Der sichere Außenposten

Fraunhofer IEM garantiert höchste Sicherheitsstandards bei „Vor-Ort"-Datenlösung OSIRIS

Wie gelingt eine sichere Datenablage, ein geschützter Datenaustausch auch an unsicheren Orten? Besonders für weltweit agierende Unternehmen stellt sich diese Frage immer öfter. Die preisgekrönte Plattform OSIRIS kann genau das. Bei ihrer Entwicklung setzte Janz Tec von Beginn an auf die Zusammenarbeit mit dem Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM. Nach dem Prinzip „Security by Design" begleitete das Forschungsinstitut die Erarbeitung des Sicherheitskonzeptes und prüft auch das fertige Produkt auf Herz und Nieren. Konkret heißt das: Die Forscher versuchen, OSIRIS zu hacken.

„Bisher ist uns das nicht gelungen, sowohl Soft- als auch Hardware von OSIRIS sind extrem sicher", stellt Sven Merschjohann, Wissenschaftler am Fraunhofer IEM, gleich zu Beginn klar. „Trotzdem: Vor allem Software ist niemals ‚fertig'. Ständig müssen zum Beispiel aktuelle Versionen aufgespielt werden." Deshalb hat Sven Merschjohann besonders darauf geachtet, dass OSIRIS über einen zuverlässigen Mechanismus für zukünftige Softwareupdates verfügt.

Regelmäßige Aktualisierungen sind nur ein Bestandteil des Sicherheitskonzeptes, das Janz Tec, Paderborner Experte für industrielle Computersysteme, gemeinsam mit den Wissenschaftlern des Fraunhofer IEM eigens für seine mit dem Prädikat „BEST OF 2017" beim INNOVATIONSPREIS IT 2017 ausgezeichnete Secure Appliance Lösung erstellt hat. Das fertige Sicherheitskonzept ist Ergebnis umfangreicher Arbeiten bereits im Produktentwicklungsprozess: Das Thema Sicherheit wurde bei OSIRIS gleich zu Beginn in der Konzeptphase als explizite Anforderung an Hard- und Software aufgenommen. „Dieser integrative Ansatz verringert zum einen unsere Entwicklungszeit, zum anderen haben wir nun ein Produkt mit perfekt abgestimmten Sicherheitskomponenten, die nicht erst nachträglich – also im Ernstfall – nachgerüstet werden müssen", erläutert Dr. Markus von Detten, Leiter Systems Engineering und Softwareentwicklung bei Janz Tec.

IT-Sicherheit: bedarfsgerecht für jedes Budget

Der ganzheitliche Ansatz, der Maßnahmen zur Entwicklung sicherer software-intensiver Systeme von der Anforderungserhebung bis hin zum fertigen Produkt direkt integriert, nennt sich „Security by Design". Noch im Entwurfsstadium von OSIRIS führten die Entwickler eine umfangreiche Bedrohungsanalyse durch. Aus verschiedenen Szenarien zu Schwachstellen im System oder zu Angriffen von außen leiteten sie Schutzziele ab, die sie im weiteren Entwicklungsprozess stets im Blick behielten.

Gerade für kleine und mittlere Unternehmen ist es wichtig, hierbei den Kosten-Nutzen-Aspekt zu berücksichtigen. Um das Entwicklungsbudget und auch die Kosten für das Endprodukt nicht durch unnötige Features zu belasten, sollte kritisch hinterfragt werden, welche Sicherheitsmaßnahmen für das jeweilige Produkt tatsächlich nötig sind. „Ich bin überzeugt, dass es auch für mittelständische Unternehmen pragmatische Lösungen mit überschaubaren Kosten gibt. IT-Security kann sich jeder leisten: Mit einem vernünftigen und bedarfsgerechten Konzept", so Sven Merschjohann.

OSIRIS ist eine große Lösung für die Industrie, die viel können muss: Es geht um einen sicheren Außenposten für Produkt- und Prozessdaten, einen sicheren und effizienten Datenaustausch zwischen weltweit verteilten Teams oder ganzen Produktionsstätten mit dem heimischen Server.

Redaktion
Kirsten Harting | Fraunhofer IEM | Telefon +49 5251 54 65-107
Zukunftsmeile 1 | 33102 Paderborn | www.iem.fraunhofer.de | kirsten.harting@iem.fraunhofer.de

Daten sollen lokal sicher abgelegt werden und „unter Aufsicht“ mit der Zentrale synchronisiert werden. Deshalb ist das Sicherheitskonzept von OSIRIS umfangreich und erfüllt höchste Standards. Detailliert beschreibt es sowohl den physischen Aufbau als auch die Softwarestruktur und gibt an, welche Maßnahme in welchem Szenario greift. Die Wissenschaftler vom Fraunhofer IEM haben die einzelnen Vorkehrungen sorgfältig geprüft: Wo und wie liegen sensible Informationen physisch auf der Plattform? Welche kryptographischen Methoden werden verwendet? Werden ausreichend Authentizitätsnachweise gefordert? Entsprechen die Verschlüsselungen den gängigen Standards? Sind für OSIRIS regelmäßige Softwareupdates auch im laufenden Betrieb vorgesehen? Orientierung zu Richtlinien und Standards bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI), die internationale ISO/IEC 27000-Reihe sowie die IEC 62443, die die Grundlage der Arbeit der Wissenschaftler am Fraunhofer IEM war.

Auf dem Prüfstand

Exzellente Software-Entwickler und die Handbücher des BSI hat Janz Tec selbst. Trotzdem hält Dr. Markus von Detten eine Zusammenarbeit mit den Fraunhofer-Forschern für unerlässlich: „Unsere Kunden verlassen sich auf die uneingeschränkte Sicherheit unserer Produkte, da sichern wir uns doppelt ab, mit einem neutralen Blick von außen.“

Diese doppelte Absicherung führt so weit, dass sich Sven Merschjohann schließlich in die Rolle eines potenziellen Angreifers versetzt. Systematisch versucht er, Sicherheitslücken der OSIRIS-Software zu finden und sich – dieses Mal ohne Zugangsberechtigung - Zugriff auf die Plattform zu verschaffen. So stellt Janz Tec sicher, dass die Daten seiner Kunden bestmöglich abgesichert sind und nicht in Hände unberechtigter Dritter gelangen können. Würde sich ein Einfallstor finden, könnte Janz Tec diesen Fehler sofort an seine Kunden kommunizieren und ihn beim nächsten Update beheben. Bei OSIRIS kratzt Sven Merschjohann jedoch vergeblich an der Tür: Alle Schlösser bleiben versiegelt.

Redaktion
Kirsten Harting | Fraunhofer IEM | Telefon +49 5251 54 65-107
Zukunftsmeile 1 | 33102 Paderborn | www.iem.fraunhofer.de | kirsten.harting@iem.fraunhofer.de

Sicherer Datenaustausch vor Ort und mit der Unternehmensszentrale: Das Fraunhofer IEM hat das Sicherheitskonzept der Server-Plattform OSIRIS auf Herz und Nieren geprüft.

Foto: Janz Tec / Fraunhofer IEM

Redaktion
Kirsten Harting | Fraunhofer IEM | Telefon +49 5251 54 65-107
Zukunftsmeile 1 | 33102 Paderborn | www.iem.fraunhofer.de | kirsten.harting@iem.fraunhofer.de

Sven Merschjohann vom Fraunhofer IEM prüft den „sicheren Außenposten“ OSIRIS auf höchste Software-Sicherheitsstandards.

Foto: Fraunhofer IEM

Redaktion
Kirsten Harting | Fraunhofer IEM | Telefon +49 5251 54 65-107
Zukunftsmeile 1 | 33102 Paderborn | www.iem.fraunhofer.de | kirsten.harting@iem.fraunhofer.de