Komplettlösung als Appliance

Zum sicheren und komfortablen Betrieb des JANUS-Dienstes steht ein speziell hierfür entworfenes Appliance-System zur Verfügung (siehe Titelfoto dieser Broschüre). Die Appliance verfügt über alle notwendigen Medien-Laufwerke, einen physikalischen Schutz für die Boot-DVD und andere Anschlüsse sowie einen Touchscreen zur komfortablen Bedienung. Sie kann als Wand- oder Tischgerät betrieben werden.

Wartung und Support
Wartung und Support können ausschließlich über PRESENSE bezogen werden.

Integration
Die JANUS-Software kann zusätzlich individuell an die Bedürfnisse einzelner Behörden angepasst und mit Infrastruktur integriert werden.

Bezug
Die JANUS-Appliance ist direkt bei der PRESENSE Technologies zu beziehen. Auch außerhalb der Bundesverwaltung können Software und Appliance-System als „PRESENSE PROVAIA“ von Firmen und Behörden über PRESENSE Technologies bezogen werden.

SecurITy made in Germany

Informationen

Sie haben weitere Fragen zu unseren Produkten? Nehmen Sie gerne Kontakt mit uns auf oder besuchen Sie **janus.pre-sense.de**

T +49 . 40 . 244 24 07-0
E janus@pre-sense.de

Unseren Support erreichen Sie von 9–17 Uhr (werktags, ohne Wochenenden und Feiertage).

T +49 . 180 . 1 . PRESENSE
(+49 . 180 . 1 . 773 736)[1)]
E janus-support@pre-sense.de

1) Ein Anruf kostet 3,9 Cent pro Minute aus dem dt. Festnetz. Aus Mobilfunknetzen sind abweichende Tarife möglich.

PRESENSE
IT-SICHERHEIT – BERATUNG UND LÖSUNGEN

PRESENSE Technologies GmbH
Nagelsweg 41
D-20097 Hamburg
www.pre-sense.de

T +49 . 40 . 244 24 07-0
F +49 . 40 . 244 24 07-24
E info@pre-sense.de

JANUS-Flyer DE-04-2024

JANUS
BY PRESENSE —
IT-SICHERHEIT FÜR BEHÖRDEN

Der optimale Perimeterschutz für mobile Datenträger

Anwendungsgebiete

Mit der Wechseldatenträger-Schleuse (WDS) „JANUS“ wird den Bundesbehörden ein Sicherheitsprodukt zur Verfügung gestellt, das aktuelle Risiken beim Austausch von Informationen mithilfe von Datenträgern erheblich reduziert.

Netzwerkübergänge werden mittels Perimeterschutz bereits erfolgreich überwacht. Der Import und Export von Informationen über mobile Datenträger jedoch birgt heute ein hohes Risiko für die IT-Sicherheit. Oftmals ist der Antivirus-Scanner am Arbeitsplatz die einzige Bastion, die die internen Netze vor Schadprogrammen schützt, die sich auf mobilen Datenträgern befinden.

JANUS, beispielsweise im Foyer eines Gebäudes platziert, ermöglicht den Mitarbeitern bei Betreten des Hauses die eigenverantwortliche Überprüfung von mitgeführten Datenträgern aller gängigen Typen, bevor diese am Arbeitsplatz-PC eingesetzt werden. Neben der Prüfung bietet JANUS die Möglichkeit, Datenträger vollständig zu kopieren oder unsichere Dokumente in sichere Dateiformate zu konvertieren.

Leistungsumfang

JANUS verfügt über folgende Funktionen:

- Überprüfen von Datenträgern mit mindestens zwei verschiedenen Antivirus-Scannern auf Schadprogramme
- Unterstützung für Microsoft BitLocker, TrueCrypt, VeraCrypt und verschlüsselte Archive (ZIP, ...)
- Unterstützung von Krypto-USB-Sticks, z.B. von Kanguru, Kingston, IronKey oder Blockmaster
- Erkennen und ggf. Deaktivieren von Autorun- und Autoplay-Funktionen
- Erkennen und ggf. Löschen von potentiell schadhaften Dateien
- Konvertieren von Dokumenten von gebräuchlichen Dateiformaten in die offenen Dokumentenformate ODF oder PDF
- Kopieren von geprüften/konvertierten Dateien auf andere mobile Datenträger oder auf Netzlaufwerke
- Sicheres Löschen von mobilen Datenträgern

Management-System

Das Management-System (JANUS-MS) wird als Add-On-CD für ein Linux-System auf Basis von openSUSE ausgeliefert. Damit wird die eigentliche Wechseldatenträgerschleuse, kurz WDS, als Kiosk-System über eine einfach zu bedienende Webbrowser-Oberfläche konfiguriert. Anschließend kann von dort die für den Betrieb von JANUS notwendige Live-CD/DVD jederzeit generiert werden. Das JANUS-MS bietet eine Vielzahl von Konfigurationsmöglichkeiten, die Datenträgerschleuse optimal dem Sicherheitsbedarf der Behörde anzupassen.

Live-CD/DVD (Kiosk-System)

Die mit dem JANUS-MS erstellte Live-CD/DVD wird in das Gerät, das als Wechseldatenträgerschleuse dienen soll, eingelegt. Das System bootet von CD/DVD und ist anschließend mit einer gekapselten Bedieneroberfläche betriebsbereit. Die aktuellen Virensignaturen können über das Internet (Live Update) nachgeladen werden.

Der für die Wechseldatenträgerschleuse ausgewählte PC sollte für aktuelle Linux-Versionen (openSUSE) geeignet sein. Wünschenswert ist eine Ausstattung mit leistungsfähiger, jedoch stromsparender Hardware, mindestens zwei optischen Laufwerken, einem Speicherkartenleser sowie zwei für den Anwender zugänglichen USB-Ports.