Provaia

Sicherheitsschleuse für mobile Datenträger

PRESENSE Technologies GmbH

Q4/2011

Warum brauchen wir eine Provaia?

Durch die Professionalisierung der Untergrund-Ökonomie, nehmen die Angriffe auf die Informationstechnik von Behörden, Unternehmen und Bürgern stetig zu. Neben der Internetkriminalität steigt auch die Anzahl von Cyber-Attacken, deren Ziele – zum Teil politisch motiviert – in der Sabotage oder Spionage liegen. Mobile Datenträger und manipulierte Dokumente sind dabei aktuelle Angriffsvektoren, bei denen die üblichen Schutzmaßnahmen an ihre Grenzen stoßen. Dies wurde erstmals durch die Schäden von „Conficker“ aufgezeigt. Mit „Stuxnet“ – von Experten als Cyber-Waffe bezeichnet – sind kaskadierende Effekte möglich, die kritische Infrastrukturen komplett lahmlegen können.

Durch die allgegenwärtige Verfügbarkeit von USB-Speichermedien oder Speicherkarten, wurden diese schleichend zu festen Bestandteilen von Arbeitsabläufen und häufig auch beim Datenaustausch mit Dritten. Dies führt zu einer unbedarften Handhabung, die Gefahr wird nicht mehr wahrgenommen, so dass selbst in besonders sensiblen und daher vom übrigen Netzwerk getrennten IT-Systemen mobile Datenträger zum Datentransfer genutzt werden.

84% aller Unternehmen sind Cyber-Angriffsopfer

Quelle http://www.crn.de/security/artikel-91065.html

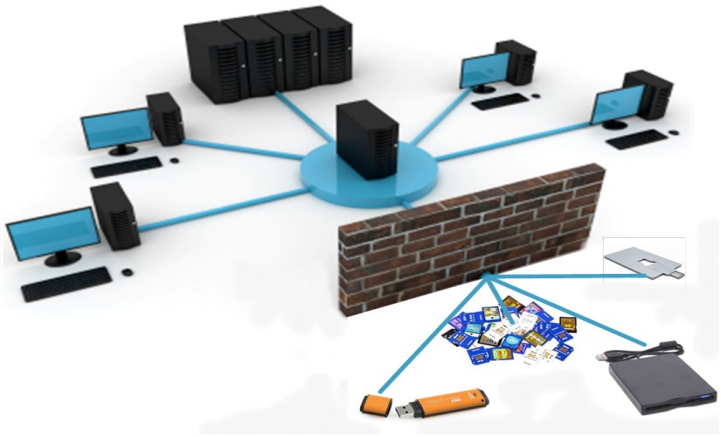
Trend zu USB-Würmern - Jeder vierte Virus kommt zu Fuß

Quelle http://www.spiegel.de/netzwelt/web/0,1518,714776,00.html

Die Vorfälle aus der jüngsten Vergangenheit zeigen deutlich, dass jeder PC-Arbeitsplatz ein potentielles Einfallstor für Schadsoftware darstellt. Sicherheitsmaßnahmen, die unter dem Begriff „Endpoint Security“ zusammengefasst werden, verringern zwar das Risiko, können aber nicht alle Angriffsvektoren abdecken. Ist eine Schadsoftware erst einmal auf einem Endgerät, dann steht einer Ausbreitung in einem Netzwerk nicht mehr viel im Weg. In sensiblen Bereichen ist es daher unverantwortlich, Datentransfers ohne Perimeterschutz vorzunehmen. Schutzmaßnahmen allein am Endgerät sind - auch im Hinblick auf zukünftige Angriffsvektoren – unzureichend.

Sauber getrennt, sicher verbunden!

Ein Lösungsansatz für diese Problematik ist die Sicherheitsschleuse **Provaia**. Die Datenträgerschleuse der PRESENSE Technologies GmbH unterbindet wirkungsvoll die Verbreitung von Schadsoftware. **Provaia** ist eine hoch gesicherte Appliance, durch die eine Sicherheitszone (Perimeter) im Vorfeld eines Netzwerkes realisiert wird, in der mobile Datenträger gefahrlos geprüft und gereinigt werden können.



Provaia wird als Kiosk-System mit Touchscreen ausgeliefert und stellt eine vollständig gekapselte und einfach zu bedienende Oberfläche bereit.

<u>Diese „Firewall“ für mobile Datenträger stellt folgende Funktionen zur Verfügung:</u>

- Überprüfen von Datenträgern mit mindestens *zwei verschiedenen Antivirus-Scannern* auf Schadprogramme (Alternativ sind auch weitere/andere AV-Scanner erhältlich)
- Erkennen und ggf. Deaktivieren von Autorun- und Autoplay-Funktionen
- Erkennen und ggf. Löschen von potenziell schadhaften Dateien
- Entfernung von aktiven und nicht sichtbaren Inhalten aus Dokumenten
- Konvertierung von gebräuchlichen Dateiformaten in sichere Formate (z.B. PDF/a)
- Import und Export von geprüften/konvertierten Dateien auf mobile Datenträger oder Netzlaufwerke
- Sicheres Löschen von mobilen Datenträgern
- Unterstützung von TrueCrypt-Containern und Krypto-USB-Sticks

Wie kann Provaia eingesetzt werden?

Es sind eine Vielzahl unterschiedlicher Einsatz-Szenarien für **Provaia** denkbar.

Primär natürlich an Stellen, wo ein Datentransfers zwischen Bereichen mit unterschiedlichen Sicherheitsniveaus vorgenommen werden sollen; einige Beispiele:

- **Allgemeines Prüfterminal in Selbstbedienung**

  Ein frei zugängliches **Provaia**-System kann im Eingangsbereich oder im Foyer von Mitarbeitern oder Besuchern bei Bedarf zur Prüfung von Wechselmedien genutzt werden, die sie erhalten haben, oder an Dritte weitergeben möchten. Damit wird ein Beitrag zur Sensibilisierung der Mitarbeiter erbracht und Verantwortlichkeit präsentiert. Die Bedienung erfordert kein IT-Wissen und keine aufwändigen Schulungen, womit die IT-Mitarbeiter (Administratoren) entlastet werden.

- **Alltägliche Nutzung am Arbeitsplatz**

  Provaia kann, ähnlich einem Arbeitsgruppen-Drucker, von den Mitarbeitern einer Abteilung gemeinsam im Rahmen der täglichen Verwendung von Wechselmedien genutzt werden. Nach einer Authentifizierung an der Schleuse können Mitarbeiter Dateien direkt in Ihre Arbeitsverzeichnisse importieren. Eine Nutzung von mobilen Datenträgern am Arbeitsplatz-PC ist nicht mehr erforderlich. Der Benutzer wird auf konforme Arbeitsabläufe beschränkt; auch entlang komplexer Verarbeitungsabläufe. Unterschiedliche Komponenten und Software-Bausteine (Virenscanner, Datei-Konverter, usw.) werden in einer einheitlichen Verarbeitungskette integriert.

- **Nutzung im Rahmen einer Zugangskontrolle**

  Eine Platzierung im Zugangsbereich eines sensitiven Bereiches (z.B. Rechenzentrum oder Produktionssteuerung) ermöglicht - selbstständig oder unter Aufsicht von Sicherheitspersonal - die Prüfung von einzubringenden mobilen Datenträgern auf Schadsoftware. Im Kontext mit Besucher-Management-Systemen können damit Prozesslücken geschlossen werden.

- **Daten-Austausch mit externen Stellen, Kunden oder Publikumsverkehr**

  Bei Organisationen, die regelmäßig Daten über mobile Datenträger von Dritten entgegennehmen oder an diese versenden, kann **Provaia** an zentraler Stelle (Poststelle, Sekretariat usw.) zur schnellen, normierten und protokollierten Prüfung von Medien verwendet werden und eine „Quer-Infektion“ von nacheinander geprüften Medien verhindern.

  Dies dürfte z.B. bei der Annahme von Kundenaufträgen (beispielsweise bei Druckereien, Copyshops, im Verlagswesen oder im Gesundheitswesen) der Fall sein.

- **Zertifizierte IT / SCADA-Systeme**

  Im industriellen Umfeld, beispielsweise in der Automatisierungstechnologie und bei leittechnischen Systemen, werden zertifizierte IT-Systeme eingesetzt, bei denen keine zusätzliche Software installiert werden darf. Müssen Daten auf solche IT-Systeme transferiert werden, muss eine Überprüfung der mobilen Datenträger im Vorfeld vorgenommen werden. Dies gilt ebenso in der Medizintechnik und allgemein in sicherheitskritischen Umgebungen.

Vorteile des Provaia Ansatzes

Gegenüber der Prüfung mobiler Datenträger durch einen Administrator oder bei Verwendung eines einfachen Scan-PCs bietet der Ansatz von **Provaia** eine Reihe von attraktiven und sicherheitstechnischen Vorteilen:

- **Sichere Plattform**

  Provaia setzt auf einen speziell gehärteten und minimalisierten Betriebssystem-Kern auf Basis von openSUSE Linux. Durch ein nicht beschreibbares Bootmedium ist eine Kompromittierung des Systems ausgeschlossen. Eine derartige Absicherung ist auf einem Arbeitsplatz nicht möglich, da dieser individuell verwendbar bleiben muss.

- **Umfangreiche Prüfungen**

  Die Schleuse kann umfangreichere Prüfungen, Säuberungen und Datenkonvertierungen vornehmen, da umfangreiche, spezialisierte Software vorgehalten werden kann, was auf einem Arbeitsplatz-PC nicht praktikabel wäre.

- **Schutz der Endsysteme**

  Der Arbeitsplatz des Benutzers oder die Industrieanlage erhält nur die bereits geprüften Daten, und kommt mit einem möglicherweise bösartigen Speichermedium nicht in Berührung. Angriffe auf Ebene des USB-Protokolls, der Dateisystem-Metadaten sowie auf Betriebssystemdienste (Autostart, Icon-Interpretation, Datei-Vorschau) sind ausgeschlossen.

- **Komfortable Touchscreen-Bedienung**

  Die Bedienung erfordert kein IT-Wissen und keine Schulungen, jeder Benutzer kann mobile Datenträger in Selbstbedienung prüfen und säubern. Komplexe Verarbeitungsabläufe (Virenscanner, Datei-Konverter, Inhalts-kontrolle, Schnittstellenkontrolle usw.) werden zu einer einheitlichen und sicherheitskonformen Verarbeitungs-kette zusammengeführt. Damit wird eine hohe Benutzerakzeptanz erreicht.

- **Zentrale Kontrolle / Protokollierung**

  Die Schleuse als zentraler Durchgangspunkt ermöglicht ein zentrales Berichtswesen und eine zentrale Quarantäne. Auftretende Probleme können einfacher erkannt und behoben werden. Für das IT-Sicherheitsmanagement werden wichtige Kennzahlen geliefert.

- **Flexibilität**

  Die **Provaia**-Management-Software bietet eine Vielzahl von Konfigurationsmöglichkeiten, die über einen Webbrowser administriert werden können. Durch eine individuelle Integration in die vorhandene Infrastruktur, kann **Provaia** optimal an den Sicherheitsbedarf einer Organisation angepasst werden. Ebenso ist eine Interaktion mit weiteren Sicherheitssystemen möglich.

- **Qualitätsgesicherte Updates**

  IT-Systeme zur Abwehr von Schadprogrammen müssen kontinuierlich gepflegt werden, nur durch aktuelle Programmversionen und die der Installation von sicherheitsrelevanten Updates, kann eine dauerhafte Sicherheit gewährleistet werden. Daher wird jedes Update umfangreichen Tests im Labor unterzogen, bis es zum Download freigegeben wird. Die Qualitätssicherung umfasst auch die AV-Signaturen.

- **„Plug-and-Protect“**

  maximal 2 Kabel anschließen (Strom und ggf. Netzwerk), Live-CD (erstellt mittels Management-system) einlegen, einschalten – **Fertig!**

...und Stuxnet, Conficker & Co. bleiben draußen!

Weitere Informationen erhalten Sie durch: