SYNTAX

Sicherheit für Ihre SAP-Systeme

Wie sich Unternehmen gegen Cyberattacken auf ihre SAP-Systeme schützen können

Cyberkriminelle nutzen viele Wege, um in ein System einzudringen. Bei Phishing-Attacken nehmen sie gezielt Mitarbeiter ins Visier, um an ihre Zugangsdaten zu gelangen. Oft ist aber nicht der Mitarbeiter das Problem, sondern die Software an sich. Bei Zero Day Exploits nutzen Hacker bisher unbekannte oder kürzlich bekannt gegebene Schwachstellen im Code von Anwendungen, um sich Zugriff zu verschaffen.

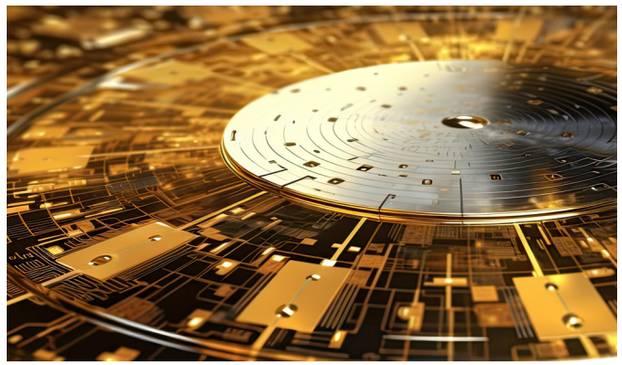
Damit sie einen solchen Angriff auf unternehmenskritische SAP-Systeme verhindern können, müssen Unternehmen schnell reagieren und eine Reihe von Herausforderungen meistern.

IT-Security: Ungeliebt, aber wichtig

IT-Sicherheit ist ein unternehmensintern oft kontrovers diskutiertes Thema. Effektive Maßnahmen sind nicht nur ressourcenintensiv, ihr Sinn wird zudem mitunter ganz nach dem Motto „There is no glory in prevention“ infrage gestellt, wenn sie funktionieren – und eben nichts passiert. Wesentlich größer als die Kosten für ein funktionierendes Sicherheitssystem ist jedoch der Schaden, der bei einem erfolgreichen Angriff entstehen kann. Denn ist die Infrastruktur kompromittiert und sind die Systeme verschlüsselt, kann das einen kompletten Stillstand sämtlicher Geschäftsaktivitäten, und zwar nicht nur für einige Tage, sondern für mehrere Wochen bedeuten. Das verursacht zum einen enorme finanzielle Verluste und schädigt zum anderen auch die Reputation des betroffenen Unternehmens erheblich. Lieferanten, Partner oder Endkunden – alle könnten durch die Auswirkungen einer geglückten Attacke beeinträchtigt werden, und gerade in der fertigenden Industrie kostet jede stillstehende Anlage Geld. Wer dieses Risiko eingeht und an der Sicherheit seiner Systeme spart, zahlt im Zweifelsfall einen wesentlich höheren Preis.

Sicherheitsrisiko SAP Vulnerabilities

Auch und gerade im Hinblick auf SAP-Software spielt IT-Security eine zentrale Rolle. Unternehmen setzen integrierte und vernetzte SAP-Lösungen in nahezu allen operativen Bereichen ein, von ERP über Maschinensteuerung bis hin zu Afterservices und CRM. Diese Verzahnung bringt viele Vorteile wie eine effizientere Prozessabwicklung und die Möglichkeit, alle relevanten Business-Aktivitäten zentral abzubilden und steuern zu können. Doch sie birgt auch ein gewisses Risiko. Denn wie bei jeder anderen Software besteht auch bei SAP die Gefahr, sich über sogenannte Vulnerabilities, also Schwachstellen im Code, angreifbar zu machen. Werden diese Sicherheitslücken nicht rechtzeitig geschlossen, können sie ein Einfallstor für Cyberkriminelle sein. Bei geschäftskritischer Software wie SAP bedeuten verschlüsselte oder gestohlene Daten zumindest eine Beeinträchtigung aller wichtigen ERP-Prozesse, zum Beispiel in den Bereichen Einkauf, Personalwesen, Projektmanagement, Controlling oder Finance. Das macht es in den meisten Fällen unmöglich, das Tagesgeschäft aufrecht zu erhalten. Der so entstehende Schaden ist gravierend, selbst wenn Unternehmen dem Angreifer Lösegeld zahlen, um ihre Systeme schnell wieder nutzen zu können. Denn sie müssen darauf vertrauen, dass die Erpresser dann auch Wort halten und die Daten wieder verfügbar machen – eine Garantie dafür gibt es nicht.



SAP Security Notes - Schnelligkeit ist Trumpf

Angreifer bedienen sich immer der neuesten Schwachstellen, die auch in unterschiedlichsten Kombinationen mit anderen, bereits bekannten, aber eventuell nicht geschlossenen Sicherheitslücken zum Angriff genutzt werden. Daher ist es enorm wichtig, die Schwachstellen und deren Bedeutung für die eigene Systemlandschaft zu kennen. SAP veröffentlicht am zweiten Dienstag eines jeden Monats, dem SAP Security Patch Day, eine Aufstellung neu bekannt gewordener Vulnerabilities in allen SAP-Lösungen. Die entsprechenden SAP Security Notes informieren über die Schwachstellen und stellen die notwendigen Patches bereit, die zeitnah eingespielt werden müssen, um möglichen Angriffen vorzubeugen und Schaden abwenden zu können. Sind die Vulnerabilities bekannt, ist es für versierte Hacker ein Leichtes, ein Programm zu schreiben, das die Systeme abfragt und nicht behobene Lücken direkt ausnutzt.

Herausforderungen für Security-Verantwortliche

1 Effiziente Durchführung der Security Patches

Ohne externen Partner stehen Unternehmen enorm unter Zeitdruck, wenn es darum geht, Sicherheitslücken in SAP rechtzeitig zu erkennen und zu schließen. Dafür setzen sie meistens auf eine manuelle Durchführung durch Mitarbeiter. Hier liegt die Verantwortung in den Händen weniger interner Spezialisten. Das ist sehr zeitaufwendig, da die Experten zunächst alle SAP Security Notes mit dem eigenen System abgleichen müssen, bevor sie tätig werden können.

2 Abhängigkeit von internen Fachkräften

Wer sich jahrelang auf einige interne Experten verlässt, schafft Abhängigkeiten. In den meisten Fällen nutzen Unternehmen mehrstufige und entsprechend skalierte SAP-Landschaften, über deren genaue Verzahnung und Architektur oftmals nur wenige Kollegen Bescheid wissen. Wenn die entsprechenden Spezialisten aus Alters- oder Karrieregründen das Unternehmen verlassen, wandert mit ihnen auch wichtiges, firmenspezifisches Fachwissen über die SAP-Systeme ab. Sollten die Nachfolger dann am nächsten SAP Security Patch Day aufgrund mangelnder Kenntnis einen relevanten Patch übersehen, ist die gesamte Systemlandschaft gefährdet.

3 Historisch gewachsene Systemlandschaften

Die meisten SAP-Systeme in Unternehmen sind historisch gewachsen. Da sie teils über Jahre nach und nach erweitert wurden, gibt es nur in den seltensten Fällen jemanden im Unternehmen, der seit Beginn der Einführung dabei war und mit allen Besonderheiten vertraut ist. Gerade bei kleineren Unternehmen laufen daher oft SAP-Systeme, die vor Jahren aufgesetzt und seitdem nicht gepatcht wurden, weil es niemanden gibt, der sich im Detail auskennt. Sie sind ein enormes Sicherheitsrisiko, das schnell behoben werden sollte.

4 Digitale Transformation

Die digitale Transformation im Allgemeinen und die Umstellung auf SAP S/4HANA bis spätestens 2030 im Speziellen ist für viele Unternehmen ein Mammutprojekt, das umfangreiche Ressourcen der IT-Abteilung bindet. Das bringt Verantwortliche vor dem Hintergrund eines chronischen Fachkräftemangels in ein Dilemma. Wer seine bestehenden IT-Ressourcen für eine umfassende Digitalisierung einsetzt, muss trotzdem permanent sicherstellen, dass diese nicht an anderer Stelle fehlen – zum Beispiel im Bereich IT-Security. Und auch für die Fachkräfte selbst ist es in Anbetracht der fordernden Aufgaben und der umfangreichen Projekte immer schwieriger, stets auf dem neuesten Stand zu bleiben, um Angriffe abzuwehren.

Vorteile der Zusammenarbeit mit einem erfahrenen Partner

Unternehmen, die ihre SAP-Systeme dauerhaft und effektiv schützen möchten, sollten beim Thema IT-Security auf die Zusammenarbeit mit einem erfahrenen Partner setzen. Dort überwachen Sicherheitsexperten alle relevanten Updates, Vulnerability Reports und Security Notes und sind so immer auf dem neuesten Stand hinsichtlich möglicher akuter Bedrohungen. Sämtliche bekannt gewordenen Schwachstellen, die die SAP- Systeme des Kunden betreffen, werden dann umgehend mindestens gemeldet, oder (falls im Leistungsumfang enthalten) direkt gepatcht – natürlich in Absprache mit dem Kunden. Zweiteres geht am schnellsten und unkompliziertesten, wenn die SAP-Landschaft direkt im dienstleistereigenen Rechenzentrum gehostet wird.

Was ein versierter Security-Partner mitbringen muss

Um herauszufinden, was ein geeigneter Dienstleister mitbringen muss, gibt es einige Anhaltspunkte, die bei der Auswahl eine Rolle spielen sollte:

- **Technische Expertise und Know-how im SAP-Umfeld**

  Nur wer sich mit den zu schützenden SAP-Systemen auskennt, kann dafür sorgen, dass Schwachstellen schnell gepatcht und nicht zum Einfallstor für Cyberattacken werden.

- **Eigenes Security Operations Center (SOC) mit 24/7-Betrieb**

  Ein SOC ist mit spezialisierten Profis besetzt, für die IT-Sicherheit zum Tagesgeschäft gehört. Sie erstellen ein Gesamtbild der aktuellen Bedrohungslage und leiten bei Angriffen oder anderen kritischen Ereignissen umgehend Gegenmaßnahmen ein.

- **Enger Kontakt zu SAP**

  Wer sich einen offiziellen SAP-Partner an die Seite holt, profitiert unter anderem von dessen direkten Kommunikationskanälen mit entsprechenden Experten. Das beschleunigt die notwendige Abstimmung im Notfall und verringert Abhängigkeiten – ein entscheidender Vorteil, wenn es darum geht, seine SAP- Systeme bei einer Attacke zu schützen.

- **SAP Hosting**

  Idealerweise kombinieren Unternehmen die Auslagerung von Security-Dienstleistungen mit der Entscheidung, die Systeme extern hosten zu lassen. Dann liegen die SAP-Systeme auch physisch bei einem versierten Partner, der ein SOC betreibt und ihnen alle Services aus einer Hand bieten kann.

- **Branchenspezifische Beratung**

  Ein erfahrener Dienstleister kennt sich nicht nur mit technologischen Aspekten aus, er weiß auch um branchenspezifische Anforderungen und Besonderheiten. So kann er beispielsweise in einem Fertigungsbetrieb die zuständigen IT-Fachkräfte beraten, wie sich eine geplante Downtime für Security Patches mit dem Produktionsplan vereinbaren lässt.

Syntax - Ein Partner auf Augenhöhe

Security ist Vertrauenssache, deswegen spielt bei der Wahl des richtigen Anbieters neben den oben genannten „harten“ Faktoren auch immer die menschliche Komponente eine wichtige Rolle. Verantwortliche für IT-Security erwarten eine Beratung auf Augenhöhe und professionelle Unterstützung. Sie wünschen sich einen kompetenten und verlässlichen Partner, der ihnen dabei hilft, beim Thema Security gegenüber dem Management und den operativen Teams im eigenen Betrieb mit konkreten Zahlen und Fakten (zum Beispiel anhand einer Bewertung bekannter Schwachstellen auf einer Severity-Skala) wichtige Überzeugungsarbeit zu leisten. Als langjähriger und erfahrener Hosting- und IT-Experte unterstützt Syntax seine Kunden als SAP-Partner bei der Entwicklung und Umsetzung einer Sicherheitsstrategie – egal ob die betroffenen Systeme On-Premises oder in einer bei Syntax gehosteten Private Cloud liegen. Ein detailliertes Statement of Work (SOW) regelt die Zuständigkeiten und Services, um alle eingesetzten SAP-Systeme auf dem aktuellen Stand zu halten. Es bietet dem Kunden ein flexibles Patch-Management, das von präventiven Maßnahmen wie einem einfachen Hinweis auf entdeckte Sicherheitslücken im System über ein automatisches Patchen bis hin zu weiterführenden Maßnahmen im Fall eines Angriffs sowie schnelle Hilfe im Notfall reicht. Das entlastet die IT-Abteilung, die sich dann mit einem sicheren Gefühl auf wertschöpfende Aufgaben konzentrieren kann.

Checkliste für Security-Partner

- ☑ **SAP-Know-how und Security-Expertise aus einer Hand**
- ☑ **Enger, direkter und permanenter Kontakt mit SAP**
- ☑ **Eigenes Security Operations Center mit 24/7-Betrieb**
- ☑ **Tatkräftige Unterstützung im Notfall**
- ☑ **Breites Service-Spektrum von präventiven Maßnahmen bis zum aktiven Eingreifen bei Angriffen**

SAP Vulnerability Management ist ein Security Service von Syntax und somit ein Teil des Security-Portfolios, das wir unseren Kunden anbieten. Weitere Services runden die Sicherheit Ihres Unternehmens ab.

Geren beraten wir Sie zum rund um das Thema Sicherheit und Abwehr von Gefahren – damit Sie SICHER in die Zukunft blicken können.

SYNTAX

SYNTAX

Über Syntax

Syntax ist ein global agierender IT-Dienstleister und einer der führenden Managed Cloud Provider für den Bereich Enterprise Critical Applications. Spezialisiert auf IT-Lösungen für die Fertigungsindustrie und weitere Branchen, bietet das Unternehmen ein breites Spektrum an Technologielösungen, zuverlässige Professional Services, umfassende Beratungsleistungen sowie bewährte Application Management Services – damit die geschäftskritischen Cloud-Anwendungen der Kunden jederzeit performant, zuverlässig und zukunftsorientiert arbeiten.

In Europa gehört Syntax zu den SAP-Partnern der ersten Stunde und verfügt über eine einmalige Kombination aus Manufacturing-Know-how und SAP-Expertise.

Mit 50 Jahren Erfahrung und mehr als 700 Kunden auf der ganzen Welt verfügt Syntax über fundiertes Know-how bei der Implementierung und dem Management von Multi-ERP-Installationen in geschützten privaten, öffentlichen oder hybriden Umgebungen. Syntax arbeitet eng mit SAP, AWS, Microsoft und anderen führenden Technologieanbietern zusammen, um zu gewährleisten, dass die Anwendungen der Kunden nahtlos und sicher funktionieren – als solide Basis für unternehmensweite Innovationskraft.

Hauptsitz des 1972 gegründeten Unternehmens ist das kanadische Montreal, die Europazentrale liegt in Weinheim. Darüber hinaus hat Syntax weitere Niederlassungen in Asien, Nord- und Mittelamerika sowie Europa.

SAP Gold Partner

Syntax Systems GmbH & Co. KG
Höhnerweg 2-4
69469 Weinheim, Germany
+49 (0)6201 80-8008
kontakt@syntax.com
syntax.com/de-de/