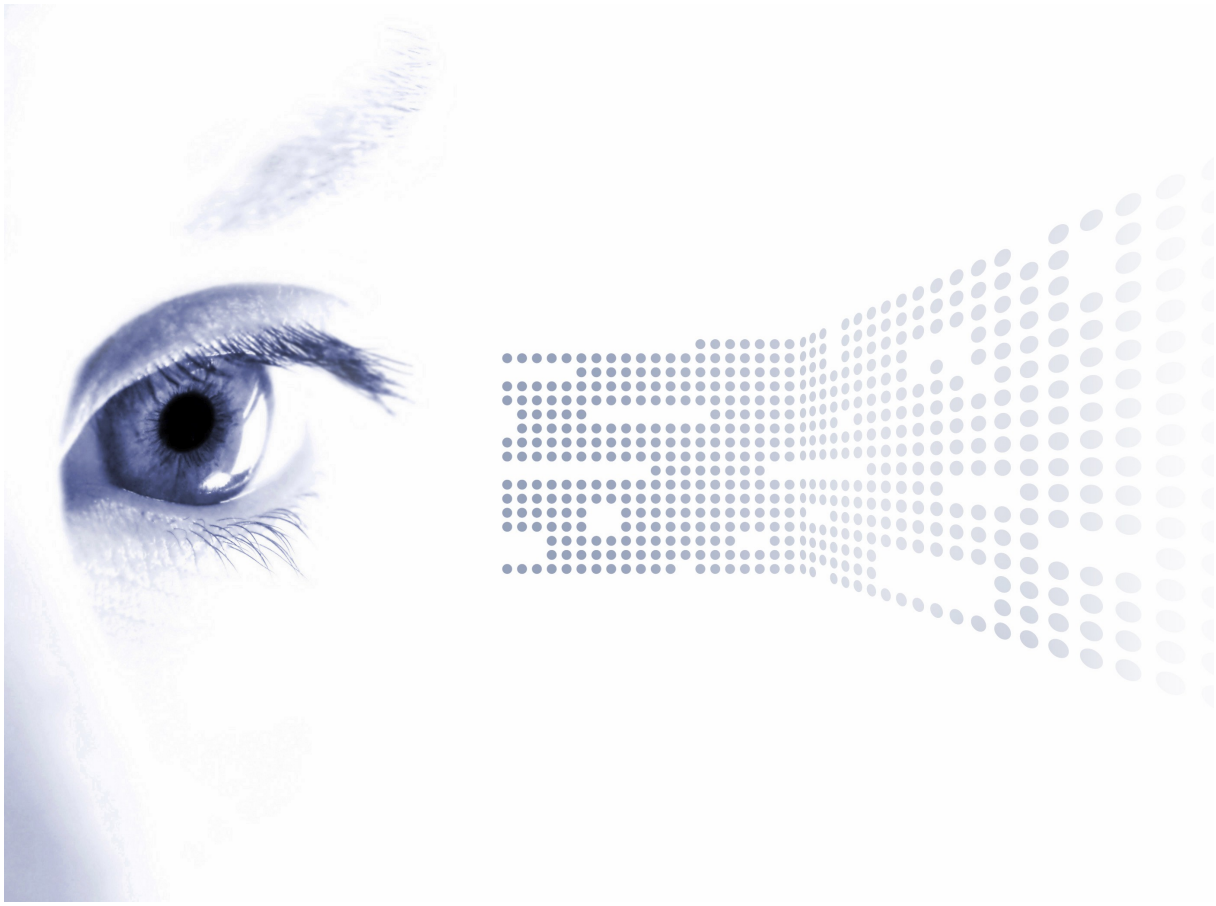


Sicherheitsrisiko

mobile Datenträger

Version 1.2, April 2011

PRESENSE Technologies GmbH
Sachsenstr. 5
20097 Hamburg

E-Mail: info@pre-sense.de
Internet: www.pre-sense.de

Alte und neue Angriffsvektoren

Die Bedrohungen für Informationsinfrastrukturen durch bösartige Software nehmen weiterhin zu. Neben der Häufigkeit der Angriffe steigen insbesondere deren technische Komplexität sowie die pro Schadprogramm auftretende Anzahl an Varianten stark an. Die hohe Anzahl der Schadprogramme lässt die Dimension der Untergrund-Ökonomie erahnen. Es geht hier um harte wirtschaftliche Interessen, so dass die Professionalisierung der Internetkriminalität stark angestiegen ist. Es wird inzwischen die traditionelle Wertschöpfungskette abgedeckt; per Internet kann Schadsoftware für jeden Zweck - auf individuelle Anforderungen zugeschnitten - beauftragt werden. Und neben breit gestreuten Angriffen mit dem Ziel, Botnetze für Spam-Verteilung oder DDoS-Angriffe aufzubauen, sehen sich Unternehmen und Behörden immer häufiger auch gezielten Angriffen ausgesetzt, deren Absichten in der (Wirtschafts-)Spionage oder auch politischen Motiven liegen.

Vor gut zwei Jahren erfolgte die Verbreitung von Schadprogrammen zumeist über Netzwerke und deren Dienstleistungen (z.B. per E-Mail). Diese Angriffsvektoren sind auch weiterhin problematisch, erheblich brisanter sind derzeit jedoch Gefährdungen, die allein durch das Surfen im Internet - Stichwort Drive-by-Download - und durch den Austausch von Informationen über mobile Datenträger gegeben sind. Beiden Angriffsvektoren ist gemeinsam, dass traditionelle Sicherheitsmaßnahmen nur unzureichend Schutz bieten.

Eine offene Flanke bei Unternehmen und Behörden ist häufig durch die Nutzung von mobilen Datenträgern gegeben. Dieser Aspekt ist nachhaltig durch die Kollateralschäden des Internetwurms „Conficker" in den Vordergrund getreten. Dieser „Wurm" hat in den industrialisierten Staaten erst seine Schadwirkung entfalten können, nachdem er sich auch über mobile Datenträger verbreiten konnte. Die originäre Verbreitungsmethode über das Internet hat Unternehmen zunächst nicht getroffen, da der Perimeterschutz ausreichend war. Schadsoftware, die sich über mobile Datenträger verbreitet, stellt derzeit die populärste Malware-Kategorie dar, wie die Top10-Listen der AV-Hersteller belegen.

Seit Conficker nutzen immer mehr Schadprogramme neben Web-Downloads oder infizierten E-Mails auch Wechseldatenträger wie USB-Sticks oder Speicherkarten zur Infektionsübertragung zwischen Systemen. Derartige Medien haben inzwischen eine weite Verbreitung gefunden und wurden schleichend zu einem festen Bestandteil von Arbeitsabläufen in vielen Unternehmen und häufig auch beim Datenaustausch mit Dienstleistern oder Kunden. Selbst für den Datenaustausch mit besonders sensiblen und daher vom übrigen Netzwerk und Internet getrennten Systemen werden Wechseldatenträger zum Im- und Export von Daten genutzt und ermöglichten so „Stuxnet" Zugang zu kritischen Industrieanlagen.

Noch einmal davongekommen – aber wie lange geht es noch gut?

Durch den Conficker-Wurm wurden Anfang 2009 massive Störungen bei den Streitkräften in mehreren EU-Mitgliedsstaaten verursacht, wodurch die Aufgabenerfüllung nicht mehr gewährleistet war bzw. stark eingeschränkt wurde. Mit „Stuxnet" - von Experten als Cyber-Waffe bezeichnet – sind kaskadierende Effekte möglich, die kritische Infrastrukturen komplett lahmlegen können. Noch ist unklar, woher „Stuxnet" stammt. Klar ist hingegen, dass der Code nicht konzipiert wurde, um Geld zu stehlen oder an persönliche Daten zu gelangen. „Stuxnet" wurde mit fundiertem Wissen um die Industrieanlagensteuerung mit SCADA-Technologie (Supervisory Control and Data Acquisition) entwickelt und verwendete vier bis dahin unbekannte Windows-Sicherheitslücken, sogenannte Zero-Day-Exploits. In sensiblen Bereichen ist es daher unverantwortlich, Datentransfers ohne Perimeterschutz vorzunehmen. Schutzmaßnahmen allein am Endgerät sind - auch im Hinblick auf zukünftige Angriffsvektoren – unzureichend.

Worin bestehen die Gefahren?

Mit der Markteinführung der ersten USB-Sticks, auch Memory-Sticks oder USB-Speicher genannt, hat sich der Datentransport und der Informationsaustausch grundlegend verändert. USB-Speicher bieten eine kosteneffiziente Möglichkeit praktisch alle Arten von Informationen zu speichern und zu transportieren. Digitale Kameras und Mobiltelefone haben diesen Siegeszug ebenfalls massiv gefördert. Inzwischen sind die Preise für USB-Speicher soweit gesunken, dass diese verstärkt auch als Werbeartikel zum Einsatz kommen. Neben dem Firmenlogo auf dem Gehäuse, können zusätzlich Verbraucherinformationen aufgespielt werden und die den Nutzeffekt verstärken.

Die allgegenwärtige Verfügbarkeit und die unbedarfte Nutzung von USB-Speichermedien muss als ein zentrales Problem betrachtet werden!

Wer schnell ein paar Urlaubsbilder für den Fotoausdruck oder Dokumente zur Vervielfältigung für den Copyshop auf einen USB-Speicher kopiert, riskiert eine

Infizierung des Speichermediums beim Dienstleister. Diese Vorgehensweise kann im privaten Bereich möglicherweise toleriert werden, im Rahmen von dienstlichen Aufgabenwahrnehmung ist dies jedoch nicht akzeptabel. Auch muss ein „DualUse", also die gemeinsame private und dienstliche Nutzung eines mobilen Datenträgers untersagt werden.

Solange nicht nachvollzogen werden kann, wo beispielsweise ein USB-Stick angeschlossen war und in welchem sicherheitstechnischen Zustand die betreffenden Systeme waren, birgt die Nutzung ein Risiko. Arbeitsräume in Hochschulen, Terminals in einem Internet-Cafe, selbst Präsentationssysteme bei Messen und Tagungen eignen sich hervorragend zur Übertragung unerwünschter Software.

Gerade bei der Verwendung des Betriebssystems Windows, entfalten maliziöse USB-Speichermedien ihr größtes Schadpotential. Um die Handhabung für den Benutzer zu vereinfachen, wird von Windows die so genannte AutoStart-Funktion unterstützt, durch die bei der Aktivierung eines Speichermedium automatisch Anwendungen gestartet werden. Beispielsweise kann ein Bildbetrachter gestartet werden, der die auf dem Speichermedium enthaltenen Bilddateien öffnet und auf der Benutzeroberfläche anzeigt. Eine präparierte Bilddatei könnte nun eine Schwachstelle in der Anwendung ausnutzen, um ein Schadprogramm auf dem Computer zu installieren, auch könnte direkt Schadcode ausgeführt werden. Der Phantasie der Angreifer sind hier wenig Grenzen gesetzt.

Dieser Angriffsvektor hat „Conficker" zum Erfolg verholfen. Die Deaktivierung dieser Funktion bereitete dem Hersteller einige Mühe und ist bislang auch nur für USB-Geräte möglich. Bei CD-Rom oder DVD ist dies nicht möglich; so dass eine besondere Gefahr von U3-Speichermedien ausgeht, hier wird dem Betriebssystem eine Partition auf dem Datenträger als CD-ROM präsentiert, so dass getroffene Schutzmaßnahmen wieder umgangen werden können. Im Juli wurde eine neue Schwachstelle im Windows Betriebssystems bekannt, die in Verbindung mit einem infizierten mobilen Datenträgern, zu einer - vom Benutzer unbemerkten - Installation von Schadsoftware führen kann. Neben dem Einstecken des USB-Sticks ist keine weitere Benutzerinteraktion erforderlich.

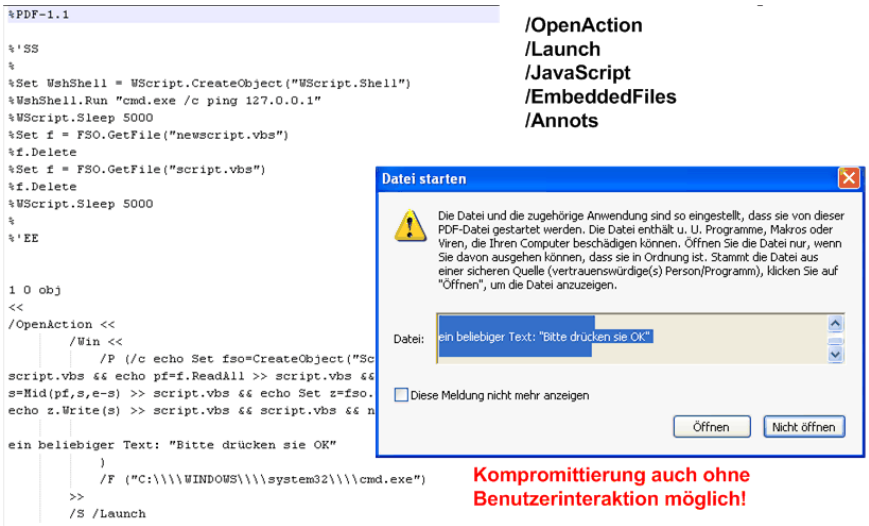
Gefährliche Inhalte oder gefährliche Dokumentenformate?

Selbstverständlich birgt auch der Inhalt von Dokumenten Gefahren, diese sind jedoch nicht spezifisch für mobile Datenträger. Nicht nur in Webseiten, sondern auch in Office-Dokumenten können aktive Inhalte (Makros, ActiveX-Elemente, Scripte, …) eingebettet sein, die eigentlich dem Benutzer die Arbeit erleichtern sollen. Einem Angreifer eröffnen diese aktiven Inhalte wiederum vielfältige Möglichkeiten, einen Rechner zu kompromittieren, da die Ausführung der Inhalte wie ein lokales Programm und zumeist unbemerkt vom Anwender erfolgt.

Für den Austausch von Dokumenten hat sich im letzten Jahrzehnt das portable Dokumentenformat (PDF) etabliert. Eine offen gelegte Spezifikation, die Verfügbarkeit von Anwendungen für alle gängigen Betriebssysteme und die einfache Integration in beliebte Webbrowser sind eine Reihe von Gründen für die Beliebtheit des Formats. Auch wurde PDF lange Zeit als ein „sicheres" Format betrachtet, obwohl schon vor Jahren Möglichkeiten diskutiert wurden, mit denen es

möglich sein sollte Kommandozeilenbefehle auszuführen. Es handelt sich hier um so genannte Leistungsmerkmale, nicht um Schwachstellen.

Die in der Akzeptanz begründete hohe Verbreitung von Anwendungen, mit denen PDF-Dokumente erzeugt und dargestellt werden können, führt zu einer ähnlichen Situation, wie sie bei den Betriebssystemen zu beobachten ist; der Marktführer wird zum primären Ziel der Angreifer.



Die gewünschte Universalität eines PC-Arbeitsplatzes führt in ein Dilemma. Eine Vielzahl von Geschäftsprozessen wurde bewusst oder schleichend modifiziert, weil z.B. durch mobile Datenträger Medienbrüche verhindert werden können. Damit behindern Anforderungen an die Arbeitsplatzumgebung die Umsetzung von Maßnahmen, die aus Gründen der Sicherheit dringend erforderlich wären. Die Verwendung von mobilen Speichermedien in verschiedensten Produkten der Informationstechnologie ist Realität, ein striktes Verbot wäre kontraproduktiv, da viele Prozesse umständlicher gestaltet werden müssen, was sich negativ auf die Benutzerakzeptanz auswirken dürfte.

Wir haben doch schon Firewall, Endpoint Security, DeviceControl, …

Warum reicht das nicht aus?

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.

- Ein **Virenscanner** ist nur so gut, wie seine Aktualität. Aber bei der Menge der täglich produzierten und in Umlauf gebrachten Schadsoftware ist es illusorisch zu glauben, dass jede Gefahr gebannt werden kann. Die Erkennungsrate bei bekannter Schadsoftware liegt bei 20 aktuellen Produkten zwischen 81,8% und 99,3%. Und was ist mit unbekannter Schadsoftware?
- Eine umfassende **Kontrolle der Schnittstellen** ist ein konsequenter Schritt, um die Verwendung von mobilen Datenträgern zu steuern und so einem unerwünschten Abfluss von Informationen vorzubeugen. Das Eindringen von Schadsoftware kann aber nur bedingt unterbunden werden, da hier der mobile Datenträger und nicht dessen Inhalt im Vordergrund steht. Und was ist mit Krypto-USB-Sticks?

- Eine **lokale Firewall** soll primär gegen Netzwerkangriffe schützen, befindet sich die Schadsoftware bereits im Netz, ist der Nutzwert gering, da zur Verbreitung zumeist Schwachstellen in freigegebenen Netzwerkprotokollen ausgenutzt werden.

Im Idealfall kann mit Endpoint-Security das Sicherheitsniveau deutlich gesteigert werden, aber man darf nicht vergessen, dass diese Maßnahmen die letzte Bastion und einzige Barriere gegen das Eindringen digitaler Schädlinge über mobile Datenträger sind. Wie im Begriff Endpoint-Security bereits verankert, wir sprechen vom Endgerät oder Arbeitsplatz-PC. Ein multifunktionales IT-System für beliebige Aufgabenstellungen, es sind daher unzählige Softwarepakete installiert mit einer unbekannten Anzahl von Schwachstellen. Dies kann zu unerwünschten Seiteneffekten führen, die die getroffenen Sicherheitsmaßnahmen unbemerkt neutralisieren können.

- Welche Auswirkungen hatte der letzte Patch?
- War die letzte Aktualisierung erfolgreich?
- Wann kommt der nächste „Zero-Day-Exploit"?
- Darüber hinaus können Sie auf die Phantasie und den Ideenreichtum der Benutzer vertrauen!

Ein ungeprüfter mobiler Datenträger gehört nicht ans Endgerät!

Ist eine Schadsoftware erst einmal auf einem Endgerät, dann steht einer Ausbreitung in einem Netzwerk nicht mehr viel im Weg.

Auch hier hat uns Conficker vorgeführt, wie verwundbar unsere IT-Infrastrukturen sind, wenn der Perimeterschutz durchbrochen werden konnte. Die Infizierung nur eines Endgeräts war ausreichend, um bei den betroffenen Organisationen die IT teilweise wochenlang lahmzulegen. Eine Verbreitung kann aber auch schleichend erfolgen, wenn der Schadcode sich ausschließlich über mobile Datenträger oder Netzlaufwerke verbreitet.

Eine Anbindung an das Internet ohne eine Firewall ist undenkbar und inzwischen auch nicht mehr ausreichend. Je nach Sicherheitsanforderungen werden Dienste eingesetzt, mit denen die Kommunikation auf der Anwendungsebene analysiert („Web-Application-Firewall") und entsprechend den Vorgaben einer Sicherheitsrichtlinie unterbunden werden kann. Damit wird das Risiko deutlich gesenkt, sofern es sich um bekannte Angriffsmuster handelt.

Sauber getrennt, sicher verbunden!

Für mobile Datenträger ist ein Perimeterschutz oder eine Sicherheitsschleuse mehr als überfällig, wie die Ereignisse der jüngsten Vergangenheit schmerzvoll aufgezeigt haben. Angreifer nehmen das Angebot gerne an, mobile Datenträger in Verbindung mit Schwachstellen in Microsoft Betriebssystemen und anfällige PDF-Reader sind die Top-Angriffsvektoren, wie den Berichten der Hersteller von Antivirus-Produkten zu entnehmen ist. Ein erster Ansatz in diese Richtung wurde mit Scan-PCs unternommen, an denen mobile Datenträger durch die Nutzer

überprüft werden konnten. Da zumeist dasselbe Betriebssystem wie bei den Arbeitsplätzen verwendet wurde, ist das Sicherheitsniveau vergleichbar mit eingesetzten Endpoint-Security Lösungen, also verwundbar durch neue Angriffsmethoden. Bedingt durch das Fehlen von Alternativen, muss ein sicherer Im- und Export von Daten in sensiblen Bereichen durch einen Administrator realisiert werden, was aus verschiedenen Gründen suboptimal ist.

Als Konsequenz der Erfahrungen mit Angriffen über mobile Datenträger hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Konzept des Perimeterschutz für mobile Datenträger weiterentwickelt und in Auftrag gegeben. Unter der Projektbezeichnung „Janus" steht den Bundesbehörden ein Produkt zur Verfügung, durch das aktuelle Angriffsvektoren bzw. Verbreitungswege von Schadsoftware wirkungsvoll unterbunden werden können. Mit Provaia wird dieser Schritt konsequent weitergeführt - ein auf die Prüfung und sichere Handhabung von Daten auf Wechselmedien zugeschnittenes und gehärteten Spezialsystems. Provaia wird zusammen mit einer abgestimmten Hardware-Plattform in Form eines Kiosk-Systems mit Touchscreen ausgeliefert. Bedienelemente wurden von vornherein entsprechend ausgelegt und eine Bildschirmtastatur integriert, so dass eine komfortable und sichere Bedienung möglich ist. Die Auslegung des Systems mit entsprechender Systemleistung (insbesondere Hauptspeicher) garantiert dem Benutzer schnelle Reaktionszeiten sowie schnelle Arbeitsabläufe. Neben der Dokumentation stehen für Provaia detaillierte Informationen und Vorlagen für die Einbindung in ein IT-Grundschutzkonzept bereit, die die Integration dieses Sicherheitsdienstes in bestehende Sicherheitskonzepte vereinfachen.

Provaia wird von einer bootbaren-CD gestartet und stellt eine vollständig gekapselte und einfach zu bedienende Oberfläche bereit. Diese „Firewall" für mobile Datenträger stellt folgende Funktionen zur Verfügung:

- Überprüfen von Datenträgern mit mindestens *zwei verschiedenen Antivirus-Scannern* auf Schadprogramme
- 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 offene Formate (ODF, PDF oder 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

Vorteile dieses Ansatzes

Gegenüber der Prüfung mobiler Datenträger am Arbeitsplatz oder der Verwendung eines einfachen Scan-PCs bietet der Ansatz von Provaia eine Reihe von attraktiven und sicherheitstechnischen Vorteilen:

- Sichere Plattform

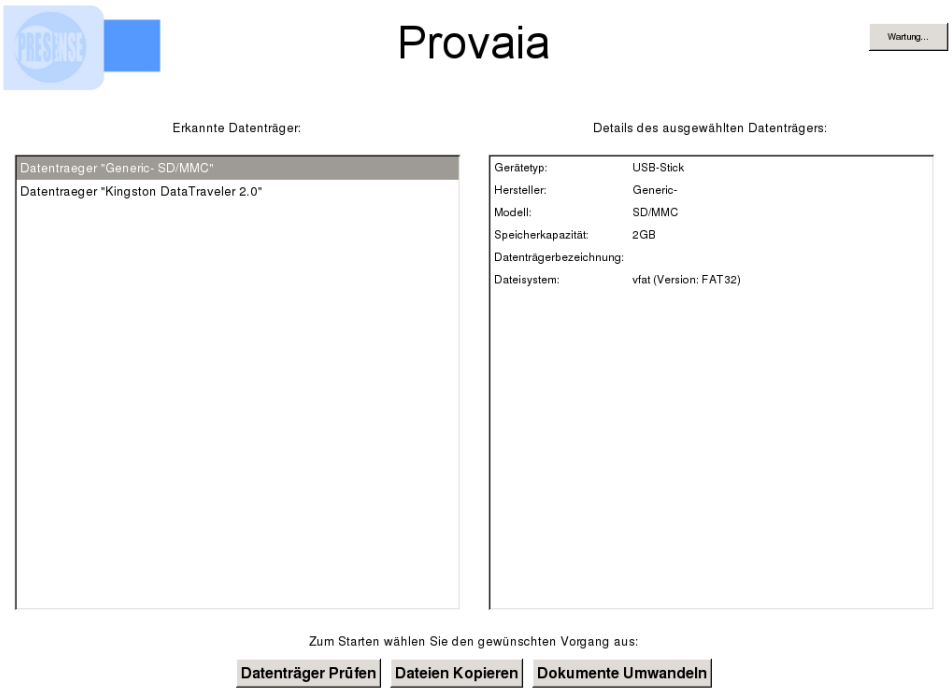
  Die Schleuse setzt auf einem speziell gehärteten und minimalisierten Betriebssystem-Kern auf. Alle nicht direkt zur Diensterbringung notwendigen Systemkomponenten wurden entfernt, Rechte getrennt und minimalisiert. Eine derartige Absicherung ist auf einem Arbeitsplatz nicht möglich, da dieser individuell verwendbar bleiben muss.

  Da es sich um eine Live-CD handelt, kann die Vertrauenswürdigkeit zwischen zwei Prüfvorgängen jederzeit durch einen Neustart des Systems sichergestellt werden.

  Der Arbeitsplatz des Benutzers 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 für angeschlossene Medien (Autostart, Icon-Interpretation, Datei-Vorschau) sind ausgeschlossen.

- Arbeitsabläufe

  Unterstützung des Benutzers und weitgehende Automatisierung machen die Prüfungen schneller und komfortabler.



  Der Benutzer wird auf sicherheitskonforme Arbeitsabläufe beschränkt; auch entlang komplexer Verarbeitungsabläufe. Unterschiedliche Komponenten und Software-Bausteine (Virenscanner, Datei-Konverter, Inhaltskontrolle, Schnittstellenkontrolle usw.) werden zu einer einheitlichen Verarbeitungskette integriert.

Zugriffe des Benutzers auf das System und die von dort erreichbaren Netzwerkdiensten werden auf auf notwendige bzw. akzeptable Bereiche beschränkt.

Automatische Hintergrund-Aktionen wie Logging, Berichte und Quarantäne.

- 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 (Return of Investment).

  Datenkonvertierung in vertrauenswürdige Formate, sowie Verifikation und Normalisierung bieten ein deutlich höheres Sicherheitsmaß als es ein Virenscanner ermöglicht und insbesondere eine Abwehr bisher unbekannter Angriffe.

  Open Source ermöglicht den Einsatz von speziell für Sicherheitszwecke instrumentierter Versionen von Werkzeugen wie zum Beispiel von Office-Programmen oder PDF-Konvertern.

- Aktualität der Prüfungen und Metadaten

  Die Anzahl der Systeme, auf denen die sicherheitsrelevanten Konfigurationen und Datenbestände aktuell gehalten werden müssen, sinkt stark. Die Aktualisierung der Prüfumgebung kann nicht durch Abhängigkeiten anderer auf dem System installierter Softwarepakte verhindert werden.

- Einbindung von nicht-Mitarbeitern und nicht-vertrauenswürdigen Benutzern bzw. der Öffentlichkeit

  Arbeitsplatz-Scans ermöglichen nur Mitarbeitern die Prüfung von mobilen Datenträgern, ausgezeichnete Scan-PCs bieten nicht genug Einschränkungen bei Systemzugang und Wahl von Arbeitsabläufen. Diese sind zumeist komplex in Bedienung und Interpretation von Dialogen. Die Schleuse erfordert kein IT-Wissen und keine Schulungen und erlaubt so einer größeren Personengruppe, mobile Datenträger in Selbstbedienung konform zur Sicherheitsrichtlinie zu prüfen und zu säubern.

- Zentrale Kontrolle / Protokollierung

  Die Schleuse als zentraler Durchgangspunkt ermöglicht ein zentrales Berichtswesen und eine zentrale Quarantäne. Auftretende Probleme können einfacher erkannt und behoben werden.

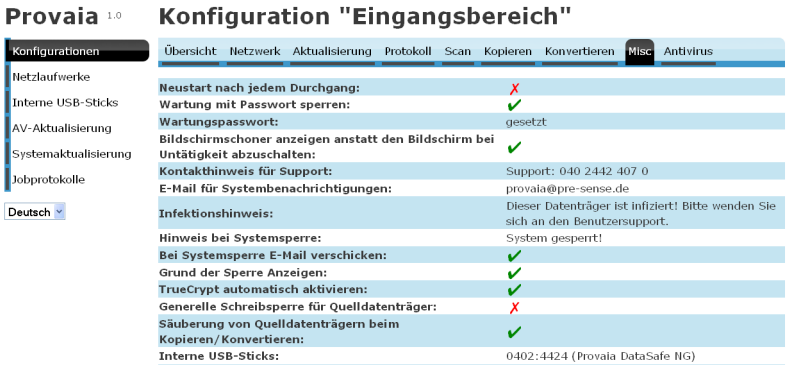
Zwar hat die Verwendung einer Datenschleuse im Gegensatz zur Prüfung am Arbeitsplatz für den Benutzer den Nachteil, dass er sich zur Provaia-Appliance begeben muss. Dieser wird jedoch durch die dort vorhandene Automatisierung der Abläufe ausgeglichen.

Management der Appliance(s)

Das Provaia-Management-System wird als Add-On-CD für ein Linux-System auf Basis von OpenSuse ausgeliefert und kann komfortabel über einen Webbrowser administriert werden.

Das Provaia-Management-System bietet eine Vielzahl von Konfigurations-möglichkeiten, um die Appliance optimal dem Sicherheitsbedarf einer Organisation anzupassen:

- Individuelle Anpassung an die Infrastruktur
- Verwaltung beliebig vieler Provaia-Appliances
- Reporting, Logging- u. Quarantäne-funktionen
- Integration in das IT-Sicherheitsmanagement



Abschließend kann von dort die für den Betrieb von Janus notwendige Live-CD jederzeit generiert werden.

Mögliche Einsatzszenarien

Es sind eine Vielzahl unterschiedlicher Einsatz-Szenarien für die Provaia-Appliances denkbar; einige Beispiele:

- Interne Nutzung

  Janus 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.

- Allgemeines Prüfterminal in Selbstbedienung

  Ein frei zugängliches Provaia-System kann von Mitarbeitern oder Besuchern bei Bedarf zur Prüfung von Wechselmedien, die sie erhalten haben, oder an Dritte weitergeben möchten.

- Nutzung im Rahmen einer Zugangskontrolle

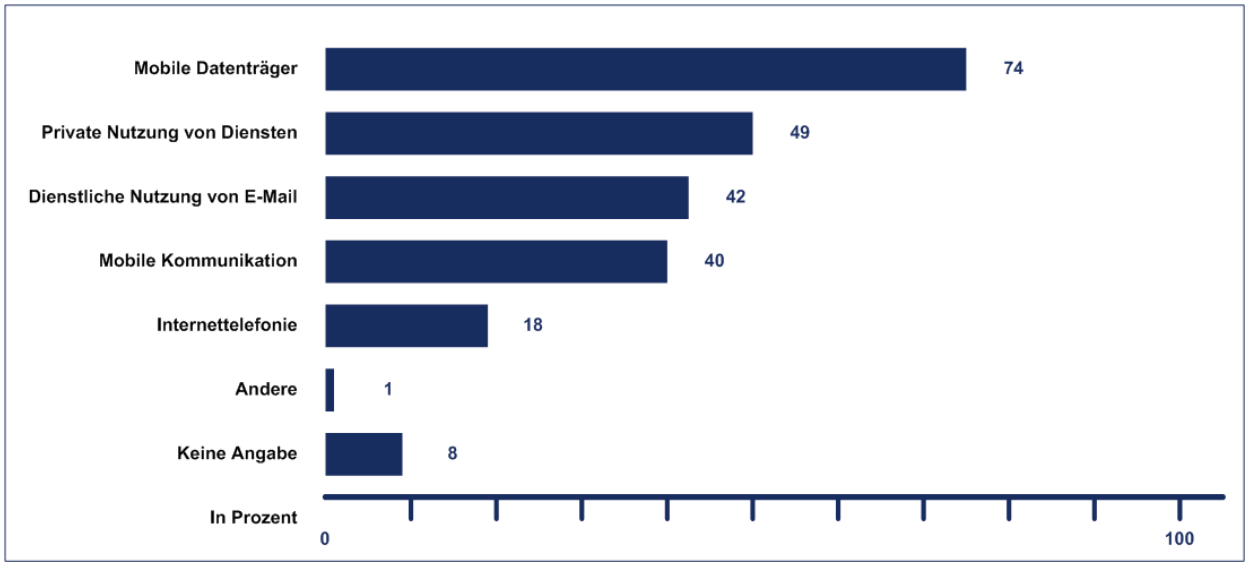
  Eine Platzierung im Foyer eines Gebäudes oder im Zugangsbereich eines sensitiven Bereiches (z.B. Rechenzentrum) ermöglicht selbstständig oder unter Aufsicht von Sicherheitspersonal die Prüfung von einzubringenden Wechselmedien auf Schadsoftware oder den direkten Import von Daten in einen dafür vorgesehenen Bereich im Netzwerk.

- Daten-Austausch mit externen Stellen oder Publikumsverkehr

  Organisationen, die regelmäßig Wechselmedien von Dritten empfangen, oder an diese senden, können Provaia-Systeme an zentraler Stelle (Betrieb, Poststelle, Sekretariat) zur schnellen, normierten und protokollierten Prüfung von Medien verwenden und eine „Quer-Infektion" von nacheinander geprüften Medien verhindern.

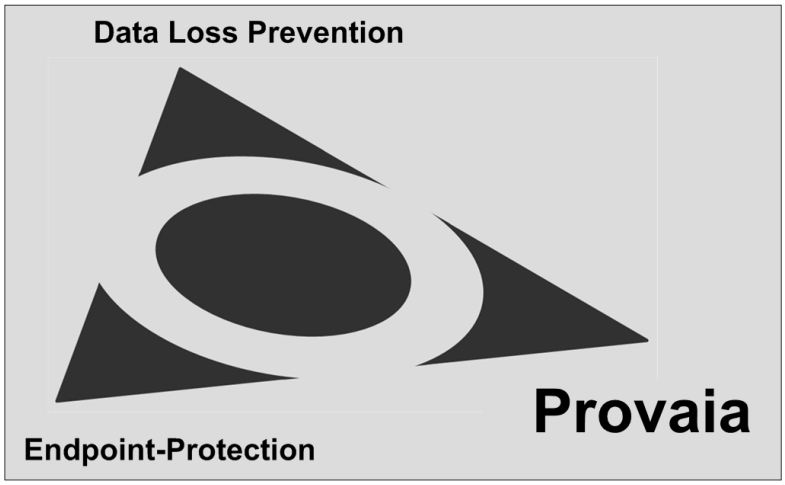
Prävention, Reaktion und Nachhaltigkeit

In einer Studie der KPMG[1] wurden Informationen zur Computerkriminalität in der deutschen Wirtschaft ermittelt und aufbereitet. Für die an der Studie beteiligten Unternehmen geht das höchste Risiko bei der Anwendung von ITK-Technologien, durch die Nutzung mobilen Datenträgern aus.



Natürlich darf an dieser Stelle nicht unerwähnt bleiben, dass der Abfluss von sensiblen Informationen aus den Unternehmen - neben den Bedrohungen durch Schadsoftware - eine sehr hohe Priorität besitzt.

Bei der Betrachtung der Sicherheitsrisiken ist es daher unerlässlich, alle Aspekte zu berücksichtigen, die durch die Verwendung von mobilen Datenträgern gegeben sind. Das IT-Sicherheitsmanagement – in Eintracht mit dem Risiko- und Compliance-Management einer Organisation - muss sicherstellen, dass bekannte Schwachstellen adressiert und letztendlich auch geschlossen werden. Provaia bietet einen innovativen Ansatz zur sicheren Handhabung von mobilen Datenträgern, der etablierte Lösungen integriert und fortschreibt.



Konformität zum Daten-schutz und Einsatz-möglichkeiten im Rahmen des Geheimschutz runden die Lösung ab.

Eine Firewall für mobile Datenträger muss als ein elementarer Baustein einer nachhaltigen IT-Sicherheitsstrategie betrachtet werden.

[1] E-Crime-Studie 2010 / Computerkriminalität in der deutschen Wirtschaft / KPMG

