Kompetenzzentrum
Öffentliche IT

KOMPETENZZENTRUM ÖFFENTLICHE INFORMATIONSTECHNOLOGIE

DAS ÖFIT-TRENDSONAR DER IT-SICHERHEIT

Nicole Opiela, Petra Hoepner, Mike Weber

Fraunhofer
FOKUS

IMPRESSUM

Autoren:
Nicole Opiela, Petra Hoepner, Mike Weber

Gestaltung:
Jan Dennis Gumz, Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

1. Auflage Mai 2016

INNOVATIONEN ERÖFFNEN
NEUE HORIZONTE.

INHALTSVERZEICHNIS

IT-SICHERHEIT ALS HERAUSFORDERUNG

IT-Sicherheitsvorfälle und der damit einhergehende Schaden für die Wirtschaft, den öffentlichen Sektor und Privatpersonen nehmen seit Jahren stetig zu.[1] Laut Schätzungen einer von McAfee[2] im Jahr 2014 veröffentlichten Studie kosten allein Cyberkriminalität und Cyberspionage die Weltwirtschaft jährlich etwa 400 Milliarden US-Dollar. Für Deutschland wird der Schaden auf 1,6 % des BIP beziffert.

In einer zunehmend vernetzten Welt können IT-Vorfälle gravierende Konsequenzen haben, wenn sie beispielsweise die Sicherheit kritischer Infrastrukturen gefährden. Dabei müssen solche Vorfälle nicht auf vorsätzliche Attacken oder Hacking-Angriffe zurückgehen, wie der im Mai 2015 bekannt gewordene Angriff auf das interne Datennetz des deutschen Bundestages. Auch menschliches Versagen, System- oder Implementierungsfehler und Umweltfaktoren können die IT-Sicherheit beeinträchtigen. IT-Sicherheit und Datenschutz geraten daher zunehmend in den Fokus von Öffentlichkeit, Behörden und Unternehmen.

Die Gefahren im Netz verändern sich und nehmen stetig zu. Um bei diesem Wettrennen von neuen Bedrohungslagen und Schutzmaßnahmen nicht das Nachsehen zu haben, ist es wichtig, bereits heute die Möglichkeiten von morgen zu kennen. Nur so wird es möglich, sich wirksam und vorausschauend auch gegen neue Risiken und Gefahren abzusichern. Unter diesen Voraussetzungen die richtigen, zukunftsfesten Entscheidungen zu treffen – dazu möchte das ÖFIT-Trendsonar einen Beitrag leisten.

Dabei kann und will das ÖFIT-Trendsonar kein Einkaufsratgeber für die richtigen IT-Sicherheitsprodukte sein. Zum einen geht der Blick über den aktuellen Status quo hinaus, zum anderen hängt die angemessene Sicherheitslösung immer vom konkreten Anwendungsfall ab. Dabei spielen technologieferne Aspekte eine wichtige Rolle, von denen Sicherheits- und Risikomanagement, Security-by-Design, Vertrauen, Resilienz und die Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter zu den wichtigsten zählen. Solche Fragen von Organisation und Prozessen bleiben ebenso unberücksichtigt wie Bewertungen des Schutzniveaus konkreter Lösungen.

Stattdessen wurden generalisierbare Kriterien für Technologietrends identifiziert, die für konkrete Entscheidungen zur Ausgestaltung der IT-Sicherheit wichtig sein können. Unter Trends werden dabei IT-Sicherheitslösungen verstanden, bei denen zurzeit maßgebliche Entwicklungen zu beobachten oder in Zukunft zu erwarten sind. Diese Entwicklungen können beispielsweise durch technologische Durchbrüche, aber auch durch veränderte Rahmenbedingungen oder Gesetze ausgelöst werden. Leitfragen der Analyse sind etwa: Wird die technologische Basis einer heute eingekauften Lösung auch morgen noch tragfähig sein? Wie steht es mit der Konkurrenzsituation am Markt und wie leicht lassen sich vorhandene Lösungen untereinander austauschen? Diese Publikation kann damit als Überblick für all diejenigen dienen, die sich mit den Entwicklungen in der IT-Sicherheit vertraut machen möchten. Jenseits aller Hypes und oftmals stürmischen technologischen Entwicklungen geht das Sonar in die Tiefe und beleuchtet Aspekte der vorgestellten Technologietrends, die sich erst offenbaren, wenn man unter die Oberfläche schaut. So werden Indikatoren und Bewertungen präsentiert, die für die IT-Sicherheitspolitik ebenso wertvoll sein können wie für die konkrete Entscheidung zur Ausrichtung der eigenen IT-Systeme.

Das ÖFIT-Trendsonar steht auch online zur Verfügung und erlaubt den direkten Vergleich von einzelnen Technologietrends unter: http://www.oeffentliche-it.de/trendsonar.

[1] Vgl. Europäische Kommission (2013): »Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace« S. 3 oder Europäische Kommission (2013): »Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union« S. 2; https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security; zuletzt abgerufen am: 09.03.2016.

[2] McAfee; Center for Strategic and International Studies (2014): »Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II«; http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf; zuletzt abgerufen am: 12.02.2016.

[3] European Union Agency for Network and Information Security (2016): »ENISA Threat Landscape 2015«; https://www.enisa.europa.eu/publications/etl2015/; zuletzt abgerufen am: 12.02.2016.

DAS ÖFIT-TRENDSONAR IM ÜBERBLICK

Das ÖFIT-Trendsonar der IT-Sicherheit schafft einen Überblick über wichtige derzeitige und zukünftige Technologieentwicklungen. Hierzu werden 32 Technologietrends identifiziert, nach fünf Hauptanwendungsfeldern kategorisiert und anhand zweier Ausprägungen bewertet.

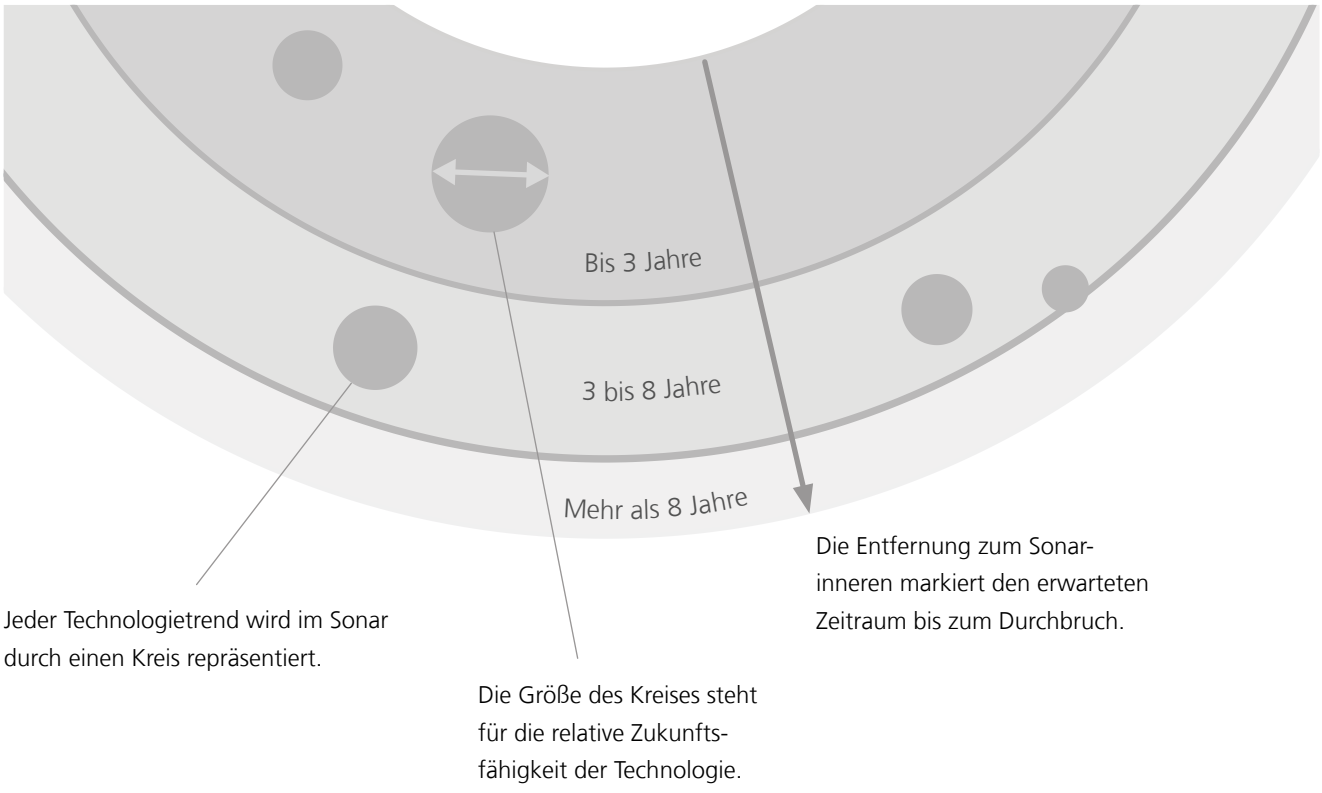
Als zentrale Bewertungskriterien werden die Zukunftsfähigkeit und der Zeitraum bis zum erwartbaren Durchbruch der Technologie dargestellt (s. Abbildung 1):

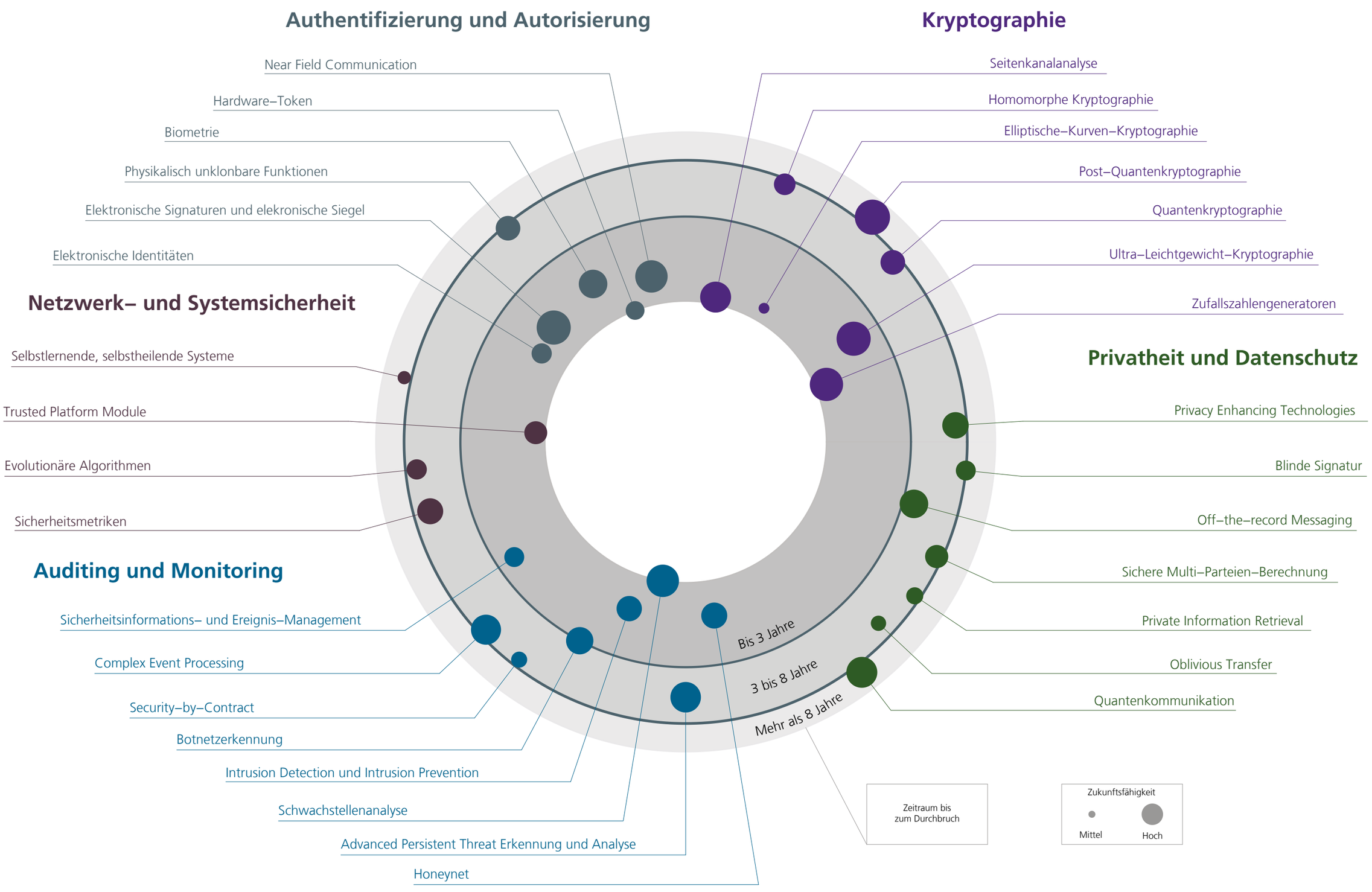
Unter **Zukunftsfähigkeit** wird die Zeitspanne verstanden, innerhalb derer die Lösung noch hinreichende Sicherheit verspricht. Sie ist daher umso niedriger, je eher bereits absehbar ist, dass technologische Neuerungen die Lösung ersetzen oder obsolet machen werden.

Der **Zeitraum bis zum Durchbruch** gibt an, wie viele Jahre es noch dauern wird, bis der Technologietrend als zuverlässig, technologisch robust und effektiv einsetzbar gilt. Mit dem Durchbruch lässt sich eine signifikante Verbreitung erwarten.

So ergibt sich auf einen Blick, wann eine technologisch reife Lösung mit welchem Potenzial für eine dauerhafte Umsetzung zur Verfügung steht.

Abbildung 1: Schematische Darstellung des Sonars




Authentifizierung und Autorisierung
Near Field Communication
Hardware–Token
Biometrie
Physikalisch unklonbare Funktionen
Elektronische Signaturen und elekronische Siegel
Elektronische Identitäten
Netzwerk– und Systemsicherheit
Selbstlernende, selbstheilende Systeme
Trusted Platform Module
Evolutionäre Algorithmen
Sicherheitsmetriken
Auditing und Monitoring
Sicherheitsinformations– und Ereignis–Management
Complex Event Processing
Security–by–Contract
Botnetzerkennung
Intrusion Detection und Intrusion Prevention
Schwachstellenanalyse
Advanced Persistent Threat Erkennung und Analyse
Honeynet
Kryptographie
Seitenkanalanalyse
Homomorphe Kryptographie
Elliptische–Kurven–Kryptographie
Post–Quantenkryptographie
Quantenkryptographie
Ultra–Leichtgewicht–Kryptographie
Zufallszahlengeneratoren
Privatheit und Datenschutz
Privacy Enhancing Technologies
Blinde Signatur
Off–the–record Messaging
Sichere Multi–Parteien–Berechnung
Private Information Retrieval
Oblivious Transfer
Quantenkommunikation
Bis 3 Jahre
3 bis 8 Jahre
Mehr als 8 Jahre
Zeitraum bis zum Durchbruch
Zukunftsfähigkeit
Mittel
Hoch

DAS ÖFIT-TRENDSONAR IM DETAIL

Für den Einsatz von Technologien sind nicht nur zukunftsbezogene Aspekte von Bedeutung, auch die Marktstruktur und die Möglichkeiten zur Einbindung in bestehende Systeme spielen eine große Rolle. Als Anhaltspunkte zur Beantwortung solcher Fragen werden zu jedem Technologietrend die Verfügbarkeit entsprechender Produkte (Angebot), ihre Marktdurchdringung (Nachfrage) und der Grad der Standardisierung bewertet. So ergibt sich eine Gesamtschau aus fünf Kriterien, die bei der zukunftsbezogenen und praxisrelevanten Einschätzung von Technologietrends berücksichtigt werden sollten. Diese fünf Bewertungen wurden mittels qualitativer Verfahren von Expertinnen und Experten des Fraunhofer-Instituts für Offene Kommunikationssysteme (FOKUS) ermittelt. Sie werden in Form eines Netzdiagramms wiedergegeben (s. Abbildung 2). Je größer die vom Netzdiagramm umschlossene Fläche, desto stärker sind die Kategorien ausgeprägt.

Ergänzend und teils kontrastierend werden quantitative Kenngrößen dargestellt. Hierzu wurden Daten aus Forschungsförderprogrammen auf Bundes- und EU-Ebene, aus wissenschaftlichen Literaturdatenbanken, aus Gründungsplattformen, aus Normungsdatenbanken und Suchmaschinenanfragen herangezogen.

Quantitative Indikatoren
- Existenz nationaler oder europäischer **Forschungsförderung** seit 2010 (✔ vorhanden, ✘ nicht vorhanden)
- Entwicklung wissenschaftlicher **Publikationen** bis und seit 2010 (↗ Anstieg, ↘ Abnahme, → gleichbleibend, ✘ nicht vorhanden)
- Existenz innovationsorientierter **Gründungen** seit 2009 (✔ vorhanden, ✘ nicht vorhanden)
- **Normentwürfe und Normen** (◐ Verhältnis, ○ nicht vorhanden)
- Entwicklung von **Suchanfragen** zwischen 2009 und 2015 (↗ Anstieg, ↘ Abnahme, → gleichbleibend, ✘ nicht vorhanden)

In der Gesamtschau der zukunfts- und gegenwartsbezogenen Einschätzungen sowie quantitativen Indikatoren ergeben sich Hinweise für die Anwendung der skizzierten Technologien.

Zukunftsfähigkeit
Ist bereits absehbar, dass eine Technologie nur (noch) eine geringe Zukunftsfähigkeit aufweist und deuten weder Forschungsförderprogramme noch der Trend bei wissenschaftlichen Publikationen auf eine Neujustierung, sollte bereits frühzeitig über Alternativen nachgedacht und die Migration vorbereitet und geplant werden. Zudem sollten nicht alle Lösungen auf die gleiche Technologie bauen, da sich durch eine Diversifizierung der technologischen Basis auch bei Schwachstellen oder Umstellungen die Kontinuität der Geschäftsprozesse sicherstellen lässt.

Handlungsfelder
- Technologische Basis diversifizieren
- Zukunftsfähigkeit angewandter Technologien fortlaufend prüfen und frühzeitig Alternativen identifizieren

Reife
Ausgereifte Technologien versprechen bewährten Schutz. Gleichwohl können veränderte Bedrohungen neue Lösungen erforderlich machen, mit denen noch nicht in gleicher Weise Erfahrungen gesammelt werden konnten.

Handlungsfeld
- Balance zwischen Reife und Innovationsgrad finden

Angebot
Vorsicht ist geboten, wenn die Technologie von nur wenigen Anbietern vertrieben wird und das Gründungsgeschehen keine Hinweise auf baldige Änderung der Angebotslage bietet. Sofern sich aus der Angebotslage Abhängigkeiten ergeben können, sollten Alternativen genau geprüft werden.

Handlungsfeld
- Alternativen prüfen

Nachfrage
Ist ein zukunftsfähiger Trend bereits verfügbar aber kaum verbreitet, kann dies mehrere Gründe haben. Unter Umständen ist die Technologie noch sehr neu und daher wenig bekannt, sodass unerfahrenere Kunden skeptisch sind und lieber bei etablierten Lösungen bleiben. Die Entwicklung der Suchanfragen bietet hierfür Hinweise. Es könnte zudem sein, dass eher kleine Technologieanbieter über eine sehr geringe Sichtbarkeit verfügen. Eine geringe Marktdurchdringung gebietet also Vorsicht,

IN DER GESAMTSCHAU DER EINSCHÄTZUNGEN UND INDIKATOREN ERGEBEN SICH HINWEISE FÜR DIE ANWENDUNG DER TECHNOLOGIEN.

entbindet aber nicht von der Notwendigkeit, sich ein umfassendes Bild über verfügbare Marktlösungen im Zusammenspiel mit den eigenen Anforderungen zu verschaffen, statt aus Gewohnheit auf die Produkte bekannter großer Firmen zurückzugreifen.

Handlungsfelder
- Eigene Sicherheitsanforderungen erfassen und definieren
- Überblick über vorhandene Marktlösungen und Anbieter verschaffen

Standardisierung

Standards tragen zu mehr Wettbewerb bei, verbessern die Interoperabilität und können Qualitätsniveaus festlegen. Geringer Standardisierungsgrad und relativ wenig Normentwürfe bergen daher Risiken für den Einsatz der Technologie.

Ein großes Angebot, breite Nachfrage und ein hoher Standardisierungs- sowie Reifegrad gehen möglicherweise mit nur geringer Zukunftsfähigkeit einher. Zwischen diesen Aspekten gilt es die angemessene Balance für das eigene Anwendungsszenario zu finden. Dabei bleibt das erforderliche Sicherheitsniveau ausschlaggebend, während die hier betrachteten Aspekte ergänzend hinzugezogen werden können.

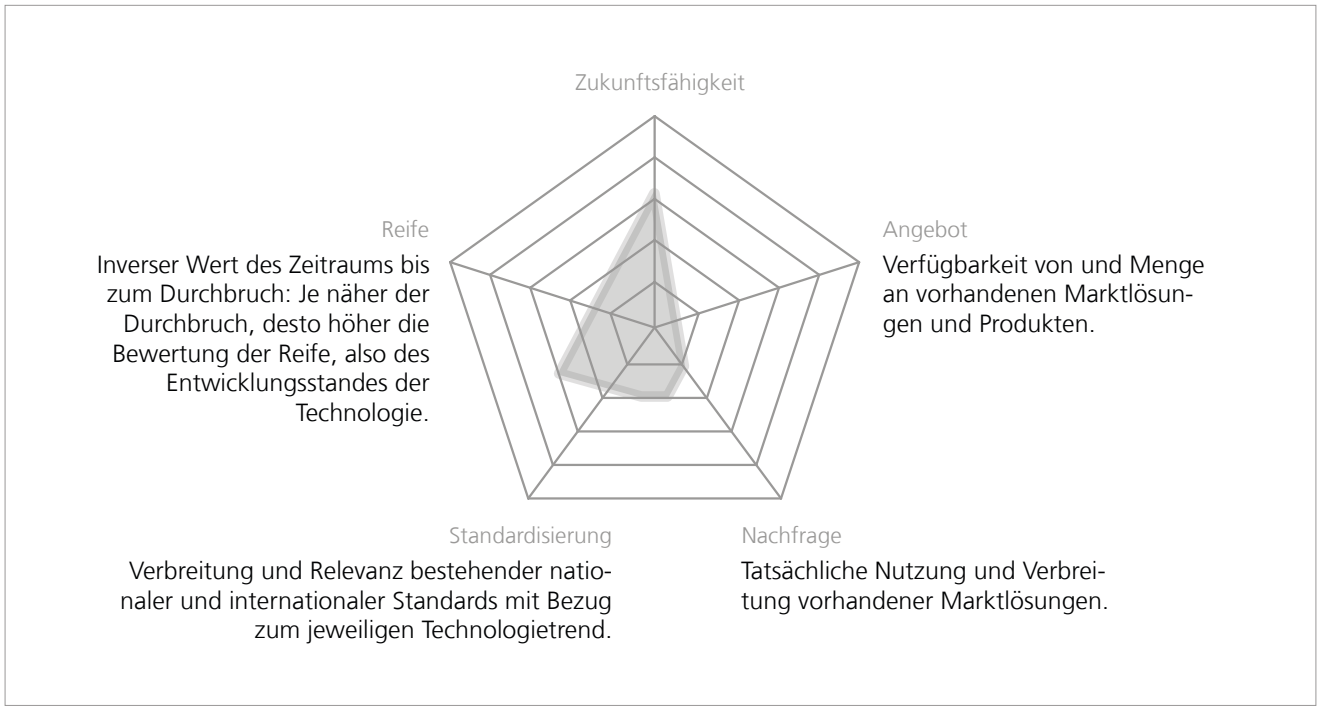
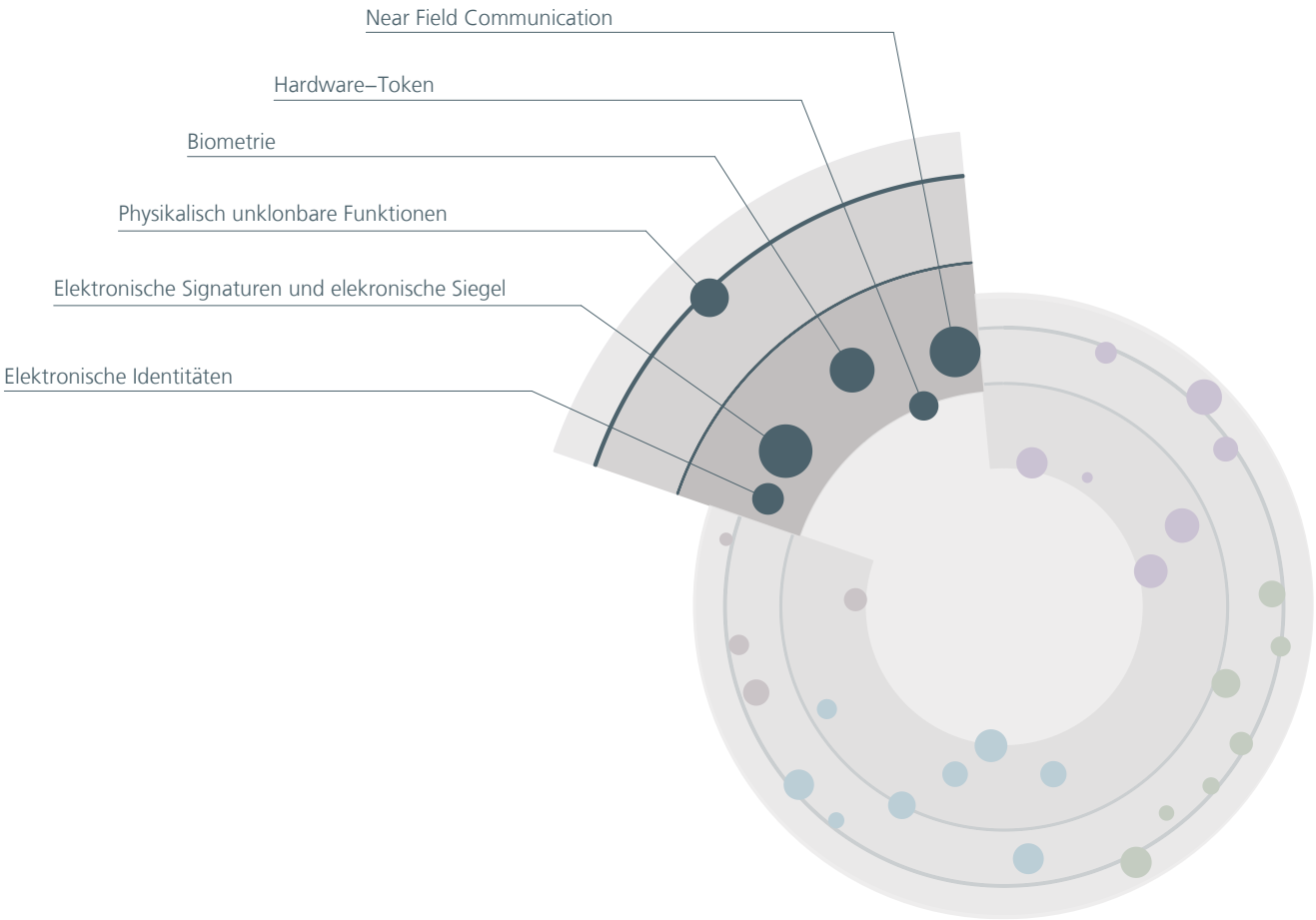


Abbildung 2: Schematische Darstellung eines Netzdiagramms

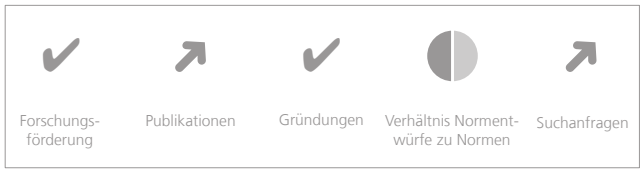
AUTHENTIFIZIERUNG UND AUTORISIERUNG

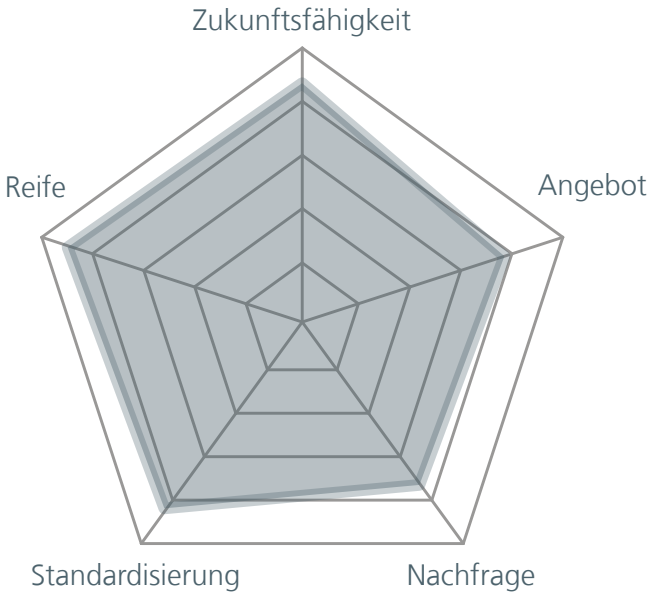
Um den Zugang zu Systemen, Prozessen und Dienstleistungen zu ermöglichen, muss ein Nutzer identifizierbar sein, d. h. bestimmte Identitätsinformationen müssen überprüft werden können. Für die sichere Nutzung ist die Authentizität dieser Identitätsdaten von entscheidender Bedeutung. Sind sie gefälscht, veraltet oder von zweifelhafter Herkunft, kann auch eine sichere Infrastruktur keine vertrauenswürdige Kommunikation erzeugen. Hat sich ein Nutzer authentisiert, muss entschieden werden, welche Berechtigungen dieser Nutzer hat. Die Autorisierung umfasst die Zuweisung und Überprüfung von Zugriffsrechten auf Daten, Dienste und Ressourcen.



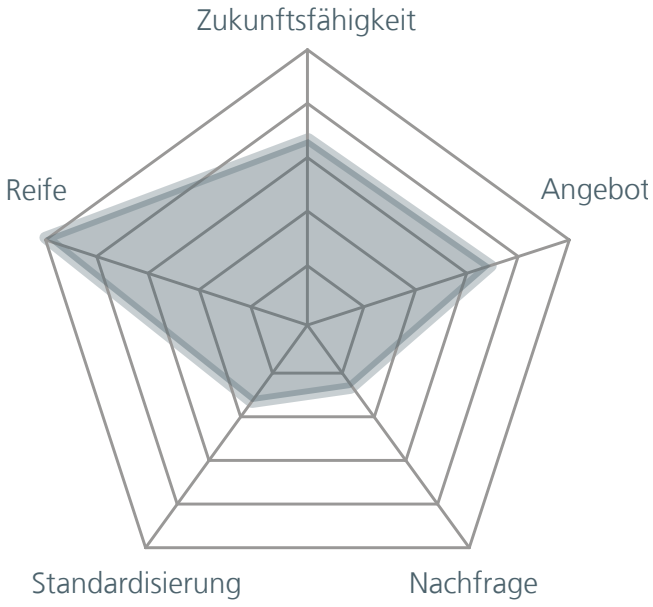
NEAR FIELD COMMUNICATION (NFC)

Near Field Communication (deutsch: Nahfeldkopplung) dient dem kontaktlosen Datenaustauch im Nahbereich von wenigen Zentimetern. Viele Geräte wie Smartphones, PDAs oder auch Kreditkarten besitzen bereits einen NFC-Chip. Lediglich durch das Aneinanderhalten NFC-fähiger Geräte können Daten ausgetauscht oder Informationen und Dienste abgerufen werden. Hauptanwendungsgebiete sind Bezahlanwendungen für kleinere Beträge, elektronische Eintrittskarten, aber auch die Zeiterfassung oder Zutrittskontrolle. Neue Anwendungsmöglichkeiten werden im Smart Home oder Internet der Dinge erschlossen.

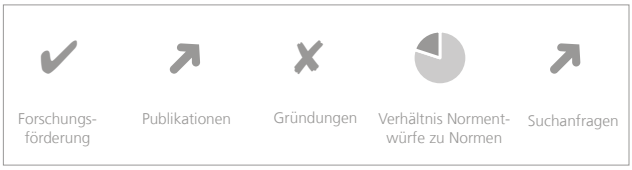




HARDWARE-TOKEN

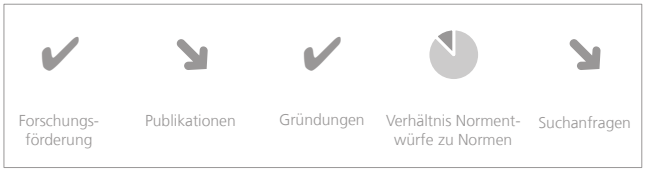


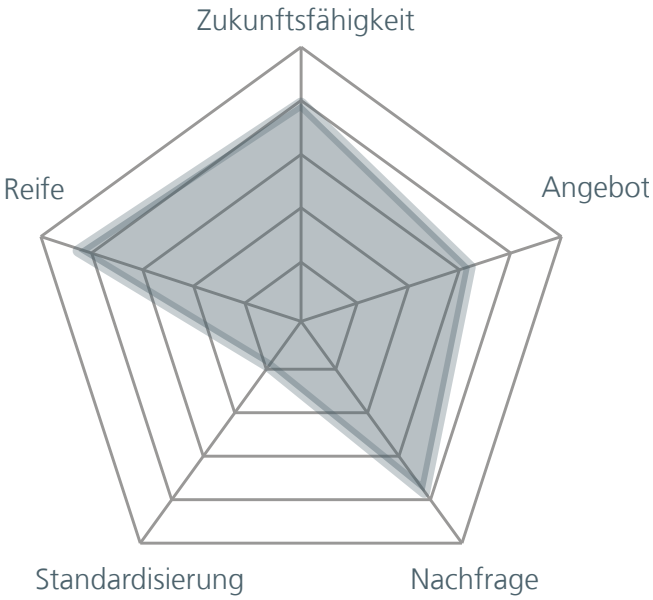
Hardware-Token sind Gegenstände, wie beispielsweise USB-Sticks, Smartcards oder RFID-Token, die der Identifizierung und Authentifizierung von Nutzern dienen. Wird eine starke Authentisierung für sicherheitskritische Anwendungsbereiche gefordert, kommt häufig eine Kombination von Wissen und Besitz zum Einsatz. Als Faktor Besitz dienen die Hardware-Token, die in Verbindung mit dem Faktor Wissen (PIN oder Passwort) verwendet werden. Neue Entwicklungen wie FIDO-Token sollen an unterschiedlichen Geräten universell einsetzbar sein.



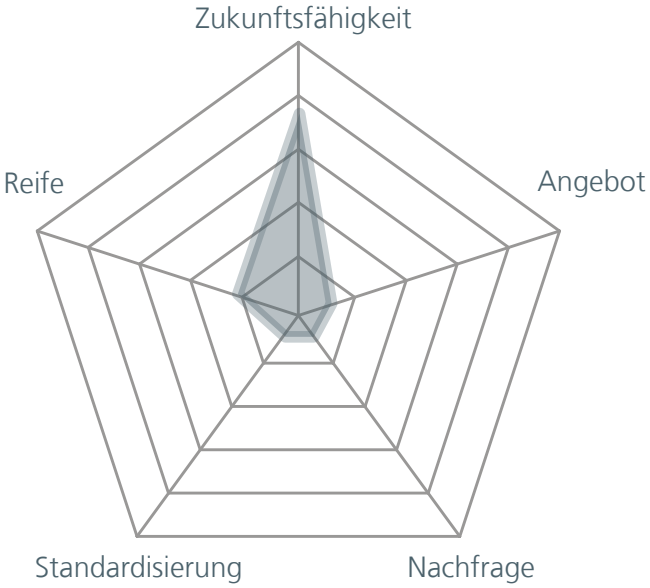
BIOMETRIE

Biometrie dient der automatisierten Erkennung von Personen anhand ihrer physiologischen oder verhaltensbedingten Eigenschaften. Biometrische Verfahren für die Authentisierung verwenden ein oder mehrere biometrische Merkmale wie beispielsweise Fingerabdruck, Iris, Handschrift oder auch Gesichtserkennung. Bei deren Einsatz für Zugang oder Zutritt muss eine akzeptable Erkennungsleistung gewährleistet werden und eine Lebendprüfung stattfinden, damit keine Nachbildungen von Fingern oder Gesichtsmasken eingesetzt werden können. Neue und verbesserte Verfahren sollen einfach verwendet werden können und gleichzeitig die falsche Erkennung und falsche Zurückweisungen von Personen minimieren.



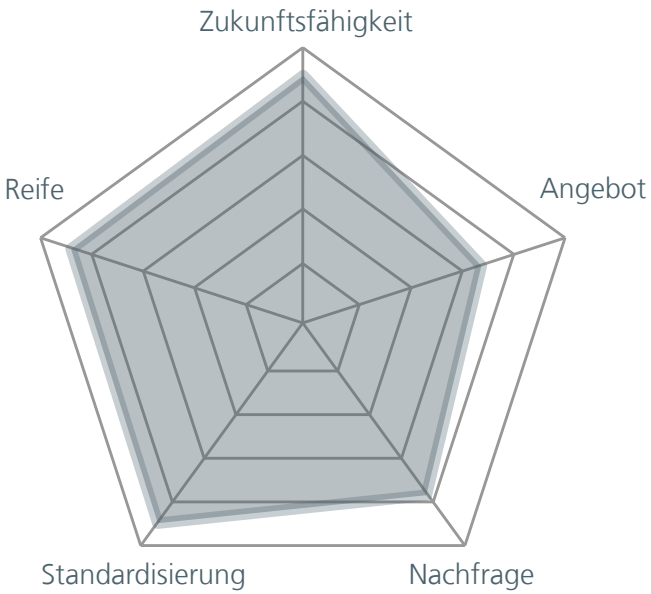


PHYSIKALISCH UNKLONBARE FUNKTIONEN

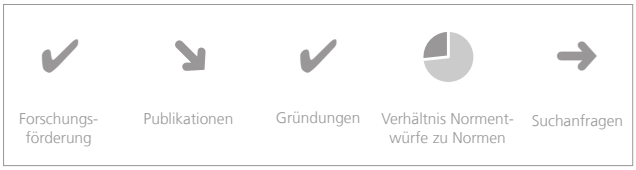


Physikalisch unklonbare Funktionen dienen zur Erzeugung eines physikalischen Fingerabdrucks von Gegenständen als Pendant zum biometrischen Fingerabdruck von Menschen. Sie basieren darauf, dass jedes Objekt eindeutige physikalische Eigenschaften besitzt, welche sich weder justieren noch reproduzieren lassen. Ausgenutzt werden dafür physikalische Variationen, die bei Herstellungsprozessen auftreten. Ein Anwendungsgebiet ist beispielsweise die Verhinderung von Produktpiraterie. Hier wird der physikalische Fingerabdruck eines Produkts beim Hersteller registriert, sobald die Ware produziert wurde. Um eine erhaltene Ware zu überprüfen, wird ihr physikalischer Fingerabdruck bestimmt und anschließend beim Hersteller verifiziert.

ELEKTRONISCHE SIGNATUREN UND ELEKTRONISCHE SIEGEL

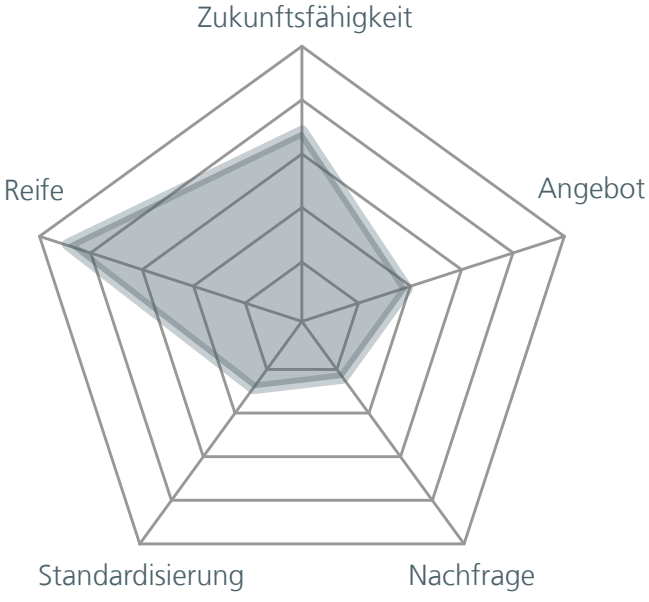


Elektronische Signaturen und Siegel verknüpfen Daten und Dokumente mit Informationen über die Identität des Signierenden bzw. Siegelerstellers. Qualifizierte elektronische Signaturen (QES) sind der handschriftlichen Unterschrift rechtlich gleichgestellt. Qualifizierte elektronische Siegel wurden als Pendant zur QES eingeführt, um juristischen Personen die Möglichkeit zu geben, den Ursprung und die Unversehrtheit von elektronischen Dokumenten rechtsverbindlich zu garantieren. Sie können auch verwendet werden, um digitale Besitzgegenstände einer juristischen Person wie beispielsweise Softwarecode zu kennzeichnen. Mit der EU eIDAS-Verordnung werden ab dem 1. Juli 2016 qualifizierte elektronische Signaturen und Siegel grenzüberschreitend in Europa anerkannt.



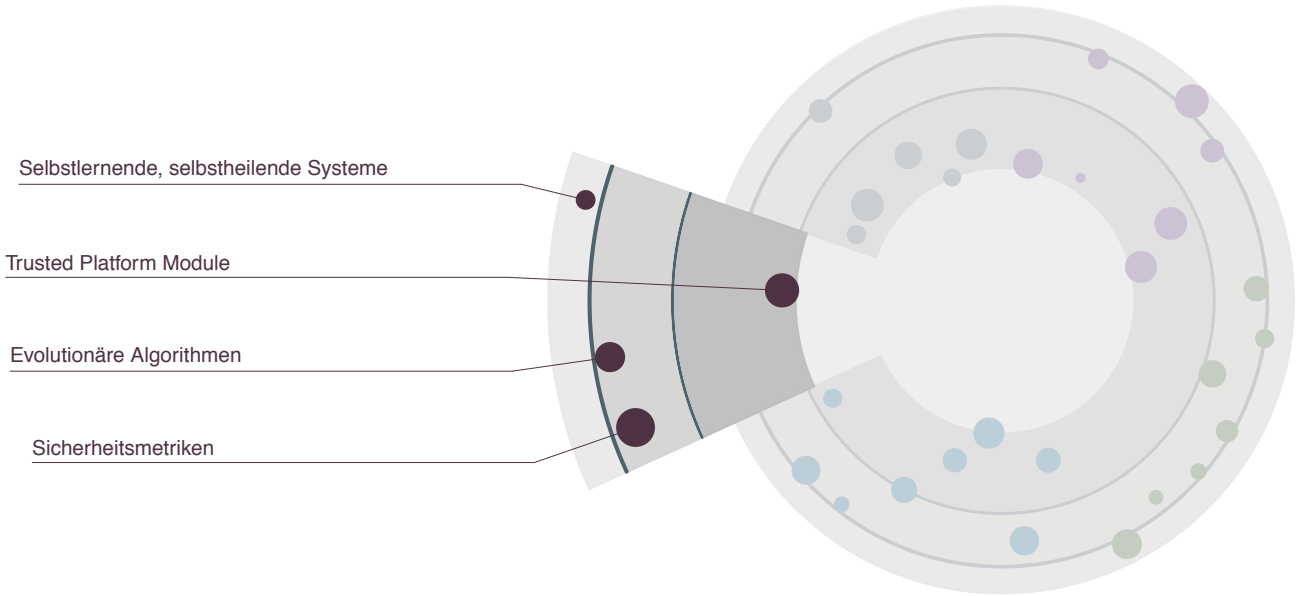
ELEKTRONISCHE IDENTITÄTEN (eID)

Die Identität einer natürlichen oder juristischen Person wird durch verschiedene Eigenschaften beschrieben, wie beispielsweise Name, Anschrift, Geburtsdatum, Email-Adressen oder auch Pseudonyme. In der virtuellen Welt werden Namen und Eigenschaften durch Attribute einer elektronischen Identität abgebildet. Seit 2010 stellt der deutsche Staat seinen Bürgerinnen und Bürgern mit dem Personalausweis eine elektronische Identität aus. Andere europäische Staaten haben eID Lösungen mittels Software-Zertifikaten, Smartcards oder Smartphones etabliert. Eingesetzt werden eIDs bei der Identifizierung und Authentifizierung.



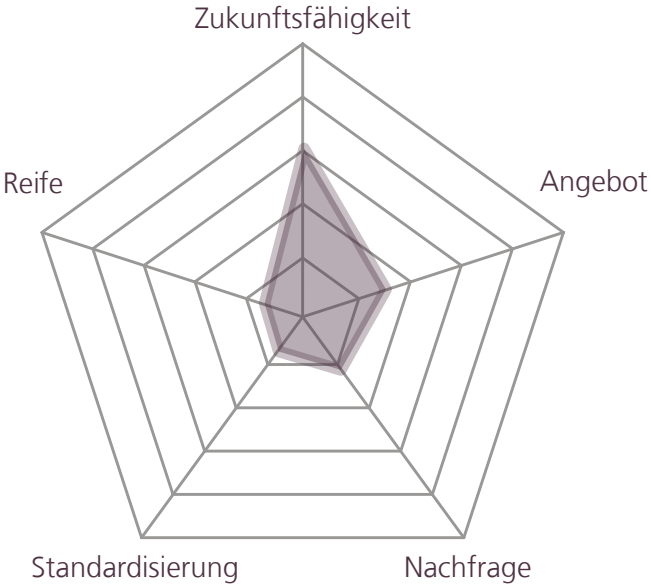
NETZWERK- UND SYSTEMSICHERHEIT

Netzwerk- und Systemsicherheit umfasst unterschiedliche Sicherheitsmaßnahmen und -verfahren, die Sicherheitsvorfälle verhindern (Prävention), diese während des Betriebs entdecken (Detektion) oder nach Sicherheitsvorfällen Schäden beheben sollen (Reaktion).

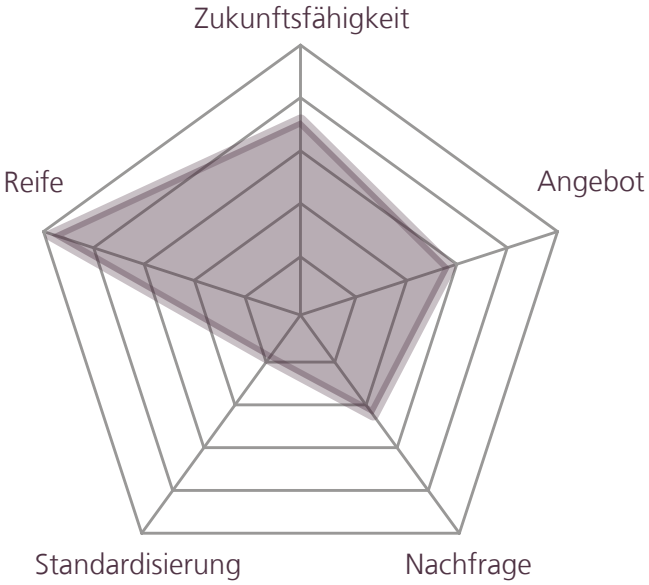


SELBSTLERNENDE, SELBSTHEILENDE SYSTEME

IT-Sicherheit durch Abschottung kann in komplexen, vernetzten Systemen nur bedingt funktionieren. Zunehmend gewinnen Funktionen zur Stärkung der Widerstandsfähigkeit und der inneren Abwehrkraft von Systemen an Bedeutung. Dies umfasst die Diagnose, Lernfähigkeit und korrektive Adaption an neue Gegebenheiten durch selbstlernende bzw. selbstheilende Systeme in Anlehnung an das Immunsystem des Menschen. Die Vorsilbe »selbst« verweist darauf, dass ein System diese Aufgaben eigenständig im Rahmen seiner Möglichkeiten übernimmt, ohne dass eine konkrete Reaktion schon bei der Entwicklung des Systems vorgegeben wurde. Die verschiedenen Aufgaben können in der Realität widersprüchlich sein und daher eine hohe technische Intelligenz vom System verlangen.



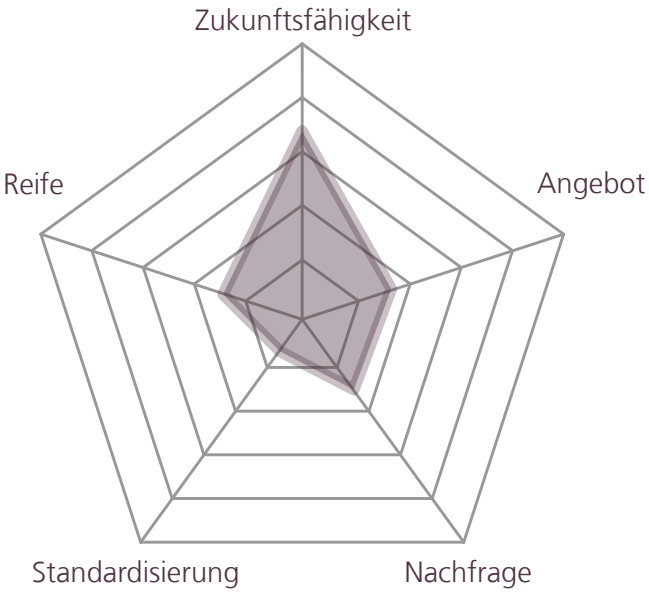
TRUSTED PLATFORM MODULE (TPM)

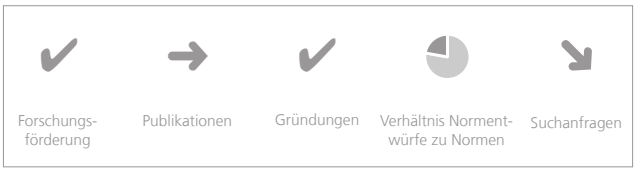


Trusted Platform Modules sind Chips, die einen Computer oder andere Rechensysteme um Sicherheitsfunktionen wie Zufallsgeneratoren, Schlüsselgenerierung und -ablage, kryptographische Versiegelung von Systemkonfigurationen oder Ausstellung von Bescheinigungen für die Authentifizierung von Geräten erweitern. Mit TPMs wird die Hardware identifizierbar und Veränderungen am System können erkannt werden. TPM Chips befinden sich zwar seit Jahren in Computern, werden bisher aber nur eingeschränkt verwendet, da sie die Kontrollmöglichkeiten der Nutzer stark einschränken. Das Fernhalten unerwünschter Software kann beispielsweise sowohl Virensoftware als auch Konkurrenzsoftware betreffen.

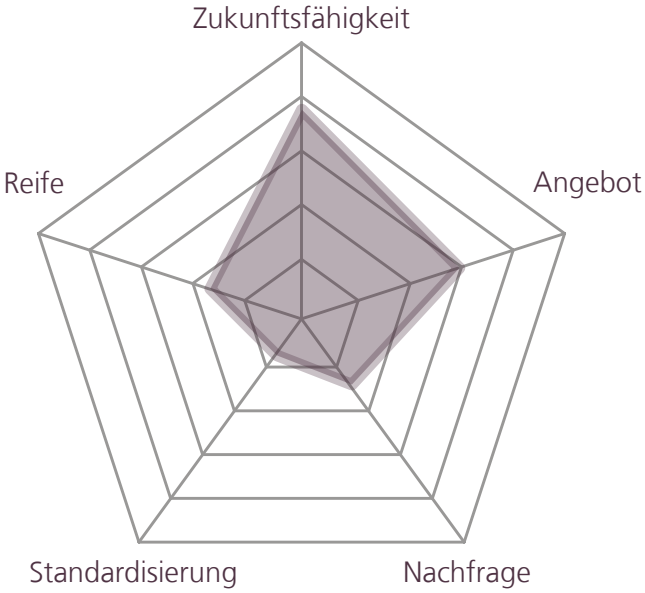
EVOLUTIONÄRE ALGORITHMEN

Evolutionäre Algorithmen orientieren sich an der biologischen Evolution und bilden deren Prozesse nach. Komplexe multimodale Problemstellungen werden durch Annäherungen und Anpassungen an die beste Lösung optimiert, wobei auch mehrere unterschiedliche Lösungen geliefert werden können. Ständige Verbesserungen basieren auf dem Wechselspiel zwischen Variation und Selektion. Anwendungsgebiete für evolutionäre Algorithmen sind Simulation und Modellierung, die auch zur Stärkung der Robustheit von Systemen angewendet werden können.

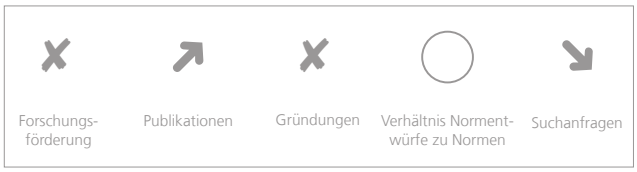


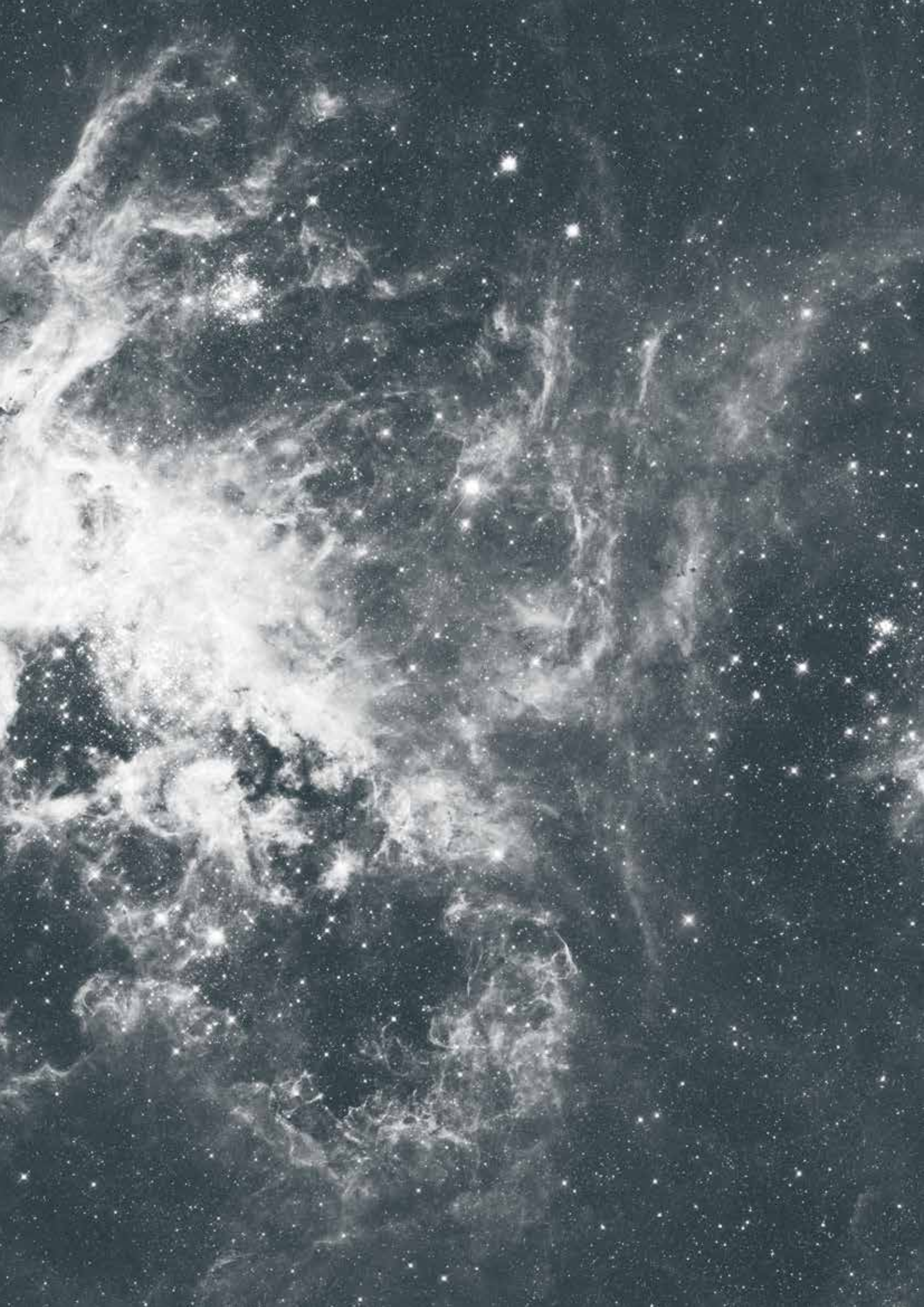


SICHERHEITSMETRIKEN



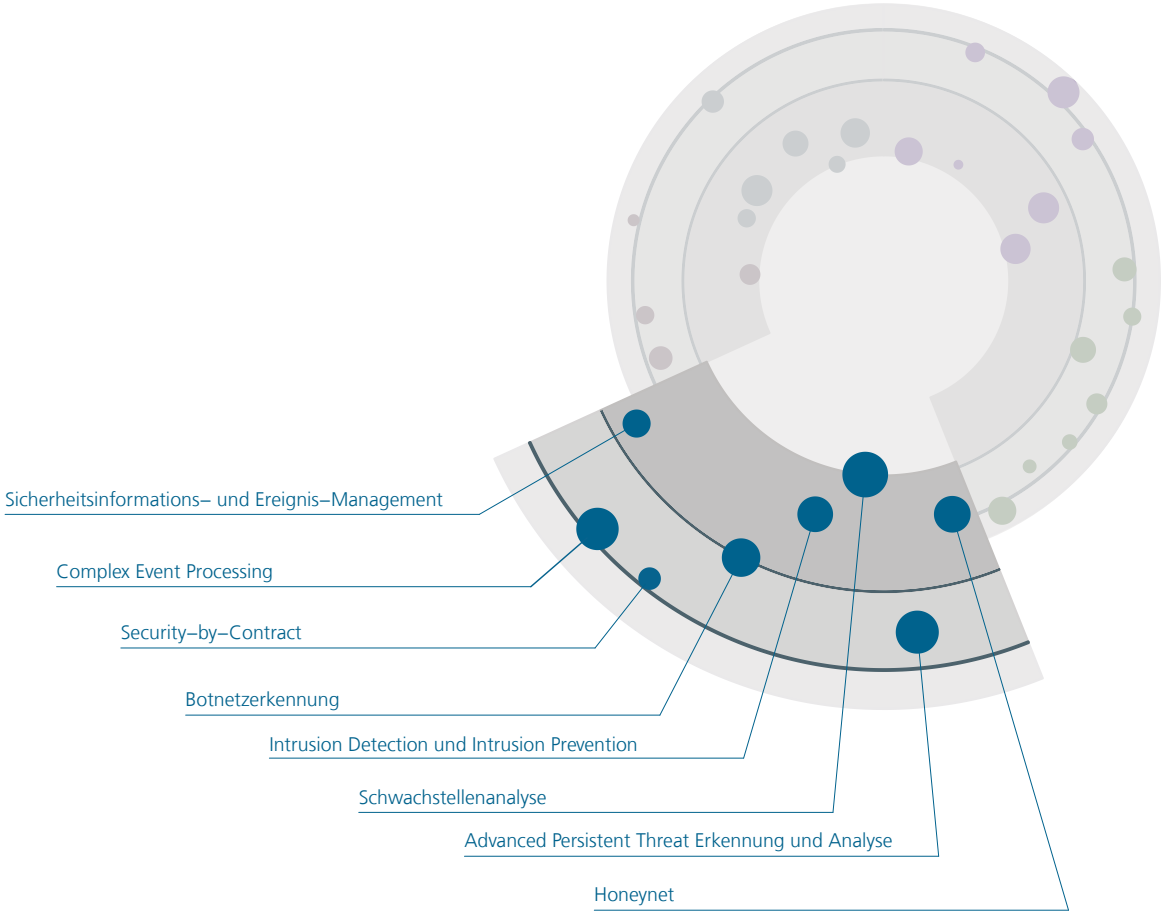
Um den Grad der Informationssicherheit in Systemen und Infrastrukturen zu bewerten, muss Sicherheit gemessen werden können. Sicherheitskennzahlen dienen dabei als objektive, quantifizierbare Maßzahlen, um Sicherheitsentscheidungen sowohl während der Anschaffungsphase als auch während des Betriebs treffen zu können. Ein Ziel von Sicherheitsmetriken ist der Nachweis, dass die geplanten und umgesetzten Sicherheitsmaßnahmen eine spezifische Sicherheitspolitik erfüllen. Entscheidungen und Bewertungen hinsichtlich der IT-Sicherheit werden so transparent und nachvollziehbar. Anwendungsgebiete für Sicherheitsmetriken sind die Beurteilung der Sicherheitslage, Sicherheitsmanagement oder Cyberversicherungen.





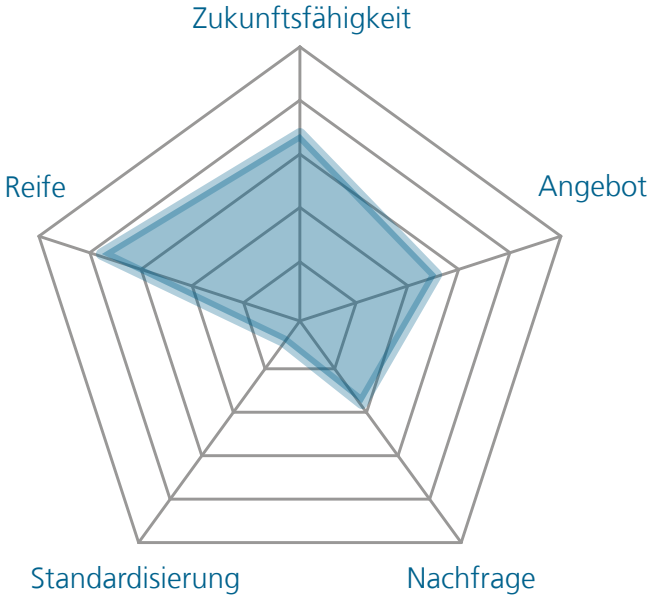
AUDITING UND MONITORING

Auditing und Monitoring sind Überbegriffe für die automatisierte Erfassung, Überwachung und Protokollierung von sicherheitsrelevanten Ereignissen in IT-Infrastrukturen.

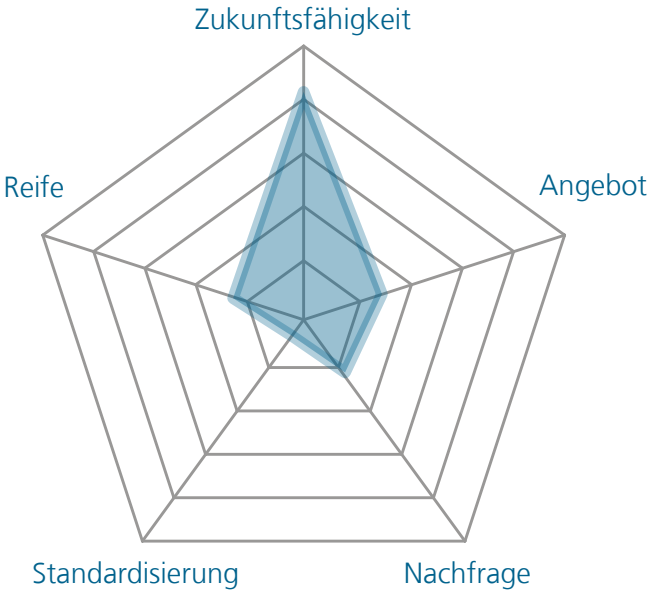


SICHERHEITSINFORMATIONS- UND EREIGNIS-MANAGEMENT (SIEM) TECHNOLOGIEN

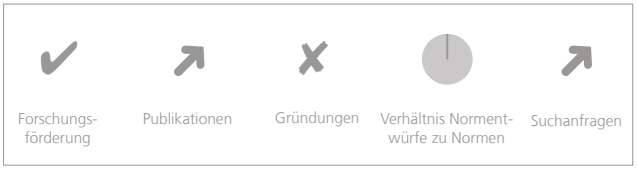
Sicherheitsinformations- und Ereignis-Management Technologien unterstützen das Sammeln und Auswerten von sicherheitsrelevanten Informationen aus verschiedenen Geräten, Netzen, Systemen oder Anwendungen nach vorab definierten Kriterien. Werden Bedrohungen oder kritische Zustände erkannt, können in Echtzeit Alarmfunktionen aktiviert und geeignete Sicherheitsmaßnahmen initiiert werden. Die Zeitspanne zwischen Angriff und Abwehr soll so verkürzt werden. Durch Big Data Technologien, forensische Werkzeuge und fortschrittliche Sicherheitsanalysen werden SIEM Technologien für die Gefahrenerkennung und -abwehr ständig verbessert.



COMPLEX EVENT PROCESSING TECHNOLOGIEN

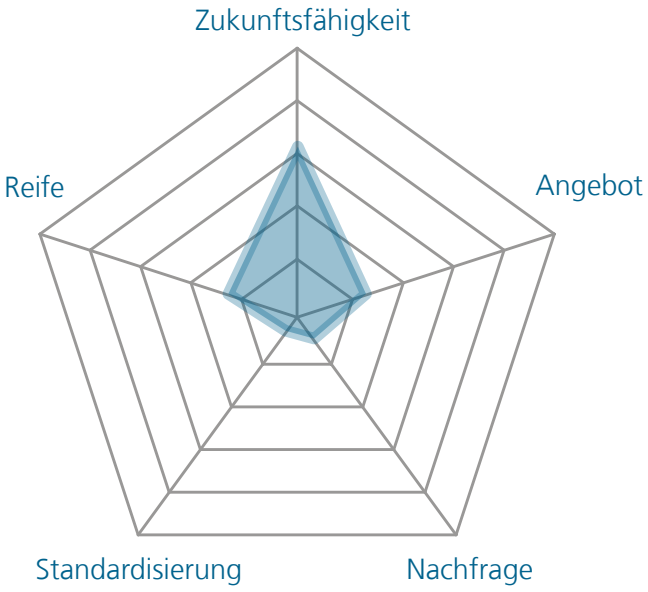


Complex Event Processing (deutsch: Verarbeitung komplexer Ereignisse) umfasst Methoden, Techniken und Werkzeuge für das kontinuierliche Sammeln, Analysieren und Verarbeiten von Ereignissen. Komplexe Ereignisse sind dabei das Resultat einer intelligenten Kombination und Korrelation mehrerer Ereignisse. Bestimmte Zustände oder Situationen lassen sich nur dann erkennen, wenn mehrere Ereignisse in Kombination auftreten. Um verschiedenartige Datenströme in Echtzeit zu verarbeiten und die Ereignisse zu extrahieren und zu analysieren, müssen von diesbezüglichen Systemen hohe Lasten verkraftet werden. Einsatzgebiete sind beispielsweise Netzwerküberwachung, öffentliche Sicherheit, Katastrophenschutz oder Energiemanagement.

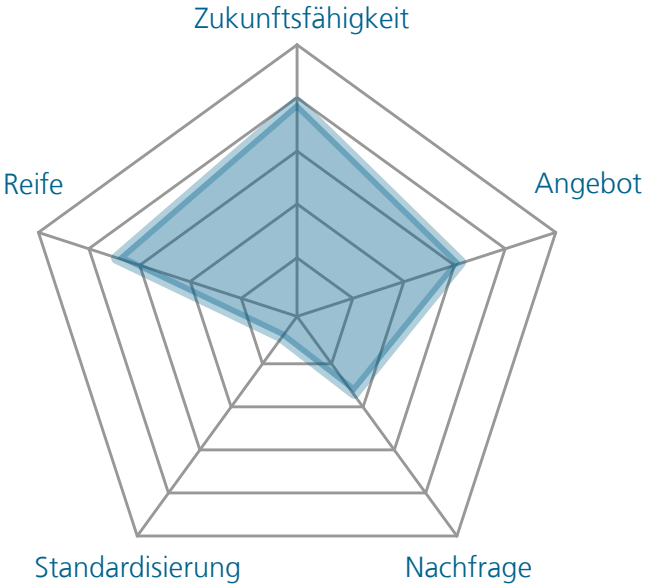


SECURITY-BY-CONTRACT / COMPLIANCE ÜBERWACHUNG

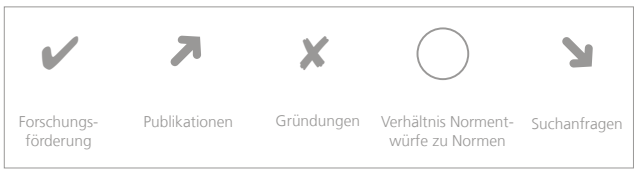
Security-by-Contract bezeichnet Verträge zwischen Dienstleistungserbringer und -nachfrager, die einen bestimmten Schutzbedarf definieren und den Sicherheitsleistungsumfang für die IT-Systeme garantieren. Ziel ist es, ein bestimmtes Sicherheitsniveau zu erreichen. Eine Vereinbarung von Sicherheitsniveaus anstatt konkreter Sicherheitsmaßnahmen erfordert und erlaubt dem Dienstleistungserbringer eine flexible und zeitnahe Anpassung an aktuelle Bedrohungen. Diese Vertragsvereinbarungen müssen überwacht und überprüft werden können. Compliance Überwachung dient der Überwachung der Einhaltung des vertraglich vereinbarten Sicherheitsniveaus sowie von Richtlinien, Vorschriften oder Gesetzen. Die abstrakte Beschreibung der erforderlichen Sicherheit basierend auf potenziellen Risiken sowie die Überprüfbarkeit des Sicherheitsniveaus in Form von geeigneten Sicherheitsmaßnahmen in Echtzeit sind bisher nur ansatzweise vorhanden.



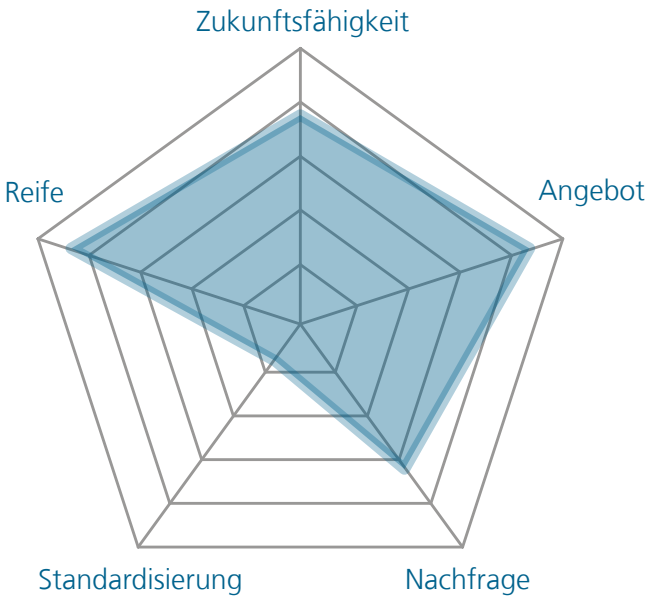
BOTNETZERKENNUNG



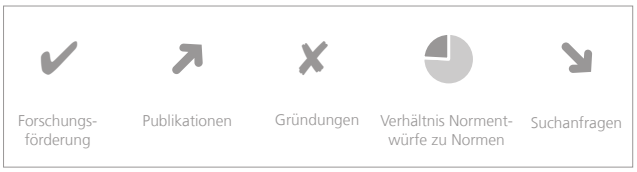
Botnetze sind gekaperte und vernetzte Rechner, die von Cyberkriminellen für Straftaten genutzt werden. Bot-Programme laufen in den infizierten Rechnern meist unbemerkt im Hintergrund. Die meisten Bots können von zentralen Servern bzw. Operatoren gesteuert werden. Sie werden beispielsweise für das Versenden von Spam, DDos-Attacken oder Phishing genutzt. Verbesserte Erkennungsmaßnahmen sind für Betroffene auch zukünftig erforderlich.



INTRUSION DETECTION SYSTEME (IDS) UND INTRUSION PREVENTION SYSTEME (IPS)

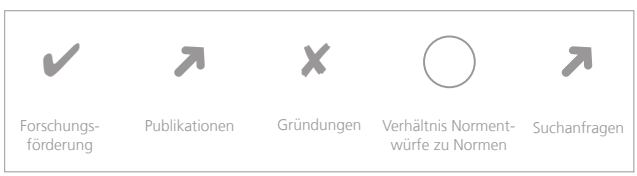


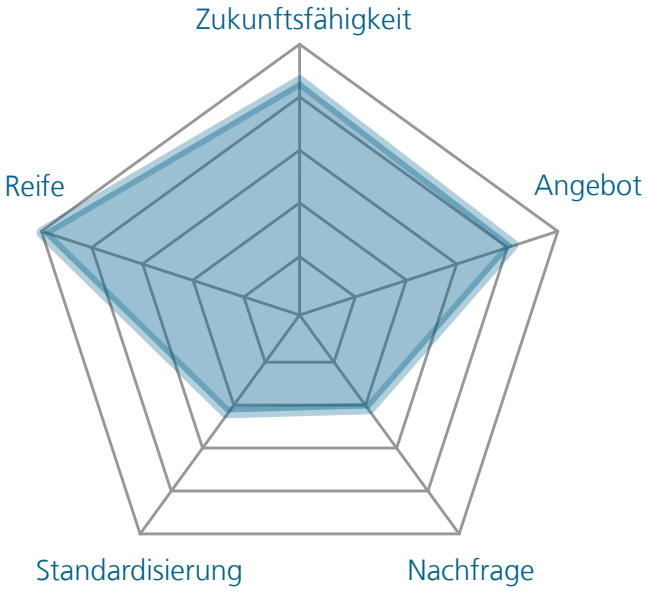
Intrusion Detection und Intrusion Prevention Systeme sind Werkzeuge, die IT-Systeme oder Netze aktiv überwachen. Das Ziel ist es, Ereignisse herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten (englisch intrusion: »Eindringen«). Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Die Verfahren basieren auf Mustererkennung, um ein Abweichen von einem Normalzustand zu signalisieren. Mit heuristischen Methoden sollen auch bisher unbekannte Angriffe erkannt werden. Während IDS Angriffe nur erkennen, sollen IPS diese auch abwehren bzw. verhindern.



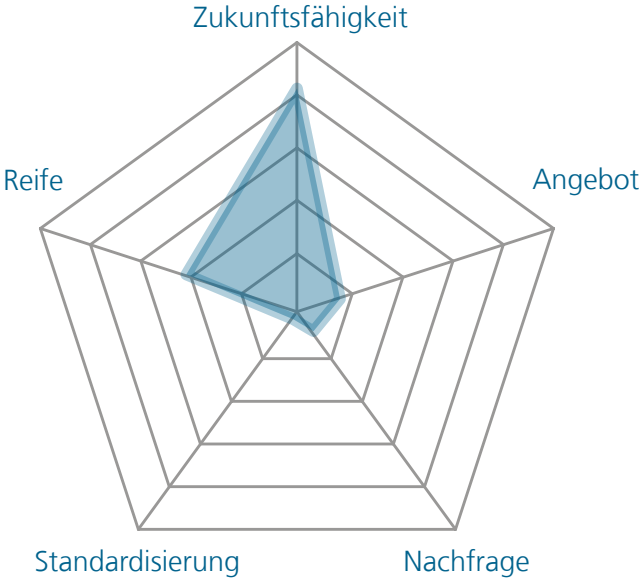
SCHWACHSTELLENANALYSE / VULNERABILITY DETECTION

Schwachstellen (englisch: vulnerability) sind Fehler eines IT-Systems oder einer Organisation, durch die diese für Bedrohungen anfällig werden. Eine Bedrohung oder eine Schwachstelle allein reichen jedoch nicht aus, um die Sicherheit eines Systems zu gefährden. Eine Gefährdung für das angegriffene System besteht nur dann, wenn eine Bedrohung auf eine existierende Schwachstelle trifft. Die Ursachen für Schwachstellen sind vielseitig und können in der Konzeption, Implementierung oder auch im Betrieb liegen und umfassen ebenfalls Design- oder Konstruktionsfehler, menschliches Fehlverhalten oder ungenügende Standortsicherheit. Schwachstellenanalysen dienen dazu, diese Fehler systematisch zu finden, um Bedrohungen und Angriffsszenarien abzuwenden.





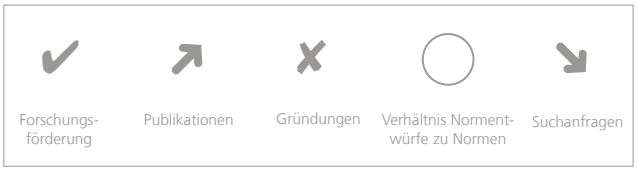
ADVANCED PERSISTENT THREAT (APT) ERKENNUNG UND ANALYSE

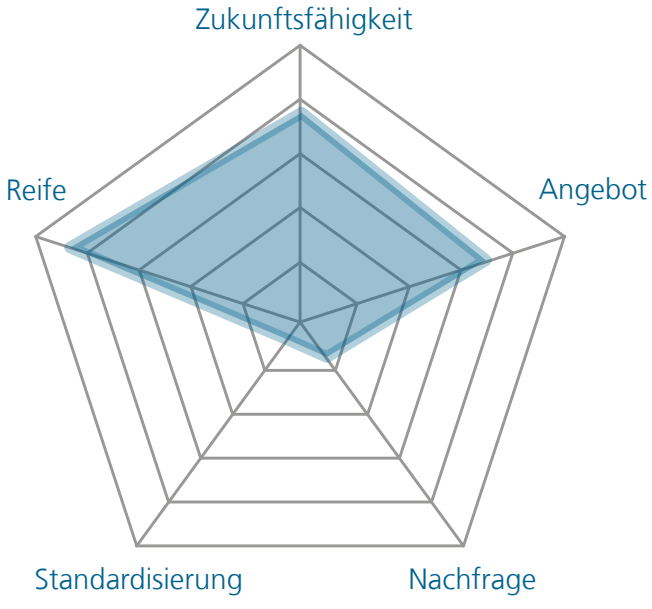


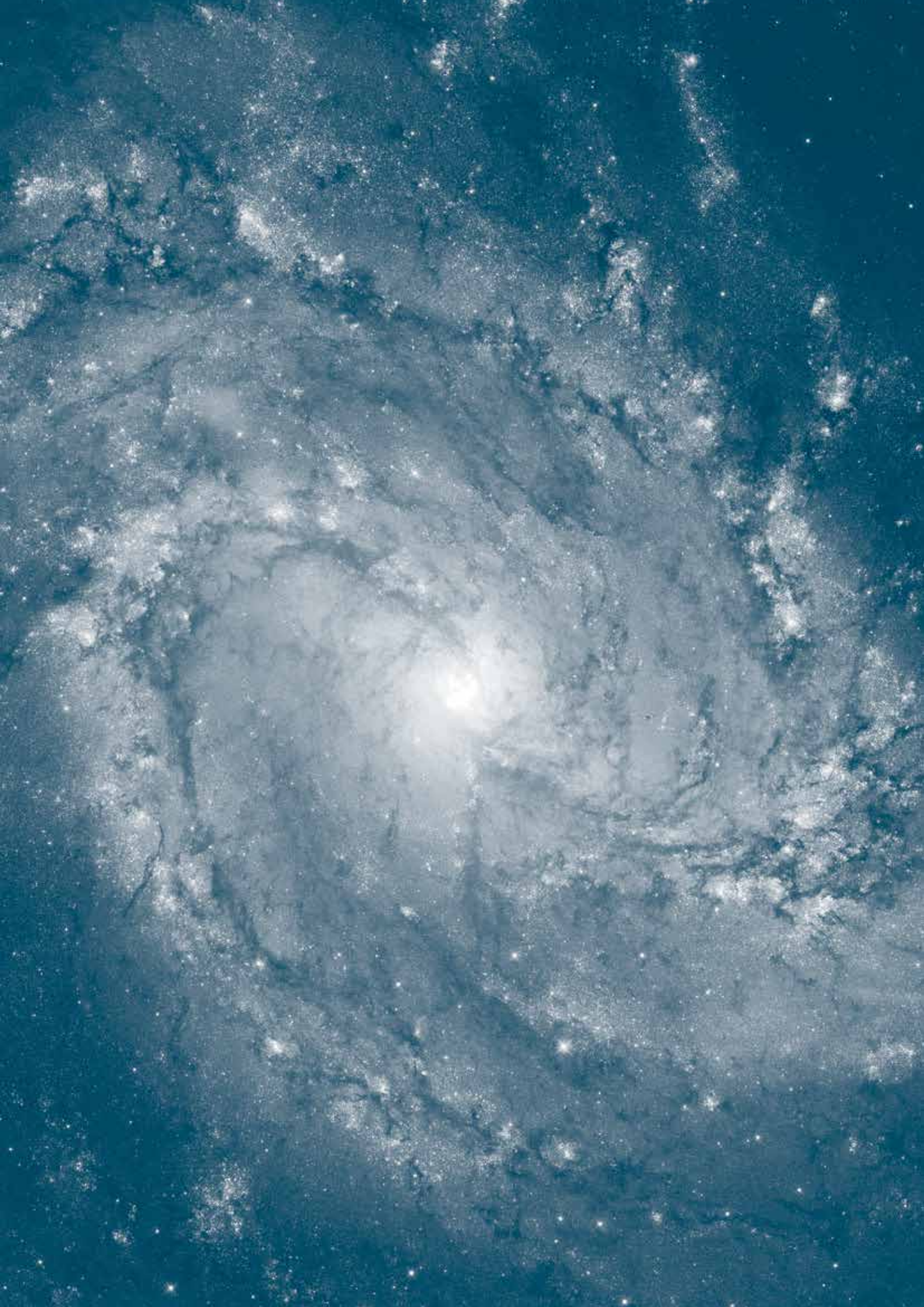
Advanced Persistent Threats sind komplexe und zielgerichtete Angriffe auf ein oder wenige Opfer. Diese Angriffe werden vom Angreifer akribisch und mit aufwändiger Spezialsoftware vorbereitet und dauern lange an. APTs sollen möglichst unentdeckt bleiben, um über einen längeren Zeitraum Daten auszuspähen oder anderen Schaden zu verursachen. Ziele dieser Angriffe sind kritische IT-Infrastrukturen sowie vertrauliche Daten von Behörden und Unternehmen aller Branchen. Aufgrund des hohen Schadenpotenzials sind die Erkennung und Analyse dieser Angriffe zwingend erforderlich, gestalten sich jedoch sehr schwierig. Nur das Sammeln, Analysieren und Korrelieren von Sicherheitsinformationen aus verschiedenen Quellen kann Hinweise zur Erkennung geben.

HONEYNET

Honeypots simulieren Schwachstellen in IT-Netzen oder Anwendungen, ohne dabei das System zu gefährden. Sie sollen Hacker anziehen bzw. vom eigentlichen Ziel wegleiten, so wie Bären mit einem Honigtopf sowohl abgelenkt als auch in eine Falle gelockt werden können. Werden mehrere Honeypots zu einer Infrastruktur verbunden, wird das als Honeynet bezeichnet. Honeynets sollen umfangreiche Informationen über Angriffsmuster und Angreiferverhalten liefern, um die Sicherheit stetig verbessern zu können.

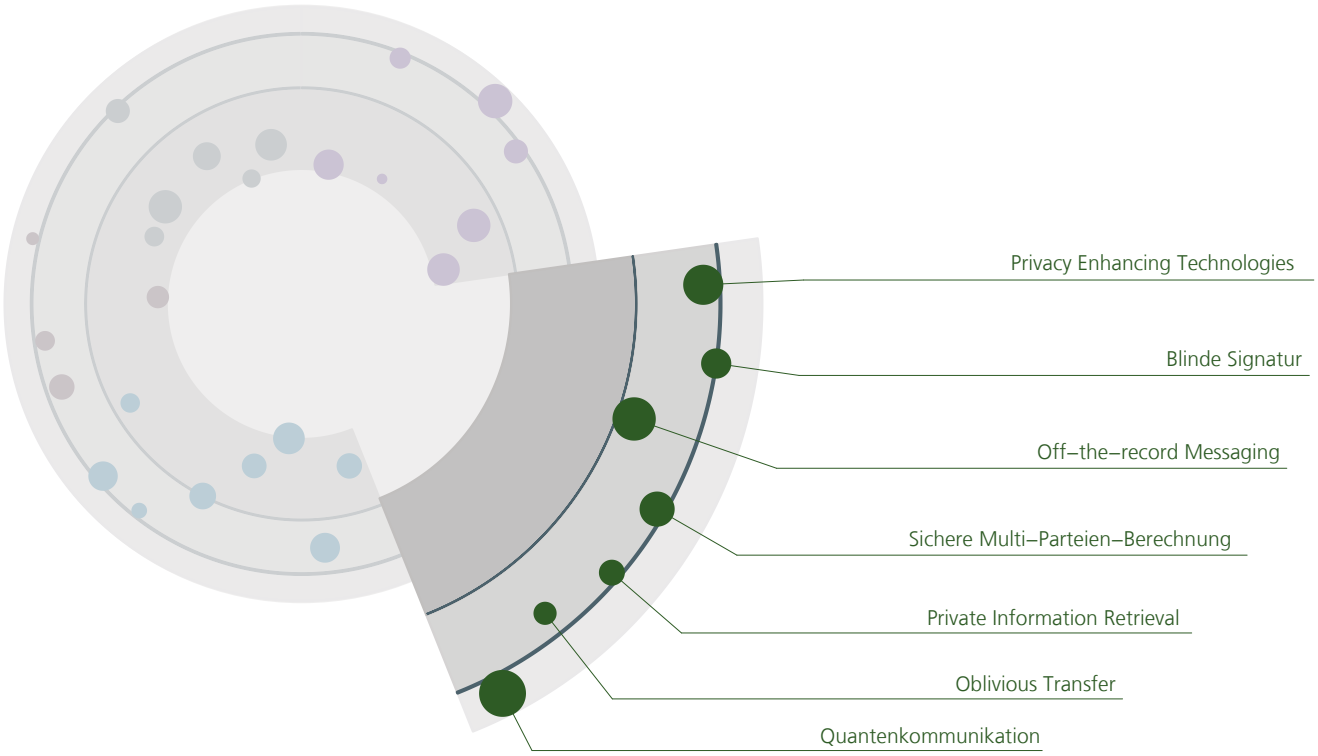






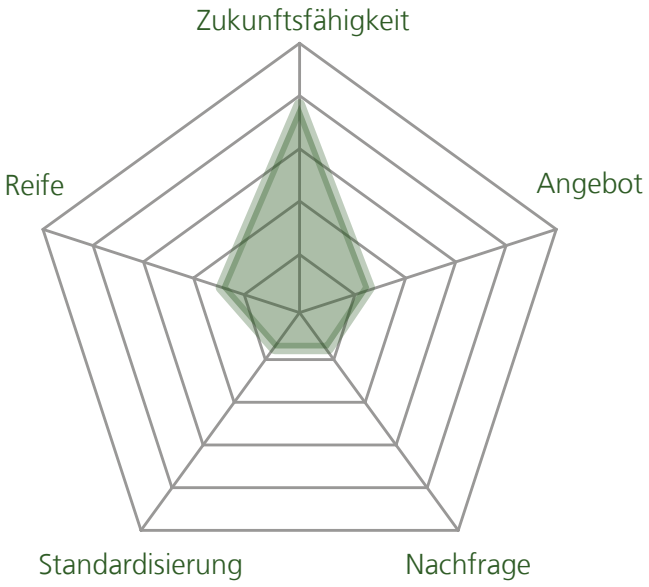
PRIVATHEIT UND DATENSCHUTZ

Privatheit und Datenschutz gewinnen im Zeitalter von Big Data, Cloud Computing und Social Media zunehmend an Bedeutung und müssen mit technischen Mitteln ermöglicht und unterstützt werden.

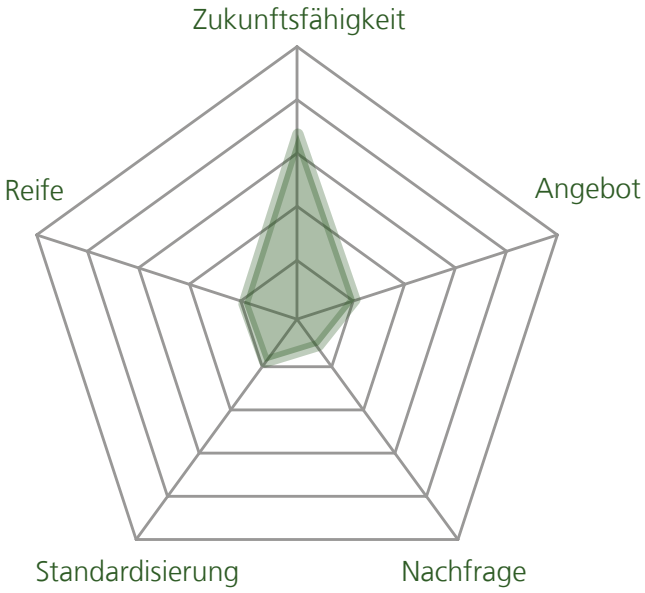


PRIVACY ENHANCING TECHNOLOGIES (PETs)

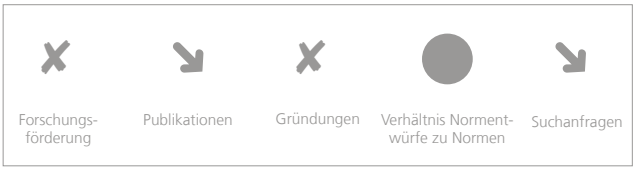
Privacy Enhancing Technologies ist ein Sammelbegriff für Technologien zum Schutz der Privatsphäre. Dazu gehören Technologien zur Anonymisierung bzw. Pseudonymisierung von Identitäten, kryptographische Ansätze zum Schutz sensitiver Daten, Techniken zur expliziten Einwilligung von Nutzern, Verhinderung ungewollter Nachverfolgung, Transparenz und Kontrolle der eigenen Daten, der digitale Radiergummi, Datensparsamkeit, Anonymisierung von offenen Daten, vertrauliche Kommunikation und weitere. Die wesentlichen Ziele sind, so wenig wie nötig persönliche Daten zu sammeln und die Datensicherheit, Zweckbindung und Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten sicherzustellen.



BLINDE SIGNATUR

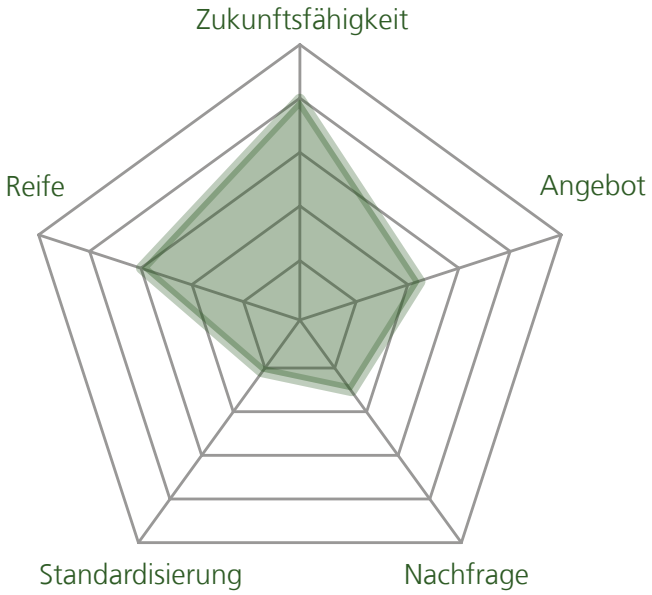


Blinde Signaturen sind eine Variante der digitalen Signatur, bei der ein Unterzeichner ein Dokument unterzeichnet, dessen Inhalt er nicht kennt. Die Unterschrift bestätigt somit nicht den Dokumenteninhalt sondern dessen Echtheit. Blinde Signaturen unterstützen Privatheit und Anonymität, da sie keine Rückschlüsse auf denjenigen zulassen, der das signierte Dokument verwendet. Einsatzmöglichkeiten sind beispielsweise elektronisches Bargeld, bei der die Bank nicht wissen soll was jemand wo gekauft hat, aber trotzdem die Echtheit des Geldes bestätigt. Ebenfalls sind blinde Signaturen für elektronische Wahlen sinnvoll, da geheim bleiben muss, wer wie gewählt hat, aber die Gültigkeit des Wahlzettels bestätigt wird.

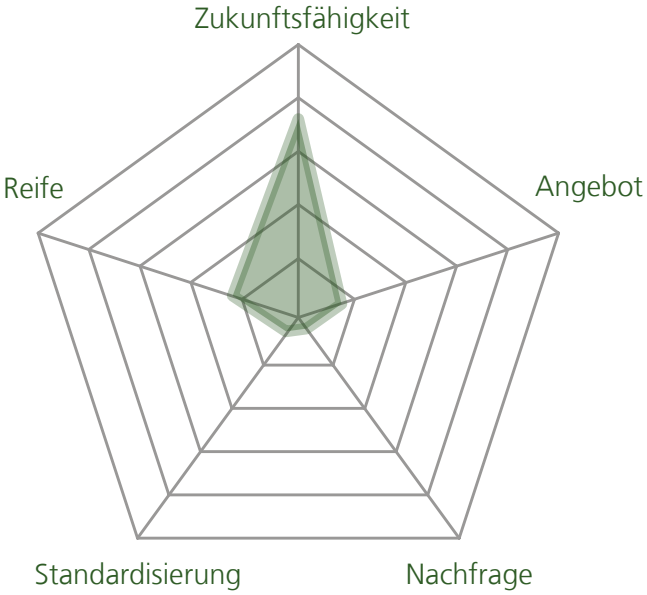


OFF-THE-RECORD (OTR) MESSAGING

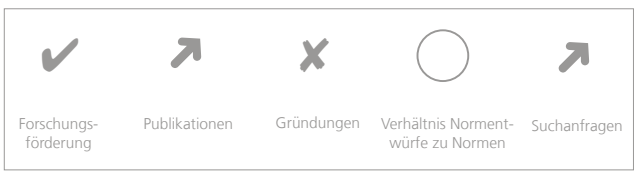
Off-the-Record Messaging ist ein Protokoll zur Verschlüsselung von Instant Messaging Nachrichten. Ziel ist es, sein Gegenüber zu authentifizieren und die Kommunikation vertraulich zu gestalten. Im Nachhinein können die ausgetauschten Nachrichten jedoch nicht mehr als authentisch nachgewiesen werden. Verwendet werden kurzlebige Sitzungsschlüssel; daher kann später nicht mehr festgestellt werden, ob ein bestimmter Schlüssel von einer bestimmten Person genutzt wurde.



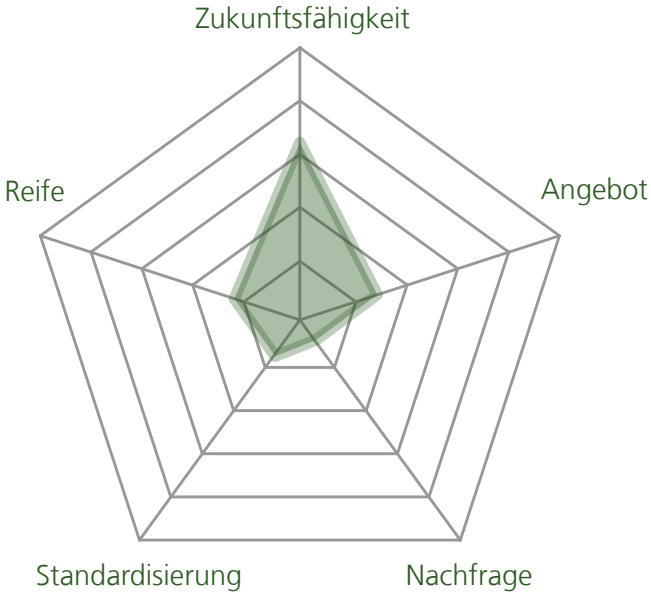
SICHERE MULTI-PARTEIEN-BERECHNUNG



Sichere Multi-Parteien-Berechnung bezeichnet ein privatheitunterstützendes, kryptographisches Protokoll, bei der gemeinsame Berechnungen auf geheimen Eingaben jeder Partei durchgeführt werden können und die Geheimnisse trotzdem erhalten bleiben. Ursprung ist das sogenannte Millionärsproblem, bei dem zwei sich gegenseitig misstrauende Millionäre herausfinden können, wer von ihnen reicher ist, ohne dass sie sich ihren Besitz gegenseitig offenlegen müssen. Da sensitive Daten bei der sicheren Multi-Parteien-Berechnung erhalten bleiben, kommen als Anwendungsgebiete beispielsweise Onlineauktionen oder Onlinewahlen in Betracht.



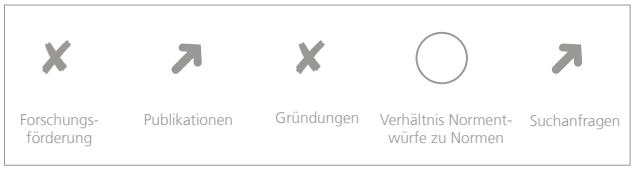
PRIVATE INFORMATION RETRIEVAL

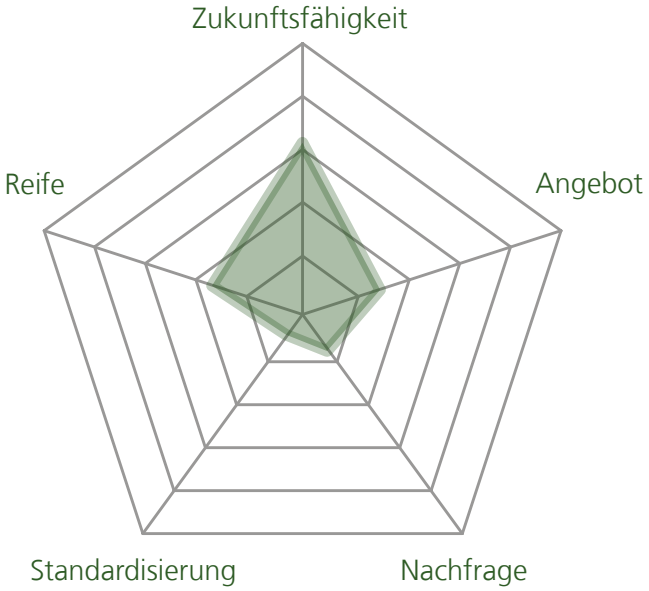


Private Information Retrieval ist ein kryptographisches Verfahren, bei dem Datenbankanfragen gestellt werden können, ohne dass die Datenbank bzw. der Datenbank-Administrator Kenntnis über den Inhalt der Anfrage erhält. So wird die Privatheit des Anfragenden unterstützt, auch wenn er öffentliche Datenbanken benutzt. Die Anfragen können daher auch nicht miteinander verknüpft werden, um die Interessen des Anfragenden zu ermitteln.

OBLIVIOUS TRANSFER

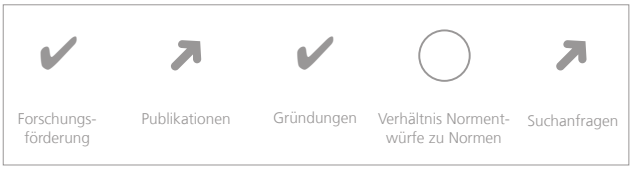
Oblivious Transfer ist ein kryptographisches 2-Parteien-Protokoll, bei dem ein Sender aus einer Menge von Informationen einen bestimmten Teil zu einem Empfänger überträgt, jedoch der Sender nicht weiß, welchen Teil er gesendet hat. Varianten des Protokolls gewährleisten so den Austausch von Geheimnissen, ohne dass eine neutrale dritte Partei eingeschaltet werden muss. Jeder erfährt das Geheimnis des anderen zur gleichen Zeit. Ein Anwendungsbereich ist das Unterzeichnen von Verträgen. Wollte man bisher sichergehen, dass beide Parteien einen Vertrag unterzeichnen, der für den jeweils Unterschreibenden sofort gültig wird, wurde beispielsweise ein Notar eingeschaltet. Mit Oblivious Transfer ist dies auch ohne die neutrale dritte Partei elektronisch möglich.

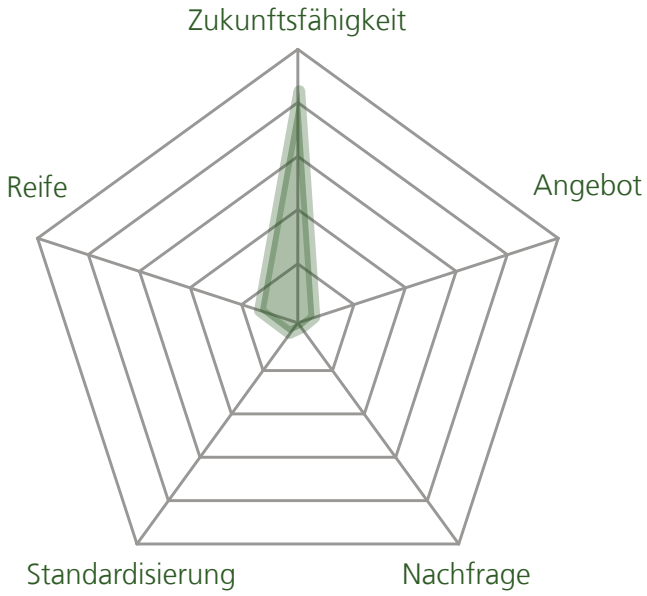


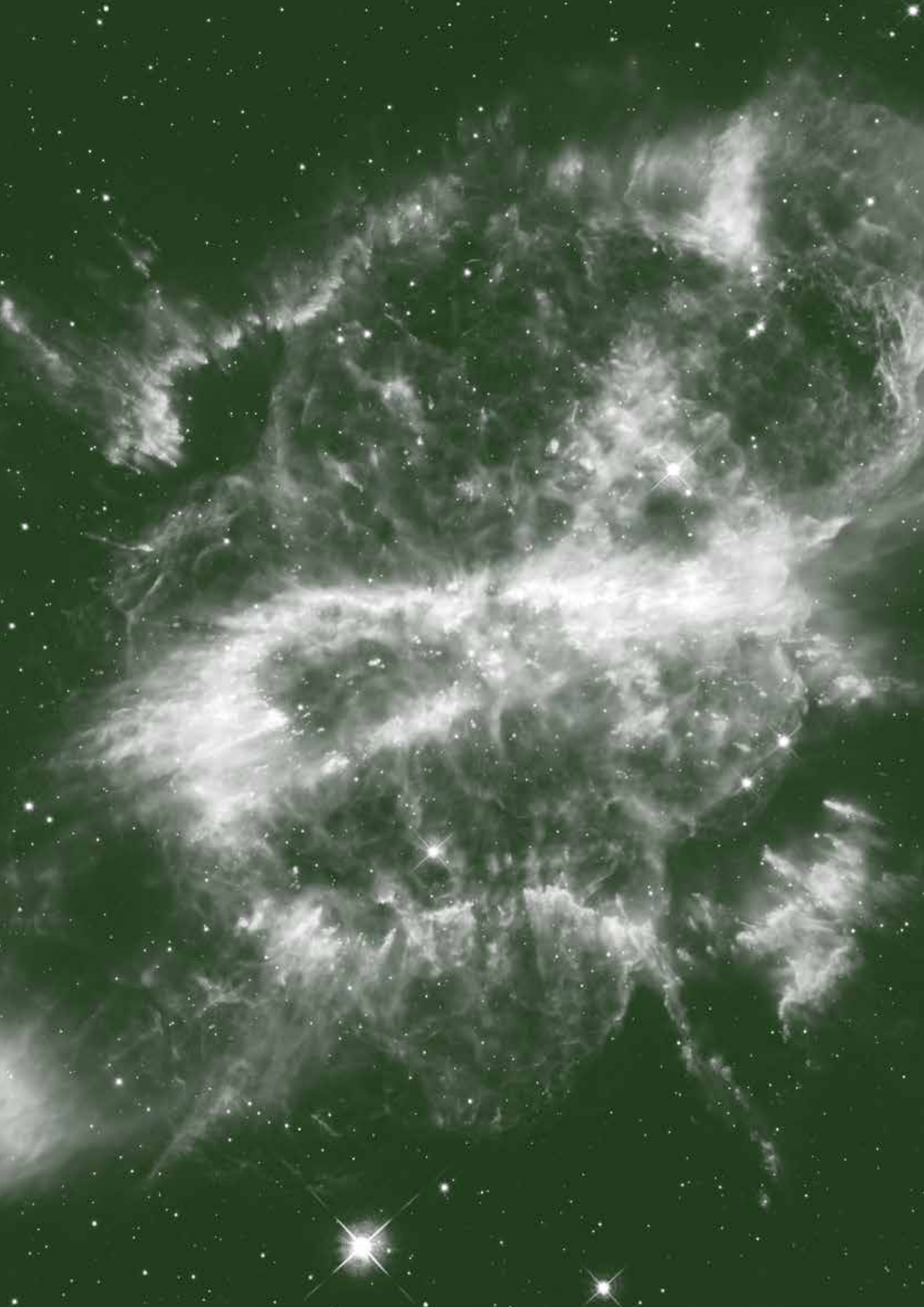


QUANTENKOMMUNIKATION

Die Datenübertragung durch einzelne Lichtteilchen wird als Quantenkommunikation bezeichnet. Eine Besonderheit gegenüber normaler Kommunikation ist, dass sich ein Quantenzustand von einem Ort zu einem anderen ohne ein physikalisches Medium übertragen lässt. Das wird auch Quantenteleportation genannt. Zwei Quanten werden zu einem gemeinsamen quantenphysikalischen Zustand verschränkt. Auch wenn sie getrennt werden, bleiben sie über große Strecken miteinander verbunden. Albert Einstein hatte den Effekt als spukhafte Fernwirkung bezeichnet. Zukünftige Einsatzbereiche sind abhörsichere, extrem schnelle Netzwerke.

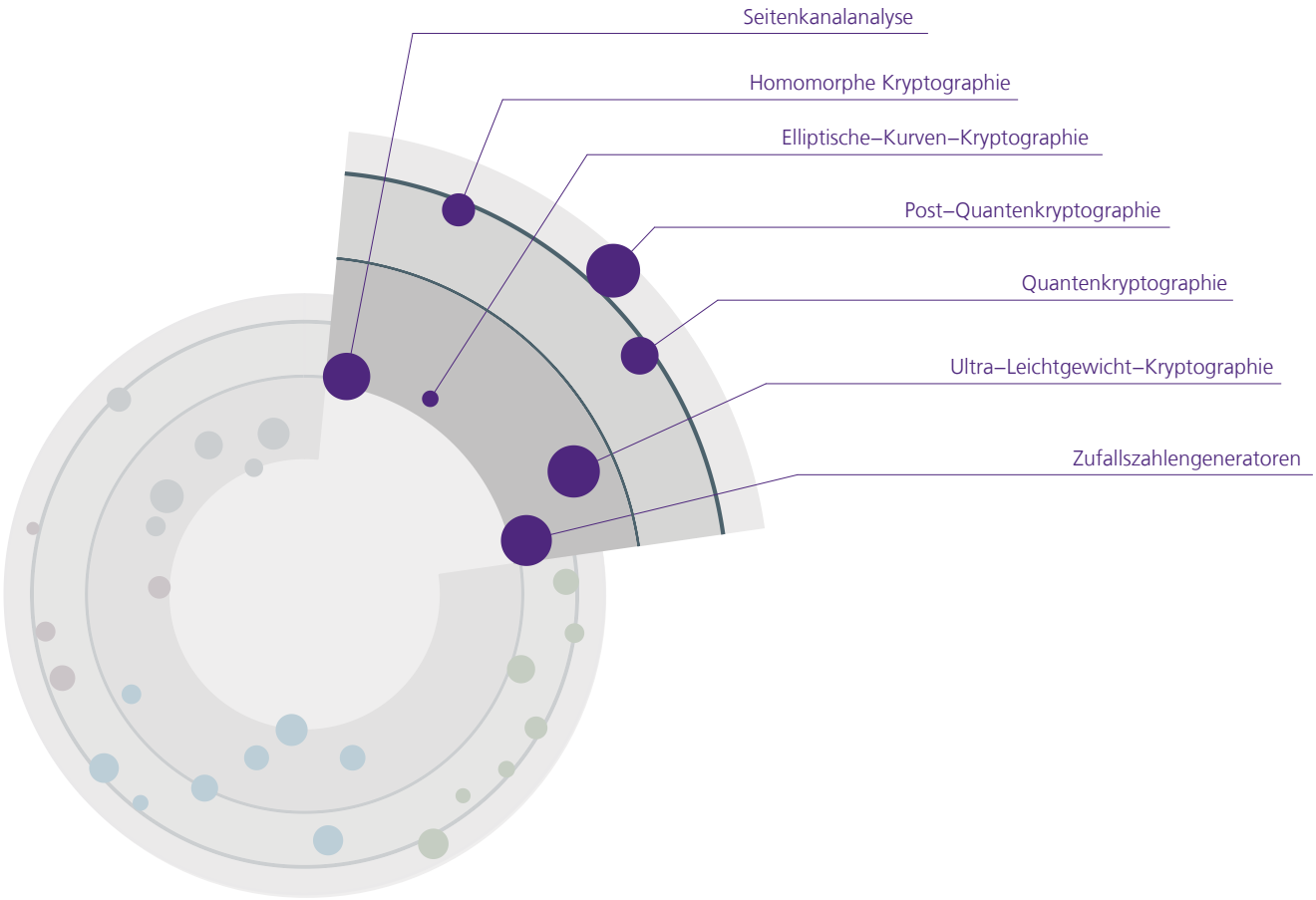






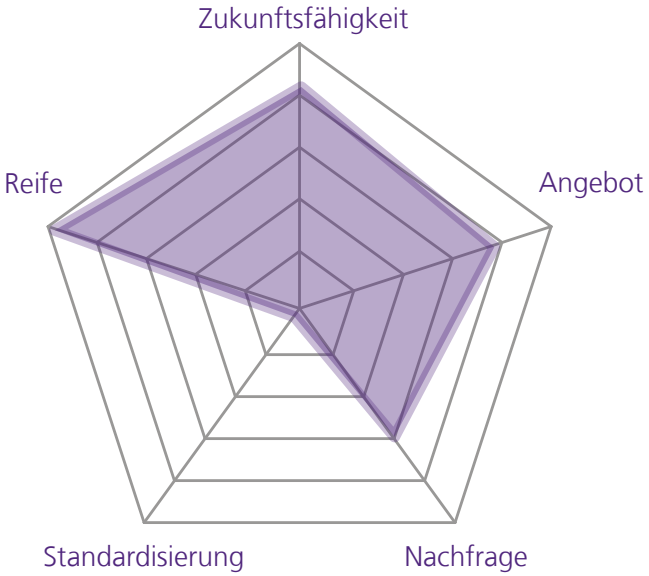
KRYPTOGRAPHIE

Kryptographie umfasst Verfahren zur Verschlüsselung von Daten, um Vertraulichkeit und Integrität zu gewährleisten.

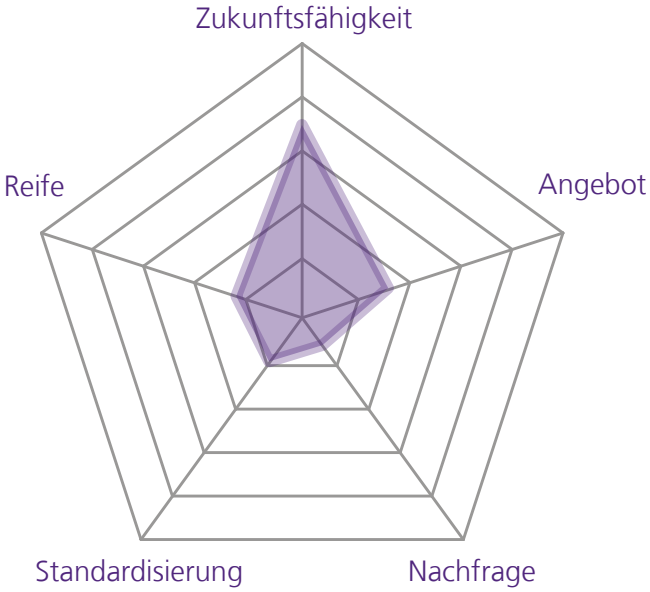


SEITENKANALANALYSE

Seitenkanalangriffe sind Angriffe, die nicht auf das kryptographische Verfahren selbst, sondern auf die physische Implementierung eines Kryptosystems wie beispielsweise Smartcards oder Sicherheitstoken zielen. Genutzt werden für diese Angriffe messbare Daten wie Zeit, Energieverbrauch des Prozessors, elektromagnetische Abstrahlung oder akustische Geräusche. Analysiert man diese, werden gegebenenfalls geheime Schlüssel extrahiert, d. h. es besteht eine universelle Gefahr der Kompromittierung für diese kryptographischen Geräte. Seitenkanalanalyse ist daher Bestandteil der Schwachstellenanalyse in der Common Criteria Zertifizierung von Chipkarten und ähnlichen Geräten.



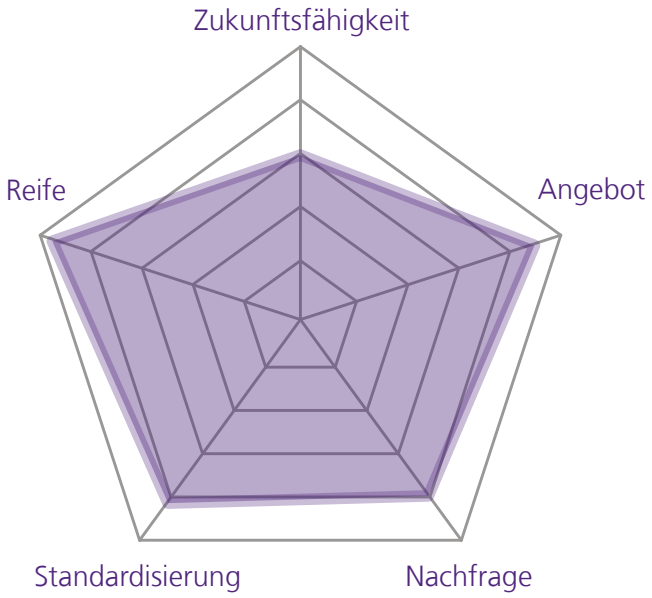
HOMOMORPHE KRYPTOGRAPHIE



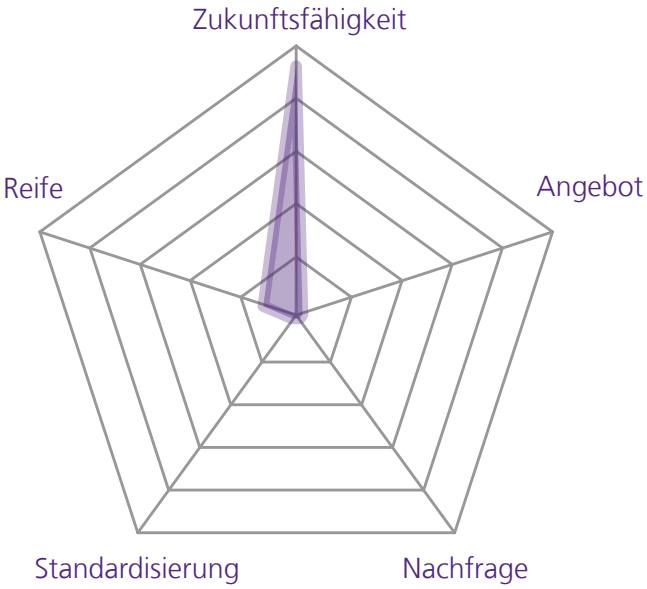
Homomorphe Kryptographie erlaubt Berechnungen auf verschlüsselten Daten, ohne dass diese entschlüsselt werden müssen. Insbesondere beim Cloud-Computing verspricht man sich einen großen Gewinn an Privatheit. Verschlüsselte Daten werden in einer Cloud abgelegt. Dort können sie durchsucht oder verarbeitet werden ohne sie zu entschlüsseln. Das Ergebnis wird verschlüsselt zurück gesendet. Der Cloud-Anbieter kennt weder die Daten noch die Ergebnisse. Bisher ist homomorphe Kryptographie allerdings noch sehr rechenintensiv und viele Teilbereiche wie Einstellungen oder Rechnerarchitektur sind noch wenig erforscht.

ELLIPTISCHE-KURVEN-KRYPTOGRAPHIE

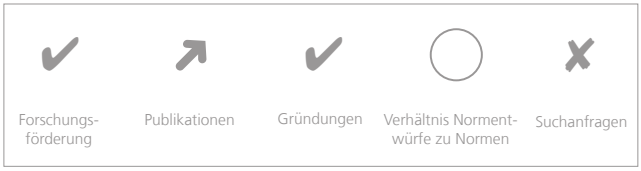
Elliptische Kurven sind mathematische Strukturen, die sich für kryptographische Verfahren nutzen lassen. Vorteilhaft gegenüber herkömmlichen Kryptoverfahren sind die kürzeren Schlüssellängen, die höhere Geschwindigkeit und geringere Speicheranforderungen. Einsatzgebiete sind daher Geräte, bei denen Speicher- oder Rechenkapazität knapp sind, wie beispielsweise bei Smartcards. Elliptische-Kurven-Kryptographie wird heute für den Zugriffsschutz auf Chips von Reisepässen vieler europäischer Staaten und des deutschen Personalausweises verwendet. Elliptische Kurven treten in verschiedenen Varianten auf, wobei einige als fehleranfällig oder unsicher gelten. Daher werden diese auch weiterhin erforscht.



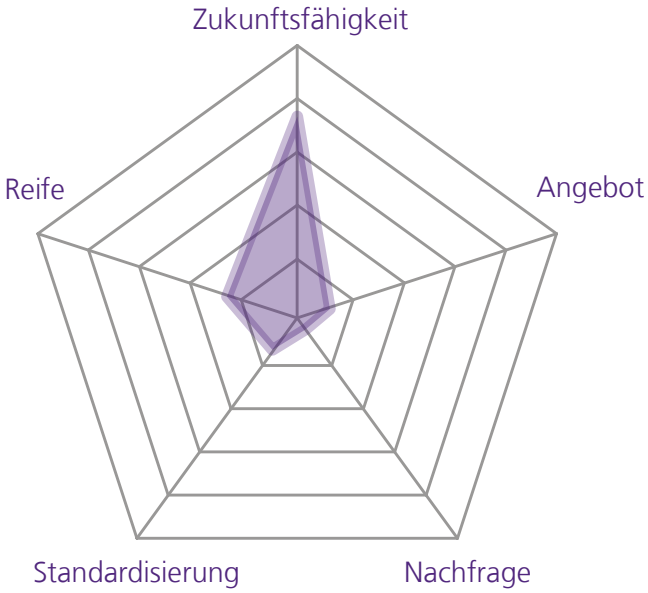
POST-QUANTEN-KRYPTOGRAPHIE



Gegenwärtig geht man davon aus, dass zukünftige Quantencomputer mit Hilfe von physikalischen Effekten bestimmte mathematische Probleme lösen könnten, an denen heutige Computer scheitern. Insbesondere könnte das kryptographische Public-Key-Verfahren betreffen, d. h. Verschlüsselung und Authentisierung wären gefährdet. Das Forschungsgebiet der Post-Quanten-Kryptographie beschäftigt sich daher mit kryptographischen Verfahren, die auch mit Quantencomputern nicht gebrochen werden können.

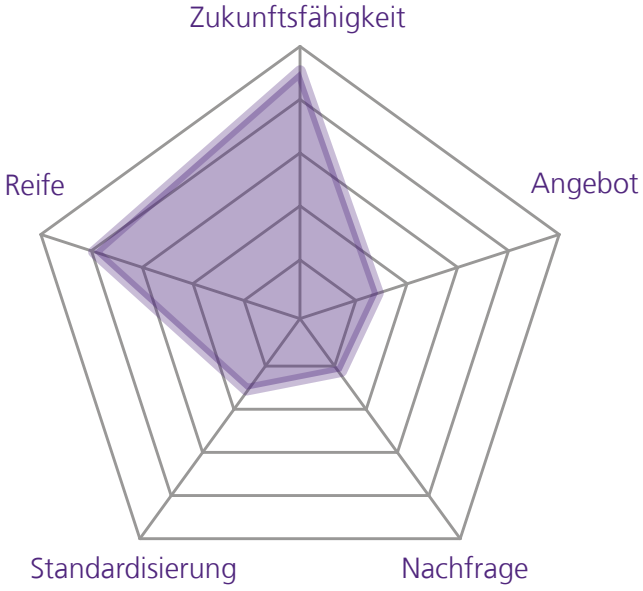


QUANTENKRYPTOGRAPHIE



Quantenkryptographie verwendet quantenmechanische Effekte (üblicherweise Lichtquanten) als Bestandteil kryptographischer Verfahren oder zur Kryptoanalyse. Quanten ändern ihre Eigenschaften, wenn sie einer Messung unterzogen bzw. beobachtet werden. So können im Gegensatz zu herkömmlichen kryptographischen Verfahren beispielsweise Angreifer entdeckt werden, die den Kommunikationskanal belauschen, weil deren Messungen die Daten beeinflussen. Demzufolge können zwei Kommunikationspartner feststellen, ob ein zwischen ihnen übertragener Verschlüsselungsschlüssel abgefangen wurde. Derzeit ist der technische Aufwand für Quantenkryptographie relativ hoch und die Länge der Übertragungsstrecken noch eingeschränkt.

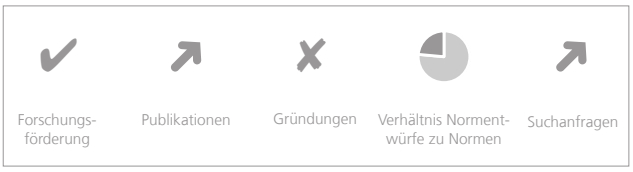
ULTRA-LEICHTGEWICHT-KRYPTOGRAPHIE / KRYPTOGRAPHIE FÜR RESSOURCENARME GERÄTE

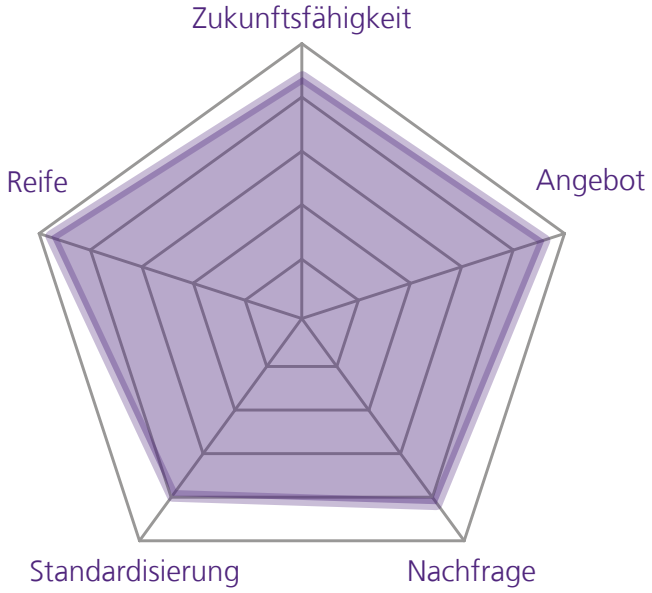


Ressourcenbeschränkte oder ressourcenarme Systeme, wie RFID Tags, eingebettete Systeme oder Sensoren, benötigen kryptographische Verfahren, die wenig Anforderungen an Prozessorleistung und Speicherplatz stellen und gleichzeitig schnell und ausreichend sicher sind. Mögliche Einsatzgebiete sind das Internet der Dinge für verschiedene Gegenstände des alltäglichen Lebens zur Sicherung von Vertraulichkeit, aber auch das Rechtemanagement für Autorisierungsentscheidungen.

ZUFALLSZAHLENGENERATOREN

Sichere Zufallszahlen bilden das Fundament der Kryptographie. Kryptographische Verfahren benötigen starke Zufallszahlen, d. h. Zufallszahlen, die nicht vorhersagbar sein dürfen. Zufallszahlengeneratoren erzeugen diese. Ein sicherer Zufallszahlengenerator benutzt dafür nicht-deterministische Quellen, wie physikalische Prozesse (z. B. thermisches Rauschen). Einsatzgebiete sind u. a. die Schlüsselerzeugung für symmetrische und asymmetrische Verschlüsselungsverfahren, Authentifikationsprotokolle und digitale Signaturverfahren. Die Erzeugung von Zufallszahlen in deterministischen Maschinen wie Computern (d. h. eine konkrete Eingabe liefert immer das gleiche Ergebnis) bleibt eine Herausforderung.





POLITISCHE HANDLUNGSFELDER

Die Technologietrends unterscheiden sich in Bezug auf die bewerteten Kriterien mitunter deutlich voneinander. So finden sich viel beachtete Trends mit großen Erwartungen an ihre weitere Entwicklung ebenso, wie Technologien, deren hoher Reifegrad bei vergleichsweise geringer Zukunftsfähigkeit darauf hindeutet, dass sie ihren Zenit aktuell bereits überschreiten. Diese Unterschiede verweisen auch auf politische Gestaltungsmöglichkeiten, um IT-Sicherheitstechnologien voranzubringen. Bezogen auf die fünf Bewertungskriterien ergeben sich Handlungsfelder, die je nach Technologie und Anwendungsfeld unterschiedlich intensiv verfolgt werden können.

Zukunftsfähigkeit
Um die Zukunftsfähigkeit einer Technologie langfristig zu gewährleisten, sind Investitionen in die Grundlagenforschung erforderlich. Durch Forschungspolitik kann diese gezielt gefördert werden.

Handlungsfeld
– Förderung der Grundlagenforschung

Reife
Wenn einer Technologie eine hohe Zukunftsfähigkeit zugeschrieben wird, die Lösungen jedoch noch keine hinreichende technologische Reife erlangt haben, sind anwendungsorientierte Förderkonzepte und andere Instrumente der Innovationsförderung angeraten.

Handlungsfelder
– Förderung anwendungsorientierter Forschung
– Anwendung gezielter innovationspolitischer Instrumente wie beispielsweise vorkommerzielle Auftragsvergabe

Angebot
Innovationspolitische Instrumente können auch dann angeraten sein, wenn marktfähige Lösungen nicht oder kaum verfügbar sind. Ferner können eher industriepolitische Maßnahmen zielführend sein, wenn eine Ausweitung des Angebots an konkreten Umsetzungsschwierigkeiten in der Branche scheitert.

Handlungsfelder
– Wirtschafts- und Gründungsförderung
– Investitionsanreize schaffen

Nachfrage
Werden erwünschte Sicherheitstechnologien nur wenig nachgefragt, kann der öffentliche Sektor sowohl direkt als auch indirekt auf eine Änderung hinwirken. Zum einen tritt der öffentliche Sektor selbst als großer Nachfrager am Markt auf. Durch eine stärkere Berücksichtigung bei öffentlichen Beschaffungsvorgängen kann die Nachfrage gesteigert werden. Zum anderen wirken erhöhte Sicherheitsanforderungen auf die private Nachfrage.

Handlungsfelder
– Berücksichtigung im öffentlichen Einkauf
– Gezielte Regulierung der Sicherheitsanforderungen

Standardisierung
Standardisierung erweist sich als Schwachpunkt vieler der betrachteten Technologietrends. Hier kann der öffentliche Sektor zum einen durch die Nutzung bestehender Standards von deren Vorzügen profitieren. Dies steigert zugleich die wirtschaftliche Bedeutung der Standardsetzung. Zum anderen kann er durch aktive Normungsarbeit besonders relevante Technologiefelder unterstützen und beeinflussen.

Handlungsfelder
– Bestehende Standards in die IT-Strategie einbeziehen
– Aktive Mitarbeit in der Normung

ANHANG A: METHODISCHE ANMERKUNGEN

Die Identifikation und Analyse der Technologietrends im Bereich der IT-Sicherheit erfolgte durch qualitative Methoden, die durch quantitative Analysen flankiert wurden. Den Kern bilden qualitative Bewertungen durch Expertinnen und Experten des Fraunhofer-Instituts für Offene Kommunikationssysteme, die durch Literaturarbeit inspiriert und durch quantitative Ergebnisse ergänzt wurden.

Die initiale Auswahl möglicherweise relevanter Trends erfolgte durch die Analyse einschlägiger Publikationen sowie der Forschungsprogramme auf Bundes- und EU-Ebene. Ergänzt durch Literaturrecherchen und die unten näher beschriebenen, quantitativen Indikatoren wurden diese Technologietrends in mehreren Experteninterviews kategorisiert und hinsichtlich ihrer Relevanz bewertet.

Im nächsten Schritt wurden die Trends mithilfe eines Online-Tools hinsichtlich jeder der fünf Dimensionen Zukunftsfähigkeit, Zeitraum bis zum Durchbruch, Angebot, Nachfrage und Standardisierung auf einer Skala von Null bis zehn bewertet. Für die Anwendungsbereiche Authentifizierung und Autorisierung, Netzwerk- und Systemsicherheit, Privatheit und Datenschutz und Kryptographie lagen nach Ende des Bewertungszeitraums für jeden Trend insgesamt sechs individuelle Einschätzungen vor, in der Kategorie Auditing und Monitoring lag die Zahl bei fünf. Um die Bewertung nicht durch Ausreißer zu verzerren, wurden bei vier gültigen Bewertungen diejenigen nicht in die Auswertung miteinbezogen, die um vier Punkte oder mehr von der nächsthöheren oder nächstniedrigeren Bewertung abwichen.

Diese Onlineerhebung wurde durch einen vorhergehenden und einen nachfolgenden Expertenworkshop gerahmt. Durch den vorhergehenden Expertenworkshops konnte ein gemeinsames Verständnis der zu bewertenden Technologietrends sowie der Bewertungskriterien erreicht werden. Der nachfolgende Workshop diente der Validierung der Ergebnisse. Hier wurden Abweichungen diskutiert und die vorläufigen Ergebnisse durch die quantitativen Indikatoren kontrastiert. Durch dieses Vorgehen wurde das gemeinsame Verständnis von Gegenstand und Bewertung geschärft und einzelne Ergebnisse konnten angepasst werden.

Die quantitativen Ergänzungen stützen sich auf Suchanfragen bei verschiedenen Datenbanken. Im Einzelnen wurden die nachfolgend beschriebenen Datenbanken für die fünf Indikatoren herangezogen:

Für die Daten aus den **Forschungsförderprogrammen** wurden auf EU-Ebene die beiden Forschungsprogramme FP7 und Horizont 2020 (Stand: November 2015) und auf Bundesebene alle Informatikprojekte der Deutschen Forschungsgemeinschaft (DFG) sowie alle IKT-Forschungsprojekte mit Sicherheitsbezug unter Förderung des Bundesministeriums für Bildung und Forschung (BMBF) analysiert. Hierbei wurden nur Forschungsprojekte mit Förderbeginn ab 2010 berücksichtigt.

Die Daten zu **wissenschaftlichen Publikationen** stammen aus der Datenbank Scopus. Es wurde eine Stichwortsuche durchgeführt, in der auch Synonyme und gängige Abkürzungen berücksichtigt wurden. Die Suchergebnisse wurden nach Erscheinungsdatum der Publikation kategorisiert. Dabei wurden alle Publikationen mit Erscheinungsdatum bis einschließlich 2009 sowie alle später erschienenen Publikationen zusammengefasst. Die Daten beziehen sich auf den Stand vom Dezember 2015. Der Vergleich der beiden Gruppen erlaubt Aussagen dazu, wie sich die Publikationstätigkeit zu einem Technologietrend entwickelt hat.

Die Existenz von **Gründungen** mit Bezug zu den jeweiligen Technologietrends wurde auf Basis der Daten der Crowdfunding-Plattformen Kickstarter und Indiegogo ermittelt. Dabei wurden alle Gründungen miteinbezogen, deren Finanzierung seit 2009 anvisiert wurde. Die Analyse umfasst somit nicht das gesamte Gründungsgeschehen, sondern nur die durch diese Plattformen erfassten, in der Regel sehr innovationsorientierten Gründungen.

Zur Ermittlung der Anzahl der **Normentwürfe und Normen** wurde die Datenbank des Deutschen Instituts für Normung e. V. (DIN) herangezogen. In ihr werden DIN-Normen, aber auch ISO-Normen, VDE-Normen oder technische Regeln und Normentwürfe aufgelistet. Die Anzahl der erfassten Normen und Entwürfe in der DIN-Datenbank mit Stand Januar 2016 wurden addiert. Basierend auf diesem Wert wurde das Verhältnis der Anzahl der Normen zur Anzahl der Entwürfe berechnet und abgebildet. Die Anzahl der Normen und Entwürfe korrespondiert mit der Einschätzung zum Standardisierungsgrad. Ist die Anzahl der Entwürfe im Verhältnis zur Anzahl der Normen sehr klein, kann ein Trend als weitgehend etabliert betrachtet wer-

DEN KERN DER ANALYSE BILDEN QUALITATIVE BEWERTUNGEN, DIE DURCH QUANTITATIVE ERGEBNISSE ERGÄNZT WERDEN.

den. Anders herum deutet ein hoher Anteil an Entwürfen auf eine große Dynamik des Technologietrends.

Für die **Suchanfragen** wurden Statistiken von Google Trends genutzt. Es wurden die monatlichen Durchschnittswerte der Suchanfragen für die Jahre 2009 und 2015 erfasst. Untersucht wurde dabei, wie sich der Durchschnittswert der monatlichen Suchanfragen von 2009 im Vergleich zu 2015 verändert hat. Bei sehr ähnlichen Durchschnittswerten für beide Jahre wird Konstanz der öffentlichen Aufmerksamkeit angenommen. Für einige sehr neue Trends liegen noch keine Statistiken vor.

Die Identifikation der relevanten Datenbankeinträge erfolgte über die jeweiligen Suchbegriffe, die in einigen Fällen durch Abkürzungen oder Synonyme ergänzt wurden. Angesichts der mitunter geringen Eindeutigkeit der begrifflichen Abgrenzung einzelner Technologietrends muss die Belastbarkeit dieser Analysen realistisch eingeschätzt werden. Die Indikatoren werden daher nur schematisch wiedergegeben: nach Vorhandensein (geförderte Forschungsprogramme und Gründungen), nach Tendenz der Nennungshäufigkeit (Publikationen und Suchanfragen) und nach Verhältnis von Normentwürfen zu Normen.

Verwendete Datenquellen:

Bundesregierung: »Förderkatalog«; http://foerderportal.bund.de/foekat/jsp/SucheAction.do?actionMode=searchreset; zuletzt abgerufen am: 06.04.2016.

Deutsche Forschungsgemeinschaft; http://www.dfg.de/gefoerderte_projekte/informationssysteme/index.html; zuletzt abgerufen am: 06.04.2016.

Deutsches Institut für Normung e.V.; http://www.din.de/de/meta/suche/; zuletzt abgerufen am: 06.04.2016.

Google Trends; https://www.google.com/trends/; zuletzt abgerufen am: 06.04.2016.

Indiegogo; https://www.indiegogo.com; zuletzt abgerufen am: 06.04.2016.

Kickstarter; https://www.kickstarter.com/; zuletzt abgerufen am: 06.04.2016.

Offenes Datenportal der Europäischen Union (2015): »CORDIS – EU research projects under FP7 (2007-2013)«; https://open-data.europa.eu/de/data/dataset/cordisfp7projects; zuletzt abgerufen am: 06.04.2016.

Offenes Datenportal der Europäischen Union (2015): »CORDIS – EU research projects under Horizon 2020 (2014-2020)«; https://open-data.europa.eu/de/data/dataset/cordis-h2020projects-under-horizon-2020-2014-2020; zuletzt abgerufen am: 06.04.2016.

Scopus; http://www.scopus.com/; zuletzt abgerufen am: 06.04.2016.

ANHANG B: QUELLENVERZEICHNIS

Anti-Botnet Beratungszentrum; https://www.botfrei.de/index.html; zuletzt abgerufen am: 06.04.2016.

Armknecht, Frederik; Sadeghi, Ahmad-Reza (2010): »Physikalische Fingerabdrücke gegen Produkt-Piraterie«; erschienen im Wissenschaftsmagazin der TU Darmstadt, Herbst 2010; https://www.tu-darmstadt.de/media/illustrationen/referat_kommunikation/publikationen_km/themaforschung/2010_02/Seiten_42_45.pdf; zuletzt abgerufen am: 06.04.2016.

Bauer, Curt (2016): »NFC – was ist das?«; 22.2.2016; http://praxistipps.chip.de/nfc-was-ist-das_12294; zuletzt abgerufen am: 06.04.2016.

Beutelspacher; Albrecht; Neumann, Heike B.; Schwarzpaul, Thomas (2009): »Kryptografie in Theorie und Praxis: Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld«; Vieweg+Teubner Verlag; ISBN 978-3-8348-0977-3.

Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter (2015): »Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge«; 8. Auflage; Springer Spektrum; ISBN 3834819271.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) (2010): »Cloud Computing – Was Entscheider wissen müssen«; https://www.bitkom.org/Publikationen/2010/Leitfaden/Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen/BITKOM-Leitfaden-Cloud-Computing-Was-Entscheider-wissen-muessen.pdf; zuletzt abgerufen am: 06.04.2016.

Böck, Hanno (2014): »Post-Quanten-Kryptographie: Sicher trotz Quantencomputern«; 03.10.2014; http://www.golem.de/news/post-quanten-kryptographie-sicher-trotz-quanten-computern-1410-109617.html; zuletzt abgerufen am: 06.04.2016.

Bundesamt für Sicherheit in der Informationstechnik (BSI): »Einführung in die technischen Grundlagen der biometrischen Authentisierung«; https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/TechnischeGrundlagen/technischegrundlagen_node.html; zuletzt abgerufen am: 06.04.2016.

Bundesamt für Sicherheit in der Informationstechnik (BSI): »IT-Grundschutz, Glossar und Begriffsdefinitionen«; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html; zuletzt abgerufen am: 06.04.2016.

Engels, Daniel; Fan, Xinxin; Gong, Guang; Hu, Honggang; Smith, Eric M. (2010): »Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices«; erschienen in Financial Cryptography and Data Security, Volume 6054, Lecture Notes in Computer Science, S. 3-18.

Europäische Kommission (2013): »Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace«; https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security; zuletzt abgerufen am: 09.03.2016.

Europäische Kommission (2013): »Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union«; https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security; zuletzt abgerufen am: 09.03.2016.

European Union Agency for Network and Information Security (ENISA) (2016): »ENISA Threat Landscape 2015«; https://www.enisa.europa.eu/publications/etl2015/; zuletzt abgerufen am: 12.02.2016.

European Union Agency for Network and Information Security (ENISA) (2015): »Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan, Version 1.0«; Dezember 2015; https://www.enisa.europa.eu/publications/pets; zuletzt abgerufen am: 06.04.2016.

IT-SICHERHEIT IST UND BLEIBT EIN KATZ-UND-MAUS-SPIEL.

Fromm, Jens; Welzel, Christian; Hoepner, Petra; Pattberg, Jonas (2013): »ÖFIT White Paper. Vertrauenswürdige digitale Identität: Baustein für öffentliche IT«; Oktober 2013; https://www.oeffentliche-it.de/documents/10181/14412/Vertrauensw%C3%BCrdige+digitale+Identit%C3%A4t+Baustein+f%C3%BCr+%C3%B6ffentliche+IT; zuletzt abgerufen am: 06.04.2016.

Höfling, Jürgen (2013): »SIEM-Produkten fehlen noch Intelligenz und Prävention«; ZDNet, 02.05.2013; http://www.zdnet.de/88153652/siem-produkten-fehlen-noch-intelligenz-und-pravention/; zuletzt abgerufen am: 06.04.2016.

Kammerhofer, Sabine (2011): »Implementierung von Sicherheitskennzahlen in den IT-Grundschutz«; Diplomarbeit, Juli 2011; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/DA_Sabine_Kammerhofer_pdf.pdf?__blob=publicationFile; zuletzt abgerufen am: 06.04.2016.

Karlsruher Institut für Technologie (KIT): »Sichere Mehrparteienberechnung«; https://crypto.iti.kit.edu/index.php?id=research-tpc; zuletzt abgerufen am: 06.04.2016.

Kelm, Stefan (2006): »Mit Honeynet Hacker fangen«; 11.09.2006; http://www.heise.de/netze/artikel/Mit-Honeynet-Hacker-fangen-221592.html; zuletzt abgerufen am: 06.04.2016.

Killmann, Wolfgang; Wicke, Guntram; Lochter, Manfred (2011): »Evaluierungsleitfaden für die Seitenkanalanalyse von ECC-Implementierungen«; Vortrag auf dem 12. Deutschen IT-Sicherheitskongress, 12. Mai 2011; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/12ter/Praesentationen/12_Mai_Parksaal/Wicke_Killmann-Evaluierungsleitfaden-Seitenkanalanalysen-ECCImplementierungen.pdf?__blob=publicationFile; zuletzt abgerufen am: 06.04.2016.

Lischka, Konrad (2013): »Kontroll-Chips: So will die PC-Industrie Kunden entmündigen«; erschienen in Spiegel Online, 23.8.2013; http://www.spiegel.de/netzwelt/web/trusted-platform-module-so-will-die-pc-industrie-kunden-entmuendigen-a-917950.html; zuletzt abgerufen am: 06.04.2016.

McAfee; Center for Strategic and International Studies (2014): »Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II«; http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf; zuletzt abgerufen am: 12.02.2016.

Menz, Nadja; Hoepner, Petra; Tiemann, Jens; Koußen, Frank (2015): »White Paper S2: Safety und Security aus dem Blickwinkel der öffentlichen IT«; April 2015; https://www.oeffentliche-it.de/documents/10181/14412/Safety+und+Security+aus+dem+Blickwinkel+der+%C3%B6ffentlichen+IT; zuletzt abgerufen am: 06.04.2016.

Pollmann, Maike (2012): »Quantenkommunikation: Rekordverdächtige Teleportation gelungen«; 22.05.2012; http://www.spektrum.de/news/rekordverdaechtige-teleportation-gelungen/1152292; zuletzt abgerufen am: 06.04.2016.

Rötzer, Florian (2001): »Quantenteleportation und Kryptographie«; 07.05.2001; http://www.heise.de/newsticker/meldung/Quantenteleportation-und-Kryptographie-40715.html; zuletzt abgerufen am: 06.04.2016.

Schmidt, Jürgen (2015): »Festgenagelte Zertifikate. TLS wird sicherer durch Certificate Pinning«; erschienen in c't 23/2015, S. 118; https://shop.heise.de/katalog/festgenagelte-zertifikate; zuletzt abgerufen am: 06.04.2016.

NEBEN DEN TECHNISCHEN MÖGLICHKEITEN
BEDARF ES AUCH ORGANISATORISCHER
UND RECHTLICHER MASSNAHMEN.

Schwan, Ben (2010): »Voll homomorphe Verschlüsselung in der Cloud«; 16.06.2010; http://www.heise.de/newsticker/meldung/Voll-homomorphe-Verschluesselung-in-der-Cloud-1021361.html; zuletzt abgerufen am: 06.04.2016.

SecuPedia: »Advanced Persistent Threat«; http://www.secupedia.info/wiki/Advanced_Persistent_Threat; zuletzt abgerufen am: 06.04.2016.

Seeger, Bernhard (2010): »Complex Event Processing: Auswertung von Datenströmen, Kontinuierliche Kontrolle«; erschienen in iX, 2/2010; http://www.heise.de/ix/artikel/Kontinuierliche-Kontrolle-905334.html; zuletzt abgerufen am: 06.04.2016.

Spiegel Online (2008): »Quantenkryptografie: Physiker demonstrieren unknackbares Netzwerk«; 08.10.2008, http://www.spiegel.de/netzwelt/tech/quantenkryptografie-physiker-demonstrieren-unknackbares-netzwerk-a-582951.html; zuletzt abgerufen am: 06.04.2016.

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, eIDAS-Verordnung. http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=DE; zuletzt abgerufen am: 06.04.2016.

Walton, Jeffrey; Steven, John; Manico, Jim; Wall, Kevin; Iramar, Ricardo (2016): »Certificate and Public Key Pinning«; https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning; zuletzt abgerufen am: 06.04.2016.

Weicker, Karsten (2015): »Evolutionäre Algorithmen«; 3. Auflage; Springer Vieweg; ISBN 978-3-658-09957-2.

Wikipedia; https://de.wikipedia.org/wiki/; zuletzt abgerufen am: 06.04.2016.

GEFÖRDERT VOM

Bundesministerium
des Innern

KONTAKT

Nicole Opiela
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de

kre | 1604 (Fotos: https://pixabay.com/; Grafiken: Fraunhofer FOKUS)