Wir haben das UEFI Secure Boot Problem gelöst! – eklatante Sicherheitslücke kann nun geschlossen werden

DAS PROBLEM: Selbst bei einer eigenen Cloud-Infrastruktur und Software-Architektur macht eine kompromittierte Hardware-Ebene den Deutschland Stack unwirksam

Möglicher Datenab- und Zufluss (Backdoors), Abhängigkeiten, Erpressbarkeit und Kill-Switches gefährden die innere und äußere Sicherheit Deutschlands und damit ein Leben in Frieden, Freiheit und Wohlstand gemäß unseres in Art. 1 GG verbrieften Menschenbilds und Menschenrechtsverständnisses.[1] Während die Cloud-Infrastruktur und Software-Architektur bereits durch offene Schnittstellen, nationale Champions und den German-Led CMS Stack (ANCS, SINA, SDoT, NAVICS und weitere Komponenten) souveräner gestaltet werden können, bleibt die Hardware-Ebene – Chips, Prozessoren, ASICs – ein kritisches Souveränitätsrisiko: Selbst bei einer eigenen Cloud-Infrastruktur und Open Source Software-Architektur kann eine kompromittierbare Hardware-Ebene den gesamten Stack unwirksam machen – ein zivil-militärisches Problem. Wir haben die Lösung für dieses Problem entwickelt, halten die IPO und sind startklar.

WIR

Eine informelle intra- und interdisziplinäre dimensionenübergreifende zivil-militärische Gruppe engagierter Menschen[2] (Fachexperten), die als selbstreguliertes, virtuelles High Performance Team in Form einer „disruptiv-radikalen Zelle“ in einem inkrementell-iterativen, agilen Prozess eigeninitiativ ohne wirtschaftliche und/oder Lobby- oder Karriereinteressen wirkt, erzeugt durch forschungs- und wertebasierten Expertise(vor)Sprung die Hebelwirkung, die wir im Hamburger Hafen erleben: Mit einer Handvoll Schleppern werden die größten Containerschiffe der Welt auf der Stelle umgedreht. Dieses Wirkprinzip ist auf jeden Turnaround anwendbar. Um das Kernteam herum liegen in konzentrischen Kreisen so viele Beteiligte, quer über das gesamte Spektrum von Industrie, Bundeswehr, Administration und Politik, dass die erforderliche Menge an Menschen, kritische Masse und Bandbreite reicht, um jeden Turnaround – unabhängig von Branche, Organisationsform und -größe – zu bewältigen. Wir bringen uns gerade (rechtzeitig) in eine vertragsfähige Rechtsform.

HABEN

Nationale digitale Souveränität entsteht nicht primär durch den Bau einer eigenen deutschen Foundry, sondern durch vollständige Transparenz des Chip-Designs als offene Instruction Set Architecture (ISA) in Kombination mit KI-gestützter Design-Absicherung (Pre-Silicon) und KI-basierter Validierung des realen Silizium-Verhaltens (Post-Silicon).

DIE LÖSUNG

Innere und äußere Sicherheit werden horizontal und vertikal von der Bundesebene bis in den letzten Winkel der Kommune und für jede Anwendung zivil und militärisch gleichermaßen realisiert.[3] In Konsequenz bieten wir die Beteiligung an den IPO ausschließlich dem Bundesamt für Sicherheit in Informationstechnik (nachfolgend BSI abgekürzt) an, und zwar nur als zivil-militärische (Bund-Länder, Staatswohl/Wirtschaft/Gesellschaft, ordnungs- und prozesspolitische) Eigenschutz-Lösung, verbunden mit der Hoheit über sämtliche Schnittstellen, Schlüssel und Zertifizierungen, die daraufhin neu zu entwickelnden Lösungen und die entsprechenden Patente sowie mit vertraglicher technischer/technologischer und (sicherheits)rechtlicher (Werte)Kontrolle nach DEU/EU Verfassungskonformität.

SICHER[4]

Technologie(vor)Sprung setzt Expertise(vor)Sprung voraus. Es reicht nicht, IPO zu erwerben, wenn nicht im BSI bei eklatantem Personalmangel durch gezielte Expertisebildung und Technologieeinführung die Menschen gleichzeitig entlastet und in die Lage versetzt werden, an der Weiterentwicklung aktiv mitzuwirken. Sicherheit kann nur durch Expertise(vor)Sprung hergestellt werden: Immer den einen Schritt schneller und voraus zu sein, bietet Sicherheit. Dabei erweist sich die forschungs- und wertebasierte Expertisebildung als potenzielles Alleinstellungsmerkmal: die 4V, wie wir sie nennen: Verantwortung, Vertrauen, Verlässlich- und Verbindlichkeit als Grundlage für renditestarkes, ressourcenschonendes (Mensch, Zeit, Geld), minimalistisches und dabei schnell skalierbares, technologieoffenes & dabei nachhaltiges (intra- und intergenerational gerechtes) Wachstum – made in, made by and made for Germany.

Kontakt: Prof. Dr. (habil) FKpt d. R. Beatrix Palt, b.palt@inp-hamburg.com, +49 160 96907669

1 Vgl. Beatrix Palt & Team, Norbert Dippel, Michael Dost, Markus Lehmann & Team, Andreas Stemick & Team (2025). Wertebasierte Expertisebildung – Sicherheit ist das Strukturbestimmende Element: nationale digitale Hard- & Software-Souveränität als gesellschaftliche Aufgabe; Beatrix Palt, Michael Dost, Andreas Stemick & Team (2025). Expertisebildung heißt es wahrhaben wollen – nationale Software-Autonomie bis 2029 als Teil der nationalen Souveränität. Ein Denkanstoß. Das sind Band 6 und 7 der Schriftenreihe des INP. Jenseits der Begrenztheit – Projekte anders denken. www.inp-hamburg.com

2 Die Namen sind an den entscheidenden Stellen bekannt. Dieser Onepager ist durch die IPO-Träger autorisiert.

3 Vgl. Ralph Brinkhaus, der – grob zusammen gefasst - propagiert, dass der Bund horizontal und vertikal die Verantwortung für Cyber Sicherheit übernimmt, zur Verfügung stellt und die Menschen durch Expertisebildung befähigt (Vgl. z.B. Wirtschaftstag der Innovationen des Wirtschaftsrats e.V. am 05.11.2025 in Berlin).

4 „Mit 3% der Belegschaft wurden initial innerhalb von 6 Monaten bei geringem zeitlichem und persönlichem Investment – durchschnittlich 16 Stunden verteilt auf 6 Monate - exponentielle Leistungssteigerungen von zwischen 70% und 100% dadurch erreicht, dass die Selbstwirksamkeit entfaltet wurde.Nachweislich waren die Menschen doppelt so schnell, die Kosten um 50% reduziert und das Risiko signifikant um den Faktor vier gesunken.“ Vgl. Palt, Onepager zum Expertise(vor)Sprung – wer kann, der kann! vom 27.05.26, www.inp-hamburg.com.