EFFICIENT EXTENDED ENTERPRISE

EXTRA

ONLINE - April 2019 e-3.de

IT-SECURITY

Angriffe auf SAP-Anwendungen über Dokumente und Dateien

Laut einer Studie des Ponemon Institutes gaben insgesamt 75 Prozent der befragten US-Unternehmen an, dass sie eine Malware-Infizierung ihres SAP-Systems für „wahrscheinlich“ oder gar „sehr wahrscheinlich“ halten. Derselben Studie zufolge sind 65 Prozent der Unternehmen wegen einer möglichen Malware-Infizierung ihres SAP-Systems beunruhigt und 58 Prozent halten es für generell sehr schwierig, SAP-Anwendungen wirksam abzusichern. Anwendungen zu „Content-Management and Collaboration“ sowie „Data-Management“, die besonders im Rahmen von Dokumenten-Management relevant sind, gelten als am anfälligsten für Cyber-Angriffe.

Die Erkenntnis, dass SAP-Anwendungen und -Plattformen nicht inhärent sicher sind, ist nicht neu. Denn wenngleich sich in vielen Unternehmen beharrlich die Meinung hält, dass Segregation of Duties, Authentifizierung, Autorisierungen und Rollenmodelle die Grundpfeiler der „SAP Security“ seien, zeigen zahlreiche Vorträge auf einschlägigen Hacker- und Security-Konferenzen seit nunmehr zehn Jahren, dass immer wieder kritische Sicherheitslücken in SAP-Plattformen und -Anwendungen gefunden werden. Zur Abgrenzung von traditionell Business-Logik-fokussierter „SAP Security“ hat sich daher „SAP Cyber-Security“ als neue Disziplin im SAP-Umfeld entwickelt.

Eine Auswertung der mittlerweile über 4000 von SAP veröffentlichten Sicherheitshinweise unter ebensolchen SAP-Cyber-Security-Aspekten zeigt auf, dass etwa die Hälfte der Hinweise Content-relevante Sicherheitsproblematiken betrifft. Mit den in diesen Hinweisen adressierten Sicherheitslücken können SAP-Anwendungen oder Benutzer durch „Content“ – also Benutzer-Eingaben im weitesten Sinne – beeinträchtigt oder sogar vollständig kompromittiert werden. Bei näherer Betrachtung solcher Content-basierter Angriffsszenarien im SAP- Kontext muss man bei „Content“ zunächst zwischen strukturierten und unstrukturierten Daten unterscheiden:

- Als strukturierte Daten bezeichnet man all jene Informationen, die typischerweise in Datenbank-Tabellen abgelegt werden. Ihr Sinn und ihre Bedeutung sind definiert und werden von der Anwendung verarbeitet. Zum Beispiele Rechnungsfälligkeits-Daten, Anzahl des Lagerbestandes eines bestimmten Artikels, Brutto-Monatsgehalt eines Mitarbeiters, Lieferantennummer usw.
- Als unstrukturierte Daten bezeichnet man Dateien und extern generierte Dokumente ohne feste Struktur. Sie werden von der Anwendung zwar gespeichert und verwaltet und haben in der Regel einen Bezug zu einem Geschäftsvorfall oder einer sonstigen Transaktion, der eigentliche Inhalt der unstrukturierten Daten, also deren Bedeutung, wird von der Anwendung aber nicht erfasst. Zum Beispiel Bilder, Beleg-Scans, PDFs, Pläne/CAD-Dateien, Videos usw.

Beide Arten von Content, strukturiert und unstrukturiert, gelangen über verschiedene Vektoren in SAP-Anwendungen. Allen voran Eingaben und Uploads von internen und externen Benutzern im Rahmen der normalen, interaktiven Nutzung der Anwendung. Aber auch über E-Mails, Daten-Importe von externen Anwendungen (z. B. über SAP PI/PO), Web Services sowie über die Anbindung bestehender Content-Repositorien und Dokumenten-Management-Systeme gelangt Content in SAP-Anwendungen.

Content-basierte Angriffsszenarien

Angriffe sind generell sowohl über strukturierten als auch unstrukturierten Content möglich. Bei Angriffen in strukturiertem Content handelt es sich dabei im Wesentlichen um Exploits klassischer Application-Level Sicherheitslücken durch Cross-Site Scripting, Cross-Site Request Forgery, Directory Traversals, SQL- und Command-Injections sowie Umleitungen. Da diese im Wesentlichen den Grundprinzipien von Web-Application-Security folgen, haben Unternehmen diese oft im Blick und versuchen zumindest allgemeine Angriffe mit

Web-Application-Firewalls abzuwehren. Risiken, die aber mit dem Upload oder Import von unstrukturierten Daten einhergehen, werden oft übersehen – auch weil viele Administratoren der Ansicht sind, betriebssystemseitige Virenscanner böten hier Schutz. Letzteres ist ein Irrtum, der fatale Folgen haben kann, denn Datei-Uploads in SAP-Anwendungen bleiben tatsächlich von diesen Scannern völlig unbehelligt. Zeit also, die Risiken, die von Datei-Uploads ausgehen, im Detail zu betrachten – insbesondere da diese Risiken für jede SAP-Anwendung gelten, die Datei- oder Dokumenten-Uploads und Downloads implementiert.

Upload von Viren und Malware

Viren und Malware sind die wohl offensichtlichsten Gefahren beim Upload von Dokumenten. Malware findet sich heute in nahezu jedem Dateiformat und nutzt Sicherheitslücken in den Anzeigeprogrammen, um bösartigen Code auf dem betroffenen System auszuführen oder eine persistente Malware zu installieren. In vielen Fällen ist dazu keinerlei Benutzeraktion notwendig. Das Öffnen einer bösartigen PDF-Datei, oder gar nur das Ansehen eines manipulierten Bildes genügen, um darin verborgenen Schadcode auszuführen.

Viren, Würmer, Trojaner und andere Malware, die in einem SAP-System gespeichert sind, stellen für dieses System selbst zunächst keine unmittelbare Bedrohung dar. Im Zuge der direkten Einbindung externer User in Geschäftsprozesse besteht aber die Gefahr eines erheblichen Imageschadens, sollte gerade das SAP-System bei Kunden, Partnern und Zulieferern als „Virenschleuder“ gelten. Letztlich lassen sich bei einem Viren-Vorfall durch eine Datei aus einem SAP-System auch Schadenersatz-Ansprüche gegen dessen Betreiber ableiten, wenn nach dem Stand der Technik übliche Schutzmechanismen unzureichend oder gar nicht implementiert wurden. Im Bereich öffentlicher Verwaltungen, die an Vorgaben des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) gebunden sind, gilt es darüber hinaus die Maßnahmen der IT-Grundschutz-Kataloge zu beachten. Diese schreiben seit 2008 den Virenschutz beim Hoch- und Herunterladen von Dateien aus SAP-Anwendungen vor.

Cross-Site Scripting mit Dokumenten

Bei Web-Anwendungen findet sich Cross-Site Scripting (XSS) seit Jahren in den Top 10 der häufigsten und kritischsten Angriffsvektoren mit strukturiertem Content. Aber auch mit Dateien lassen sich XSS-Angriffe konstruieren, die dann zum Tragen kommen, wenn die entsprechend präparierte Datei auf einem Client angezeigt wird. Uploads von Dateiformaten, die clientseitig im Browser angezeigt werden, sollten daher besonders kritisch geprüft werden. Beispielsweise können Angreifer eine manipulierte SVG-Bilddatei oder eine PDF-Datei mit eingebettetem JavaScript in eine SAP-Anwendung hochladen. Bei Usern, die diese Datei dann im Kontext der SAP-Anwendung ansehen, wird das JavaScript ausgeführt und kann die bestehende, authentifizierte Session zur SAP-Anwendung nutzen, um Aktionen im Namen des angemeldeten Users auszuführen.

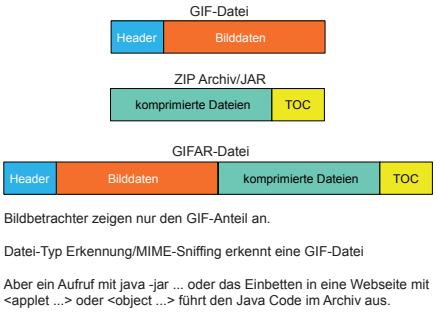
Aber auch Dateien, die in clientseitigen Anwendungen verarbeitet werden, können zum Teil für XSS-Angriffe genutzt werden. So bieten Office-Dokumente, PDF-Dateien, diverse Bild- und Grafik-Formate, MP3-Dateien und viele andere Datei-Formate die Möglichkeit, Metadaten über das Dokument (z. B. Autor, Firma, Copyright usw.) im Dokument zu speichern. In diesen Inhaltsfeldern lassen sich ebenfalls HTML-Tags und Skripte für XSS-Angriffe hinterlegen.

Solche Metadaten-XSS-Angriffe sind deutlich komplexer und funktionieren nur mit Anwendungen, die diese Metadaten auslesen und anzeigen. Für diese aber sind sie ein ernst zu nehmendes Risiko.

Die Implikationen von XSS sind erheblich kritischer als beim Upload von Malware. Mit XSS lassen sich z. B. SAP-Web-Anwendungen in ihrem Aussehen verändern. In der Praxis bedeutet dies, dass neben dem offensichtlichen „defacing“ der Anwendung auch subtilere Änderungen möglich sind. So können z. B. zusätzliche Log-in-Fenster eingeblendet werden, um legitime Benutzer-Zugangsdaten zu erbeuten.

Aktive Inhalte in Dokumenten

Zahlreiche Dateiformate bieten Automatisierungen an, mit denen die Benutzerfreundlichkeit komplexer Dokumente vereinfacht werden soll. Allgemein bekannt in diesem Zusammenhang sind natürlich Makros in Office-Dokumenten und die damit verbundene Sicherheitsproblematik. Viele erinnern sich in diesem Zusammenhang an den Ausbruch des „Melissa“-Wurms Ende 1999, der weltweit 20 Prozent aller PCs infizierte und einen geschätzten Schaden von über 80 Millionen US$ verursachte. Weniger bekannt ist aber, dass Makro-Malware eine wahre Renaissance erlebt und aktuelle Malware und Ransomware oftmals Office-Makros als einen Infizierungsvektor benutzt. Das Adobe-PDF-Format bietet ebenfalls Scripting-Optionen mit JavaScript sowie die Möglichkeit, eigene ausführbare Dateien direkt in das Dokument einzubetten. Diese können automatisch beim Öffnen des Dokumentes oder beim Ausfüllen von Formularen aufgerufen werden. Manche PDF-Viewer führen Scripts sogar ohne Benutzer-Warnung aus. Bei anderen, wie dem Adobe Reader, kann die Sicherheitsabfrage zudem so verändert werden, dass dem arglosen Benutzer suggestive oder irreführende Anweisungen angezeigt werden.



Einschleusen von Java-Code mittels einer GIFAR-Chamäleon-Datei.

Neben diesen gebräuchlichen Dokumenten-Formaten bieten natürlich HTML und XML sowie das relativ neue, universelle Vektor-Grafik-Format SVG die Möglichkeit, JavaScript einzubetten oder gar komplexere, meist Browser-gebundene aktive Komponenten wie Java, Flash, Silverlight, Shockwave oder XSLT zu verwenden.

Aus sicherheitstechnischer Sicht sind Makros oder selbstaktivierende Skripts generell bedenklich, unabhängig vom Kontext. Angesichts der Sensitivität der Daten, die in einem SAP-System verarbeitet werden, und der Tatsache, dass die aktiven Inhalte im Dokument im Trust-Kontext der SAP-Anwendung ausgeführt würden, verbietet sich deren Nutzung eigentlich von allein. Da aktive Inhalte aber nicht per Definition als Malware gelten, werden sie von normalen Virenscan-Lösungen in der Regel nicht geblockt.

Chamäleon-Dateien

Dateien, die die Erkennungsmerkmale zweier oder mehr Dateiformate erfüllen, bezeichnet man als Chamäleon-Dateien. Ein sicherheitsrelevantes Beispiel sind sogenannte GIFAR-Dateien, also einer zusammengesetzten Datei aus einem GIF-Bild und einem Java-Archiv (JAR). Bei einem GIF-Bild befindet sich der Header der Datei am Anfang derselben, die Bild-Daten stehen im Anschluss daran. Bei einem ZIP-Archiv – und damit auch bei auf ZIP basierenden Formaten wie Office OOXML oder Ja-

va-Archiv JAR – befindet sich ein Inhaltsverzeichnis ganz am Ende der Datei und verweist auf die enthaltenen, komprimierten Dateien davor. Verkettet man eine GIF- und eine JAR-Datei, erhält man eine GIFAR-Chamäleon-Datei.

Bildbetrachter, Web-Browser und andere Datei-Erkennungstechniken – sogar viele Virenscanner – erkennen diese als eine normale GIF-Bilddatei.

Der Aufruf mit Javas-Jar oder das Einbetten in HTML mittels eines <applet ...> oder <object ...> Tags führt aber zur Ausführung der im hinteren Teil der Datei befindlichen Java-Klassen. Als zweistufiger Angriff ausgeführt, bei dem eine im System gespeicherte GIFAR-Datei mittels eines XSS-Angriffs aufgerufen wird, führt somit dazu, dass Angreifer beliebigen Java-Code clientseitig zur Ausführung bringen können. Wie bei aktiven Inhalten gilt auch hier, dass der Java-Code im Kontext der Web-Anwendung ausgeführt wird. Damit hat er Zugriff auf die authentifizierte Verbindung zur SAP-Anwendung und könnte völlig unbemerkt Aktionen auf der Basis dieser Verbindung mit den Berechtigungen des angemeldeten Benutzers ausführen.

Viren- und Content-Scan über das SAP Virus Scan Interface

Handelsübliche Virenschutz-Lösungen, die den SAP-Server auf Betriebssystem-Ebene schützen, bieten keinen Schutz vor vorgenannten Angriffsszenarien. Sie überwachen in der Regel Zugriffe auf das Dateisystem. Solche Zugriffe finden jedoch beim Transfer von Daten in und aus der Anwendung nicht statt. Auch netzwerkbasierte Ansätze für HTTP oder Host-Intrusion-Prevention-Lösungen scheitern, sobald End-to-End-SSL-Verschlüsselung eingesetzt wird, und versagen völlig bei SAP-proprietären Protokollen wie dem SAP-GUI-Protokoll DIAG.

Aus diesen Gründen hat SAP bereits mit NetWeaver 04 das Virenscan Interface NW-VSI zum Schutz vor Content-basierten Angriffen in unstrukturierten Daten eingeführt. Diese Schnittstelle ermöglicht es, Datei-Uploads und -Downloads transparent und Policy-gesteuert zu scannen. Gefährliche Inhalte werden geblockt, bevor sie die Anwendung erreichen. Die aktuelle, zweite Generation der NW-VSI wurde um eine Vielzahl granularer Content-Filter-Möglichkeiten erweitert. Sie kann nicht nur zur Abwehr von Viren verwendet werden, sondern auch für gefährliche Inhalte, die nicht ausdrücklich Malware sind, für SAP-Anwendungen aber dennoch Gefahrenpotenziale darstellen, beispielsweise XSS, aktive Inhalte oder Chamäleon-Dateien.

Dank der durchgängigen Integration können Nutzern aussagekräftige Informationen angezeigt werden, wenn ein Upload geblockt wird. Auch eine ausführliche Protokollierung im SAP Security Audit Log sowie Überwachung über CCMS sind vorhanden.

Dieses Virus Scan Interface ist natürlich nicht nur in NetWeaver, sondern auch in S/4, Business Objects, Mobile Platform, HANA-XS und nahezu allen anderen SAP-Produkten verfügbar und nutzbar.

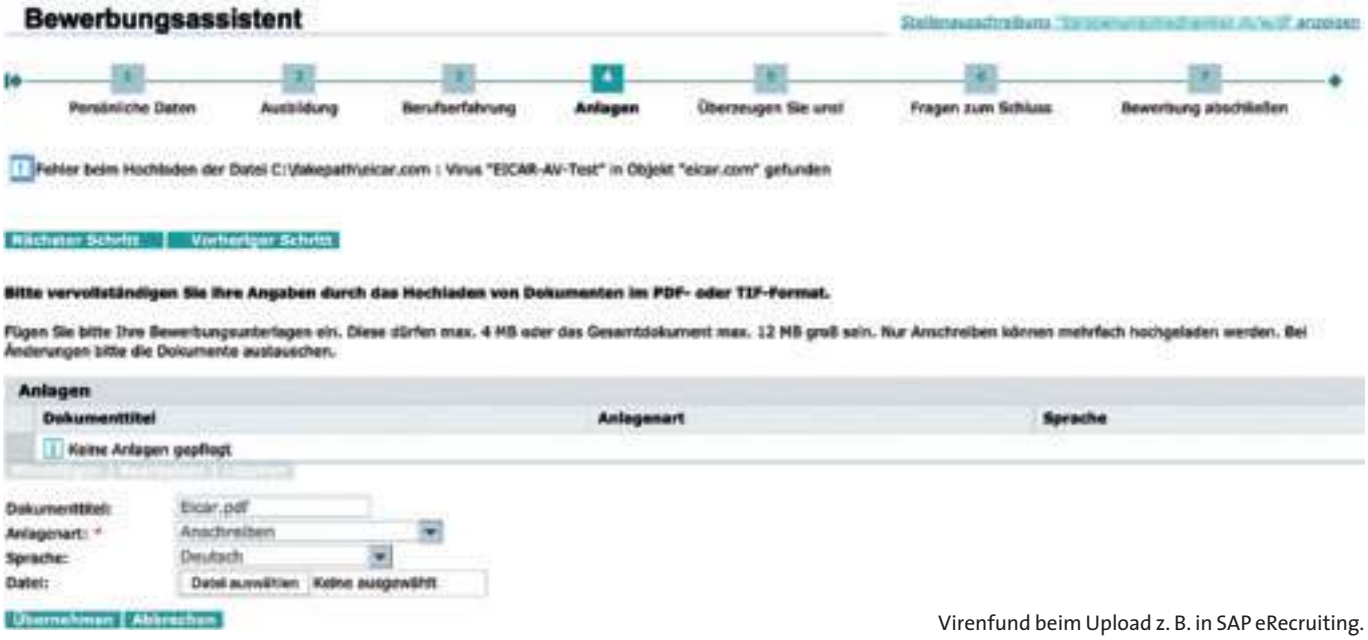
SAP selbst stellt aber die eigentlichen Scanner zum Erkennen besagter Gefahren nicht zur Verfügung, sondern verweist auf Ecosystem-Partner. Im Rahmen einer SAP-Zertifizierung können Security-Hersteller ihre Virenscan- und Content-Security-Lösungen für NW-VSI prüfen und abnehmen lassen. Zertifizierte Produkte für NW-VSI sind in SAP-Hinweis 1494278 aufgeführt. Details zur Implementierung von Viren- und Content-Scan mit dem im Dokumenten-Umfeld häufig verwendeten SAP Content Server werden in SAP-Hinweis 1751530 behandelt.

Fazit

Grundsätzlich gilt, dass bei SAP-Anwendungen eine Reihe von Gefährdungspotenzialen existiert, die über die klassischen „SAP-Security"-Aspekte rund um die Absicherung der Business-Logik hinausgehen. Insbesondere im Zuge der zunehmenden Einbindung von externen Usern, Partnern, Zulieferern und mobilen Benutzern erwächst daraus die Anforderung, den Content, der in SAP-Anwendungen abgelegt wird, zu prüfen, um eine Gefährdung von Nutzern und System so weit wie möglich zu reduzieren.

Über den Autor

Jörg Schneider-Simon befasst sich seit über 20 Jahren mit IT-Security. Nach beruflichen Stationen beim Firewall-Hersteller CheckPoint und Virenscan-Anbieter Trend Micro gründete er 2005 bowbridge Software und fokussiert sich seither mit seinem Team auf die Absicherung unternehmenskritischer SAP-Anwendungen vor Content-Angriffen.



Virenfund beim Upload z. B. in SAP eRecruiting.

Stadt Essen sichert elektronische Akten in SAP gegen dateibasierte Bedrohungen

Als zentraler IT- und Telefonie-Dienstleister betreut und berät das Essener Systemhaus (ESH) zahlreiche Fachbereiche, Institute und Eigenbetriebe und Beteiligungsgesellschaften der Stadt Essen, darunter Einwohner- und Straßenverkehrsamt, auch die Stadtwerke, Verkehrsbetriebe, die Essen Marketing GmbH und die Essener Wirtschaftsförderungsgesellschaft mbH. Zum Verantwortungsbereich des ESH gehören dabei unter anderem die Betriebssicherung und Weiterentwicklung des SAP-basierten Verfahrens „elektronische Akte“, mit dem die Stadt Essen verwaltungsinterne Prozesse effizienter gestaltet.

Risiko Upload

Sachbearbeiter aus den einzelnen Verwaltungsbereichen können heute bei Bedarf Dateien direkt in sdas SAP-System hochladen, um so alle relevanten Informationen in einer elektronischen Akte zu sammeln. „Der direkte Upload von Dateien durch Anwender bringt Effizienzvorteile, aber auch erhebliche Risiken mit sich – nicht nur für die elektronische Akte, sondern auch für das SAP-Gesamtsystem“, sagt Raimund Fechtner, zuständig für Beratung und Anwendungsentwicklung der SAP-Basisdienste beim ESH.

Um diese Risiken zu adressieren, startete ESG die Suche nach einer SAP-zertifizierten Lösung zum Schutz vor Malware und anderen dateibasierten Bedrohungen. „Neben der Sicherheit stand für uns dabei eine möglichst geringe Beeinträchtigung der Performance im Fokus, um die dauerhafte Anwenderakzeptanz zu gewährleisten“, erläutert Michael Rudwilleit, beim ESH zuständig für User und Berechtigungen im Bereich SAP-Basisadministration sowie für SAP-Sicherheit.

> *Mit bowbridge Anti-Virus for SAP Solutions können wir den Datei-Upload umfassend schützen, ohne Beeinträchtigungen der Performance oder Funktionalität.*
>
> Michael Rudwilleit,
> zuständig für SAP-Basisadministration und SAP-Sicherheit beim ESH.

Security – Made for SAP

Nach Evaluierung der Anbieterlandschaft und einer Anfrage im Forum der Deutschsprachigen SAP-Anwendergruppe (DSAG) entschied sich das Team schließlich für bowbridge Anti-Virus for SAP Solutions. Als einzige SAP-zertifizierte Sicherheitslösung auf dem Markt erfüllt Anti-Virus for SAP Solutions alle Anforderungen der aktuellen NW-VSI-2.0-Spezifikation und lässt sich dementsprechend nahtlos mit SAP-eigenen Überwachungs- und Protokollfunktionen integrieren.

Mit der Lösung von bowbridge wurde zudem eine Filterung von Dateien nach MIME-Typ realisiert, bei der bestimmte Inhalte (z. B. ausführbare Dateien) grundsätzlich blockiert und andere risikobehaftete Formate (z. B. Office-Dokumente, E-Mails, PDFs) auf versteckte Malware überprüft werden. Im Gegensatz zur SAP-Standardfilterfunktion lässt sich bowbridge dabei nicht von einer Manipulation der Dateiendung täuschen, denn der MIME-Typ wird anhand des Inhalts identifiziert. Passen Inhalt und Dateiendung nicht zusammen oder wird Malware gefunden, verhindert die Sicherheitslösung den Upload.

Sicher ist sicher

Nach einer 40-tägigen Testphase erfolgte die Produktivstellung problemlos. Dazu Raimund Fechtner: „Anpassungen der Anwendung oder Änderungen am Upload-Szenario waren nicht notwendig, die Implementierung verlief reibungslos.“ Im Ergebnis hat die Stadt Essen mit der SAP-basierten digitalen Akte Verwaltungsvorgänge effizienter gestaltet und Mitarbeitern die Arbeit erleichtert. Durch die Implementierung von bowbridge Anti-Virus for SAP Solutions konnte das ESH für das Verfahren ein Höchstmaß an Sicherheit und Betriebskontinuität erzielen, bei geringem Implementierungsaufwand. Und auch in einem weiteren wichtigen Punkt konnte bowbridge laut Michael Rudwilleit überzeugen: „Das Malware-Scanning hat keine spürbaren Auswirkungen auf die Performance. Anwender können also ohne Einschränkungen die Vorteile der elektronischen Akte nutzen.“

> *Wir haben die am Markt verfügbaren Produkte evaluiert und auch die Meinungen anderer SAP-Nutzer eingeholt. Die Vorteile von bowbridge Anti-Virus for SAP Solutions sind eindeutig.*
>
> Raimund Fechtner,
> zuständig für Beratung und Anwendungsentwicklung der SAP-Basisdienste beim ESH.