Keine Chance für Industriepiraten und Co

Keine Chance für Industriepiraten und Co
Was anmutet wie in einem Science-Fiction-Film, soll in den Produktionshallen der Zukunft bald Realität werden: Produkte, die in Fertigungslinien wissen, wo sie sind, welche Schritte sie bereits durchlaufen haben und was ihnen zum fertigen Produkt noch fehlt. Die Anlagen stimmen ihre Arbeitsschritte miteinander ab und tauschen Informationen aus. Der Techniker muss die Hallen für die Wartungen nicht mehr betreten, sondern überprüft die Maschinen aus der Ferne. Kurzum: Produkte und Anlagen werden intelligent. Man spricht dabei auch von Industrie 4.0, also der Industrie der vierten Generation nach Mechanisierung, Elektrifizierung und Digitalisierung.
Einer der Knackpunkte: Die Anlagen kommunizieren über ein Datennetz miteinander, und auch die Produkte müssen sich einloggen. Der Mensch steuert und überwacht die Produktion über diese Netzverbindung - so behält er die Anlagen auch dann im Blick, wenn er gerade nicht in der Produktionshalle ist. Hinzu kommen Fernwartungen und Fernaktualisierungen von Software. Für all diese Funktionen ist eines unabdingbar: Ein sicherer Zugang, der Industriepiraten und Saboteuren den Zugriff verweigert. Zwar können Unternehmer die normale Internetverbindung für einen solchen Datenverkehr nutzen, und sie etwa über ein Virtual Private Network, kurz VPN, absichern. Was viele jedoch nicht wissen: VPN ist nicht gleich VPN - und nicht jeder VPN-Zugang ist sicher, verrät Bartol Filipovic, Bereichsleiter am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC in Garching.
Die Forscher haben einen Router entwickelt, der über einen sicheren VPN-Zugang verfügt, Berechtigungs- und Firewall-Funktionalitäten sichern diesen weiter ab. Die notwendigen Sicherheitsprotokolle können auch direkt in die Anlagen und Maschinen beim Industriekunden integriert werden. Das System ist ein Software-Bausatz: Die Basiskomponenten haben wir bereits entwickelt, diese können wir dann jeweils an die speziellen Anforderungen der Kunden anpassen, sagt Filipovic. Das dauert etwa vier Wochen. Die Forscher integrieren dabei auch einfache Systeme wie Sensoren, die beispielsweise in der Pharmaindustrie Füllstände anzeigen oder die Mischverhältnisse angeben - denn auch diese sollen ihre Information nicht an Unberechtigte weitergeben.
Physischer Schutz: Folie schlägt Alarm
Das System schützt die Unternehmen einerseits vor Spionen, die sich aus der Ferne in das Netz hacken wollen. Anderseits schlägt es auch Datendieben ein Schnippchen, die Routern und Platinen ihre Geheimnisse vor Ort entlocken möchten. Eine spezielle Folie auf den sicherheitsrelevanten Gehäusen meldet sofort, wenn jemand versucht, die Schutzhülle aufzuschrauben, um sensible Daten abzugreifen. Die am AISEC entwickelte Folie wird auf das Router-Gehäuse oder auch direkt auf die Platine, also die Leiterplatte mit den für die Steuerung wichtigen Elementen wie Mikrocontrollern, Chips, Dioden und anderen sicherheitskritischen Recheneinheiten angebracht und an mehreren Punkten verschweißt. Ist der Router ausgeschaltet, ist jegliche Software darauf verschlüsselt abgelegt. Ist er jedoch in Betrieb, so braucht er die entschlüsselten Programmcodes. Der jeweilige Schlüssel hängt von den Folieneigenschaften ab. Verändert man diese - etwa indem man die Folie aufreißt oder durchbohrt, um an die Platine heranzukommen - erkennt die Folie den Angriff in wenigen Millisekunden und handelt umgehend: Sie löscht alle sicherheitsrelevanten Daten, die unverschlüsselt vorliegen.
Unbefugte Eindringlinge kommen nicht an die Software heran. Für den Unternehmer ist das Löschen der Daten jedoch kein Problem: Er kann die Software einfach neu aufspielen und eine neue Folie anbringen. Mit der Kombination aus Software und Folie erreichen wir ein ideales Sicherheitsniveau, sagt Filipovic, und wie wichtig das ist, hat das Jahr 2013 sehr deutlich gezeigt. Sichere Soft- und Hardware für die Kommunikation ist grundlegend für die Weiterentwicklung der Produktion in Richtung Digitalisierung und Industrie 4.0, der Schutz vor Spionage, Sabotage und Produktpiraterie wichtig für Innovation und eine starke Wettbewerbsposition.

Fraunhofer-Gesellschaft
Hansastraße 27 c
80686 München
Deutschland
Telefon: +49 (89) 1205-0
Telefax: +49 (89) 1205-7531
Mail: info@fraunhofer.de
URL: http://www.fraunhofer.de

<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=556774" width="1" height="1">

Pressekontakt

Fraunhofer Gesellschaft

80686 München

fraunhofer.de
info@fraunhofer.de

Firmenkontakt

Fraunhofer Gesellschaft

80686 München

fraunhofer.de
info@fraunhofer.de

Fraunhofer ist die größte Organisation für anwendungsorientierte Forschung in Europa. Unsere Forschungsfelder richten sich nach den Bedürfnissen der Menschen: Gesundheit, Sicherheit, Kommunikation, Mobilität, Energie und Umwelt. Und deswegen hat die Arbeit unserer Forscher und Entwickler großen Einfluss auf das zukünftige Leben der Menschen. Wir sind kreativ, wir gestalten Technik, wir entwerfen Produkte, wir verbessern Verfahren, wir eröffnen neue Wege. Wir erfinden Zukunft.