Link: https://www.computerwoche.de/a/100-prozent-sicher-geht-nicht,2501749

Produktsicherheit

100 Prozent sicher geht nicht

Datum: 12.01.2011
Autor(en): Elke Senger-Wiechers

Die Firewall als Schutz vor Angriffen auf die Applikationslandschaft bietet angesichts immer neuer Bedrohungen längst keine ausreichende Sicherheit mehr. Standardisierte Schnittstellen und einheitliche Datenübertragungsprotokolle stellen sowohl an die Softwareentwicklung als auch beim Betrieb neue Anforderungen hinsichtlich der Sicherheit.

Die Trojaner Stuxnet und Duqu demonstrierten eindrucksvoll, was ein modernes Angriffsszenario ausmacht: Die Manipulation ist so gut getarnt und so minimal, dass sie über lange Zeit unbemerkt bleibt - der Schaden kann dabei von Kleinstbeträgen, die monatlich auf ein Konto wandern, bis zur Sabotage kritischer Systeme reichen. "Das war erst die Spitze des Eisbergs", glaubt Sachar Paulus, Senior Analyst beim auf IT-Sicherheit spezialisierten Beratungshaus KuppingerCole. Er geht davon aus, dass Spionage und Sabotage durch das organisierte Verbrechen in Zukunft eine der Hauptbedrohungen für Unternehmen darstellen. Die für die "IT Security"-Studie von IDC befragten 200 Unternehmen halten aktuell jedoch die eigenen Mitarbeiter für das schwächste Glied in der IT-Security-Kette. "Rein von den Möglichkeiten stimme ich zu", kommentiert Paulus.

Über mögliche Missbrauchsfälle nachdenken

Von Fehlbedienungen und falschem Einsatz der Software geht die größte Gefahr aus. Gerade bei ERP-Software treffe es sehr häufig zu, dass eine entwickelte Software eine bestimmte Branche unterstützt. Während des Betriebs ergebe sich dann aber ein anderer industrieller Einsatz. "Schon hat man einen Kontext mit einer Bedrohungssituation, an die bei der Entwicklung nicht gedacht wurde", beschreibt Paulus das Problem. "Für Softwarehersteller ist das sehr schwierig zu antizipieren." Schon in der Planung eines Produktes müssen sie sich daher über mögliche Missbrauchsfälle Gedanken machen und entsprechende Sicherheitsanforderungen formulieren. Rund 200 davon fließen in neue Produkte etwa von SAP ein. Damit die Anforderungen laufend aktuell bleiben, beschäftigt das Walldorfer Softwarehaus ein Expertenteam. "Die Sicherheitsanforderungen bilden die Grundlage für unsere Arbeit in Entwicklung, Validierung, Qualitätssicherung und vielen anderen Bereichen des Unternehmens. So haben wir die Chance, Sicherheitslücken idealerweise von vornherein zu vermeiden oder aber frühzeitig zu entdecken und binnen kürzester Zeit zu schließen", so Gunter Bitz, Leiter Produktsicherheit Governance. Zusätzlich werden noch während der Codierungsphase und am fertigen Produkt mittels laufender, standardisierter Testverfahren mögliche Fehler erkannt und zeitnah korrigiert.

SAP in der BSIMM-Studie vorne dabei

In Benchmark-Studien rangieren die Produkte der Walldorfer am oberen Ende der Sicherheitsskala. Bei der jüngsten Building- Security-In-Maturity-Model-Studie (BSIMM) schnitt SAP als eines der zehn besten Unternehmen ab. An der Studie haben 42 Unternehmen teilgenommen und freiwillig ihre Sicherheitsstandards überprüfen und gegeneinander abgleichen lassen - darunter Microsoft, Google und Symantec. "Solche Netzwerke sind für große Softwarehersteller sehr wichtig, um sich auszutauschen und ihr Wissen aktuell zu halten", erklärt Paulus. Er selbst war Gründungsmitglied der Non-Profit- Vereinigung SAFECode, wo auch SAP-Mann Bitz im Vorstand sitzt. "Das Ziel, von SAFECode ist es, auch Herstellern, die sich keine eigene Research-Abteilung leisten können, Best Practices zur sicheren Softwareentwicklung zugänglich zu machen", erläutert SAP-Experte Bitz.

"Unverantwortlich, Patches zu ignorieren"

eMagazin SAP AGENDA zum Thema Unternehmen sicher machen

Wieso Firmen Patches nicht ernst nehmen - Wie Identity Management bei der TU Darmstadt neu justiert wurde und Wo die Cloud-Daten sicher sind- erfahren Sie, im aktuellen **eMagazin SAP AGENDA**[2].

Bisher sind noch keine größeren Angriffe auf SAP-Systeme bekannt geworden. Was jedoch nicht so bleiben muss. "Auf Sicherheitskonferenzen hat das Thema SAP-Sicherheit in den letzten Jahren zugenommen", meint Fritz Bauspieß, Mitarbeiter im Global Active Support bei SAP. Er und sein Team helfen den Kunden mit Informationen, Services und Tools, ihre IT-Systeme sicher zu konfigurieren und zu betreiben. SAP stellt zudem Security-Patches zur Verfügung, auch für Produkte, die längst am Markt sind. Genau hier schlummert aber eines der größten Risiken. "Von den Anwendern ist es absolut unverantwortlich, diese Patches zu ignorieren und nicht sofort einzuspielen", sagt Paulus. Weiter hätten sie auch die Pflicht, dem Hersteller bereits im Vorfeld ihre Anforderungen zu kommunizieren und sich nach einem Security-Management-System wie der ISO-27001-Zertifizierung zu richten. "Die aktive Mitwirkung der Anwender durch entsprechend sichere Konfiguration und Nutzung der Software ist unerlässlich", meint auch Support-Mann Bauspieß. "Ohne sie lässt sich kein sicherer Betrieb erreichen." Letztlich müsse jedoch jedes Unternehmen selbst entscheiden, welches Restrisiko es zu tragen bereit sei.

Links im Artikel:

[1] **http://itunes.apple.com/de/app/sap-agenda/id454699216?mt=8**

[2] **https://www.computerwoche.de/subnet/sap/agenda201104/**
