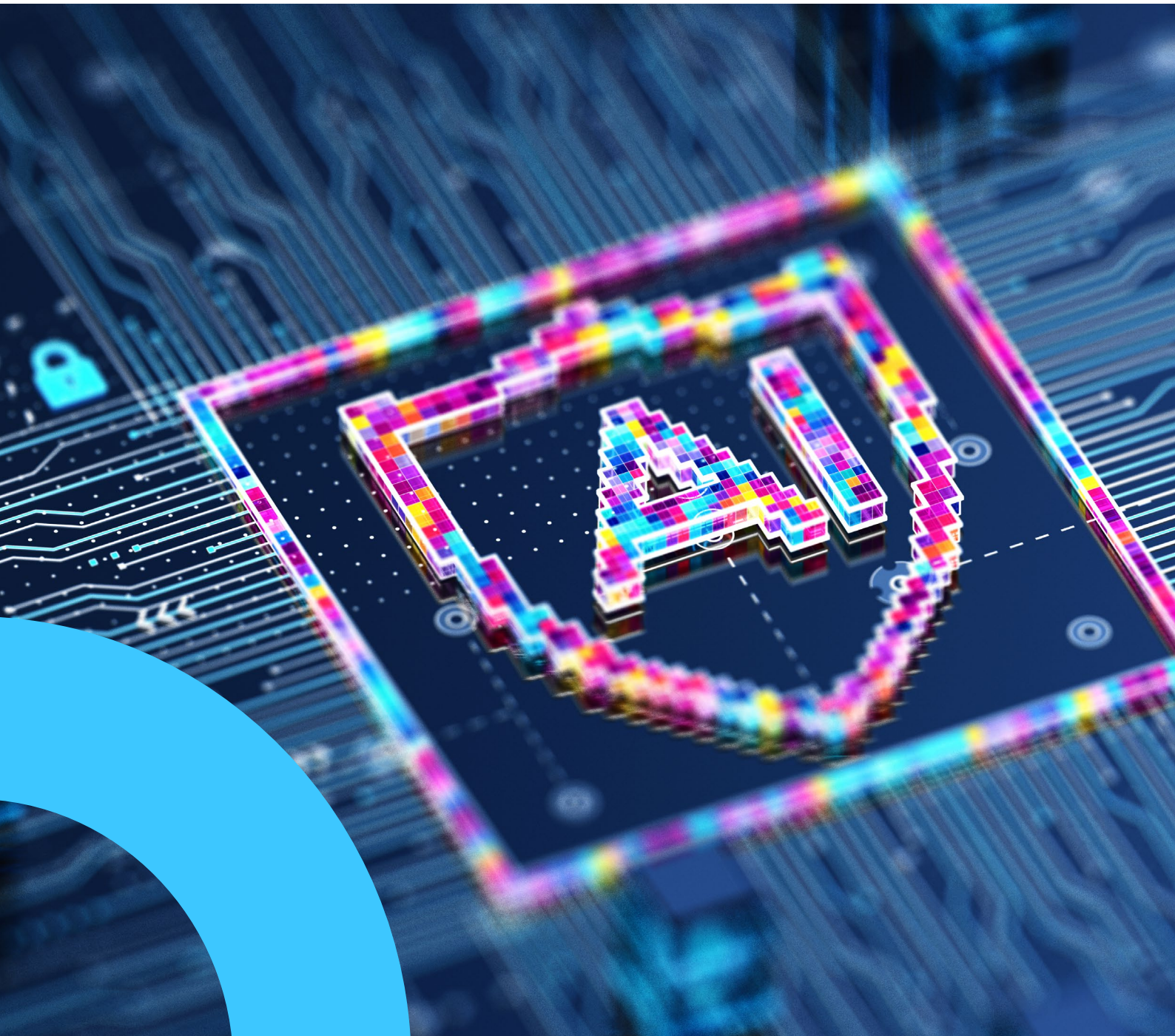


Adaptive Cyber-Resilienz im Zeitalter der Künstlichen Intelligenz

Digitale Souveränität und Vertrauen mit der
Geschwindigkeit von KI sichern



C-Level-Briefing

Cybersecurity hat einen Wendepunkt erreicht. Ausschlaggebend dafür ist eine grundlegende Veränderung ihrer operativen Rahmenbedingungen.

Die klassischen Sicherheitsperimeter werden bereits seit Jahren durch Mobilität, hybrides Arbeiten, Globalisierung, Cloud-Technologien und digitale Ökosysteme aufgelöst. Neu sind jedoch **Geschwindigkeit** und **Dimension** dieser Entwicklung.

Bedrohungen agieren heute mit **Maschinengeschwindigkeit** und überholen damit Sicherheitskonzepte, die nach wie vor überwiegend auf menschlichen Reaktionszeiten basieren. Gleichzeitig verändert Künstliche Intelligenz sowohl die Angriffs- als auch die Verteidigungsseite grundlegend. Regulatorische Anforderungen verlangen heute keine punktuellen Nachweise mehr, sondern eine kontinuierliche und jederzeit belegbare Wirksamkeit von Sicherheitsmaßnahmen. Parallel dazu hat sich digitale Souveränität von einem politischen Diskussionsthema zu einer operativen Notwendigkeit entwickelt.

Cyber Risiken gelten inzwischen als das weltweit bedeutendste Geschäftsrisiko und stehen damit im Mittelpunkt der Aufmerksamkeit von Vorständen und Geschäftsleitungen. Gleichzeitig wachsen trotz steigender Budgets die Erwartungen der Stakeholder schneller als die Investitionen. Risiken, Kosten und regulatorische Anforderungen entwickeln sich dynamischer als viele Sicherheitsprogramme. Für das Management stellt sich daher längst nicht mehr die Frage, ob mehr in Cybersecurity investiert wird, sondern ob die Organisation im Ernstfall schnell wieder Kontrolle erlangen kann – und ob sie dies jederzeit nachweisen kann.

**Die Prinzipien von Cybersecurity bleiben bestehen. Das Betriebsmodell muss sich ändern.
Es muss mit maschineller Disziplin ausgeführt werden.**

Die heutigen Cybersecurity-Architekturen, auf die sich die meisten Unternehmen verlassen, basieren auf soliden Prinzipien, wurden aber für die Ausführung in menschlicher Geschwindigkeit, über fragmentierte Umgebungen hinweg konzipiert und weitgehend durch Dokumentation belegt. Dieses Modell reicht nicht mehr aus, da IT und OT konvergieren, KI und Datenpipelines zu operativen Abhängigkeiten werden, Ökosysteme expandieren und Störungen sich schneller über Abhängigkeiten hinweg ausbreiten, als Menschen koordinieren können.

Zusätzliche Tools und Kontrollen allein schließen diese Umsetzungslücke nicht. Entscheidend ist ein Wandel in der operativen Sicherheitsdisziplin: weg von einer rein präventionsorientierten Ansammlung von Kontrollen, hin zu einem resilienten Betriebsmodell, das Störungen antizipiert, Auswirkungen begrenzt und eine schnelle Wiederherstellung ermöglicht.

Atos nennt dies **Adaptive Cyber Resilience**.

Adaptive Cyber Resilience versteht Cybersecurity nicht als weiteres Framework, eine zusätzliche Checkliste oder einen neuen Technologie-Stack. Vielmehr beschreibt sie eine adaptive Betriebsdisziplin, deren Ziel darin besteht, unter allen Bedingungen die Kontrolle zu behalten, Störungen schnell zu bewältigen und Resilienz kontinuierlich nachzuweisen. Dieses Betriebsmodell basiert auf vier untrennbar miteinander verbundenen Grundprinzipien:

- Künstliche Intelligenz ist integraler Bestandteil der Security Operations
- Digitale Souveränität wird als grundlegendes Architekturprinzip verstanden
- Cybersecurity wird anhand geschäftlicher Ergebnisse und nicht anhand der Anzahl implementierter Werkzeuge bewertet
- Die Verantwortung des Menschen bleibt erhalten – auch wenn operative Abläufe mit Maschinengeschwindigkeit erfolgen

Adaptive Cyber Resilience bringt Geschwindigkeit und Disziplin zusammen. In einem kontinuierlichen Zyklus aus **Vorbereitung** (Prepare), **Reaktion** (Respond), und **Anpassung** (Adapt) wird Resilienz von einem Zielbild zu einer steuerbaren operativen Fähigkeit. **Prepare** schafft Bereitschaft, bevor eine Störung eintritt. **Respond** begrenzt Auswirkungen und ermöglicht eine schnelle, technisch nachweisbare Wiederherstellung. **Adapt** sorgt dafür, dass sich Sicherheit kontinuierlich weiterentwickelt und mit dem geschützten Umfeld Schritt hält. Eine übergreifende Governance- und Steuerungsebene verbindet dabei die strategischen Zielsetzungen des Vorstands mit der operativen Umsetzung und schließt die Lücke zwischen Unternehmensstrategie und täglichem Sicherheitsbetrieb.

Dieses Whitepaper erläutert, welche Veränderungen Cybersecurity heute prägen, welche Fragen Führungskräfte beantworten müssen und wie Unternehmen durch konsequente operative Umsetzung die Kontrolle zurückgewinnen können. Es richtet sich an Entscheiderinnen und Entscheider, die Verantwortung für Geschäftsergebnisse tragen – nicht an Organisationen, die sich noch in einer Experimentierphase befinden.

Atos bringt dabei mehr als 25 Jahre Erfahrung aus dem Betrieb geschäftskritischer Systeme, souveräner Infrastrukturen und hochregulierter Branchen ein. Mit Atos Cybersecurity Services und Eviden Cybersecurity Products verbindet Atos diese Erfahrung zu einem integrierten Betriebsmodell, das auch unter hoher Belastung, in komplexen Umgebungen und über lange Zeiträume hinweg zuverlässig funktioniert.

Cybersecurity wird neu definiert. Organisationen werden diese Zukunft entweder durch disziplinierte Widerstandsfähigkeit gestalten oder unter Druck darauf reagieren.

Der Wandel: Warum das bisherige Modell nicht mehr ausreicht

Jeder Vorstand betrachtet Cybersecurity heute als strategisches Risiko. Deutlich weniger Unternehmen können jedoch eine einfache Frage beantworten: **Wenn morgen etwas schiefgeht – wie schnell gewinnen wir die Kontrolle zurück, und können wir dies jederzeit nachweisen?**

Diese Lücke zwischen Problembewusstsein und tatsächlicher Handlungsfähigkeit ist kein Zeichen mangelnden Engagements. Sicherheitskontrollen bleiben wichtig. Compliance bleibt wichtig. Doch statische Kontrollmechanismen und periodische Nachweise passen nicht mehr zu den heutigen Betriebsrealitäten.

Unternehmen arbeiten heute in dynamischen Abhängigkeiten zwischen Cloud, IT, OT, Partnern, APIs, Datenströmen und KI-Systemen. Dadurch entsteht eine Angriffsfläche, die weit über die Grenzen hinausgeht, für die viele Sicherheitsmodelle ursprünglich entwickelt wurden. Gleichzeitig eröffnet diese Entwicklung die Chance, Kontrollen effizienter und wirkungsorientierter zu gestalten. Das Ergebnis ist ein wachsendes Risiko, das häufig schwer sichtbar, selten durchgängig verantwortet und zunehmend schwierig einzudämmen ist.

Der klassische Sicherheitsperimeter hat an Bedeutung verloren. Heute entstehen wirksame Grenzen vor allem über Identitäten, APIs sowie zunehmend über Modelle und Agenten, die über Ökosysteme hinweg agieren. Kontrolle ist verteilt, Abhängigkeiten sind tief verankert, und viele Organisationen haben kein vollständiges Bild mehr von den Umgebungen, die sie schützen müssen. Dafür gibt es mehrere Gründe:

1. KI verändert die Gleichung dauerhaft

KI beschleunigt Cybersicherheit nicht nur – sie verändert das Kontrollmodell. Angriffe erfolgen schneller, Schwachstellen werden früher ausgenutzt, und klassische Security Operations geraten an ihre Grenzen. Gleichzeitig führen agentenbasierte Systeme delegierte Entscheidungsbefugnisse in digitale Prozesse ein. Wird ein solcher Agent kompromittiert, entsteht weit mehr als ein Datenschutzproblem. Der Agent wird zu einem digitalen Insider mit der Fähigkeit, selbstständig Handlungen auszuführen.

2. Geopolitische Spannungen haben Cybersecurity zu einer Souveränitätsfrage gemacht

Staatlich unterstützte Bedrohungsakteure, Instrumentalisierung in der Lieferkette und die Fragmentierung der globalen Technologielandschaft haben Cybersecurity untrennbar mit souveräner Kontrolle verbunden. Organisationen, die in verschiedenen Rechtsordnungen operieren, sehen sich nun einem Bedrohungsumfeld gegenüber, das nicht nur von kriminellen Akteuren, sondern auch von nationalen Zielen, wirtschaftlichem Zwang und Informationskrieg geprägt ist. Wer die Daten besitzt, die Infrastruktur kontrolliert und die Technologie liefert, bestimmt nun das Cyberrisiko der Organisation in Echtzeit.

3. Komplexität hat die Kontrolle überholt

Mehr Tools garantieren keine Kontrolle. Mehr Warnmeldungen garantieren keine besseren Entscheidungen. Da KI Angriffe beschleunigt und vernetzte OT die Kontrolllücke vergrößert, muss Sicherheit daran gemessen werden, wie schnell sie Bedrohungen

erkennen, eindämmen und wiederherstellen kann. Das Problem liegt nicht mehr allein in der Technologie. Es liegt in einem Betriebsmodell, das seinem Zweck nicht mehr gerecht wird.

4. Die Realität in den Vorstandsetagen

Cybersecurity entscheidet heute über Geschäftskontinuität, regulatorische Risiken und digitale Souveränität. Vorstände und Geschäftsleitungen tragen zunehmend Verantwortung für Risiken, die sie oftmals weder vollständig beobachten noch unmittelbar kontrollieren können. Gleichzeitig gleichen sich regulatorische Erwartungen weltweit immer stärker an. Sicherheitsmaßnahmen müssen kontinuierlich wirksam sein und ihre Belastbarkeit auch unter realen Betriebsbedingungen nachweisen. Da Sicherheitsverletzungen inzwischen als realistischer Ausgangspunkt betrachtet werden, wird Cybersecurity an ihren Ergebnissen gemessen: Wie schnell werden Angriffe erkannt? Wie wirksam lassen sich ihre Auswirkungen begrenzen? Wie schnell gelingt die Wiederherstellung? Und lässt sich all dies objektiv belegen?

5. Das Innovationsdilemma

Jede digitale, Cloud- und KI-Transformationsinitiative erweitert die Angriffsfläche. Jede neue Anwendung bringt einen Software-Stack, eine Lieferkette und neue Abhängigkeiten mit sich. Jeder zusätzliche Datenfluss und jeder agentische Workflow schafft neue Angriffspunkte. Wird Sicherheit erst am Ende eines Projekts geprüft, bleibt sie dauerhaft im Reaktionsmodus. Sicherheit muss von der Planung bis zum Betrieb eingebettet, kontinuierlich und adaptiv werden.

Das bisherige Sicherheitsmodell scheitert letztlich daran, dass es Cybersecurity als Sammlung einzelner Kontrollmechanismen für weitgehend stabile Systeme versteht.

Die heutige Unternehmens-IT ist jedoch dynamisch, verteilt, hochgradig vernetzt und gleichzeitig den Anforderungen von Angreifern, Regulierungsbehörden und der eigenen digitalen Transformation ausgesetzt.

Cybersecurity kann deshalb nicht länger als spezialisierte Funktion am Rand der Organisation bestehen. Sie muss integraler Bestandteil des Unternehmens werden – mit klarer Verantwortung der Geschäftsbereiche und eindeutiger Rechenschaftspflicht auf Führungsebene.

Dieser Wandel ist unumgänglich. Er ist die Voraussetzung für eine sichere Unternehmensführung in einer zunehmend digitalen Welt.

Das neue Gebot: Was sich ändern muss

Die Erkenntnis, dass sich das bestehende Modell weiterentwickeln muss, reicht nicht aus. Die entscheidendere Frage ist, wodurch es ersetzt werden soll. Die Antwort liegt nicht in Verfeinerungen, Erweiterungen oder schrittweisen Verbesserungen. Vielmehr geht es darum, die praktische Umsetzung von Cybersecurity grundlegend neu zu definieren.

Erforderlich ist ein grundlegender Wandel in der Art und Weise, wie Cybersecurity konzipiert, gesteuert und betrieben wird, von einer statischen, kontrollbasierten Disziplin hin zu einem dynamischen, resilienzgetriebenen Betriebsmodell, das mit Geschäftsergebnissen im Einklang steht.

Die wichtigste Veränderung betrifft dabei nicht die Technologie, sondern Führung und Governance. Technologie ermöglicht diesen Wandel – sie ist jedoch nicht sein Ausgangspunkt. Für einige Organisationen hat diese Entwicklung bereits begonnen. Für viele andere beschreibt sie den Weg, den modernes Cybersecurity-Management künftig einschlagen muss. Im Folgenden werden die fünf zentralen Veränderungen erläutert, die diesen Wandel prägen.

1. Von zusätzlichen Kontrollen zu kontinuierlicher Steuerung

Der Wandel besteht nicht darin, mehr vom Gleichen schneller zu tun. Es geht darum, Security so zu gestalten, dass sie kontinuierlich steuerbar, messbar und handlungsfähig wird.

Security Operations werden heute von einer Flut an Warnmeldungen überrollt. Mehr Alarme bedeuten jedoch nicht automatisch mehr Kontrolle. Im Mittelpunkt muss deshalb der Übergang von einer alarmgetriebenen zu einer informationsgestützten Entscheidungsfindung stehen. Signale müssen in konkrete Maßnahmen übersetzt werden, die nach ihrem geschäftlichen Einfluss priorisiert, mit Kontext angereichert und mit hoher Geschwindigkeit umgesetzt werden.

2. Von rein menschlicher Cybersecurity zu einer Zusammenarbeit von Mensch und KI

Moderne Bedrohungen entwickeln sich heute mit einer Geschwindigkeit, einem Umfang und einer Komplexität, die menschliche Teams allein nicht mehr bewältigen können. Cybersecurity auf Maschinengeschwindigkeit erfordert daher KI-gestützte Erkennung, Priorisierung und Reaktion. Künstliche Intelligenz ersetzt dabei nicht das menschliche Urteilsvermögen, sondern erweitert dessen Leistungsfähigkeit. KI muss integraler Bestandteil eines klar geregelten Betriebsmodells sein, in dem jede automatisierte Aktion nachvollziehbar, reversibel und einer verantwortlichen Instanz zugeordnet werden kann. Die letztendliche Verantwortung verbleibt stets beim Menschen.

3. Von standardisierter Cybersecurity hin zu kontextbezogener, souveräner und ergebnisorientierter Sicherheit

Einheitsmodelle werden der Vielfalt moderner Unternehmensrisiken nicht gerecht.

Risikotoleranz und Prioritäten unterscheiden sich je nach Geschäftsmodell, regulatorischen Verpflichtungen, Souveränitätsanforderungen und Abhängigkeitslandschaft. Deshalb muss Sicherheit kontextbezogen gestaltet und an Ergebnissen gemessen werden, die Vorstände verstehen und steuern können.

Eine regulierte Bank und ein multinationales Unternehmen, das mit staatlichen Daten arbeitet, haben nicht dieselben Prioritäten, Abhängigkeiten oder akzeptablen Risikoniveaus.

4. Cybersecurity als zentrale Unternehmensfunktion

Cybersecurity kann nicht länger als technische Funktion innerhalb der IT gesteuert werden. Sie ist heute eine geschäftskritische Kernfunktion, die unmittelbar Einfluss auf Umsatzsicherung, Vertrauen von Kunden und Partnern, regulatorische Handlungsfähigkeit sowie die Einführung neuer Technologien hat. Daraus ergeben sich neue Anforderungen an die Unternehmensführung: Cybersecurity benötigt eine Steuerung auf Vorstandsebene, messbare Kennzahlen für die Geschäftsbereiche, klar definierte Verantwortlichkeiten innerhalb des gesamten Partnerökosystems sowie eine enge Einbindung in strategische Entscheidungen zu Digitalisierung, Cloud, Künstlicher Intelligenz, Unternehmensakquisitionen, der Zusammenarbeit zwischen Mensch und Maschine sowie den Anforderungen an die digitale Souveränität.

5. Von Schutz zu adaptiver Resilienz

Prävention ist nach wie vor notwendig, reicht aber allein nicht mehr aus. Bei der Cybersecurity muss davon ausgegangen werden, dass es zu Störungen kommen wird, und es muss die Bereitschaft bestehen, kritische Vorfälle zu erkennen, die Auswirkungen einzudämmen, kritische Abläufe aufrechtzuerhalten und sich zügig wieder zu erholen. Dies ist der Wandel vom reinen Schutz hin zu adaptiver Widerstandsfähigkeit – eine Betriebshaltung, die unter Druck aufgebaut, getestet, gemessen und kontinuierlich verbessert wird.

Nach dem CrowdStrike Global Threat Report 2026 sank die durchschnittliche Zeit bis zur lateralen Ausbreitung eines eCrime-Angriffs im Jahr 2025 auf nur noch 29 Minuten. Im schnellsten beobachteten Fall vergingen zwischen Erstzugriff und Ausbreitung lediglich 27 Sekunden.

- 2026 CrowdStrike Global Threat Report



Die entscheidenden Fragen, die sich jeder Vorstand heute stellen sollte

Der Übergang zu einer adaptiven Cyber-Resilienz beginnt nicht mit technischen Detailfragen, sondern mit den richtigen Führungsfragen.

Sie zeigen, ob Cybersecurity tatsächlich als operative Führungsaufgabe verstanden wird oder ob sie sich im Wesentlichen auf dokumentierte Prozesse und Compliance-Nachweise beschränkt.

Top 10 Fragen

1

Sind sich alle Geschäftsverantwortlichen der Cyberrisiken in ihren Prozessen und Produkten bewusst und tragen sie dafür Verantwortung – mit klar definierten Entscheidungsbefugnissen, Kennzahlen und Eskalationswegen?

2

Verfügen wir über eine durchgängige Sicht auf Identitäten, Zugriffsrechte, privilegierte Berechtigungen sowie die Identitäten von Maschinen und KI-Agenten über unsere gesamte hybride IT-Landschaft hinweg?

3

Falls morgen ein Sicherheitsvorfall eintritt: Können wir ihn schnell genug erkennen, seinen Ausbreitungsradius nachvollziehen, wirksam eindämmen und den Geschäftsbetrieb zügig wiederherstellen?

4

Sind unsere Datenpipelines und Plattformen für KI-Agenten wirksam gegen Datendiebstahl und Manipulation von KI-Systemen geschützt?

5

Haben wir die Assets und Geschäftsprozesse identifiziert und geschützt, die für Umsatz, operative Leistungsfähigkeit und das Vertrauen des Marktes von entscheidender Bedeutung sind?

6

Ist unser gesamtes Cybersecurity-Ökosystem darauf vorbereitet, KI-gestützte Angriffe zu erkennen und mit Maschinengeschwindigkeit darauf zu reagieren?

7

Verfügen wir über eine Strategie, um die Sicherheits- und Souveränitätsrisiken der Plattformen, Daten und KI-Modelle zu beherrschen, von denen wir abhängig sind?

8

Ist unsere Cybersecurity ausreichend aufgestellt, um unsere Wachstumsstrategie zu unterstützen – einschließlich der Erschließung neuer Märkte, der Sicherung des Kundenvertrauens sowie der Einführung von Cloud-Technologien, KI und anderen Zukunftstechnologien?

9

Wissen wir jederzeit, wo unsere KI-Systeme betrieben werden, unter wessen Kontrolle sie stehen und welche Garantien hinsichtlich Sicherheit und digitaler Souveränität bestehen?

10

Verfügen wir über einen zukunftssicheren Plan für den Zeitpunkt, an dem Quantencomputer heutige kryptografische Verfahren angreifen können?

Unternehmen, die sich diese Fragen ehrlich stellen und die daraus gewonnenen Erkenntnisse konsequent umsetzen, werden diese Lücke schließen. Wer ihnen hingegen ausweicht, wird die Antworten erst im Ernstfall erhalten mit potenziell langfristigen Auswirkungen auf das Geschäft.

Unsere Vision: Wie wir darauf reagieren

Cybersecurity braucht kein weiteres Framework. Die Anforderungen der Cybersecurity erfordern heute ein anderes Betriebsmodell, das auf wachsende Komplexität, Geschwindigkeit, Souveränität und Verantwortlichkeit ausgelegt ist.

Atos nennt dieses Modell **Adaptive Cyber Resilience**.

Es beschreibt den Wandel:

Von fragmentierten Werkzeugen zu kohärenter Kontrolle.

Von statischen Abwehrmechanismen zu adaptiver Resilienz.

Von periodischer Compliance zu kontinuierlicher Nachweisbarkeit.

Von Prävention als Ziel zu Kontinuität als Ergebnis.

Adaptive Cyber Resilience vereint vier untrennbare Veränderungen:

1. KI im Zentrum der Security Operations
2. Digitale Souveränität als operative Anforderung
3. Sicherheit gemessen an Geschäftsergebnissen
4. Die menschliche Verantwortung bleibt auch dann erhalten, wenn die Ausführung mit maschineller Geschwindigkeit läuft

Dies ist keine Zukunftsvision, sondern das Betriebsmodell, das Cybersecurity heute benötigt.

1. KI für die Sicherheit. Sicherheit für KI

Künstliche Intelligenz verändert Cybersecurity in zweifacher Hinsicht. Zum einen beschleunigt sie Sicherheitsprozesse und erhöht deren Wirksamkeit. Zum anderen entstehen durch KI neue Systeme, die selbst geschützt und gesteuert werden müssen.

Auf der Verteidigungsseite verbessert KI Geschwindigkeit, Präzision und Konsistenz sicherheitsrelevanter Entscheidungen – von der Priorisierung von Risiken über den Nachweis von Sicherheitskontrollen bis hin zu Schutzmaßnahmen, Angriffserkennung und Incident Response.

KI darf dabei nicht lediglich ein weiteres Werkzeug sein. Sie muss zum operativen Kern moderner Security Operations werden.

Durch großskalige Mustererkennung über Millionen von Ereignissen hinweg ermöglicht sie Bedrohungserkennung mit Maschinengeschwindigkeit, eine kontinuierliche Überwachung von Identitäten und Cloud-Sicherheitskonfigurationen sowie Reaktionszeiten, die sich von Stunden auf wenige Sekunden verkürzen. Eine solche Analyseleistung wäre durch menschliche Teams allein nicht mehr zu bewältigen.

Richtig eingesetzt entwickelt sich Cybersecurity dadurch von einer Vielzahl isolierter Einzelmaßnahmen zu einer kontinuierlichen, informationsgestützten Entscheidungs- und Steuerungsfunktion.

Gleichzeitig entsteht eine zweite, ebenso wichtige Dimension: Wenn Unternehmen KI und agentische Systeme in ihre Geschäftsprozesse integrieren, werden diese Systeme selbst zu kritischen digitalen Assets.

Diese müssen gezielt abgesichert werden. KI-Modelle, Trainingsdaten, Entscheidungspipelines und agentische Workflows schaffen neue Angriffsflächen und erfordern neue Formen von Governance, Überwachung und Laufzeitkontrolle. Wenn KI nicht nur Ergebnisse erzeugt, sondern Aktionen auslöst, verschieben sich die zentralen Risiken: Neben Datenexposition und Missbrauch treten Kontrollverlust, Zielabweichungen und unbeabsichtigtes autonomes Verhalten.

Die Steuerung muss zur Laufzeit durchsetzbar sein, nicht zur Entwurfszeit impliziert. Das bedeutet, Autonomie zu begrenzen, KI-Verhalten beobachtbar zu machen, Richtlinien kontinuierlich durchzusetzen und die Fähigkeit zu bewahren, die Ausführung zu unterbrechen, wenn das Verhalten von den beabsichtigten Zielen abweicht. Entscheidungen und Handlungen müssen nachvollziehbar und prüfbar bleiben, mit expliziter menschlicher Verantwortlichkeit.

Ohne diese Disziplin skaliert die KI-Fähigkeit schneller als die Fähigkeit einer Organisation, Risiken zu kontrollieren. Damit wird KI zu einem geregelten, prüfaren und vertrauenswürdigen Bestandteil des Unternehmens, selbst wenn die Autonomie zunimmt.

Atos verankert KI im Kern von Cybersecurity, getrieben von einem **doppelten Auftrag: die Beschleunigung der Sicherheitsabläufe und die Absicherung der KI-Systeme selbst**.



Evidens Vertrauensfundament für Künstliche Intelligenz

Mit dem Übergang von Künstlicher Intelligenz aus Pilotprojekten in geschäftskritische Anwendungen wird Vertrauen zu einer technischen Eigenschaft, die gezielt entwickelt werden muss. Es entsteht nicht von selbst. **Eviden Cybersecurity-Produkte bieten die grundlegenden Cyber-Fähigkeiten, die erforderlich sind, um KI im großen Maßstab vertrauenswürdig zu machen.**

1. **Der Schutz von Daten geht heute über die Verschlüsselung klassischer IT-Umgebungen hinaus und umfasst die gesamte KI-Pipeline, Daten während der Nutzung sowie Retrieval-Augmented Generation (RAG). Dadurch wird die Vertraulichkeit von Daten entlang des gesamten Lebenszyklus – von der Datenaufnahme bis zur Inferenz – sichergestellt.**
2. **AI Identity Governance** steuert Berechtigungen, Zugriffsrechte, Lebenszyklen, Nachvollziehbarkeit und kontinuierliches Monitoring, damit Zugriffe und Aktionen kontrollierbar, nachvollziehbar und verantwortbar bleiben.
3. **Digitale Identitäten für KI-Agenten** stellen durch Zertifikate oder Identity Wallets sicher, dass autonome Agenten eindeutig identifiziert und kryptografisch abgesichert werden. Dadurch entstehen Authentifizierung, Vertrauen und Nachverfolgbarkeit über Organisations- und Systemgrenzen hinweg.

Gemeinsam helfen diese Grundlagen Kunden dabei, KI mit Vertrauen einzusetzen und zugleich Kontrolle, Verantwortlichkeit und Nachvollziehbarkeit zu bewahren – auch wenn Autonomie, Skalierung und regulatorische Anforderungen zunehmen.



Souveränität als operative Disziplin

Digitale Souveränität hat sich zu einem strategischen Thema entwickelt. Gleichzeitig gehört sie noch immer zu den am wenigsten operationalisierten Konzepten im Bereich der Cybersecurity.

In vielen Unternehmen beschränkt sich digitale Souveränität nach wie vor auf Compliance-Anforderungen wie Datenresidenz, vertragliche Regelungen zur Gerichtsbarkeit, Lieferantenbewertungen oder die Auswahl zertifizierter Cloud-Anbieter.

Diese Maßnahmen sind notwendig – sie reichen jedoch nicht aus.

In einer Welt, in der KI-Modelle, Cloud-Infrastrukturen und agentenbasierte Systeme grenzüberschreitend arbeiten, muss digitale Souveränität zu einer operativen Disziplin werden, die über den gesamten IT-Stack hinweg konsequent umgesetzt wird. Sie darf nicht erst im Nachhinein als juristische Fragestellung behandelt werden.

Dies setzt bewusste Entscheidungen über Anwendungen, Infrastrukturen und Lieferketten voraus. Unternehmen müssen festlegen, wo Daten gespeichert und verarbeitet werden, welche Modelle als vertrauenswürdig gelten und wie weit die Autonomie intelligenter Systeme reichen darf. Es bedeutet, zu verstehen, dass Souveränität kein Entweder-oder-Konzept ist.

Sie beschreibt vielmehr ein Spektrum unterschiedlicher Kontrollgrade, das sich nach der Schutzbedürftigkeit der jeweiligen Ressourcen, den regulatorischen Anforderungen und den geschäftlichen Folgen eines möglichen Kontrollverlusts richtet.

Digitale Souveränität legt fest, wer die Kontrolle über Daten, Modelle und Entscheidungen besitzt.

Cybersecurity sorgt dafür, dass diese Kontrolle wirksam, resilient und technisch durchsetzbar bleibt.

Ohne digitale Souveränität fehlt Cybersecurity die notwendige Verantwortlichkeit.

Für Atos ist digitale Souveränität deshalb ein grundlegendes Architekturprinzip, das von Beginn an in jede Lösung integriert wird. Sicherheit ist kein nachträglich hinzugefügtes Element, sondern Bestandteil der Architektur selbst. Dies gilt unabhängig davon, ob Anwendungen in Public-, Private-, Hybrid- oder souveränen Cloud-Umgebungen betrieben werden. Ebenso wichtig ist, dass Governance, Nachvollziehbarkeit und Kontrolle unabhängig vom Betriebsmodell oder den jeweils geltenden geopolitischen Rahmenbedingungen erhalten bleiben. Im Mittelpunkt stehen dabei drei zentrale Fragen: Wo benötigen wir digitale Souveränität? Welchen Grad an Souveränität benötigen wir? Welche operativen Konsequenzen ergeben sich aus diesen bewusst getroffenen Entscheidungen?

Von Kontrollen zu messbarer Wirkung

Die Cybersecurity-Industrie hat Jahrzehnte damit verbracht, sich selbst anhand von Inputs, eingesetzten Werkzeugen, implementierten Kontrollen, bestandenen Audits und erworbenen Zertifizierungen zu messen. Die Vorstände sind damit nicht mehr zufrieden. Sie stellen eine andere Frage.

Welche Wirkung haben unsere Cybersecurity-Investitionen tatsächlich auf die entscheidenden Geschäftsergebnisse?

Dazu gehören beispielsweise die durchschnittliche Zeit bis zur Erkennung eines Angriffs (MTTD), die Zeit bis zu seiner Eindämmung (MTTC), die Dauer der Wiederherstellung (MTTR), vermiedene Betriebsunterbrechungen, verhinderte Datenabflüsse, vermiedene regulatorische Sanktionen, erhaltenes Kundenvertrauen sowie die Sicherstellung der operativen Geschäftskontinuität.

Ergebnisorientierte Sicherheit verbindet Cybersecurity-Aktivitäten direkt mit der Geschäftsleistung – in Echtzeit, nicht nur in Quartalsberichten. Es erfordert kontinuierliche Messung, transparente Berichterstattung und die Disziplin, die Haltung basierend auf den Daten anzupassen.

Atos richtet Cybersecurity-Aktivitäten konsequent an messbaren Geschäftsergebnissen aus. Diese werden in geschäftsnaher Sprache definiert, kontinuierlich verfolgt und mit den Verantwortlichkeiten von Vorstand und Führungsteam verknüpft.

Menschen, Verantwortlichkeit und die nächste Generation von Cyber-Führung

Kein Betriebsmodell – unabhängig von seinem technologischen Reifegrad – kann menschliches Urteilsvermögen, Verantwortung und Führung ersetzen. Was sich verändert, ist jedoch das Profil zukünftiger

Cybersecurity-Führungskräfte.

Sie müssen Künstliche Intelligenz verstehen, operativ denken und Risiken mit hoher Geschwindigkeit bewerten können. Sie müssen nachvollziehen, wie KI-Systeme Entscheidungen treffen, wo ihre Grenzen liegen, wann menschliches Eingreifen erforderlich ist und wie sich KI-generierte Erkenntnisse in belastbare Entscheidungen auf Vorstandsebene übersetzen lassen.

Dabei handelt es sich nicht lediglich um eine Erweiterung bestehender Kompetenzen. Es ist ein grundlegender Generationenwechsel. Die Leistung von Cybersecurity-Teams wird künftig nicht mehr danach beurteilt, wie viele Warnmeldungen sie bearbeiten, sondern danach, wie erfolgreich sie KI-gestützte Sicherheitsprozesse führen und gleichzeitig die menschliche Entscheidungsverantwortung bewahren.

Atos gestaltet diesen Wandel aktiv. Mit KI-orientierten Aus- und Weiterbildungsprogrammen, der gezielten Entwicklung von Cybersecurity-Führungskräften sowie hybriden Betriebsmodellen, in denen Mensch und KI eng zusammenarbeiten, schafft Atos die Voraussetzungen für Cybersecurity mit Maschinengeschwindigkeit – ohne die Verantwortung des Menschen aus der Hand zu geben.

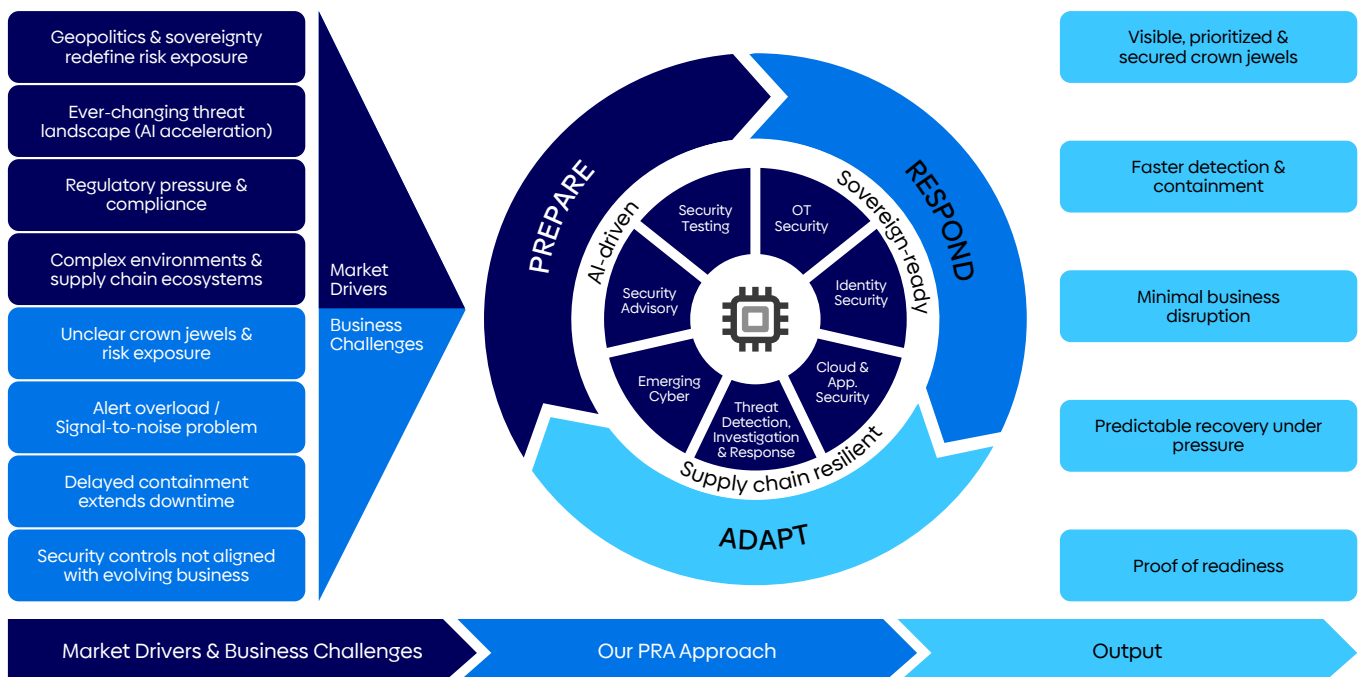


Von der Vision zur Umsetzung: Wie Unternehmen Cyber-Resilienz operationalisieren

Adaptive Cyber Resilience in die Realität umzusetzen, erfordert mehr als nur Absicht. Es erfordert ein Betriebsmodell, das kontinuierlich, unter Druck und über ein fragmentiertes Ökosystem hinweg funktionieren kann.

Hier wird Absicht zur Disziplin.

Ein kontinuierliches Betriebsmodell für KI-gestützte Cyber-Resilienz



Prepare. Respond. Adapt.

Cyber-Resilienz lässt sich nicht als einmaliges Transformationsprogramm oder lineares Projekt aufbauen. Sie muss als kontinuierlicher Kreislauf verstanden werden. Der Prepare-Respond-Adapt-(PRA)-Ansatz ermöglicht es Unternehmen, an jedem Punkt einzusteigen, ihre Sicherheitsmaßnahmen gezielt dort zu stärken, wo sie den größten geschäftlichen Nutzen entfalten, und ihre Resilienz kontinuierlich weiterzuentwickeln.

PRA ist weder ein weiteres Framework noch eine Checkliste oder ein Reifegradmodell. Es handelt sich um ein adaptives Betriebsmodell, das etablierte Sicherheitsstandards und Frameworks in eine kontinuierliche operative Umsetzung überführt – unter den Bedingungen KI-gestützter Bedrohungen, wachsender Systemabhängigkeiten und dauerhaft steigender regulatorischer Anforderungen.



Prepare bedeutet, Risiken zu reduzieren und Vertrauen zu stärken, bevor eine Störung eintritt. Es konzentriert sich darauf, die Exponierung kontinuierlich zu verstehen, geschäftskritische Ressourcen zu identifizieren und Sicherheit und Souveränität standardmäßig in Architekturen, Plattformen und Prozesse einzubauen. Dazu gehören Expositionsmanagement, Compliance by Design, belastbare Sicherheitsfundamente mit integrierter Wiederherstellungsfähigkeit.

Prepare geht nicht davon aus, dass Systeme fehlerfrei sind. Vielmehr basiert dieser Ansatz auf der Annahme

kontinuierlicher Veränderungen und der Notwendigkeit, Sicherheitsmaßnahmen permanent zu überprüfen und ihre Wirksamkeit auch unter Belastung sicherzustellen. Ziel ist es, sowohl die Eintrittswahrscheinlichkeit als auch die Auswirkungen von Sicherheitsvorfällen zu reduzieren und gleichzeitig eine Sicherheitsarchitektur zu schaffen, die Belastungen standhält, ohne ihre Funktionsfähigkeit zu verlieren. Prepare beantwortet letztlich eine grundlegende Frage:

Wenn morgen ein Sicherheitsvorfall eintritt – sind wir heute darauf vorbereitet?

Threat Detection and Incident Response (TDIR)

TDIR bildet die End-to-End-Fähigkeit von Atos zur Cyberabwehr und unterstützt Unternehmen über den gesamten Incident Lifecycle innerhalb des PRA-Modells. Nach dem Verizon Data Breach Investigations Report gehen rund 20% aller Cyberangriffe auf bekannte Schwachstellen zurück. Gleichzeitig hat sich der Zeitraum zwischen der Veröffentlichung einer Schwachstelle und ihrer aktiven Ausnutzung von mehreren Monaten auf wenige Tage oder sogar Stunden verkürzt.

Kontinuierliche Transparenz über die eigene Angriffsfläche ist deshalb unverzichtbar. Im Rahmen des Continuous Threat Exposure Management identifiziert TDIR exponierte Systeme und realistische Angriffspfade frühzeitig, sodass Risiken bereits vor ihrer Ausnutzung reduziert werden können. Kommt es dennoch zu einem Sicherheitsvorfall, entscheidet die Reaktionsgeschwindigkeit über das Ausmaß der Auswirkungen. TDIR kombiniert KI-gestützte Managed Detection and Response (MDR) mit einem virtuellen SOC-Analysten, um Untersuchungen zu beschleunigen und Sicherheitsvorfälle schneller einzudämmen. Interne Benchmarks von Atos zeigen eine Verkürzung der Untersuchungsdauer um bis zu 60% bei KI-optimierten Warnmeldungen sowie eine Reduzierung der Bearbeitungszeit phishingbezogener Vorfälle um bis zu 90%. Dadurch verbessern sich Kennzahlen wie Mean Time to Detect (MTTD) und Mean Time to Recover (MTTR) nachweislich.

Ergänzt wird dieser Ansatz durch Krisensimulationen und Tabletop-Übungen, die Unternehmen dabei unterstützen, ihre organisatorische Resilienz gegenüber einer zunehmend komplexen Bedrohungslage kontinuierlich auszubauen.



Respond bedeutet, Störungen zu erkennen, einzudämmen, zu mindern und zu reparieren.

Sie kombiniert KI-verstärkte Erkennung, schnelle Eindämmung, koordiniertes Krisenmanagement sowie entwickelte, einstudierte und nachweisbare Wiederherstellungsfähigkeiten.

Die Reaktion muss mit maschineller Geschwindigkeit ablaufen und dabei die Entscheidungsbefugnis des Menschen erhalten. Die Recovery sollte bereits in der

Reaktionsphase mit erprobten Abläufen und einer kontrollierten Wiederherstellung eingeplant werden, und zwar bereits während des Vorfalls. Jede Aktion muss nachverfolgbar, auditierbar und reversibel sein.

Widerstandsfähigkeit wird unter Druck bewiesen. Die Reaktion ist erfolgreich, wenn die geschäftliche Wirkung begrenzt ist, Services schnell wiederhergestellt werden und Kontrolle demonstriert werden kann, nicht nur erklärt.

Adapt ist die kontinuierliche Anpassung der Cybersecurity an Veränderungen des Umfelds, sei es durch neue Vorschriften, aufkommende Bedrohungen, technologische Veränderungen oder Geschäftstransformation. Adapt stellt sicher, dass die Sicherheit nicht aus der Linie gerät, während sich das Unternehmen weiterentwickelt.

Dazu gehört die Anpassung der Kontrollen an neue regulatorische Anforderungen, die Integration von Erkenntnissen aus Bedrohungsinformationen und Simulationen, die Verfeinerung von Erkennung und Reaktion basierend auf aufkommendem Angreiferverhalten sowie die Antizipation zukünftiger Risiken wie Post-Quantum-Kryptographie oder agentische KI-Exposition.

Adapt verwandelt Erfahrung, Veränderung und Weitblick in verbesserte Einsatzbereitschaft. Das Ziel ist einfach: Sicherstellen, dass derselbe Vorfall nie auf die gleiche Weise passiert und dass die Sicherheit auch dann wirksam bleibt, wenn sich die Lage verändert.

Prepare-Respond-Adapt ist das operative Rückgrat der Cyber-Resilienz. Prepare baut das Fundament. Respond schützt die Kontinuität unter Stress. Adapt hält die Sicherheit über die Zeit relevant.

Dieser kontinuierliche Verbesserungszyklus ermöglicht es Atos, Kunden in jeder Phase ihrer Resilienzreise zu unterstützen: dort anzusetzen, wo sie heute stehen, und sie gezielt zu dem Reifegrad zu führen, den sie für ihre Geschäfts- und Risikosituation benötigen.

Post Quantum Cryptography (PQC): Ein Resilienz-Imperativ

Die Migration nach der Post Quantum Cryptography (PQC) ist keine zukünftige Überlegung mehr. Sie ist eine unmittelbare Notwendigkeit, getrieben durch greifbare Fortschritte im Quantencomputing und zunehmend explizite Empfehlungen nationaler Behörden weltweit.

Digitales Vertrauen basiert auf Kernelementen wie Identität, sicherer Kommunikation, Softwareintegrität und Datenschutz, die alle auf Kryptographie basieren, die nicht ewig zuverlässig bleiben wird. Die heute gesammelten Daten können später von kryptographisch relevanten Quantencomputern entschlüsselt werden, voraussichtlich um 2035.

Die PQC-Migration wird Jahre dauern und muss jetzt beginnen, über die CISO-Funktion hinaus. Sobald die Kryptographie versagt, kann das Vertrauen nicht mehr schnell wiederhergestellt werden, und die Geschäftskontinuität, regulatorische Exposition und das Marktvertrauen werden gleichzeitig beeinträchtigt.

Die Einführung neuer kryptografischer Algorithmen allein genügt jedoch nicht.

Erforderlich ist eine Crypto Agility, die den gesamten kryptografischen Technologie-Stack umfasst und zukünftige Anpassungen ohne grundlegende Systemumbauten ermöglicht.

Mit den Eviden Cybersecurity Products stellt Atos hierfür europäische, PQC-fähige kryptografische Grundlagen bereit. Diese unterstützen durchgängige Anwendungsfälle – von digitalen Zertifikaten über Datenschutz bis hin zu sicherer Kommunikation.

Was macht PRA umsetzbar

Governance als Cyber-Kontrollschicht

Die meisten Organisationen verfügen über Fähigkeiten; Was fehlt, ist Kohärenz zwischen ihnen. Eine Governance-Kontrollschicht übersetzt die Risikobereitschaft auf Vorstandsebene in durchsetzbare Prioritäten, Verantwortlichkeit und Investitionsentscheidungen. Sie verbindet Sicherheitsarchitektur und Unternehmensstrategie miteinander und stellt sicher, dass der Prepare-Respond-Adapt-Zyklus, der Technologie-Stack, das Partnerökosystem und die verantwortlichen Führungskräfte als integriertes Gesamtsystem agieren – und nicht als voneinander getrennte Einzelinitiativen.

Cybersecurity als Bestandteil der Unternehmenstransformation

Cyber-Resilienz kann nicht nachträglich ergänzt werden. Sicherheit muss von Anfang an in digitale, Cloud- und KI-Initiativen integriert sein. Sie prägt Architekturentscheidungen, Datenflüsse, Modellauswahl, Partnerökosysteme sowie die Verantwortlichkeiten

zwischen Mensch und KI, bevor Systeme in Betrieb gehen oder Modelle skaliert werden.

Wenn Resilienz früh verankert ist, beschleunigt Sicherheit die Transformation. Wird sie erst spät hinzugefügt, wird sie zur Einschränkung und Risiko baut sich unbemerkt auf.

Ein orchestriertes Ökosystem macht Resilienz skalierbar

Keine Organisation kann Cyber-Resilienz allein sicherstellen. Moderne Cybersecurity basiert auf einem komplexen Zusammenspiel von Hyperscalern, spezialisierten Sicherheitslösungen, Unternehmensplattformen, Technologiepartnern und internen Kompetenzen. Entscheidend ist daher die Fähigkeit, dieses gesamte Ökosystem innerhalb eines einheitlichen Governance- und Betriebsmodells zu orchestrieren. Atos verbindet bewusst technologische Wahlfreiheit mit architektonischer Unabhängigkeit. Dadurch werden Sicherheitskontrollen, Anforderungen an die digitale Souveränität, regulatorische Vorgaben und geschäftliche Erfolgskennzahlen über alle beteiligten Anbieter hinweg konsistent umgesetzt.

Die CISO-Agenda für die nächsten 24 Monate

Die erfolgreiche Umsetzung von Cybersecurity erfordert eine konsequente Verbindung von Strategie und operativer Umsetzung. In den kommenden zwei Jahren werden sich erfolgreiche CISOs auf eine klar definierte Anzahl strategischer Prioritäten konzentrieren, um die Cyber-Resilienz ihrer Organisation messbar zu stärken.



Übergreifende Governance- und Steuerungsebene etablieren, die Cybersecurity-Entscheidungen eng mit der Unternehmensstrategie verbindet.



Resilienz von Beginn an in jede Architektur integrieren, mit einem konsequent datenzentrierten Sicherheitsansatz.



Cybersecurity-Teams für den Umgang mit KI qualifizieren, damit sie hybride Betriebsmodelle aus Mensch und KI sicher steuern und die Autonomie intelligenter Systeme verantwortungsvoll kontrollieren können.



Kontinuierliche Transparenz und Sichtbarkeit: Organisationen benötigen durchgängige Transparenz über ihre Assets, Identitäten und Angriffsflächen. Denn Schutz beginnt mit Sichtbarkeit.



Identitäten als zentrale Steuerungs- und Kontrollebene etablieren – für Menschen, Maschinen und KI-Agenten gleichermaßen.



Cybersecurity anhand geschäftlicher Ergebnisse messen und die Berichterstattung gegenüber Geschäftsleitung konsequent an Unternehmenskennzahlen ausrichten.



KI als integralen Bestandteil aller Cybersecurity-Domänen etablieren, wobei KI die operative Skalierung übernimmt und der Mensch die Entscheidungsverantwortung behält.



Souveränität und regulatorische Compliance operationalisieren, sodass ihre Einhaltung jederzeit nachgewiesen werden kann – nicht nur im Rahmen von Audits.



Die Migration zu Post-Quantum-Kryptografie jetzt beginnen, bevor heutige kryptografische Verfahren ihre Schutzwirkung verlieren.

Organisationen, die notwendige Maßnahmen aufschieben, werden denselben Zeitraum überwiegend damit verbringen, auf die Folgen unterlassener Entscheidungen zu reagieren.

Atos: Glaubwürdigkeit, die unter Druck skaliert

Adaptive Cyber-Resilienz kann nicht allein durch Vision erreicht werden. Es erfordert Erfahrung, Umfang und die Fähigkeit, in Umgebungen zu agieren, in denen ein Scheitern keine Option ist.

Als europäischer Marktführer im Bereich Cybersecurity vereint die Atos langjährige Expertise, industrielle Betriebskompetenz und vertrauenswürdige Sicherheitsgrundlagen, um Resilienz in der Praxis wirksam umzusetzen. Dabei verbindet Atos die Cybersecurity-Services für die operative Umsetzung, die Cybersecurity-Produkte von Eviden als Vertrauensanker sowie die Beratungs- und Transformationskompetenz von Atos Amplify.

Erfahrung, die operative Exzellenz prägt

Atos verfügt über mehr als 25 Jahre Erfahrung bei der Bereitstellung von Cybersecurity-Lösungen für Großunternehmen, öffentliche Institutionen und geschäftskritische Infrastrukturen.

In dieser Zeit hat sich Atos gemeinsam mit den grundlegenden Veränderungen der Cybersecurity weiterentwickelt – von klassischen Perimeter-Sicherheitsmodellen über Cloud- und Hybridarchitekturen bis hin zur Konvergenz von IT und OT sowie zu KI-gestützten, informationsbasierten Security Operations. Diese Veränderungen wurden nicht als Reaktion auf Markttrends umgesetzt, sondern aus der praktischen Notwendigkeit heraus, komplexe Betriebsumgebungen dauerhaft sicher zu betreiben.

Gerade in hochregulierten Branchen und unter Krisenbedingungen ist diese operative Erfahrung entscheidend.

Cyber Services für den kontinuierlichen Betrieb

Atos Cyber Services sind für den kontinuierlichen Betrieb über Branchen und Regionen hinweg konzipiert. Sie verbinden Beratungs- und Governance-Leistungen, Sicherheitsarchitektur, Threat Intelligence, Security Operations, Incident Response, Krisenmanagement sowie Wiederherstellungsprozesse zu einem integrierten Leistungsangebot.

Durch ein weltweites Netzwerk mit starker regionaler Präsenz verbindet Atos globale Skalierbarkeit mit lokaler Nähe zu Kunden, Regulierungsbehörden und Betreibern kritischer Infrastrukturen. Dadurch begleitet sie Unternehmen über den gesamten Prepare-Respond-Adapt-Zyklus hinweg – nicht als Folge einzelner Projekte, sondern als konsistente Betriebsdisziplin, die sich an Geschäftsauswirkungen, regulatorischen Anforderungen und den Entscheidungen des Managements orientiert.

Eviden Cybersecurity Products als Vertrauensanker für Kryptografie und Datenschutz

Mit Eviden stellt Atos Cybersecurity-Produkte bereit, die in Europa entwickelt wurden und Security by Design als grundlegendes Architekturprinzip umsetzen. Diese Lösungen adressieren zentrale Vertrauensmechanismen wie digitale Identitäten, Kryptografie, Zugriffssteuerung und Datenschutz.

Sie wurden speziell für Umgebungen entwickelt, in denen Nachweisbarkeit, langfristige Sicherheit und regulatorische Konformität unverzichtbar sind.

Die Eviden Cybersecurity Products erfüllen höchste Zertifizierungs- und Sicherheitsanforderungen sensibler und regulierter Branchen. Sie bilden stabile Sicherheitsanker, auf deren Grundlage Cyber Services auch über lange Lebenszyklen und in sich wandelnden Bedrohungslandschaften zuverlässig betrieben werden können.

Ein pragmatischer Ansatz für digitale Souveränität

Souveränität wird von Atos als eine operative Fähigkeit behandelt, die in der Art und Weise verankert ist, wie Systeme entworfen und verwaltet werden.

Durch Eviden Cybersecurity Products und Atos Cyber Services ist Souveränität in bewusste Entscheidungen und Architekturen eingebettet, die steuern, wo Daten gespeichert und zugänglich sind, wie Identitäten verwaltet werden und wie kritische Prozesse geschützt werden. Dies wird mit einer globalen Präsenz und starken lokalen Lieferfähigkeiten kombiniert, die regulatorische, sektorspezifische und operative Realitäten widerspiegeln.

Dieser Ansatz ermöglicht es Organisationen, Kontrolle, Autonomie und Resilienz in ihren gesamten IT- und OT-Stacks zu behalten, selbst wenn sich Vorschriften, Abhängigkeiten oder geopolitische Bedingungen ändern.

KI als Bestandteil der Cyber Operations

KI ist seit vielen Jahren Bestandteil der Cybersecurity-Operations von Atos – ausgerichtet auf Skalierung, Geschwindigkeit und Komplexität, nicht als kurzfristiger Beschleunigungstrend.

Innerhalb der Atos Cyber Services unterstützt KI unter anderem die Korrelation sicherheitsrelevanter Ereignisse, die Priorisierung von Risiken sowie eine schnellere Erkennung und Reaktion auf Sicherheitsvorfälle. Gleichzeitig bleibt die Verantwortung des Menschen jederzeit eindeutig definiert. Mit Eviden wird darüber hinaus Security for AI als eigenständige Disziplin verstanden. Sie umfasst Governance, Laufzeitüberwachung sowie die jederzeit nachweisbare Kontrolle über KI-Systeme.

Dies ermöglicht es Organisationen, KI als Verstärker für Resilienz zu nutzen, ohne Vertrauen, Compliance oder Souveränität zu beeinträchtigen.

Eine Mission. Zwei Leistungsbereiche.

Atos verfolgt ein klares Ziel: **Adaptive Cyber Resilience** in der Praxis umsetzbar zu machen.

Dieses Ziel wird durch zwei eng verzahnte Leistungsbereiche erreicht: **Atos Cyber Services** und **Eviden Cybersecurity Products**. Gemeinsam bilden sie ein integriertes Betriebsmodell für Cyber-Resilienz, das KI-Fähigkeiten einbindet, digitale Souveränität von Anfang an berücksichtigt, Fragmentierung reduziert und eine kontinuierliche Anpassung an neue Anforderungen ermöglicht.

So entwickelt sich adaptive Cyber-Resilienz vom Konzept zur operativen Realität.

Mit hoher Geschwindigkeit. Im großen Maßstab. Auch unter Druck. Und dauerhaft.





Lassen Sie uns ins Gespräch kommen!

Mit der zunehmenden Beschleunigung der Bedrohungslage durch Künstliche Intelligenz und der wachsenden Komplexität digitaler Ökosysteme wird Adaptive Cyber Resilience zu einer Grundvoraussetzung für die Sicherung der Geschäftskontinuität.

Unabhängig davon, an welchem Punkt Ihrer Transformation Sie sich befinden, unterstützen wir Sie dabei.

Prepare – Transparenz über Ihre geschäftskritischen Ressourcen und Abhängigkeiten zu gewinnen, Risiken gezielt zu priorisieren und Cybersecurity dort zu verankern, wo sie den größten Beitrag zur Geschäftskontinuität leistet.

Respond – Sicherheitsvorfälle frühzeitig zu erkennen, ihre Auswirkungen wirksam einzudämmen und den Geschäftsbetrieb unter Belastung schnell wiederherzustellen.

Adapt – Ihre Sicherheitsstrategie kontinuierlich an neue Bedrohungen, technologische Entwicklungen, regulatorische Anforderungen und veränderte Geschäftsbedingungen anzupassen.

Nehmen Sie Kontakt auf unter:
atoscybersecurity@atos.ai

Die Tech-Ambition der Atos Group

Die Strategie der Atos Group basiert auf drei eng miteinander verknüpften Prioritäten: Agentic AI für Mission-Critical-Umgebungen, digitaler Souveränität und Security. Gemeinsam schaffen sie die Voraussetzungen dafür, dass Organisationen mit Zuversicht innovieren, die Kontrolle über ihre kritischen digitalen Assets bewahren und in einer zunehmend komplexen Welt sicher agieren können. Getragen wird dieser Anspruch durch die komplementären Stärken von Atos, Atos Amplify und Eviden.

Atos

Atos ist die Marke der Atos Group für KI-gestützte, sichere und ganzheitliche digitale Services. Atos entwirft, entwickelt und betreibt kritische digitale Umgebungen, die Leistungsfähigkeit, Ausfallsicherheit und Souveränität fördern. So unterstützt Atos öffentliche und private Organisationen weltweit dabei, die Kontrolle über ihre Daten und IT-Infrastrukturen zu bewahren und gleichzeitig regulatorische Anforderungen zu erfüllen.

Atos unterstützt Kunden bei der Modernisierung ihrer zentralen IT-Systeme, der Beschleunigung ihrer Cloud- und Datentransformation, der Stärkung ihrer Cybersicherheit sowie der Bereitstellung sicherer digitaler Arbeitsplatzlösungen.

Als vertrauenswürdiger Partner beim Betrieb komplexer und geschäftskritischer Umgebungen unterstützt Atos Organisationen in stark regulierten und souveränen Kontexten.

atos.ai



Atos Amplify ist die auf KI ausgerichtete Consulting- und Advisory-Einheit der Atos Group. Sie unterstützt Organisationen dabei, strategisch wichtige Entscheidungen zu treffen und diese in messbare Geschäftsergebnisse zu überführen.

Durch die Verbindung von tiefem Branchenwissen, unternehmerischem Verständnis und KI-getriebener Innovation arbeitet Atos Amplify gemeinsam mit seinen Kunden daran, Transformationsstrategien zu entwickeln, die Einführung neuer Technologien zu beschleunigen und Mehrwert aus Daten, KI und digitalen Plattformen zu erschließen. Der Consult-to-Build-Ansatz verbindet Strategie und Umsetzung und unterstützt Organisationen dabei, Komplexität zu bewältigen, digitale Souveränität zu stärken, ihre Resilienz zu erhöhen und nachhaltiges Wachstum zu fördern.

Auf Grundlage menschenzentrierter Werte und verantwortungsvoller KI-Prinzipien ermöglicht Atos Amplify Organisationen, Transformation mit Vertrauen, Transparenz und Verantwortlichkeit zu gestalten.

atos.ai/atos-amplify

EVIDEN

Eviden ist die Marke der Atos Group mit Schwerpunkt auf Cybersecurity-Produkten, Mission-Critical Systemen und Vision AI.

Als vertrauenswürdiger Partner für Organisationen im öffentlichen und privaten Sektor setzt Eviden fortschrittliche Analysefähigkeiten ein und unterstützt seine Kunden dabei, die Widerstandsfähigkeit, Kontinuität und Resilienz ihrer Betriebsabläufe sicherzustellen.

Das Portfolio kombiniert fortschrittliche Cybersecurity-Technologien, Lösungen für digitale Identitäten, Fähigkeiten zum Schutz von Daten sowie Mission-Critical Systeme für besonders anspruchsvolle Einsatzumgebungen mit KI-gestützten Echtzeit-Monitoring- und Analysefähigkeiten.

Mit mehr als 2.200 Expertinnen und Experten sowie über 720 Patenten trägt Eviden dazu bei, Menschen, Daten und kritische Infrastrukturen weltweit zu schützen – an der Schnittstelle von Intelligenz, Souveränität und Vertrauen.

eviden.com

Über Atos Group

Die [Atos Group](#) ist ein weltweit führender Anbieter im Bereich der digitalen Transformation. Mit ca. 56.000 Mitarbeitenden und einem Jahresumsatz von ca. 7,2 Mrd. EUR (auf Basis des künftigen Unternehmenszuschnitts) agiert das Unternehmen in 54 Ländern unter zwei Marken: Atos für Services und Eviden für Produkte und Systeme. Als europäische Nummer eins in der Cybersicherheit und führend im Bereich Cloud arbeitet die Atos Group für eine sichere und dekarbonisierte Zukunft und bietet maßgeschneiderte KI-gestützte End-to-End Lösungen für alle Branchen. Atos Group ist an der Euronext Paris notiert.

Erfahren Sie mehr über uns
[atos.ai](#)

Beginnen Sie das Gespräch mit uns



Atos Group ist eine eingetragene Marke der Atos Group. © Atos Group. Vertrauliche Informationen, die der Atos Group gehören und nur vom Empfänger verwendet werden dürfen. Dieses Dokument oder ein Teil davon darf ohne vorherige schriftliche Genehmigung der Atos Group nicht reproduziert, kopiert, verbreitet und/oder verteilt oder zitiert werden.

107924 - EM + HC - CYBERSECURITY

The Atos logo is displayed in a large, bold, blue font. The letters 'A', 't', 'o', and 's' are connected, with the 't' and 'o' having a unique, stylized design.