Pressemeldung

Studie von SAP-Security-Spezialist Onapsis ermittelt die drei meistbenutzten Angriffsvektoren auf SAP-Systeme

Mehr als 95 Prozent aller untersuchten Systeme haben Schwachstellen, über die Hacker Zugriff auf sensible Informationen erlangen und geschäftswichtige Unternehmensprozesse unterbrechen können

Pressekontakt:

Onapsis Inc.
Gerhard Unger

Tel +49 – 8192 – 9970890
gunger@onapsiscom

Havana Orange GmbH
Michael Eckstein
Birkenleiten 41
D-81543 München

Tel +49 – 89 – 9 21 31 51-59
men@havanaorange.de

München/Boston, 6. Mai 2015 – Onapsis, global agierender Experte für die Sicherheit von geschäftswichtigen Unternehmens-Applikationen und führender Anbieter von SAP-Cyber-Security-Lösungen, hat die drei häufigsten Vorgehensweisen bei Cyber-Attacken auf SAP-Anwendungen ermittelt. Diese Angriffsvektoren setzen geistiges Eigentum, Finanz-, Kreditkarten-, Kunden- und Lieferantendaten sowie in Datenbanken gespeicherte Informationen der weltweit größten Unternehmen einem hohen Risiko aus. Für seine Studie untersuchte das Onapsis Research Labs hunderte von SAP-Installationen. 95 Prozent dieser SAP-Systeme wiesen Schwachstellen auf, über die Hacker vollständigen Zugriff auf die Geschäftsdaten und -prozesse der betroffenen Unternehmen erlangen können.

Darüber hinaus hat Onapsis in seiner Studie herausgefunden, dass es bei den meisten Unternehmen 18 Monate oder länger dauert, bis Patches für gefundene Schwachstellen implementiert werden. Allein im Jahr 2014 hat SAP 391 Sicherheitspatches veröffentlicht – im Durchschnitt also mehr als 30 pro Monat! Nahezu 50 Prozent dieser Patches hat SAP mit einer hohen Priorität eingestuft.

Weltweit setzen über 250.000 Unternehmen SAP-Lösungen ein – darunter 87 Prozent der Global 2000-Konzerne und 98 Prozent der weltweit wertvollsten Marken. SAP-Systeme speichern die wertvollsten und sensibelsten Unternehmensinformationen – und werden von herkömmlichen IT-Sicherheitsansätzen nicht geschützt.

„Das Thema SAP-Cyber-Security wird von vielen Unternehmen nicht ernsthaft genug verfolgt, da nicht geklärt ist, wer dafür zuständig ist – das SAP-Betriebsteam oder das IT-Sicherheitsteam. Dies hat uns wirklich überrascht“, sagt Mariano Nunez, CEO und Gründer von Onapsis. „Die meisten eingespielten Patches sind nicht sicherheitsrelevant, kommen verspätet oder öffnen neue Schwachstellen für den Betrieb des SAP-Systems. Jeden Tag werden neue Datenlecks bekannt, ohne dass CISOs davon erfahren – weil ihnen die Visibility für ihre SAP-Anwendungen fehlt. Onapsis untersucht fortlaufend die Angriffe, denen die Industrie ausgesetzt ist. Wir arbeiten direkt mit unseren Kunden, dem Markt und Regierungsbehörden zusammen, um Angriffen proaktiv vorzubeugen und geeignet darauf zu reagieren, wenn sie erfolgen.“

„CEOs nehmen irrtümlicherweise an, dass ihre wichtigsten Geschäftsprozesse und -daten vor Cyber-Attacken geschützt sind. Doch die heutige Definition von Anwendungssicherheit muss auf die Anwendungsebene von SAP-Unternehmensapplikationen erweitert werden. Dies muss auf Ebene der Geschäftsführung diskutiert werden. Ein Datenleck in einem SAP-System kann ein Unternehmen dutzende von Millionen Dollar kosten – pro Minute“, sagt Renee Guttman, Vice President, Office of the CISO, Accuvant und früherer CISO von Coca-Cola.

Die drei meistbenutzten Angriffsmethoden für Attacken auf SAP-Systeme

Onapsis Research Labs hat tausende von Schwachstellen untersucht, um die drei am häufigsten verwendeten Ansätze und für das Hacken von geschäftswichtigen, in SAP gespeichert Daten und für das Unterbrechen von zentralen Geschäftsprozessen zu ermitteln:

1. Bedrohungen von Kunden- und Kreditkarteninformationen, die den Austausch zwischen SAP-Systemen ausnutzen: Die Angriffe setzen an einem System mit niedrigen Sicherheitseinstellungen an und hangeln sich zu einem geschäftswichtigen System vor, indem sie fernsteuerbare Funktionsmodule im Zielsystem ausführen.
2. Attacken auf Kunden- und Lieferantenportale: Dazu werden Backdoor-Anwender im SAP J2EE Benutzermanagement-Modul erzeugt. Durch das Ausnutzen einer Schwachstelle können die Hacker Zugriff auf SAP-Portale und Prozessintegrations-Plattformen sowie die damit verbundenen, internen Systeme erlangen.
3. Angriffe auf Datenbanken über proprietäre SAP-Protokolle: Für diese Attacke werden Betriebssystembefehle mit den Rechten bestimmter Benutzer ausgeführt und Schwachstellen im SAP RFC-Gateway ausgenutzt. Der Hacker erhält Zugriff auf jede in der SAP-Datenbank gespeicherte Information und kann diese verändern.

„Die Echtzeit-Plattform SAP HANA verschlimmert die Situation sogar noch. Die Zahl neuer Sicherheitspatches, die speziell diese neue Plattform betreffen, hat um 450 Prozent zugenommen. Hinzu kommt, dass SAP HANA als Kernkomponente im Zentrum des SAP-Ökosystems platziert ist. Daten, die in den SAP-Plattformen gespeichert werden, müssen nun sowohl in der Cloud als auch im Unternehmen geschützt werden“, führt Nunez aus. „Onapsis Research Labs ist das führende Unternehmen für SAP-Cyber-Security, das SAP hilft, SAP HANA-betreffende Sicherheitsschwachstellen zu identifizieren und zu beheben.“

Aktionsplan für CISO

Handelsunternehmen, Energieversorger, Hersteller, Pharmakonzerne und andere Global 2000-Organisationen, die geschäftswichtige Prozesse über Lösungen der SAP Business Suite betreiben, sollten unbedingt die neusten SAP Sicherheitshinweise befolgen. Sie sollten zudem sicherstellen, dass ihre Systeme korrekt konfiguriert sind, um geltende Compliance-Anforderungen zu erfüllen und das Sicherheitsniveau zu erhöhen. Diese Aktivitäten sollten einem Aktionsplan folgen, der SAP-Cyber-Security als Teil der Unternehmensstrategie und -Roadmap etabliert:

- Visibility in SAP-basiert Komponenten realisieren, um gefährdete Werte zu identifizieren.
- Vorsorge vor Sicherheits- und Compliance-Probleme durch kontinuierliche Überwachung treffen.
- Neue Bedrohungen, Angriffe und anomales Benutzerverhalten als Gefährdungsindikatoren (Indicators of Compromise, IOC) erkennen und mit geeigneten Maßnahmen darauf reagieren.

Über Onapsis

Onapsis liefert die vollständigste Security-Lösung für die Sicherheit von geschäftswichtigen Applikationen. Als führender Experte für SAP Cyber-Security gibt Onapsis IT-Sicherheits- und Audit-Teams leistungsfähige Instrumente an die Hand, mit denen sie eine verlässliche Visibility und Kontrolle über komplexe Bedrohungen, Cyber-Risiken und Compliance-Lücken erlangen, die ihre Unternehmensanwendungen bedrohen.

Onapsis hat seine Hauptniederlassung in Boston, Massachuchettes (USA) und unterstützt mit seinen Lösungen 160 Global-2000-Kunden, darunter 10 führende Handelsunternehmen, 20 führende Energiekonzerne und 20 führende Hersteller. Onapsis Lösungen sind darüber hinaus der De-facto-Standard für führende Beratungs- und Audit-Firmen wie Accenture, IBM, Deloite, Ernest & Young, KPMG und PwC.

Zu den Lösungen von Onapsis zählt die Onapsis Security Platform – die meistgenutzte SAP-zertifizierte Cyber-Security-Lösung im Markt. Anders als generische Sicherheitsprodukte ermöglichen Onapsis kontextbewusste Lösungen sowohl präventive Kontrollen für das Überwachen von Schwachstellen und Compliance-Anforderungen als auch Funktionen für das Erkennen und sofortige Reagieren auf ungewöhnliche Ereignisse. Onapsis Produkte können Risiken reduzieren, die möglicherweise Auswirkungen auf geschäftswichtige Prozesse und Daten haben.

Über offene Schnittstellen lässt sich die Plattform mit SIEM-, GRC- und Netzwerksicherheitsprodukten kombinieren. Dies ermöglicht eine nahtlose Integration von SAP-Applikationen in bestehende Schwachstellen-, Risiko- und Reaktions-Managementprogramme.

Die Lösungen greifen auf das Onapsis Research Labs zurück, das mit intelligenten Analyseverfahren kontinuierlich Sicherheitsbedrohungen aufdeckt, die SAP-Systeme betreffen. Die Experten des Onapsis Research Labs waren die ersten, die über SAP

betreffende Cyber-Attacken berichtet haben. Sie haben mittlerweile hunderte Sicherheitslücken aufgedeckt und Unternehmen dabei unterstützt, diese zu beheben. Die Schwachstellen betreffen die SAP Business Suite, SAP HANA und SAP Mobile-Installationen.

Weitere Informationen sind unter www.onapsis.com sowie über Twitter, Google+ oder LinkedIn erhältlich.