Umfassender Schutz vor inhaltsbasierten Cyber-Angriffen auf SAP Anwendungen

SAP-basierte Webanwendungen sind die Basis zahlreicher integrierter Geschäftsprozesse. Die Einbindung externer Geschäftspartner und mobiler Benutzer über traditionelle Web User-Interfaces sowie innovative UI5- und FIORI-Apps machen Ihre SAP Anwendungen aber angreifbar.

Schutz vor Cross-Site Scripting

bowbridge Application Security erkennt und blockt Eingaben und Parameter, die Teil eines Cross-Site Scripting Angriffes sein können. Damit ist Ihre Anwendung vor unberechtigten Veränderungen (Defacing) geschützt. Auch die Übernahme etablierter Sitzungen (Session Hijacking), das Ausspähen von Benutzerkonten und Malware-Infektionen durch Drive-by-Downloads werden wirksam verhindert.

Schutz vor Injections

In bowbridge Application Security sorgt eine Kombination aus Angriffssignaturen und komplexer Heuristik im Anti-SQLi Modul für die zuverlässige Erkennung eingeschleuster SQL-Anweisungen. Das Modul erkennt sowohl die SAP-eigene OpenSQL- als auch die native SQL-Syntax und verhindert so das nicht autorisierte Auslesen und Verändern von Datensätzen in der SAP-Datenbank.

Eingeschleuste Betriebssystem-Kommandos werden erkannt und gemäß der Security Policy geblockt.

Schutz vor Directory Traversals

Die zuverlässige Erkennung absoluter oder relativer Pfade in Benutzereingaben und URL-Parametern verhindert, dass Directory Traversal Lücken ausgenutzt werden können.

bowbridge Application Security schützt Anwendungen so vor unerlaubtem Anzeigen und Modifizieren von Daten und Dateien außerhalb des Anwendungskontexts.

Schutz vor Open Redirects

Umleitungen werden bei Webanwendungen vielfach sinnvoll eingesetzt. Offene Redirects, also durch Benutzereingaben beeinflussbare Umleitungen, stellen jedoch ein häufig vorhandenes, erhebliches Sicherheitsrisiko dar.

bowbridge Application Security erkennt Umleitungen und unterbindet die Weiterleitung zu nicht-autorisierten Zielen. Legitime Benutzer werden gegen das Ausspionieren von Daten und Malware Infektionen in Folge von Umleitungen zu Drive-by-Downloads geschützt.

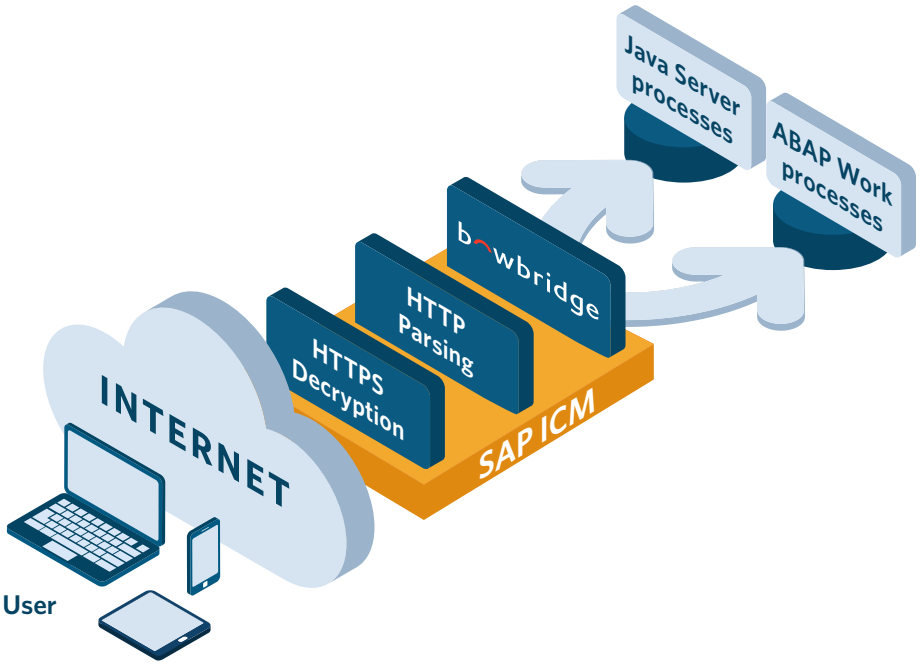
Maximale Performance

Neben höchster Sicherheit garantiert die modulare Architektur von bowbride Application Security auch den Erhalt maximaler Anwendungs-Performance. Alle Content Scans werden vollständig *in-Memory* durchgeführt und können bei Bedarf auf mehrere Engines lastverteilt werden.

Durch die Implementierung als Content Security Adapter im SAP Internet Communications Manager (ICM) entfällt zudem die separate Dekodierung des Datenstroms.

bowbridge Application Security auf einen Blick

- Schutz vor Cross-Site Scripting
- Schutz vor SQL-Injections
- Schutz vor Kommando-Injections
- Schutz vor Directory Traversal
- Schutz vor Open Redirects



Über die Hälfte aller SAP Sicherheitshinweise adressieren Sicherheitslücken, die durch manipulierte Inhalte ausgenutzt werden können. Diese Fixes betreffen jedoch nur den SAP Standard, nicht die umfangreichen Custom-Code Anwendungen in gängigen SAP-Implementierungen. Der Prüfung von Benutzer-Eingaben und externen Anwendungsparametern muss daher ein besonderes Augenmerk gelten, um den sicheren Betrieb und die Integrität von SAP Anwendungen zu gewährleisten.

Ermöglicht Ende-zu-Ende Verschlüsselung

Mit bowbridge Application Security bleiben Verbindungen Ende-zu-Ende verschlüsselt, vom Web-Browser des Benutzers bis zum SAP Application Server. Insbesondere in gehosteten und cloudbasierten SAP-Umgebungen ist dies ein wichtiges, Compliance-relevantes Merkmal (z. B. PCI-DSS und GDPR), das mit alternativen Technologien, wie Web Application Firewalls, nicht gewährleistet werden kann.

Automatische Updates

bowbridge Application Security verfügt über automatische Aktualisierungsfunktionen, die den administrativen Aufwand minimieren. Ihre SAP Anwendung ist mit stets aktuellen Filtern optimal geschützt. Über ein skalierbares, weltweit verfügbares Content Distribution Network stellt bowbridge Updates für die Erkennung neuester Angriffsmuster bereit. Diese werden ohne Ausfallzeiten automatisch heruntergeladen und zum Schutz Ihrer Anwendung verwendet.

Breiter Plattform Support

bowbridge Application Security ist auf zahlreichen Plattformen verfügbar. Neben Microsoft Windows Server und Linux werden auch verschiedene UNIX-Varianten auf zahlreichen Hardware Plattformen unterstützt.

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)

SAP:

- AS ABAP: SAP_BASIS 640 SP 11 und höher
- AS Java: SAP J2EE SP 13 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