AI Security Workshop

Schaffen Sie gemeinsam mit uns ein einheitliches Security-Verständnis zu Generative AI und Agentic AI – von der technologischen Einordnung und typischen Anwendungsfällen über Risiken und Angriffsvektoren bis hin zu Schutzmaßnahmen und Lösungsansätzen.

Situation – AI ist in aller Munde

Laut Gartner werden die Ausgaben für AI-Technologien im Jahr 2026 weltweit voraussichtlich etwa 2,5 Billionen US-Dollar betragen, was einem Anstieg von 44% gegenüber dem Vorjahr entspricht. AI-Technologien sind dabei längst auch in verschiedenen Ausprägungen sowie zu unterschiedlichen Einsatzzwecken in deutschen Unternehmen und Behörden angekommen. Die Anwendungsfälle variieren dabei enorm und umfassen mitunter:

- Verwendung von **AI-Assistenten** wie ChatGPT, Claude AI oder Perplexity für die tägliche Arbeit
- Integration von **AI Coding-Agenten** wie Cursor AI oder Claude Code in Entwicklungsumgebungen und Entwicklungsprozessen
- Nutzung von **persönlichen AI-Agenten** wie OpenClaw zur autonomen Erledigung von beliebigen Aufgaben auf dem eigenen Endgerät
- Aufbau dedizierter **AI-Infrastrukturen**, um eigene Modelle für spezifische Business Use Cases optimieren oder entwickeln zu können – entweder im eigenen Data Center oder in der Cloud

Die enorm schnelle **AI-Adaptionsrate** bringt dabei sowohl Herausforderungen für die organisatorische als auch für die operative IT-Sicherheit mit sich.

Herausforderung – „Security für AI“

Gezielte Cyber-Angriffe gegen AI-Systeme und AI-Infrastrukturen sowie die daraus resultierenden Sicherheitsvorfälle nehmen bereits massiv zu.

Währenddessen setzt sich die Security-Branche noch immer intensiv damit auseinander, wie AI-Technologien effektiv mit technischen Lösungen gegen diese Cyber-Angriffe abgesichert werden können.

So bezeichnen einige Security-Experten AI aktuell gemeinhin als schwächstes Glied in der Kette, welches es Cyber-Kriminellen ermöglicht, langjährig erfolgreich etablierte Schutzmaßnahmen und Security-Wirkprinzipien mit einfachsten Mitteln zu überwinden.

Neben den häufig noch fehlenden Governance- und Compliance-Vorgaben zur rechtssicheren Nutzung von AI, sehen sich insbesondere die operativen IT-Security-Teams mit verschiedensten Fragestellungen zur sicheren Verwendung und zum Schutz von AI konfrontiert:

- Welche neuartigen Angriffsvektoren entstehen bei der Verwendung von AI-Technologie und wie können wir uns davor schützen?
- Welche unterschiedlichen Arten von AI-Tools gibt es und sind diese bereits bei uns im Einsatz sowie zur Nutzung freigegeben (Stichwort **Shadow AI**)?
- Wie funktionieren AI-Agenten grundsätzlich und können diese überhaupt sicher betrieben werden?
- Wie lassen sich eigene AI-Infrastrukturen und Large Language Models (LLMs) sicher betreiben?

Lösungsansatz – AI Security Workshop

Der AI Security Workshop bietet einen strukturierten Einstieg in das Themenfeld „Security für AI“. Hierbei wird die notwendige Basis zur systematischen Absicherung und für den sicheren Einsatz von AI-Technologien in Unternehmen und Behörden geschaffen.

Innerhalb des eintägigen Security Workshops erarbeiten wir unter anderem:

- Ein einheitliches Verständnis zu den Technologien Generative AI und Agentic AI sowie den damit verbundenen Security-Implikationen
- Typische Anwendungsfälle für den Einsatz von Generative und Agentic AI sowie damit verbundene IT-Risiken und potenzielle Angriffsvektoren
- Tiefergehende Analyse von aktuellen Cyber-Angriffen gegen AI-Systeme
- Etablierte Security Best Practices, AI Security Frameworks und verschiedene Lösungsansätze zur Absicherung von AI

Zur Ausgestaltung des Workshops greifen die Security Consultants der Controlware auf ihre langjährigen praktischen Erfahrungen im Kontext Offensive Security und Cyber Defense zurück.

Nutzen – Was nehmen Sie mit?

Nach Abschluss des AI Security Workshops verfügen Sie über ein einheitliches tiefergehendes Verständnis zu Risiken sowie konkreten Angriffsvektoren rund um Generative AI und Agentic AI. Weiterhin haben Sie einen Überblick über aktuelle Security Best Practices sowie Lösungs- und Architekturansätze zur Absicherung von AI-Systemen.

Das erlangte Wissen erlaubt es Ihnen, das eigene Sicherheitsniveau im Kontext AI zu bewerten und dieses durch eine Ableitung entsprechender operativer sowie strategischer Maßnahmen zu optimieren.

Warum Controlware?

Die Controlware GmbH ist einer der führenden unabhängigen Systemintegratoren und Managed Service Provider. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Cloud-, Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Der Betrieb erfolgt dabei über das ISO 27001- und ISO 9001-zertifizierte Customer Service Center der Controlware.

Unsere Spezialisten verfügen über Expertisen in verschiedensten Branchen, mit vielfältigen Technologien und für unterschiedlichste Unternehmensgrößen.

Die Kombination unserer langjährigen Expertise (Controlware Security seit 1996) mit marktführenden Anbietern von Security-Lösungen steht für erfolgreiche Projekte.

Zusätzlich verschafft uns der höchste Partnerstatus von Controlware bei nahezu allen unseren etablierten Technologie-Partnern zahlreiche Vorteile, die wir gerne an Sie weitergeben.

Mit unseren Controlware Offensive Security und Cyber Defense Services erhalten Sie für Ihr Unternehmen modular passende Security Services – mit konkreten Handlungsempfehlungen von unseren erfahrenen Analysten, die zu Ihrer Infrastruktur passen.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de