Traditionelle Antiviren-Lösungen versagen beim Schutz unternehmenskritischer SAP Anwendungen: Datei-Uploads und -Downloads bleiben ungeprüft. SAP-User und SAP Anwendungen laufen Gefahr, durch bösartige Inhalte kompromittiert zu werden.

bowbridge - Security made for SAP

bowbridge Anti-Virus ist die weltweit einzige Content Security Lösung, die von Grund auf für die besonderen Anforderungen des SAP Virus Scan Interfaces (NW-VSI) enwickelt wurde.
Sie kann nicht nur Datei-Uploads und -Downloads in SAP-Anwendungen erkennen und filtern, sondern enthält auch zahlreiche Funktionalitäten zum Schutz der SAP Anwendung vor Bedrohungen, die von traditionellen Anti-Virus Lösungen nicht als Gefahr eingestuft werden. bowbridge Anti-Virus integriert sich nahtlos in SAP Konfigurations- und Monitoring-Werkzeuge.

Virenscan-Technologie von McAfee® und Sophos®

bowbridge Anti-Virus enthält zwei Virenscan Engines zur Auswahl. Ganz gleich, ob Sie sich für die Scanning-Technologie von McAfee oder Sophos entscheiden, sie haben in jedem Fall die Gewissheit, dass die Daten in Ihrer SAP Anwendung von marktführenden Anti-Malware Engines geprüft werden.
Der integrierte ICAP-Client ermöglicht zudem alternativ oder ergänzend die hochverfügbare und lastverteilte Anbindung zentraler Netzwerk-Virenscan Dienste diverser Hersteller, wie z.B. Symantec®, Trend Micro®, Kaspersky Labs®, usw.

Schutz vor Cross-Site Scripting

Durch das Einbetten von ausführbaren Inhalten in Datei-Typen, die im Client-Browser dargestellt werden, können Angreifer auch mit Dateien Cross-Site Scripting (XSS) Angriffe ausführen. bowbridge Anti-Virus erkennt zuverlässig Cross-Site Scripting in zahlreichen Dateitypen und blockt diese gemäß der für die Anwendung definierten Security-Policy.

Aktive Inhalte

Aktive Inhalte – zum Beispiel Makros in Office Dokumenten oder JavaScript in PDF-Dateien – gelten nicht ausdrücklich als Malware und werden daher von Virenscannern nicht geblockt.
Angreifer können mit manchen aktiven Inhalten in Dateien jedoch unbemerkt Aktionen in der SAP Anwendung oder auf dem Client mit den Rechten des angemeldeten Benutzers ausführen.
bowbridge Anti-Virus verfügt über umfangreiche Filter- und Erkennungsmöglichkeiten für aktive Inhalte.

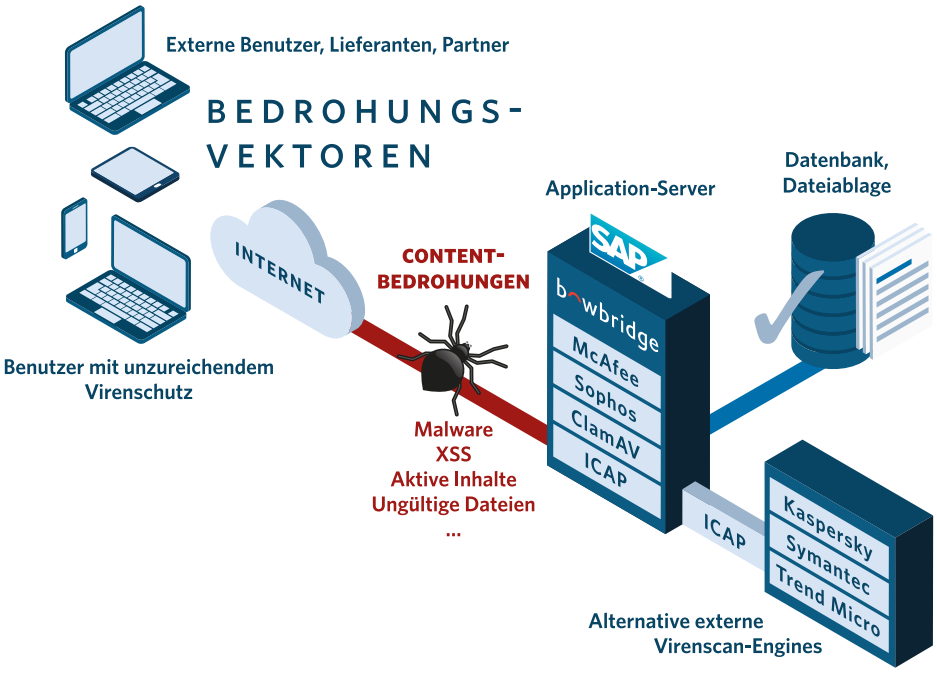
Inhaltsbasierte MIME Filter

Die SAP-eigenen Filtermöglichkeiten für Datei-Typen sind auf die Endung des Dateinamens beschränkt. Angreifer können diese Filter durch einfaches Umbenennen von Dateien umgehen und so unerwünschte Inhalte in die Anwendung hochladen.
bowbridge Anti-Virus ermöglicht Blacklist- und Whitelist-Filter auf Basis des MIME-Types. Dieser wird durch eingehende Analyse des Datei-Inhaltes ermittelt.
Zusätzlich prüft Anti-Virus, ob der so ermittelte MIME-Type und die Endung der Datei zueinander passen.

bowbridge Anti-Virus auf einen Blick:

- Schutz vor Uploads von Viren und Malware
- Erkennung von Cross-Site Scripting
- Blocken gefährlicher aktiver Inhalte
- Inhaltsbasierte MIME-Filter
- SAP-zertifiziert für NW-VSI 2.0
- Keine Code-Anpassungen erforderlich

SAP® Certified
Integration with SAP NetWeaver®



SAP-zertifiziert – mit Sicherheit kompatibel

Bereits vier Mal in Folge wurde bowbridge Anti-Virus von SAP zertifiziert und erfüllt alle Zertifizierungskriterien der aktuellen NW-VSI 2.0 Spezifikation. Die anspruchsvolle Zertifizierung von SAP stellt sicher, dass Stabilität und Zuverlässigkeit von Anwendungen und die Integrität verarbeiteter Daten zu jeder Zeit gewährleistet sind.

Unterstützt alle SAP Anwendungen - ohne Coding

Die Verwendung des SAP Virus Scan Interface ermöglicht es, Content Security mit bowbridge Anti-Virus in nahezu jede SAP Anwendung zu integrieren, ohne deren Code anpassen zu müssen. Neben ABAP und Java Application Server ist bowbridge Anti-Virus auch mit NetWeaver Gateway, FIORI- und UI5 Apps, SAP Mobile Platform, SAP Business Objects, Content Server, Document Center, Enterprise Portal und vielen weiteren Anwendungen kompatibel.

Offen und integrierbar

bowbridge Anti-Virus unterstützt zahlreiche Betriebssysteme, zum Teil auf mehreren Hardware-Plattformen.

Dank des Skripting-fähigen Event- und Alerting-Interfaces sind neben der McAfee ePolicy Orchestrator Integration auch die Anbindung von SIEM Lösungen diverser Dritthersteller schnell und einfach realisierbar.

Systemvoraussetzungen:

Unterstützte Betriebssysteme:

- HP-UX 11.31 und höher (PA-RISC und IA64)
- IBM AIX 6.1 und höher
- Linux (SLES 11 und höher RHEL 7.0 und höher)
- Microsoft Windows Server 2008 und höher
- Oracle Solaris 10 und höher (SPARC und x86_64)

Speicher:

- RAM: ca. 250MB (ca. 5MB bei ICAP)
- Disk: maximal 1,5 GB

SAP:

- AS ABAP: SAP_BASIS 640 SP 11 und höher
- AS Java: SAP J2EE SP 13 und höher
- HANA XS: SP09 und höher
- Mobile Platform 3.0 und höher
- Business Objects 4.2 SP3 und höher

bowbridge Software GmbH
Altrottstraße 31 ⌒ 69190 Walldorf ⌒ Germany

t +49-6227-69899-50
e sales@bowbridge.net
w www.bowbridge.net

SAP Silver Partner

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig