



NICHT NUR DIE VERTEIDIGER NUTZEN KI – SONDERN AUCH DIE ANGREIFER

Die Integration von Künstlicher Intelligenz in die Cybersicherheit ist unaufhaltsam, wirft aber auch Fragen nach Vertrauen und Kontrolle auf. Wie gelingt der Spagat zwischen innovativer Technologie und verlässlichem Schutz? Daniel Neuhaus, CEO, und Markus Ehrenmann, CTO der Open Systems AG zeigen auf, wie Transparenz, eine starke Datenbasis sowie der «Human-in-the-loop»-Ansatz eine ganzheitliche Sicherheit im KI-Zeitalter gewährleisten.



Daniel Neuhaus
Chief Executive Officer
Open Systems



Markus Ehrenmann
Chief Technology Officer
Open Systems

Herr Neuhaus, Herr Ehrenmann, derzeit ist KI in aller Munde und viele Unternehmen fragen sich, welche Partner sie auf ihrem Weg in die KI-Zukunft begleiten können. Warum sollte man Open Systems in diesem Zusammenhang berücksichtigen?

Daniel Neuhaus: Wir unterscheiden uns vor allem in zwei zentralen Punkten deutlich vom Wettbewerb: Zum einen setzen wir nicht auf Einzellösungen, sondern auf eine zentrale Plattform. Viele Anbieter im Cybersecurity-Markt bieten sogenannte «Point Solutions» an, sprich isolierte Lösungen für einzelne Aufgaben wie E-Mail-Sicherheit oder Zugriffskontrolle. Doch diese Fragmentierung erhöht für Unternehmen die Komplexität, die Kosten und die Fehleranfälligkeit – denn man muss «Sicherheit» ganzheitlich denken. Open Systems verfolgt dagegen einen Plattformansatz: Netzwerk- und Sicherheitsfunktionen werden in einer vollständig integrierten Lösung zusammengeführt. Das sorgt für Effizienz, Transparenz und Stabilität im Betrieb.

Und wobei handelt es sich beim zweiten Differenzierungsmerkmal?

Daniel Neuhaus: Um das Kundenerlebnis! In einem Markt, der von M&A-Aktivitäten geprägt ist und in dem sich Technologien zunehmend angleichen, entsteht Differenzierung heute über den Service. Darum setzen wir von Open Systems auf ein holistisches 360°-Service-Modell, das Technologie mit dem Betrieb und dem Serviceerlebnis eng verzahnt. Oder anders ausgedrückt: Künstliche Intelligenz entfaltet dann ihre volle Wirkung, wenn man sie mit menschlicher Kompetenz vereint. Dieses holistische Angebot überzeugt auch namhafte Analysten: Open Systems wurde mehrfach als führender Anbieter im Bereich “Managed SASE” ausgezeichnet.



Künstliche Intelligenz entfaltet dann ihre volle Wirkung, wenn man sie mit menschlicher Kompetenz vereint.



Worum handelt es sich bei SASE genau?

Markus Ehrenmann: SASE steht für «Secure Access Service Edge» und kombiniert Netzwerksicherheit und Konnektivität in einem cloudbasierten Modell. Es ermöglicht Nutzerinnen und Nutzern somit sicheren Zugriff auf Anwendungen und Daten – unabhängig davon, wo sie sich befinden. Bei Open Systems bieten wir eine vollständig gemanagte SASE-Lösung, die sich flexibel anpasst und höchste Sicherheitsstandards erfüllt. Mit Blick nach vorn bauen wir auf unsere starke Datenbasis und investieren gezielt in diverse KI-Frameworks – um unseren Kundinnen und Kunden auch künftig das bestmögliche, adaptive Service-Erlebnis zu bieten.

Open Systems existiert bereits seit Jahrzehnten. Wie schafft man es auch nach über 35 Jahren am Markt, ein ganzheitliches Kundenerlebnis sicherzustellen?

Daniel Neuhaus: Ganz wichtig hierfür ist es, nicht nur auf die Technologie zu fokussieren – denn ein ganzheitliches Kundenerlebnis ist das Resultat eines durchdachten, zukunftsorientierten Geschäftsmodells. Dazu gehören Effizienzgewinne durch optimierte Total Cost of Ownership (TCO) ebenso wie die Fähigkeit, Unternehmen bei regulatorischen Anforderungen wie NIS2 oder DORA wirksam zu unterstützen. Unsere Kunden erwarten heute nicht einzelne Produkte, sondern ein verlässliches «Rundum-Sorglos-Paket» aus Technologie und Services. Wir begleiten globale Marktführer wie den Bauchemiehersteller Sika oder den Systemanbieter GEA über viele Jahre hinweg bei der Transformation ihrer Netzwerk- und Sicherheitsarchitektur. Diese langjährige Erfahrung fließt in jedes neue Projekt ein – spürbar, strukturiert und nachhaltig.

Markus Ehrenmann: Gleichzeitig ist Vertrauen entscheidend: Kunden wollen wissen, mit wem sie es zu tun haben. Hat der Partner tiefgehende Engineering-Kompetenz? Wie stabil ist das Team – wie steht es um Fluktuation und Know-how-Erhalt? Woher rekrutiert der Partner seine Talente, und aus welchem politischen Umfeld heraus agiert er? Wie werden Daten verarbeitet, gespeichert und geschützt? Und: Ist das Unternehmen finanziell solide aufgestellt – oder nur eine kurzfristige Erscheinung am Markt? Diese und viele weitere Fragen fließen in den Entscheidungsprozess ein. Open Systems überzeugt hier durch Transparenz,

Substanz und ein starkes Fundament – technologisch, personell und unternehmerisch. Wir sind ein Schweizer Unternehmen, das den hiesigen Markt und die geltenden Regulationen kennt. Mit unserem Mutterkonzern, der Schweizerischen Post, stellen wir uns nachhaltig als verlässlicher und kompetenter Cybersecurity-Partner auf.

Wie integrieren Sie konkret Künstliche Intelligenz in Ihre Plattform und Produkte?

Markus Ehrenmann: Wir verfolgen zwei komplementäre Ansätze zur Integration von KI – beide entwickeln wir konsequent weiter. Beim ersten Ansatz geht es darum, KI oder AI für operative Sicherheit in Echtzeit einzusetzen. Das bedeutet, dass unsere Dienste für sichere, stabile Konnektivität sorgen – etwa, indem sie schädliche Webseiten, infizierten Datenverkehr oder Phishing-E-Mails zuverlässig erkennen und blockieren. Hier setzen wir auf klassische Machine-Learning-Methoden wie Mustererkennung und Klassifikation. Dabei kombinieren wir die Ergebnisse mehrerer Analysequellen, um möglichst umfassenden Schutz zu gewährleisten.

Und wie lautet der zweite Ansatz?

Markus Ehrenmann: Wir nutzen Generative AI auf Basis unserer eigenen Betriebsdaten. Im laufenden Betrieb erfassen wir umfangreiche Telemetriedaten, z. B. welche Webseiten aufgerufen oder blockiert wurden, ergänzt durch Prozessdaten – meist unstrukturierte Texte. Diese Datenbasis bildet die Grundlage für unsere diversen KI-Frameworks. Wir entwickeln damit spezialisierte AI-Agenten, die als virtuelle Experten bestimmte Prozesse oder Kundenanfragen bearbeiten können. Miteinander kombiniert bilden sie einen intelligenten Copiloten, der Daten analysiert, Diagnosetools nutzt und wie ein erfahrener Mitarbeitender agiert. Der Mehrwert für unsere Kunden ist vielschichtig: Schnellere Reaktionszeiten sowie ein effizienterer Ressourceneinsatz bei gleichbleibend hoher oder steigender Qualität stellen entscheidende Pro-Argumente dar. Ein weiterer wichtiger Benefit: Durch die aggregierte, anonymisierte Nutzung von Daten über verschiedene Kunden hinweg können wir Bedrohungen frühzeitig erkennen und präventiv Schutzmassnahmen auch für andere Kunden aktivieren – damit spannen wir einen kollektiven Schutzschirm auf, der mit jeder neuen Information intelligenter wird.

Wie unterstützt KI konkret die Mitarbeitenden Ihrer Kundenbetriebe bei ihrer täglichen Arbeit?

Markus Ehrenmann: Das lässt sich nur bedingt pauschal beantworten – die Einsatzmöglichkeiten von KI entwickeln sich rasant weiter. Entscheidend ist, dass wir die Technologie gezielt so einsetzen, dass sie Qualität und Effizienz steigert – und dabei regulatorische Anforderungen jederzeit berücksichtigt werden. Aktuell sehen wir drei zentrale Anwendungsbereiche in unserem Unternehmen. Der erste betrifft die schnelle, umfassende Recherche: KI unterstützt unsere Mitarbeitenden bei der Informationsbeschaffung zu Markttrends, technologischen Entwicklungen und in der Dokumentation – schneller und tiefergehend, als es manuell möglich wäre. Der zweite Anwendungsbereich betrifft das effizientere Software-Engineering: Gerade bei neuen Projekten (Vibe Coding) leisten Software-Copiloten wertvolle Unterstützung. Bei der Wartung bestehender Software ist jedoch Fingerspitzengefühl gefragt – hier kann unkritischer Einsatz die Codequalität beeinträchtigen. Wir setzen AI gezielt dort ein, wo ihre Stärken liegen, und kennen auch ihre Grenzen. Und zu guter Letzt der dritte Aspekt: die Steigerung von Qualität und Reaktionsgeschwindigkeit in Service und Betrieb, der aktuell unser wichtigstes Einsatzfeld darstellt.

Inwiefern ist dieser Anwendungsbereich der wichtigste?

Markus Ehrenmann: Weil KI uns dabei hilft, auf Kundenanfragen und Vorfälle schneller und gezielter zu reagieren – durch vorbereitete Analysen, Vorschläge inkl. Handlungsoptionen. So bleibt mehr Zeit für die wirklich wichtigen Entscheidungen. Alle genannten Aspekte dienen unserem übergeordneten Ziel: Als Technologieunternehmen fördern wir aktiv den Einsatz von KI-Tools – denn nur wenn unsere Mitarbeitenden innovativ arbeiten, bleiben auch wir als Organisation innovativ.



Unser Ziel besteht letztlich darin, die Mitarbeitenden gezielt zu entlasten: Repetitive, fehleranfällige oder unattraktive Aufgaben übernimmt die KI – so bleibt mehr Raum für strategische Kundenberatung und kreative Problemlösung.

Viele Fachleute betonen, dass KI nicht ohne menschliche Intelligenz funktioniert. Sie haben ebenfalls die menschlichen Kompetenzen bereits angesprochen. Wie kombinieren Sie KI und HI (Human Intelligence) im Service?

Markus Ehrenmann: Wir verfolgen einen klaren Human-in-the-loop-Ansatz (der Mensch behält den Überblick): Jede kritische Massnahme oder Änderung in unserem Service wird von einem zertifizierten Mission-Control-Ingenieur – unserem spezifisch ausgebildeten und hochspezialisierten Team für den operativen 24/7-Betrieb – geprüft und freigegeben. So stellen wir sicher, dass Qualität und Verantwortung auch im Zeitalter von KI gewahrt bleiben. Zugleich verstehen wir diesen Prozess als Feedback-Loop für unseren KI-Copiloten – die menschliche Entscheidung hilft dem System, kontinuierlich zu lernen und besser zu werden.

Transparenz ist ebenfalls zentral: Nutzerinnen und Nutzer werden immer informiert, wenn sie mit einem KI-Agenten kommunizieren. Das schafft Vertrauen und ermöglicht eine bessere Einordnung der Situation. Unser Ziel besteht letztlich darin, die Mitarbeitenden gezielt zu entlasten: Repetitive, fehleranfällige oder unattraktive Aufgaben übernimmt die KI – so bleibt mehr Raum für strategische Kundenberatung und kreative Problemlösung. Das steigert nicht nur die Effizienz, sondern auch die Motivation im Team.

Welche wesentlichen Entwicklungen im Bereich SASE und AI erwarten Sie – und wie bereiten Sie sich darauf vor?

Daniel Neuhaus: SASE ist ein Plattformansatz, der Netzwerk- und Sicherheitsfunktionen konsolidiert. Der Markt verlagert sich von isolierten Perimeterlösungen hin zu integrierten, Cloud-nativen Konzepten, in denen Zero Trust, automatisiertes Threat Detection und proaktive Posture Management-Komponenten, auch in Bezug auf KI, nahtlos zusammenspielen. Dies entspricht dem steigenden Bedarf an durchgängiger Transparenz und Skalierbarkeit in hybriden IT-Umgebungen, wie wir sie bei unseren Kunden vorfinden.

Der Einsatz von Künstlicher Intelligenz, insbesondere generativen und domänenspezifischen Modellen, verändert die Bedrohungslage grundlegend. KI steigert zwar Effizienz und Automatisierung, schafft jedoch gleichzeitig neue potenzielle Angriffsflächen. Besonders im Sicherheitskontext kann der unkontrollierte Einsatz von KI-Systemen zu erhöhter Verwundbarkeit führen wie etwa durch fehlerhafte Outputs, mangelnde Absicherung von Modellschnittstellen oder unzureichende Kontrollmechanismen.

Parallel dazu verändert sich die Art und Weise, wie Nutzer mit Systemen interagieren. Klassische Benutzeroberflächen treten zunehmend in den Hintergrund, während ereignis- und ergebnisorientierte Abläufe, häufig gesteuert durch KI oder Agentic Frameworks, in den Vordergrund rücken.

Technologien wie SASE und KI verändern die Spielregeln. Darum setzen wir auf eine zukunftsorientierte Führung und schaffen eine Kultur, die Lernagilität, Veränderungskompetenz und unternehmerischen Mut stärkt. Denn die Zukunft bleibt ungewiss.



Technologien wie SASE und KI verändern die Spielregeln. Darum setzen wir auf eine zukunftsorientierte Führung und schaffen eine Kultur, die Lernagilität, Veränderungskompetenz und unternehmerischen Mut stärkt.



Markus Ehrenmann: KI steigert nicht nur unsere Effizienz – sondern auch die der Angreifer. Wir beobachten einen Wandel hin zu gezielten Angriffen auf Netzwerkebene und personalisierten Phishing-Versuchen. Generell durchlaufen Unternehmen nun einen grundlegenden Sicherheitswandel: von Perimeter-Sicherheit hin zu Zero Trust, getrieben durch SASE, MDR und die zunehmende Cloud-Nutzung (IaaS, PaaS, SaaS). Themen wie Security Posture Management werden dadurch zentral. Wir unterstützen unsere Kunden, ihre Verwundbarkeit während dieser Transformationen minimal zu halten. Unsere Lösungen entstehen in Co-Creation-Prozessen – mit Fokus auf Nutzerfreundlichkeit, relevanten Funktionen und messbarem Wertbeitrag. Auch die Kommunikation verändert sich, sie wird kontextbezogener und ereignisgesteuert. Dafür entwickeln wir Agenten, die unsere bisherigen formularbasierten Portale ablösen und dynamische Interaktionen ermöglichen. Generative KI beschleunigt diese Entwicklung. Agenten übernehmen Prozesse in Plattformen wie Salesforce oder ServiceNow – und wir öffnen uns dafür, über sichere Schnittstellen auch mit den Agenten unserer Kunden zu interagieren. Denn in einer vernetzten Welt ist Vertrauen das wertvollste Gut – und genau darauf bauen wir bei Open Systems.

Über Open Systems:

Open Systems AG ist ein führender Anbieter von integrierten, Managed SASE-Lösungen, der Netzwerk- und Sicherheitslösungen auf einer cloudbasierten Plattform vereinen. Open Systems unterstützt Unternehmen und Organisationen in mehr als 180 Ländern mit einem ganzheitlichen, kundenorientierten Servicemodell, das Expertensupport rund um die Uhr garantiert. Die Kombination aus innovativer Plattform, integrierten Lösungen und exzellentem Service gewährleistet einen sicheren, zuverlässigen und sorgenfreien Netzwerkbetrieb – selbst in den komplexen IT-Infrastrukturen globaler Produktionsunternehmen bis hin zu NGOs.

Nebst zuverlässiger Konnektivität über Cloud-, On-Premises- und Hybrid-Umgebungen hinweg bietet die Lösung auch ein intuitives Kundenportal für ein herausragendes Nutzererlebnis. Unterstützt durch eine zentrale Datenplattform und 24x7 Managed Services steigert Open Systems nebst der Sicherheit auch die betriebliche Effizienz und beschleunigt Innovationen – für sichere Netzwerke, die mit Ihrem Unternehmen wachsen. Das Schweizer Cybersecurity-Unternehmen mit Hauptsitz in Zürich wurde 1990 gegründet und ist seit 2024 eine Konzerngesellschaft der Schweizerischen Post.

Weitere Informationen unter open-systems.com.



Open Systems bietet Managed SASE-Lösungen, die Netzwerk- und Sicherheitsfunktionen in einer cloudbasierten Plattform vereinen und hybride IT-Umgebungen sicher vernetzen – für mehr Effizienz, Sicherheit und maximale Skalierbarkeit.