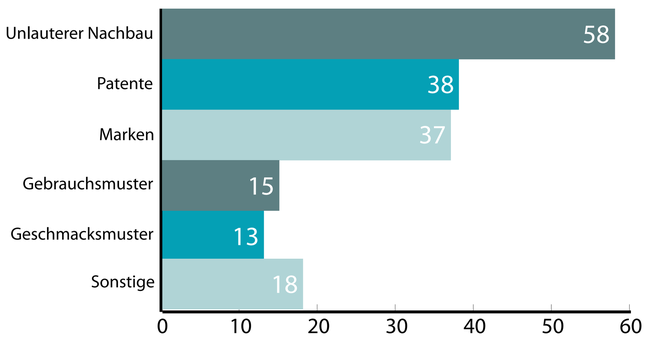
SCHUTZ VOR PRODUKTPIRATEN

Eingebettete Systeme • Know-how • Innovationen • Investitionsgüter • Ideen • Wettbewerbsfähigkeit

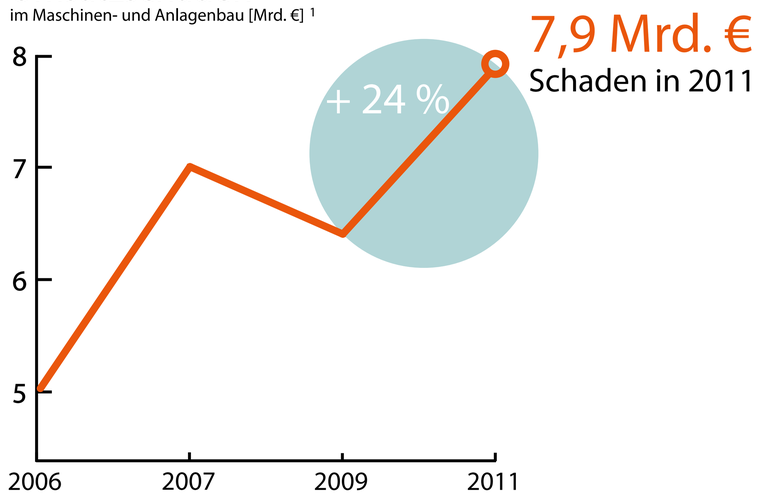
Schutzrechtsverletzungen

Arten der verletzten Schutzrechte durch Produkt- und Markenpiraterie im Jahr 2012 [%], Mehrfachnennungen möglich[1]



Umsatzschaden

im Maschinen- und Anlagenbau [Mrd. €] [1]



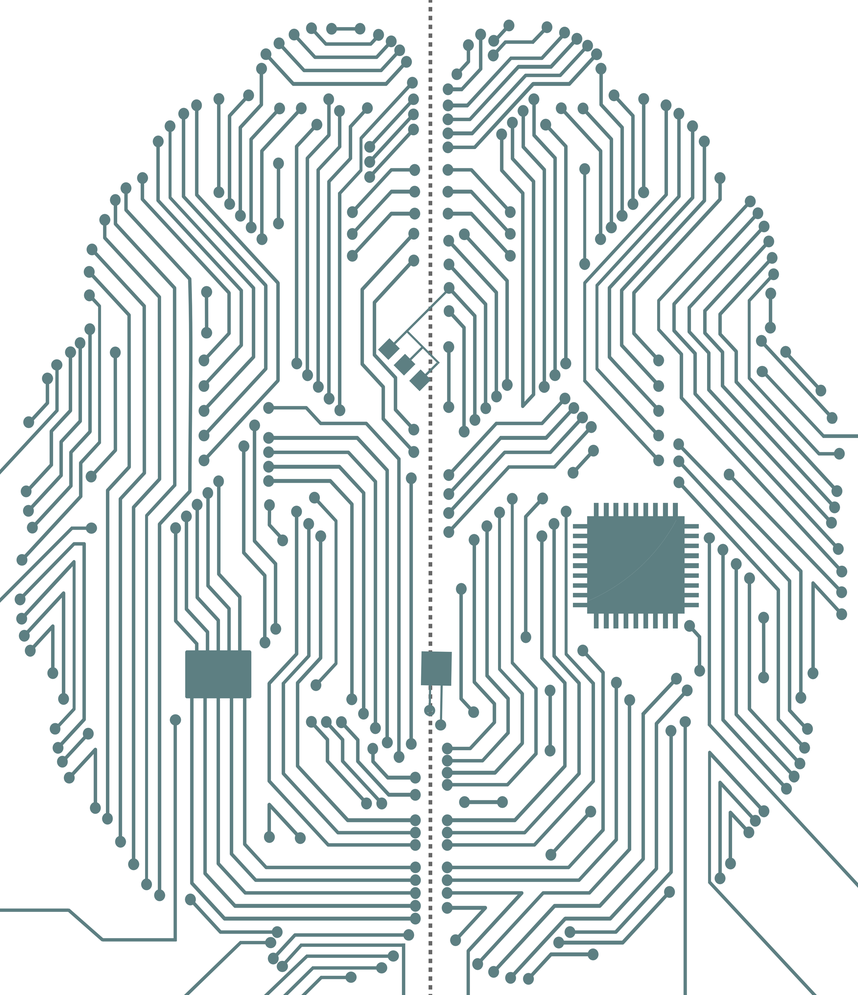
650 Mrd. $
betrug der Gesamtumfang der globalen Schattenwirtschaft im Jahr 2008[3]

44 %
der betroffenen Unternehmen ergreifen nach der Entdeckung eines Plagiats keine weiteren Maßnahmen[1]

ANGRIFFSSZENARIEN[2]

Fokussierung und Spezialisierung
Gezielte Analyse von Kern-Know-how im Produkt, um einen qualitativ gleichwertigen Nachbau zu erhalten

Substitution und Abwandlung
Mangels Technologiebeherrschung erfolgt lediglich funktionale Nachahmung eines Orginals



Hardware Reverse Engineering

Produkt-Teardown
Identifikation des Produktaufbaus, der Bauteile, der internen Platinen und Komponenten

System-Analyse
Analyse der elektronischen Funktionsweise und des Signal-Zeitverlaufs

Prozess-Analyse
Untersuchung der verwendeten Fertigungstechnologie

Schaltkreis-Extraktion
Rekonstruktion der Chip-internen Schaltung

Software Reverse Engineering

Code-Identifikation
Auslesen des Firmware-Codes aus nicht-flüchtigen Speichern (z. B. Flashbausteine) → Analyse des Maschinen-Codes eines Mikrocontrollers → Modifikation im Maschinen-Code ermöglichen Änderungen der Firmware-Funktionalität

Wirtschaftliche Schäden

Produktnachahmung
Know-how-Verlust

GEGENMAßNAHMEN[2]

Individuelle Lösungen aus Hard- und Softwareschutz
Optimalen Schutz bieten Produkt-spezifische Lösungen, bei denen Hardware und Software ineinander greifen und somit Unternehmenswerte im Produkt sichern

Hardware Reverse Engineering

Produkt-Teardown
Kann erschwert werden durch:
Verzicht auf Bauteil-Beschriftungen
Verwendung von Nicht-Standardbauteilen
Vergießen der Schaltung

System-Analyse
Kann erschwert werden durch:
Mehrschichtige Platinen
Verschleierung bzw. Verschlüsselung der elektrischen Signale
Verwendung elektronischer Fingerabdrücke

Software Reverse Engineering

Speicherschutzmechanismen verhindern das Auslesen von Firmware-Code

Verschlüsselung verhindert die Decodierung von Maschinenbefehlen
Veschleierung erschwert die Analyse des Programmablaufs

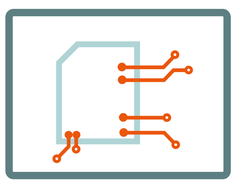
→ Änderungen an der Firmware werden verhindert

Schutz von Unternehmenswerten

Kopierschutz
Know-how-Schutz

Glossar

Produktpiraterie
Verbotenes Nachahmen und Vervielfältigen von Waren, für die ein anderer Hersteller rechtmäßig Erfindungsrechte, Designrechte und Verfahrensrechte besitzt.[4]



Eingebettetes System
Elektronisches System (Computer), das in einen speziellen Anwendungsbereich eingebunden ist.[2]

Reverse Engineering
Prozess, der ein bestehendes System analysiert, um seine Komponenten und ihre Beziehungen zu identifizieren.[5]

Rapid Prototyping
Herstellung von Werkstücken nach einem am Computer erstellten 3D-Modell.[6]

Quellen:
(1) Basierend auf: VDMA (2012): Produktpiraterie 2012.
(2) Fraunhofer AISEC (2011): Schutz eingebetteter Systeme vor Produktpiraterie.
(3) BASCAP (2011): Estimating the global economic and social impacts of counterfeiting and piracy.
(4) Nach Wildemann et al. (2007): Plagiatschutz: Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie.
(5) Nach Chikofsky und Cross (1990): Reverse Engineering and Design Recovery: A Taxonomy.
(6) http://www.golem.de/specials/rapid-prototyping/

Kontakt:
Bartol Filipovic
Parkring 4
85748 Garching bei München

Telefon +49 89 3229986-128
Fax +49 89 3229986-299
bartol.filipovic@aisec.fraunhofer.de
www.aisec.fraunhofer.de

@FraunhoferAISEC

Fraunhofer AISEC