ReCAppS

Remote Controlled Application System

itWatch GmbH

Stresemannstr. 36
D-81547 München
Tel. : +49 (0) 62 03 01 00
Fax : +49 (0) 69 39 28 04
www.itWatch.de
info@itWatch.de

ReAppS

Remote Controlled Application System

Die Gefährdungslage

- Die Email eines „Freundes" enthält einen Link. Durch das Anklicken installiert sich ein Wurm, Trojaner oder sonstiger Schadcode.
- Der USB-Stick oder die CD von einer Veranstaltung enthält Spyware um Ihre Daten abzusaugen und per http-s verschlüsselt ins Internet hochzuladen.
- Ihr Geschäftspartner überreicht Ihnen vertrauliche Daten verschlüsselt auf einem USB-Stick. Wie stellen Sie sicher, dass die Daten nicht risikobehaftete Makros enthalten?
- Gehackte Webseiten von seriösen Unternehmen verbreiten Schadcode.

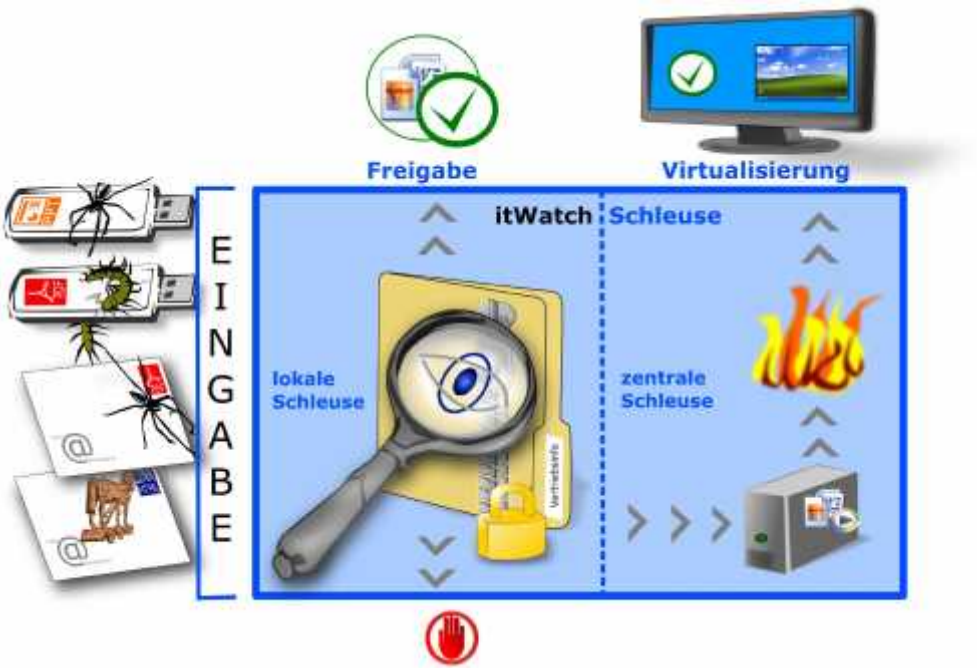
Die Herausforderungen

- Das Sperren von externen Datenträgern oder bestimmten Internetseiten verhindert sinnvolle Business Prozesse.
- Content Filter am Gateway oder auf der Firewall können nur auf Klartext-Daten wirken - aus Datenschutzgründen darf oftmals der SSL-verschlüsselte Verkehr nicht aufgebrochen werden.
- Webseiten mit aktiven Inhalten können nicht einfach verboten werden.
- Das Wiederherstellen und Bereinigen von verseuchten Systemen kostet Zeit, Ressourcen und Geld.
- Vertrauliche Informationen tauchen bei WikiLeaks auf oder gehen an Mitbewerber.
- Verschlüsselte und gezippte Dateien und Archive müssen im Klartext überprüft werden.
- Verbote verhindern die Zufriedenheit und die Produktivität.

Die Lösung für zufriedene Anwender, trotz Sicherheit

1. Die integrierte lokale Schleuse:

Entschlüsselung und rekursive Dekomprimierung von Dateien erfolgen in einer lokalen Quarantäne – dort können die Inhalte im Klartext geprüft werden. Je nach Ergebnis werden die einzelnen Dateien gemäß zentraler Richtlinien geblockt und sicher gelöscht, zur Prüfung an Dritte weitergeleitet oder freigegeben. Ein Zugriff der Benutzer während der Überprüfung ist technisch verhindert. Der Rechner kann somit nicht durch Schadcode infiltriert werden. Zusätzliche Hardware und lange Wege sind unnötig.



2. Die virtuelle Schleuse:

Effiziente Arbeitsumgebungen benötigen aus Sicht des Anwenders die Möglichkeit auch kritische Aktionen sofort durchzuführen. Kritisch ist zum Beispiel das Anklicken einer problematischen URL, das Herunterladen von ausführbaren Elementen aus dem Internet oder das Installieren einer unbekannten Anwendung von einem fremden Datenträger. Für den sicheren Betrieb von Browsern hat das BSI mit ReCoBS ein Konzept vorgestellt, welche das sichere Surfen durch Auslagern des Browsers in die DMZ ermöglicht. Die itWatch Lösungen nutzen dieses Verfahren nicht nur zum sicheren Betrieb des Browsers sondern für alle ungeplanten, sicherheitskritischen Aktionen:

- das automatische Auslagern und Ausführen von Executables in einer virtuellen Umgebung hinter einer Firewall oder in der Cloud
- Verarbeitung oder Ansicht von kritischen Daten, die von fremden Datenträgern oder unsicheren Anwendungen auf den Client importiert werden sollen.

In der „remote controlled Session" hat der Anwender alle nötigen Rechte (z.B. Installation, etc.) ohne die produktive Umgebung zu gefährden. Inhalte werden sowohl auf dem remote controlled System als auch auf dem Client des Anwenders nach den zentralen Vorgaben kontrolliert, so dass kein Schadcode ins interne Netz gerät und der Anwender trotzdem alle aktiven Inhalte nutzen und beliebige Daten einsehen kann. Drucken und Datentransport unterstützen den Anwender vollautomatisch. Das standardmässige Zurücksetzen der remote controlled Umgebung eliminiert eventuell eingebrachte kritische Veränderungen vor dem nächsten Start. Individualisierung / Personalisierung der remote controlled Session für den angemeldeten User lässt sich über das User Profil erzielen. Zufriedene Anwender, die alles eigenständig tun können ohne Gefährdung der internen Systeme schaffen effiziente IT-Umgebungen.