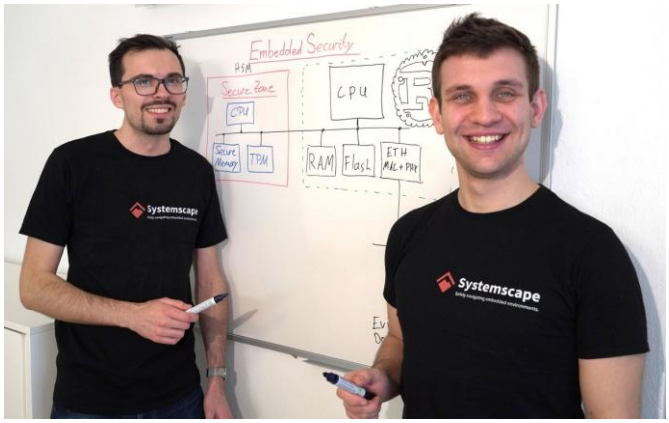
Ingenieure wagen Startup | Themenabend 29.01.2025

Der Schritt von der Ingenieurstätigkeit in die Selbstständigkeit ist vermeintlich riskant – aber er bietet auch große Chancen. Wie kann ein junges Unternehmen das herausfordernde Umfeld von Cybersicherheitsvorfällen, steigenden Bedrohungen für IoT-Geräte, komplexen Regulierungen, hohen Entwicklungskosten und Mangel an Security-Experten unternehmerisch angehen? Wer als Ingenieur den Sprung in die Selbstständigkeit wagt, steht vor vielen Herausforderungen jenseits der technischen Expertise.

Darüber berichteten die Gründer der Systemscape GmbH, Julian Dickert und Joel Schulz-Andres, bei diesem online Themenabend des VDI Arbeitskreises „Unternehmer und Führungskräfte“. Sie gaben konkrete Einblicke in ihre Startup-Erfahrung: Welche Planungsschritte bei der Gründung wirklich notwendig waren und welche Vorbereitungen sich als überflüssig herausstellten. Es bleibt vor allem stetig ein Spagat zwischen technischer Entwicklung und unternehmerischen Aufgaben. Die Teilnehmenden erhielten bei wertvolle Erkenntnisse zur Unternehmensgründung im technischen Umfeld.



Die Referenten Joel Schulz-Andres und Julian Dickert, beide Elektroingenieure, beschäftigen sich seit über 10 Jahren mit eingebetteten Systemen. Da aus ihrer Sicht das Thema Sicherheit im Embedded Bereich zu lange vernachlässigt wurde, wollen sie das mit ihrem Unternehmen ändern und vorantreiben. Dabei setzen sie auf die Programmiersprache Rust, die die beiden als die transformative Maßnahme für mehr Cybersicherheit im Embedded Umfeld sehen. Sie vergleichen den Umstieg auf Rust damit, dass man sofort zu einer solchen Maßnahme greifen würde, mit der sich 80% aller Verkehrsunfälle oder gleichviel Arbeitsunfälle in der Industrie verhindern ließen. Sie halten die Vorteile der speichersicheren Programmiersprache Rust für überwältigend.

Die lebhafte Diskussion der Teilnehmenden drehte sich schließlich weniger um Unternehmensgründung, sondern viel intensiver um Cybersicherheit für eingebettete Systeme und was die Programmiersprache Rust leistet. Deshalb wurden hierzu viele Fragen besprochen.

Schätzungen der US-Regierungsbehörde NIST führen etwa 70-80 % aller Sicherheitslücken auf Speicherfehler zurück.

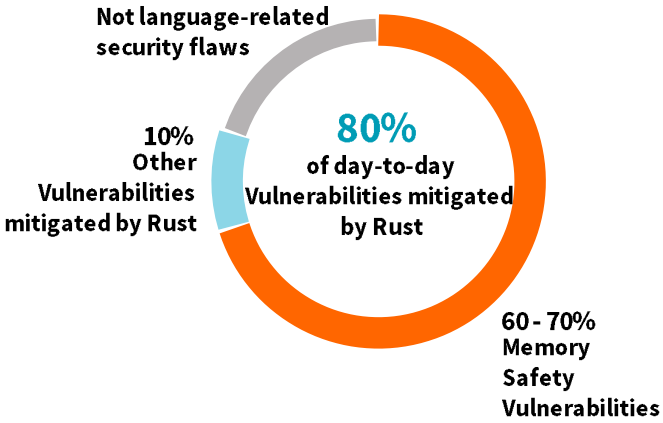


Bild: Anteil typischer Sicherheitslücken, die Rust verhindert (Quelle: Systemscape)

Die Verwendung einer speichersicheren Sprache wie Rust könne Sicherheitslücken und Datenlecks in Computersystemen zuverlässig verhindern, denn viele der gefährlichsten Schwachstellen wie Buffer Overflow, Use-after-free Fehler und Race Conditions treten bei speichersicheren Sprachen nicht auf. Diese Klasse von Fehlern wird mit Rust bereits zur Kompilierzeit verhindert und sie sind nicht durch aufwändige Code-Reviews und statische Analyse-Tools zu finden. Durch weitere Sprach- und Compilerfeatures werde nicht nur die Sicherheit drastisch erhöht, sondern auch die Zuverlässigkeit der Software verbessert und Entwicklern geholfen, besseren Code zu schreiben. Gerade für Ingenieure sei Rust eine interessante Alternative, meinen die Gründer, da sich auch ohne tiefgreifende Programmierkenntnisse und jahrzehntelange Programmiererfahrung ein zuverlässiger und sicherer systemnaher Code schreiben ließe.

Julian Dickert und Joel Schulz-Andres,
Gründer Systemscape GmbH

Dipl.-Ing. Christa Holzenkamp,
Leitung VDI Arbeitskreis Unternehmer und Führungskräfte

VEREIN DEUTSCHER INGENIEURE | Bezirksverein München, Ober- und Niederbayern e.V.
Westendstraße 199 (TÜV) | 80686 München | +49 89 5791-2200 | www.VDI-Sued.de
Amtsgericht München VR 4284 | Vorstandsvorsitz: Andreas Wüllner, Prof. Dr. Peter Pfeffer (stv.)