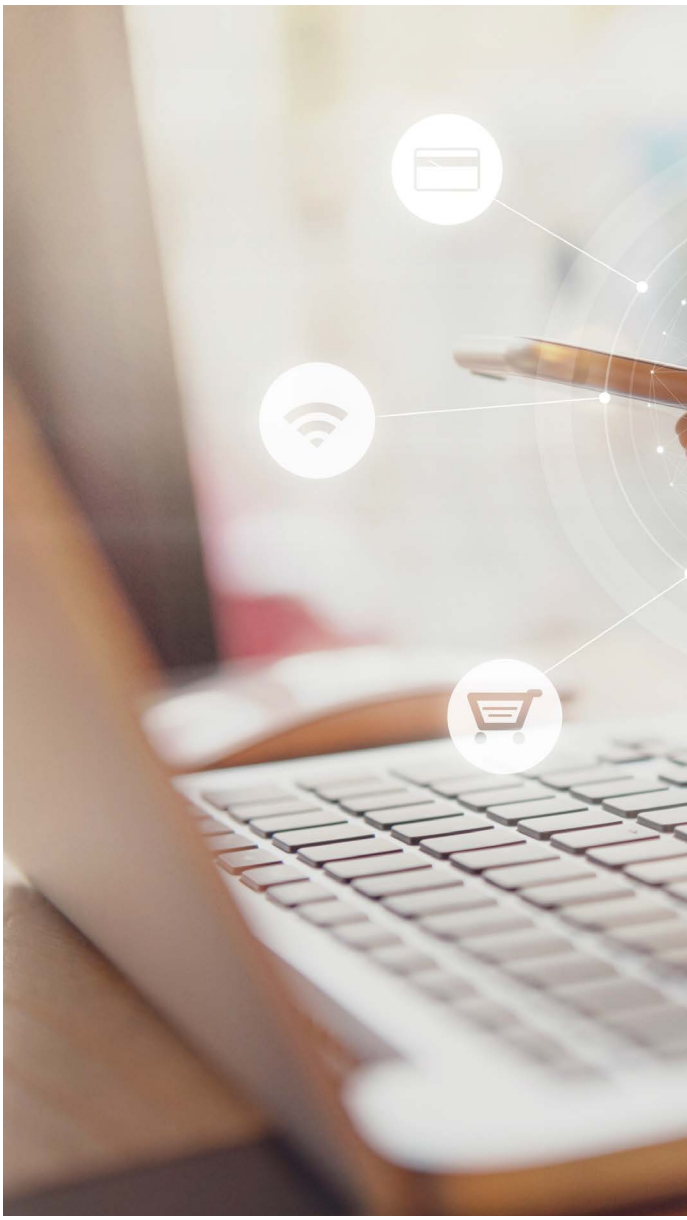
Was ist Sicherheit im digitalen Zeitalter?

Bei geschätzt mehreren Milliarden vernetzten Dingen im Jahr 2020 rückt das Thema Sicherheit immer stärker in den Mittelpunkt der öffentlichen (Forschungs-)Diskussion. Wer hört die Sprachbefehle, die die vernetzte Wohnung steuern? Wer kann ein fabriksneues Auto aufsperren? Lässt sich die neue Produktionsmaschine der vernetzten Fabrik von außerhalb übernehmen?

Birgit Baustädter



„Spiel meine Nachmittags-Playlist!“ – eine harmlose Bitte an unsere Smart Speaker, wie sie wohl häufig in der vertrauten und zunehmend vernetzten Umgebung der eigenen vier Wände ausgesprochen wird. Genauso wie wir unsere Wohnungen zunehmend mit smarten Gegenständen ausstatten, nimmt die Vernetzung auch in der Fahrzeugbranche, im Gesundheitswesen und in der Industrie zu.

> **Kryptografie ist die Basis, die Grundlage jeder Sicherheit.**
>
> **Christian Rechberger**

Oft wissen wir wenig darüber, was mit den so generierten Daten geschieht. Aber wir vertrauen. Vertrauen darauf, dass die Gegenstände gegen Störungen und unbefugten Zugriff abgesichert sind und unsere Daten nur die Personen zu Gesicht bekommen, die dazu befugt sind. Vertrauen, dass sich unbefugte Personen keinen Zugriff auf unsere höchstpersönlichen Lebensbereiche oder kritische Infrastrukturen verschaffen können.

„In der Realität ist das aber anders. Sind Daten einmal in einer Cloud auf einem internationalen Server, dann verliert man die Kontrolle über die Daten“, erklärt Christian Rechberger vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz. „Von technischer Seite sehen wir das anders – es ist sehr wohl möglich, dass die User/innen die Kontrolle über ihre Daten behalten und trotzdem die volle Funktionalität und den Service der Cloud erhalten.“

SICHERE SYSTEMARCHITEKTUR

Je mehr sich unsere Welt vernetzt, desto wichtiger ist es auch, dass sie sich sicher vernetzt – das Thema Cybersecurity rückt nicht erst in den vergangenen Jahren in den Fokus der wissenschaftlichen Forschung. Wohl aber rückt es erst seit wenigen Jahren stärker ins Blickfeld der Öffentlichkeit. Die Offenlegung von Sicherheitslücken wie Meltdown und Spectre, für die ein internationales Team rund um Daniel Gruss, Moritz Lipp, Michael Schwarz und den TU Graz-Professor Stefan Mangard verantwortlich ist, schürte das Sicherheitsbewusstsein.

„Absolute Sicherheit wird es am Ende des Tages nicht geben“, stellt Mangard fest. Er ist Leiter der Arbeitsgruppe Secure Systems am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie. „Aber wir können mit der Art, wie

Immer mehr smarte Gegenstände begleiten uns im Alltag.
oatawa – AdobeStock

wir Computersysteme bauen, deren Sicherheit auf einen neuen Level bringen.“ Derzeit laufen Sicherheitsforschende mit Angreifenden um die Wette – tut sich eine Sicherheitslücke auf, muss sie so schnell wie möglich geschlossen werden. „Parallel zu diesem Katz-und-Maus-Spiel, das unsere derzeitigen Systeme noch verlangen, arbeiten wir an neuen Systemarchitekturen. Sie sollen dann von vornherein eine bestimmte Art von Angriffen gar nicht erst möglich machen.“

Im vom European Research Council (ERC) geförderten Projekt Sophia beschäftigen sich Mangard und sein Team mit der Absicherung von Computerprozessoren, analysieren ungewollte Zugriffsmöglichkeiten und sichern gefundene Hintertürchen effizient ab. „Es ist immer ein Drahtseilakt – mehr Sicherheit geht meist mit sinkender Performance einher“, erklärt Mangard. So fanden die Forschenden im Projekt auch die Sicherheitslücken Meltdown und Spectre. Hier nutzen Angreifende aus, dass ein Prozessor, um möglichst schnell zu sein, bereits Rechenschritte wie den Zugriff auf bestimmte Daten vorwegnimmt und vorbereitet, bevor überhaupt zum Beispiel die Zugriffsberechtigungen geprüft werden. Ist die Zugriffsberechtigung nicht vorhanden, verwirft der Prozessor die vorbereiteten Daten zwar wieder, aber diese vorbereiteten Daten erzeugen Seiteneffekte, wie zum Beispiel Zeitdifferenzen, die unter bestimmten Umständen von Angreifenden zum Bestimmen vertraulicher Informationen ausgenutzt werden können. Die bei der Veröffentlichung der Sicherheitslücken ebenfalls veröffentlichte Abwehrmöglichkeit – der Patch – machte Computer dann zwar sicher, aber eben auch langsamer.

„Eines der größten Probleme in der Security ist, dass sie so schwer quantifizierbar ist“, erklärt Stefan Mangard. „Ich merke sofort, wenn mein Computer schneller oder langsamer arbeitet – wenn ich aber in die Sicherheit investiere, dann merke ich subjektiv erst einmal gar nichts oder maximal Geschwindigkeitseinbußen.“ So gesehen ist jeder öffentlichkeitswirksame Hack für die Forschenden ein Vorteil: Die breite Masse wird sensibler für das so wichtige Thema Daten- und Computersicherheit. „Wir brauchen momentan einfach Zeit und Geld, um die richtigen Technologien zu entwickeln. Und einen gewissen Druck vom Markt, damit bereits bestehende Sicherheitstechnologien in neuen Produkten von vornherein eingesetzt werden.“

CYBERSECURITY CAMPUS GRAZ

Hier kommt der neu gegründete Cybersecurity Campus Graz ins Spiel. Gemeinsam mit dem international renommierten Zertifizierungsunternehmen SGS baut die TU Graz in den kommenden Jahren ein Forschungs-, Lehr- und Zertifizierungszentrum für Cybersecurity in der Grazer Inffeldgasse auf. Stefan Mangard ist im Zentrum für die wissenschaftliche Ausrichtung verantwortlich und gerade darum bemüht, die Forschungsagenda des Campus mit Themen und Projekten zu befüllen. „Der Cybersecurity Campus soll ein Bindeglied zwischen der Grundlagenforschung und der Anwendung in der Industrie sein.“ >

! Näheres zum Cybersecurity Campus Graz lesen Sie auf Seite 10.

IOT: COMPUTER IM MINI-FORMAT

Der Fokus im Cybersecurity Campus Graz wird auf den Herausforderungen der Zukunft liegen – allen voran auf dem Internet der Dinge (Internet of Things, kurz IoT), das mit seinen Computern im Mini-Format die Sicherheitsforschung vor neue Herausforderungen stellt. „Man spricht von Milliarden Computern weltweit, die man gar nicht mehr sieht – im Lichtschalter, in Glühbirnen oder in der Smartwatch“, erklärt Christian Rechberger, Professor und Leiter der Arbeitsgruppe Cryptography am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz. Auf fingerspitzenkleinen Computern, wie sie zum Beispiel in Smartwatches verbaut sind, ist jeder Millimeter Speicherplatz heiß umkämpft und nicht zuletzt kostspielig – wer möchte schon eine Smartwatch, die zentimeterdick ist? „Die Herausforderung ist es, Sicherheit zu gewährleisten, obwohl sie fast nichts kosten darf.“

Rechberger begegnet dieser Herausforderung mit neuen Überlegungen in der Kryptografie. Sie ist eines der mächtigsten Instrumente, wenn es darum geht, Computersysteme sicher zu machen. Mittels mathematischer Methoden werden Daten verschlüsselt und sichergestellt, dass sie auf ihrem Weg weder abgefangen noch manipuliert werden können. „Die Kryptografie kann man als Basis jeder Sicherheit sehen“, erklärt Rechberger. „Ist die Basis nicht sicher, dann kann auch alles, was darauf aufbaut, nicht sicher sein.“

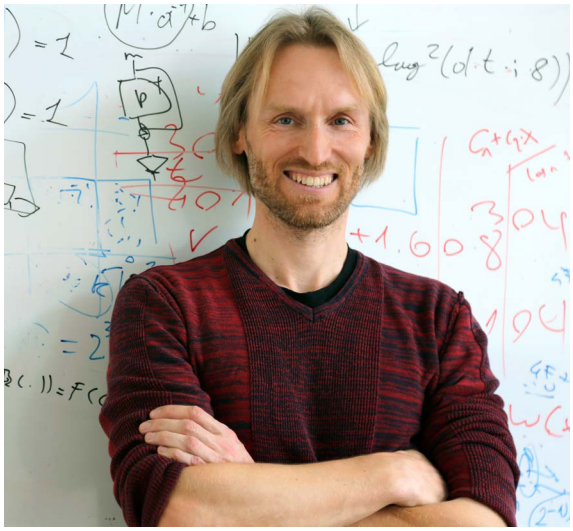
Gerade eben konnte im Bereich Kryptografie ein neuer internationaler Erfolg verbucht werden: Ein Team rund um Maria Eichlseder – Postdoc im Bereich Kryptografie – konnte mit dem Algorithmen-Bündel ASCON bei einem internationalen Wettbewerb überzeugen. ASCON wurde als beste Lösung im Bereich leichtgewichtige Algorithmen empfohlen – also für Verfahren, die mit möglichst geringen Ressourcen auskommen.

> **Sicherheit heißt, dass es keine Frage von Glück ist, ob ein System wie erwartet funktioniert, sondern dass man sich darauf verlassen kann.**
>
> **Maria Eichlseder**

Das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie wird von Reinhard Posch geleitet. Der Sicherheitsexperte ist Chief Information Officer der Österreichischen Bundesregierung und koordiniert gemeinsam mit einem Gremium die IT-Vorhaben von Ländern und Ministerien. Zentral war er an dem Projekt digitale Signatur und anderen Entwicklungen im Bereich E-Government beteiligt.

Die Arbeitsgruppen am Institut beschäftigen sich mit:

- Core Security (Leiter: Daniel Gruss),
- Cryptography (Leiter: Christian Rechberger),
- E-Government (Leiter: Arne Tauber),
- Java-Security (Peter Lipp),
- Secure Systems (Leiter: Stefan Mangard) und
- Systematic Construction of Correct Systems (Leiter: Roderick Bloem).



Links: Bezeichnet Kryptografie als „Basis jeder Sicherheit“: IT-Spezialist Christian Rechberger
Bildquelle: Baustädter – TU Graz

Rechts: Baut erfolgreiche Verschlüsselungsalgorithmen: Maria Eichlseder
Bildquelle: Lunghammer – TU Graz

„Wir fragen uns auf wissenschaftlicher Seite, was die minimalsten Berechnungen sind, die wir gerade noch hernehmen und clever kombinieren können, um die Chips abzusichern“, erklärt Rechberger die Zugangsweise.

KÜNSTLICHE INTELLIGENZ UND QUANTENCOMPUTER

Neben dem Internet der Dinge – das sowohl für Mangard als auch Rechberger das zentrale Thema der kommenden Jahre sein wird – stellen neue Entwicklungen noch weiterer Aufgaben: die künstliche Intelligenz und die Quantencomputer. „Aus Forschungssicht ist die künstliche Intelligenz aber eine ganz harte Nuss“, stellt Mangard fest. „Lernende Algorithmen werden immer besser, aber eine kleine Manipulation in den Daten kann sie vollkommen aus dem Tritt bringen. Wenn künstliche Intelligenz einmal sehr viel verbreiteter sein wird als heute, dann kann das ein großes Problem werden.“ Und aus Sicht der Datensicherheit fügt Rechberger hinzu: „Künstliche Intelligenz muss mit unzähligen Daten gefüttert werden. Aber ist das wirklich sicher? Und ist die Privatsphäre gewährleistet? Wir arbeiten jetzt schon an einer Möglichkeit, lernende Algorithmen erfolgreich mit verschlüsselten Daten zu versorgen, ohne ihre Lernfähigkeit zu beeinflussen.“ >

CHI-5 Uniform, reusing gates, sanitized with sinks

IB2 IB0 IC2 ID2 IB1 IC1 ID1 IA0 IA1 IA2 IA3 IA4 IB3 IB4 IC0 IC3 IC4 ID0 ID3 ID4

CHI-3 plain

CHI-3 masked

CHI-3 masked, sanitized, CoSIFA

4. Security Analysis

enhance security analysis with existing
about florians zero-sum distinguisher fo

maybe get rid of analysis and only refer

4.1. Basic Properties

In this section, we give some known pr
ble 14 in Appendix A shows the differe
and output differences. As can be seen i
ability of the S-box is 2^{-2} and its differ
the biases of the linear approximation
masks. The maximum linear probabil
number is 3.

Let x_0, x_1, x_2, x_3, x_4 and y_0, y_1, y_2, y_3, y_4
where x_0 refers to the most significa
Then the algebraic normal form (AN

$y_0 = x_4x_1 + x_3 + x_2$
$y_1 = x_4 + x_3x_2 + x_3$
$y_2 = x_4x_3 + x_4 + x_2$

$6 = 3 + 13$ rounds, EM).

Anfang 2018 unterzeichneten neun Organisationen bei der Munich Security Conference eine Absichtserklärung zur intensiveren Forschung im Bereich Cybersecurity – die Charter of Trust. 2019 ist die Gruppe der Unterstützer auf 16 angewachsen. Ebenfalls seit diesem Jahr ist die TU Graz als erste universitäre Einrichtung Kooperationspartnerin der internationalen Initiative für mehr Sicherheit im digitalen Zeitalter.

Quantencomputer sind heute noch keine Realität – aber ihnen wird eine große Zukunft vorhergesagt. Mit ihrer völlig neuen Art zu rechnen werden sie wesentlich leistungsstärker als alle bisher bekannten Computersysteme sein. Was für die Nutzenden ein großes Plus ist, kann für die Sicherheit ein noch viel größeres Problem werden. „Unsere heutigen Methoden beruhen auf der Sicherheit, mit derzeitigen Rechenmethoden zwar theoretisch geknackt werden zu können, allerdings nur in einem Zeitraum von mehreren Milliarden Jahren“, erklärt Rechberger. „Quantencomputer könnten das aber relativ schnell erledigen.“

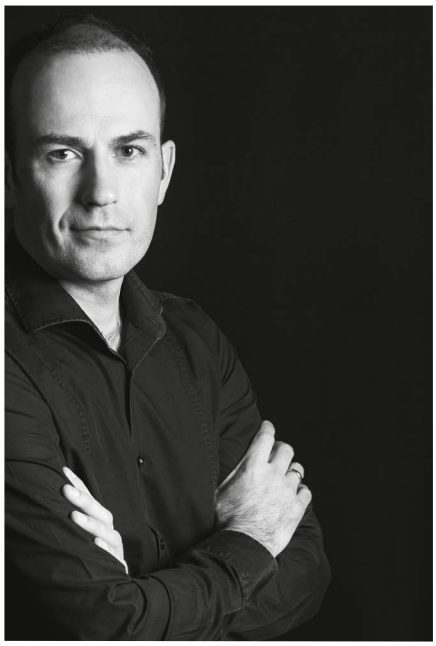
Sein Team ist mit zwei Einreichungen am aktuell laufenden Wettbewerb „Post-Quantum Cryptography“ der US-amerikanischen Zertifizierungsbehörde NIST beteiligt. Der Wettbewerb sucht nach Signatur-, Schlüsselaustausch- und Verschlüsselungsverfahren, die Angriffen durch Quantencomputer widerstehen. Die beiden Signaturverfahren Picnic und SPHINCS+ wurden im Februar 2019 als Kandidaten für die zweite Runde bestätigt.

SECURITY UND SAFETY

„Spannend wird das Thema Security auch, wenn der Safety-Aspekt hinzukommt“, erklärt Stefan Mangard. Unter „Security“ versteht man, ein System vor Angreifenden zu schützen. Im Bereich „Safety“ geht es darum, die Gesundheit des Menschen vor einem fehlerhaften Computersystem zu schützen. Die Kernkompetenz im Bereich Safety findet sich am Institut für Technische Informatik. Die Arbeitsgruppe Industrial Informatics rund um Georg Macher beschäftigt sich hauptsächlich mit diesem Aspekt der Sicherheit in der industriellen Anwendung. Auch hier ist Cybersecurity ein immer größeres Thema – über Kryptografie, Seitenkanalattacken und Authentifizierung. Die Forschenden kümmern sich um einen ganzheitlichen Entwicklungsansatz und Engineering-Prozesse.

Ein interessantes Beispiel ist der Bereich „Automotive“. „Fahrzeuge sind heute schon hoch vernetzt und bieten dadurch immer mehr Angriffsflächen. In kaum einer anderen Branche wird aktuell deutlich, wie wichtig die Interaktion von Safety und Security ist“, erklärt Senior Scientist Macher. Das zeigt sich sehr plakativ anhand des Beispiels einer elektronischen Lenkradsperre. „Ist sich das Sperrsystem unsicher, ob es nun die Sperre aktivieren soll oder nicht, dann gibt es zwei Blickwinkel: Aus Sicht der Systemsicherheit – der Security – ist es besser, wenn das Lenkrad vorsorglich gesperrt wird. Sperrt das System nicht, kann dies mit Diebstahlintention erfolgen und das Fahrzeug steht mit geringem Schutz in der Parklücke. Aus Sicht der Insassensicherheit – also

> **„100 Prozent Security gibt es nicht. Wir machen es den Angreifenden so schwer wie möglich.**
>
> **Georg Macher**



Mit dem Internet der Dinge wird unsere Welt immer bequemer. Kontaktloses Bezahlen, Automatisierung im Haushalt, autonomes Fahren und intelligente Fabriken sind nur einige Beispiele. Neue Mobilfunkstandards ermöglichen eine schnellere Interaktion zwischen Geräten und so neue Anwendungsfälle. Immer, wenn Dinge gut sind, schläft auch das Böse nicht, sondern erforscht neue Möglichkeiten, unsere Gesellschaft und unsere Lebensweise zu schädigen.

Martin Schaffer
Globaler Geschäftsführer für Sichere Produkte & Systeme, SGS Digital Trust Services

Bildquelle: alex.

Konsumgüter überschwemmen unsere Märkte nahezu ungefiltert, wenn es um IT-Sicherheit geht. Es gibt kaum Vorschriften oder Gesetze. Die Herausforderung ist vielfältig. Denn Sicherheit lässt sich nur lösen, wenn Geräte sicher gegenüber Angriffen während des gesamten Lebenszyklus konzipiert sind. Dies erfordert, dass Geräte aktualisiert werden, um auf neue Angriffstrends reagieren zu können. Das wiederum erfordert Back-End-Systeme, die solche Dienste anbieten und auf gesicherten Kanälen mit den Geräten kommunizieren. Und selbst wenn man es schafft, sichere Lösungen anzubieten: Kann man sicher sein, dass sie richtig implementiert, konfiguriert, bereitgestellt und betrieben werden?

der Safety – ist es besser, nicht zu sperren. Das Fahrzeug könnte gerade fahren und ein Defekt könnte die Grundlage der Unsicherheit sein. In diesem Fall muss das Lenkrad funktionieren."

Um funktionierende und sichere Systeme für den Straßen- und auch Fabriksalltag zu schaffen, fokussieren sich Macher und seine Kolleginnen und Kollegen auf systematische Dependability-by-Design-Ansätze – Ansätze, die sowohl Safety als auch Security vereinen. Diese Ansätze basieren unter anderem auf „Security-Primitiven", die auch das Nachbarinstitut von Mangard und Rechberger entwickelt. „Unser Fokus liegt auf einem sicheren, kompletten Entwurfs- und Entwicklungsprozess kritischer Industriesysteme. Safety und Security sind wichtige Teilaspekte der ganzheitlichen Entwicklung, die wir zum Beispiel im Projekt HyUnify für Wasserkraftwerke oder im Projekt MEMCONS für die Automotive-Branche eingebunden haben. Die Zuverlässigkeit des Systems basiert nicht nur auf der Entwicklung neuer Technologien, sondern auch auf deren korrekter Anwendung, der sicherheitskritischen Denkweise der Entwickler/innen und dem Bereitstellen eines entsprechenden Entwicklungsprozesses. Safety/Security Engineering ist nicht Technologie alleine, es ist ein Lifestyle."

Fokussiert auf die Interaktion zwischen Safety und Security: Georg Macher
Bildquelle: Baustädter – TU Graz

> **Security sollte immer vorhanden sein, ohne dass man sich als Nutzende/r ständig darum kümmern muss.**
>
> **Stefan Mangard**

Neben den real umsetzbaren Systemen beschäftigt sich Macher auch mit der Zukunft der Branche: Im 2018 gestarteten Projekt Drives beschäftigen sich die Forschenden mit dem Zukunftsbild der Automotive-Branche im Jahr 2030 und skizzieren, welche Arbeitsbereiche es zusätzlich geben wird und welche Ausbildungen und Trainings die Profis der Zukunft brauchen werden. „Ein Job, der sicher dazukommen wird, ist der Automotive Cybersecurity Engineer und darauf müssen wir unsere Studierenden vorbereiten. Nicht Security- oder Branchenwissen alleine ist nötig, sondern T-shaped Entwickler/innen, die neben tiefem Fachwissen auch ein breites Allgemeinwissen besitzen", erzählt Macher.

WENN SECURITY KEIN THEMA MEHR IST

Die Zukunft bringt also immer mehr und immer neue Herausforderungen für die Sicherheit in Computersystemen und der sie benutzenden Menschen. Stefan Mangard fasst die Bestrebungen zusammen: „Unser Ziel ist es, dass Security immer vorhanden ist, ohne dass man sich ständig z. B. via Updates darum kümmern muss. Solange das aber der Fall ist, sind unsere Lösungen nicht gut genug. Es ist nicht die Zeit, sich auf unseren Lorbeeren auszuruhen. Für uns beginnt die Arbeit gerade erst." ■

Eine Möglichkeit, den Markteintritt unsicherer Produkte zu verhindern, sind entsprechende Gesetzgebungen, Normen und Konformitätsbewertungen. In anderen Bereichen unseres täglichen Lebens sind sie gängig: Autos müssen Crashtests durchlaufen, neuartige Medikamente müssen zugelassen werden, bevor sie verkauft werden dürfen, Spielzeug für Kinder muss bestimmten Sicherheitskontrollen unterzogen werden, elektrische Systeme müssen Konformitätstests durchlaufen und so weiter. Bei einer traditionellen Konformitätsbewertung sind die Kriterien aber recht statisch. Die physikalischen Gesetze ändern sich nicht, das heißt, einen Tag nach der Freigabe eines Zertifikats führt die Wiederholung eines Tests in der Regel zum gleichen Ergebnis. In der Cybersicherheit ist das nicht der Fall. Die Angriffe ändern sich ständig. Was heute Stand der Technik ist, ist am nächsten Tag vielleicht schon veraltet.

Daher muss die Konformitätsbewertung revolutioniert werden, um mit diesem neuen Umstand umgehen zu können. Eine Folge davon ist die strategische Forschungskooperation von SGS mit der TU Graz im Cybersecurity Campus Graz. Während sich die TU Graz stark auf die Erforschung neuer Architekturen und Konzepte konzentriert, um Zukunftstechnologien nachhaltig sicher zu machen, bringt SGS den Gesichtspunkt der nachweisbaren Sicherheit während des gesamten Lebenszyklus eines Produkts oder Systems ein. In naher Zukunft muss alles kontinuierlich und effizient unter Berücksichtigung von Zeit und Kosten auf Resistenz gegen Angriffe überprüft werden. Dies erfordert einerseits, dass neue Technologien nicht nur sicher, sondern auch effizient testbar gestaltet werden. Andererseits erfordert es potenziell neue Methoden beim Testen, Prüfen und Zertifizieren von Produkten, Systemen, Infrastrukturen, Betreibern, Services und Cloud-Lösungen.

Der Cybersecurity Campus Graz ist ein hervorragendes Umfeld, um die Kräfte zu bündeln, um an disruptiven Lösungen zu arbeiten, und lädt Partner aus der Industrie ein, sich zusammenzuschließen und sich einzubringen. ■