Befragung zur Lage der Hardwaresicherheit in Deutschland 2021 und Anforderungen an eine separate Schutzelektronik

HTV Halbleiter-Test & Vertriebs-GmbH, Bensheim, Deutschland

Kurzfassung

Im täglichen Leben werden Menschen künftig noch mehr elektronischen Bauteilen vertrauen müssen, die beispielsweise in selbstfahrenden Autos, Servicerobotern oder unseren alltäglichen elektronischen Systemen und Geräten zum Einsatz kommen. Zusätzlich werden unter dem Stichwort Internet of Things (IoT) eine steigende Anzahl von Geräten miteinander vernetzt, die wiederum hard- und softwareseitig immer mehr angreifbare Schwachstellen aufweisen.

Das diesem Bericht zugrundeliegende Vorhaben „Verhinderung von Angriffen auf Elektroniksysteme durch innovative Multi-Sensorik“ (VE-SAFE)“ wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16ME0236K vom 01.03.2021 bis 29.02.2024 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren. Im Vorhaben wird eine Überwachungselektronik entwickelt, die zusammen mit einer bislang ungeschützten Kundenelektronik in einer Leiterplatte verpresst wird. Die Überwachungselektronik ist anschließend in der Lage, mögliche Angriffe auf die Hardware (Kundenelektronik) des jeweiligen elektronischen Gerätes zu erkennen und passende Gegenmaßnahmen einzuleiten. Hersteller elektronischer Geräte sollen durch diese zusätzliche adaptierbare Sensorhülle zukünftig in der Lage sein, das Sicherheitsniveau ihrer elektronischen Baugruppen im Bereich der Hardwaresicherheit (bzw. Hardware Security) komfortabel und kostengünstig zu erhöhen.

Die HTV Halbleiter-Test & Vertriebs-GmbH ist einer der weltweiten Marktführer für Dienstleistungen rund um elektronische Komponenten und Spezialist in den Bereichen Test, Programmierung, Langzeitkonservierung und -lagerung, Analytik sowie Bearbeitung elektronischer Bauteile und Baugruppen und führt das Verbundvorhaben zusammen mit dem Fraunhofer IZM und der Jenaer Leiterplatten GmbH durch.

Im Rahmen des VE-SAFE Verbundprojektes führte HTV eine Online-Befragung im Bereich der Hersteller von elektronischen Geräten vom 13.08.2021 bis 12.11.2021 durch, um die Lage der Hardwaresicherheit in Deutschland 2021 zu erfassen und Anforderungen der Nutzer für die in diesem Projekt geförderte separate Schutzelektronik zu ermitteln.

1 Erstellung, Freigabe und Veröffentlichung der Befragung

Die Befragung wurde als Online-Befragung durchgeführt. Der erstellte Fragebogen enthielt vier Abschnitte mit insgesamt 31 Fragen.

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) (vgl. [1]) wurde der finale Fragebogen vor dem Beginn der Befragung für mögliche Korrektureingaben vorgelegt. Das BSI war mit den vorgeschlagenen Inhalten einverstanden und stufte den Detailierungsgrad des Fragebogens als passend ein, um ein gutes Feedback im Bereich der Hardwaresicherheit zu erhalten.

Die Veröffentlichung der Online-Befragung erfolgte über den Newsletter der HTV [2] und des Verbands der Automobilindustrie e.V. (VDA), sowie über unterschiedliche Webseiten der Forschungspartner und der Velektronik-Plattform [3].

Abbildung 1: Titelseite der Online-Befragung

2 Informationen zu den teilnehmenden Unternehmen

Von den angesprochenen Unternehmen füllten insgesamt 10 den Fragebogen zu diesem speziellen, komplexen und Geheimhaltungsanforderung unterliegenden Themenbereich vollständig aus (vgl. Abbildung 2). Die Unternehmen stammten aus den Branchen: Verteidigung, Sicherheitssysteme, Industrie, Großhandel & Entwicklungsdienstleitung, Industrieelektronik, Elektrotechnik, industrielle Automation, Elektronikfertigung, Luft- und Raumfahrt, Automatisierungstechnik und Halbleitertechnologie. Es handelt sich bei den meisten Unternehmen um KMUs (kleine und mittlere Unternehmen), gefolgt von Konzernen und Großunternehmen.

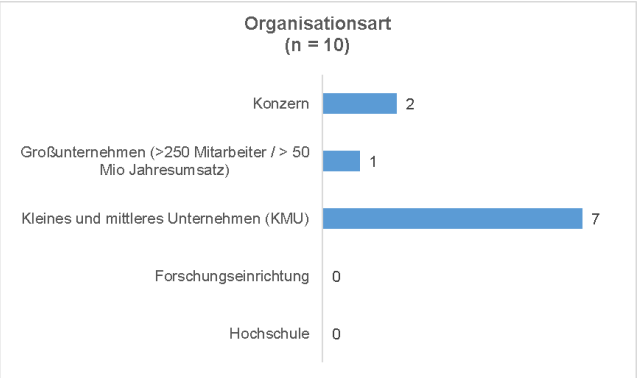

Abbildung 2: Organisationsart der teilnehmenden Unternehmen

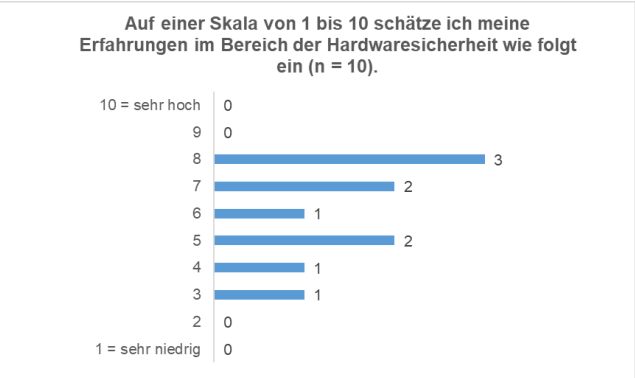

Abbildung 3: Expertise der Umfrageteilnehmer

3 Fragen zur Expertise der Teilnehmenden

Im ersten Abschnitt des Fragebogens wurden die Expertise im Bereich der Hardwaresicherheit befragt. Die Ergebnisse können wie folgt zusammengefasst werden:

- Die Teilnehmenden wiesen eine hohe Expertise im Bereich der Hardwaresicherheit elektronischer Baugruppen auf (vgl. Abbildung 3).
- Auf die Frage an welchen Konferenzen, Wettbewerben, Netzwerken und Arbeitsgruppen, die Teilnehmenden im Bereich der Hardwaresicherheit teilnehmen, wurden das „Infineon Security Partner Netzwerk“ und die „International Microelectronics Assembly and Packaging Society (IMAPS)“ genannt.
- Über Sicherheitslücken informieren sich die Teilnehmenden am häufigsten beim Bundesamt für Sicherheit in der Informationstechnik (BSI), bei Heise.de und über die firmeninterne Kommunikation.
- Die Hardwaresicherheit bei elektronischen Geräten hat für die Teilnehmenden einen hohen Stellenwert.
- Den Teilnehmenden sind im Bereich der Hardwaresicherheit als Standards und Normen am häufigsten die Common Criteria für IT-Sicherheit (CC) bekannt, gefolgt von den Federal Information Processing Standards (FIPS) und der IEC 62443 (Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme) (vgl. Abbildung 4).
- Nur 10% der Teilnehmenden stimmten der Aussage zu, dass die aktuell zur Verfügung stehenden Standards und Normen im Bereich der Hardwaresicherheit ausreichend sind für die Entwicklung sicherer elektronischer Geräte (vgl. Abbildung 5).

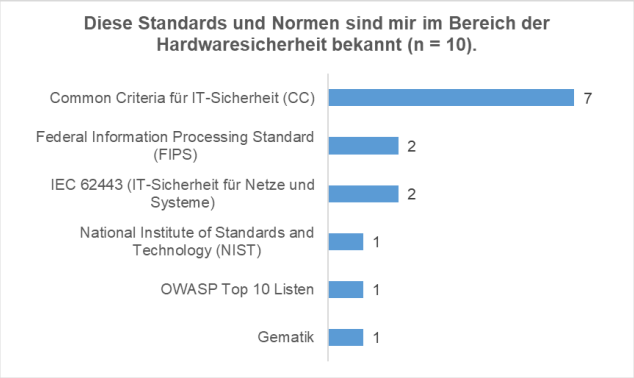

Abbildung 4: Bekannte Normen und Standards im Bereich der Hardwaresicherheit

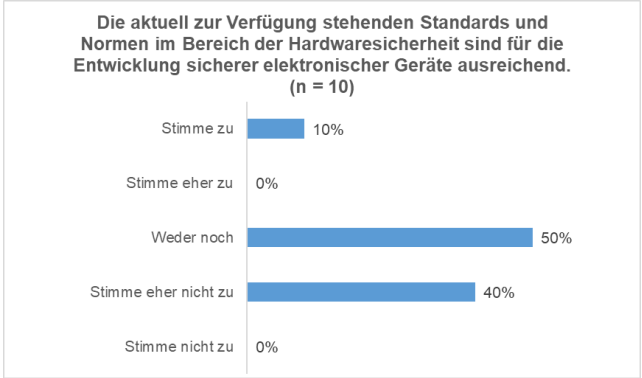

Abbildung 5: Normen und Standards zur Entwicklung sicherer elektronischer Geräte

4 Stand der Hardwaresicherheit in den teilnehmenden Unternehmen

Im zweiten Abschnitt wurden Fragen zur Hardwaresicherheit von Produkten aus dem eigenen Unternehmen gestellt. Die Ergebnisse können wie folgt zusammengefasst werden:

- Die Mehrzahl der Teilnehmenden (90%) gab an, dass die Hardwaresicherheit in ihrem Unternehmen einen hohen Stellenwert hat.
- Von den Teilnehmenden gaben 60% an, dass die Hardwaresicherheit der im eigenen Unternehmen produzierten Geräte hoch ist (vgl. Abbildung 6).
- Zu den schützenswertesten Inhalten in elektronischen Geräten zählten die Teilnehmenden unter anderem die Firmware, die erzeugten und gespeicherten Anwendungsdaten (z. B. auch Schlüssel) und das Design/Layout der elektronischen Baugruppe.
- Die Hälfte der Teilnehmenden schätzte, dass die implementierten Sicherheitsfunktionen der im eigenen Unternehmen hergestellten elektronischen Geräte eine ausreichende Qualität aufweist.
- Die Mehrzahl der Teilnehmenden (70%) hielt es für wahrscheinlich, dass Angriffe auf die elektronischen Geräte der eigenen Organisation erfolgen. Staaten wurden dabei am häufigsten als mögliche Angreifer genannt, gefolgt von Hackern und Mitbewerbern.
- Angriffe können von den Geräten der befragten Unternehmen in 30% der Fälle erkannt werden (vgl. Abbildung 7).
- Von den Befragten hielten es 70% für gefährlich, wenn Daten aus den elektronischen Geräten der eigenen Organisation in den Besitz eines Angreifers gelangen.
- Die Mehrzahl der Teilnehmenden (70%) machte keine Aussagen darüber, welche Zeit einem Angreifer für einen Angriff auf ein elektronisches Gerät der eigenen Organisation zur Verfügung steht.
- Die Teilnehmenden schätzten, dass die Angriffe auf elektronischen Geräte ihrer Organisation am häufigsten auf eine „Manipulation der Funktion“ und das „Abhören der Kommunikation“ abzielen und am häufigsten Oszilloskope, Analysesoftware und Logikanalysatoren für die Angriffe eingesetzt werden (vgl. Abbildung 8).
- Als Schwachstellen, die am häufigsten von Angreifern ausgenutzt werden, gaben die Teilnehmenden eine „Manipulation der Stromversorgung“, „offene Programmierschnittstellen“ und die Ausnutzung von „Schwankungen in der elektromagnetischen Abstrahlung“ an.
- Bei den befragten Unternehmen gaben 40% an, dass ihre elektronischen Geräte gegen Angriffe über „offene Programmierschnittstellen“ und „unverschlüsselte Kommunikation“ geschützt sind. Nur 30% der Teilnehmenden gaben an vor Angriffen in Bezug auf den Stromverbrauch oder das Timing von Signalen geschützt zu sein (vgl. Abbildung 9).
- Ein Großteil der befragten Unternehmen (80%) gab an, seinen Entwicklern Vorgaben zu machen, Gegenmaßnahmen zum Schutz vor Angriffen in die elektronischen Geräte zu integrieren.
- Die am häufigsten vorgegebenen Gegenmaßnahmen gegen Angriffe sind in den Produkten der befragten Unternehmen: „Deaktivierung von Debug-Schnittstellen“, „Verschlüsselung der Anwendungsdaten“,

„Siegel oder Plomben“, „Verwendung von Security Chips, die ein bestimmtes EAL-Level der CC aufweisen“ und „Verschlüsselung der Firmware/Bitstrom“.

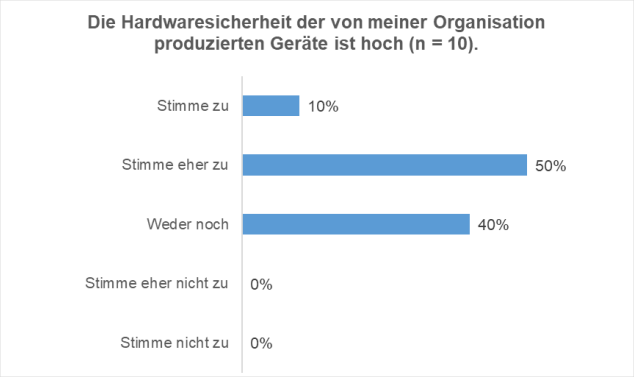

Abbildung 6: Hardwaresicherheit der im Unternehmen produzierten Geräte

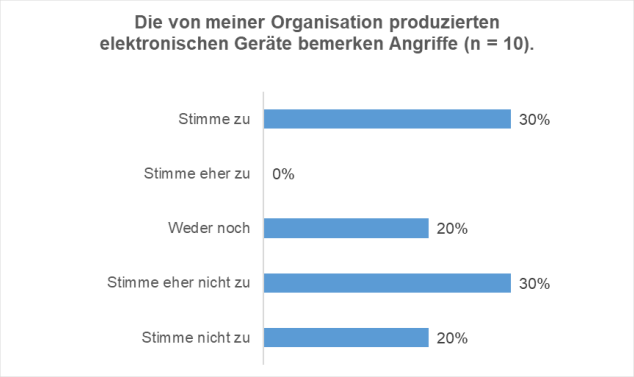

Abbildung 7: Aktive Erkennung von Angriffen

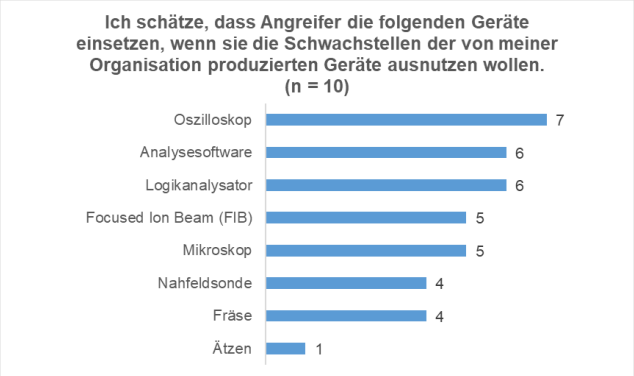

Abbildung 8: Häufig verwendete Werkzeuge für den Hardware-Angriff

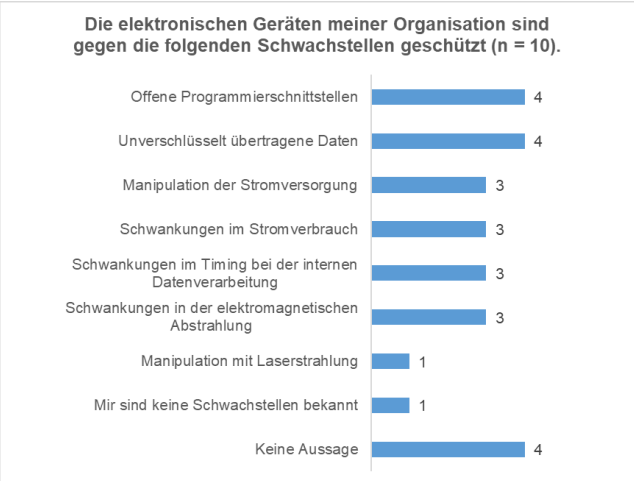

Abbildung 9: Gegenmaßnahmen

Die folgenden Wünsche wurden von den Teilnehmenden in Bezug auf die Hardwaresicherheit aktuell verfügbarer elektronischer Bauteile und Geräte geäußert:

- Stromsparendere Versionen für bisherige Versionen
- Mehr innovative Security Chips, bzw. deutliche Weiterentwicklung
- Leitungslängenmessung bei Mäander in Platinen, zum Schutz vor Anbohren
- Ultraschall oder lasergestützte Gehäuseöffnungserkennung für batteriebetriebene Geräte

5 Anforderungen an die im Verbundvorhaben VE-SAFE entwickelte Schutzhülle

Im dritten Abschnitt wurden befragt, welche Eigenschaften der im Verbundvorhaben VE-SAFE entwickelten Schutzhülle für den praktischen Einsatz gefordert oder gewünscht sind. Die Ergebnisse können wie folgt zusammengefasst werden:

- Ein Großteil der Teilnehmenden (80%) war der Ansicht, dass eine separate Elektronik zur Erkennung und Abschwächung von Angriffen sinnvoll ist (vgl. Abbildung 10).

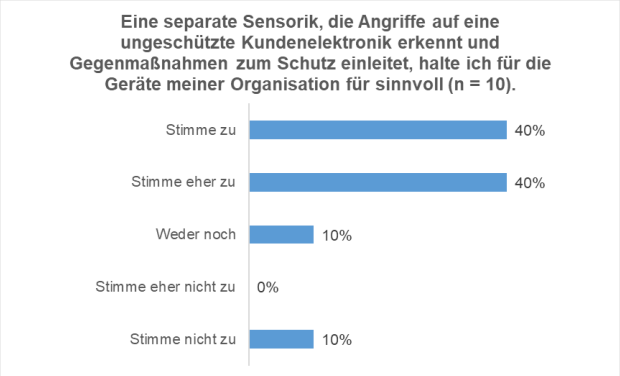

Abbildung 10: Eine separate Elektronik zum Erkennen von Angriffen ist sinnvoll.

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, hielten die Teilnehmenden bei den folgenden Produkten oder Anwendungsbereichen für sinnvoll:
  - Wenn sensible Kundendaten sicher gelöscht werden müssen (z. B. Geräte für die Verteidigung)
  - IoT-Sensoren und IoT-Gateways
  - Für Bereiche wie z. B.: Telekommunikation, Medizintechnik, autonomes Fahren, Automatisierungstechnik, usw.
  - Geräte mit Kommunikationsschnittstellen und insbesondere, wenn diese funkbasierend sind

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, darf die Baugruppe nach Aussage der Teilnehmenden nur um den folgenden Faktor vergrößern:
  - Allgemein:
    - so klein wie möglich
    - Vergrößerungsfaktor: 0 - 10%
    - einfach und unauffällige Integration der Sensorik bei einem Redesign im Rahmen der Produktpflege
    - Integration ohne signifikante Erhöhung des Platzbedarfs der elektronischen Baugruppe
    - extrem niedrigen Stromverbrauch
  - IoT-Sensoren: 10 x 20 mm^2
  - IoT Gateway: egal

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, darf die Baugruppe nach Aussage der Teilnehmenden nur um den folgenden Faktor verteuern:
  - Verteidigung:
    - nicht relevant
  - Sicherheitssysteme / Elektronik:
    - 0 - 10%
  - Industrie, Großhandel & Entwicklungsdienstleitung:
    - IoT-Sensoren bis ca. 5,- Euro
    - IoT-Gateway bis ca. 9,- Euro
  - Industrielle Automation & Automatisierungstechnik:
    - Am besten gar nicht.

„Viele Kunden verstehen nicht, warum sie für etwas mehr Geld ausgeben sollen, was ihnen erstmal keinen Nutzen bringt.
Hier fehlt m.E. noch viel Verständnis und Hintergrundwissen bei den Endanwendern.“
(Zitat eines Teilnehmenden)

- Eine separate Sensorik, die Angriffe auf eine ungeschützte Kundenelektronik erkennt und Gegenmaßnahmen zum Schutz einleitet, muss nach Aussage der Teilnehmenden die folgenden Eigenschaften aufweisen, damit sie in der Praxis eingesetzt wird:
    - BSI-Zulassung
    - stromsparend
    - leicht konfigurierbar
    - kompaktes Modul (z. B. LGA)
    - geringe Eingriffe in Hardware bei Integration
    - unauffällig
    - kostengünstig
    - keine Quereffekte (z. B. „Fehlalarme“)
    - robust gegen Erschütterungen
    - Erkennung erfolgter Manipulationen beim Gerätestart
    - lange Lagerzeit (ca.10 Jahre).
    - Eignung für industriellen Temperaturbereich (-40°C bis +100°C)
    - selbstständige Manipulationserkennung

6 Fazit

Durch die durchgeführte Online-Befragung zur Lage der Hardwaresicherheit in Deutschland in 2021 konnten viele wertvolle Erkenntnisse gewonnen werden.

Aus Sicht der Teilnehmenden gibt es ein großes Verbesserungspotential der zur Verfügung stehenden Standards und Normen im Bereich der Hardwaresicherheit für die Entwicklung sicherer elektronischer Geräte. Nur 10% hielten den aktuellen Umfang der zur Verfügung stehenden Normen und Standards für ausreichend (vgl. Abbildung 5). Die Teilnehmenden nannten aber z. B. Standards wie den ISO/SAE 21434 „Road vehicles – Cybersecurity engineering“ nicht. Dies zeigt, dass bestehende Sicherheitsstandards noch weiter in der deutschen Industrie bekannt gemacht werden sollten.

Vorgaben für die sichere Entwicklung elektronischer Geräte, geben 80% der an dieser Umfrage teilnehmenden Unternehmen.

Nur 30% der Geräte der teilnehmenden Unternehmen verfügen bis jetzt über eine separate Elektronik zur aktiven Angriffserkennung (vgl. Abbildung 7)

Bei den befragten Unternehmen geben lediglich 40% an, dass ihre elektronischen Geräte gegen häufige Angriffe (z. B offene Programmierschnittstellen) geschützt sind (vgl. Abbildung 9).

Zusammenfassend ist daher ein Großteil der Teilnehmenden (80%) der Ansicht, dass eine separate Elektronik zur Erkennung und Abschwächung von Angriffen für die Geräte ihrer Organisationen, wie sie im Rahmen des Verbundprojektes VE-SAFE entwickelt wird, sinnvoll ist (vgl. Abbildung 10). Im Rahmen der Online-Befragung wurden viele Details zu Anforderungen, die eine solche separate Schutzelektronik in den unterschiedlichen Industrieanwendungen aufweisen sollte, mitgeteilt.

7 Literatur

[1] BSI. Bundesamt für Sicherheit in der Informationstechnik. www.bsi.bund.de, 2021.

[2] HTV. Das Hochleistungszentrum für elektronische Bauelemente. www.htv-gmbh.de, 2022.

[3] Velektronik. Vertrauenswürdige Elektronik. https://www.velektronik.de/bmbf-gefoerdertes-projekt-safe-befragung-zum-thema-hardwaresicherheit/, 2021.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung