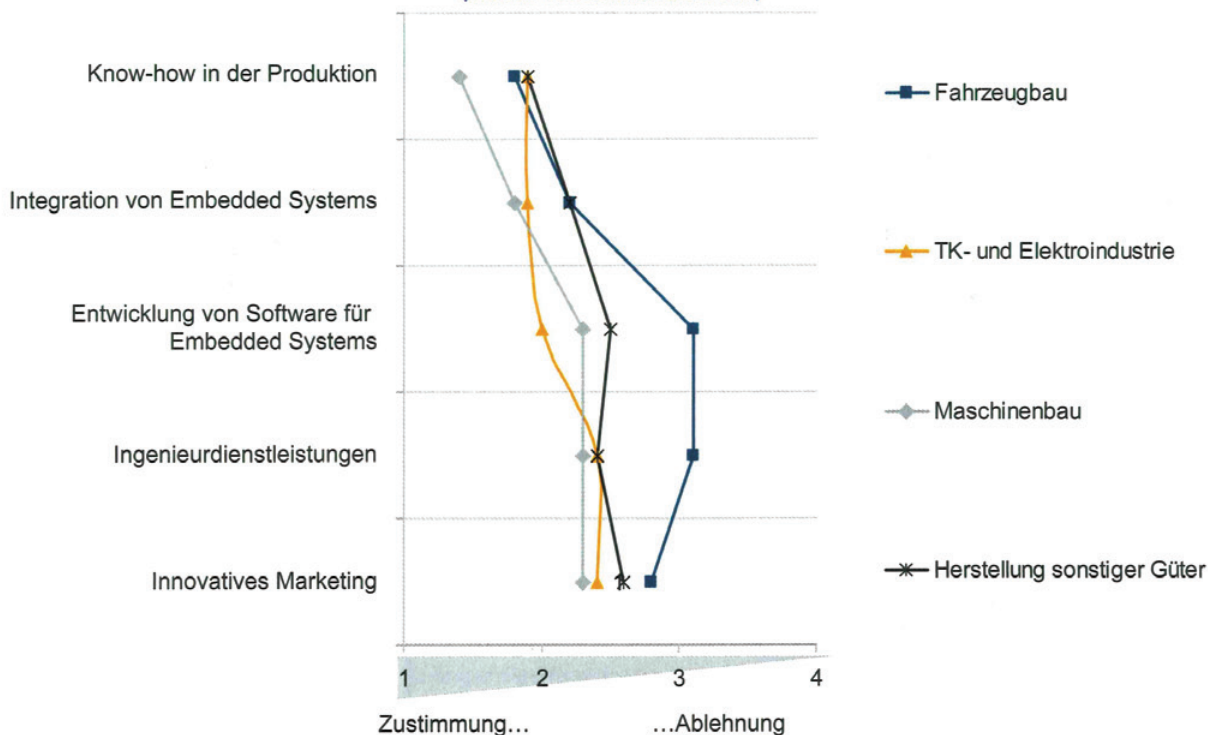


Embedded-Systeme können den Unterschied machen

(Basis 176 Unternehmen)



Alleinstellungsmerkmale aus Anwendersicht nach Branchen (Quelle: BITKOM 2008)

Embedded: Marktchancen durch Spezialwissen

Embedded-Systeme haben strategische Bedeutung für die Investitionsgüterindustrie. Vernetzte Anwendungsbereiche erhöhen dabei die Gefahr durch externe Manipulation. Projektfelder skizziert Thomas Müller, Geschäftsführer SOLCOM Unternehmensberatung GmbH.

Welche modernen Arbeitsmethoden markieren hauptsächlich moderne Embedded-Sicherheitslösungen?

Thomas Müller: Mit dem durch die NSA verifizierten Sicherheitskonzept MILS (Multiple Independent Levels of Security) sind die USA Vorreiter auf diesem Gebiet. Das Konzept bzw. vergleichbare Methoden finden ebenso bei uns Anwendung. Elementar wichtig ist nicht nur die Arbeitsmethodik sondern eine konsequente Vorgehensweise die bis zum letzten Detail verfolgt wird. Das gesamte Sicherheitskonzept ist immer nur so gut wie das

schwächste Glied in der Kette. Denn genau hier setzen potenzielle Angreifer an. Da in den meisten Fällen von einer einzigen Sicherheitslücke ausgegangen wird, sind differenzierte und mehrstufige Sicherheitsebenen eine sinnvolle Maßnahme, um ein Eindringen erfolgreich zu verhindern.

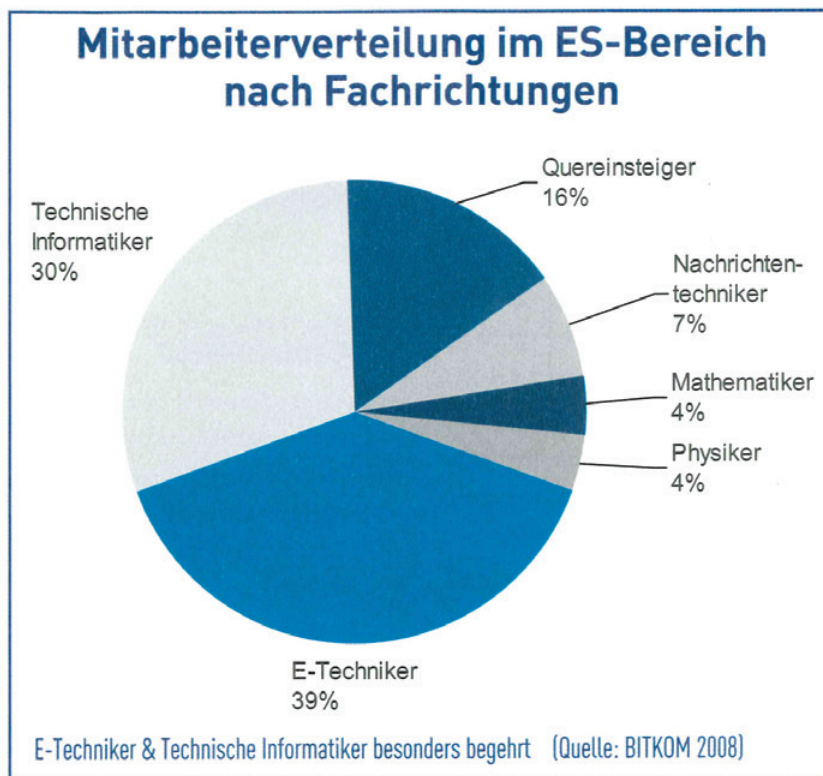
Welche wichtigen Sicherheits-Projekte können im Embedded-Umfeld entstehen?

Thomas Müller: Die Liste ist so lang wie der Einfallsreichtum derjenigen Personen reicht, die sich mit dem Aus-

hebeln von Sicherheitslösungen beschäftigen. Dazu gehören z. B. Schutz von Firmware und Hardware durch Fremdmodifikation, Mechanismen zu Produkt- und Kopierschutz, Management von Berechtigungen und Schlüsselverteilungen für kryptographisch abgesicherte Anwendungen und Verschlüsselung von Messgeräten und anderen Komponenten, die über ein Datennetz erreichbar sind.



Thomas Müller, Geschäftsführer SOLCOM Unternehmensberatung GmbH: „Die richtige Methodenkompetenz, nachgewiesen durch entsprechende Zertifizierungen und Erfahrungen, ist der Weg zu Projektaufträgen.“



Diese Aufgaben teilen sich im Wesentlichen auf drei Bereiche auf. Erstens Hersteller von Sicherheitsapplikationen wie bspw. Verschlüsselungssoftware / -Tools, Firewalls, fälschungssicheren Produkten bis hin zu Mustererkennung, entsprechenden Sensoren und Biometrie. Zweitens Hersteller von Technik, die besonderen Sicherheitsanforderungen genügen müssen z.B. abhörsicherer Funk, Chipkarten mit kritischen Daten, elektronische Schlüssel. Und Drittens Anbieter von Dienstleistungsangeboten, die die Produkte der beiden bereits genannten Bereiche dem Endnutzer zugänglich machen. Hier sind Angebote notwendig, die die Sicherheitsanforderungen auch methodisch und menschlich berücksichtigen.

Welche Experten mit welchem Know-how sind dafür künftig besonders gefragt?

Welche Nachfrage besteht nach Freelancern in diesem Bereich?

Thomas Müller: Kaum ein Hersteller von allgemeiner oder spezieller Sicherheitstechnik lässt sich in die Karten schauen und unternehmenskritisches Spezialwissen ist nur sehr wenigen bekannt.

In den Kern, und darum geht es bei Embedded-Systemen, werden nur wenige Externe vorstoßen können. Die Anwendung der erwerbaren Produkte und deren sicherheitsorientierter Einsatz wird im Wesentlichen das Aktivitätsfeld sein. Hier ist die richtige Methodenkompetenz, im besten Fall nachgewiesen durch entsprechende Zertifizierungen und

Erfahrungen, der Weg um entsprechende Projektaufträge zu erhalten. Wenn wir das Ethernet-Umfeld als Beispiel heranziehen dann sind neben fundierten Erfahrungen in der embedded Entwicklung auch Know-how in Technologien wie IPsec, VPN, Encryption, IKE, Firewalls, Signatures, Authentication, DoS, SSL sowie TCP/IP, NAT und Portforwarding von Vorteil.

Wie zahlt sich Spezial-Know-how aus?

Thomas Müller: Embedded-Systeme verrichten ihren Dienst in einer Fülle von Anwendungsbereichen. Oftmals bestehen auch komplexe Gesamtstrukturen aus einer Vielzahl solcher Systeme. Durch die zunehmende und weitreichende Vernetzung dieser Anwendungsbereiche, steigt auch die Gefahr durch externe Manipulation beziehungsweise Schädigung. Hier zeichnen sich enorme Marktchancen für Spezialwissen ab. Trotz der Brisanz findet allerdings oft eine Verdrängung der Sachverhalte bei den meisten Unternehmen statt. Die Gefahr ist zwar identifiziert, wird aber nicht ausreichend in den Fokus gerückt. Meistens gibt erst ein größerer Zwischenfall Anlass für eine Priorisierung dieses Themas, der sich dann auch in konkreten Projekten und damit einer verstärkten Nachfrage nach Spezialwissen bemerkbar macht.

Link
www.solcom.de