gematik

Sicherheitsstrategie 2030

Für eine vertrauenswürdige Telematikinfrastruktur

Die Telematikinfrastruktur (TI) verbindet die Beteiligten des deutschen Gesundheitswesens und lässt die Zahl digitaler Versorgungsprozesse wachsen. Millionen Versicherte sowie Beschäftigte in Praxen, Krankenhäusern, Apotheken und weiteren Einrichtungen verlassen sich zunehmend auf ihre Dienste.

Die TI ist damit das digitale Rückgrat des Gesundheitswesens und Teil der kritischen Infrastrukturen Deutschlands. Mit ihrer Bedeutung wachsen die Anforderungen an ihre Sicherheit. Gesundheitsdaten benötigen einen besonders hohen Schutz. Zugleich müssen digitale Dienste zuverlässig verfügbar sein, weil Störungen direkte Auswirkungen auf die Versorgung haben können. Sicherheitsmechanismen müssen sich daher im Alltag bewähren und so gestaltet sein, dass sie die Arbeit der Nutzerinnen und Nutzer unterstützen.

Die Sicherheitsstrategie 2030 beschreibt, wie die gematik den Schutz der TI unter veränderten technologischen und geopolitischen Bedingungen weiterentwickelt. Im Mittelpunkt stehen vier Ziele:

- sensible Gesundheitsdaten und die informationelle Selbstbestimmung der Versicherten schützen;
- digitale Versorgungsprozesse zuverlässig und krisenfest gestalten;
- die digitale Souveränität und Handlungsfähigkeit der TI stärken;
- Sicherheit wirksam und zugleich nutzerfreundlich umsetzen.

Diese Ziele werden über drei strategische Handlungsfelder verfolgt:

- eine ganzheitliche risikobasierte Security Governance,
- die Weiterentwicklung der Sicherheitsarchitektur sowie
- der Ausbau der operativen Sicherheit und Resilienz.

Warum wir Sicherheit weiterentwickeln

Die Digitalisierung im Gesundheitswesen ermöglicht schnellere sowie innovative Prozesse, steigert Effizienz und verbessert die Inklusion. Sie trägt dazu bei, trotz Fachkräftemangels, steigenden Kostendrucks und des demografischen Wandels eine leistungsfähige und verlässliche Patientenversorgung sicherzustellen. Mit jeder zusätzlichen digitalen Anwendung wächst jedoch auch die Abhängigkeit von stabilen Systemen. Gleichzeitig vergrößert sich die mögliche Angriffsfläche.

Cyberangriffe werden professioneller, schneller und arbeitsteiliger durchgeführt. Neben klassischer Cyberkriminalität gewinnt die hybride Kriegsführung an Bedeutung, die kritische Infrastrukturen (KRITIS) stören und dadurch die Gesellschaft verunsichern soll. Auch das Gesundheitswesen ist ein attraktives Angriffsziel, weil medizinische Daten einen hohen Schutzbedarf haben und viele Versorgungsprozesse nur eine geringe Ausfalltoleranz besitzen.

Künstliche Intelligenz (KI) beschleunigt diese Entwicklung. Spezialisierte Modelle können Software automatisiert untersuchen, Schwachstellen schneller finden und Angriffe in größerem Maßstab vorbereiten. Dadurch verkürzt sich die Zeit zwischen dem Bekanntwerden einer Schwachstelle und ihrer möglichen Ausnutzung. Durch KI erhalten außerdem Akteure mit geringerer technischer Erfahrung Zugang zu leistungsfähigen Angriffswerkzeugen.

Technologische und geopolitische Abhängigkeiten werden ebenfalls zu einem Sicherheitsfaktor. Kritische Komponenten, Cloud-Infrastrukturen und besonders leistungsfähige KI-Modelle stammen häufig von wenigen Anbietern außerhalb Europas. Wenn der Zugang eingeschränkt wird oder Anbieter ihre Bedingungen ändern, kann dies die Reaktions- und Entwicklungsfähigkeit europäischer Institutionen beeinträchtigen. Die Kontrolle über Abhängigkeiten und die eigenen Handlungsoptionen gehört deshalb zur Sicherheitsvorsorge.

Die Sicherheitsstrategie der gematik ist entstanden, um den neuen Rahmenbedingungen gerecht zu werden und zukünftige Entwicklungen zu antizipieren. Dies wirkt auf die Sicherheitsarchitektur der Telematikinfrastruktur ebenso wie auf ihre technische Überwachung und die Governance aller Beteiligten im Kern der TI und ihrem Ökosystem.

Zielbild für das Jahr 2030

Unser Ziel ist ein digitaler Gesundheitsraum, der resilient und überprüfbar vertrauenswürdig ist und die Hoheit über hochsensible Gesundheitsdaten wahrt.

Drei Handlungsfelder bilden das fachliche Gerüst der Sicherheitsstrategie:

- → Die ganzheitliche risikobasierte Security Governance ordnet Verantwortlichkeiten entlang der Versorgungsprozesse. Sie schafft die Grundlage, um Risiken einheitlich zu bewerten, die Sicherheitsleistung beteiligter Unternehmen zu überprüfen und bei Bedarf verbindlich einzugreifen.
- → Die Weiterentwicklung der Sicherheitsarchitektur schafft eine einheitliche und anpassungsfähige Sicherheitsbasis für die TI 2.0. Wiederverwendbare Sicherheitsbausteine, Zero Trust, sichere digitale Identitäten, souveräne Cloud-Technologien und Post-Quanten-Kryptografie reduzieren Komplexität und schaffen Zukunftsfähigkeit.
- → Operative Sicherheit und Resilienz verbinden kontinuierliches Monitoring inkl. KI-gestützter Anomalieerkennung mit schnellen Analyse- und Reaktionsprozessen. Ein rund um die Uhr besetzter Leitstand, der weitere Ausbau der Security-Operations-Fähigkeiten und eine systematische Krisenvorsorge sollen Angriffe früh begrenzen und die Versorgung auch unter Belastung unterstützen.

Die drei Handlungsfelder greifen ineinander. Erkenntnisse aus dem Betrieb verändern die Risikobewertung. Daraus folgen Anpassungen an Anforderungen und Architektur. Neue Schutzmechanismen werden wiederum im laufenden Betrieb auf ihre Wirksamkeit geprüft.

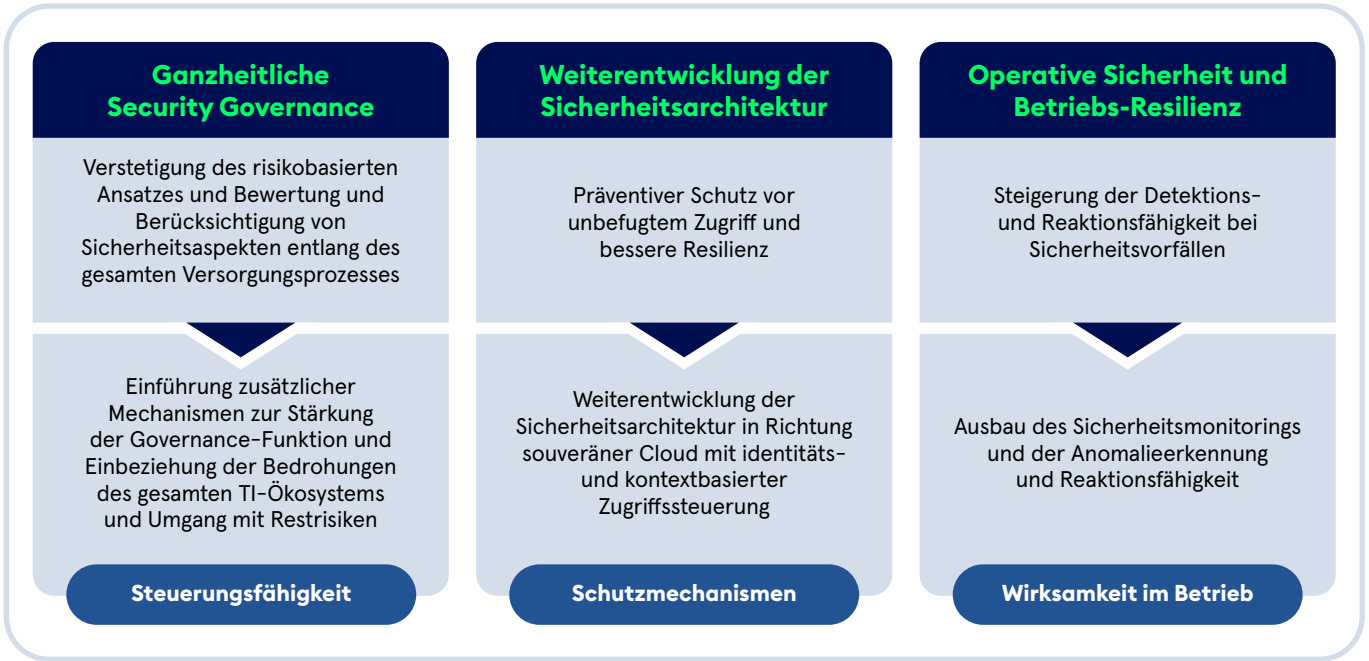


Abbildung 1: Die strategischen Handlungsfelder der Sicherheitsstrategie

Ganzheitliche risikobasierte Security Governance

Sicherheit entlang Versorgungsprozesse

Ein Sicherheitsvorfall richtet sich nicht nach technischen oder organisatorischen Zuständigkeitsgrenzen. Eine Schwachstelle kann in einem zentralen TI-Dienst, bei einem Hersteller, in einem Primärsystem oder in der Betriebsumgebung einer angeschlossenen Einrichtung entstehen. Ihre Wirkung kann sich dennoch über die gesamte Versorgungskette ausbreiten.

Die gematik betrachtet Sicherheit deshalb Ende-zu-Ende entlang des Versorgungsprozesses. Ausgangspunkt sind Versorgungs- und Nutzungssituationen: Wer greift auf welche Daten zu, welche Systeme sind beteiligt, welche Abhängigkeiten bestehen und welche Folgen hätte eine Störung oder Manipulation? Diese Betrachtung beginnt bei Konzeption und Entwicklung und reicht über Beauftragung bzw. Zulassung und Betrieb bis zum Ende des Produktlebenszyklus.

Dabei bleiben die jeweiligen Verantwortlichkeiten erhalten. Für zentrale Dienste und Komponenten trägt die gematik eine unmittelbare Steuerungsverantwortung. Bei dezentralen Produkten und Anwendungen setzt sie Sicherheitsanforderungen und überprüft deren Einhaltung, während Hersteller und Betreiber für ihre Systeme verantwortlich bleiben. Praxen, Krankenhäuser und andere Einrichtungen verantworten ihre lokalen Betriebsumgebungen. Die gematik beobachtet zugleich, welche Risiken von angeschlossenen Systemen auf die TI einwirken können, und unterstützt die Beteiligten durch Anforderungen, Informationen und Beratung.

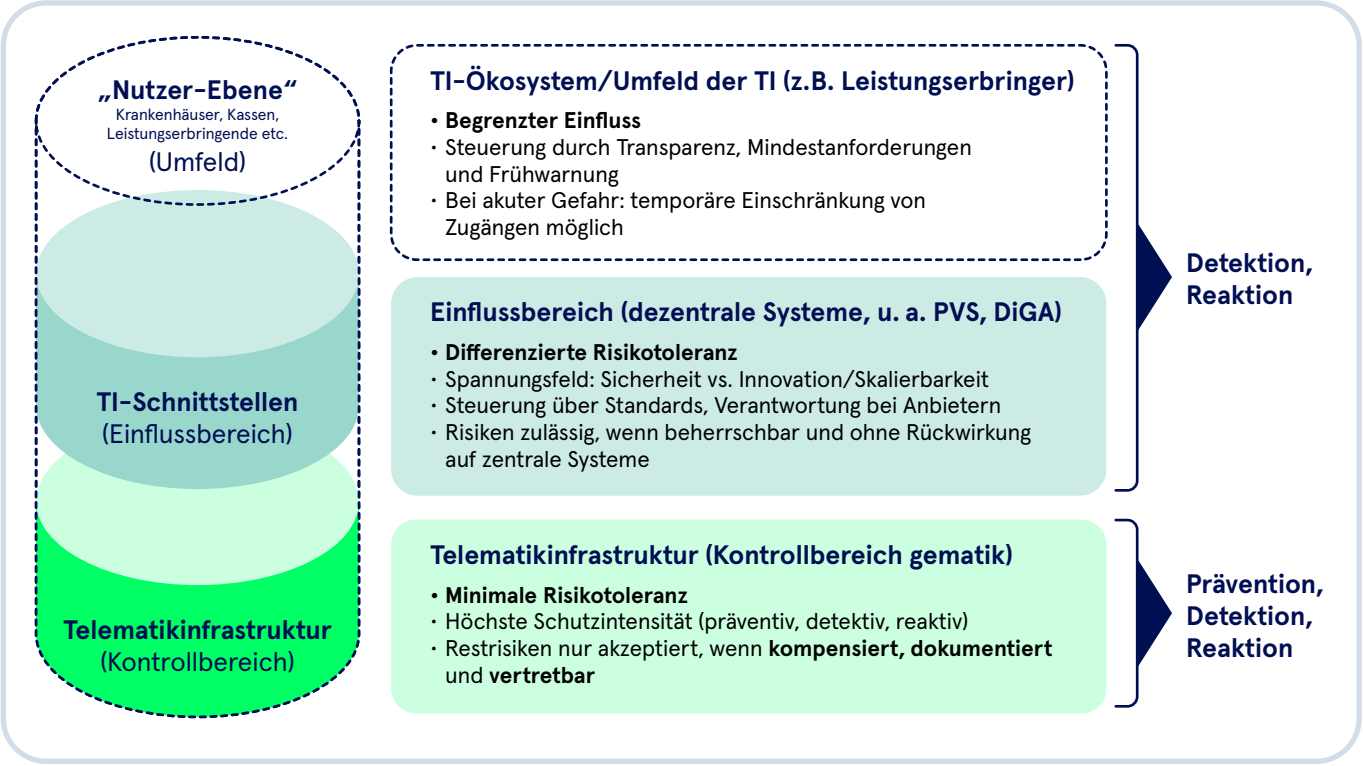


Abbildung 2: Security Governance für das TI-Ökosystem

Risikoorientiertes Handeln und Innovationen ermöglichen

Schutzmaßnahmen richten sich an der Kritikalität eines Dienstes, der betroffenen Daten und der möglichen Auswirkungen auf die Versorgung aus. Für zentrale und versorgungsrelevante Dienste gilt eine besonders geringe Risikotoleranz: Präventive, erkennende und reaktive Maßnahmen werden dort eng miteinander verbunden.

In anderen Bereichen gilt es, Sicherheit, Innovationsfähigkeit und Nutzbarkeit in ein angemessenes Verhältnis zu bringen. Eine hohe formale Zulassungshürde schützt beispielsweise nicht automatisch besser, wenn sie schnelle Sicherheitsupdates erschwert oder Hersteller die Einstellung entwickeln, sie seien dadurch aus ihrer eigenen Verantwortung

entlassen. Deshalb erleichtert die gematik, wenn möglich, die Prüfung vor dem Markteintritt und ergänzt sie durch eine stärkere kontinuierliche Überwachung im laufenden Betrieb.

Der TI-Security-Standard bildet hierfür einen einheitlichen Rahmen. Anbieter und Betreiber müssen ihre Sicherheitsfähigkeit nicht nur bei der Zulassung, sondern kontinuierlich nachweisen. Dazu gehören, je nach Kritikalität, Audits, Penetrationstests, Schwachstellenanalysen, Notfallübungen und die Übermittlung sicherheitsrelevanter Informationen. Erkenntnisse werden zu einem anbieterübergreifenden Lagebild zusammengeführt.

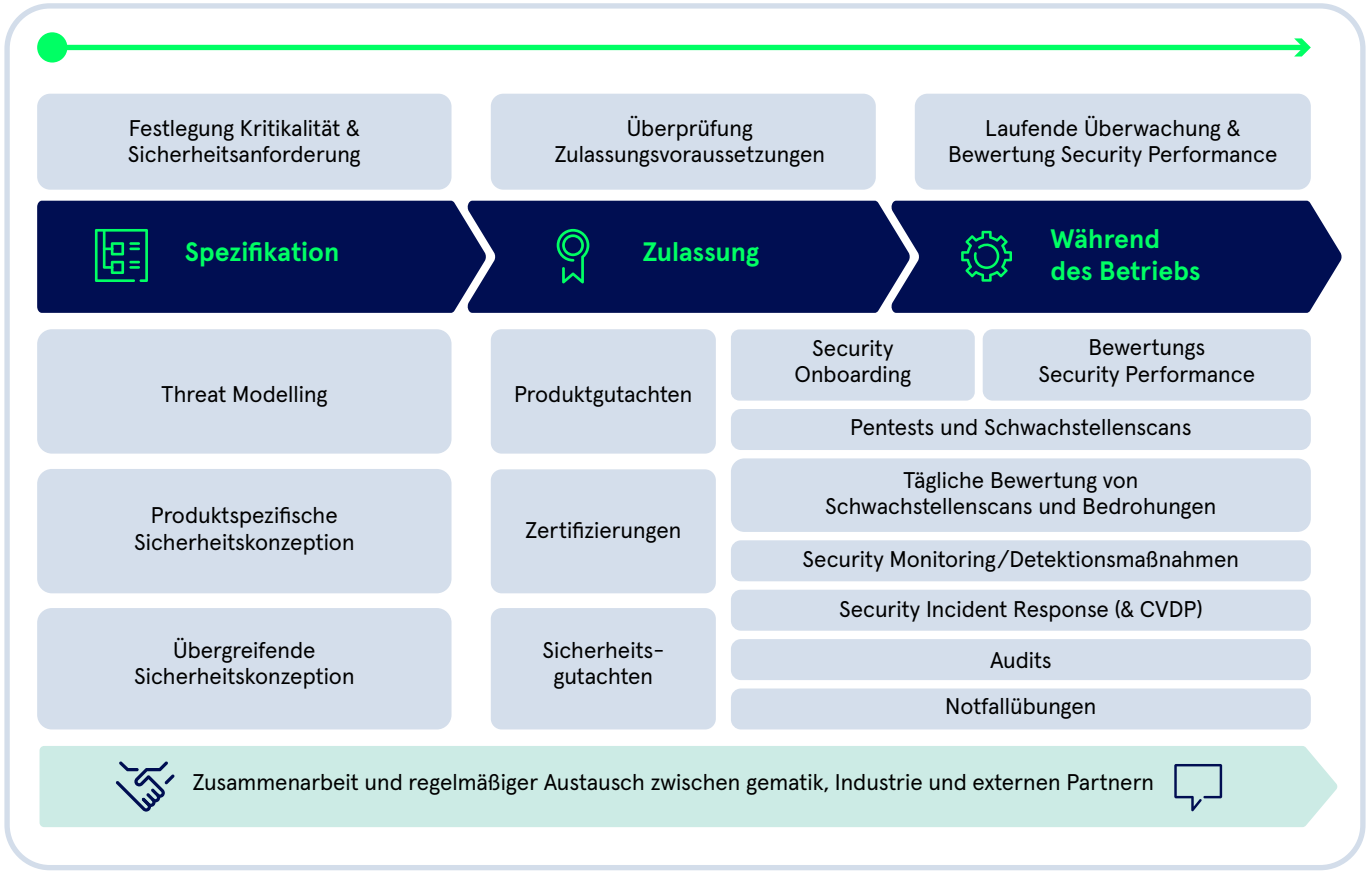


Abbildung 3: Von der Spezifikation bis zur kontinuierlichen Überwachung

Sicherheitsanforderungen müssen sich zugleich im Versorgungsalltag bewähren. Rückmeldungen aus Praxen, Krankenhäusern und weiteren Einrichtungen fließen deshalb stärker in die Bewertung ein. Ein hohes Schutzniveau ist nur dauerhaft tragfähig, wenn die vorgesehenen Maßnahmen verständlich, praktikabel und verhältnismäßig sind.

Weiterentwicklung der Sicherheitsarchitektur

Sicherheit als Eigenschaft der Plattform

Die TI 2.0 erhält eine stärker standardisierte und modular aufgebaute Sicherheitsarchitektur. Zentrale Sicherheitsfunktionen stehen als wiederverwendbare Bausteine bereit, werden also nicht für jede Anwendung neu und unterschiedlich entwickelt. Anwendungen können auf geprüfte Plattformdienste zurückgreifen. Sicherheitsupdates und neue Anforderungen lassen sich dadurch zentral umsetzen und schneller in der Breite wirksam machen.

Eine gemeinsame Referenzarchitektur legt fest, welches Sicherheitsniveau zu erreichen ist. Sicherheit wird von Beginn an in Entwicklung und Bereitstellung eingebaut. Reviews, unabhängige Sicherheitsgutachten, Penetrationstests und kontinuierliches Monitoring prüfen anschließend, ob die vorgesehenen Maßnahmen im Betrieb tatsächlich wirken. Erkenntnisse aus diesen Prüfungen fließen in die Weiterentwicklung der Plattform zurück.

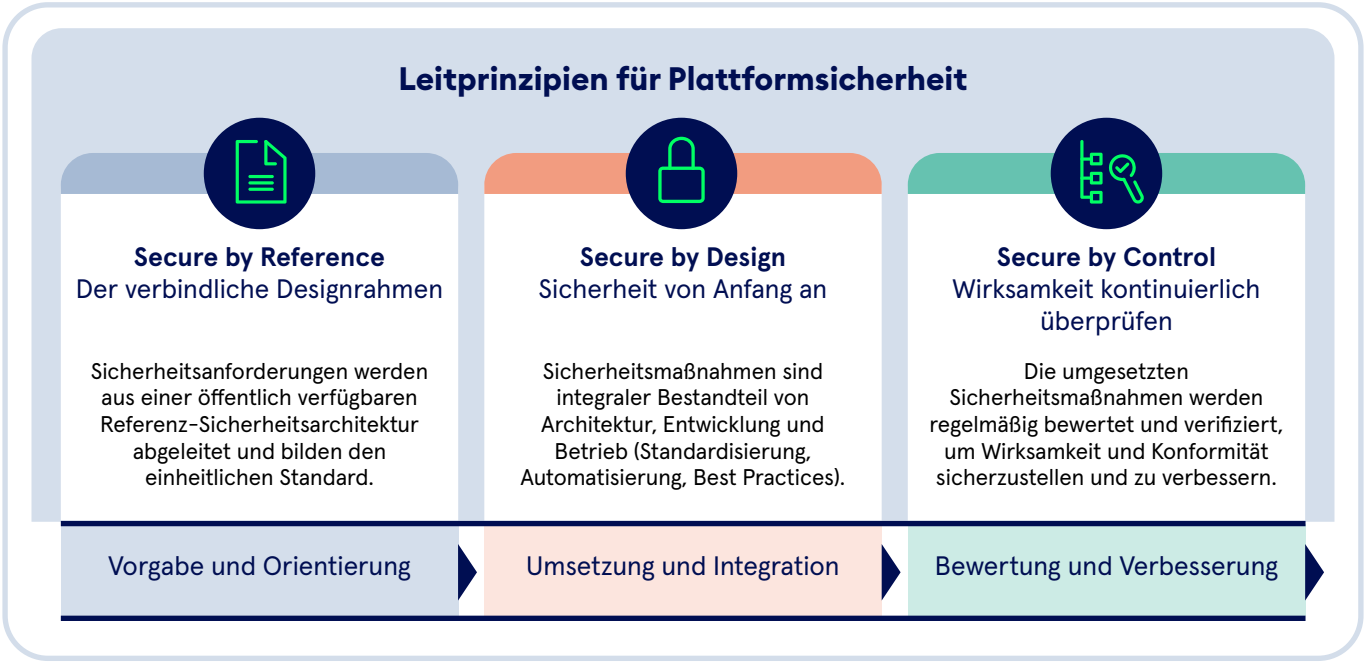


Abbildung 4: Leitprinzipien der Plattformsicherheit

Zugriffe kontinuierlich prüfen

Zero Trust ist ein Kernbaustein dieser Architektur. Die heutige TI setzt in weiten Teilen auf ein geschlossenes Netz und eine starke Kontrolle beim Zugang. In der TI 2.0 reicht der erfolgreiche Eintritt in das Netz nicht mehr aus, um auch weitere Aktivitäten als vertrauenswürdig einzustufen. Jede relevante Anfrage wird anhand von Identität, Kontext und Risiko bewertet.

Der Zeta-Guard soll diese Sicherheitslogik schrittweise für die Dienste der TI verfügbar machen. Er kann auffällige oder riskante Zugriffe erkennen und zentral vorgegebene Schutzmaßnahmen durchsetzen. Gefahren lassen sich dadurch gezielter begrenzen, ohne dass der Zugang für alle Nutzerinnen und Nutzer gleichermaßen eingeschränkt wird.

Sichere digitale Identitäten bilden dafür eine wichtige Grundlage. Die heute eingesetzten Karten bieten ein hohes Vertrauensniveau, sind für mobile Anwendungen jedoch nicht immer praktikabel. Künftig sollen auch kartenunabhängige und mobil nutzbare Identitäten mit einem vergleichbar hohen Schutzniveau verfügbar sein. Die gematik arbeitet dazu gemeinsam mit dem BSI an der Einbindung europäischer Lösungen wie der European Digital Identity Wallet (EUDI-Wallet)

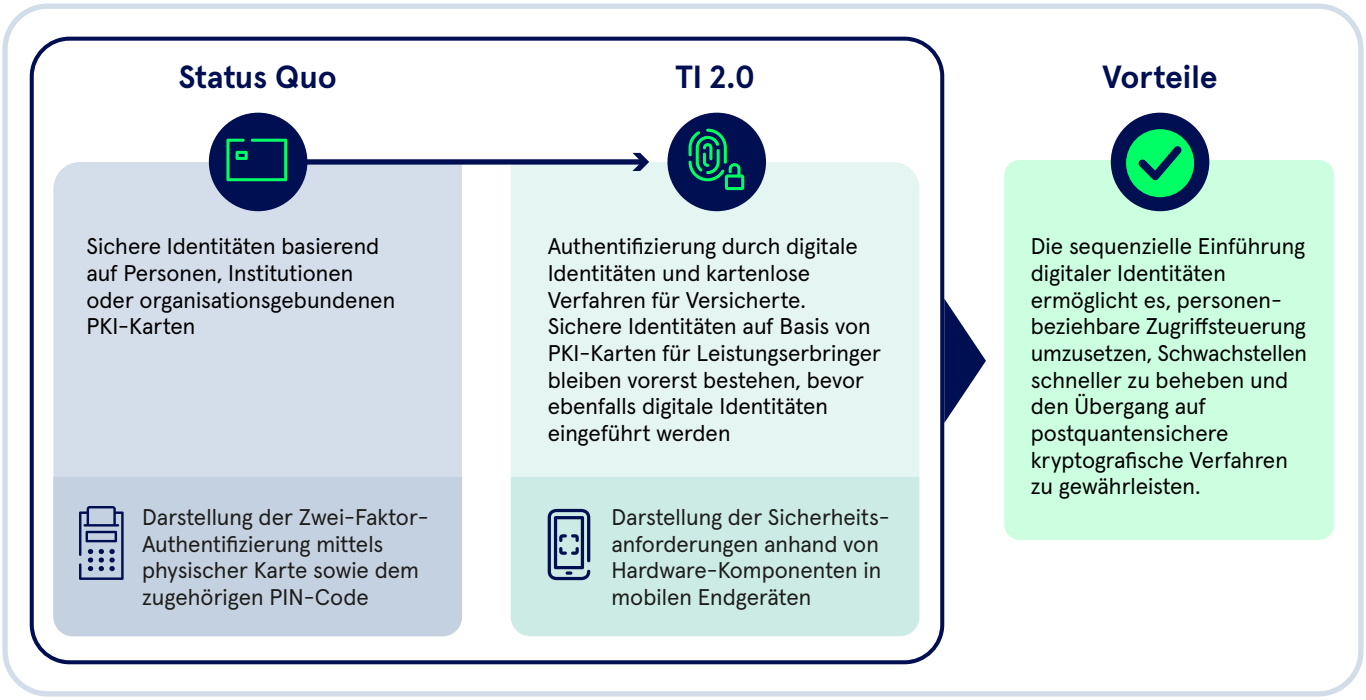
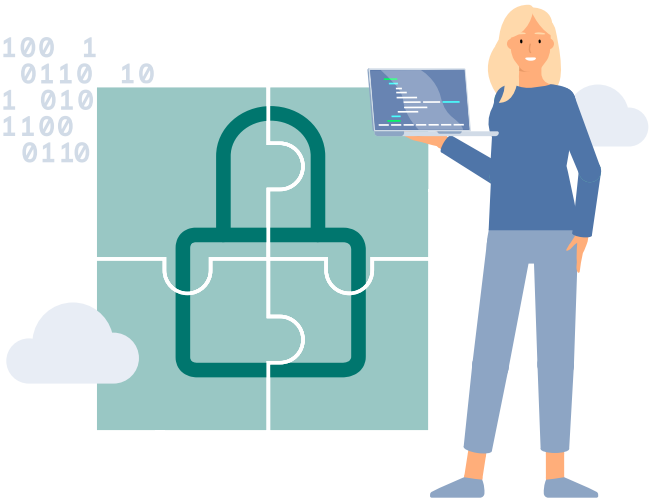


Abbildung 5: Digitale Identitäten in der TI 2.0



Digitale Souveränität als Sicherheitsprinzip

Digitale Souveränität bedeutet für die gematik, kritische Dienste und Daten auch unter veränderten technischen, wirtschaftlichen und geopolitischen Bedingungen kontrollieren und schützen zu können. Der Standort eines Rechenzentrums und die Einhaltung formaler Vorgaben sind dafür wichtig, reichen allein aber nicht aus.

Abhängigkeiten, Komponenten und Schnittstellen müssen transparent sein. Systeme müssen überprüfbar und soweit möglich austauschbar bleiben. Offene Standards, Open Source und modulare Architekturen erleichtern unabhängige Sicherheitsprüfungen, verringern die Bindung an einzelne Anbieter und erhalten technische Handlungsoptionen. Bei der Auswahl und Gestaltung von Cloud-Diensten werden deshalb auch Portierbarkeit, Nachweisbarkeit und die tatsächlichen Zugriffsmöglichkeiten des Betreibers berücksichtigt.

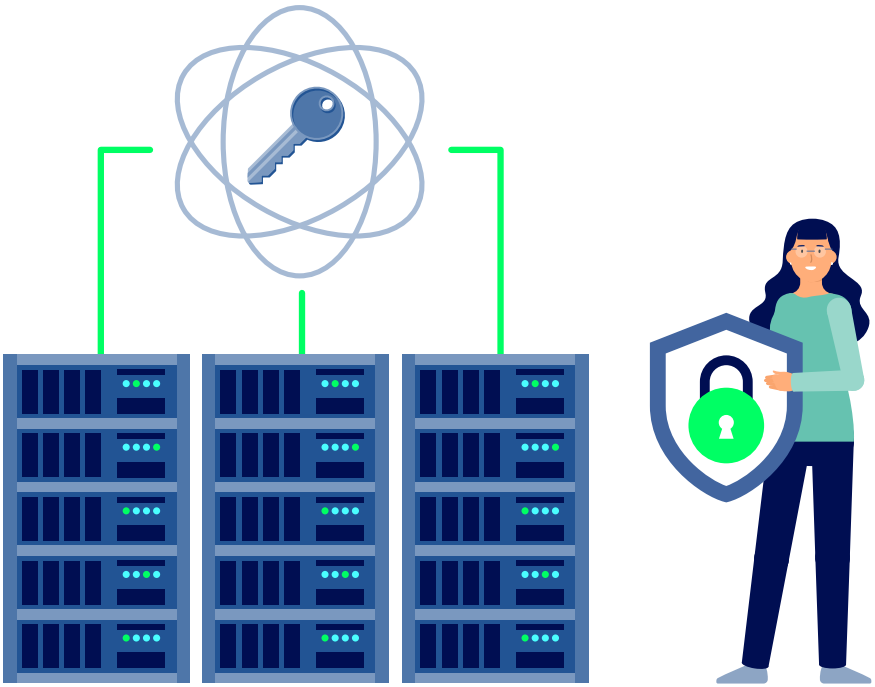
Healthcare Confidential Computing schafft dafür einen kryptografisch geschützten Verarbeitungsraum in der Cloud. Daten werden auch während ihrer Verarbeitung geschützt. Technische Nachweise ermöglichen es der gematik, zu prüfen, ob ausschließlich zugelassene Software in der vorgesehenen Umgebung ausgeführt wird. Dieses Modell verbindet die Skalierbarkeit und Verfügbarkeit moderner Cloud-Technologien mit einem hohen Schutz vor unberechtigten Zugriffen, auch durch den Betreiber der Infrastruktur.

Vorbereitung auf künftige Quantencomputer

Leistungsfähige Quantencomputer sind ein Hoffnungsträger für bahnbrechende Innovationen in Wissenschaft, Medizin und Industrie. Sie könnten aber auch einen Teil der heute eingesetzten kryptografischen Verfahren brechen. Angreifer können verschlüsselte Daten bereits heute speichern, um sie später mit neuer Technik zu entschlüsseln. Für Gesundheitsdaten, die über viele Jahre vertraulich bleiben müssen, ist dieses sogenannte Store-now-decrypt-later-Szenario besonders relevant.

Die elektronische Patientenakte (ePA) nutzt bereits hybride kryptografische Verfahren. Diese kombinieren etablierte klassische Methoden mit post-quanten-sicheren Verfahren. Die ePA ist damit schon heute gegen Store-now-decrypt-later-Angriffe abgesichert und dient als konkretes Beispiel für die weitere Modernisierung der TI.

Für weitere Anwendungen wird die Umstellung schrittweise vorangetrieben. Der Schutz von Datenübertragung und Datenspeicherung soll vor Ende 2030 in der Breite wirksam sein.



Secure by Reference: Was ist der Sicherheitsstandard?

Die Referenz-Sicherheitsarchitektur gibt den verbindlichen Designrahmen vor.

Referenz-Sicherheitsarchitektur: Öffentliche, stabile Referenz

Leitplanken & Prinzipien

- Sicherheitsziele
- Richtlinien (Policies)
- Compliance & regulatorische Vorgaben
- Architekturprinzipien (z. B. Least Privilege, Zero Trust, Privacy by Design)

Artefakte & Guidance

- Guidelines
- Policies
- Standards (z.B. BSI, NIST, ISO/IEC 27001)
- Designmuster
- Blueprints
- Best Practices
- Methoden
- Übergreifendes Bedrohungsmodell

Modulare Sicherheitsbausteine (Beispiele)

Zero Trust	Digitale Identitäten	Digitale Souveränität	Healthcare Confidential Computing	Post-Quanten-Kryptografie
Durchgängige Verifizierung, Minimaler Zugriff, kontinuierlich	Vertrauenswürdige Identitätsverwaltung und starke Authentifizierung	Datenhoheit, Transparenz und Kontrolle über Cloud-Dienste	Schutz sensibler Gesundheitsdaten während der Verarbeitung	Kryptografische Verfahren resistent gegen zukünftige Quantenangriffe

Einmaligkeitsprinzip (eine Ausprägung) | **Open Source** | **State-of-the-Art**

Secure by Design: Wie wird der Sicherheitsstandard umgesetzt?

Sicherheit wird von Beginn an in Architektur, Entwicklung und Betrieb integriert.

Umsetzung in der Cloud-Plattform: Sicherheit als integraler Bestandteil

Plattformdienste & Sicherheitsbausteine

Die referenzierten Bausteine werden zentral als Plattformdienste bereitgestellt und betrieben.

Nutzung durch Anwendungen und Dienste

Standardisierte, sichere Nutzung der Plattformdienste durch alle Anwendungen in der Telematikinfrastruktur.

Prinzipien in der Umsetzung (Secure Software Development)

- **Security by Default**
- **Security as Code**
- **Automatisierung & Orchestrierung**
- **Kontinuierliche Integration & Härtung**

Leitprinzip: Secure by Design – Sicherheit ist von Beginn an eingebaut.

Secure by Control: Wie wird die Wirksamkeit nachgewiesen?

Die Umsetzung wird regelmäßig bewertet, überprüft und kontinuierlich verbessert.

Bewertung & Evaluierung: Sicherheit kontinuierlich überprüfen und verbessern

Überprüfung der Sicherheitsmaßnahmen

- Reviews von Sicherheitskonzepten (Architektur- & Design-Reviews)
- Externe Sicherheitsgutachten (unabhängige Bewertung)
- Penetrationstests, Tools & Tactics Analyse (Technische Überprüfung)
- Weitere Prüfungen (Schwachstellenanalysen, Audits, Konfigurationsprüfungen, Monitoring)

Erkenntnisse und Maßnahmen

Ableitung von Verbesserungen und Anpassungen für Architektur, Bausteine und Prozesse

Leitprinzip: Secure by Control – Wirksamkeit wird nachgewiesen und verbessert.

Kontinuierlicher Verbesserungsprozess
Lernen – Anpassen – Weiterentwickeln

Nutzen für die Plattformsicherheit

- **Homogene & konsistente Sicherheitsarchitektur**
- **Zentrale Weiterentwicklung & schnelle Anpassung**
- **Effizienz durch Wiederverwendung**
- **Hohe Sicherheit & Compliance-Nachweis**
- **Vertrauen & Transparenz für alle Beteiligten**

Abbildung 6: Kernelemente der Plattformsicherheit

Operative Sicherheit und Resilienz

Sicherheit kontinuierlich prüfen

Eine Zulassung bestätigt, dass ein Produkt zu einem bestimmten Zeitpunkt festgelegte Anforderungen erfüllt. Im laufenden Betrieb verändern sich jedoch Software, Konfigurationen, Nutzung und Bedrohungslage. Die gematik ergänzt die initiale Prüfung deshalb durch eine kontinuierliche Sicherheitssteuerung.

Zyklische Prüfungen wie Audits, Penetrationstests und Notfallübungen liefern vertiefte Bewertungen. Kontinuierliche Verfahren wie Schwachstellenscans, die Auswertung von Sicherheitsmeldungen und die Analyse externer Bedrohungsinformationen machen Veränderungen zwischen diesen Prüfungen sichtbar.

Das Security Monitoring führt Informationen aus unterschiedlichen Quellen zusammen. Dazu gehören Alarme der TI-Anbieter, anwendungsspezifische Anomalien, Erkenntnisse aus der Beobachtung der Angriffsfläche, Informationen nationaler und internationaler Partner sowie sicherheitsrelevante Daten aus der Zero-Trust-Architektur. Eine zentrale SIEM-Plattform korreliert diese Informationen und unterstützt die schnelle Bewertung.

Das Monitoring folgt klaren Datenschutzvorgaben. Personenbeziehbare Informationen werden grundsätzlich pseudonymisiert und auf das notwendige Maß beschränkt. Eine Zuordnung zu einer konkreten Identität erfolgt nur bei einem begründeten Verdacht und bezogen auf den jeweiligen Einzelfall.

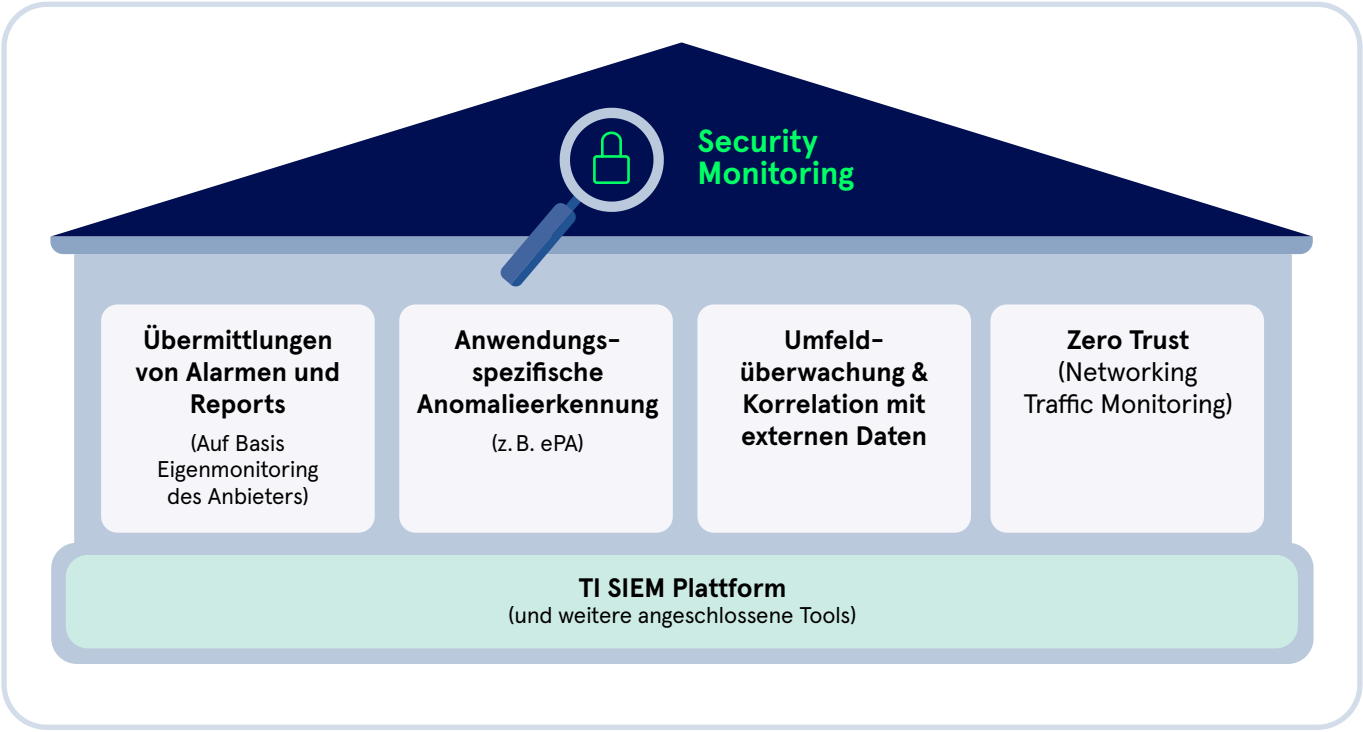


Abbildung 7: Säulen des Security Monitorings

Rund um die Uhr reagieren können

Die gematik verfügt bereits über einen 24/7 besetzten Leitstand mit Sicherheitskompetenz. Dort werden technische Störungen, Auffälligkeiten im Monitoring, Schwachstellen und Sicherheitsvorfälle gemeinsam betrachtet. Die Fähigkeiten des Security Operations Centers werden weiter ausgebaut, um Ereignisse möglichst früh einordnen und geeignete Gegenmaßnahmen einleiten zu können.

Detektion allein verhindert noch keinen Schaden. Deshalb werden die technische Erkennung und verbindliche Reaktionsprozesse eng miteinander verbunden. Bei einer konkreten Gefahr müssen Maßnahmen schnell, risikobasiert und so gezielt wie möglich wirken. Die Zero-Trust-Architektur schafft künftig zusätzliche Möglichkeiten, auffällige Zugriffe einzuschränken, ohne unnötig ganze Dienste oder Nutzergruppen zu beeinträchtigen.

Versorgung auch in Krisen unterstützen

Resilienz umfasst mehr als die Wiederherstellung technischer Systeme. Digitale Versorgungsprozesse müssen auch unter außergewöhnlichen Belastungen möglichst funktionsfähig bleiben. Für besonders kritische Situationen sind deshalb geeignete Ersatzverfahren vorzubereiten. Ein digitaler Ausfall darf nicht zu einem Ausfall der medizinischen Versorgung führen.

Eine sichere TI kann in einem Krisen- oder Katastrophenfall selbst zur Stabilisierung beitragen. Wenn andere Kommunikationswege beeinträchtigt sind, kann sie den Zugang zu versorgungsrelevanten Informationen und die Koordination zwischen Leistungserbringenden unterstützen. Sicherheit und Resilienz werden deshalb gemeinsam geplant, regelmäßig geübt und anhand realer Erfahrungen weiterentwickelt.

Künstliche Intelligenz als Enabler der Sicherheitsstrategie

Künstliche Intelligenz ist kein separates Handlungsfeld. Sie verändert die Bedrohungslage und unterstützt zugleich die Arbeit in allen drei Handlungsfeldern.

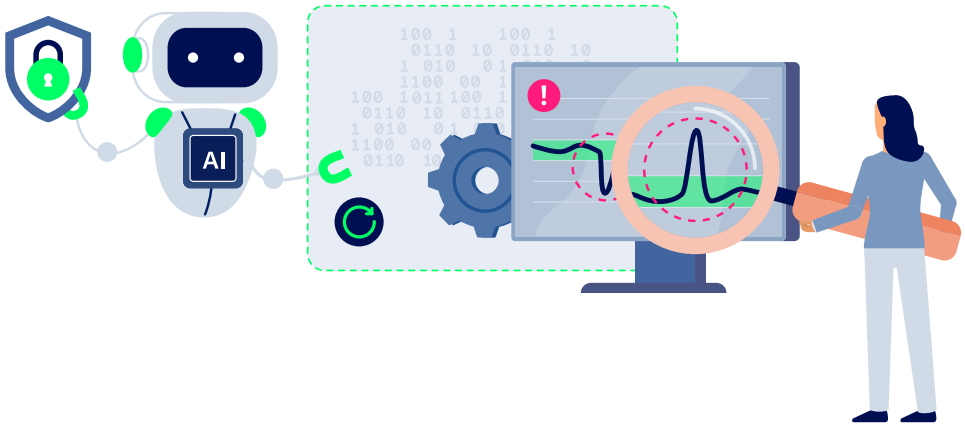
Auf der Angriffsseite können spezialisierte Modelle große Mengen von Softwarecode untersuchen und auch komplexe Logikfehler identifizieren. Angriffe lassen sich schneller vorbereiten, variieren und automatisieren. Dadurch sinken die Einstiegshürden und die verfügbare Reaktionszeit wird kürzer. Auch koordinierte Meldungen von Schwachstellen werden zunehmen, weil Sicherheitsforschende vergleichbare Werkzeuge einsetzen.

Der Zugang zu besonders leistungsfähigen Modellen wird selbst zu einer Frage digitaler Souveränität. Viele führende Modelle werden von wenigen Unternehmen außerhalb Europas kontrolliert. Zugriffsbeschränkungen oder zeitlich verzögerte Verfügbarkeit führen zu einer Fähigkeitslücke für den Schutz kritischer Infrastrukturen in Europa. Die gematik muss daher dauerhaft Zugang zu geeigneten Modellen und Rechenressourcen sicherstellen und ihre Abhängigkeiten beherrschbar gestalten.

Auf der Verteidigungsseite kann KI große Datenmengen schneller auswerten und Zusammenhänge erkennen, die mit statischen Regeln allein schwer sichtbar werden. Sie unterstützt insbesondere:

- die laufende Bewertung von Bedrohungen und Angriffsflächen,
- Threat Modeling sowie Architektur- und Codeanalysen,
- die Suche nach Schwachstellen und komplexen Logikfehlern sowie
- die Erkennung ungewöhnlicher Nutzungsmuster.

Die gematik baut den kontrollierten Zugang zu spezialisierten KI-Modellen für Sicherheitsanalysen als strategische Fähigkeit auf. Dazu gehört der Einsatz eines Security-LLM für architekturbasierte Analysen, Threat Modeling, die Erkennung komplexer Schwachstellen und die Priorisierung von Maßnahmen. Die Verfahren werden schrittweise in Entwicklungs-, Prüf- und Betriebsprozesse integriert.



Vertrauen durch Transparenz und Zusammenarbeit

Vertrauen entsteht, wenn Schutzmaßnahmen nachvollziehbar sind und ihre Wirkung im Betrieb überprüft wird. Die gematik will deshalb transparent darstellen, welche Maßnahmen umgesetzt wurden, welche Restrisiken bestehen und wo Grenzen der eigenen Einflussmöglichkeiten liegen.

Ein wichtiger Bestandteil ist das Coordinated Vulnerability Disclosure Program. Es bietet Sicherheitsforschenden einen verlässlichen Weg, Schwachstellen zu melden, und schafft klare Abläufe für Bewertung, Behebung und Veröffentlichung. Externe Hinweise werden als Beitrag zur Verbesserung der TI behandelt.

Open Source unterstützt diesen Ansatz. Öffentlich zugänglicher Quellcode ermöglicht unabhängige Prüfungen und erleichtert die Beteiligung der Sicherheitsforschung. Mit der Plattformstrategie soll der Anteil offen entwickelter TI-Komponenten weiter steigen.

Sicherheit entsteht im Gesundheitswesen durch Zusammenarbeit. Die gematik stimmt sich eng mit dem Bundesministerium für Gesundheit, dem BSI und dem BfDI ab. Industriepartner setzen Anforderungen in Produkten und im Betrieb um. Praxen, Krankenhäuser und andere Einrichtungen geben wichtige Rückmeldungen zur Wirksamkeit und Nutzbarkeit von Sicherheitsmaßnahmen. Forschung, Hochschulen und KRITIS-Organisationen tragen zusätzliche Erkenntnisse zu Schwachstellen und Bedrohungen bei.

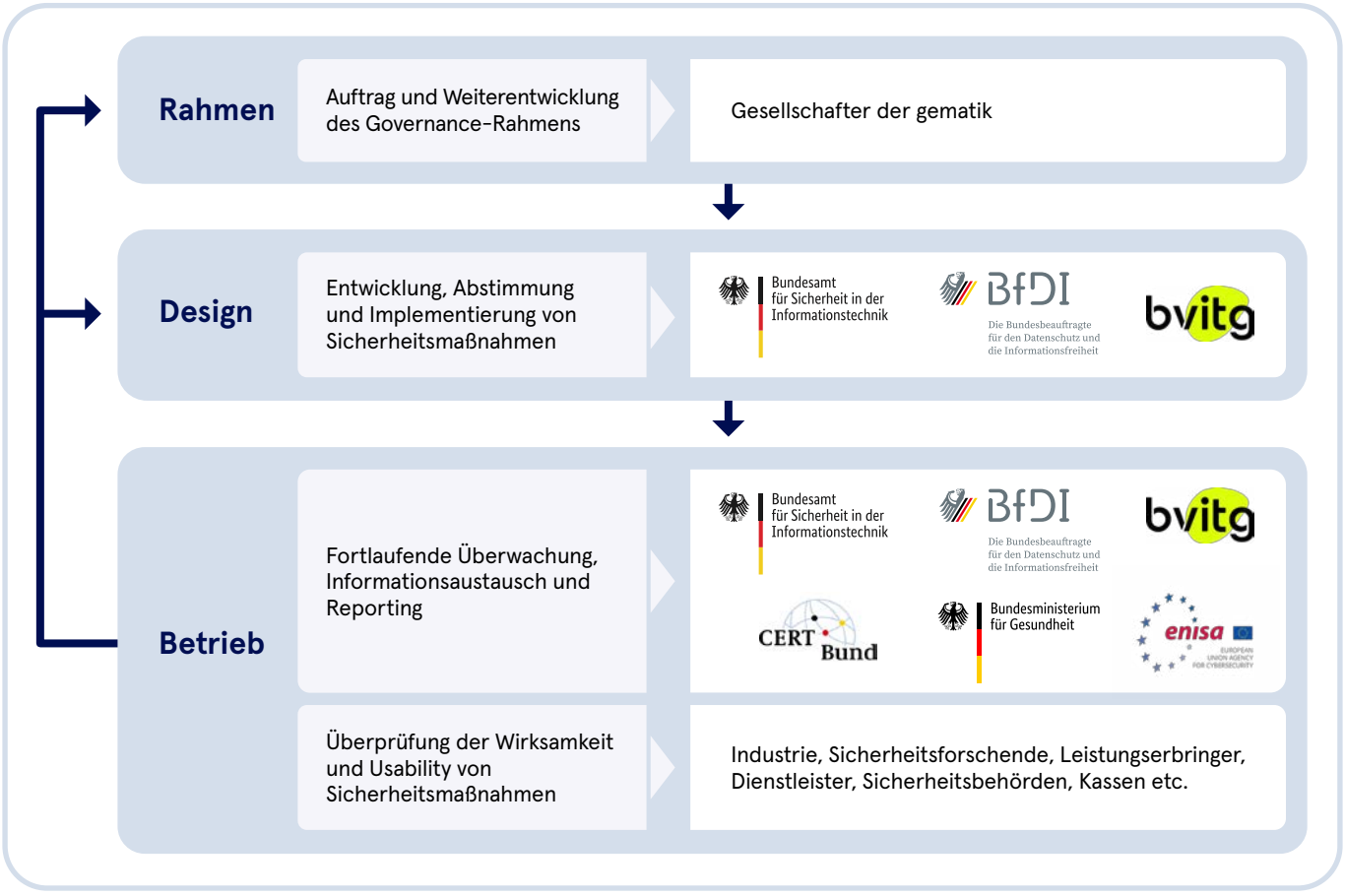
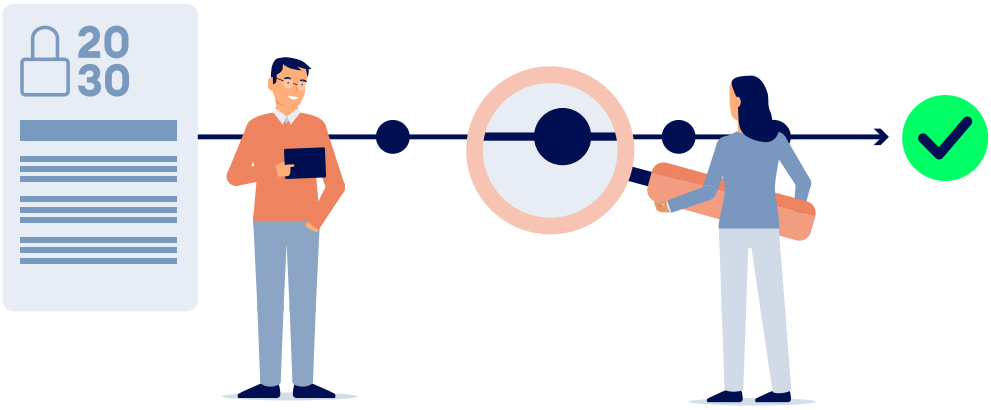


Abbildung 8: Zusammenarbeit der unterschiedlichen Stakeholder im Gesundheitswesen

Mit dem Europäischen Gesundheitsdatenraum wächst auch die grenzüberschreitende Verantwortung. Sicherheitsvorfälle, Abhängigkeiten und Angriffsmuster enden nicht an nationalen Grenzen. Die gematik baut deshalb den Austausch mit europäischen Digital Health Agencies aus. Gemeinsame Kontaktwege, der Austausch von Bedrohungsinformationen und abgestimmte Krisenprozesse werden die Reaktion auf Vorfälle mit grenzüberschreitender Wirkung verbessern.



Unser Weg bis zum Jahr 2030

Die Sicherheitsstrategie wird in mehreren, parallel laufenden Entwicklungsschritten umgesetzt. Nicht alle Maßnahmen können gleichzeitig abgeschlossen werden. Einige Schutzmechanismen wirken bereits heute, andere benötigen neue technische Plattformen oder international verfügbare Standards.

Was heute bereits wirkt

Der TI-Security-Standard schafft einen einheitlichen Rahmen für die laufende Sicherheitssteuerung von Anbietern und beauftragten Dienstleistern. Sicherheitsprüfungen, Schwachstellenanalysen, Monitoring und Notfallübungen ergänzen die Zulassung. Der Leitstand der gematik ist rund um die Uhr besetzt. Für die elektronische Patientenakte bestehen bereits anwendungsspezifische Verfahren zur Anomalieerkennung. Ihre hybride kryptografische Absicherung schützt schon heute gegen Store-now-decrypt-later-Angriffe.

Schwerpunkte in den Jahren 2026 und 2027

Die gematik entwickelt den TI-Security-Standard und die zugehörigen Steuerungsprozesse weiter. Der Zeta-Guard wird schrittweise eingeführt und die ersten modularen Sicherheitsbausteine für die TI 2.0 werden vorbereitet. Die SIEM-Plattform und KI-gestützte Detektionsverfahren werden ausgebaut. Neue Austauschformate mit Versorgung, Industrie, Sicherheitsforschung und europäischen Partnern ergänzen die technische Entwicklung.

Schwerpunkte in den Jahren 2027 bis 2029

Die Ende-zu-Ende-Betrachtung wird stärker in operative Steuerungsmechanismen überführt. Erste zentrale Sicherheitsdienste der Plattform werden breit eingesetzt und die Zero-Trust-Architektur wird auf weitere Nutzungsketten ausgeweitet. Ein umfassenderes Attack Surface Monitoring verbessert die Sicht auf Risiken in angeschlossenen und umgebenden Systemen. Verhaltensbasierte und KI-gestützte Analysen beziehen zusätzliche Datenquellen ein. Die Fähigkeiten des 24/7-Leitstands und des Security Operations Centers werden weiter vertieft.

Langfristige Perspektive ab 2030

Mit der weiteren Migration zur TI 2.0 entsteht ein stärker standardisiertes und besser steuerbares Plattformmodell auf Basis souveräner Cloud-Technologien und des Healthcare Confidential Computings. Die Zahl von Sonderlösungen und schwer kontrollierbaren Übergängen wird reduziert. Post-quanten-sichere Verfahren werden für Datenübertragung und Datenspeicherung in der Breite der TI wirksam sein. Detektions- und Reaktionsprozesse können auf einer konsolidierten Datengrundlage stärker automatisiert werden. Die Umstellung bestimmter Signaturkomponenten wird über 2030 hinaus fortgeführt, sobald Standards und geeignete Geräte verfügbar sind.

Die gematik überprüft regelmäßig die Umsetzung in allen Entwicklungsschritten. Operative Reviews bewerten den Fortschritt in den einzelnen Handlungsfeldern. Strategische Reviews beziehen interne und externe Partner ein und ermöglichen Anpassungen an neue Bedrohungen, Technologien sowie Erfahrungen aus dem Betrieb.

Handlungsfeld	Kurzfristig (2026)	Mittelfristig (bis 2028)	Langfristig (2030+)
Governance	→ Weiterentwicklung TI-Security-Standard & Security Governance Lifecycle → Schärfung der Sanktionsmechanismen → Reality Checks mit neuen Stakeholder-Gruppen	→ Umsetzung des ganzheitlichen Governance-Modells (Kontroll-, Einfluss- & Umfeldbereich) → Operationalisierung neuer gesetzlicher Mandate	→ gematik als zentrale Sicherheitsagentur für das deutsche digitale Gesundheitswesen → Etablierter Partner gegenüber europäischen DiHAs
Sicherheits-architektur	→ Einführung Zeta-Guard → Konzeption modularer Sicherheitsbausteine (Referenz Architektur)	→ Ausrollen erster zentraler Plattform-Services nach Einmaligkeitsprinzip → Zero-Trust-Zugriffssteuerung Ende-zu-Ende → Start PQC-Migration	→ Vollständige TI 2.0 auf souveräner Cloud (HCC) → Komplexitätsreduktion der Infrastruktur → PQC in der Breite wirksam
Reaktionsfähigkeit & Resilienz	→ Security-Monitoring-Strategie 2.0 (Detektion & Verifikation) → Aufbau SIEM-Plattform & erste KI-gestützte Anomalieerkennung	→ Ende-zu-End-Umfeldbetrachtung (Attack Surface Monitoring) → 24/7-Leitstand & SOC vollständig etabliert	→ Automatisierte, KI-gestützte Detektions- & Reaktionsprozesse → Resilienz als eigenständiges Sicherheitsziel operativ verankert
Kooperation & Kommunikation	→ Aufbau strukturierter Austauschformate mit europäischen DiHAs → Ausbau CVDP	→ Board of Trust operativ → Gemeinsame Threat-Intelligence-Plattform mit BSI & EU-Partnern	→ Belastbare grenzüberschreitende Incident- & Krisenkoordination im EHDS

Abbildung 9: Übersicht der strategischen Meilensteine, Handlungsfelder & Maßnahmen

Fazit

Die Sicherheitsstrategie 2030 setzt einen Rahmen für die Weiterentwicklung der TI. Ihr Erfolg zeigt sich in ihrer Wirkung: Risiken werden früher erkannt, Vorfälle schneller begrenzt, Schutzmaßnahmen nachvollziehbar verbessert und digitale Versorgungsprozesse auch unter Belastung unterstützt. Dabei antizipiert die Sicherheitsstrategie die technologische Weiterentwicklung, geopolitische Herausforderungen und damit verbundene hybride Bedrohungslagen sowie sich verändernde Motive und Methoden in der Cyberkriminalität.

Version: 1.0
Stand: 4. September 2026
Status: Erste finale Version

Herausgeber:
gematik GmbH
Rosenthaler Straße 30 | 10178 Berlin
© gematik GmbH
www.gematik.de