KI SICHER EINFÜHREN UND NUTZEN

achermann ict-services
SOPHOS

BEGLEITDOKUMENT ZUM WEBINAR
«KI SICHER NUTZEN – ENABLEMENT TRIFFT SECURITY»

1

KI-Gremium aufbauen

Bevor Regeln definiert werden, bringen Sie die richtigen Personen an einen Tisch. Ein interdisziplinäres KI-Gremium, auch «AI Board» genannt, ist der Ort, an dem strategische Fragen, technische Möglichkeiten und alltagsnahe Bedürfnisse zusammenfinden. Aus der gemeinsamen Arbeit im Gremium kristallisiert sich oft natürlich heraus, wer aus dem Kreis die operative KI-Verantwortung übernehmen möchte oder soll.

Zusammensetzung
IT/Security, Datenschutz (DSB), Vertretung der Geschäftsleitung sowie aus Fachbereichen wie HR, Marketing oder Operations.

Aufgaben
Strategie und Positionierung, Use-Case-Bewertung, Freigaben, Risiko-Monitoring, Schulungs- und Kommunikationsplanung.

Rhytmus
Quartalsweise Sitzungen, ad hoc bei neuen Use Cases, neuen Tools oder Vorfällen.

2

KI Readiness Check

Operative Standortbestimmung des Reifegrads über die drei Säulen Strategie und Planung, Daten und Infrastruktur sowie People, Kultur und Zusammenarbeit. Ergebnis: Reifegrad- Einschätzung, Quick Wins, priorisierter Pilot-Backlog und eine 12-Monats-Roadmap als Grundlage für die folgenden Schritte.

3

KI Kompass

Strategische, gemeinsam getragene Position der Organisation zu den drei Spannungsfeldern Geschäft und Ökonomie, Mensch und Ethik sowie Governance und Regulierung. Ergebnis: Living Document mit Leitplanken plus ein bis zwei konkrete KI-Quartalsziele, halbjährlich überprüft.

Synthese

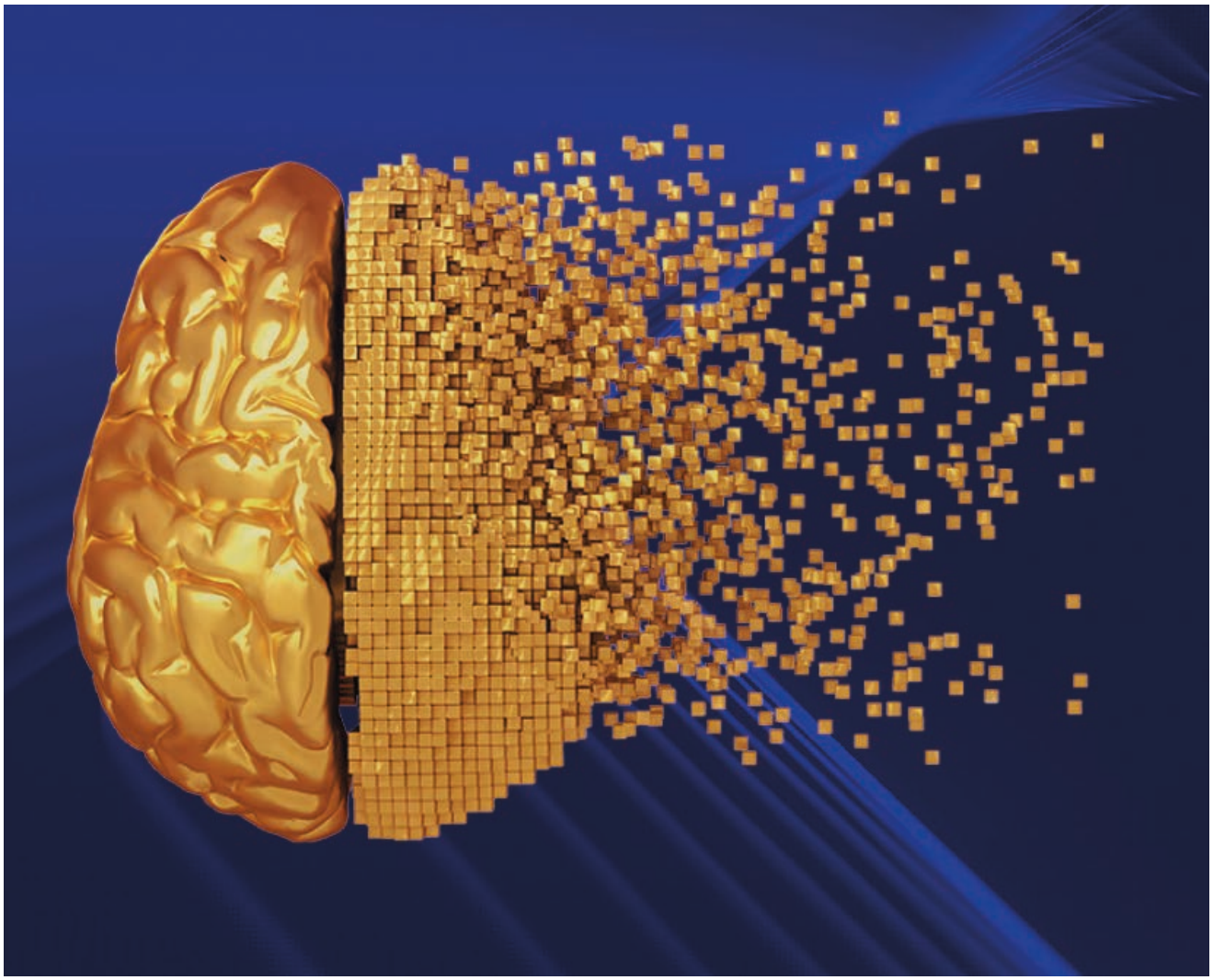
VOM BEFUND ZUM LEBENDEN KONZEPT

Die vier Schritte sind keine isolierten Bausteine. Sie greifen ineinander und werden in ein Gesamtkonzept verarbeitet, das sich kontinuierlich weiterentwickelt:

Quick Win *nach dem AI Readiness Check aus dem Befund (Reifegrad, Quick Wins, Top-Risiken) entsteht die erste pragmatische Version der Guidelines aus Schritt 4, zugeschnitten auf die eigene Organisation.*

Strategische Verankerung *durch den KI-Kompass. Die Positionierung zu den drei Spannungsfeldern präzisiert die Leitplanken. Daraus werden konkrete Regeln in den Guidelines.*

Guidelines *als lebendes Dokument. Die KI-Guidelines sind nie «fertig». Sie verändern sich mit neuen Use Cases, Tools und Regulierung. Halbjährlicher Review als Routine.*



4

KI-Guidelines für die tägliche Nutzung

- ✓ Nur durch die KI-verantwortliche Person freigegebene Tools nutzen (Microsoft 365 Copilot, weitere im zentralen Register)
- ✓ KI-Ergebnisse vor jeder externen Verwendung kritisch prüfen. Quellen, Fakten, Tonalität.
- ✓ KI-generierte Inhalte gegenüber Kundinnen und Kunden als solche kennzeichnen (Transparenzpflicht).
- ✓ Sensitivity Labels konsequent anwenden. Copilot respektiert EXTRACT/VIEWRechte.
- ✓ Kritische Entscheidungen mit Auswirkung auf Menschen immer per Humanin-the-loop prüfen.
- ✓ Neue Use Cases über die Checkliste «Neue Produkte» bei der KI-verantwortlichen Person zur Freigabe einreichen.
- ✓ KI-Vorfall (Halluzination mit Folgen, Datenabfluss, Verdacht auf Shadow AI) sofort an die KI-verantwortliche Person und den oder die DSB melden.

- ✗ Geschäftsdaten in öffentliche KI-Dienste eingeben (ChatGPT-Free, Claude-Free, Gemini-Free).
- ✗ Private KI-Accounts oder private Geräte für geschäftliche KI-Nutzung verwenden.
- ✗ Nicht genehmigte KI-Plugins, Browser-Erweiterungen oder Drittanbieter-KI installieren.
- ✗ KI ohne Prüfung für Social Scoring, Emotionserkennung am Arbeitsplatz oder Profiling einsetzen (verbotene Praktiken Art. 5 EU AI Act).
- ✗ Inhalte erzeugen, die fremde Urheber-, Marken- oder Persönlichkeitsrechte verletzen.
- ✗ Kritische Entscheidungen (Personal, Kredit, Zugang) vollständig automatisieren.
- ✗ Zweck einer freigegebenen KI-Anwendung ändern, ohne den CISO/ KI Gremium erneut einzubinden.

Freigabeprozess nach ICH-WIR-ALLE-Methodik

Ebene	Was es betrifft	Beispiele	Freigabe durch
ICH	Persönliche KI-Nutzung für die eigene Produktivität	Copilot für eigene E-Mails, individuelle Agents	KI-Verantwortliche/r (CISO oder Co-Lead DSB)
WIR	Team- oder Abteilungs-KI für gemeinsame Nutzung	Team-Agents, abteilungsspezifische Workflows Kernprozesse, die von spezifischen Teams getragen werden, werden hier mit KI angereichert oder völlig neu gedacht und umgesetzt	KI-Administrator KI-Verantwortliche/r (CISO oder Co-Lead DSB) in Zusammenarbeit mit den Fachabteilungen

Ebene	Was es betrifft	Beispiele	Freigabe durch
ALLE	Unternehmensweite KI-Anwendungen	Zentrale Copilot-Policies, unternehmensweite Agents. Zentrale Unterstützungspro-zesse (Rechnungswesen, HR, Marketing, Interne IT) werden hier mit KI angereichert oder völlig neu gedacht und umgesetzt	Leadership-Board (LSB) KI-Verantwortliche/r (CISO oder Co-Lead DSB) in Zusammenarbeit mit den Fachabteilungen

5

Technische Unterstützung der Guidelines

«Regeln wirken nur, wenn sie technisch durchgesetzt werden.» Zwei Werkzeugwelten ergänzen sich:

Microsoft 365 Copilot und Agents

setzen die DOs am Arbeitsplatz um: Sensitivity Labels, DLP-Richtlinien und Audit-Logs erzwingen den korrekten Umgang mit Daten, freigegebene Agents (ICH/WIR) ersetzen Shadow-AI-Tools.

Sophos Workspace Protection

kontrolliert den Zugriff auf KI-Dienste über den Protected Browser, blockiert unsanktionierte GenAI-Plattformen, schafft Sichtbarkeit über tatsächliche Nutzung und hält Shadow AI im Zaum.

6

Umsetzung nach ICH - WIR - ALLE

Die Einführung folgt der IWA-Methodik und adressiert drei Perspektiven: die einzelne Person, das Team und die gesamte Organisation. Diese Perspektiven sind keine starre Reihenfolge, sie können parallel und situativ gestartet werden.

ICH

INDIVIDUELLE BEFÄHIGUNG
Copilot im Alltag, Prompts und Routinen. Jede Person wird selbst handlungsfähig.

WIR

KERNPROZESSE IM TEAM
Use Cases entlang täglicher Abläufe, geteilte Spielregelnund gelebter KI-Einsatz.

ALLE

ORGANISATIONSWEITE PLATTFORM
KI im Intranet, Wissen, Suche und Self-Service für alle Mitarbeitenden. Bei einem KI-Vorfall: Datenabfluss oder Verdacht auf Shadow AI -> sofort an die KI-verantwortliche Person.

IT, die befreit.

SOPHOS achermann ict-services