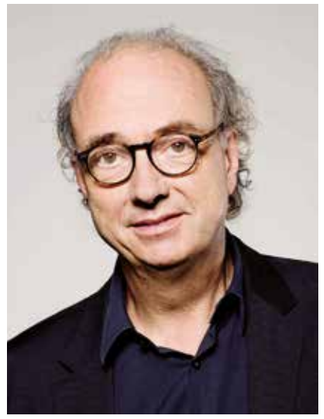
CAST

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY

CAST: Für mehr Kompetenz in der Cybersicherheit



Die Digitalisierung unserer Wirtschaft und Gesellschaft schreitet unaufhaltsam voran: eine rasante Entwicklung, verbunden mit ungeahnten Möglichkeiten, aber auch neuen Risiken. Eine breite Kompetenz in der Cybersicherheit ist hier für alle Beteiligten vonnöten.

Bereits vor 20 Jahren hat das Competence Center for Applied Security Technology (CAST) die Bedeutung von/der Cybersicherheit erkannt und seine Arbeit aufgenommen. Organisiert als gemeinnütziger Verein versteht sich CAST als Plattform und Kompetenznetzwerk für alle Fragen und Belange der Cybersicherheit. CAST bietet ein breites Spektrum an Leistungen: Workshops, Beratung, Tutorials, Nachwuchsförderung, Vernetzung und Wissensaustausch. So unterstützt CAST seine Mitglieder bei der Auswahl und beim Einsatz von bedarfsgerechter Sicherheitstechnologie.

Ziel des CAST ist es, angesichts des hohen Bedarfs an Cybersicherheit in allen Wirtschaftszweigen und Bereichen der öffentlichen Verwaltung, die Entwicklung der notwendigen Kompetenz nachhaltig zu unterstützen.

Mit dieser Broschüre stellen wir Ihnen ausgewählte Felder der Cybersicherheit vor, die im Rahmen monatlicher Workshops regelmäßig im CAST diskutiert werden.

Werden auch Sie Mitglied im CAST, profitieren Sie von seinen Angeboten, tragen Sie aktiv zu den Zielen des CAST bei und lassen Sie uns gemeinsam für eine sichere Cyberwelt sorgen.

Ihr

Johannes Buchmann

Prof. Dr. Johannes Buchmann
1. Vorstandsvorsitzender des CAST e. V.

CAST
COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY

Automotive Security

Die Informationstechnologie (IT) ist mittlerweile fester Bestandteil moderner Fahrzeuge und einer der größten Innovationsmotoren. Moderne Fahrzeug-Bordnetze bestehen teilweise aus über 100 Steuergeräten (engl. Electronic Control Units, ECUs), die verschiedene Fahrzeugfunktionen in Hard- und Software realisieren. Unterschiedliche Schnittstellen ermöglichen sowohl die Kommunikation der ECUs untereinander als auch die Vernetzung mit der Umwelt. Die Vernetzung wird in zukünftigen Fahrzeuggenerationen immer weiter voranschreiten, da moderne Mehrwertdienste wie z. B. ortsbasierte Dienste (engl. Location-based Services), aber auch Funktionen des autonomen Fahrens, ohne den Austausch von Daten nicht oder nur mit eingeschränkter Funktionalität realisierbar sind. Daten werden dabei an mobile Endgeräte wie Smartphones oder Tablets, andere Fahrzeuge, Infrastrukturkomponenten an der Straße, aber auch über das Internet an Backendsysteme von Herstellern und verschiedenen Dienstanbietern gesendet. Jedoch ergeben sich dadurch auch neue Herausforderungen in Bezug auf die IT-Sicherheit und den Datenschutz. So muss z. B. verhindert werden, dass Angreifer Fahrzeugfunktionen manipulieren und Leib und Leben der Insassen gefährden oder Bewegungsprofile erstellen.

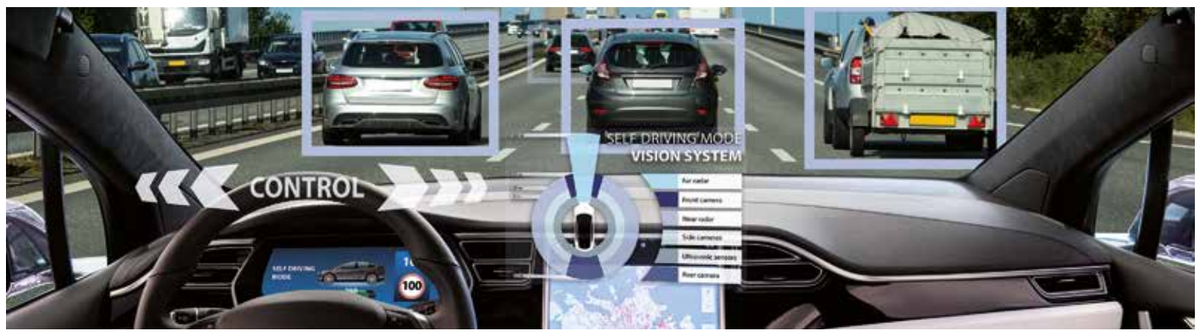
In solch sicherheitskritischen Systemen müssen deshalb geeignete IT-Sicherheits- und Datenschutzmaßnahmen schon beim Entwurf berücksichtigt werden (engl. Security and Privacy By Design). Praktikable Lösungen müssen dabei die speziellen Automotive-Anforderungen erfüllen, wodurch meist neue Konzepte entwickelt werden müssen.

Besondere Herausforderungen ergeben sich beispielsweise durch die lange Lebenszeit der eingesetzten eingebetteten Systeme. So können kryptographische Schlüssel gebrochen werden oder die eingesetzten kryptografischen Algorithmen werden unsicher. Wenn die Entwicklung der Quantencomputer weiter so voranschreitet, würden asymmetrische Verfahren wie RSA, DSA oder Diffie-Hellman auf einen Schlag unsicher. Auch bei symmetrischen Verfahren wie AES müsste die Schlüssellänge von 128 auf 256 Bit erhöht werden, sodass diese weiterhin sicher sind. Entsprechend müssen bereits jetzt entsprechende Vorkehrungen zur kryptografischen Agilität und Verfahren zum sicheren Over-the-Air-Code-Update getroffen werden. Problematisch kann jedoch eine weitere Eigenschaft der eingesetzten eingebetteten Systeme sein: deren Ressourcenbeschränkungen. So müssen bereits jetzt die eingesetzten kryptografischen Verfahren an die Ressourcenbeschränkungen angepasst werden. Verfahren der Post-Quantum-Kryptographie benötigen jedoch meist mehr Ressourcen und haben oft zusätzliche Anforderungen. Dies muss ebenfalls jetzt schon bei der Entwicklung berücksichtigt werden. Eine weitere Herausforderung ist die physikalische Zugreifbarkeit, welche das Auslesen von kritischen Daten oder die Manipulation von Firmware ermöglicht. Ein Angreifer könnte bspw. ein Motorsteuergerät manipulieren, um eine höhere Leistung zu haben. Schutz können hier z. B. spezielle Hardware-Sicherheits-Module und Verfahren zur Überwachung der Systemintegrität bieten.

Mit solchen Fragestellungen zur IT-Sicherheit und dem Datenschutz im Automotive-Umfeld beschäftigt sich das CAST-Mitglied Fraunhofer-Institut für Sichere Informationstechnologie (SIT). Fraunhofer SIT besitzt langjährige Erfahrung in der Durchführung von Sicherheitsanalysen sowie in der Konzeption und Realisierung von Hard- und Softwarelösungen im Automotive-Kontext. Themen umfassen u. a. sichere Entwicklungsprozesse, Sicherheitsanalysen und -tests, Integration von Hardware-Sicherheits-Modulen, leichtgewichtige und Post-Quantum-Kryptographie, Vehicle2X-Kommunikation. Auch bietet das SIT verschiedene Schulungen mit Praxisübungen zum Thema Automotive Security an.

Prof. Dr. Christoph Krauß, Professor für Netzwerksicherheit an der Hochschule Darmstadt, Abteilungsleiter Cyver-Physical Systems und Automotive Security am Fraunhofer SIT

Moderation CAST-Workshop
„Automotive Security“



Neue Aufgaben der IT-Sicherheit: Umsetzung der Datenschutz-Grundverordnung

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) unmittelbar in der gesamten Europäischen Union. Durch sie hat der Datenschutz eine völlig neue rechtliche Grundlage bekommen. Wie wirkt sich diese auf die Praxis der Datensicherheit aus?

Die DSGVO führt viele Regelungen der bisherigen Europäischen Datenschutzrichtlinie von 1995 fort. Da das deutsche Datenschutzrecht der Richtlinie entsprach, bleibt dessen Grundansatz erhalten und sind viele Regelungen der DSGVO mit den bisherigen Datenschutzregelungen vergleichbar. Neu ist etwa die Ausweitung des räumlichen Anwendungsbereichs durch das Marktortprinzip. Die DSGVO gilt dadurch für die Verarbeitung personenbezogener Daten aller Personen, die sich in der Union aufhalten, unabhängig davon, wo auf der Welt die Datenverarbeitung stattfindet. Neu sind einige Pflichten der Datenverarbeiter wie zusätzliche Dokumentations- und Informationspflichten. Neu ist auch der Versuch, durch viele verfahrensbezogene Regelungen den Vollzug des Datenschutzrechts in der Union zu vereinheitlichen. Für Verstöße gegen die Verordnung drohen künftig drastische Sanktionen: bis zu 20 Mio. Euro oder im Fall eines Unternehmens bis zu 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Für die Datensicherheit ist die ausdrückliche Auflistung der Grundsätze der Datenverarbeitung bedeutsam. Sicherheitsziele sind danach, dass die Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden dürfen, dass sie dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen und dass sie in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Vor allem setzt die DSGVO das Ziel, dass die Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Diese Ziele sind nicht neu, auch ihre Konkretisierung in der sehr unsystematischen Vorschrift zur Datensicherheit sind bekannt. Diese benennt einige Ziele und Maßnahmen, allerdings unter der Maßgabe, dass der Verantwortliche entscheidet, welche Maßnahmen er „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ ergreifen will, um „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (siehe Art. 32 DSGVO).

Neu ist, dass diese Sicherheitsziele durch eine datenschutzgerechte Systemgestaltung und durch datenschutzfreundliche Voreinstellungen erreicht werden sollen und dass die Gewährleistung der Datensicherheit bei riskanten Datenverarbeitungen in einer Datenschutzfolgenabschätzung überprüft werden sollen. Neu ist auch, dass ein positives Ergebnis einer externen Überprüfung von Datenschutz und Datensicherheit in einem Datenschutzzertifikat zum Ausdruck gebracht werden kann, das im Wettbewerb verwendet werden darf.

Die DSGVO erhebt zwar den Anspruch, das Datenschutzrecht angesichts der Herausforderungen der digitalisierten Welt zu modernisieren. Sie spricht jedoch in keiner einzigen Regelung die spezifischen Grundrechtsrisiken moderner IT an wie z. B. smarte Informationstechniken im Alltag, Künstliche Intelligenz, selbstlernende Assistenzsysteme, Big Data, Cloud Computing oder datengetriebene Geschäftsmodelle. Schon gar nicht bietet sie für diese eine Lösung. Die gleichen Zulässigkeitsregeln, Zweckbegrenzungen oder Rechte der betroffenen Person gelten für die Mitgliederliste des kleinsten Vereins ebenso wie für die risikoreichsten Formen der Datenverarbeitung in Weltkonzernen und mächtigen Behörden. Insofern zeichnet sich die DSGVO durch eine schädliche Risikoneutralität bezogen auf Grundrechtsgefährdungen betroffener Personen aus.

Im Ergebnis enthält die DSGVO bekannte Anforderungen an die Datensicherheit, stellt dem Verantwortlichen weitgehend frei, welche Sicherheitsmaßnahmen er tatsächlich ergreift, nutzt aber neue Instrumente, um die Gewährleistung von Datensicherheit zu überprüfen und ein positives Ergebnis deutlich zu machen. Hinsichtlich der modernen Risiken des Datenschutzes, wie sie etwa mit Ubiqutious Computing, Big Data, Cloud Computing, Künstlicher Intelligenz, Robotik und Automatisierung verbunden sind, ist sie jedoch enttäuschend. Statt diesen Risiken durch klare Anforderungen zu begegnen, ist sie bezogen auf die Zulässigkeit der Datenverarbeitung, die Grundsätze des Datenschutzes und die Rechte der betroffenen Personen risikoneutral.

Prof. Dr. Alexander Roßnagel, Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes, Universität Kassel

Moderation CAST-Workshop „Recht und IT-Sicherheit“

Quantencomputer-resistente Sicherheit

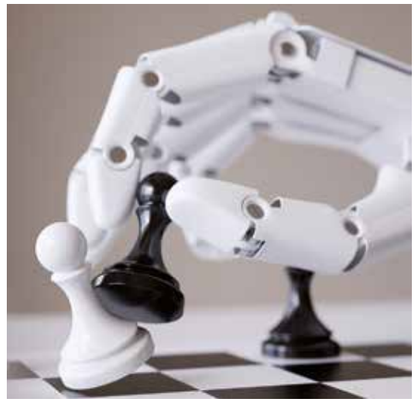
Bereits im Jahr 1982 hat Richard Feynman festgestellt, dass klassische Rechner nicht dazu geeignet sind, physikalische Systeme effizient zu simulieren. Er schlussfolgerte daher, dass Rechner, die auf den Gesetzen der Quantenmechanik beruhen, diese Aufgaben besser lösen können. Damit war eine neue Ära angebrochen und neuartige Quantenalgorithmen, die auf sogenannten Quantencomputern ausgeführt werden, haben sich hervorgetan. Die Einsatzgebiete und praktischen Möglichkeiten haben sich seither vervielfacht. Diese reichen von der Pharmabranche bis hin zu Big Data und Anwendungen der Künstlichen Intelligenz (KI). Das Ziel besteht in vielen Anwendungen darin, große Datenmengen in sehr viel kürzerer Zeit zu verarbeiten und damit die Effizienz und Kostenstruktur deutlich zu verbessern. An den hohen Investitionen in die Entwicklung von Quantencomputern beobachtet man, dass Unternehmen und Länder, vergleichbar mit der Zeit der Mondlandung, geradezu in Konkurrenz stehen, um den ersten praktikablen Quantenrechner anbieten zu können, da sie sich hierdurch ein enormes Marktpotenzial versprechen.

Die Entwicklung von praktikablen Quantencomputern birgt jedoch auch eine der größten Gefahren unserer Zeit. Im Jahr 1994 hat Peter Shor in seiner bahnbrechenden Arbeit einen Quantenalgorithmus vorgestellt, der nahezu alle in der Praxis genutzten Public-Key-Verschlüsselungs- und Signaturverfahren brechen kann. Die Dimension des Ausmaßes ist verheerend, denn solche kryptografischen Sicherheitsmechanismen bilden das Fundament unserer modernen IT-Sicherheitsinfrastruktur. Sie liegen beispielsweise dem im Internet eingesetzten TLS-Protokoll zugrunde, mit dem der Versand von vertraulichen E-Mails und Finanztransaktionen abgesichert wird. Unternehmen werden seit jeher aufgefordert, angemessene Maßnahmen schon jetzt zu ergreifen, um die negativen Folgen frühzeitig abzuwehren. Hierbei sollten auch die langen Umstellzeiten in Unternehmen und die lange Lebensdauer von IoT-Geräten, Maschinen und Autos berücksichtigt werden. Befinden sich diese erst einmal im Einsatz, sind Veränderungen nicht mehr oder nur noch mit einem enormen (Ressourcen-)Aufwand verbunden. Die Möglichkeit, heute verschlüsselte Daten zu speichern, um sie später zu entschlüsseln, bekräftigt einen zügigen Wechsel zusätzlich.

Sogenannte Quantencomputer-resistente Sicherheitslösungen versprechen hier Abhilfe. Sie können dazu genutzt werden, um die bisherige IT-Infrastruktur umzurüsten. Anders als traditionelle Sicherheitsmechanismen, wie z. B. RSA und Elliptische-Kurven-Kryptografie (ECC), basieren die zukunftssicheren Verfahren auf mathematischen Problemen, die nicht von Quantencomputern effizient gelöst werden können. Beispiele hierfür sind hash-, code- oder auch gitterbasierte Sicherheitstechnologien. Erste Standardisierungsbemühungen in dieser Hinsicht wurden im Jahr 2017 durch das National Institute of Standards and Technlogy (NIST) eingeleitet. Neben diesen Verfahren gibt es auch andere Alternativen, wie z. B. den Quantenschlüsselaustausch (QKD), bei dem die Sicherheit auf quantenmechanische Effekte zurückgeführt wird.

Dr. Rachid El Bansarkhani,
CEO von QuantiCor Security GmbH

Moderation CAST-Workshop
„Quantentechnologie und
Quantencomputer-resistente Sicherheit“



IT-Forensik erfordert hochqualifizierte Spezialisten

In den letzten Jahren haben die Verbreitung und der Gebrauch von elektronischen Geräten drastisch zugenommen. Traditionelle Informationsträger wie Bücher, Fotos, Briefe und Schallplatten wurden durch E-Books, digitale Fotografie, E-Mails, MP3s, soziale Netzwerke und die Cloud ersetzt. Dieser Wandel geht einher mit der wachsenden Speicherkapazität von heutigen Datenträgern, die von ein paar Megabyte auf mehrere Terabyte anwuchsen. Weiterhin speichern Anwender viele ihrer Informationen in der Cloud oder bei Anbietern sozialer Netzwerke.

Im Falle eines mutmaßlichen Schadensfalls eines IT-Systems (z. B. Angriff über das Netzwerk mit möglichem illegalen Abfluss von Informationen; mutmaßlicher Besitz/Verbreitung kinderpornografischer Schriften) ist es wichtig, die mit dem zu untersuchenden Vorfall zusammenhängenden digitalen Spuren auszuwerten. Dazu bedarf es zahlreicher Schritte wie Identifikation von Datenquellen digitaler Spuren sowie deren Sicherung, Selektion, Analyse, Auswertung und Dokumentation. Typischerweise führt dies zu einer enormen digitalen Datenmenge an unterschiedlichen Speicherorten. Der Bereich der Informatik, der sich dieser Thematik widmet, heißt digitale Forensik.

Die allgemeine Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen Handlungen, die möglicherweise rechtswidrig sind, systematisch untersucht werden. Zentraler Ausgangspunkt ist eine Frage des Rechts, zu deren Beantwortung wissenschaftliche Methoden unterschiedlicher Fachdisziplinen beitragen. Bekannte forensische Teilgebiete sind die forensische Medizin oder Rechtsmedizin (z. B. mit der typischen Fragestellung, wann und warum der Tod der Person eingetreten ist), die forensische Toxikologie (z. B. mit der typischen Fragestellung, ob ein unnatürlicher Tod durch eine Vergiftung herbeigeführt wurde) oder eben die digitale Forensik bzw. IT-Forensik im Kontext von rechtlichen Fragen zu IT-Systemen.

Malware ist ein wichtiges Thema im Zusammenhang mit IT-Sicherheitsvorfällen. Moderne Malware hinterlässt auf dem persistenten Datenträger oft keine verwertbaren Spuren, sondern agiert ausschließlich im Hauptspeicher. Daher gewinnt die Sicherung und Analyse des Hauptspeichers an Bedeutung. Auf diesem Gebiet der digitalen Forensik gibt es zahlreiche offene Forschungsfragen, an denen Forscher (z. B. am CRISP in Darmstadt) arbeiten.

Aufgrund der Komplexität und Diversität von IT-Systemen bedarf es geschulten Personals zur Durchführung einer IT-forensischen Untersuchung. Unternehmen und Behörden haben dies aufgenommen und richten eigene Expertise ein bzw. bieten IT-forensische Dienstleistungen an. Zur Aus- und Weiterbildung haben Hochschulen und andere Weiterbildungseinrichtungen Module, Zertifikate oder Studienprogramme eingerichtet, die IT-Forensiker aus- bzw. weiterbilden. Der CAST-Verein führt beispielsweise jährlich im Dezember einen Workshop zum Thema Internetkriminalität und Forensik durch. Die Workshops bieten eine gute Plattform, um über aktuelle Trends der digitalen Forensik informiert zu werden und sich darüber auszutauschen. Die Hochschule Darmstadt hat mehrere Lehrmodule zur digitalen Forensik im Studienprogramm, die von den Studierenden gerne belegt werden. Durch Gastvorträge erfahrener IT-Forensiker erhalten die Studierenden Einblicke in diese interessante Welt. Einige dieser Studierenden der letzten Jahre sind mittlerweile selbst als IT-Forensiker tätig.

Prof. Dr. Harald Baier, Internetsicherheit und Grundlagen der Informatik,
Hochschule Darmstadt

Moderation CAST-Workshop
„Forensik und Internetkriminalität"

Biometrische Gesichtserkennung

Unter Biometrie versteht man ein Verfahren zur Wiedererkennung von Personen. Biometrische Verfahren analysieren das Verhalten/Bewegungen des Menschen und/oder eine Eigenschaft der biologischen Charakteristika. Die biologischen Charakteristika gliedern sich einerseits in anatomische Charakteristika, die geprägt werden durch Strukturen des Körpers und andererseits in physiologische Charakteristika, die geprägt werden durch Funktionen des Körpers wie beispielsweise die Stimme. Der Vorgang der biometrischen Authentisierung liefert eine eindeutige Verknüpfung einer natürlichen Person mit ihrer Identität, unabhängig davon, wo diese Identität gespeichert ist. Der Vorgang der biometrischen Wiedererkennung lässt sich in die folgenden Schritte untergliedern:

- Erfassung der biologischen Charakteristika mit geeigneten Sensoren
- Vorverarbeitung zur Datenverbesserung
- Merkmalsextraktion zur signifikanten Beschreibung der Muster
- Vergleich der Merkmale mit den vorab gespeicherten Referenzdaten

Der Vorgang bedingt, dass eine Person vorab eingelernt wurde (Enrolment), um die notwendigen Referenzdaten zu bilden. Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen Dokument (zum Beispiel einem Reisepass) kombiniert werden, kann die biometrische Referenz (z. B. Passfoto) auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1-Vergleich). Bei einem Identifikationssystem hingegen wird das erfasste Bild mit vielen eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster ermittelt (1:n-Vergleich). Die Ähnlichkeit zwischen beiden Bildern muss jedoch ein definiertes Mindestmaß erreichen, damit eine zuverlässige Zuordnung der mit dem Referenzbild verbundenen Identität vorgenommen werden kann. Für die Biometrie geeignete Charakteristika sollten die folgenden Eigenschaften erfüllen:

- Verbreitung: Jede natürliche Person sollte die Charakteristik haben
- Einzigartigkeit: Die Charakteristik ist unterschiedlich für jede Person
- Beständigkeit: Die Charakteristik verändert sich nicht mit der Zeit
- Messbarkeit: Die Charakteristik ist mit geringem Aufwand messbar
- Performanz: gute Erkennungsleistung, geringer Aufwand der Algorithmen
- Akzeptabilität: Die Methode wird von der Zielgruppe angenommen
- Sicherheit: Es ist schwer, ein Replikat der Charakteristik zu erstellen

Werden einzelne Eigenschaften in einem mono-modalen System nicht erfüllt, so können multi-modale Systeme eine Lösung sein, bei denen man beispielsweise eine Gesichtserkennung mit einer Iriserkennung verbindet, um eine ausreichende Erkennungsleistung des biometrischen Systems zu erzielen. Zu einem gewissen Anteil sind Charakteristika genetisch oder durch Verhalten und Umwelt geprägt. Ein gut geeignetes biometrisches Charakteristikum wird jedoch in erster Linie durch Zufallsfaktoren ausgeprägt (bspw. Fingerabdruck, Muster der Iris).

Große biometrische Systeme, wie die forensischen Anwendungen der Kriminalämter, sind in der Regel offen gestaltet, damit Daten in einem einheitlichen standardisierten Format zwischen verschiedenen Dienststellen ausgetauscht werden können. Auch heutige Grenzkontroll-Anwendungen sind offene Systeme, da ein Personaldokument, das ggf. außerhalb Deutschlands produziert wurde, zur Einreise ausgelesen werden muss. Das Speichern von biometrischen Daten im Pass in einem Standardformat (ISO-19794-4:2005,ISO-19794-5:2005) ist dazu eine notwendige Voraussetzung.

Einige biometrische Systeme, wie in der Grenzkontrolle, werden bewusst nur unter Betreuung von Grenzbeamten betrieben, um Präsentations-Angriffe – wie zum Beispiel mit Gummi oder Silikon-Masken – auf die biometrische Erfassung zu detektieren. Für manche Sensoren können schon heute gute Sicherheitseigenschaften festgestellt werden, d. h. ein Sensor lässt sich nicht durch Artefakte (d. h. Fälschungen oder Plagiate einer Charakteristik) täuschen. Solche Sensoren sind dann auch für unbetreute Systeme in der physikalischen Zugangskontrolle zu Gebäuden geeignet oder beim Online-Banking, wodurch erheblich Personal eingespart werden kann. Zu beachten ist dabei, dass analoge Repräsentationen der biometrischen Charakteristik in der Regel unbeabsichtigt hinterlassen werden, z. B. Fingerabdrücke in guter Qualität auf der glatten Smartphone-Oberfläche. Diese könnten als Basis zur Erstellung eines Gummifingers dienen, mit dem dann der Fingerprint-Sensor angegriffen wird.

Ein Schwerpunkt der aktuellen Biometrie-Forschung ist es daher, Detektions-Mechanismen für derartige Präsentationsangriffe zu entwickeln, was z. B. durch die Erfassung zusätzlicher Informationen (z. B. Venenmuster, die schwieriger fälschbar sind) erfolgen kann.

Prof. Dr. Christoph Busch, Professor für Biometrie an der Norwegian University of Science and Technology (NTNU) und der Hochschule Darmstadt.

Moderation CAST-Workshop „BIOSIG“ (IEEE Conference)

Kennzahlen zur Überwachung und Steuerung des Informationssicherheitssystems Schritte zum Aufbau eines KPI-Systems

Key Performance Indicators (KPIs), nachfolgend kurz als „Kennzahlen“ bezeichnet, helfen dabei, den Grad der Zielerreichung, die Erfüllung von Compliance-Vorgaben und die dabei erreichte Effizienz zu bewerten. Sie liefern Hinweise für die Steuerung von Investitionen und tragen dazu bei, Fehlentwicklungen frühzeitig erkennen und korrigieren zu können.

Während betriebswirtschaftliche Kennzahlen seit langer Zeit etabliert sind und in vielen Unternehmen und Behörden einen wichtigen Beitrag zur Steuerung ihrer Prozesse leisten, befindet sich die Anwendung von Kennzahlen zur Informationssicherheit im Vergleich dazu noch in einer eher initialen Phase – und dies, obwohl es etwa mit NIST SP 800-55 und der vor zwei Jahren aktualisierten Norm ISO/IEC 27004:2016 sogar eigene Standards gibt, in denen Anforderungen an sinnvolle Kennzahlen und Vorgehensweisen für deren Entwicklung definiert sind.

Eine Erklärung für die zurückhaltende Nutzung von Kennzahlen ist ohne Zweifel, dass sich Sicherheit nicht so einfach messen lässt wie Arbeitsproduktivität oder betrieblicher Erfolg. Gleichwohl lassen sich auch im Bereich der Informationssicherheit Indikatoren finden, anhand derer sich Effektivität und Effizienz von Maßnahmen und die Güte von Prozessen bewerten lassen. Um diesem Zweck zu genügen, müssen Kennzahlen alle wichtigen Aspekte der Informationssicherheit einer Organisation abdecken, sie müssen aussagekräftig sein und Handlungsrelevanz besitzen, und selbstverständlich muss der Aufwand für die Erhebung der notwendigen Daten vertretbar sein.

In der Praxis zeigt sich, dass diese Anforderungen in ihrer Gesamtheit nicht einfach zu erfüllen sind. Gerade im Bereich der Informationssicherheit bewahrheitet sich oft die Regel, dass das, was leicht zu messen ist, nur eine geringe Relevanz hat, beziehungsweise umgekehrt, dass ausgesprochen wichtige Sachverhalte nur ausgesprochen schwer in adäquate Berechnungsformeln übersetzt werden können. Während sich technische Sachverhalte noch vergleichsweise leicht in Zahlenwerten ausdrücken lassen, fällt dies für die „weichen“ Faktoren, etwa die Awareness und das Know-how der Benutzer zur Informationssicherheit, wesentlich schwieriger. In der Praxis sind daher pragmatische Lösungen nötig, um das, was gemessen werden soll, mit dem, was gemessen werden kann, in Einklang zu bringen.

Bewährt hat sich daher ein schrittweises Vorgehen, das mit einem Pilotprojekt beginnt, um mit einem begrenzten Set an Kennzahlen Erfahrungen in der Spezifizierung, Erhebung und Auswertung zu sammeln. Dabei ist die Beteiligung sowohl der Fachverantwortlichen als auch der Zuständigen für IT und Informationssicherheit sehr hilfreich. Eine breite Beteiligung erleichtert es, relevante Kennzahlen zu definieren, ein geeignetes Raster zu deren Beschreibung zu entwickeln und die technisch-organisatorischen Voraussetzungen zur Erhebung der notwendigen Messwerte zu schaffen.

Wichtig ist zudem die Spezifizierung der Zielgruppen: Während die Leitungsebene primär an eher übergreifenden strategischen Kennzahlen interessiert ist, benötigen die IT-Administration operationale Kennzahlen, also solche, die ihr Aufschlüsse über die Qualität der Umsetzung konkreter technischer und organisatorischer Sicherheitsmaßnahmen liefern. Geeignete Kommunikationsmaßnahmen sollten zudem das Projekt begleiten, um eine breite Akzeptanz zu sichern. So ist etwa die Personalvertretung einzubinden, wenn auch organisatorische Aspekte reflektiert werden.

Mit der Erfahrung aus einem Pilotprojekt kann das Set an Kennzahlen dann zu einem Kennzahlensystem ausgebaut werden, das den unterschiedlichen Zielgruppen wie IT-Administratoren, der Geschäftsführung und den IT-Sicherheitsbeauftragten wichtige Informationen für die Überwachung und Steuerung des Informationssicherheitssystems liefert.

Mechthild Stöwer und Reiner Kraft, Fraunhofer SIT, Darmstadt - Sankt Augustin

Moderation CAST-Workshop „Management der Informationssicherheit”

Die Bedeutung der IT-Sicherheit und der Bedarf an Privatsphärenschutz haben nicht zuletzt durch Berichte über Cyberkriminalität, Wirtschaftsspionage, Identitätsdiebstahl sowie Aktivitäten ausländischer Geheimdienste zugenommen. Dabei erweisen sich u. a. mobile Technologien und Endgeräte als Einfallstor für solche Aktivitäten.

Smartphones und Tablet-Computer stellen mobile Plattformen mit einer hohen Integrationsdichte an Technologien und Funktionalitäten für mobile Dienstnutzung dar. Sie verfügen über Kommunikationsschnittstellen wie GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), LTE (Long Term Evolution), WLAN (Wireless Local Area Network) und Bluetooth sowie über Sensoren, Kameras oder etwa einen elektronischen Kompass. Darüber hinaus bieten sie diverse Anwendungsschnittstellen wie etwa Web-Browser und umfangreiche Interaktionsmöglichkeiten mittels Hardwareschnittstellen wie beispielsweise USB. In ähnlicher Weise sind auch eingebettete Computer, z. B. in Chipkartensystemen, Kraftfahrzeugen, HDMI-Sticks oder Kommunikationsknoten in Sensornetzwerken und vernetzten Industrieanlagen zu betrachten, bei denen es neben der systemischen Sicherheit u. a. auch auf Anforderungen hinsichtlich der physischen Sicherheit ankommt. Inzwischen gehört das Forschungsgebiet „Embedded Systems Security“ zu den relevanten Gebieten der IT-Sicherheitsforschung.

Alle Funktionalitäten und Technologien von mobilen und eingebetteten Systemen eröffnen vielfältige Anwendungsmöglichkeiten, für private, aber auch für geschäftliche Zwecke. Im Bereich der mobilen Kommunikation reicht die Funktionalität von Smartphones dabei weit über die reinen Kommunikationsanwendungen wie Telefonie hinaus. Für unterschiedliche Einsatzgebiete wie Text- und Multimedia-Messaging, mobiles Bezahlen, Fitness-Tracker, Authentifizierungs- sowie Lokalisierungs- und Telemedizinanwendungen gelten im jeweiligen Kontext unterschiedliche Sicherheitsanforderungen und -herausforderungen. Bei so vielfältigen und überlappenden Einsatzgebieten mobiler Technologien in Unternehmen, Verwaltungen und nicht zuletzt im Privatleben ist der IT-Sicherheit eine besonders hohe Priorität einzuräumen.

Momentan wird weltweit an 5G (Mobilfunk der fünften Generation) gearbeitet und die zugehörigen Technologien erprobt. Die Übertragungsgeschwindigkeit von 5G soll etwa das Zehnfache der LTE-Geschwindigkeit betragen und unter anderem die Konnektivität von Maschinen und Geräten verbessern. Technologisch wird 5G durch mmWave (millimeter Wave), MIMO (Multiple Input Multiple Output), SDN (Software Defined Networking), NFV (Network Functions Virtualization), IoT und Cloud Computing getrieben. Grundsätzlich wird 5G als Schlüsseltechnologie der digitalen Transformation angesehen und wird unter dem Blickwinkel der IT-Sicherheit und des Privatsphärenschutzes standardisiert. Hierzu werden entsprechende Spezifikationen erstellt und veröffentlicht. Die Bedrohungen, die mit 5G einhergehen, ergeben sich unter anderem auch aus der vorgesehenen Integration anderer Zugangstechnologien (wie z. B. UMTS, LTE und WLAN) über eine dafür vorgesehene Schnittstelle. Konsequenterweise erbt 5G somit auch existierende, ggf. noch unbekannte Bedrohungen vorheriger Technologien.

Dr. Kpatcha M. Bayarou, Abteilungsleiter Mobile Systems und Networks am Fraunhofer SIT

Moderation CAST-Workshop
„Mobile und Embedded Security”

Information Security - Beyond the “castle“

Not too long ago, achieving IT security was like building a castle. One builds up a wall securing the perimeter, this being fences and buildings for physical security and firewalls for network security. The market and outer town were also protected by a wall, but access was easier granted. Often different rings of walls separated the castle in different access areas, where different people would have access to. In IT this is mapped to DMZs and network zones or physical access areas.

But the castle‘s ruler had to adapt to long range weapons like bows, or siege weapons like catapults, against which his soldiers on top of the walls could not so easily defend. He had to identify the source of the attack and find measures to stop them. The bows he could defend with bows on his own, but for siege weapons alternative ways were needed.

Burning arrows, setting the town on fire, then made clear: own forces were not only needed on the outer wall of the castle, but also within. Intruders, doing sabotage and killings, made sure fighters were needed within, and so the duties of the forces multiplied.

Arming the people, making them aware of threats and how to react upon them, fighting on their own or calling the guard, relieved the situation for the soldiers. They could concentrate on the actual fights. But having a coordinator, who was not involved in the actual fighting, but kept the oversight, was now even more essential.

But even doing this all, an attack with air bound weapons would have been fatal: without preparation in form of anti-aircraft guns, which must have been acquired before, the castle would have fallen.

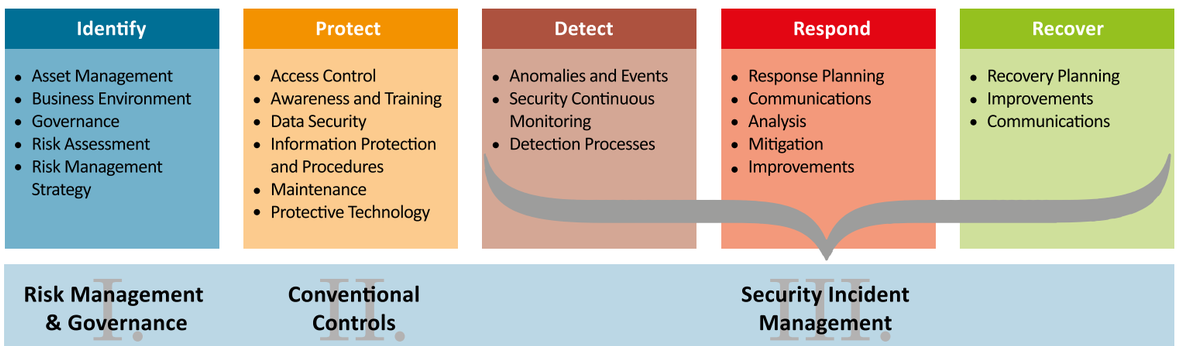
Same applies to information security: physical security at the perimeter and firewalls are not enough. Security measures are necessary and must be enforced, but the idea of protecting against all possible harms, if it ever was possible, will not work anymore. We do not know how the attacker will approach us. And the question is not, if, but when an attack will occur. But we can prepare for the attacks to come by staying informed on recent activities. And be prepared to react on them.

So, state of the art information security systems do not only focus on protection by building up defenses, but also improve detecting attacks and reacting upon them. The sooner a compromise is identified, the sooner one can stop it and keep damage at a minimum.

Besides improving technical measures like log analysis or intrusion detection, making employees aware of threats and enabling them to detect mischief, help identify and correct the situation can cover many aspects, where no technical solution is feasible or affordable.

Risk management will help setting focus: Identifying assets and their worth, defining the intended security level, keeping known risks up to date. Based on this one can decide on where to improve defense, where to look for mischief, how to respond and recover from it. And where to accept risk.

Marion Steiner, Senior IT Security Expert
Head of Business Development and Consulting Services @ISW



NIST Cyber Security Framework

Competence Center for Applied Security Technology
CAST e. V.
Rheinstrasse 75
D-64295 Darmstadt

Telefon: +49 6151 869230
Fax: +49 6151 869224
E-Mail: info@cast-forum.de
https://www.cast-forum.de

Mitglieder:
https://www.cast-forum.de/mitglieder

Geschäftsführung: Claudia Prediger
E-Mail: Claudia.Prediger@cast-forum.de

CAST
COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY

JS/DEUTSCHLAND • Concept: JS/MEDIA TOOLS A/S • 37700 • www.jsdeutschland.de