THE AI-READY BOARD

by
Rene Schmidli

Rene Schmidli

René Schmidli, ein Finanzexperte mit über 30 Jahren Investmenterfahrung, deckte bereits 1993 als Finanzanalyst den Technologiesektor ab und begleitete im Jahre 2000 ein Tech-IPO in der Schweiz. Heute arbeitet er selbstständig in verschiedenen Verwaltungsrats- und Beratungsfunktionen. Im Dezember 2024 schrieb er, motiviert von der rasanten Entwicklung bei KI, seine CAS-Arbeit über Generative AI bei Mateusz Dolata an der Universität Zürich, um eine praxisnahe Betrachtung von AI-Strategie und Governance-Themen in Verwaltungsräten vorzunehmen.

"In einer hypervernetzten Welt, in der Künstliche Intelligenz die Sicherheitslandschaft grundlegend verändert, wird Cybersecurity zum entscheidenden Faktor – wichtiger denn je"

Alvaro Amato

Alvaro Amato, Executive mit über 20 Jahren internationaler Führungserfahrung. Mit Schwerpunkten in Sales & Marketing sowie Cybersecurity verfügt er über ausgewiesene Expertise in für Verwaltungsräte strategisch relevanten Themen. Er ist Regional Director Globals EMEA & APAC und Verwaltungsratspräsident der Schweizer Niederlassung bei Check Point, absolvierte den EMBA an der Universität Zürich sowie das International Board Certificate der Universität Bocconi und HSG St. Gallen. Sein Fokus liegt auf Cybersecurity, AI und Unternehmensstrategie in Internationalen Boards.

Künstliche Intelligenz verändert die Spielregeln der Cybersecurity grundlegend – sie ist zugleich mächtige Angriffswaffe wie auch unverzichtbares Verteidigungsinstrument

---

Rene Schmidli: Cyber Security wird regelmässig als eine der Top Prioritäten bei Umfragen unter Verwaltungsräten genannt. Neu gesellt sich der Begriff AI hinzu. Du stehst täglich im Kontakt mit Kunden als Vertreter von Check Point Software, einer der ältesten und bekanntesten Cyber-Security-Firmen der Welt. Gib uns doch einen ersten Überblick, wie die zwei abstrakten Begriffe im Zusammenhang stehen.

Alvaro Amato: Grundsätzlich kann unterschieden werden zwischen AI als Angriffswaffe oder aber Angriffe auf und über die eingesetzte AI selbst.

Künstliche Intelligenz ist längst zur mächtigen Angriffswaffe im Cyberraum avanciert. Sie versetzt Cyberkriminelle in die Lage, Angriffsflächen neu auszunutzen und Angriffsmuster zu perfektionieren. Mithilfe generativer AI werden täuschend echte Stimmen, Bilder und Videos erzeugt, die gezielt für Social-Engineering-Attacken genutzt werden, etwa bei CEO-Fraud oder Identitätsdiebstahl. Deepfakes lassen sich so authentisch generieren, wie nie zuvor, während automatisierte Phishing-Kampagnen durch AI eine neue Qualität erreichen: Personalisierte Nachrichten wirken glaubwürdiger, erschweren klassische Schutzmechanismen und hebeln gewohnte Erkennungsroutinen aus. Gleichzeitig ermöglicht AI, Sicherheitslücken in Code oder Systemen schneller zu erkennen und automatisiert von der Analyse bis zur Entwicklung neuer Schadsoftware vorzugehen. Damit hat sich die Dynamik der Angriffe entschieden beschleunigt und professionalisiert.

Doch auch die AI selbst gerät zunehmend ins Visier raffinierter Angreifer. Mit Techniken wie Prompt Injection oder gezielter Manipulation der Trainingsdaten können sie die Modelle „umprogrammieren" z.B. Zugriff

auf vertrauliche Daten, oder gezielt falsche Outputs provozieren. Gekonntes Data Poisoning sorgt dafür, dass schon kleine Veränderungen im Input die Entscheidungsgrundlage von Modellen nachhaltig verfälschen. Stellt man sich das z.B. im Rahmen einer Kreditvergabe vor, wird die Tragweite schnell ersichtlich. Nicht zuletzt versuchen Angreifer, geistiges Eigentum durch Model Theft oder Reverse Engineering zu extrahieren, indem sie etwa über API-Abfragen Strukturen und Inhalte der Modelle rekonstruieren. Das zeigt: Die Bedrohungslage wandelt sich rasant, und aus Sicht der Cyberabwehr ist ein tiefes Verständnis für die neuen, AI-basierten Angriffsformen ebenso entscheidend wie kontinuierliche Innovation und wachsame, menschliche Expertise an der Seite moderner Technologie.

Rene Schmidli: Was bedeutet die veränderten Spielregeln konkret für das Bedrohungsszenario aus Sicht einer Firma?

Alvaro Amato: Künstliche Intelligenz verändert die Spielregeln im Cybercrime-Markt grundlegend: Dank „Crime-as-a-Service"-Modellen und leistungsstarken AI-Tools können selbst technisch unerfahrene Angreifer heute komplexe Attacken aufsetzen, die früher nur absoluten Experten vorbehalten waren. Dadurch sinken die Eintrittsbarrieren dramatisch, während Geschwindigkeit und Volumen von Angriffen rasant zunehmen. Hochprofessionelle Attacken werden zur Massenware, die sich innerhalb kürzester Zeit millionenfach ausrollen lassen und auch gezielt an schwächere Infrastrukturen angepasst werden. Der Cybercrime-Markt erlebt damit eine Demokratisierung: Gefährliches Expertenwissen wird für breitere Tätergruppen zugänglich, wodurch Verteidiger vor völlig neue Herausforderungen gestellt werden.

Rene Schmidli: Wo liegen nun die grössten Einfallstore in einem Unternehmen?

Alvaro Amato: Ein Unternehmen kann technologisch bestens aufgestellt sein und doch bleiben seine Mitarbeiter das grösste Einfallstor für moderne Cyberattacken. Gerade im Jahr 2025 ist Social Engineering in Verbindung mit immer ausgefeimteren Phishing-Methoden das dominante Angriffsmuster. Nahezu jeder zweite Cybersicherheitsvorfall geht auf menschliche Fehler oder Manipulation zurück. AI-gestützte Mails, Deepfakes und betrügerische Kommunikationskanäle werden so realistisch, dass selbst geschulte Personen nur schwer zwischen echt und fake unterscheiden können. Die zunehmend hybride Arbeitswelt verschärft die Situation: Geräte und Dienste außerhalb geschützter Netzwerke machen es Attackierenden leicht, Schwachstellen auszunutzen oder Schatten-IT zu etablieren. Sensibilisierung und fortlaufende Awareness sind heute elementarer Teil jeder nachhaltigen Sicherheitsstrategie.

Neben dem „Faktor Mensch" sind ungesicherte technische Schnittstellen die Achillesferse im digitalen Unternehmen. Ungeschützte Cloud-Dienste, vernachlässigte APIs oder vernetzte Endgeräte am Netzwerkrand öffnen oft Türen für kriminelle Akteure – insbesondere, wenn Patches und Sicherheitsupdates zu spät eingespielt werden. Auch die Einbindung von Lieferanten und externen Partnern über gemeinsam genutzte Plattformen oder AI-Modelle schafft neue Angriffsflächen entlang der gesamten Supply Chain. Cyberkriminelle nutzen diese Verkettungen gezielt, um Umgehungspfade zu finden oder Zugriff auf besonders sensible Unternehmensbereiche zu erlangen. Moderne Angriffsmuster kombinieren technische Exploits und psychologische Manipulation zu einem dichten Bedrohungsnetz, das strategische Weitsicht, technische Resilienz und ein wachsames Risikomanagement auf höchster Ebene erfordert.

Rene Schmidli: Viele Unternehmen beginnen mit AI-Projekten in kontrollierten Sandbox-Umgebungen, um Risiken zu minimieren. Wie passt Shadow AI in dieses Bild, wenn Mitarbeitende AI-Tools außerhalb der vorgesehenen Systeme und Prozesse nutzen?

Alvaro Amato: Sandbox-Umgebungen sind gezielt dafür konzipiert, AI-Anwendungen sicher und risikofrei zu testen: Sie reduzieren potenzielle Schäden durch klare Trennung, Monitoring und Einschränkungen im Zugriff auf produktive Daten und Systeme. Shadow AI hingegen bezeichnet AI-Anwendungen, die von Mitarbeitenden ohne offizielle Freigabe und Governance eingesetzt werden und damit außerhalb der Sicherheitskontrollen ablaufen. Das birgt erhöhte Risiken, da solche inoffiziellen AI-Tools oft sensible Daten ungeschützt weiterverarbeiten und ungefiltert mit externen Anbietern kommunizieren. Shadow AI entzieht sich

somit der Disziplin und den Schutzmechanismen, die Sandboxen bieten. Unternehmen müssen daher verstärkt Transparenz schaffen, ein Vertrauens- und Schulungsklima etablieren sowie klare Richtlinien und Überwachungsmechanismen einführen, um Shadow AI zu kontrollieren und die Vorteile von kontrollierten Sandbox-Experimenten nicht durch versteckte Risiken zunichtezumachen.

Rene Schmidli: Nun haben wir die Risiken, welche AI-indiziert von aussen und innen im Zusammenhang mit Cyber auftauchen können, gut abgesteckt. Wie kann nun AI seinerseits eingesetzt werden, um Cyber-Risiken zu reduzieren? Welche Ansätze bestehen und in welche Richtung entwickelt sich das «ewige Wettrennen», zwischen Angreifer und Verteidiger?

Alvaro Amato: Wie Du richtig sagst, hat die Münze je zwei Seiten und AI sich zu einem unverzichtbaren Werkzeug für die Cybersicherheit respektive zur Abwehr entwickelt. Durch die kontinuierliche Analyse von Nutzer- und Netzwerkverhalten kann AI subtile, ungewöhnliche Aktivitäten erkennen, die auf Angriffe oder Gefahren durch eigene Mitarbeitende respektive kompromittierte Konten hinweisen (Insider-Bedrohungen). Dadurch lassen sich Betrugsversuche oder unberechtigter Zugriff bereits in einem frühen Stadium identifizieren und verhindern, lange bevor Menschen diese Muster überhaupt bemerken.

Darüber hinaus ermöglichen AI-gestützte Systeme die automatisierte Erkennung und sofortige Reaktion auf Bedrohungen. Sie verarbeiten und analysieren in Echtzeit riesige Datenmengen, identifizieren potenzielle Gefahren und leiten umgehend Gegenmassnahmen ein. Dies verkürzt die Zeit zwischen Erkennung und Reaktion erheblich.

Ein weiterer entscheidender Vorteil ist die Lernfähigkeit der AI, als Gegenmassnahme zu immer neuen Angriffsstrategien. Die Modelle verbessern sich kontinuierlich durch Maschinelles Lernen und passen sich an neue Bedrohungsmuster an. So können sie selbst unbekannte oder Zero-Day-Bedrohungen (eine bis heute unbekannte Schwachstelle, die neu ausgenützt wird) präzise erkennen und abwehren. Zudem ermöglicht die AI-basierte Vernetzung und Kontextanalyse von Informationen aus verschiedenen Quellen das Erkennen komplexer Angriffsszenarien, was die Prävention und Reaktion weiter optimiert.

Nicht zuletzt spielt AI eine wichtige Rolle beim Schutz sensibler Daten. Sie überwacht den Datenfluss und Zugriffe, erkennt unerlaubte Datenbewegungen oder Schatten-IT und hilft so, Datenverluste sowie Compliance-Verstöße effektiv zu verhindern.

Rene Schmidli: Die Materie ist komplex, bedarf aber wegen ihrer Tragweite einer strategischen Herangehensweise, welche auch in einem Verwaltungsrat einen festen Platz haben muss. Risikobasierte Ansätze, welche versuchen, ökonomische Einflüsse zu quantifizieren, scheinen das Mittel der Wahl zu sein, um Investitionsentscheide bezüglich Cybersicherheit auch im Zeitalter von AI sinnvoll treffen zu können. Kannst Du mir dazu etwas sagen?

Alvaro Amato: Ja, gerne, Du hast Recht. AI ist nicht nur ein technisches Thema, sondern ein strategischer Vermögenswert, der beide Seiten hat: grosses Innovationspotenzial wie auch neue komplexe Risiken. Verwaltungsräte müssen diese Risiken verstehen und in ihre Gesamtstrategie für Unternehmensrisikomanagement, inklusive Cybersicherheit, integrieren. Ein risikobasierter Ansatz heisst, dass nicht nur qualitative Einschätzungen, sondern konkrete, messbare Grössen verwendet werden, um AI-Risiken einzuschätzen. Ein bekanntes Modell ist der FAIR Ansatz (Factor Analysis of Information Risk), welcher eine probabalistische und finanzielle Bewertung von AI-Risiken ermöglicht. Der Prozess umfasst fünf klare Schritte: Kontextualisierung der Risiken, Definition des Geltungsbereichs, Quantifizierung von Eintrittswahrscheinlichkeiten und finanziellen Folgen, Priorisierung von Gegenmassnahmen sowie eine datengestützte Entscheidungsfindung.

Der Vorteil liegt darin, dass eine gemeinsame Sprache zwischen Risikomanagern und Entscheidungsträgern geschaffen wird. AI-Risiken werden in konkreten Zahlen «messbar» gemacht, z.B. erwartet finanzielle Verluste (Kundenabwanderungen, Bussgelder, Schadenersatzforderungen etc.) mit Eintrittswahrscheinlichkeiten versehen, so dass kalkulierte Entscheidungen möglich sind. Durch das systematische Vorgehen werden AI-

Risiken, wie andere Risiken offengelegt, was Transparenz schafft, eine sinnvolle Überwachung und Investitionspolitik erleichtert.

Rene Schmidli: Wie lässt sich nun die Wirksamkeit oder die Effizienz von ergriffenen Massnahmen beurteilen?

Alvaro Amato: Die Effizienz von AI-gestützten Abwehrsystemen bei Cyberangriffen bemisst sich primär an der Geschwindigkeit und Präzision, mit der Bedrohungen erkannt und abgewehrt werden. Wichtige Kennzahlen sind dabei die Mean Time to Detect (MTTD) und Mean Time to Respond (MTTR), welche messen, wie schnell Angriffe identifiziert und neutralisiert werden. Je kürzer diese Zeiten, desto höher die Effizienz des Systems, da automatisierte AI-Reaktionen den manuellen Aufwand drastisch reduzieren und Security-Teams ermöglichen, mehr Vorfälle bei gleichem Personal zu bearbeiten.

Darüber hinaus spielt die Automatisierungsrate eine zentrale Rolle: Wie viele Abwehrreaktionen können selbstständig durch AI ohne menschliches Eingreifen ausgeführt werden? Eine hohe Quote automatisierter Abwehraktivtäten steigert die Produktivität und minimiert menschliche Fehlerquellen.

Neben der Effizienz ist die Effektivität der Schutzmassnahmen entscheidend. Hierzu zählen die Quote der verhinderten Vorfälle, oft als Blockierquote angegeben, sowie die Reduktion des Schadensausmasses durch erfolgreiche Abwehr. AI-Systeme sind in der Lage, auch unbekannte Zero-Day-Angriffe mit sehr hohen Blockraten von bis zu 99,8% abzuwehren, wie es z.B. Check Point Software Technology an den Tag legt. Dies senkt signifikant die potenziellen finanziellen Schäden, etwa durch Ausfallzeiten oder Datenverluste. Business-relevante Kennzahlen wie Systemverfügbarkeit, vermiedene Ausfallstunden und abgesicherte Datenlecks werden dadurch positiv beeinflusst.

Moderne AI-basierte Sicherheitssysteme operieren rund um die Uhr in Echtzeit und nutzen kontextbezogene Mustererkennung, um selbst komplexe und neuartige Angriffe mit chirurgischer Präzision zu neutralisieren, ohne den normalen Geschäftsbetrieb zu stören. So ergibt sich ein umfassender Schutz, der die Sicherheit deutlich erhöht und gleichzeitig die Ressourcen von Sicherheitsteams optimal nutzt.

Insgesamt zeigen erfolgreiche AI-Abwehrmassnahmen eine Kombination aus schneller Erkennung, hoher Automatisierung, maximaler Blockierquote und signifikanter Schadensminderung, was sowohl Betriebskosten senkt als auch die Resilienz gegenüber Cyberbedrohungen stärkt.

Rene Schmidli: Cyber-Risiken sind nicht neu, erhalten aber aufgrund der Möglichkeiten der Angreifer als auch der Verteidiger dank AI eine neue Dimension, wobei der Mensch als Angriffspunkt nach wie vor das grösste Risiko bleibt. Welche abschliessende Empfehlung hast Du bezüglich AI-Governance für einen Verwaltungsrat?

Alvaro Amato: So ist es, und deshalb reicht es nicht, nur auf technische Schutzmechanismen zu setzen. Es braucht eine klare organisatorische Antwort. Ein wirksames Awareness-Programm beginnt damit, Transparenz über die eingesetzten Systeme zu schaffen: Welche KI-Tools werden genutzt, wo liegen Risiken, und wo könnten sich Schattenlösungen einschleichen, die ausserhalb der Unternehmensrichtlinien betrieben werden? Darauf aufbauend gilt es, Mitarbeitende nicht nur zu schulen, sondern ihnen auch eine gemeinsame Sprache und ein Verständnis für Chancen und Risiken von AI zu vermitteln. So entsteht ein Bewusstsein, das im Alltag trägt und verhindert, dass gut gemeinter, aber unkontrollierter Einsatz von Werkzeugen zu erheblichen Sicherheitslücken führt.

Parallel dazu braucht es eine Governance-Struktur, die das Thema nicht dem Zufall überlässt. Unternehmen sollten ein interdisziplinäres Gremium schaffen, in dem IT, Recht, Compliance und Fachbereiche zusammenwirken, um den Einsatz von AI zu steuern. Dieses Gremium definiert klare Rollen und Verantwortlichkeiten, etabliert Risikoklassen für unterschiedliche Anwendungen und sorgt dafür, dass ressourcenintensive Prüfungen dort erfolgen, wo sie am dringendsten sind. Ein dreistufiges Verteidigungsmodell, das operative Teams, Governance-Funktionen und interne Revision voneinander trennt, schafft zusätzliche Sicherheit und

Transparenz. Bezogen auf den Verwaltungsratsgremien gehört das Thema idealerweise in das Risk & Audit Committee. Standardisierte Rahmenwerke wie ISO 42001 oder der NIST AI Risk Management Framework geben dabei Orientierung und machen Governance überprüfbar und vergleichbar (Organisation und Rollen).

Für den Verwaltungsrat bedeutet das in der Konsequenz, dass er sich nicht allein auf technologische Antworten verlassen darf. Seine Aufgabe ist es, den Rahmen zu setzen, in dem Innovation sicher stattfinden kann: durch klare Governance, durch Bewusstseinsschaffung im Unternehmen, durch gezielte Kontrolle und durch eine kontinuierliche Weiterentwicklung der Massnahmen. Damit wird Governance zum Schlüsselinstrument, das nicht Innovation hemmt, sondern sie nachhaltig ermöglicht – und den Menschen vom grössten Risiko zum entscheidenden Erfolgsfaktor.