

Technologieradar 2025

IT-Perspektiven und -Trends
für den Public Sector

Technologieradar 2025

IT-Perspektiven und -Trends
für den Public Sector

Vorwort der BRZ-Geschäftsführung

Die aktuelle Ausgabe des BRZ-Technologieradars liefert eine Einschätzung unserer BRZ-Expertinnen und -Experten zu den Einsatzmöglichkeiten aktueller IT-Trends und zukunftsweisender Technologien im öffentlichen Sektor. Das BRZ ist das Kompetenzzentrum für die Digitalisierung in der Bundesverwaltung und hat den Anspruch, technologische Entwicklungen frühzeitig zu erkennen sowie Chancen und Risiken des Technologieeinsatzes auszuloten.

Künstliche Intelligenz im Vormarsch

Insbesondere im Bereich der generativen künstlichen Intelligenz wurden in den letzten Jahren enorme Fortschritte erzielt. Mit der zunehmenden Verbreitung von KI-Anwendungen und -Modellen stehen Unternehmen weltweit vor der Herausforderung, einen sicheren und verantwortungsvollen Umgang mit KI-Anwendungen zu finden. Möglichen Effizienzgewinnen stehen hohe Anforderungen an Bias-Mitigation, Datenschutz und Datensicherheit gegenüber. Im Schwerpunktkapitel zeigen BRZ-Expertinnen und -Experten mögliche Anwendungsfälle für generative KI in der Softwareentwicklung. Einen weiteren Schwerpunkt setzen wir zum Thema „Digitaler Humanismus“, bei dem die Entwicklung menschenzentrierter digitaler Lösungen im Fokus steht.

Nachhaltigere Rechenzentren im Fokus

Eng verbunden mit dem Thema künstliche Intelligenz ist auch die Frage der Nachhaltigkeit und Umweltverträglichkeit der Technologie. Aktuell führt der KI-Trend zu einem erhöhten Strombedarf in den darauf spezialisierten Rechenzentren. Im BRZ beschäftigen wir uns bereits seit vielen Jahren mit dem Thema „Nachhaltige Technologien“ und passen unsere Rechenzentrums- und Büroinfrastruktur Schritt für Schritt an. Durch den verantwortungsvollen Einsatz von KI, aber auch durch den Einsatz moderner Softwarelösungen wie Cloud-Anwendungen oder Server-Virtualisierung können Ressourcen geschont und das Konzept „Green IT“ besser umgesetzt werden.

Roland Ledinger
Geschäftsführer BRZ

Christine Sumper-Billinger
Geschäftsführerin BRZ





Inhalt

5 Vorwort der BRZ-Geschäftsführung

8 Technologieradar 2025

25 BRZ-Schwerpunktthemen

26 Nachhaltige
Informationstechnologie

40 Künstliche Intelligenz in der
Softwareentwicklung

54 Cyber Threat Intelligence
(CTI)

64 Digitaler Humanismus

*Sie wollen noch
mehr über das BRZ
und seine Produkte wissen?
Bestellen Sie den
BRZ-Newsletter auf brz.gv.at*



Technologieradar 2025

Technologiemanagement bildet die Basis für innovative Lösungen für unsere Kunden und den technologischen Fortschritt des Unternehmens. Das BRZ prüft Trends und Technologien in Richtung ihrer Anwendbarkeit für den öffentlichen Sektor. Für das Technologieradar 2025 wurden eine Reihe von Trends und Technologien konsolidiert oder aus dem Radar entfernt, da sie bereits Produktreife erlangt haben oder mittlerweile obsolet geworden sind.



Als Teil der BRZ-Strategie ist das Technologiemanagement, angesiedelt im Bereich des Enterprise-Architekturmanagements, die Basis für innovative Solutions für unsere Kunden und den technologischen Fortschritt des Unternehmens insgesamt. Das BRZ prüft Trends vor allem in Richtung ihrer Anwendbarkeit für den öffentlichen Sektor. Auch für das Technologieradar 2025 wurden wieder neue Technologien untersucht. Technologien, die bereits in bestellbaren BRZ-Produkten zum Einsatz kommen, werden sukzessive aus dem Radar entfernt.

Das BRZ-Technologieradar unterstützt bei der Identifikation, Auswahl und Bewertung von Technologien sowie anderen organisationsrelevanten Schwerpunkten und bringt diese in einer Grafik („Radar“) übersichtlich auf den Punkt. Im Radar 2025 wird die bewährte Aufteilung in die Kernbereiche „Technologie“, „Geschäftstrends“, „Touchpoint“ und „Methoden und Arbeitsweisen“ weitergeführt.

Neuerungen im Technologieradar 2025

Neunzehn Trends und Technologien wurden neu hinzugefügt:

- | | |
|--|-------------------------------|
| 1. Artificial General Intelligence (AGI) | 11. DNA Storage |
| 2. IT for Green | 12. DNA Computing |
| 3. Artificial Intelligence | 13. Edge Computing |
| 4. Synthetic Data | 14. Quantum Computing |
| 5. Neuromorphic Computing | 15. AI Augmented Development |
| 6. Homomorphic Encryption | 16. Machine-Learning-Methoden |
| 7. AI Supercomputing | 17. Responsible AI |
| 8. Large Action Model (LAM) | 18. CTI/CTEM |
| 9. Large Recurrent Action Model (LRAM) | 19. Digitale Kompetenz |
| 10. Agentic AI | |

Einige Trends und Technologien konnten nicht den Erwartungen entsprechen oder wurden begrifflich konsolidiert:

- **Web3** hat sich als Buzzword mit falschen Versprechungen herauskristallisiert. Die versprochene „Dezentralisierung des Web“ ist nicht zu erwarten.
- **Metaverse**: Diese stark mit Virtual-Reality-Anwendungen verbundene Technologie scheitert vorerst an zu vielen Einzelinteressen von IT-Industrie bzw. deren großen Playern und mangelnder Akzeptanz bei Usern. Dem gegenüber steht kein erkennbarer Business Need bei potenziellen Kunden. Es ist aus heutiger Sicht nicht mit einer Realisierung vor 2040 zu rechnen.

- **Bring Your Own Environment (BYOE):** Unternehmen und Behörden setzen weiterhin auf sichere „managed devices“.
- **Anything as a Service:** XaaS ist zu unspezifisch für den Einsatz in der Verwaltung.
- **Natural Language Processing (NLP), Machine Learning & ML OPs, Retrieval Augmented Generation** und **Kognitive Services:** Diese Technologien stehen stark in Zusammenhang mit KI-Technologien, insbesondere der generativen KI (Gen AI), werden daher nicht mehr gesondert betrachtet und unter dem Begriff „Artificial Intelligence“ konsolidiert.
- Der **Digital Twin** wird nur mehr als Citizen Twin näher betrachtet.
- **Supply unchained** wird nicht mehr gesondert aufgeführt, sondern in Zusammenhang mit Green IT betrachtet.
- Der Trend der **Personalisierung** wird als Teilaspekt innerhalb der Total Experience betrachtet.
- **Accelerated Legacy Modernization** wurde als Aspekt in Hyperautomation integriert.

Bereits im Status der Produktreife:

- integrierte One Stop Shops
- Digital Identity Ecosystems (Beispiel: ID Austria)
- Data Analytics
- Cloud Transformation ist als Business Trend realisiert.

Zusammengezogen und/oder neu zugeordnet:

- Die Trends **Wissenstransfer** und **Lebenslanges Lernen** wurden vereint und nunmehr unter dem Begriff Wissensmanagement geführt.
- Die Trends/Technologien **Intelligente Sicherheit, Cybersecurity und Cybersecurity Mesh** wurden unter dem Begriff Cybersecurity zusammengefasst.
- **KI-Spezialtechnologien** aus 2024 wurden in den Geschäftstrend Artificial Intelligence verschoben.
- **Supply Chain** wird als Aspekt der IT-for-Green-Thematik verstanden.
- **Personalisierung** wurde mit Total Experience verschmolzen und in den Kernbereich Geschäftstrends verschoben.
- **Intelligent Process Automation (IPA)** ist nunmehr dem Kernbereich Methoden und Arbeitsweisen zugeordnet und dient dem Geschäftstrend Hyperautomatisierung.
- Die Technologie **Hyperautomation** umfasst jetzt die Aspekte IPA, Robotic Process Automation (RPA) und Intelligente Automatisierung.



Abbildung 1:

Technologieradar 2025

Geschäftstrends



Touchpoint

Legende: 2025 neu aufgenommen bereits im Radar angeführt

Technologie



Beobachten

LAM

6G

Näher Betrachten

Edge Computing

Homomorphic Encryption

AI Supercomputing

Ausprobieren

IoT

5G

Low-Code-/ No Code-Plattformen

Agentic AI

Quanten-Computing

Generative KI

LLM

LRAM

DNA Computing

Einführen

Cybersecurity

Neuromorphic Computing

DNA Storage

Digital Core

Synthetic Data

Zero Trust

Agile Cultural Mindset

Machine-Learning-Methoden

Prompt Engineering

Anonymisierung

Data Governance

Intelligenter Arbeitsplatz

Tokenization

AI Augmented Development

CTI/CTEM

Responsible AI

Methoden & Arbeitsweisen



 **Technologie**

Begriff	Anwendung im Public Sector	Status
<p>NEU Quanten-Computing</p>	<p>Quanten-Computing wird herkömmliche Computer nicht ersetzen. Services, die auf Quanten-Computing basieren, werden eher als Cloud-Service konsumierbar sein. Anwendungsgebiete, die das Potenzial für Realisierung haben, sind etwa:</p> <ul style="list-style-type: none"> - Optimierungsaufgaben, z. B. in den Bereichen Finanzwirtschaft und Logistik sowie Optimierungen von Forschungsmodellen - Simulationen, beispielsweise um neue chemische Stoffe für Biotechnologie oder Medikamente zu erforschen - maschinelle Lernverfahren, etwa als quantenmaschinelles Lernen für verschiedenste Aufgabengebiete wie etwa Mustererkennung - die Generierung von echten Zufallszahlen <p>Quanten-Computing könnte auch die Geschwindigkeit und/oder Qualität von maschinellem Lernen verbessern. Anders als bei der Computing-on-Silicon-Technologie gibt es für Quantencomputer keine einheitlich definierte physische Rechenschicht und es ist daher nicht möglich, plattformübergreifende Services auf Quantenebene zu kombinieren. Dies führt zu einer sehr großen Vielfalt potenzieller Plattformen und daraus folgender Inkompatibilitäten. Der Markt ist stark fragmentiert, Investitionen werden aktuell zurückgefahren.</p>	<i>Beobachten</i>
<p>NEU DNA Computing</p>	<p>DNA Computing nutzt DNA-Moleküle anstelle von Bits für parallele Berechnungen. Es verwendet Milliarden verschiedener Moleküle, um massive parallele Prozesse effizient durchzuführen, und könnte in bestimmten Fällen schneller und energieeffizienter arbeiten als klassische Methoden. Während es traditionelle Systeme nicht ersetzt, kann es bei spezifischen Rechenaufgaben hilfreich sein. In acht bis zehn Jahren könnte DNA Computing große datenintensive Parallelverarbeitungsaufgaben übernehmen.</p>	<i>Beobachten</i>
<p>NEU DNA Storage</p>	<p>Täglich werden weltweit mehrere Hundert Petabyte an neuen Daten erzeugt. Ein einziges Gramm DNA könnte diese Datenmenge speichern.</p> <p>Bei der DNA-Speicherung handelt es sich um den Prozess der Kodierung und Dekodierung binärer Daten in und aus synthetisierten DNA-Strängen. Binäre Sequenzen können in DNA-Sequenzen kodiert werden, die synthetisiert und gespeichert werden können. Um die Daten abzurufen, muss das DNA-Molekül sequenziert und dekodiert werden. DNA ist aufgrund der Dichte, Haltbarkeit und Nachhaltigkeit ein potenziell attraktives Medium für die Archivierung von Daten.</p> <p>Aufgrund der Fähigkeit, Fehlerprüfungen und Selbstreparaturen durchzuführen, kann DNA als Datenspeichermedium und Computerplattform für Anwendungen geeignet sein.</p> <p>Daten in DNA-Speichern können im Vergleich zu aktuellen Technologien Tausende von Jahren unverändert überdauern und bleiben frei von Qualitätsverlust oder Laufwerksausfällen. In datenintensiven Branchen wird es voraussichtlich in etwa acht Jahren ein vollständiges DNA-Ökosystem als konsumierbares Unternehmensprodukt geben. Zu den Branchen gehören das Gesundheitswesen, das Bankwesen, das Finanzwesen, das Versicherungswesen, die Versorgungswirtschaft und der öffentliche Sektor. Die Verteidigungs-, Forschungs- und Geheimdienstgemeinschaften werden voraussichtlich die ersten Anwender sein.</p>	<i>Beobachten</i>

Begriff	Anwendung im Public Sector	Status
6G	6G ist der generische Name für den Mobilfunk der nächsten Generation. Die sechste Generation des Mobilfunks wird die aktuellen 5G-Fähigkeiten verbessern und diese hinsichtlich Spitzendatenrate (z. B. 100 Gbps bis 1 Tbps), Verbindungsdichte und Energieeffizienz deutlich übertreffen. Funktionen und der Zeitplan für 6G sind noch nicht final definiert, der kommerzielle Start ist um 2030 zu erwarten. Wichtig erscheint seit 5G auch die Verkürzung der Latenzzeit, damit Ortung und Lokalisierung wirklich im Sub-Meterbereich möglich wird. Das ist eine Voraussetzung für selbstfahrenden Verkehr und ähnliche Anwendungen.	<i>Beobachten</i>
NEU Homomorphic Encryption	Homomorphe Verschlüsselung (HE) ermöglicht Berechnungen mit verschlüsselten Daten. Dies erlaubt die vertrauliche Verarbeitung von Daten ohne Klartext. HE lässt vertrauliche Datenverarbeitung zu, die bisher durch Datenschutz nicht möglich war. Technisch basiert HE auf Gitterverschlüsselung (Postquantenkryptografie). Mögliche Einsatzgebiete: <ul style="list-style-type: none"> – Analysen der Daten im verschlüsselten Zustand, sodass Daten nie im Klartext gesehen und dennoch genaue Ergebnisse erzielt werden – Teilen und Bündeln von Daten unter Vertragsteilnehmenden – Freigabe von Benutzerdaten bei gleichzeitigem Schutz der Privatsphäre 	<i>Näher betrachten</i>
NEU Neuromorphic Computing	Neuromorphic Computing ahmt das Gehirn mit digitalen oder analogen Techniken nach und verspricht Effizienzsteigerungen bei rechenintensiven Aufgaben. Neuromorphe Systeme nutzen Spiking Neural Networks (SNNs) statt Deep Neural Networks (DNNs) und können mit kleineren Datensätzen trainiert werden, da sie einfache Verarbeitungselemente und hohe Interkonnektivität kombinieren. Diese Architektur bietet hohe Leistung bei geringem Stromverbrauch und eignet sich ideal für Mustererkennung und Signalanalyse.	<i>Näher betrachten</i>
NEU AI Supercomputing	AI Supercomputing kombiniert moderne Rechenbeschleuniger, Spezialsoftware, Hochgeschwindigkeitsnetzwerke und leistungsoptimierten Speicher, um das Training und die Bereitstellung komplexer KI-Modelle zu beschleunigen. Diese GPU-basierte Technologie bringt geostrategische Herausforderungen mit sich, da 92 Prozent der Chips vom taiwanesischen Hersteller TSMC stammen. Die Technologie erhöht den Energieverbrauch der KI-Rechenzentren deutlich und führt zu Engpässen in deren Energieversorgung.	<i>Beobachten</i>
NEU Large Action Models (LAM)	LAM kann man als Iteration der Large Language Models (LLM) verstehen oder als Kombination von LLM mit KI-Agenten. Durch die Kombination von LLM und LAM können Benutzer:innen Ziele in natürlicher Sprache formulieren, während LAM die erforderlichen Aktionen planen und KI-Agenten einsetzen, um diese umzusetzen. LAM ermöglichen intuitive, flexible und personalisierte Interaktionen und könnten die UI/UX grundlegend verändern. Voraussetzung ist die Interoperabilität vieler Dienste. Hindernisse auf dem Weg zum LAM sind der hohe Rechenbedarf und Energieaufwand sowie fehlendes Vertrauen in die Zuverlässigkeit der zukünftigen Technologie.	<i>Beobachten</i>
NEU Agentic AI	Bei Agentic AI geht es um den nächsten Schritt in der Funktionalität von KI-Tools: Sind die bisherigen Chatbots als Content-Erzeuger bekannt, werden die KI-Agenten (Agents) Aktionen ausführen und autonome Entscheidungen treffen können. Die Marktdurchdringung soll von einem Prozent im Jahr 2024 auf 33 Prozent bis 2028 steigen. 15 Prozent der täglichen Arbeitsentscheidungen werden dann durch agentenbasierte KI getroffen.	<i>Näher betrachten</i>

Begriff	Anwendung im Public Sector	Status
NEU Large Recurrent Action Model (LRAM)	Aktuell basieren KI-Dienste hauptsächlich auf LLM und Transformer-Architektur. Für Echtzeitanwendungen (z. B. mobile Roboter, autonome Fahrzeuge) sind diese Modelle aus heutiger Sicht nicht geeignet. Erste Ergebnisse aus der modernen Forschung zeigen, dass LRAM im Vergleich zu Transformern sowohl in Bezug auf Leistung als auch Geschwindigkeit eine geeignete technologische Weiterentwicklung sein kann.	Näher Betrachten
NEU Edge Computing	Edge Computing ist die Technologie für die Verarbeitung von Daten nahe der Quelle ihrer Entstehung, also dort, wo vernetzte Geräte (Internet of Things/IoT) und Menschen Informationen erzeugen oder nutzen. Dies verbessert Latenz, Bandbreite, Autonomie und Sicherheitsaspekte, was zu mehr Nachhaltigkeit führt. Edge-Computing-Standorte befinden sich zwischen der Edge (nahe den Sensoren) und dem Core (Cloud oder zentrales Rechenzentrum). Obwohl Edge Server und Zero-Touch-Software (keine menschlichen Eingriffe notwendig) noch nicht vollständig ausgereift sind, treiben das Internet of Things und die Vernetzung ihre Entwicklung voran.	Näher Betrachten
NEU Synthetic Data	Synthetische Daten sind Daten, die künstlich generiert werden. Synthetische Daten werden als Ersatz für reale Daten in einer Vielzahl von Anwendungsfällen verwendet, darunter Datenanonymisierung, Entwicklung von KI und maschinellem Lernen (ML), datenschutzgerechte Weitergabe von Daten usw. Die zeitaufwendige und teure Aufgabe der Erstellung von Testdaten kann durch synthetische Daten obsolet werden. Einsatzzwecke sind in vielen Bereichen zu sehen, in der Medizin, in der Verwaltung, im Softwaredesign - und natürlich können mit synthetischen Daten auch KI-Modelle verbessert werden.	Ausprobieren
Low Code / No Code-Plattformen (LC/NC)	Entwickler:innen und Engineers sind gefragte Arbeitskräfte, und die digitale Transformation führt zu einer steigenden Nachfrage auf dem Arbeitsmarkt. Für diese Zielgruppe stellen KI-Copilots eine passende unterstützende Technologie dar. LC/NC-Plattformen haben das Potenzial, aus allen Mitarbeitenden Technologinnen bzw. Technologen zu machen und so zur Demokratisierung der Technologie- und Datennutzung beizutragen. Auch die Low-Code-/No-Code-Plattformen können mit KI-Technologien kombiniert werden. Beide Technologien existieren aktuell nebeneinander, jedoch ist eine weitergehende Integration zu erwarten.	Ausprobieren
5G	5G ist ein in Ausbau begriffener Mobilfunkstandard und birgt viel Potenzial: Das 5G-Satellitenspektrum wird es ermöglichen, über Low-Orbit-Satelliten zu kommunizieren und damit praktisch eine weltweite Abdeckung für 5G-kompatible Endgeräte zu erreichen. Der Netzausbau ist in den österreichischen Ballungsräumen mittlerweile auf hohem Niveau, Endgeräte der neueren Generationen sind bereits 5G-tauglich. Durch die Nutzung des Millimeterwellenspektrums sind sehr hohe Datendurchsätze von vielen Endgeräten gleichzeitig möglich, allerdings nur mit kleiner Reichweite. Hier sind in Zukunft insbesondere IoT Use Cases zu verorten, der Einsatz im Bereich des Public Sectors entwickelt sich laufend.	Ausprobieren
Large Language Models (LLM)	Large Language Models (LLM) sind die technologische Basis der bekannten KI-Web-Tools namhafter Softwareentwickler (z. B. ChatGPT). Durch die Verarbeitung riesiger Datenmengen mit der Transformer-Technologie ermöglichen LLM, für Menschen verständliche Inhalte zu generieren. Die Modalität ist dabei nicht auf Text bzw. Sprache beschränkt, andere Modalitäten sind etwa Bilder, Videos und Audio. LLM sind für die Verarbeitung riesiger Datenmengen gebaut, allerdings ist ihr Ressourcenverbrauch sehr hoch. 2025 sind erste Stimmen zu hören, dass die Weiterentwicklung der KI auf der bestehenden Transformer-Technologie an ihre Grenzen stößt. Im Bereich des Public Sectors werden bereits Proof of Concepts (PoCs) umgesetzt. Eine Herausforderung ist die sichere und performante Umsetzung von LLM „on premise“. Die Umsetzung über Cloud-Infrastruktur ist bereits weiter fortgeschritten und wird produktiv eingesetzt.	Ausprobieren

Begriff	Anwendung im Public Sector	Status
Internet of Things (IoT)	IoT (Internet of Things) ist ein Sammelbegriff für physische und virtuelle Objekte, die über das Internet vernetzt sind. Mit zunehmender Energieeffizienz von Sensoren und der Verlagerung der Datenbearbeitung und Speicherung in die Peripherie (Edge) wird diese Technologie ein starker Treiber für mannigfaltige Use Cases: autonomes Fahren, Supply Chain Tracking, Smart-City-Projekte, Mautsysteme, Verkehrsleitsysteme, Automatisierung, landwirtschaftliche Nutzung etc.. Wichtige beteiligte Technologien sind 5G und Edge Computing.	<i>Ausprobieren</i>
Generative KI	Unter generativer KI versteht man die Fähigkeit von KI-Modellen, mit menschlicher Kommunikation neue Variationen von Inhalten von Bildern, Videos, Audio und Text zu erstellen bzw. auch Bilder, Texte etc. zu analysieren. Generative KI-Anwendungen haben das Potenzial, Menschen durch ein breites Spektrum an Aufgaben zu unterstützen, wodurch die Produktivität gesteigert, Kosten gesenkt und neue Wachstumschancen eröffnet werden. Generative KI-Plattformen haben sich etabliert und die prinzipielle Nützlichkeit ist anerkannt. Der Hype zur generativen KI ist ungebrochen und die Entwicklung geht rasant weiter. Die Integration in Unternehmenslösungen ist der nächste Schritt. Die großen Technologieanbieter wetteifern um die besten Produkte hinsichtlich Integration, Sicherheit, Funktionalität und Preis. Die technologische Basis sind LLM mit Transformer-Technologie.	<i>Einführen</i>
Digital Core	Der „Digital Core“ bezeichnet das zentrale digitale Fundament eines Unternehmens. Es umfasst Software (wie ERP-Systeme), Datenbanken, Cloud-Infrastruktur, Analyse-Tools und digitale Prozesse. Der digitale Kern ermöglicht die Automatisierung von Geschäftsprozessen, effizientes Datenmanagement und die Nutzung von Echtzeitinformationen. Ein starker digitaler Kern ist entscheidend für Wettbewerbsfähigkeit und Anpassung an eine digitalisierte Welt. Digital-Core-Initiativen sind oft mit der Transformation in die Cloud verbunden.	<i>Einführen</i>
Cybersecurity	Cybersecurity beschreibt den aktiven Schutz von Computersystemen, Netzwerken und Programmen vor digitalen Angriffen. Ein umfassender Schutz reicht von der Aufklärung der Mitarbeiter:innen über Prozesse im Arbeitsumfeld bis hin zu eingesetzten Technologien und Softwareprodukten. Das Vertrauen der Nutzer:innen ist hier zu stärken, diese müssen sich auf die Datensicherheit verlassen können. Eine der Maßnahmen dafür ist ein Identitätsmanagement der nächsten Generation zur Erhöhung des Schutzes und des Vertrauens. Cybersecurity Mesh Architecture ist ein Begriff, der sich auf ein Netzwerk von Sicherheitsmaßnahmen und -technologien bezieht, die eine nahtlose Integration von Sicherheitslösungen und eine verbesserte Reaktionsfähigkeit auf Angriffe ermöglichen. Das Zero-Trust-Konzept ist die methodische Grundlage dieses Trends. Die Technologien oder Technologiekombinationen sind die Antwort auf die exponentiell gestiegenen Sicherheitsanforderungen im modernen Cloud-Computing und Mobile Working. Mit dem Schlagwort Intelligente Sicherheit fließt auch immer mehr KI-Technologie in die Security-Produkte der Hersteller ein.	<i>Einführen</i>



Geschäftstrends

Begriff	Anwendung im Public Sector	Status
<p>NEU</p> <p>Allgemeine Künstliche Intelligenz / Artificial General Intelligence (AGI)</p>	<p>Allgemeine Künstliche Intelligenz (AGI) ist die Intelligenz einer Maschine, die jede intellektuelle Aufgabe erfüllen kann, die ein Mensch ausführen kann. Diese Eigenschaft wird zukünftigen autonomen KI-Systemen zugeschrieben. Ergebnisse sollen in einer Vielzahl realer oder virtueller Umgebungen dem eines Menschen vergleichbar sein. AGI kann auf ein viel breiteres Spektrum von Use Cases angewendet werden und umfasst kognitive Flexibilität, Anpassungsfähigkeit und allgemeine Problemlösungsfähigkeiten. Dieser Hypothese stehen noch keine technologischen Grundlagen gegenüber.</p>	<p><i>Beobachten</i></p>
<p>Diversity, Equity and Inclusion in IT (DEI)</p>	<p>Das DEI-Akronym steht für Prinzipien, die eine diverse und inklusive Arbeitsumgebung schaffen. Hier wird jeder Mitarbeiterin unabhängig von ethnischer Zugehörigkeit, Geschlecht, sexueller Orientierung oder Religion fair behandelt. DEI fördert Chancengleichheit, Respekt und Wertschätzung. Es trägt zur positiven Unternehmenskultur bei und unterstützt die Entwicklung besserer Softwarelösungen, die unterschiedliche Benutzergruppen berücksichtigen, wie User Experience, Bias-Vermeidung und Barrierefreiheit.</p>	<p><i>Näher betrachten</i></p>
<p>Citizen Twin / Invisible Citizens</p>	<p>Digitale Modelle von Bürgerinnen und Bürgern werden erstellt, um Statistiken zu generieren, die Verwaltungsbehörden bei Entscheidungen unterstützen, beispielsweise bei der Ausrichtung medizinischer Behandlungen oder der Identifikation sicherheitsrelevanter Entwicklungen in sozialen Medien. Aggregierte Versionen dienen dazu, breitere Muster, Ressourcennutzung und gesellschaftliches Verhalten zu erkennen. Dabei sind stets strenge Datenschutz- und Ethikrichtlinien anzuwenden.</p>	<p><i>Näher betrachten</i></p>
<p>NEU</p> <p>SCHWERPUNKTTHEMA</p> <p>IT for Green</p>	<p>Daten und Informationstechnologie können dazu beitragen, den Ressourcenverbrauch zu optimieren. Wichtige Umsetzungen sind in der Supply Chain und in der Industrieproduktion zu erwarten oder bereits Realität. Die User Experience steigt durch diese detaillierte Information deutlich. Technologische Treiber sind Internet of Things (IoT), Edge Computing und Robotic Process Automation, übergeordneter Geschäftstrend ist Nachhaltigkeit und Total Experience.</p>	<p><i>Ausprobieren</i></p>
<p>Hyperautomation</p>	<p>Hyperautomatisierung in der Verwaltung ist ein systematischer Ansatz, um so viele Geschäfts- und IT-Prozesse wie möglich schnell zu erkennen, zu prüfen und in IT-Systemen zu automatisieren. Es umfasst die koordinierte Nutzung verschiedener Technologien, Werkzeuge oder Plattformen wie KI, robotergesteuerte Prozessautomatisierung sowie Low-Code/No-Code-Ansätze. Methodisch kommt dabei Intelligent-Process-Automation zum Einsatz. Automatisierungsprogramme werden häufig parallel zu Legacy-Modernisierungsinitiativen gestartet, um veraltete Architekturen, Hardware- und Softwareanwendungen durch moderne Lösungen zu ersetzen. Es existieren verschiedene Modernisierungsansätze; typischerweise werden Anwendungen im Rahmen solcher Programme auf ein Cloud-Bereitstellungsmodell migriert. Im BRZ steht mit der Containerplattform PaaS eine geeignete Umgebung für die Modernisierung von Altsystemen zur Verfügung.</p>	<p><i>Ausprobieren</i></p>
<p>Data Driven Decision Support</p>	<p>Entscheidungsintelligenz in der Verwaltung verbessert Entscheidungen durch das Verständnis ihrer Prozesse und durch Feedback. Sie versteht, wie Entscheidungen getroffen werden und wie ihre Ergebnisse durch Rückmeldung bewertet und verbessert werden. Sie nutzt systematisch datengesteuerte Technologien wie KI und Analytik. Diese Intelligenz gilt für strategische, managementbezogene und operative Entscheidungen.</p>	<p><i>Ausprobieren</i></p>

Begriff	Anwendung im Public Sector	Status
Digitale Souveränität des Staates	Durch die zunehmende Digitalisierung der Verwaltung und deren Services ist besonderes Augenmerk darauf zu legen, dass die eingesetzten IT-Produkte und -Dienstleister die digitale Souveränität (u. a. durch Herstellerabhängigkeit, rechtliche Bedingungen je Anbieter-/ Datenstandort, Informationssicherheit) nicht schwächen oder gar sukzessive abbauen. Digitale Souveränität ist auch ein wesentlicher, gesamteuropäisch zu betrachtender Aspekt bei der Verwendung von Cloud-Services für die öffentliche Verwaltung und beim Einsatz von Open-Source- Software.	<i>Ausprobieren</i>
NEU Artificial Intelligence (AI) / Künstliche Intelligenz (KI)	Jedes Quartal werden neue KI-Lösungen auf den Markt gebracht, die Entwicklung ist enorm, der Ressourcenverbrauch durch die erforderlichen Computersysteme ebenfalls. Die Technologien beginnen sich zu diversifizieren, ebenso beginnt sich die Infrastruktur den Erfordernissen anzupassen. Technologische Treiber sind ML, NLP, Kognitive Services, RAG, LLM und LRAM. Die drei wesentlichen methodische Grundlagen für das Training von KI im maschinellen Lernen sind überwachtes, unüberwachtes und bestärkendes Lernen (Supervised, Unsupervised und Reinforcement Learning).	<i>Ausprobieren</i>
Total Experience (TX)	Total Experience (Gesamterlebnis) ist ein Ansatz, der die Disziplinen User Experience (UX), Citizen/Constituent Experience (CX), Employee Experience (EX) und Multi-Experience (MX) für eine ganzheitlichere Servicegestaltung und -bereitstellung kombiniert. Eine TX-Strategie verknüpft digitale und nicht digitale Techniken aus den Disziplinen CX, EX, UX und MX, um das Vertrauen von Bürgerinnen und Bürgern sowie Mitarbeitenden in die und die Zufriedenheit mit den staatlichen Dienstleistungen zu steigern und Services zu personalisieren. Personalisierung soll eine maßgeschneiderte direkte Ansprache ermöglichen, die auf individuelle Bedürfnisse und Anforderungen von Kunden eingeht.	<i>Einführen</i>
SCHWERPUNKTTHEMA Nachhaltigkeit (Sustainable Technology)	Informationstechnologie ist ein zentraler Baustein bei der Frage, wie Ressourcenschonung und Nachhaltigkeit in der Wirtschaft umgesetzt werden können. Die IT selbst ist dabei möglichst nachhaltig zu gestalten: Zurzeit haben Technologien, die das größte Potenzial zur Verbesserung der Nachhaltigkeit haben, auch den größten ökologischen Fußabdruck.	<i>Einführen</i>
Wissensmanagement	Mit dem Ausscheiden erfahrener Mitarbeiter:innen aus Unternehmen oder Organisationen – insbesondere auch in der Verwaltung – gehen wertvolle Kenntnisse und Erfahrungen verloren. In dieser Hinsicht ist es unabdingbar, auf technologische Lösungen zu setzen, um dieses Wissen zu dokumentieren, zu speichern und nahtlos zu übertragen. Digitale intelligente Lösungen, vernetzte Wissensdatenbanken und Kollaborations-Tools erleichtern die Erfassung und Weitergabe des Know-hows der ausscheidenden Mitarbeiter:innen. Der gezielte Einsatz von Wissensmanagementtechnologie gewährleistet, dass Organisationen in Zeiten des demografischen Wandels effektiv und effizient in der Verwaltung und Erfüllung ihrer Aufgaben bleiben und ihr technologisches Potenzial vollständig ausschöpfen können. Auch die Art und Weise, wie Unternehmen ihre Mitarbeiter:innen weiterbilden, ändert sich rasant. Digitale Trends kommen mit hohem Tempo und fordern Anpassungen an den Puls der digitalen Transformation. Die bevorstehende Pensionierungswelle im öffentlichen Dienst erfordert ein verstärktes Augenmerk auf ein effizientes Wissensmanagement.	<i>Einführen</i>



Touchpoint

Begriff	Anwendung im Public Sector	Status
NEU Digitale Kompetenz	Digitale Kompetenz (Digital Literacy) ist die Fähigkeit einer Person, Informationen auf digitalen Medienplattformen zu finden, zu bewerten und zu kommunizieren. Digitale Kompetenz vereint sowohl technische als auch kognitive Fähigkeiten. Sie besteht aus der Verwendung von Informations- und Kommunikationstechnologien zum Erstellen, Bewerten und Teilen von Informationen. Digitale Kompetenz kann verhindern, dass Personen online getäuscht werden, da Betrugsversuche oft Menschen ohne digitale Bildung irreführen können.	Einführen
Demokratisierung der Technologie	Technologie weltweit und breit zugänglich zu machen, ist durch moderne Ansätze möglich geworden. Der Zusammenfluss von Cloud Computing und Open Source hat neue Wege eröffnet, Technologien zu verbreiten. Generative KI erleichtert es Millionen von Benutzerinnen und Benutzern, die keine Programmierkenntnisse haben, traditionelle KI-Technologien sowie Low-Code-/No-Code-Plattformen zu nutzen. LLM-Plattformen ermöglichen es, Wissen in Unternehmen auf verständliche Weise zu übermitteln.	Ausprobieren
Augmented Reality / Virtual Reality	Die Erweiterung der Realitätswahrnehmung kann alle menschlichen Sinnesmodalitäten ansprechen. Unterstützende Geräte, wie beispielsweise größere AR- oder VR-Brillen, ermöglichen die Darstellung und gleichzeitige Wahrnehmung der physischen Realität in einer virtuellen Umgebung in Echtzeit. In der sogenannten „gemischten Realität“ wird die reale Welt mit der virtuellen Realität verknüpft. So können virtuelle Objekte in Aufnahmen einer Handykamera projiziert werden. Mixed Reality kann insbesondere die Durchführung von Tests für Prototypen unter realen Bedingungen erleichtern.	Ausprobieren
New Work	Die Lockdowns während der Pandemie waren ein wichtiger Faktor für den kulturellen und wirtschaftlichen Wandel in der Arbeitswelt, aber nicht der einzige. Die Grundlage dafür war bereits vorhanden: die digitale Transformation. Die Grenzen zwischen Arbeit und Freizeit verschwimmen zunehmend, was das Konzept des Work-Life-Blending anstelle der traditionellen Work-Life-Balance aufkommen lässt. Mit der Zunahme der Automatisierung von Aufgaben durch Maschinen stellt sich die Frage, welche Rolle der Mensch künftig einnehmen wird. HR-Abteilungen bemerken diese veränderten Bedingungen, und Unternehmen passen sich entsprechend an.	Einführen
Self Sovereign Identity (SSI)	Self Sovereign Identity (SSI) stellt einen bedeutenden Trend im Bereich der digitalen Identität dar, bei dem Einzelpersonen die Kontrolle über ihre digitalen Identitäten (Avatare) erhalten. Ziel ist es, das Vertrauen in Transaktionen mit Stakeholdern zu erhöhen. Die Europäische Union hat mit eIDAS ein kompatibles System für SSI entwickelt. Der Trend zur dezentralen Identitätsverwaltung und Bring Your Own Identity (BYOI) fordert traditionelle Konzepte der Identitätsverwaltung heraus oder erweitert deren Funktionen, um solche Szenarien zu ermöglichen, beispielsweise den digitalen Altersnachweis in der App „eAusweise“.	Einführen
Design for All	Design for All soll allen Bürgerinnen und Bürgern die Teilnahme an der Informationsgesellschaft ermöglichen, sowohl technologisch als auch nicht technologisch. Digitale Barrierefreiheit macht es Menschen mit Beeinträchtigungen möglich, mit Informationssystemen zu kommunizieren. Technologien wie Sprachassistenten und Screen-Reader fördern die Inklusion. Viele Staaten, darunter Österreich, haben Gesetze zur digitalen Barrierefreiheit erlassen.	Einführen

Begriff	Anwendung im Public Sector	Status
<p>SCHWERPUNKTTHEMA Digitale Ethik / Digitaler Humanismus</p>	<p>Digitale Ethik beschäftigt sich mit den Auswirkungen des digitalen Wandels auf den Menschen als Individuum und auf die Gesellschaft. Die wesentlichen Aufgaben der digitalen Ethik sind, konsistente Begründungen für moralisches Handeln und normative Standards zu erarbeiten sowie deren soziale Auswirkungen zu untersuchen. Ein weiterer Aspekt ist die digitale Gleichberechtigung, siehe DEI (Diversity, Equity, Inclusion). Digitale Ethik bietet auch den ethischen Rahmen für den Trend Responsible AI. Digitaler Humanismus ist ein Konzept, das die Beziehung zwischen Mensch und Technologie in den Mittelpunkt stellt, und zielt darauf ab, technologische Entwicklungen so zu gestalten, dass sie den Menschen dienen und humanistische Werte wie Mitgefühl, Ethik und soziale Verantwortung fördern.</p>	<p><i>Einführen</i></p>



Methoden & Arbeitsweisen

Begriff	Anwendung im Public Sector	Status
<p>NEU Verantwortungsvolle KI / Responsible AI</p>	<p>Verantwortungsvolle KI bezieht sich auf die Entwicklung und den Einsatz künstlicher Intelligenz unter Berücksichtigung ethischer, sozialer und rechtlicher Standards. Ziel ist es, sicherzustellen, dass KI-Systeme transparent, fair, sicher und im Einklang mit Werten und Gesetzen eingesetzt werden. Es konkretisiert Prinzipien der digitalen Ethik in der KI. Verantwortungsvolle KI erfordert die Zusammenarbeit von Fachleuten aus Informatik, Ethik, Recht und Sozialwissenschaften. Zu den Kernprinzipien gehören Transparenz, Fairness, Sicherheit, Datenschutz und Nachhaltigkeit. Verantwortungsvolle KI trägt dazu bei, das Vertrauen in KI-Technologien zu fördern und potenzielle negative Auswirkungen auf Gesellschaft und Individuen zu minimieren.</p>	<p><i>Näher betrachten</i></p>
<p>NEU SCHWERPUNKTTHEMA Cyber Threat Intelligence (CTI) / Continuous Threat Exposure Management (CTEM)</p>	<p>Threat Intelligence oder Cyber Threat Intelligence (CTI) umfasst die strukturierte Sammlung, Analyse und Verbreitung von Informationen über Cyberbedrohungen. Ziel ist es, Bedrohungen frühzeitig zu erkennen, zu verhindern und effektiv darauf zu reagieren, indem das Verhalten von Angreifern sowie deren Taktiken und Schwachstellen analysiert werden. Continuous Threat Exposure Management (CTEM), seit 2022 in der Cybersicherheit verwendet, beschreibt kein bestimmtes Produkt bzw. keine Technologie, sondern einen modernen Prozess. Es geht darum, Schwachstellen kontinuierlich zu identifizieren, zu bewerten, Risiken abzuleiten und deren Minderung zu priorisieren. Viele Sicherheitsprodukte integrieren diesen Ansatz mittlerweile in ihre Systeme.</p>	<p><i>Näher betrachten</i></p>
<p>NEU Machine-Learning-Methoden</p>	<p>Die drei wesentlichen methodische Grundlagen für das Training von KI im maschinellen Lernen sind:</p> <ul style="list-style-type: none"> - Überwachtes Lernen (Supervised Learning): Hierbei werden vorklassifizierte Trainingsdaten verwendet, die Methode ist für Klassifikations- und Regressionsaufgaben geeignet. - Unüberwachtes Lernen (Unsupervised Learning): Es sind keine vorklassifizierten Trainingsdaten erforderlich. Diese Methode ist gut geeignet, um bisher unbekannte Strukturen in Daten zu identifizieren. - Bestärkendes Lernen (Reinforcement Learning): In einer Simulationsumgebung wird durch Trial-and-Error gelernt, hierfür sind keine vordefinierten Trainingsdaten erforderlich. 	<p><i>Ausprobieren</i></p>

Begriff	Anwendung im Public Sector	Status
<p>NEU</p> <p>SCHWERPUNKTTHEMA</p> <p>AI Augmented Development</p>	<p>AI Augmented Development bezeichnet die Unterstützung und Erweiterung des Softwareentwicklungsprozesses durch den Einsatz künstlicher Intelligenz (KI). Dabei kommen KI-Tools zum Einsatz, um Entwicklerinnen und Entwicklern dabei zu helfen, effizienter zu arbeiten, qualitativ gleichwertig Software schneller zu erstellen und repetitive Aufgaben zu automatisieren. KI-Unterstützung gibt es für Design, Coding, Reengineering und Testing.</p> <p>Der Markt von Entwicklungs-Tools hat eine enorme Dynamik und praktisch kein Hersteller verweigert die Integration von KI.</p>	<i>Ausprobieren</i>
Tokenization	<p>Das Ersetzen sensibler Daten durch Tokens eröffnet zahlreiche neue und sichere Kommunikationsmöglichkeiten. Dadurch wird der Informationsaustausch zwischen Bürgerinnen und Bürgern sowie administrativen Stellen erheblich vereinfacht und effizienter gestaltet, während gleichzeitig ein deutlich erhöhter Schutz gewährleistet wird.</p>	<i>Ausprobieren</i>
Agile Cultural Mindset	<p>Ein Agile Cultural Mindset beschreibt die Einstellung eines Unternehmens, das in einem agilen Umfeld operiert. Dazu gehören Respekt, Zusammenarbeit, Verbesserungs- und Lernzyklen, Eigenverantwortung. Fokus auf die Wertschöpfung und die Fähigkeit, sich an Veränderungen anzupassen. Diese Einstellung ist wesentlich, um leistungsfähige, agile Teams zu entwickeln. Der Mehrwert für Kunden wird schnell sichtbar.</p>	<i>Einführen</i>
Prompt Engineering	<p>Die Aufgabe eines Prompt Engineers besteht darin, Abfragen zu formulieren und das LLM-System zu testen und zu optimieren. Ziel ist es, das LLM mit prompt-basierten Aufgaben zu trainieren. Anschließend kann das LLM als Service genutzt werden. Das kommandobasierte Eingabeparadigma wird durch die KI in ein neues Paradigma der absichtsbasierten Interaktion geändert, bei dem Benutzer:innen dem Computer mitteilen, was sie möchten, anstatt wie es umgesetzt werden soll.</p>	<i>Einführen</i>
Data Governance	<p>Data Governance umfasst die Erzeugung, die Sicherung und den Austausch von Daten in einem Unternehmen. Es beinhaltet Richtlinien und Prozesse, um Daten korrekt, konsistent, verfügbar, sicher und geschützt zu halten. Verantwortlichkeiten und Zuständigkeiten werden festgelegt, um Datenqualität, Datenschutz und Compliance-Standards sicherzustellen. Wichtige Aspekte sind Datenstandards, Metadatenmanagement, Datenklassifizierung, Zugriffskontrolle und Datenlebenszyklusmanagement. Data Governance schafft Vertrauen in Daten und ermöglicht datenbasierte Entscheidungen. Datenqualität wird anhand von Korrektheit, Vollständigkeit, Konsistenz, Rechtzeitigkeit, Gültigkeit und Eindeutigkeit gemessen.</p>	<i>Einführen</i>
Anonymisierung	<p>Basierend auf den rechtlichen Grundlagen der Datenschutz-Grundverordnung (DSGVO) sind Anonymisierung und Pseudonymisierung nicht nur ein wesentliches Erfordernis für die Weitergabe und Verarbeitung personenbezogener Daten, sondern auch eine Voraussetzung für das Training künstlicher Intelligenz. Um personenbezogene Daten für die Entwicklung neuer Geschäftsmodelle zu nutzen, müssen Anonymisierungs-Tools oder Tools zur Erstellung synthetischer Daten eingesetzt werden. Technologische Trends wie Homomorphic Encryption können die Risiken der Datenschutzverletzung minimieren.</p>	<i>Einführen</i>

Begriff	Anwendung im Public Sector	Status
Intelligenter Arbeitsplatz	Ein intelligenter Arbeitsbereich (Smart Workspace) setzt sich aus folgenden drei Faktoren zusammen: Raum, Technologie und Mensch. Beim Faktor Raum geht es darum, die Räumlichkeiten den unterschiedlichen Bedürfnissen und Arbeitssituationen (Call, Denkarbeit, Meeting) der Mitarbeiter:innen entsprechend anzupassen. Tätigkeiten und Räume werden bewusster auf Kollaboration (und deren Tools) ausgelegt. Meetings können dezentral abgehalten werden und Mitarbeiter:innen können verstärkt zeit- und ortsunabhängig arbeiten. COVID-19 hat die Dynamik dieses Trends stark beschleunigt und auch nach der Pandemie bleibt die Dynamik in Teilen der Welt hoch. Die Modernisierung der BRZ-Räumlichkeiten trägt diesem Trend Rechnung.	<i>Einführen</i>
Zero Trust	Zero Trust ist keine Technologie, sondern eine Sicherheitsarchitektur, die dynamische und explizite Konzepte statt statischer verwendet. Das Prinzip vertraut keinem Gerät, User oder Dienst, egal ob innerhalb oder außerhalb des Unternehmensnetzwerks. Dieses Paradigma, das seit 1990 besteht, wird in einer vernetzten Welt immer wichtiger. Zero Trust verlangt bei jedem Datenzugriff Autorisierung und Validierung. Erfolgreiche Umsetzung erfordert hoch skalierende Systeme und Automatisierung.	<i>Einführen</i>



Schwerpunktthemen 2025

In den vier folgenden Kapiteln widmen wir uns Themen, die für den technischen Fortschritt insbesondere im Bereich E-Government in Österreich und Europa, aber auch gesellschaftlich von Bedeutung sind:

1. **Nachhaltige Informationstechnologie**, als Überbegriff für die Umsetzung von ressourcenschonenden IT-Systemen, um Ziele in den Bereichen Umwelt, Soziales und Unternehmensführung zu erreichen (ESG).
2. **Künstliche Intelligenz in der Softwareentwicklung**, als Anwendungsfall von KI-Systemen, die bei der Erstellung von Softwarecode unterstützen können.
3. **Cyber Threat Intelligence**, ein aktuelles Sicherheitskonzept, das unterschiedliche Aspekte von Cybersecurity adressiert.
4. **Digitaler Humanismus**, als Konzept, das die Beziehung zwischen Menschen und Technologie in den Mittelpunkt stellt.

Nachhaltige Informations- technologie



Nachhaltigkeit ist ein wichtiges Thema, um den schonenden und energieeffizienten Umgang mit den natürlichen Ressourcen zu steuern. Viele Technologien nutzen bereits ESG-Prinzipien (Environment/Social/Governance), um Ziele für Umwelt, Gesellschaft und Governance zu erreichen. Nachhaltige Technologien im Allgemeinen nutzen erneuerbare Energie und sparen Energie in allen Lebensbereichen (Wohnen, Mobilität, Wirtschaft, Freizeit). Informationstechnologie kann durch moderne Softwarearchitekturen und ressourcenschonende Hardware-Infrastruktur nachhaltiger entwickelt und betrieben werden. Informationstechnologien können darüber hinaus helfen, nachhaltige Technologien zu entwickeln, zu optimieren und zu monitoren.

Das BRZ setzt bereits seit mehr als zehn Jahren auf nachhaltige technologische Entwicklung und Maßnahmen zur Reduktion des ökologischen Fußabdrucks im Rechenzentrumsbetrieb.

Nachhaltigkeit im IT-Bereich

Nachhaltigkeit im IT-Sektor umfasst energieeffiziente Rechenzentren, ressourcenschonende Hardwareproduktion und verantwortungsvollen Umgang mit elektronischen Abfällen. Häufig ist in diesem Zusammenhang von „Green IT“ die Rede. Nachhaltigkeit umfasst aber nach heutiger Auffassung mehrere Komponenten. Eine mögliche Betrachtungsweise ist die Unterteilung nach ESG.

ESG und seine Relevanz in der IT

Environment

Der Aspekt Environment (Umwelt) legt den Fokus auf Schutz und Erhalt der natürlichen Umwelt und ihrer Ressourcen. Die Minimierung der negativen Umweltauswirkungen von Unternehmensaktivitäten ist das Ziel. Ressourcenverbrauch, Treibhausgasemissionen, Abfallmanagement, erneuerbare Energien und Biodiversität sind Betrachtungselemente.

Die Abkürzung „ESG“ steht für Environment, Social und Governance (zu Deutsch: Umwelt, Soziales und Unternehmensführung) und bezeichnet ein umfassendes Regelwerk zur Bewertung der nachhaltigen und ethischen Praxis von Unternehmen.

Social

Im Bereich Social (Soziales) konzentriert sich die Betrachtungsweise auf das Wohlergehen von Menschen in der Gesellschaft oder auch im Arbeitsumfeld. Arbeitsbedingungen, Arbeitnehmerrechte, Vielfalt und Inklusion, Arbeitsplatzsicherheit, Sozialleistungen, Beziehungen innerhalb sowie zu Gemeinschaften sind hier Aspekte.

Governance

Der Aspekt Governance (Steuerung) befasst sich mit der Art und Weise, wie eine Organisation oder ein Unternehmen geführt und gelenkt wird. Aspekte sind Unternehmensstruktur, Geschäftsgebarung, ethisches Verhalten, Transparenz, Korruptionsbekämpfung, Einhaltung von Richtlinien und Transparenz in Geschäftsprozessen.

Zusammenspiel von ESG und Berichterstattung

Diese drei Dimensionen sind eng miteinander verknüpft und beeinflussen sich gegenseitig. Eine nachhaltige Entwicklung kann nur erreicht werden, wenn alle drei Aspekte berücksichtigt und in Balance gebracht werden.

ESG-Berichterstattung gewinnt an Bedeutung, wobei sowohl qualitative als auch quantitative Informationen genutzt werden, um die Leistung und den Fortschritt in diesen Bereichen zu messen und transparent zu kommunizieren. Die Umsetzung von ESG-Monitoring und -Reporting hat mit Herausforderungen zu kämpfen: Die Berichterstattung bei einer berichtspflichtigen Organisation ist komplex, die dafür erforderlichen Erfassungs- und Steuerungssysteme sind aufzubauen. Der Aufbau und der Betrieb dieser Systeme können kostenintensive Investitionen sein. ESG-Überlegungen werden in der IT-Branche zu einem zentralen Element der IT-Strategie vieler Unternehmen, einerseits bei der Nutzung, andererseits bei der Bereitstellung von Technologien.

Die CSRD-Richtlinie (Corporate Sustainability Reporting Directive) standardisiert die nicht finanzielle Nachhaltigkeitsberichterstattung. Sie verpflichtet Unternehmen, im Lagebericht über ESG-Themen zu berichten.

Rolle der IT bei ESG

Die IT spielt eine Schlüsselrolle bei der Erfassung, Verwaltung und Analyse von ESG-relevanten Daten. Sie ermöglicht die Zentralisierung von bisher dezentral vorliegenden Informationen und schafft die notwendigen Grundlagen und Transparenz für interne Entscheidungen und externe Berichterstattung. IT-Lösungen können maßgeblich zur Erreichung von Klimazielen beitragen.

Aktueller Trend: IT for Green

IT for Green bezeichnet den neueren Ansatz, um den Einsatz von Informationstechnologie zur Förderung von Nachhaltigkeit und ökologischen Zielen zu unterstützen. Dabei steht im Fokus, wie IT zur Reduzierung von Umweltbelastungen beitragen kann, indem sie umweltfreundlichere Praktiken ermöglicht oder direkt technologische Lösungen für ökologische Herausforderungen bereitstellt.

Mehr über Green IT
im BRZ: www.brz.gv.at/nachhaltigkeit



Beispiele:

- innovative digitale Lösungen für mehr Nachhaltigkeit im gesamten Unternehmen implementieren
- datengetriebene Projekte initiieren
- IT-gestützte Nachhaltigkeitsprojekte zur Senkung des Energieverbrauchs umsetzen

„Green IT“ zielt darauf ab, die Informationstechnologie selbst umweltfreundlicher zu gestalten (z. B. energieeffiziente Rechenzentren, Recycling von IT-Hardware); bei „IT for Green“ liegt der Fokus darauf, wie IT eingesetzt wird, um allgemeine ökologische Ziele zu erreichen. Insgesamt verfolgt die Branche das Ziel, den CO₂-Fußabdruck der IT-Infrastruktur zu verringern und den Energieverbrauch von Hardware, Software und Rechenzentren zu senken. Um dies zu erreichen, muss die gesamte Datenwertschöpfungskette von Data-Governance-Maßnahmen begleitet werden.

Energieverbrauch

Informationstechnologie nimmt einen immer größer werdenden Stellenwert in der Gesellschaft ein, und das bleibt nicht ohne Einfluss auf den Energieverbrauch. Die Internationale Energiebehörde schätzt die Emissionen der IT-Branche für 2026 auf acht bis zwölf Prozent der Gesamtemissionen.

BRZ-Involvement: Energieverbrauch laufend senken

Das BRZ bezieht für seine Rechenzentren 100 Prozent Ökostrom.

Seit über einem Jahrzehnt setzt das BRZ auf „Green IT“ und hat seine Infrastruktur kontinuierlich erneuert und verbessert. Bereits 2010 wurde ein umfassendes Green-IT-Maßnahmenpaket gestartet, das jährlich weiterentwickelt wird. Seit 2015 werden zudem Energieaudits gemäß Energieeffizienzgesetz durchgeführt.

Durch den Einkauf von Ökostrom über die Bundesbeschaffung GmbH wird das BRZ derzeit zu 100 Prozent mit grünem Strom aus erneuerbaren Energiequellen versorgt, die keinerlei Emissionen verursachen.

Das BRZ bezieht seine Energie CO₂-neutral durch den Einkauf von Ökostrom und setzt auf einen verantwortungsvollen Umgang mit Energie. Maßnahmen wie die Umstellung auf LED-Beleuchtung und die Nutzung von Aufzugssystemen mit Energierückgewinnung sowie Wärmerückgewinnung aus IT-Workloads haben zu einer erheblichen Reduktion des Energieverbrauchs geführt. Die Virtualisierung von Servern und Netzfunktionen sowie die Cloud-Infrastruktur (Plattform as a Service) tragen ebenfalls zur Energieeinsparung bei.

Das Abfallmanagement im BRZ setzt auf Mülltrennung und Recycling, um die Umweltbelastung zu minimieren.

Nachhaltigkeitsaspekte moderner Technologien

Cloud-Computing und KI gelten zwar auf der einen Seite als „Energiefresser“, bieten aber auf der anderen Seite viel Potenzial für Nachhaltigkeit. Auch die Herstellung, Nutzung und Entsorgung, somit der gesamte Lebenszyklus von Technologien und Komponenten, wirft Fragen der Nachhaltigkeit auf.

Cloud-Computing

Vorteile und Herausforderungen

Die Nutzung von Cloud-Ressourcen steigt weltweit, auch in Österreich, wenngleich es vereinzelt auch Unternehmen gibt, die vom Cloud-Betrieb wieder abkommen, weil der dauerhafte Gesamtbetrieb der IT teurer kommt als im lokalen Rechenzentrum. Cloud-Computing, vor allem die Virtualisierung, hilft, Ressourcen nachhaltig auszulasten und Leerlauf von Infrastruktur wie Serverhardware zu vermeiden. Die Technologie birgt neben technischen Herausforderungen auch Fragen der Souveränität von IT-Anbietern bzw. Kunden, die auf Cloud-Technologie setzen. Mit der Nutzung von Public-Cloud-Diensten geht auch ein Souveränitätsverlust einher, wenn Hyperscaler zum Einsatz kommen, deren Geschäftsmodell einen Lock-in-Effekt unterstützt. Das heißt, Lösungen und Daten, die in Cloud-Services von Hyperscalern liegen, können häufig nur schwer wieder auf einen anderen Anbieter oder eine lokale Umgebung transferiert werden. Insbesondere im öffentlichen Sektor stellt dies eine Herausforderung dar. Daher verfolgt das BRZ in der Entwicklung von Solutions eine Strategie auf Basis offener Standards, Cloud-Technologie im eigenen Rechenzentrum oder bei Cloud-Anbietern zu nutzen, um so die Abhängigkeit und den Lock-in-Effekt zu vermeiden.

Ein Hyperscaler ist ein Anbieter von Cloud-Diensten, der eine große Rechen-, Speicher- und Netzwerkressourcen-Infrastruktur betreibt und diese global und gut skalierbar bereitstellt. Die Nutzung der Cloud-Dienste von Hyperscalern birgt Risiken wie Verlust der Datensouveränität sowie Lock-in-Effekte.

Rechenleistung und Skalierbarkeit

Energieeffizienz im Rechenzentrum lässt sich aber nicht nur im Cloud-Rechenzentrumsbetrieb der Hyperscaler erreichen, dieselben Prinzipien gelten ebenso in Rechenzentren eines großen oder mittleren Unternehmens, also auch im BRZ.

Chancen der Nachhaltigkeit durch Cloud-Computing

Kosteneffizienz:

- Reduzierung von Hardware- und Wartungskosten durch Nutzung von Cloud-Ressourcen
- Pay-per-Use-Modell ermöglicht effizientere Budgetnutzung

Skalierbarkeit und Flexibilität:

- schnelle Anpassung der IT-Ressourcen an Geschäftsanforderungen
- einfaches Hoch- und Herunterfahren von Ressourcen nach Bedarf

Produktivitätssteigerung:

- verbesserte Zusammenarbeit durch gemeinsamen Zugriff auf Daten und Anwendungen
- Automatisierung von Arbeitsabläufen und Prozessen

Arbeitsproduktivität:

- Studien zeigen eine um etwa sechs Prozent höhere Arbeitsproduktivität durch Cloud-Nutzung.

Risiken und Herausforderungen

Hoher Ressourcenbedarf:

- steigende Nachfrage nach Rechenleistung und Speicherkapazität in Rechenzentren
- potenzielle Auswirkungen auf Energieverbrauch und Umwelt

Datenschutz und Sicherheit:

- Notwendigkeit robuster Sicherheitsmaßnahmen zum Schutz sensibler Unternehmensdaten

Abhängigkeit bei der direkten Nutzung von Hyperscalern:

- mögliche Einschränkungen bei Anbieterwechsel oder Datenportabilität

Komplexität der Migration:

- Herausforderungen bei der Umstellung bestehender Systeme auf Cloud-Lösungen

Das BRZ betreibt eine moderne Plattform as a Service (PaaS)-Umgebung für seine Kunden und nutzt damit die Vorteile und Chancen von Cloud-Technologie.

Künstliche Intelligenz

Künstliche Intelligenz (KI) bietet erhebliche Chancen zur Effizienzsteigerung in Unternehmen, bringt aber auch Herausforderungen mit sich.

Die heute bekannten LLM mit ihrer Transformer-Technologie sind hoch skalierbar und hervorragend geeignet für komplexe Natural Language Processing-Aufgaben, wie wir sie etwa von ChatGPT kennen. Der Rechenaufwand ist allerdings sehr hoch. Eine Alternative könnte mit der aus Long Short-Term Memory (LSTM) weiterentwickelten Technologie xLSTM entstehen, die wesentlich energieeffizienter, jedoch noch kein direkter Ersatz für LLM ist.

Mit LSTM versehene KI-Systeme sind in der Lage, sich an Langzeitabhängigkeiten und frühere Erfahrungen zu erinnern.

Hinter der Entwicklung von xLSTM stehen europäische – auch österreichische – Forschungseinrichtungen, große Technologieunternehmen und die Open-Source-Community. Diese Weiterentwicklungen zielen darauf ab, die ursprüngliche LSTM-Architektur effizienter und leistungsfähiger für moderne Anwendungen zu machen.

Tabelle: Einsatzgebiete von KI-Technologien (LSTM, xLSTM, LLM)

Kriterium	LSTM	xLSTM	LLM (z. B. GPT)
Architektur	rekurrentes Netzwerk mit Speicherzellen	erweitertes LSTM mit optimierten Mechanismen	Transformer-basierte Architektur
Verarbeitung	sequenziell	effizientere sequenzielle Verarbeitung	parallele Verarbeitung (Transformer)
Langzeitkontext	gut, aber begrenzt	verbesserte Langzeitgedächtnisfähigkeit	hervorragend mit Attention-Mechanismen
Komplexität	mittel	etwas höher als LSTM	sehr hoch
Rechenaufwand	moderat	effizienter als LSTM bei längeren Sequenzen	sehr hoch
Skalierbarkeit	begrenzt durch sequenzielle Verarbeitung	bessere Skalierbarkeit als LSTM	hoch skalierbar durch parallele Architektur
Einsatz bei kleinen Daten	gut	gut	benötigt große Datensätze

Kriterium	LSTM	xLSTM	LLM (z. B. GPT)
Typ. Anwendungen	Zeitreihen, kleine NLP-Aufgaben, Spracherkennung	ähnlich wie LSTM, aber für komplexere Aufgaben	breites Spektrum von NLP-Aufgaben
Stärken	Verarbeitung von Sequenzdaten, geringe Anforderungen	bessere Verarbeitung längerer Abhängigkeiten	Vielseitigkeit, Verarbeitung großer Datenmengen
Schwächen	Schwierigkeiten bei sehr langen Sequenzen	höhere Komplexität als LSTM, bleibt sequenziell	hoher Ressourcenbedarf

Chancen für Nachhaltigkeit mit KI

Automatisierung und Produktivitätssteigerung:

- KI kann repetitive und zeitaufwendige Aufgaben automatisieren, wodurch Mitarbeiter:innen für komplexere Tätigkeiten freigesetzt werden.
- Durch Optimierung von Prozessen und Ressourcennutzung können Unternehmen ihre Gesamtproduktivität steigern.

Verbesserte Entscheidungsfindung:

- KI-Systeme analysieren große Datenmengen in Echtzeit und liefern wertvolle Erkenntnisse für fundierte Entscheidungen.
- Dies ermöglicht eine schnellere und präzisere Reaktion auf Marktveränderungen und Kundenbedürfnisse.

Optimierung von Lieferketten und Produktion:

- KI-gestützte Systeme verbessern das Lieferkettenmanagement durch präzisere Nachfrageprognosen und optimierte Lagerhaltung – davon können auch IT-Endabnehmer profitieren.
- In der Produktion können Durchlaufzeiten verkürzt und die Maschinenauslastung maximiert werden .

Personalisierte Kundenerlebnisse:

- KI-gestützte Chatbots und virtuelle Assistenten können User-Verhalten analysieren und dazu beitragen, den Kundenservice zu verbessern und zu individualisieren. Davon können auch Bürgerservice-Anwendungen der Verwaltung profitieren.

Risiken und Herausforderungen

Hoher Energieverbrauch:

- Der steigende Einsatz von KI, insbesondere in Rechenzentren, führt zu einem erhöhten Energiebedarf, vor allem die LLM-Technologie ist sehr energiehungrig.
- Prognosen deuten auf einen Anstieg des weltweiten Energiebedarfs für Rechenzentren von knapp 500 TWh im Jahr 2022 auf über 800 TWh im Jahr 2026 hin.

Datenschutz und Sicherheit:

- Die Verarbeitung großer Datenmengen durch KI-Systeme erfordert robuste Sicherheitsmaßnahmen zum Schutz sensibler Informationen.
- Es besteht die Gefahr von Datenmissbrauch oder Datendiebstahl.

Abhängigkeit von KI-Systemen:

- Eine zu starke Abhängigkeit von KI-gestützten Entscheidungen kann die menschliche Urteilsfähigkeit beeinträchtigen.
- Bei Systemausfällen oder Fehlern können kritische Geschäftsprozesse beeinträchtigt werden.

Ethische Bedenken:

- Der Einsatz von KI wirft Fragen zur Verantwortlichkeit und Transparenz bei automatisierten Entscheidungen auf.
- Es besteht die Gefahr von Voreingenommenheit in KI-Algorithmen, die zu unfairen Ergebnissen führen kann.

Um die Chancen von KI optimal zu nutzen und gleichzeitig die Risiken zu minimieren, sollten Unternehmen einen ausgewogenen Ansatz verfolgen. Dies beinhaltet Investitionen in energieeffiziente Technologien, robuste Sicherheitsmaßnahmen und die Schulung von Mitarbeiterinnen und Mitarbeitern im verantwortungsvollen Umgang mit KI-Systemen.

Anwendungsbeispiel: Energieverbrauch von KI-Anwendungen

Der Verbrauch an Energie für Google-Suchabfragen hat die Welt bisher nicht sonderlich interessiert, aber aufgrund der zunehmenden Popularität und Zugänglichkeit von mächtigen LLM-Systemen (z. B. ChatGPT, Microsoft Copilot, Google Gemini u. a.) rückt der Energieverbrauch dieser Anwendungen in den Fokus: Um den Faktor 10 mehr Energie ist für den Betrieb der KI-basierten Chatbots erforderlich. Ein Tag Nutzung von generativer KI in einem amerikanischen Cloud-Rechenzentrum hat den gleichen Energiebedarf wie eine mittelgroße Stadt.

Lebenszyklus von IT-Technologien

Von der Herstellung über die Nutzung bis zur Entsorgung – also im gesamten Lebenszyklus – einer Technologie sind unterschiedliche Maßnahmen möglich, um Nachhaltigkeit zu erreichen.

Aspekte eines nachhaltigen Technologielebenszyklus

Design und Entwicklung:

- Ressourcenschonung: Verwendung nachhaltiger, recycelbarer Materialien und modularer Designs, um die Lebensdauer der Geräte zu verlängern und Reparaturen zu erleichtern
- Energieeffizienz: Entwicklung energieeffizienter Hardware und Software, z. B. stromsparende Prozessoren oder Algorithmen mit geringem Rechenaufwand sowie energieeffiziente Programmierung

Nutzung:

- Ressourcenschonung: Verlängerung der Nutzungsdauer durch regelmäßige Updates, Reparaturservices und Weiterverwendung von Geräten
- Energieeffizienz: Einsatz energieeffizienter Geräte (z. B. ENERGY STAR-zertifiziert), Virtualisierung von Servern und Cloud-Lösungen zur gemeinsamen Ressourcennutzung

Entsorgung und Recycling:

- Ressourcenschonung: Förderung von Kreislaufwirtschaft durch Rücknahmeprogramme und Wiederverwendung von Komponenten
- Energieeffizienz: Minimierung des Energieverbrauchs beim Recycling durch optimierte Prozesse

Übergreifende Maßnahmen:

- Ressourcenschonung: Nutzung von Sharing-Plattformen und Refurbishing, um den Bedarf an neuen Geräten zu reduzieren
- Energieeffizienz: Monitoring des Energieverbrauchs über den gesamten Lebenszyklus und kontinuierliche Verbesserung der Effizienzstandards

Insgesamt erfordert der Lebenszyklus von IT-Technologien eine sorgfältige Gestaltung und Nutzung, um den Verbrauch von Ressourcen und Energie zu minimieren und Nachhaltigkeitsziele zu unterstützen.

BRZ-Involvement

Nachhaltige Beschaffung

Das BRZ beschafft eine Vielzahl standardisierter Produkte durch Abrufe aus Rahmenvereinbarungen der Bundesbeschaffung GmbH (BBG). Die naBe-Kriterien (Aktionsplan nachhaltige Beschaffung) in den betroffenen Beschaffungsgruppen sind seitens der BBG in Ausschreibungen verpflichtend anzuwenden. NaBe-konform beschaffte Produkte/Dienstleistungen sind im E-Shop der BBG durch das NaBe-Logo gekennzeichnet, es kann daher nach diesen Produkten extra gefiltert werden. Dadurch ist sichergestellt, dass das BRZ Strom, PCs und Notebooks, Monitore, Multifunktionsdrucker, aber auch Kopier- und Hygienepapier NaBe-konform beschafft.

In Österreich wurde der Aktionsplan für nachhaltige Beschaffung (naBe) ins Leben gerufen, auch das BRZ folgt bei der Beschaffung diesem Plan.

BRZ-Ausschreibungen

Das BRZ selbst führt unter anderem für Server- und Storage-Komponenten, Software und externe Dienstleistungen auch eigene Vergabeverfahren durch. Die Berücksichtigung ökologischer Aspekte kommt bei der Beschaffung von Server- und Storage-Komponenten in Betracht. Obwohl im naBe-Aktionsplan keine Kriterien für Server- und Storage-Systeme definiert sind, werden – sofern mit den vergaberechtlichen Rahmenbedingungen vereinbar – ökologische Kriterien (z. B. ENERGY STAR-Zertifizierung) berücksichtigt. Selbstverständlich werden im Rahmen der Preisbewertung auch Folgekosten wie Betriebs- und Wartungskosten miteinbezogen.

Zukünftige Perspektiven und Herausforderungen

Neben den genannten Technologien gibt es weitere, die in Zukunft eine größere Rolle spielen könnten, um Nachhaltigkeit zu erreichen.

Softwarearchitektur

Die jetzt durch den KI-Hype sehr in die Höhe getriebenen Rechenleistungen können durch nachhaltige Architektur der zur Verwendung kommenden Systeme zur Effizienz beitragen. Trotzdem wird der Energieverbrauch der IT deutlich zunehmen.

Edge Computing

Edge Computing beschreibt eine verteilte Rechner-Topologie, bei der die Datenspeicherung und -verarbeitung an optimalen Orten im Verhältnis zum Ort der Datenerstellung und -nutzung platziert werden. Edge Computing optimiert Latenz, Bandbreite, Autonomie und regulatorische bzw. Sicherheitsaspekte und unterstützt dadurch Nachhaltigkeit. Edge-Computing-Standorte erstrecken sich entlang eines Kontinuums zwischen dem absoluten Rand (wo physische Sensoren und digitale Systeme zusammenlaufen) und dem „Kern“ (der Cloud oder einem zentralen Rechenzentrum). Für IT-Verfahren im Verwaltungsumfeld spielt Edge-Computing derzeit noch keine entscheidende Rolle.

KI-Anwendungen benötigen große Mengen von Energie. Die Entwicklung geht in Richtung effizienterer Modelle mit weniger Energieverbrauch.

Neue Kühlkonzepte im Rechenzentrum

Die neuesten CPUs und GPUs verfügen über höhere Wärmedichteigenschaften als die älteren Architekturen. Darüber hinaus integrieren Serverhersteller mehr CPUs und GPUs in jedes Rack, um mit der steigenden Nachfrage nach Anwendungen für Hochleistungsrechner (HPC) und künstliche Intelligenz (KI) Schritt zu halten. Mit Liquid-Cooling, Direct-to-Chip-Liquid-Cooling und Immersionskühlung sind hier neue Technologien zur effizienteren Kühlung entstanden.

Effiziente Kühlung trägt zu einem nachhaltigeren Rechenzentrumsbetrieb entscheidend bei.

Conclusio

Prozessoren werden immer leistungsfähiger und energieeffizienter, aber sie werden in immer stärkerem Maß gebraucht, um die erforderliche Rechenleistung für neue Technologien zu erbringen. Die Folge ist ein immer höherer Ressourcenverbrauch in der IT.

Doch es kann einerseits die Energieeffizienz deutlich erhöht werden, andererseits kann die IT dazu beitragen, die großen Datenmengen aus Sensorik zu verarbeiten und wirksame Steuerungssysteme zu entwickeln.

Künstliche Intelligenz in der Software- entwicklung



Mit der Einführung von künstlicher Intelligenz (KI) in der Softwareentwicklung steht das Berufsbild der Softwareentwicklerin bzw. des Softwareentwicklers vor einem erheblichen Wandel. KI wird Softwareentwickler:innen nicht ersetzen, sondern deren Rolle erweitern und ihnen neue Werkzeuge an die Hand geben, um effizienter zu arbeiten.

KI-Tools geben Softwareentwicklerinnen und -entwicklern neue Werkzeuge an die Hand und können die Effizienz steigern.

Wandel des Berufsbildes

In vielen Fällen führt eine technische Entwicklung zu einer Transformation des Berufsbildes. Fachkräfte müssen sich weiterbilden und neue Fähigkeiten erwerben, um mit den technologischen Fortschritten mithalten zu können. Der Wandel ist also nicht nur eine Herausforderung, sondern auch eine Chance zur Weiterentwicklung und Spezialisierung.

Rolle der künstlichen Intelligenz

Die Rolle von künstlicher Intelligenz (KI) in der Softwareentwicklung sowie den zugehörigen Rollen und Prozessen wächst rasant. KI verändert nicht nur die Vorgehensweise, wie Software entwickelt wird, sondern auch, wie Mitarbeiter:innen ihre tägliche Arbeit gestalten. Von der Automatisierung repetitiver Aufgaben bis hin zur Unterstützung bei komplexen Designentscheidungen hat KI das Potenzial, den Entwicklungsprozess grundlegend zu transformieren.

KI-Tools können repetitive Aufgaben übernehmen, aber auch bei komplexen Designentscheidungen unterstützen.

Dies kann zu folgenden Verbesserungen führen:

- **Zeitersparnis:** Automatisierung von Routineaufgaben
- **Kostenreduktion:** schnellere und effizientere Entwicklung
- **Qualitätssteigerung:** bessere Code-Qualität und weniger Fehler
- **Innovationsförderung:** mehr Raum für Kreativität und strategische Entscheidungen
- **Zukunftssicherheit:** schnelle Anpassung an neue Technologien und Anforderungen

Auswirkung von KI auf den Entwicklungsprozess

Künstliche Intelligenz beeinflusst jede Phase der Softwareentwicklung, von der Anforderungsanalyse bis zur Wartung. Sie automatisiert Routineaufgaben, verbessert die Entscheidungsfindung und steigert die Effizienz.

Im Folgenden wird die Einsatzmöglichkeit von KI in der Softwareentwicklung anhand eines praxisnahen Beispiels dargestellt. Eine mögliche Beispielanforderung könnte lauten: „Entwicklung einer Applikation, die eine Steuererklärung mit einem Klick erstellt“.

KI kann dabei helfen, professionelle Grundstrukturen in der Arbeit zu setzen und zeitaufwendige Arbeit drastisch zu verkürzen. Dazu werden in diesem Beispiel alle Phasen der Softwareentwicklung durchlaufen und – wo immer möglich – auf integrative Unterstützung durch KI zurückgegriffen.

Begriffsdefinitionen

Epic: Dies ist eine übergeordnete, große Anforderung, welche die Vision und Richtung vorgibt. Die Anforderung enthält noch keine Details und kann nicht umgesetzt werden. Für die Umsetzung wird das Epic in User Stories aufgeteilt und dort die Anforderung und technische Umsetzung detailliert.

User Story: Eine User Story enthält eine kleine und spezifische Anforderung, die in einem kurzen Zeitraum (Sprint) umgesetzt werden kann. Sie enthält auch technische Umsetzungsdetails und Informationen, wie die Umsetzung getestet werden kann (Akzeptanzkriterien).

Testfall: Ein Testfall ist eine spezifische Anleitung, mit der geprüft werden kann, ob eine Anforderung korrekt umgesetzt wurde.

Coding Standards: verbindliche Richtlinien für die Erstellung von Code, um Lesbarkeit, Wartbarkeit und Qualität sicherzustellen

Boilerplate-Code: standardisierte und wiederverwendbare Codeblöcke

DevOps: Methodik für verbesserte Zusammenarbeit und Kommunikation zwischen Softwareentwicklung (Dev) und Betrieb (Operations); durch die Integration von Entwicklungs- und Betriebsprozessen wird die Effizienz gesteigert, die Qualität verbessert und die Bereitstellungsgeschwindigkeit erhöht.

KI-Unterstützung in der Anforderungsanalyse

Die Anforderungsanalyse ist eine der kritischsten Phasen, da hier der Grundstein für den gesamten Entwicklungszyklus gelegt wird. KI-gestützte Tools, die Natural Language Processing (NLP) nutzen, können Anforderungen aus Dokumenten oder Meetings extrahieren und strukturieren. Sie helfen dabei, unklare Spezifikationen zu identifizieren und Stakeholder besser einzubinden.

Vorteile:

- Reduzierung menschlicher Fehler bei der Anforderungsaufnahme
- schnellere Identifikation von Risiken und Abhängigkeiten

Beispiel: Epic für eine Steuererklärung mit einem Klick

Prompt: Formuliere ein Epic für eine Steuererklärung mit einem Klick.



Epic: Steuererklärung mit einem Klick

Beschreibung: Als Steuerzahler möchte ich meine Steuererklärung mit nur einem Klick einreichen können, um Zeit zu sparen und den Prozess zu vereinfachen.



Akzeptanzkriterien:

1. **Automatisierter Datenabruf:**
 - Die Anwendung ruft automatisch alle relevanten steuerlichen Daten von Finanzämtern, Banken und anderen Institutionen ab.
 - Die Daten werden sicher und verschlüsselt übertragen.
2. **Benutzerfreundliche Oberfläche:**
 - Die Benutzeroberfläche ist intuitiv und führt die Nutzerin bzw. den Nutzer Schritt für Schritt durch den Prozess.
 - Mehrsprachige Unterstützung ist vorhanden, um Nutzerinnen und Nutzern in verschiedenen Regionen gerecht zu werden.
3. **KI-gestützte Eingabehilfen:**
 - Künstliche Intelligenz überprüft die Eingaben und macht Vorschläge zur Optimierung der Steuererklärung.
 - Automatische Berechnungen zeigen sofortige Steuererstattungen oder -nachzahlungen an.
4. **Sicherheit und Datenschutz:**
 - Alle Daten werden verschlüsselt gespeichert und übertragen.
 - Die Anwendung erfüllt alle relevanten Datenschutzgesetze, einschließlich der DSGVO.
5. **Integration mit Steuer-Apps:**
 - Die Lösung ist kompatibel mit gängigen Steuer-Apps und üblicher Buchhaltungssoftware.
 - APIs ermöglichen die Integration mit anderer Finanz- und Buchhaltungssoftware
6. **Support und Updates:**
 - Technischer Support und Steuerberatung sind verfügbar, um Nutzerinnen und Nutzern bei Fragen und Problemen zu helfen.
 - Regelmäßige Updates stellen sicher, dass die Software immer auf dem neuesten Stand der Steuergesetze ist.

KI-Unterstützung in der Entwicklungsphase

In der Entwicklungsphase geht es darum, die Struktur der Software zu planen, die passenden Technologien zu wählen und den Code zu schreiben.

- KI-Algorithmen unterstützen bei der Auswahl optimaler Architekturentscheidungen, indem sie bestehende BRZ-Vorgaben analysieren und anwenden (beispielsweise Architektur-Blueprints).
- Die eigentliche Implementierung ist traditionell der aufwendigste Teil des Entwicklungsprozesses. KI-Tools unterstützen Entwickler:innen durch automatische Code-Vervollständigung und Vorschläge basierend auf kontextuellen Daten. Sie können Boilerplate-Code generieren und helfen bei der Einhaltung der BRZ-Coding-Standards.

Beispiel: Epic User Stories für die Umsetzung in Java

Prompt: Leite von diesem Epic User Stories für die Umsetzung in Java ab.



Hier sind einige User Stories, die aus dem Epic „Steuererklärung mit einem Klick“ abgeleitet wurden und für die Umsetzung in Java geeignet sind:

User Story 1: Automatisierter Datenabruf

Beschreibung: Als Nutzer:in möchte ich, dass die Anwendung meine steuerlichen Daten automatisch von Finanzämtern und Banken abrufen, damit ich diese nicht manuell eingeben muss.



Akzeptanzkriterien:

- Die Anwendung kann sich mit den APIs der Finanzämter und Banken verbinden.
- Die Daten werden sicher und verschlüsselt übertragen.
- Die abgerufenen Daten werden korrekt in der Anwendung angezeigt.

Technische Umsetzung in Java:

- Implementierung von REST-Clients für die APIs der Finanzämter und Banken
- Nutzung von Bibliotheken wie Spring Security für die Verschlüsselung der Datenübertragung
- Datenmodellierung und Speicherung der abgerufenen Daten in einer Datenbank (z. B. mit JPA/Hibernate)

User Story 2: Benutzerfreundliche Oberfläche

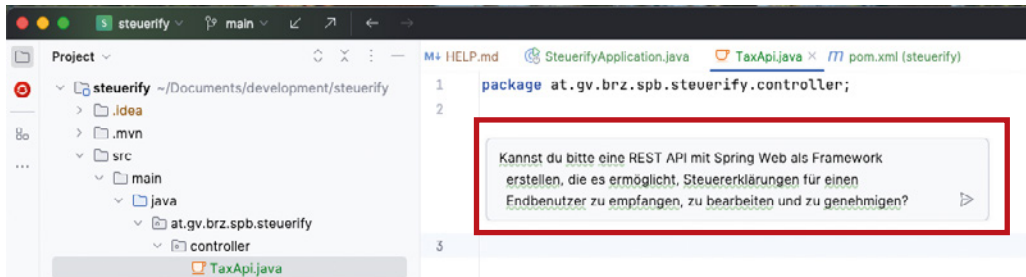
Beschreibung: Als Nutzer:in möchte ich eine intuitive Benutzeroberfläche, die mich Schritt für Schritt durch den Prozess der Steuererklärung führt, damit ich keine Fehler mache.

Akzeptanzkriterien:

- Die Benutzeroberfläche ist klar strukturiert und leicht verständlich.
- Mehrsprachige Unterstützung ist vorhanden.
- Jeder Schritt des Prozesses ist klar beschrieben.

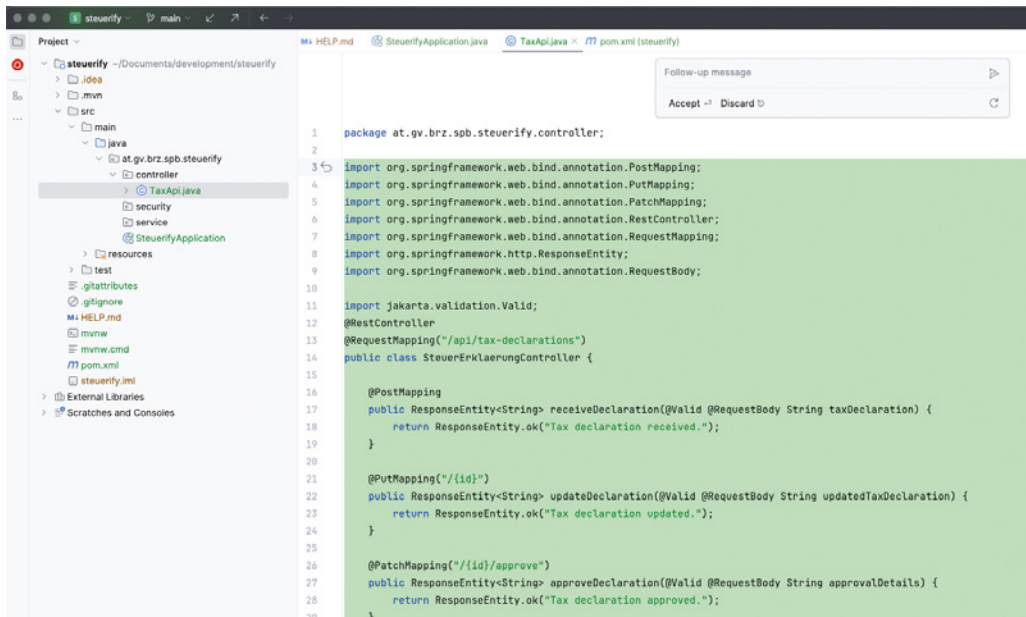
Beispiel: Developer, der direkt innerhalb der Entwicklerumgebung die KI um Unterstützung bei Erstellung der Datenschnittstelle bittet

Abbildung 2: Prompt zur Erstellung einer Datenschnittstelle



Ergebnis: Die KI liefert direkt in der Entwicklerumgebung eine Codebasis (grün hervorgehoben), die Developer an die Bedürfnisse anpassen können.

Abbildung 3: Ergebnis in der Entwicklerumgebung



KI-Unterstützung in der Qualitätssicherung

Softwaretests sind entscheidend, um die Qualität und Stabilität des Produkts sicherzustellen. KI-Tools generieren automatisch Testfälle basierend auf den Anforderungen und dem Quellcode sowie analysieren Testergebnisse, um Schwachstellen zu identifizieren.

Beispiel: Testfälle für das Epic „Steuererklärung mit einem Klick“

Prompt: Erstelle Testfälle für dieses Epic.



Hier sind einige Testfälle für das Epic „Steuererklärung mit einem Klick“:

Testfall 1: Automatisierter Datenabruf

Beschreibung: Überprüfung, ob die Anwendung steuerliche Daten automatisch von Finanzämtern und Banken abrufen kann

- **Vorbedingungen:** Die Nutzerin/Der Nutzer hat gültige Zugangsdaten zu den relevanten Institutionen.
- **Schritte:**
 1. Nutzer:in meldet sich in der Anwendung an
 2. Nutzer:in gibt Zugangsdaten zu Finanzämtern und Banken ein
 3. Anwendung ruft automatisch die steuerlichen Daten ab
- **Erwartetes Ergebnis:** Die Daten werden korrekt und vollständig abgerufen und in der Anwendung angezeigt.)



Testfall 2: Benutzerfreundliche Oberfläche

Beschreibung: Überprüfung der Benutzerfreundlichkeit der Oberfläche

- **Vorbedingungen:** Die Anwendung ist installiert und betriebsbereit.
- **Schritte:**
 1. Nutzer:in startet die Anwendung
 2. Nutzer:in navigiert durch die verschiedenen Schritte der Steuererklärung
- **Erwartetes Ergebnis:** Die Navigation ist intuitiv und verständlich, alle Schritte sind klar beschrieben.

Beispiel: Ein Developer möchte den erstellten Code innerhalb seiner Entwicklerumgebung durch KI automatisiert auf potenzielle Probleme prüfen lassen (Prompt rot, Ergebnis grün).

Abbildung 4: Automatische Prüfung von Code durch die KI

AI Assistant

Me
Find potential problems in

```

Java
1 @PostMapping
2 public ResponseEntity<String> receiveDeclaration(@Valid @RequestBody String
  taxDeclaration) {
3     try (BufferedWriter writer = new BufferedWriter(new FileWriter
      ("tax_declarations.txt", true))) {
4         writer.write(taxDeclaration);
      }
  }
  < 4 more line(s)
  
```

AI Assistant
There are several potential issues in the implementation of the `receiveDeclaration` method. Here's a detailed analysis:

1. Hardcoding the File Path

- **Problem:** The file path `"tax_declarations.txt"` is hardcoded in the method. This can cause issues if the application is deployed in an environment where the file system is different or if the application lacks permissions to access this file or directory.
- **Solution:** Use configurable paths through application properties (`application.yaml` or `application.properties`) or an environment variable. Example:

```

Java
1 @Value("${tax.declaration.file.path}")
2 private String taxDeclarationFilePath;
  
```

CI/CD sind Ansätze, um die Codebasis zu automatisieren und die Geschwindigkeit bei der Freigabe von Diensten zu erhöhen.

KI-Unterstützung bei Betrieb und Wartung

In der Deployment-Phase wird die Software in die Produktionsumgebung überführt. KI-gestützte DevOps-Tools überwachen den Deployment-Prozess und erkennen potenzielle Probleme in Echtzeit. Sie helfen bei der Optimierung von Continuous Integration/Continuous Deployment (CI/CD)-Pipelines.

Die Wartungsphase ist oft die längste Phase des Lebenszyklus einer Software.

- KI-gestützte Systeme analysieren Nutzerfeedback, identifizieren häufige Probleme und priorisieren Feature-Anfragen. Predictive-Maintenance-Algorithmen helfen, potenzielle Probleme zu erkennen, bevor sie kritisch werden.
- KI-gestützte Debugging-Tools analysieren Code auf potenzielle Fehler und schlagen Lösungen vor. Einige Systeme lernen aus vergangenen Fehlern, um Muster zu erkennen und proaktiv zu warnen.
- KI-gestützte Analysen von Datenflüssen per Anomalie-Erkennung ermöglichen das Erkennen nicht typischer Muster in den Datenströmen. Dadurch kann eine fehlerhafte Version oder auch ein Eindringen in das System viel schneller und zuverlässiger erkannt werden.

Zukünftige Auswirkungen und Herausforderungen

Beim Einsatz von KI-Tools ist darauf zu achten, die Kreativität und Innovationskraft von Menschen zu erhalten und in den Entwicklungsprozess einzubinden.

Die KI in der Softwareentwicklung steht noch am Anfang. Zukünftige Fortschritte könnten Bereiche wie die vollständige automatisierte Softwareerstellung und intelligente Entscheidungsfindung in der Architekturplanung umfassen. Gleichzeitig ist es essenziell, die Zusammenarbeit zwischen Entwicklerinnen sowie Entwicklern und KI so zu gestalten, dass die Kreativität und Innovation der Menschen erhalten bleibt.

Begriffsdefinition: Expert in the Loop

Für alle Rollen im Rahmen des Softwareentwicklungsprozesses, wie z. B. Requirements Engineer, Architektinnen und Architekten, Softwareentwickler:innen, Tester:innen oder Betriebsmitarbeiter:innen gilt ein Paradigmenwechsel, der unter „Expert in the Loop“ beschrieben wird.

Expert in the Loop (EiTL) ist ein Ansatz in der Anwendung von künstlicher Intelligenz (KI), bei dem menschliche Expertinnen und Experten in den Entscheidungsprozess eingebunden werden, um die Ergebnisse der KI zu überwachen, zu bewerten und bei Bedarf anzupassen. Es ist eine Kombination aus automatisierten KI-Systemen und menschlichem Fachwissen, die sicherstellen soll, dass Entscheidungen fundiert, ethisch korrekt und kontextuell relevant sind.

Veränderungen im Berufsbild Softwareentwickler:in

Das Berufsbild der Softwareentwicklerin bzw. des Softwareentwicklers wird durch den Einsatz von künstlicher Intelligenz (KI) in der Softwareentwicklung erheblich beeinflusst und weiterentwickelt.

Wesentliche Veränderungen und Entwicklungen, die das Berufsbild in Zukunft prägen werden:

Weniger Routine, mehr Kreativität

KI wird repetitive und zeitaufwendige Aufgaben wie das Schreiben von Boilerplate-Code, Fehlerbehebung oder einfache Tests automatisieren. Entwickler:innen können sich stärker auf kreative und anspruchsvolle Aufgaben konzentrieren, wie die Gestaltung innovativer Architekturen, strategische Planung oder die Lösung komplexer Probleme.

Neue Anforderungen an Kompetenzen und veränderte Anforderungen an die Bildung:

- **Verantwortung und Kontrolle:**
Mit dem Einsatz von KI steigt die Verantwortung der Entwickler:innen, sicherzustellen, dass die Software zuverlässig ist. Entwickler:innen werden eine zentrale Rolle bei der Bewertung und Überwachung von KI-gestützten Prozessen spielen, um ethische und technische Standards einzuhalten (siehe oben „Expert in the Loop“).
- **Lebenslanges Lernen:**
Aufgrund des schnellen technologischen Fortschritts wird kontinuierliches Lernen essenziell. Entwickler:innen müssen regelmäßig neue KI-Tools und -Methoden erlernen, um Chancen und Risiken zu kennen. Die Ausbildung von zukünftigen Softwareentwicklerinnen und Softwareentwicklern muss sich auch insofern ändern, dass diese die Kompetenz für die Prüfung der KI-Ergebnisse haben.
- **Interdisziplinäre Ausbildungen:**
Studiengänge und Trainingsprogramme werden Themen wie maschinelles Lernen, Ethik in der KI und Datenanalyse stärker integrieren

KI-Tools können genutzt werden, um Ansätze wie „Low-Code“ oder „No-Code“ voranzutreiben.

Automatisierung vs. Innovation

Da KI grundlegende Aufgaben automatisiert, wird die Entwicklung komplexer Systeme und innovativer Produkte in den Vordergrund rücken. Entwickler:innen werden verstärkt auf Architekturebene arbeiten und neue Paradigmen wie „Low-Code“ oder „No-Code“-Ansätze mittels KI vorantreiben.

Auswirkungen auf Unternehmen und Governance

Mit der zunehmenden Integration von KI müssen Unternehmen ihre Governance-Strukturen anpassen, um den neuen technologischen und regulatorischen Anforderungen gerecht zu werden. Dies umfasst erweiterte Compliance-Anforderungen, robustes Risikomanagement,

transparente Berichterstattung und kontinuierliche Schulungsprogramme. Diese Änderungen sind notwendig, um eine nachhaltige, ethische und effiziente Unternehmensführung zu gewährleisten.

Conclusio

Insgesamt bietet die Einführung von KI in die Softwareentwicklung enorme Chancen für Innovation und Effizienzsteigerung. Entwickler:innen können sich auf höherwertige Aufgaben konzentrieren und gleichzeitig sicherstellen, dass die Software den höchsten Qualitäts- und Sicherheitsstandards entspricht. Die Zukunft der Softwareentwicklung wird durch die symbiotische Zusammenarbeit von Mensch und Maschine geprägt sein, wobei KI als wertvolles Werkzeug dient, um die Herausforderungen der modernen Softwareentwicklung zu meistern.

Cyber Threat Intelligence (CTI)



Cyber Threat Intelligence (CTI) bezeichnet die strukturierte Sammlung, Analyse und Verarbeitung von Daten und Informationen über potenzielle oder bestehende Cyberbedrohungen. Ziel ist es, einen besseren Überblick über Bedrohungen zu erhalten, um Angriffe frühzeitig zu erkennen, sich darauf vorzubereiten, effektiv darauf zu reagieren und im Idealfall diese zu verhindern, indem das Verhalten von Angreifern sowie deren Taktiken und Exploits analysiert werden.

Definition und Zweck von Cyber Threat Intelligence

Cyber Threat Intelligence umfasst sowohl die gesammelten Daten selbst als auch den Prozess der Erfassung und Auswertung, um daraus Informationen und Wissen zu generieren. Der Hauptzweck besteht darin, Sicherheitsteams mit detaillierten, handlungsrelevanten Informationen über Bedrohungen zu versorgen, um Cyberangriffe proaktiv zu verhindern und zu bekämpfen. Durch die Analyse von Artefakten und die Anreicherung der Daten mit Kontextinformationen ermöglicht Cyber Threat Intelligence ein besseres Verständnis der Mechanismen, Indikatoren und potenziellen Auswirkungen von Cyberbedrohungen. Dies versetzt Unternehmen in die Lage, fundierte Entscheidungen zur Stärkung ihrer Cybersicherheit zu treffen und ihre Abwehrstrategien kontinuierlich an die sich ständig weiterentwickelnde Bedrohungslandschaft anzupassen.

Cyber Threat Intelligence ermöglicht ein besseres Verständnis von Cyberbedrohungen.

Elemente und Datenquellen

Die Informationen für Threat Intelligence stammen aus einer Vielzahl von Quellen, darunter Open Source Intelligence (OSINT), soziale Medien, technische Berichte, durch eigene Sicherheitsteams selbst analysierte sicherheitsrelevante Ereignisse sowie auch kommerzielle Dienste (Closed-Source Intelligence). Auch forensisch erfasste Daten sowie Informationen aus dem

Für die Umsetzung von CTI ist der Zugriff auf eine breite Basis an Quellen notwendig, die in ein Lagebild einfließen.

Deep Web und Dark Web können in ein umfassendes Lagebild miteinfließen. Diese breite Datenbasis ermöglicht es Sicherheitsexpertinnen und Sicherheitsexperten, ein adäquates Bild der aktuellen Bedrohungslandschaft zu erstellen, sämtliche relevanten Quellen in einer internen Threat Intelligence Platform (TIP) zusammenzufassen und diese für Analytistinnen und Analysten sowie für eingesetzte Sicherheitswerkzeuge nutzbar zu machen. Die gesammelten Daten werden sorgfältig analysiert und zu handlungsrelevanten Erkenntnissen verarbeitet, die Unternehmen dabei unterstützen, ihre Sicherheitsstrategien effektiv anzupassen und zu optimieren.

Kategorien von Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence lässt sich in drei Kategorien unterteilen, die jeweils spezifische Aspekte der Cybersicherheit adressieren:

1. **Strategische CTI** richtet sich an eine nicht technische Zielgruppe wie Führungskräfte und bietet einen Überblick über Trends und allgemeine Bedrohungslagen.
2. **Taktische CTI** konzentriert sich auf die Taktiken, Techniken und Verfahren (TTPs) von Angreifern für Sicherheitsteams.
3. **Operative CTI** liefert spezifische Details zu bevorstehenden oder laufenden Bedrohungen.

Diese Kategorisierung ermöglicht es Unternehmen, Bedrohungsinformationen gezielt für verschiedene Ebenen der Entscheidungsfindung und Sicherheitsplanung zu nutzen.

Vorteile der Nutzung von Cyber Threat Intelligence

Die Nutzung von Daten und Informationen im Bereich der Cyber Threat Intelligence bietet Unternehmen zahlreiche Vorteile zur Unterstützung der gesamtheitlichen Sicherheitsstrategie:

Mit CTI können Bedrohungen früher erkannt und die Widerstandsfähigkeit von IT-Systemen gestärkt werden.

- Früherkennung von Bedrohungen ermöglicht proaktive Maßnahmen zur Risikominimierung
- verbesserte Entscheidungsfindung durch fundierte Analysen der Bedrohungslandschaft
- effektiverer Schutz sensibler bzw. vertraulicher Daten vor unberechtigten Zugriffen
- Optimierung der Ressourcenallokation durch gezielte Priorisierung von proaktiven und reaktiven Sicherheitsmaßnahmen
- Stärkung der Widerstandsfähigkeit gegen sich ständig weiterentwickelnde Cyberbedrohungen
- Durch den Einsatz von Cyber Threat Intelligence können Organisationen die kontinuierliche Anpassung ihrer Sicherheitsmaßnahmen grundlegend unterstützen und somit ihre Abwehrfähigkeiten gegenüber potenziellen Angriffen signifikant verbessern. Cyber Threat Intelligence ist somit eine wesentliche Grundlage für Continuous Threat Exposure Management.

Relevanz für öffentliche IT

Cyber Threat Intelligence-Plattformen und -Prozesse sind für IT-Dienstleister im öffentlichen Sektor von entscheidender Bedeutung, da sie den Schutz kritischer Infrastrukturen und vertraulicher Kundendaten unterstützen. Durch die Integration fortschrittlicher Bedrohungserkennungs- und Reaktionsfähigkeiten können öffentliche Einrichtungen Cyberbedrohungen besser identifizieren und abwehren. Dies ist besonders wichtig, da der öffentliche Sektor aufgrund seiner Bedeutung für die Bereitstellung zentraler Dienste ein attraktives Ziel für Cyberkriminelle darstellt.

1. frühzeitige Erkennung und Abwehr potenzieller Angriffe auf kritische Infrastrukturen
2. verbessertes Risikomanagement durch umfassende Analyse der Bedrohungslandschaft

CTI bietet auch für IT-Dienstleister im öffentlichen Sektor Vorteile, etwa in der Erkennung von Bedrohungen bzw. in der Umsetzung von regulatorischen Maßnahmen.

3. Unterstützung bei der Einhaltung regulatorischer Anforderungen wie DSGVO oder NIS2
4. effizientere Ressourcenallokation durch Priorisierung von Sicherheitsmaßnahmen
5. Stärkung des Vertrauens der Öffentlichkeit in die Sicherheit staatlicher IT-Systeme

Continuous Threat Exposure Management (CTEM)

CTEM ist die Bezeichnung für einen modernen Prozess, Schwachstellen zu identifizieren und daraus Strategien für die Lösung von Sicherheitsproblemen abzuleiten.

Der Begriff Continuous Threat Exposure Management (CTEM) im Bereich der Cybersicherheit wird etwa seit 2022 verwendet. Er bezeichnet kein Produkt und keine Technologie, sondern steht für einen modernen Prozess, wie Schwachstellen (laufend) identifiziert, evaluiert, mögliche Risiken abgeleitet und deren Mitigation priorisiert werden können. Allerdings integrieren diverse Hersteller von Sicherheitsprodukten die Vorgehensweise in ihre Produkte.

Ziel ist es, jene Dienste bzw. Assets zu identifizieren, die den größten Bedrohungen ausgesetzt sind (Security Posture Management und Attack Surface Management), daraus Maßnahmen abzuleiten und deren Wirksamkeit laufend (kontinuierlich) zu prüfen bzw. zu validieren, um so die Sicherheit iterativ zu steigern.

Synergie von CTI und Continuous Threat Exposure Management

Durch die Integration von Cyber Threat Intelligence in CTEM können Unternehmen ihre Cybersicherheit dynamisch an neue Bedrohungen anpassen und so das Risiko erfolgreicher Angriffe erheblich reduzieren.

Threat Intelligence und Continuous Threat Exposure Management (CTEM) ergänzen sich synergetisch in der modernen Cybersicherheitsstrategie. Während Threat Intelligence Informationen über potenzielle Bedrohungen liefert, nutzt CTEM diese Erkenntnisse, um die Sicherheitslage eines Unternehmens kontinuierlich zu verbessern. CTEM integriert Threat Intelligence in einen proaktiven, fünfstufigen Prozess, der Schwachstellen identifiziert, priorisiert und behebt, bevor Angreifer sie ausnutzen können.

Die Kombination beider Ansätze ermöglicht:

- Echtzeitüberwachung und -bewertung der Bedrohungslandschaft
- Priorisierung von Risiken basierend auf aktuellen Bedrohungsinformationen
- automatisierte Reaktionen auf sich entwickelnde Sicherheitsrisiken
- kontinuierliche Verbesserung der Sicherheitsmaßnahmen durch laufende Angriffssimulationen
- effizientere Ressourcennutzung durch gezielte Behebung kritischer Schwachstellen

Status quo

Die Prozesse, Maßnahmen und Technologien im Bereich CTEM sind grundsätzlich nicht neu, aufgrund der immer größer werdenden Angriffsfläche durch:

- eine stetig steigende Anzahl an Schwachstellen in eingesetzten Standard-Softwareprodukten
- die Nutzung von Cloud-Technologien sowie von Services in der Cloud
- den Einsatz von künstlicher Intelligenz und die stetig steigende Komplexität in der IT
- die steigende Anzahl an rechtlichen bzw. regulatorischen Vorgaben

In der Folge wird die zielgerichtete, wirtschaftliche und risiko-basierte Auswahl von präventiven und reaktiven Sicherheitsmaßnahmen immer komplexer. Insbesondere die Erwartungshaltung der (vollständigen) Automatisierung im Bereich reaktiver Sicherheitsprozesse kann durch vorhandene Technologien weiterhin nicht erfüllt werden. Der Bereich der Cybersicherheit sieht sich auch zukünftig der Problematik ausgesetzt, dass präventive Maßnahmen weiterhin zu wenig Aufmerksamkeit und Anerkennung

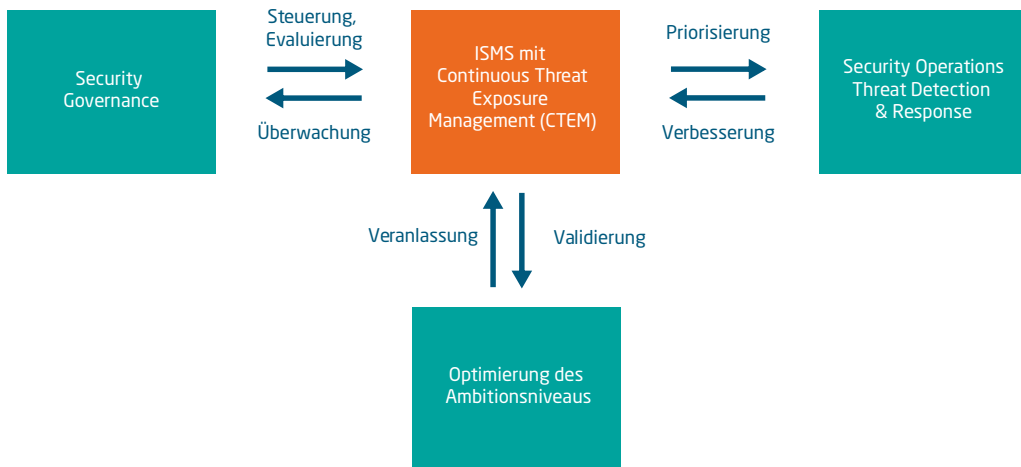
erhalten. Das ursprünglich aus dem Bereich des Gesundheitswesens stammende Zitat „There is no glory in prevention“ lässt sich somit 1:1 auch auf den Bereich der Cybersicherheit übertragen.

Grundsätze und Umsetzung

CTEM ist primär ein (neuer) Denkansatz im Informationssicherheitsmanagement.

Bedrohungen und Schwachstellen in Assets, Diensten, der Lieferkette, genutzten Cloud-Diensten und eigenen Services sollen erkannt werden, bevor dies Angreifer tun und/oder sie von diesen ausgenutzt werden. Das eher reaktive, oftmals etablierte Schwachstellenmanagement soll in eine kontinuierliche Überwachung und ein (automatisiertes) Testen überführt werden. Methoden und Maßnahmen wie Threat Hunting, Red-Teaming oder External Attack Surface Management sind hierbei das Mittel zum Zweck.

Abbildung 5: CTEM im Kontext Security Governance und ISMS



Sechs Schritte zur Umsetzung von CTEM

Zur Umsetzung eines Programms zum CTEM wird vom Marktforschungsunternehmen Gartner® ein Ansatz in fünf Schritten empfohlen, der in diesem Artikel um einen sechsten Schritt zur kontinuierlichen Verbesserung und Re-Evaluierung erweitert wird.

Scoping

Am Start sollte – wie bei jedem größeren Security-Programm üblich – der Scope bzw. Anwendungsbereich festgelegt werden. Dies betrifft grundsätzlich alle IKT-Dienste und Assets, unabhängig davon, ob diese On-Premise betrieben oder von Dritten (z. B. Cloud) bezogen werden. Im Scoping sollte auch bereits eine erste Kritikalitätsbewertung dieser Assets durchgeführt werden.

Discovery

Nach der initialen Identifikation der relevanten Assets soll in diesem Schritt festgestellt werden, welchen Bedrohungen und Risiken die identifizierten Assets tatsächlich ausgesetzt sind. Hier sollen Abweichungen zu bestehenden Sicherheitsvorgaben, Fehlkonfigurationen, aber auch fehlendes Sicherheitsbewusstsein bewertet, aufgedeckt und einer Risikobewertung unterzogen werden.

Prioritization

Wie Gartner an dieser Stelle besonders betont, sollen im Rahmen dieses Schrittes nicht alle gefundenen Schwachstellen unmittelbar mitigiert werden, sondern jene, die am wahrscheinlichsten ausgenutzt werden könnten. Die klassische Schwachstellenbewertung, z. B. auf Basis des Common Vulnerability Scoring Systems (CVSS), ist für eine angemessene und wirtschaftliche Auswahl von Maßnahmen unzureichend, da hierbei bestehende Maßnahmen, die Kritikalität oder auch die Exponiertheit nicht berücksichtigt werden.

Validation

In diesem Schritt sollten gefundene und priorisierte Schwachstellen bzw. Risiken im Kontext ihrer tatsächlichen Ausnutzbarkeit validiert werden. Dies beinhaltet auch die Prozesse zur Erkennung und Reaktion auf mögliche Angriffe. Methoden und Maßnahmen zur Validierung beinhalten unter anderem sowohl klassisches Penetration Testing und Red-Teaming, Breach and Attack Simulation als auch Threat Modeling.

Mobilization

Für die Behebung von Schwachstellen auf Basis der Priorisierung und Validierung müssen alle relevanten Stakeholder bzw. Teams in der Organisation eingebunden werden. Die wesentliche Aussage von Gartner ist hier, dass die automatische Behebung von Schwachstellen und Risiken weiterhin nicht möglich ist, insbesondere auch deswegen, da manche Schwachstellen zu gewissen Zeitpunkten nicht behoben werden können und Risiken durch andere Maßnahmen adressiert werden müssen.

Improvement

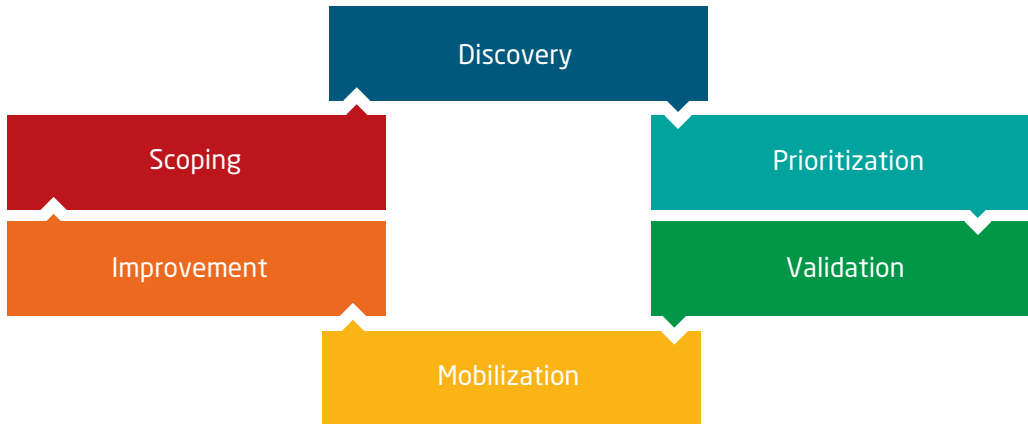
Zur Steigerung des Reifegrades eines entsprechenden CTEM-Programms sollten die entsprechenden Schritte regelmäßig wiederholt werden. Der Schritt der Mobilisierung endet grundsätzlich mit der Freigabe erforderlicher Ressourcen, Maßnahmen und Changes. Mit der Implementierung der Maßnahmen startet somit die Verbesserung bzw. Optimierung.

Herausforderungen

Die Einführung von CTEM stellt Unternehmen und Organisationen vor die Herausforderung, einen gewissen Wandel insbesondere im Bereich des Schwachstellenmanagements anzustoßen. Die Bewertung von Schwachstellen auf Basis etablierter Scoring-Systeme (wie das Common Vulnerability Scoring System – CVSS) darf nicht mit einer umfassenden Risikobewertung verwechselt werden. Nicht jede kritische Schwachstelle ist auch für die eigene Organisation kritisch und/oder

Das Common Vulnerability Scoring System (CVSS) ist ein Standard zur Bewertung von IT-Sicherheitslücken. Der CVSS-Score ist eine numerische Darstellung des Schweregrads 0–10 einer Sicherheitslücke.

Abbildung 6: Phasen eines CTEM-Programms



Quelle: Gartner²; Hinweis: ergänzt um eine sechste Phase

kann mittels eines unmittelbar verfügbaren Patches behoben werden. Für den „Blick über den Tellerrand“ hinaus ist es jedoch erforderlich, dass das Thema Cybersicherheit wieder verstärkt von allen Teilen einer Organisation betrachtet wird, um jene Punkte zu identifizieren, bei denen unmittelbarer Handlungsbedarf besteht. Entsprechende Sensibilisierungsprogramme über die Vorteile und Ziele von CTEM sowie die Unterstützung durch das Management erscheinen dazu jedenfalls erforderlich.

Conclusio

Ein CTEM-Programm ist Teil eines umfassenden Informationssicherheitsmanagements und somit auch Teil des hierfür erforderlichen Informationssicherheitsrisikomanagements. Die Erkennung und Abwehr von Angriffen ist zwar nicht Teil von CTEM, durch die entsprechende Priorisierung und Validierung von Maßnahmen und Schwachstellen können jedoch Risiken und potenzielle Vorfälle deutlich reduziert werden.

Digitaler Humanismus



Digitaler Humanismus ist ein Konzept, das die Beziehung zwischen Menschen und Technologie in den Mittelpunkt stellt. Es zielt darauf ab, technologische Entwicklungen so zu gestalten, dass sie den Menschen dienen, einen klaren Nutzen bringen, unterstützend wirken und humanistische Werte wie Ethik und soziale Verantwortung fördern.

Technologie soll nicht als Selbstzweck dienen, sondern dem Wohl der Gesellschaft und der Umwelt. Digitaler Humanismus zielt darauf ab, die digitale Transformation und technologische Entwicklung menschenzentriert zu gestalten. Er verfolgt den Ansatz, die Potenziale der Digitalisierung für eine humanere und gerechtere Zukunft zu nutzen, wobei die Technologie dem Menschen dienen soll und nicht umgekehrt. Die Förderung einer ethischen und wertebasierten Entwicklung digitaler Technologien sowie der Schutz individueller Autonomie und Würde genauso wie eine kritische Auseinandersetzung mit den Auswirkungen der Digitalisierung auf Gesellschaft und Kultur sind im digitalen Humanismus zentrale Themen.

Ursprung des Begriffs

Digitaler Humanismus verbindet humanistische Werte mit digitaler Innovation und zielt darauf ab, Technologien zu entwickeln und einzusetzen, die das menschliche Wohl fördern und die Gesellschaft positiv gestalten. Erforderlich ist eine enge Zusammenarbeit zwischen Wissenschaft, Wirtschaft, Politik und Gesellschaft, um sicherzustellen, dass digitale Technologien menschenzentriert und ethisch verantwortungsvoll gestaltet werden. Digitaler Humanismus wird auf breiter Ebene diskutiert und vorangetrieben: Bereits 2019 wurde das Wiener Manifest für Digitalen Humanismus erstellt, das von zahlreichen Vertreterinnen und Vertretern aus Wirtschaft und Wissenschaft unterzeichnet wurde. Im Rahmen der EU-Ratspräsidentschaft Deutschlands wurde 2020 die „Berliner Erklärung zur Digitalen Gesellschaft

und wertebasierten digitalen Verwaltung“ unterzeichnet. Die „Berliner Erklärung“ enthält gemeinsame Leitlinien zur digitalen Transformation in Europa, ihre Auswirkungen auf die Gesellschaft und Chancen für die Zukunft.

Umsetzung des Digitalen Humanismus

Initiativen rund um den Digitalen Humanismus in Österreich stehen im Einklang mit europäischen Prinzipien und rechtlichen Rahmenbedingungen, wie sie etwa von der Europäischen Kommission 2023 verabschiedet wurden. Ziel bei der Umsetzung eines Digitalen Humanismus in Österreich ist es, einen Rahmen für Innovation und Nutzung der digitalen Möglichkeiten zur Verbesserung der Lebensqualität der Menschen und der Stärkung des Wirtschaftsstandortes zu schaffen. Insbesondere die Entwicklungsfortschritte im Bereich der künstlichen Intelligenz, aber auch zahlreiche andere technologische Entwicklungen wie etwa Cloud-Anwendungen und Themen wie Wahlfreiheit, Partizipation, Sicherheit, Nachhaltigkeit, Solidarität oder Inklusion werfen komplexe ethische Fragen auf, die im politischen Diskurs zu erörtern sind.

Ansatzpunkte und Forderungen für menschenzentrierte Technologie

Die Digitalisierung wirkt auf verschiedene Lebensbereiche ein und kann unseren Alltag, unsere Wirtschaft und unsere Interaktionen mit Behörden und Organisationen erleichtern. Digitale Tools bringen aber nicht nur Chancen mit sich, sondern auch Risiken. Diese zu benennen und Handlungsalternativen zu erörtern, ist Teil des Diskurses rund um den Digitalen Humanismus. Es entstehen aber auch erste Standardisierungen und Normen, die den Rahmen bzw. Leitlinien für die Entwicklung von sogenannten Value-Based-Prozessen unterstützen. Die Norm ISO/IEC/IEEE 24748-7000 basiert auf dem Ansatz von Value-Based Engineering und bietet einen Leitfaden für den Aufbau und Einsatz ethischer, menschenzentrierter Technologien.

Berliner Erklärung

Die „Berliner Erklärung“ (2020) knüpft an die Tallinner E-Government-Erklärung aus 2017 an und benennt sieben Maßnahmen zur Umsetzung einer wertebasierten digitalen Transformation:

1. Stärkung der Grundrechte und demokratischen Werte in der digitalen Welt
2. Förderung sozialer Teilhabe und Inklusion
3. Förderung digitaler Kompetenzen und von „Digital Literacy“
4. Stärkung des Vertrauens in die digitale Verwaltung
5. Stärkung der digitalen Souveränität und Interoperabilität in Europa
6. Schaffung wertebasierter und menschenzentrierter KI-Systeme für den öffentlichen Sektor
7. Förderung der Resilienz und Nachhaltigkeit

Wiener Manifest für Digitalen Humanismus

Das „Wiener Manifest für Digitalen Humanismus“ stellt folgende Ansatzpunkte und Forderungen auf, die dazu beitragen sollen, Technologie nach menschlichen Werten und Bedürfnissen zu gestalten:

1. Digitale Technologien sollen so gestaltet sein, dass sie **Demokratie und Inklusion** fördern. Dies wird besondere Anstrengungen erfordern, um derzeitige Ungleichheiten zu überwinden und das emanzipatorische Potenzial digitaler Technologien zu nutzen – und damit unsere Gesellschaft inklusiver gestalten zu können.
2. **Privatsphäre und Redefreiheit** sind Grundwerte, die im Mittelpunkt unserer Aktivitäten stehen sollen. Daher müssen Strukturen wie soziale Medien oder Online-Plattformen derart geändert werden, dass freie Meinungsäußerung, Verbreitung von Informationen und Privatsphäre besser geschützt sind.
3. Es müssen wirksame Vorschriften, Gesetze und Regeln festgelegt werden, die auf einem breiten Diskurs beruhen. Sie sollen **Fairness und Gleichheit, Verantwortlichkeit und Transparenz** von Softwareprogrammen und Algorithmen sicherstellen.

4. Die Regulierungsbehörden müssen gegenüber Technologie-monopolen intervenieren. Die **Wettbewerbsfähigkeit** des Marktes muss wiederhergestellt werden, da Tech-Monopole die Marktmacht ausnutzen und Innovationen ersticken. Staaten sollen nicht alle Entscheidungen den Märkten überlassen.
5. **Entscheidungen**, deren Folgen die individuellen oder kollektiven Menschenrechte betreffen können, müssen weiterhin von Menschen getroffen werden. Die Entscheidungsträger:innen müssen für ihre Entscheidungen verantwortlich und haftbar sein. Automatisierte Entscheidungssysteme sollen die Entscheidungsfindung durch den Menschen nur unterstützen und nicht ersetzen.
6. **Wissenschaftliche Ansätze** über verschiedene Disziplinen hinweg sind Voraussetzung, um die Herausforderungen zu meistern. Technologische Disziplinen wie die Informatik müssen mit den Sozial-, Geistes- und Naturwissenschaften zusammenarbeiten, um disziplinäre „Silos“ zu durchbrechen.
7. Universitäten sind der Ort, an dem neues **Wissen** erzeugt und kritisches Denken geschärft wird. Sie haben daher eine besondere Verantwortung und sollen sich dessen auch bewusst sein.
8. Akademische und industrielle Forscher:innen müssen sich in einem offenen **Dialog** mit der Gesellschaft auseinandersetzen und ihre Ansätze reflektieren. Diese Überlegungen müssen in die tatsächlichen Praktiken der Erzeugung neuen Wissens und neuer Technologien eingebettet werden und gleichzeitig die Freiheit des Denkens und der Wissenschaft verteidigen.
9. Praktiker:innen auf der ganzen Welt sollen sich der gemeinsamen **Verantwortung für die Auswirkungen** der Informationstechnologien stellen. Es muss ein gemeinsames Verständnis darüber entstehen, dass keine Technologie neutral ist: Sowohl deren potenzielle Vorteile als auch mögliche Nachteile müssen erkannt und von Praktikerinnen und Praktikern weltweit in der Umsetzung berücksichtigt werden.

10. Es bedarf einer Vision für neue **Bildungsinhalte**, die Wissen aus den Geistes-, Sozial- und Ingenieurwissenschaften kombinieren. Im Zeitalter der automatisierten Entscheidungsfindung und künstlichen Intelligenz sind Kreativität, Reflexion und die Berücksichtigung menschlicher Aspekte für die Ausbildung zukünftiger Informatiker:innen und anderer Berufsgruppen von entscheidender Bedeutung.
11. Die **Ausbildung** in der Informatik und die Bildungsarbeit über ihre gesellschaftlichen Auswirkungen muss so früh wie möglich beginnen. Ziel ist es, den Lernenden zu ermöglichen, sowohl IKT-Kenntnisse als auch das Bewusstsein für die betreffenden Themen zu entwickeln.

Plattform Digitaler Humanismus

Die Plattform Digitaler Humanismus, bei der auch das BRZ beteiligt ist, hat sich zum Ziel gesetzt, Gesellschaft, Wirtschaft und Wissenschaft zusammenzubringen, um die verantwortungsvolle Entwicklung digitaler Technologie voranzutreiben. Teil der Plattform, die regelmäßige Dialogreihen veranstaltet sowie Publikationen herausbringt, sind auch interessierte Personen sowie Vertreter:innen der öffentlichen Hand (Städte, Länder, Bundesministerien).

Digitaler
Humanismus in
der Praxis:





Roland Ledinger
BRZ-Geschäftsführer

„Für mich ist Digitaler Humanismus wesentlich, um digitale Lösungen für Bürger:innen und Unternehmen bereitzustellen, die einen menschenzentrierten, innovativen Ansatz verfolgen. Dabei ist neben der Usability auch die Berücksichtigung von Partizipation im Entstehungsprozess und die Einhaltung eines zugrunde gelegten Wertesystems von zentraler Bedeutung. KI kann etwa immer nur unterstützen, aber nicht selbstständig entscheiden. Daher ist die Fähigkeit, Ergebnisse von digitalen Prozessen auch plausibilisieren zu können, eine wichtige Kompetenz, die uns Menschen ausmacht. Die Norm ISO/IEC/IEEE 24748-7000 basiert auf dem Ansatz von Value-Based Engineering und bietet einen Leitfaden für den Aufbau und Einsatz ethischer, menschenzentrierter Technologien. Ich sehe es für das BRZ als eine wichtige Notwendigkeit, hier die entstandene Kompetenz weiterzuentwickeln und gerade im Hype von KI nicht das Wesentliche aus den Augen zu verlieren.“

Digital Design
Principles des BRZ:



Anwendungsbeispiel: Digital Design Principles

Digital Design Principles werden weltweit eingesetzt. Sie beschreiben Grundsätze und Handlungsanweisungen, wie moderne IT-Anwendungen und -Services entwickelt werden sollen. Basierend auf den BRZ-Architekturprinzipien haben wir international Erfahrungen und Know-how ausgetauscht. So sind unsere fünf Digital Design Principles for Products entstanden.

Fünf Prinzipien stellen im BRZ das Leitbild für die Entwicklung digitaler Services und Anwendungen dar:

1. Handle zielgerichtet und benutzerzentriert.
2. Schütze die Privatsphäre und gewähre Sicherheit.
3. Standardisiere und nutze Vorhandenes.
4. Agiere verantwortungsbewusst, kosteneffizient und gemeinschaftlich.
5. Stelle zuverlässige Services zur Verfügung.

Im Fokus stehen immer die Anwender:innen, Barrierefreiheit, Sicherheit, Wirtschaftlichkeit und Zuverlässigkeit sowie das Design und der Datenschutz. Die Prinzipien richten sich in erster Linie an Personen und Organisationen, die digitale Dienste für den öffentlichen Bereich verantworten, konzipieren, entwickeln und betreiben. Die Prinzipien können von BRZ-Kunden als Vorbild bzw. Referenz verwendet werden, für die Arbeit des BRZ sind sie verbindlich.

Anwendungsbeispiel: BRZ-Kriterienkatalog für Trustworthy AI

Das BRZ hat einen Prüfkatalog erarbeitet, der unseren Kunden ein gemeinsames Verständnis zum Thema vertrauenswürdige KI (Trustworthy AI) vermitteln soll. Gleichzeitig zeigt er auf, welche Risiken mit dem Einsatz eines KI-Systems verbunden sind und wie man diese bei gleichzeitiger Nutzenmaximierung reduziert. Der höchste Nutzen beim Einsatz des Prüfkatalogs liegt in der gemeinsamen Diskussion der Fragen, den dadurch generierten Lösungsansätzen und der Entwicklung einer Kultur zum Einsatz vertrauenswürdiger KI, welche die öffentliche Verwaltung als Maßstab setzt. Das zugrunde liegende Modell zur KI-Beurteilung basiert auf Bereichen, Kriterien, Prüfpunkten und Merkmalen. Da Prüfbereiche oft abstrakt sind und im Konflikt miteinander stehen und darüber hinaus meistens Bewertungsansätze fehlen, ist es wichtig, die Operationalisierung mittels ergänzender Faktoren vorzunehmen. Die Prüfung vertrauenswürdiger KI erfolgt in den Prüfbereichen Transparenz, Verantwortung, Datenschutz, Zuverlässigkeit und Gerechtigkeit. Diese Kriterien werden auf 22 Prüfkriterien, 70 Prüfpunkte und mehr als 250 Merkmale heruntergebrochen.

BRZ-Kriterienkatalog
für vertrauens-
würdige KI:





Anwendungsbeispiel: Auszeichnung für Partizipationsplattform BRZ eDem

Die E-Demokratie-Plattform BRZ eDem wurde im Rahmen des „Digitalen Humanismus in der Praxis“-Awards mit einem Sonderpreis in der Kategorie „Projekte“ ausgezeichnet. Das BRZ beschäftigt sich seit 20 Jahren in Analysen und Projekten mit der Technik und der Schnittstelle „Technik und Mensch“ im Bereich der E-Demokratie, insbesondere der E-Partizipation. Im Rahmen eines Entwicklungsprojektes wurden Anwendungen und Umfeldbedingungen für E-Demokratie untersucht. Aufbauend auf einer sechsmonatigen Analysetätigkeit wurde bereits Anfang 2005 das erste E-Demokratie-Projekt (seidabei.at) umgesetzt.



Impressum

Medieninhaber, Herausgeber:
Bundesrechenzentrum GmbH
Hintere Zollamtsstraße 4, 1030 Wien
kommunikation@brz.gv.at

Verlagsort: Wien

Projektleitung: Julian Unger

Autor:innen: Michael Arth, Christa Burger,
Johann Kalhs, Stefan Poschinger

Grafisches Konzept: trafikant – Handel mit
Gestaltung, 1050 Wien

Layout: Giulia Bottoni, Jakob Klaunzer & Sophie Votzi

Lektorat/Korrektorat: Lettera Lektorat,
Michaela Kapusta

Bildnachweise:
BRZ/Klaus Vyhnaek (S. 5, S. 70)
iStock.com/Wavebreakmedia (S. 43, S. 45, S. 48)
iStock.com/fonikum (S. 43-46, S. 48-49)
BRZ/Jan Halwax (S. 47, S. 49)
BRZ/Sophie Votzi (S. 60, S. 63)

Druck/Herstellungsort:
Print Alliance HAV Produktions GmbH
Druckhausstraße 1, 2540 Bad Vöslau

Alle Angaben ohne Gewähr. Bei der Erstellung der
Publikation wurde generative KI genutzt.

Stand: 04/2025.

