Der Sicherheits-Chef

Ohne SAP-Software läuft in vielen Firmen nichts. Das Problem: Wer sich nicht ausreichend um sein System sorgt, hat schnell ein ernsthaftes Sicherheitsproblem, das die Unternehmens-Existenz bedroht

SAP-Systeme sind das Rückgrat der deutschen Wirtschaft“, sagt Markus Schumacher. „Sie sind sozusagen die Kronjuwelen.“ Das Problem: Nur wenigen Firmen ist klar, dass ein SAP-System ebenso wie Juwelen geschützt werden müssen. „Uns ist noch nie was passiert! Das höre ich häufiger. Bis die Firma dann Montagabend bei Wiso im ZDF kommt, weil die Personaldaten gehackt worden sind.“ Schumacher, Geschäftsführer des Heidelberger Softwaredienstleisters Virtual Forge, erklärte der Karlsruher IT-Sicherheitsinitiative, wo die Schwachpunkte liegen und wie diese ausgemerzt werden.

Schumacher macht deutlich, dass die Gefahr nicht von einer fehlerhaften Software ausgeht, „die Verantwortung für die Sicherheit trägt derjenige, der das System konfiguriert. SAP ist angreifbar, wenn Unternehmen nicht von Anfang an auf die Sicherheit achten.“ Je komplexer das System ist, desto größer ist die Herausforderung. Die Sicherheitsmaßnahmen liefert SAP gleich mit, nur müssen die auch ergriffen werden. „Viele Firmen agieren da zu sorglos.“ Und so führt der Experte in wenigen Minuten vor, wie der komplette Datenbestand eines Maschinenbauers theoretisch – ohne große Mühe und mit wenig Know-how – ausgelesen werden kann.

Laut Schumacher besteht bei vielen Unternehmen akuter Handlungsbedarf. „In einem SAP-System muss klar festgelegt sein, welcher Nutzer was darf. Ein funktionierendes Berechtigungskonzept hat zentrale Schutzfunktion.“ Er schlägt das Prinzip der minimalen Berechtigung vor. Wichtig dabei: Das System darf keine Widersprüche aufweisen.

Die zweite Maßnahme betrifft die Implementierung des Systems. „Die SAP-Basis muss gehärtet werden“, so der Softwarespezialist. Dazu gehören die Standards wie Sicherung des Netzwerks, Virenscanner, Verschlüsselung, Überwachung von Notfall-Support-Usern oder regelmäßiges Ändern der Sicherheits-Kennwörter.

„Drittens ist eine sichere Programmierung unerlässlich“, erklärt Schumacher. „Heißt: frei von Hintertüren und bekannten Sicherheitslücken.“ Dazu gehört regelmäßiges Testen der Konfiguration ebenso wie die Aktualisierung der Software. „SAP-Sicherheit ist ein dauerhafter Prozess, der alle Unternehmensbereiche betrifft.“ Schumacher fordert deshalb: „Alle Beteiligten müssen miteinander arbeiten.“ Damit die Kronjuwelen bleiben, wo sie sind – im Unternehmen. ***Robert Schwarz***

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Neue Mitglieder

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) hat drei neue Mitgliedsunternehmen.

Virtual Forge hat seinen Sitz in Heidelberg und entwickelt Sicherheitstests und -programme für SAP-Systeme.

Die InnovIT AG ist Spezialist im Rechenzentrumsbau. Das Unternehmen um die Vorstände Ralf Ebenig, Dirk Stockschläder und den Vorstandsvorsitzenden Jörg Tennigkeit hat seinen Sitz in Seeheim-Jugenheim.

Rittal aus Herborn entwickelt etwa Schaltschränke, Elektronik-Aufbau-Systeme sowie System-Klimatisierungen und gehört zur Friedrich-Loh-Gruppe.

Standard in den Firmen, aber falsch konfiguriert kann SAP ein Sicherheitsrisiko sein

Foto: Jigal Fichtner