- » PC ist sicher vor Schadsoftware geschützt
- » Durchgängige Sicherheit durch zentrale Administration
- » Sichere Nutzung aktiver Inhalte auch im VS-Umfeld

secunet safe surfer schützt Ihre Systeme und Daten beim Websurfen vor Angriffen aus dem Internet. Der Zugriff auf das Internet erfolgt über ein Remote Controlled Browser System (ReCoBS). Am Arbeitsplatz werden nur Bildschirmdaten angezeigt. **Der Vorteil: Der Arbeitsplatz hat keinen direkten Zugang mehr zum Internet. Vertrauliche Daten auf dem PC sind hochsicher vor Schadsoftware geschützt.**

secunet safe surfer – der sichere Weg ins Internet

Die Nutzung des Internets ist heute an keinem modernen Arbeitsplatz mehr weg zu denken. Die Gefahren durch Schadsoftware, die während des Websurfens unbemerkt auf den Arbeitsplatz gelangen können, sind jedoch unverändert hoch. Virens Scanner sind aufgrund der Vielzahl der Angriffsmöglichkeiten nicht mehr in der Lage, den Arbeitsplatz vor gezielten Angriffen zu 100% zu schützen. Insbesondere in hochsicheren Umgebungen oder bei der Bearbeitung von Verschluss sachen (VS) am Arbeitsplatz ist der Zugang zum Internet daher meist nur von separaten Arbeitsplätzen erlaubt. Mit dem secunet safe surfer haben wir eine Lösung entwickelt, die Ihren Mitarbeitern das sichere und komfortable Internetsurfen auch von Arbeitsplätzen mit hochschützenswürdigen Daten ermöglicht. Durch eine intelligente Trennung des Webbrowsers vom Arbeitsplatz können Schadprogramme nicht mehr durch das Surfen auf den Arbeitsplatz gelangen. Der Webbrowser des Benutzers wird auf einen zentralen Surfserver verlagert, der zum Internet speziell gesichert ist. Der Anwender erhält lediglich eine Bildschirmansicht der Webseiten und hat keinen direkten Zugriff auf das Internet.

Sicheres Surfen wird komfortabel

Der secunet safe surfer wurde gemäß den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt. Die Lösung besteht aus Client- und Server-Komponenten, die intelligent kombiniert ein sicheres und komfortables Surfen ermöglichen. Aktive Inhalte werden nur noch kontrolliert auf dem zentralen Server ausgeführt. So werden sensible Daten auf dem Arbeitsplatz besser geschützt. Folgenden Funktionen unterstützen die komfortable Internetnutzung:

- E-Mail-Versand von Downloads und Ausdrucken an den Benutzer
- E-Mail-Versand von PDF-Ausdrucken
- Direkter Ausdruck von Dokumenten auf individuelle Standarddrucker
- Copy & Paste Funktionen
- Komprimierung von Bilddaten

Für eine hohe Verfügbarkeit bei einer großen Benutzeranzahl kann die Lösung auf mehrere Server verteilt und zusätzlich redundant ausgelegt werden.

ReCoBS-konforme Sicherheitsmechanismen

Die Trennung des Webbrowsers vom Arbeitsplatz reicht allein nicht aus, um den Schutz vor Angriffen aus dem Internet sicher zu gewährleisten. Der ReCoBS-konforme secunet safe surfer stellt weitergehende Sicherheitsmechanismen bereit. Die Lösung unterstützt das ReCoBS Protection Profile (PP) und kann gemäß Common Criteria (CC) evaluiert werden und ist auch in Umgebungen mit sehr hohen Sicherheitsanforderungen einsetzbar. Beim secunet safe surfer sind u. a. folgende Sicherheitsmechanismen umgesetzt:

Täglicher automatischer Integritätscheck

In einem individuell bestimmbaren Intervall startet der zentrale Surfserver eigenständig von einem sicheren Bootmedium und überprüft die Integrität des installierten Systems gegen eine Referenzdatenbank. Über Manipulationen des Systems wird der Sicherheitsverantwortliche automatisch informiert. Anschließend erfolgt eine ebenfalls automatisierte Re-Installation des gesamten Systems. Die Re-Installation löscht jegliche durch das Surfen möglicherweise installierte Schadprogramme.

Strikte Begrenzung von Systemrechten

Die Benutzersessions auf dem Surfserver verfügen nur über minimale Rechte im Betriebssystem, so dass andere Benutzersessions nicht gefährdet sind. Auf dem Server ausgeführte Schadprogramme können Systemdateien oder sensible Daten weder lesen noch modifizieren.

Zentral aktualisierte Software

Die Benutzer behalten wie gewohnt die Möglichkeit, eigene Bookmarks zu verwalten. Die Aktualisierung der Browsersoftware, der Browser-Plugins und des Betriebssystems erfolgt von zentraler Stelle über das einfache Booten von einem integritätsgesicherten Speichermedium. Dieser Ansatz gewährleistet, dass für alle Benutzer immer die aktuellen Software- bzw. Browserversionen und empfohlenen Konfigurationen zum Einsatz kommen.

Pseudonymisierung von Anwenderdaten

Der zentrale Server speichert aus Sicherheitsgründen keine internen Anwenderdaten, wie z. B. interne Benutzerkennungen. Ein Proxy Dienst verbirgt die IP-Adressen des internen Netzes. Die Benutzerprofile werden aus Gründen des Datenschutzes pseudonymisiert abgelegt. Eine Zuordnung zu den internen Benutzern ist für Dritte aus dem Internet heraus nicht möglich, diese kann nur mit Administratorrechten erfolgen.

Abgesichertes Logging

Ein Management-Server protokolliert die Logdaten über die Ereignisse auf dem Surfserver. Beide Server sind durch einen Paketfilter voneinander getrennt. Somit können Protokolldaten unabhängig von der Sicherheit des Surfserver gespeichert werden.

Referenzprojekt Bundeskanzleramt

secunet safe surfer ist seit Januar 2007 im Bundeskanzleramt erfolgreich im Einsatz. Bei mehr als 500 Mitarbeitern hat secunet eine Architektur mit drei parallel betriebenen Servern realisiert. Die bisherigen Erfahrungen der Anwender sind durchweg positiv, da zuvor der Zugriff auf das WWW nur umständlich über separate, vom Netz getrennte PCs möglich war. Die Möglichkeit des Internet-Zugriffs vom Arbeitsplatz ohne Gefährdung des internen Netzes ist eine Bereicherung der Arbeitsmöglichkeiten für die Mitarbeiter.

Weitere Informationen:
www.secunet.com/safesurfer

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com