horn & company

CYBER & REGULATORIK PLAYBOOK 2025

//Ansprechpartner

Dr. Oliver Laitenberger
Geschäftsführender Partner

Dr. Carsten Woltmann
Partner

//Inhaltsverzeichnis

1.	**Einleitung**	**4**
2.	**Cryptoagilität in der Quanten-Ära: Warum Unternehmen jetzt handeln sollten**	5
	2.1. Kryptographie als lebendiges System	5
	2.2. Kryptografische Verfahren heute: Ein Überblick	5
	2.3. Quantencomputer als zukünftiges Sicherheitsrisiko	6
	2.4. Herausforderungen und Lösungsansätze für Cryptoagilität	7
	2.5. Cryptoagilität als Wettbewerbsfaktor	9
3.	**DSPM und CSM: Von reaktiven Maßnahmen zu proaktiver Datensicherheit**	**10**
	3.1. DSPM: Transparenz und Kontrolle über die Datenlandschaft	11
	3.2. CSM: Konsistente Sicherheitsrichtlinien in komplexen Cloud-Landschaften	11
	3.3. Die Erfolgsfaktoren von DSPM und CSM in einer integrierten Sicherheitsarchitektur	12
4.	**Mit KI gegen Cyber-Bedrohungen: Behavioral Analytics erkennt Risiken frühzeitig**	**15**
	4.1. Vom Konzept zur Wirkung – Anwendungsfälle von Behavioral Analytics	15
	4.2. Herausforderungen bei der Implementierung – Behavioral Analytics in der IT-Sicherheit	16
	4.3. Erfolgsfaktoren für die Einführung - Tipps aus der Praxis	17
	4.4. KI gehört zur modernen Cyber-Strategie	18
5.	**Next Level Cybersecurity: Orchestrierung und Automatisierung von Sicherheitsvorfällen**	**19**
	5.1. Von SOC zu SOAR – wo liegt der Unterschied?	19
	5.2. Vorgehensmodell: Vom Use Case zur Skalierung	20
	5.3. Wo SOAR seinen größten Mehrwert entfaltet	21
	5.4. Technologische Basis und Marktüberblick	21
	5.5. Automatisierung als nächster Entwicklungsschritt der Cyberabwehr	22
6.	**Zero Trust: Architektur der Zukunft oder überschätzter Hype?**	**23**
	6.1. Kernelemente einer ZTA:	23
	6.2. Die Herausforderungen für Unternehmen	24
	6.3. Zero Trust trifft DORA: Zwischen Konformität und Übererfüllung	25
7.	**Cybersecurity im Fokus: Metriken statt Bauchgefühl**	**27**
	7.1. Mehrwert von Cybersecurity-Metriken	27
	7.2. Vorgehensmodell für Cybersecurity Metriken & Reporting	29
	7.3. Kernprinzipien für wirksames Cybersecurity Reporting	30
8.	**Fazit**	**31**

//Vorwort

Seit unserer Gründung im Jahr 2009 hat sich Horn & Company als Top-Management-Beratung im deutschsprachigen Raum fest etabliert. Unser Erfolg basiert auf einem tiefen Branchenverständnis und der langjährigen Erfahrung unserer Berater, die es uns ermöglichen, die digitale Transformation unserer Klienten nachhaltig zu gestalten. Was uns dabei auszeichnet, ist die Begleitung unserer Kunden von der Strategie bis zur erfolgreichen Umsetzung – mit einem besonderen Fokus auf die drängenden Fragen einer zunehmend vernetzten und technologiegetriebenen Welt.

Im Laufe der Jahre haben wir unser Beratungsangebot kontinuierlich erweitert. Zunächst auf deutschsprachige Unternehmen und Organisationen fokussiert, betreuen wir heute auch Klienten in Österreich sowie in der mittel- und osteuropäischen Region (CEE). Über unsere Wiener Dependance stellen wir sicher, dass wir auch in diesen Märkten maßgeschneiderte Lösungen anbieten können. In den Jahren 2018/19, 2020/21, 2022/23, 2024/25 sowie 2026/27 wurden unsere Berater als „Hidden Champion des Beratermarktes" ausgezeichnet – ein Beleg für die hohe Qualität und den nachhaltigen Erfolg unserer Arbeit.

Ein besonders zentrales Thema, das unsere Kunden im Finanzsektor betrifft, ist die Cybersicherheit. Angesichts der wachsenden Bedrohungslage stehen Banken und Versicherungen unter ständigem Druck, ihre IT-Infrastrukturen sicher zu halten. Die täglichen Meldungen der BaFin und des BSI über Cyberangriffe auf Finanzinstitute verdeutlichen, dass der sichere IT-Betrieb ein Dauerthema bleibt. Neben den externen Bedrohungen durch Cyberkriminelle steigt auch die Gefahr durch Insider-Angriffe. Hinzu kommt die zunehmende Komplexität durch den verstärkten Einsatz von Cloud-Technologien, der sowohl neue Möglichkeiten als auch neue Herausforderungen mit sich bringt.

Kein Wunder also, dass Banken und Versicherungen derzeit erhebliche Summen in die Verbesserung ihrer Cybersicherheit und -Resilienz investieren. Ein wirksamer Schutz vor Cyberbedrohungen erfordert einen ganzheitlichen Ansatz, der sowohl technologische, als auch organisatorische Maßnahmen umfasst. Genau hier setzen wir mit unserer Beratung an, indem wir Unternehmen helfen, robuste und zukunftssichere Sicherheitsstrategien zu entwickeln.

Das H&C Team beobachtet für Sie die rasanten Entwicklungen in diesem Bereich genau und hat in dieser Unterlage die neuesten Anforderungen und Chancen, aus Theorie und Beratungspraxis zusammengetragen. Unsere praktischen Einblicke und Best-Practices geben Ihnen wertvolle Impulse, wie Sie Ihr Unternehmen bestmöglich schützen und zugleich zukunftssicher aufstellen können. Ob es um Cybersicherheit, Datenmanagement oder die Nutzung moderner Technologien geht – wir wissen, worauf es ankommt, und unterstützen Sie dabei, auch in einer sich ständig verändernden Bedrohungslandschaft gut vorbereitet zu sein.

Wir wünschen Ihnen eine spannende Lektüre und freuen uns darauf, Sie bei Ihren Herausforderungen zu begleiten.

Dr. Oliver Laitenberger

Dr. Carsten Woltmann

1. Einleitung

Die zunehmende Digitalisierung verändert Geschäftsmodelle, Prozesse und IT-Landschaften grundlegend und rückt Cybersecurity stärker denn je in den Fokus unternehmerischer Entscheidungen. Parallel dazu steigen sowohl die Anzahl als auch die Komplexität von Cyberbedrohungen, während regulatorische Anforderungen und Erwartungen an Transparenz, Steuerbarkeit und Wirksamkeit von Sicherheitsmaßnahmen kontinuierlich zunehmen. Unternehmen stehen damit vor der Herausforderung, ihre Cyberresilienz nicht punktuell, sondern systematisch und nachhaltig weiterzuentwickeln.

Dieses Whitepaper richtet sich an Führungskräfte und Verantwortliche, die Cybersecurity nicht isoliert als technische Disziplin betrachten, sondern als strategisches Handlungsfeld verstehen. Ziel ist es, zentrale Entwicklungen, wiederkehrende Fragestellungen und relevante Themenfelder einzuordnen und in einen übergeordneten Zusammenhang zu stellen – mit Fokus auf Praxisnähe und Umsetzbarkeit.

Im Mittelpunkt stehen Themen, die die Cybersecurity-Diskussion im vergangenen Jahr wesentlich geprägt haben und in ihrer Gesamtheit die aktuelle Sicherheitsrealität vieler Unternehmen widerspiegeln. Dazu zählen unter anderem die wachsende Bedeutung von Cryptoagilität im Kontext des Quantencomputings, der Schutz sensibler Daten in hybriden und cloudbasierten Umgebungen, Zero-Trust-Prinzipien als Leitbild moderner IT-Architekturen, der Einsatz KI-gestützter Behavioral Analytics zur frühzeitigen Erkennung von Bedrohungen, die Automatisierung von Sicherheitsprozessen im SOC-Umfeld sowie die zunehmende Bedeutung belastbarer Cybersecurity-Metriken für Steuerung und Entscheidungsfindung.

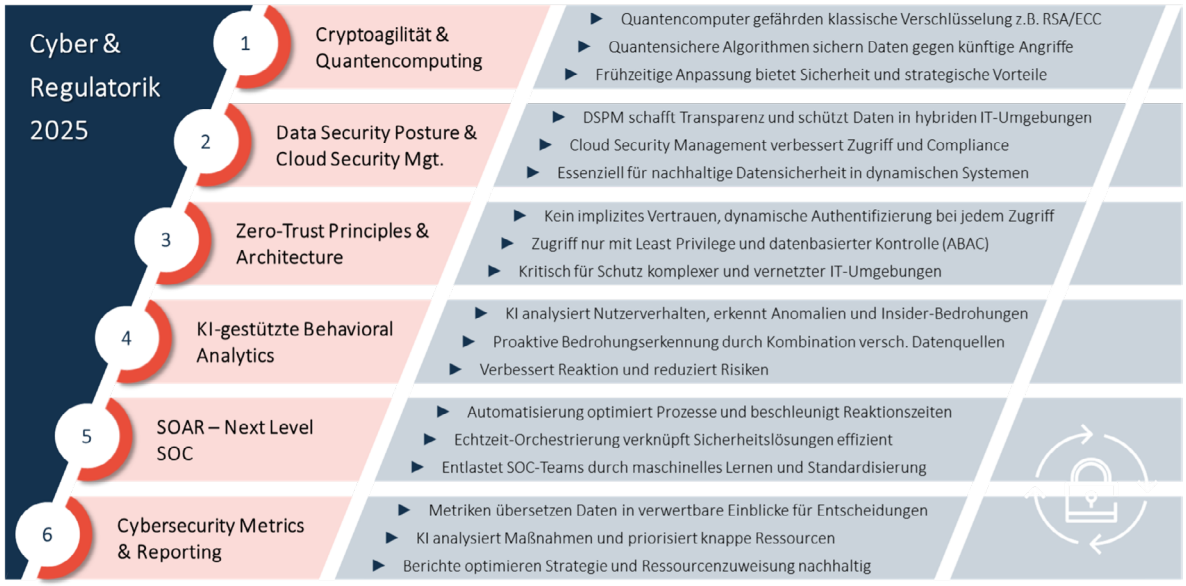

Abbildung 1: Überblick über wesentliche Cyber & Regulatorik Themen 2025

Diese Themenfelder greifen eng ineinander und verdeutlichen, wie stark technologische, organisatorische und strategische Fragestellungen im Cybersecurity Umfeld heute miteinander verknüpft sind. Sie markieren zentrale Handlungsfelder, mit denen sich Unternehmen aktuell und in den kommenden Jahren auseinandersetzen müssen, um Sicherheitsstrategien wirksam, skalierbar und zukunftsfähig auszurichten.

Vor diesem Hintergrund wurden die im vergangenen Jahr veröffentlichten Fachbeiträge in diesem Whitepaper gebündelt zusammengeführt. Die Inhalte bleiben dabei in ihrer ursprünglichen Form erhalten und bilden gemeinsam eine thematische Gesamtschau – als kompakte Sammlung, Nachschlagewerk und Orientierungshilfe für aktuelle und kommende Fragestellungen rund um die Themenlandschaft Cybersecurity und Regulatorik.

2. Cryptoagilität in der Quanten-Ära: Warum Unternehmen jetzt handeln sollten

Kryptographie ist das unsichtbare Rückgrat der digitalen Sicherheit und unserer modernen Welt. Ob geschützte Kommunikation, digitale Signaturen oder verschlüsselte Finanztransaktionen – ohne sie wäre die heutige Wirtschaft nicht denkbar. Doch diese Sicherheit gerät zunehmend unter Druck: Fortschritte in der Quanteninformatik drohen, bewährte Verschlüsselungsverfahren in den kommenden Jahren zu kompromittieren. Besonders Finanzdienstleister sind von dieser Entwicklung betroffen, da sie stark auf kryptographische Verfahren angewiesen sind, um Transaktionen zu sichern und regulatorische Anforderungen zu erfüllen. Unternehmen stehen vor einer kritischen Entscheidung: Jetzt vorausschauend in Cryptoagilität investieren oder in wenigen Jahren vor einer hektischen, kostenintensiven Umstellung stehen.

2.1. Kryptographie als lebendiges System

Kryptographie ist keine statische Technologie, die einmal eingeführt und dann für immer sicher bleibt. Im Gegenteil: Digitale Zertifikate, Schlüssel und Verschlüsselungsverfahren haben immer nur eine begrenzte Lebensdauer und werden damit im Lauf der Zeit immer anfälliger für Angriffe. Dies liegt daran, dass sich sowohl die Rechenkapazität verfügbarer Hardware als auch die Algorithmen selbst kontinuierlich weiterentwickeln. Was heute noch als sicher gilt, könnte morgen bereits kompromittiert sein. Gerade in komplexen, global vernetzten IT-Ökosystemen nimmt die Verwaltung und Erneuerung dieser „kryptographischen Werte" einen immer größeren Stellenwert ein. Ein einziger ineffizient organisierter Wechsel kann umfangreiche Systemausfälle oder massive Sicherheitslücken nach sich ziehen.

Gleichzeitig wächst die Anzahl der Staaten und Organisationen, die eigene kryptographische Standards entwickeln oder anpassen. Für Unternehmen bedeutet das konkret: Globale Interoperabilität wird noch anspruchsvoller, da ein einheitlicher Algorithmus nicht mehr ausreicht. Stattdessen müssen mehrere Verfahren gleichzeitig unterstützt werden, um den jeweiligen Anforderungen – ob behördlicher Natur oder aus Kundensicht – gerecht zu werden.

2.2. Kryptografische Verfahren heute: Ein Überblick

Unternehmen setzen auf verschiedene kryptographische Verfahren, um ihre Daten zu schützen. Die wichtigsten sind hier knapp zusammengefasst:

// **Symmetrische Verschlüsselung** (z. B. AES, ChaCha20): Schnell und effizient, aber durch den notwendigen Schlüsseltransfer potenziell anfällig für Missbrauch.

// **Asymmetrische Verfahren** (z. B. RSA, ECC, Diffie-Hellman): Setzen auf ein Schlüsselpaar und ermöglichen sichere Datenübertragungen, sind jedoch rechenintensiver und durch Quantencomputer bedroht.

// **Hash-Funktionen** (z. B. SHA-2, SHA-3): Gewährleisten Datenintegrität, sind aber selbst potenziell anfällig für zukünftige Angriffe durch Quantenalgorithmen.
// **Hybride Ansätze** (z. B. TLS): Kombinieren asymmetrische und symmetrische Methoden für eine effiziente Absicherung.

2.3. Quantencomputer als zukünftiges Sicherheitsrisiko

Quantencomputer sind kein weit entferntes Zukunftsthema mehr. Ihre einzigartige Rechenleistung basiert auf Qubits, die es ermöglichen, exponentiell schnellere Berechnungen durchzuführen als klassische Computer. Insbesondere Shor's Algorithmus birgt erhebliches Gefahrenpotenzial: RSA und ECC, die heute weit verbreiteten asymmetrischen Verfahren, könnten in wenigen Jahren innerhalb praktikabler Zeiträume gebrochen werden. Der Umstieg auf Post-Quantum-Kryptographie wird dann nicht nur sinnvoll, sondern zwingend erforderlich sein.

Mit Stand 2025 sind Prognosen davon ausgegangen, dass innerhalb eines Zeitraums von fünf bis zehn Jahren Quantencomputer existieren könnten, die klassische Verschlüsselungsverfahren gefährden. Jüngste Durchbrüche, etwa Fortschritte bei der Stabilität von Qubits und erste Erfolge in der Fehlerkorrektur, unterstreichen, dass diese Entwicklung nicht mehr nur eine theoretische Möglichkeit ist, sondern sich zunehmend konkreter abzeichnet. Unternehmen, die sich nicht frühzeitig auf diese Entwicklung vorbereiten, riskieren den plötzlichen Verlust ihrer Datensicherheit. Die Folgen wären dramatisch: Vertrauliche Finanztransaktionen könnten offengelegt, Identitätsnachweise gefälscht oder kritische Unternehmensgeheimnisse kompromittiert werden.

Neben Shor's Algorithmus stellt auch Grover's Algorithmus eine Bedrohung für bestehende kryptographische Verfahren dar. Während Shor's Algorithmus asymmetrische Kryptographie gefährdet, könnte Grover's Algorithmus die Sicherheit symmetrischer Verfahren reduzieren, indem er die erforderliche Rechenzeit zur Schlüsselsuche halbiert. Dies würde eine Verdoppelung der Schlüsselgrößen erforderlich machen, um weiterhin als sicher zu gelten.

Abbildung 2: Zentrale Bausteine zur Erreichung von Cryptoagilität.

2.4. Herausforderungen und Lösungsansätze für Cryptoagilität

Cryptoagilität bedeutet weit mehr als nur die Einführung neuer Verschlüsselungsverfahren – sie erfordert eine grundlegende Neuausrichtung der IT-Architektur hin zu mehr Flexibilität und Anpassungsfähigkeit. Angesichts der steigenden Komplexität global verteilter IT-Umgebungen und der immer kürzeren Lebenszyklen kryptographischer Algorithmen wird diese Agilität zur Notwendigkeit. Unternehmen müssen kontinuierlich neue Verfahren evaluieren und nahtlos integrieren, ohne dabei Betriebsstörungen oder Kompatibilitätsprobleme zu riskieren. Eine rein reaktive Haltung reicht nicht aus – stattdessen sollte Cryptoagilität als strategischer Bestandteil der IT-Sicherheitsarchitektur verankert werden, um langfristig auf sich wandelnde Bedrohungsszenarien vorbereitet zu sein.

Die Einführung einer cryptoagilen Architektur ist jedoch mit erheblichen Herausforderungen verbunden. Bestehende IT-Systeme sind oft nicht darauf ausgelegt, kryptografische Verfahren flexibel auszutauschen, und der Wechsel zu post-quantenresistenten Algorithmen erfordert weitreichende technische und organisatorische Anpassungen. Zusätzliche Hürden ergeben sich durch hohe Leistungsanforderungen, regulatorische Unsicherheiten und Interoperabilitätsprobleme. Unternehmen sollten sich frühzeitig mit diesen Faktoren auseinandersetzen, um unnötige Risiken zu vermeiden. Nur wer potenzielle Hindernisse rechtzeitig erkennt und gezielt adressiert, kann eine nachhaltige Cryptoagilität erfolgreich etablieren. Im Folgenden werden die zentralen Herausforderungen beleuchtet und praxisnahe Ansätze skizziert, mit denen Unternehmen diese bewältigen können:

1. Kompatibilität mit bestehenden Systemen

Hürde: Ältere IT-Infrastrukturen und Anwendungen sind oft nicht für den Einsatz neuer kryptografischer Verfahren ausgelegt. Besonders problematisch sind hardcodierte Algorithmen oder hardwaregebundene Implementierungen.

> Möglicher Lösungsansatz: Der Aufbau einer **modularen Kryptografie-Architektur** kann helfen, indem Algorithmen über standardisierte APIs eingebunden werden. Dadurch bleibt der Kern der Systeme unangetastet, während sich Sicherheitsverfahren flexibel anpassen lassen.

2. Leistungseinbußen durch komplexere Algorithmen

Hürde: Viele Post-Quantum-Algorithmen haben im Vergleich zu klassischen Verfahren höhere Rechen-, Speicher- und Bandbreitenanforderungen. Dies kann in rechenintensiven Anwendungen oder Echtzeitprozessen zu spürbaren Verzögerungen führen.

> Möglicher Lösungsansatz: Eine schrittweise Einführung hybrider Krypto-Ansätze kann helfen, Lastspitzen zu minimieren. Zudem lassen sich durch optimierte Implementierungen in Hardware, etwa durch FPGA- oder HSM-Unterstützung, Performance-Einbußen begrenzen.

3. Interoperabilitätsprobleme bei der Umstellung

Hürde: In Unternehmen existieren oft unterschiedliche Kryptografie-Standards über Abteilungen, Partner und Länder hinweg. Eine abrupte Umstellung könnte die sichere Kommunikation beeinträchtigen.

> Möglicher Lösungsansatz: Hybride Zertifikate, die klassische und PQC-Verfahren parallel unterstützen, können eine schrittweise Migration ermöglichen. Ein abgestimmter Migrationspfad sorgt dafür, dass unterschiedliche Systeme und Organisationen synchron umgestellt werden können.

4. Sicherheitsrisiken durch fehlerhafte Implementierung

Hürde: Selbst sichere Algorithmen können durch fehlerhafte Implementierungen oder unzureichende Schutzmaßnahmen angreifbar werden. Besonders Seitenkanalangriffe oder fehlerhafte Zufallszahlengeneratoren stellen ein Risiko dar.

> Möglicher Lösungsansatz: Der Einsatz von geprüften und standardisierten Krypto-Bibliotheken kann das Risiko minimieren. Regelmäßige Penetrationstests und Audits helfen, Schwachstellen frühzeitig zu erkennen und zu beheben.

5. Schwierige Modernisierung bestehender Legacy-Systeme

Hürde: Unternehmen setzen oft auf geschäftskritische Altsysteme, bei denen eine vollständige Umstellung auf neue Kryptographie-Standards technisch oder wirtschaftlich nicht kurzfristig realisierbar ist.

> Möglicher Lösungsansatz: Der Einsatz von Kryptographie-Gateways oder Proxys kann als Übergangslösung dienen, indem sie neue Sicherheitsstandards nach außen anbieten, während interne Systeme schrittweise angepasst werden.

6. Verzögerungen durch fehlende Standardisierung

Hürde: Die Standardisierung von Post-Quanten-Kryptografie ist noch nicht vollständig abgeschlossen, und regulatorische Vorgaben können sich je nach Region unterscheiden. Dies erschwert langfristige Planungen.

> Möglicher Lösungsansatz: Unternehmen sollten eine flexible Krypto-Policy etablieren, die auf modulare Algorithmen setzt. So lassen sich Standards per Konfigurationsänderung anpassen, ohne tief in bestehende Systeme eingreifen zu müssen.

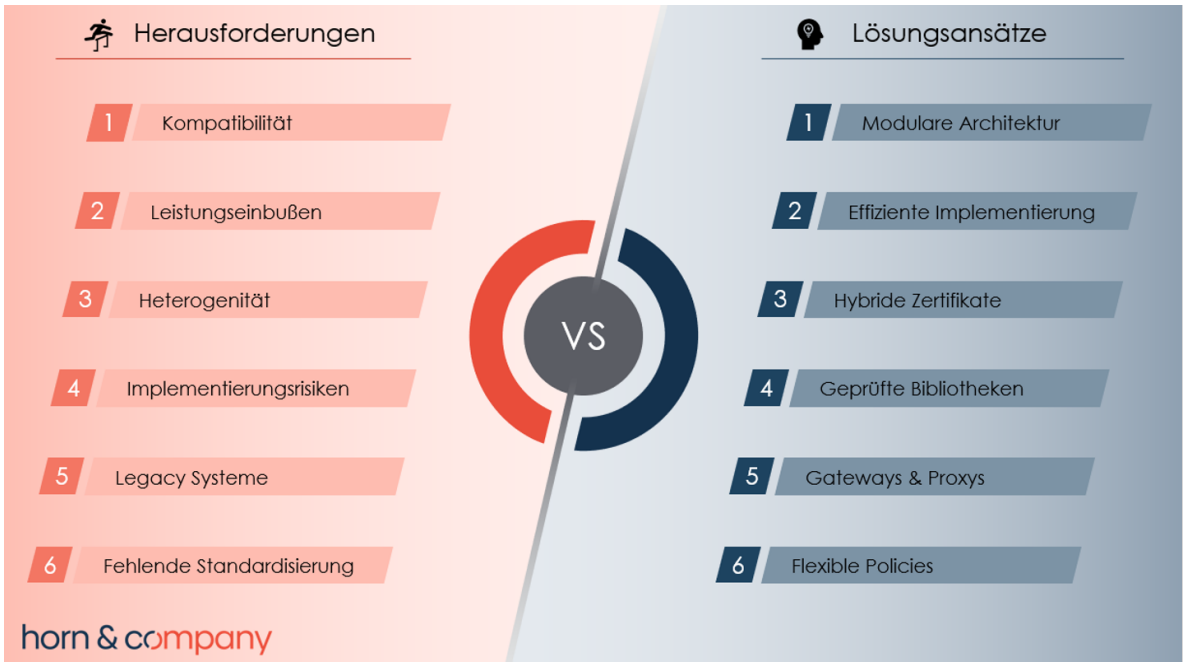

Abbildung 3: Herausforderungen und Lösungsansätze zur Etablierung von Cryptoagilität.

NIST-Standards und regulatorische Entwicklungen: Wann der Umstieg verpflichtend wird

Das US National Institute of Standards and Technology (NIST) ist federführend bei der Standardisierung von Post-Quantum-Kryptographie. Unternehmen sollten diese Entwicklungen genau verfolgen, denn sobald verbindliche Standards festgelegt sind, wird der Umstieg für viele Branchen zur regulatorischen Pflicht. Im Finanzsektor könnte dies besonders schnell gehen, da dort ohnehin strenge Compliance-Anforderungen gelten und große Geldsummen auf dem Spiel stehen. Wer frühzeitig reagiert, verhindert teure Ad-hoc-Maßnahmen und wahrt das Vertrauen von Kunden und Investoren.

Darüber hinaus existieren internationale Bestrebungen, eigene Standards einzuführen. Länder wie China oder Russland entwickeln teils eigene kryptographische Verfahren, was die globale Interoperabilität zusätzlich verkompliziert. Unternehmen sollten diese Trends beobachten, um potenzielle Konflikte bei länderübergreifenden Transaktionen zu vermeiden.

2.5. Cryptoagilität als Wettbewerbsfaktor

Die Bedrohung durch Quantencomputer ist real – doch Unternehmen können sie als Chance nutzen. Cryptoagilität ist mehr als nur ein Schutzschild gegen künftige Angriffe. Sie ist ein strategischer Vorteil, der Innovationen ermöglicht und langfristige Sicherheit garantiert.

Unternehmen, die rechtzeitig handeln, schützen nicht nur ihre Daten, sondern auch ihr Geschäftsmodell. In einer Welt, in der digitale Sicherheit über Marktpositionen entscheidet, ist Cryptoagilität kein optionales Upgrade – sie ist ein Muss für alle, die an der Spitze bleiben wollen. Wer die eigenen Kryptostrukturen nicht kontinuierlich weiterentwickelt, riskiert fatale Sicherheitslücken, Reputationsschäden und möglicherweise massive finanzielle Einbußen. Und gerade in hochsensiblen Bereichen wie dem Finanzsektor kann ein einzelner Vorfall ausreichen, um den gesamten Geschäftsbetrieb zu gefährden.

Eine zukunftssichere Kryptographie-Strategie ist daher kein Luxus, sondern eine Investition in die Stabilität und das Wachstum eines Unternehmens. Indem Organisationen jetzt die Grundlagen für Cryptoagilität legen, verschaffen sie sich entscheidende Vorteile: Sie können flexibel auf neue Bedrohungen reagieren, regulatorischen Anforderungen gelassen entgegensehen und sich zugleich als vertrauenswürdige Player am Markt positionieren. Das „Rückgrat des digitalen Vertrauens" – die Kryptographie – lebt, und nur wer mit ihren Veränderungen Schritt hält, bleibt am Ende konkurrenzfähig.

Unterstützung auf dem Weg zur Cryptoagilität

Die erfolgreiche Umsetzung von Cryptoagilität setzt sowohl technologische Anpassungen als auch strategische Weichenstellungen voraus. Verschiedene Ansätze helfen dabei, eine reibungslose Transformation zu gewährleisten:

- **// Architektur- und Tool-Beratung:** Um den optimalen Weg zur Post-Quantum-Kryptographie zu finden, bedarf es fundierter Analysen der bestehenden Infrastruktur. Dabei gilt es zu klären, welche Algorithmen sich nahtlos integrieren lassen und wo Investitionen in neue Hardware nötig werden.
- **// Prozessoptimierung:** Krypto-Updates müssen effizient in bestehende Systeme integriert werden können, ohne den laufenden Betrieb zu gefährden. Eine flexible und automatisierte Verwaltung kryptographischer Komponenten (z. B. Zertifikate, Schlüssel) hilft, Ausfallzeiten zu minimieren.
- **// Schulungen und Workshops:** Teams sollten frühzeitig für die Anforderungen der Cryptoagilität sensibilisiert werden. Schulungen und Workshops sind dabei essenziell, um Awareness für die Thematik zu schaffen und bspw. eine aktive Einbindung in Toolentscheidungen zu fördern. Nur wenn die Herausforderungen und Möglichkeiten verstanden sind, können fundierte Entscheidungen getroffen und Sicherheitsrisiken minimiert werden.

3. DSPM und CSM: Von reaktiven Maßnahmen zu proaktiver Datensicherheit

In einer Zeit, in der Daten zum Rückgrat nahezu jeder Geschäftsaktivität geworden sind, stehen Unternehmen vor einer entscheidenden Herausforderung: dem Schutz ihrer sensiblen Informationen in immer komplexer werdenden IT-Landschaften. Die zunehmende Migration in die Cloud, steigende regulatorische Anforderungen und technologische Innovationen erhöhen dabei den Druck auf die IT-Sicherheitsverantwortlichen. Gleichzeitig hat sich – nicht zuletzt durch öffentlichkeitswirksame, datenbezogene Cyber-Vorfälle – die Erkenntnis durchgesetzt, dass traditionelle Sicherheitsmaßnahmen allein nicht mehr ausreichen, um den modernen Anforderungen an Datensicherheit gerecht zu werden.

Traditionelle Sicherheitsansätze fokussieren (zu) sehr auf klar definierte Grenzen und IT-Perimeter, und reagieren primär auf bekannte Bedrohungen. Klassische Werkzeuge wie Firewalls, Antivirus-Programme oder Intrusion-Detection-Systeme basieren dabei auf statischen Regeln. Doch in einer dynamischen IT-Welt, geprägt von hybriden Architekturen, einer Vielzahl mobiler Endgeräte und zunehmend remote arbeitender Nutzer, reichen diese Maßnahmen nicht mehr aus. Die heutigen Sicherheitsrisiken entstehen immer häufiger außerhalb traditioneller Perimeter – Angreifer nutzen gezielt Schwachstellen aus, die durch inkonsistente Sicherheitsrichtlinien und unklare Datenflüsse entstehen.

Gerade in Unternehmen, deren IT-Landschaften weder vollständig on-premise noch vollständig cloud-basiert sind – und dies aus technischen, regulatorischen oder strategischen Gründen möglicherweise auch langfristig nicht sein werden – gewinnt eine integrierte Sichtweise auf Datensicherheit entscheidend an Bedeutung. Hier kommen DSPM und CSM ins Spiel. Obwohl diese beiden Bereiche oftmals noch separat behandelt werden, entfalten sie ihre volle Wirkung erst im integrierten Zusammenspiel. Und mehr noch: Durch eine nahtlose Verzahnung von DSPM und CSM entsteht eine datenzentrierte Sicherheitsstrategie, die hybride IT-Architekturen ganzheitlich absichert, indem sie den Fokus auf Daten selbst richtet und dabei dynamisch und automatisiert arbeitet.

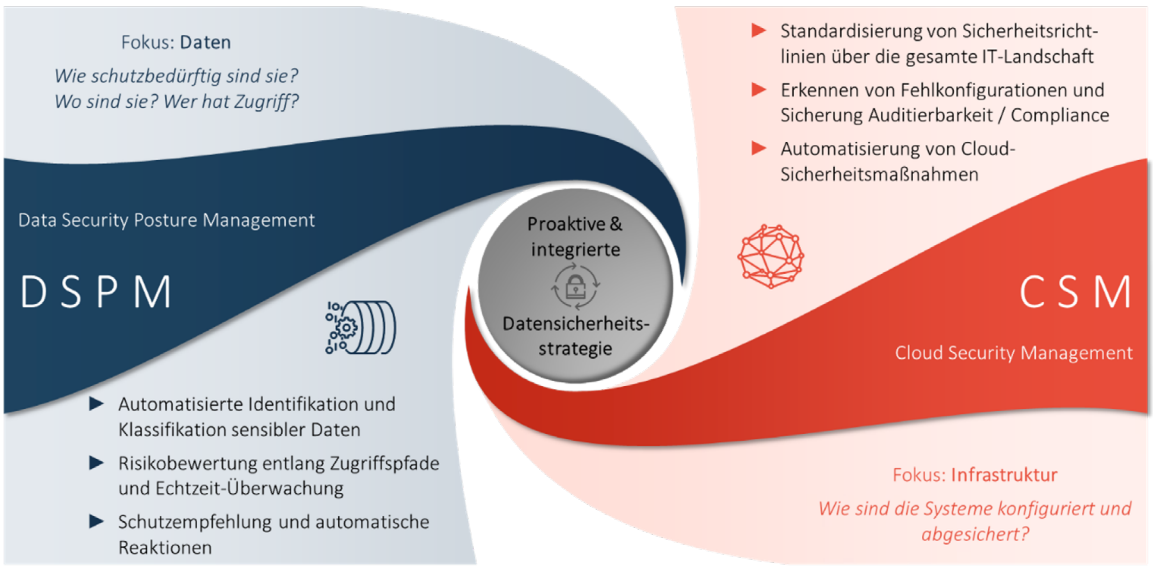

Abbildung 4: DSPM und CSM als zentrale Verfahren für eine integrierte Datensicherheitsstrategie.

3.1. DSPM: Transparenz und Kontrolle über die Datenlandschaft

DSPM stellt die Frage in den Mittelpunkt, wo sich sensible Daten über Systemgrenzen hinweg befinden, wie sie klassifiziert sind und wer auf sie zugreift. Dabei handelt es sich nicht um ein singuläres Tool, sondern um einen kontinuierlichen Sicherheitsansatz, der sich tief in die bestehende IT-Infrastruktur integriert.

Im Kern analysiert DSPM strukturierte und unstrukturierte Datenbestände automatisiert und in Echtzeit. Metadaten, Zugriffsmuster und Nutzerverhalten werden ausgewertet, um Risiken frühzeitig zu identifizieren. Dadurch können nicht nur offensichtliche Schwachstellen, etwa unverschlüsselte Daten an unsicheren Speicherorten oder veraltete Berechtigungskonzepte, erkannt, sondern auch weniger offensichtliche Bedrohungen eingegrenzt werden.

Typische Funktionalitäten moderner DSPM-Lösungen umfassen:
// automatisierte Identifikation und Klassifikation sensibler Daten (z. B. PII, Finanzdaten, IP, etc.),
// kontextbezogene Risikobewertung entlang von Zugriffspfaden und Nutzungsmustern,
// kontinuierliche Überwachung und Reporting über Dashboards,
// Empfehlungen oder direkte Einleitung von Schutzmaßnahmen (z. B. Zugriffsentzug, Verschlüsselung, Re-Zertifizierung, etc.).

So entsteht ein hohes Maß an Sichtbarkeit, das weit über die klassische Datensicherung hinausgeht, um datenorientierte Sicherheitsentscheidungen faktenbasiert, kontextsensitiv und dynamisch zu treffen.

3.2. CSM: Konsistente Sicherheitsrichtlinien in komplexen Cloud-Landschaften

In der Praxis haben die meisten IT-Landschaften heute Cloud-Komponenten – häufig mit Wildwuchs-Anteilen und heterogen über verschiedene Cloud-Anbieter verteilt. CSM setzt hier an und fokussiert sich auf die Ebene der Infrastruktur und Dienste mit dem Ziel, Sicherheit konsistent über dynamische Cloud-Umgebungen hinweg zu gewährleisten. In der Praxis bedeutet das, dass die Einhaltung von Sicherheitsvorgaben unabhängig vom genutzten Cloud-Anbieter automatisiert sichergestellt werden muss, ohne operative Flexibilität einzuschränken.

CSM verknüpft hierzu Cloud-native Funktionen wie UAM, CSPM und CWPP mit einer zentralen Steuerungsebene. So werden sicherheitsrelevante Konfigurationen fortlaufend geprüft, Verstöße gegen Richtlinien sofort erkannt und automatisiert adressiert – beispielsweise durch Quarantänemaßnahmen, Rollenzuweisungen oder Eskalationen in Incident-Response-Prozessen.

Konkret leistet CSM unter anderem:
// die Standardisierung und Durchsetzung von Sicherheitsrichtlinien über verschiedene Cloud-Plattformen hinweg,
// das Erkennen und Beheben von Fehlkonfigurationen (Security-Drifts),
// die Integration von Cloud-spezifischen Schutzmechanismen in ein übergreifendes Regelwerk,
// die konsistente Dokumentation aller sicherheitsrelevanten Vorgänge zur Auditierbarkeit und Compliance.

Damit ist CSM das organisatorische Rückgrat für sichere Cloud-Nutzung – sowohl im Tagesbetrieb als auch bei der Umsetzung strategischer Cloud-Initiativen.

3.3. Die Erfolgsfaktoren von DSPM und CSM in einer integrierten Sicherheitsarchitektur

Erst im Zusammenspiel entfalten DSPM und CSM ihre volle Wirksamkeit: Während DSPM tief in die Datenebene eintaucht, und die Daten selbst zum Ausgangspunkt der Sicherheitsstrategie erklärt, adressiert CSM die Infrastruktur, in der diese Daten gespeichert und verarbeitet werden. Die Kombination beider Perspektiven bildet die Grundlage für eine durchgehend resiliente Sicherheitsarchitektur.

Ein solcher integrierter Ansatz ermöglicht:

// ganzheitliche Transparenz entlang der gesamten Datenverarbeitungskette,
// die frühzeitige Erkennung von Risiken und Schwachstellen – sowohl im Datenbestand als auch in der Konfiguration,
// eine automatisierte, dynamische Reaktion auf Bedrohungen – abgestimmt auf den jeweiligen Kontext,
// die Einhaltung regulatorischer Anforderungen in Echtzeit, unabhängig vom Speicherort der Daten.

Gestützt durch Technologien wie KI, Machine-Learning und automatisierte Klassifizierungsalgorithmen entstehen so adaptive Sicherheitsmechanismen, die kontinuierlich lernen, priorisieren und handeln. Das Sicherheitsniveau wird damit nicht nur gehalten – es verbessert sich fortlaufend. Und genau das ist der entscheidende Unterschied zur rein reaktiven IT-Sicherheit von gestern.

	Use Case (Beispiele)		Fokus
1	Schutz sensibler Kundendaten in hybriden Umgebungen	Automatische Klassifikation, Überwachung und Schutz sensibler Daten (z.B. Finanz-, Gesundheitsdaten) sowie standardisierte Richtlinien in der Cloud	Datenschutz und Datenintegrität
2	Gewährleistung regulatorischer Compliance (z.B. DSGVO)	Lückenlose Inventarisierung und Überwachung sensibler Daten sowie Auditierbarkeit der Cloud-Sicherheitsmaßnahmen	Compliance-Sicherung
3	Transparenz und Risikomanagement bei Cloud-Migrationen	Schaffung vollständiger Transparenz über migrierte Daten und Absicherung neuer Cloud-Instanzen durch definierte Sicherheitsstandards	Migrations-Sicherheit
4	Prävention von Datenverlusten bei Remote-Arbeiten	Kontinuierliche Überwachung von Datenbewegungen und Echtzeit-Reaktion auf verdächtige Aktivitäten und Vorfälle	Schutz mobiler Arbeitsumgebungen
5	Automatisierte Erkennung und Reaktion auf Insider Threats	Analyse von Nutzerverhalten und automatisierte Reaktion auf untypische Aktivitäten in Bezug auf Daten und Zugriffe	Schutz vor internen Bedrohungen

Abbildung 5: Typische Use Cases und Schwerpunkte für eine moderne Datensicherheitsstrategie.

Zu den häufigsten Use-Cases zählen dabei:

1. Schutz sensibler Kundendaten in hybriden Umgebungen:

Unternehmen aus dem Finanz- und Gesundheitssektor stehen unter hohem regulatorischem Druck, sensible Kundendaten zu schützen und Datenschutzverletzungen zu vermeiden. DSPM hilft dabei, kritische Daten (unternehmensrelevante Daten, personenbezogene Daten, Finanzinformationen, Gesundheitsdaten, etc.) automatisiert zu klassifizieren, kontinuierlich zu überwachen und bei verdächtigen Aktivitäten oder fehlerhaften Zugriffsrechten frühzeitig Warnungen auszugeben. CSM ergänzt diese Sicht durch die Standardisierung und automatisierte Umsetzung von Sicherheitsrichtlinien über alle Cloud-Plattformen hinweg und verhindert so Inkonsistenzen, die zu Sicherheitsvorfällen führen könnten.

2. Gewährleistung regulatorischer Compliance (z. B. DSGVO):

Regulatorische Anforderungen wie die DSGVO zwingen Kunden, kontinuierlich nachzuweisen, dass sie Datenschutzrichtlinien nicht nur formulieren, sondern aktiv durchsetzen. Mit DSPM können wir dabei helfen, eine automatisierte Inventarisierung aller sensiblen Datenbestände sowie die lückenlose Dokumentation sämtlicher Datenzugriffe und Zugriffsrechte zu gewährleisten. CSM wiederum automatisiert und dokumentiert die Sicherheitsmaßnahmen in der Cloud, um jederzeit Compliance-konform zu bleiben und Audits schnell und effizient bewältigen zu können.

3. Transparenz und Risikomanagement bei Cloud-Migrationen:

Wenn Kunden Teile ihrer Infrastruktur und Anwendungen in die Cloud migrieren, entstehen häufig Risiken durch schlecht konfigurierte Systeme oder unsichere Zugriffsrechte. DSPM sorgt hier für umfassende Transparenz über alle migrierten Daten und deren Nutzung, während CSM durch standardisierte Sicherheitskonfigurationen und automatisierte Risikobewertungen sicherstellt, dass neue Cloud-Instanzen stets mit einem definierten und sicheren Sicherheitsniveau betrieben werden.

4. Prävention von Datenverlusten bei Remote-Arbeit:

Die zunehmende Nutzung mobiler Geräte und Remote-Arbeitsplätze erhöht die Gefahr unbeabsichtigter Datenverluste oder gezielter Cyberangriffe. Mit DSPM können unsere Kunden kontinuierlich Datenbewegungen zwischen Endgeräten und zentralen Systemen überwachen und auffällige Muster automatisch erkennen. In Kombination mit CSM können verdächtige Aktivitäten in Echtzeit erkannt und unterbunden werden – etwa durch sofortige Sperrung eines Zugriffs, Benachrichtigung der IT-Abteilung oder die Anpassung von Zugriffsrechten auf Basis des aktuellen Risikoniveaus.

5. Automatisierte Erkennung und Reaktion auf Insider Threats:

Insider-Bedrohungen zählen zu den schwierigsten Sicherheitsrisiken, da sie oft nur schwer frühzeitig zu erkennen sind. DSPM erlaubt unseren Kunden eine detaillierte Analyse des Benutzerverhaltens und kann so automatisiert Unregelmäßigkeiten feststellen, etwa durch Zugriffe auf ungewöhnliche Datenbestände oder Downloads größerer Datenmengen. CSM sorgt ergänzend dafür, dass in Cloud-Umgebungen Sicherheitskontrollen automatisiert ausgeführt und kritische Vorfälle direkt eingedämmt werden.

Aus unserer Praxis lässt sich also feststellen, dass DSPM und CSM für viele Kunden bereits jetzt einen entscheidenden Baustein zu ihrer Cybersicherheit hinzufügen. Aber, so wirkungsvoll die aufgezeigten Technologien und Use Cases auch sind, in der Realität sehen sich viele Unternehmen bei der Implementierung noch mit – oft ähnlichen – Hürden konfrontiert: Fehlende Transparenz über Datenflüsse, historisch gewachsene Systemlandschaften, fragmentierte Sicherheitsrichtlinien und begrenzte personelle Ressourcen im Security-Bereich sind nur einige von ihnen.

Die Einführung einer integrierten DSPM-/CSM-Architektur erfordert daher nicht nur technologische Kompetenz, sondern auch eine enge Verzahnung mit Governance- und Compliance-Strukturen sowie eine klare strategische Zielsetzung und Unterstützung durch das Management. Wer diese Herausforderungen frühzeitig adressiert, legt den Grundstein für eine zukunftsgewappnete Sicherheitsarchitektur.

So zentral DSPM und CSM für eine nachhaltige Sicherheitsstrategie sind, sie entfalten ihre volle Wirkung erst im Zusammenspiel mit der umliegenden technologischen Sicherheitsarchitektur. Ihre tiefe Integration mit ergänzenden Technologien, wie SIEM, SOAR oder XDR, verstärkt die Wirksamkeit und Effizienz der genannten Sicherheitsmechanismen enorm. Unternehmen profitieren so nicht nur von einer umfassenden Transparenz, sondern auch von der automatisierten Interaktion der Systeme untereinander, die eine schnelle, präzise und ganzheitliche Abwehr von Bedrohungen ermöglicht.

4. Mit KI gegen Cyber-Bedrohungen: Behavioral Analytics erkennt Risiken frühzeitig

Cyber-Security ist per Definition ein „Hase- und Igel"-Spiel – als „Verteidiger" ist man stets im Nachteil, insbesondere, wenn man auf einem Auge blind ist. Denn wer seine Verteidigung auf bekannte Angriffsmuster beschränkt, geht ein großes Risiko ein. Die Erfahrung mit unseren Kunden zeigt: Angreifer kennen statische Verteidigungsstrategien genau und richten ihre Angriffe konsequent auf deren Schwachstellen aus.

Verdächtiges Verhalten erkennen und rechtzeitig reagieren

Behavioral Analytics adressiert diese Schwachstellen, indem es sicherheitsrelevantes (Fehl-)verhalten in Echtzeit erkennt. Die Analyse ist dabei in der Regel personenbasiert, datengetrieben und funktioniert unabhängig von bekannten Angriffsmustern. Dadurch lassen sich Risiken frühzeitig identifizieren und gezielt entschärfen, oft noch bevor Schaden entsteht.

Damit Anomalien hinreichend präzise identifiziert werden können, muss zunächst festgestellt werden, wie der Normalzustand aussieht. Dafür überwacht das Sicherheitssystem den Netzverkehr, Nutzerverhalten und Systemvorfälle, um einen unternehmensindividuellen Referenzzustand herzuleiten. Das funktioniert zum einen datengetrieben, zum anderen aber auch in Kombination mit Plausibilisierungsregeln. Anschauliches Beispiel: An Feiertagen wird nur selten gearbeitet, unerwartete Logins an Feiertagen wären folglich ein Trigger. In der Praxis sind Muster deutlich komplexer:

// Wer loggt sich wann von wo ein?
// Auf welche Dateien und Systeme wird zugegriffen?
// Welche Datenmengen werden bewegt?
// Wie bewegt sich der Nutzer durch das Netzwerk?
// Kommt es in typischen Pausenzeiten zu unerwarteten Aktivitäten?

Die Liste ist schier endlos und in der Komplexität des Zusammenspiels aller Faktoren für Menschen nicht zu überblicken und auch für klassische Algorithmen nicht in Echtzeit auswertbar. Genau hier ist KI zum Gamechanger geworden, indem sie Anomalien im Zusammenspiel der unterschiedlichsten Faktoren in Echtzeit identifiziert, klassifiziert und in Actionable Insights kondensiert.

4.1. Vom Konzept zur Wirkung – Anwendungsfälle von Behavioral Analytics

Die Auswahl und Gewichtung von Use Cases beruhen stark auf dem konkreten Kundenumfeld und der gegebenen IT-Architektur. Grundsätzlich sollten aber die folgenden drei Use-Case-Cluster abgedeckt sein:

1. Identifikation von Insider-Bedrohungen

Mit eine der gefährlichsten und auch durch klassische Methoden besonders schwierig zu identifizierende Bedrohungen ist ein Insider-Angriff. Die Überwachung des Nutzerverhaltens im Vergleich zu anderen Nutzern mit ähnlichen Aufgaben zur Identifikation unüblicher oder verdächtiger Aktivitäten ist sowohl das stärkste Signal eines Insiderangriffs als auch die Kernstärke von Behavioral Analytics, gerade wenn sie KI-gestützt eingesetzt wird.

2. Aufdeckung kompromittierter Zugangsdaten

Ein weiterer häufiger Angriffsweg besteht in der Verwendung gestohlener Zugangsdaten, bei dem sich der Angreifer zunächst wie ein legitimer Nutzer verhält. Sobald jedoch Aktivitäten auftreten, die vom gewohnten Verhalten des eigentlichen Nutzers abweichen, wird dies durch die Analyse des Verhaltens identifiziert und es können gegebenenfalls automatisch Gegenmaßnahmen eingeleitet werden.

Es müssen nicht immer Benutzeraktivitäten sein, die zu Bedrohungen führen. Auch bei der Identifikation kompromittierter Systeme bietet Behavioral Analytics einen entscheidenden Vorteil. Klassische Sicherheitssysteme stoßen oft an ihre Grenzen, wenn Bedrohungen keine bekannten Signaturen aufweisen. Behavioral Analytics hingegen erkennt auch neuartige oder besonders ausgeklügelte Angriffe wie Zero-Day-Exploits oder APTs, indem sie auf unerwartete Verhaltensmuster statt auf starre Signaturen setzt.

Durch die detaillierte Echtzeit-Analyse des Nutzer- und System-Verhaltens vor und während eines Sicherheitsvorfalls gewinnen Sicherheitsteams wichtige Erkenntnisse über Angriffspfade, Zeitverlauf und Taktik des Angreifers. Diese Informationen ermöglichen nicht nur eine schnellere und teils automatisierte Eindämmung des Vorfalls, sondern auch eine gezielte Optimierung künftiger Reaktionsstrategien und Schließung von Sicherheitslücken.
Gleichzeitig werden Fehlalarme, beispielsweise durch harmlose Benutzeraktivitäten, die eine starre Regel triggern, deutlich reduziert.

4.2. Herausforderungen bei der Implementierung – Behavioral Analytics in der IT-Sicherheit

Wurde der Nutzen von Behavioral Analytics im Unternehmen erkannt und eine Umsetzungsentscheidung getroffen, zeigen sich in der Praxis häufig wiederkehrende Herausforderungen.

Trainingsphase und Aufbau von Referenzwerten

Bevor ein System auffälliges Verhalten erkennen kann, muss es zunächst ein Verständnis für „normales" Nutzer- und Systemverhalten entwickeln. Während dieser sogenannten Trainingsphase, die mehrere Wochen oder sogar Monate dauern kann, ist die Erkennungsleistung des Systems stark eingeschränkt. Dies muss beim Zeitplan der Implementierung berücksichtigt und durch ergänzende Sicherheitsmaßnahmen ausgeglichen werden.

Datenschutz und Mitarbeitervertrauen

Da Behavioral Analytics detaillierte Nutzungsaktivitäten erfasst, entstehen unweigerlich Fragen zum Datenschutz und zur Überwachung am Arbeitsplatz. Mitarbeitende könnten sich durch eine vermeintlich dauerhafte Beobachtung verunsichert fühlen. Der verbindlich zugesicherte Einsatzzweck sollte daher ausschließlich die Erkennung sicherheitsrelevanter Ereignisse sein. Eine transparente Kommunikation und klare und ggf. betrieblich verankerte Anwendungsrichtlinien sind entscheidend für das Mitarbeitervertrauen.

Erforderliche Fachkompetenz im Umgang mit Verdachtsfällen

Zwar identifizieren Systeme basierend auf Behavioral-Analytics-Techniken verdächtige Aktivitäten und können diese je nach Ausgestaltung auch klassifizieren, doch die abschließende Bewertung von Verdachtsfällen liegt weiterhin in der Verantwortung von IT-Sicherheitsteams. Behavioral Analytics ergänzt daher das Toolset, ersetzt jedoch keinesfalls qualifizierte Fachkräfte, die sowohl technisches Verständnis als auch Kontextwissen über betriebliche Abläufe mitbringen.

Integration in bestehende Sicherheitsinfrastrukturen

Um ihr volles Potenzial zu entfalten, sollte Behavioral Analytics eng mit bestehenden Sicherheitslösungen wie SIEM-Systemen, Identity-Management und automatisierten Gegenmaßnahmen beispielsweise durch SOAR (nächster Artikel in dieser Reihe) integriert werden. Dies erfordert zusätzlichen Aufwand und technologische Abstimmung, ermöglicht dafür jedoch eine umfassende Sicht auf Bedrohungslagen sowie eine wesentliche Verbesserung Reaktionsfähigkeit und -geschwindigkeit.

4.3. Erfolgsfaktoren für die Einführung - Tipps aus der Praxis

Damit die zuvor skizzierten Herausforderungen in der Implementierung gemeistert werden können, erfordert die Einbindung von Behavioral Analytics in die IT-Sicherheitsarchitektur eine sorgfältige Planung und strukturierte Umsetzung. Dabei sind fünf Erfolgsfaktoren wesentlich.

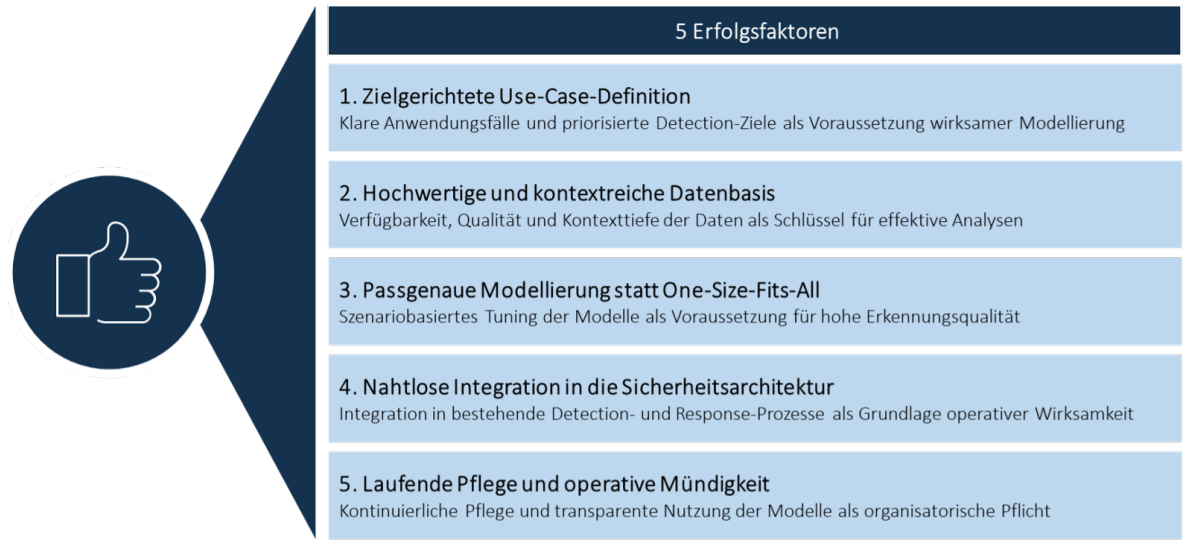

Abbildung 6: Fünf Erfolgsfaktoren zur Einbindung von Behavioral Analytics in die IT-Sicherheitsarchitektur.

1. Zielgerichtete Use-Case-Definition

Behavioral Analytics entfaltet seinen Mehrwert nur dann, wenn konkrete Anwendungsfälle im Vorfeld definiert werden: Welche Bedrohungen sollen erkannt werden? In welchen Systemen und Kontexten? Statt abstrakter Zielsetzungen braucht es klar priorisierte Detection-Ziele, an denen Modellierung und Implementierung ausgerichtet werden. Als Ankerpunkte zur Abdeckung grundlegender Anforderungen können die weiter oben genannten Use-Case Cluster herangezogen werden.

2. Hochwertige und kontextreiche Datenbasis

Die Effektivität der Analysen steht und fällt mit der Verfügbarkeit, Qualität und Relevanz der Daten. Neben klassischen Logdaten sollten auch kontextuelle Informationen, etwa Identitäten, Berechtigungen oder zeitliche Muster integriert werden. Eine frühzeitige Klärung, welche Daten verfügbar und nutzbar sind, ist entscheidend.

3. Passgenaue Modellierung statt One-Size-Fits-All

Standard-UEBA-Modelle reichen selten aus. Die Algorithmen müssen auf die definierten Bedrohungsszenarien, Organisationsstrukturen und Systeme zugeschnitten werden. Nur durch individuelles Tuning lassen sich hohe Erkennungsraten bei gleichzeitig niedriger False-Positive-Rate erreichen.

4. Nahtlose Integration in die Sicherheitsarchitektur

Behavioral Analytics darf kein Insellösungs-Dasein fristen. Die Integration in bestehende Detection- und Response-Prozesse, etwa SIEM, SOAR oder Incident-Handling-Workflows, ist essenziell für eine effektive und operationalisierbare Sicherheitswirkung.

5. Laufende Pflege und operative Mündigkeit

Modelle und Baselines veralten. Deshalb braucht es organisatorische Verantwortlichkeiten für die kontinuierliche Überwachung, Justierung und Bewertung der Analytics-Komponenten. Ebenso wichtig: Die relevanten Teams müssen in der Lage sein, Verdachtsfälle zu interpretieren und einzuordnen, ohne Blackbox-Mentalität.

4.4. KI gehört zur modernen Cyber-Strategie

Der gezielte Einsatz von Behavioral Analytics ist kein optionales Zukunftsthema mehr, sondern eine strategische Notwendigkeit. Als Bestandteil moderner Cyber-Sicherheitsarchitekturen ermöglicht Behavioral Analytics die kontinuierliche Analyse und Bewertung von Nutzer- und Systemverhalten, um verdächtige Aktivitäten frühzeitig zu identifizieren. Damit trägt diese Technologie entscheidend dazu bei, auch komplexe oder interne Bedrohungen zu erkennen, bevor Schaden entsteht oder sich ausweitet. Unternehmen, die in solche Lösungen investieren, stärken nicht nur ihre Resilienz gegenüber Cyberangriffen, sondern erfüllen zugleich wachsende Anforderungen an Transparenz, Prävention und regulatorische Compliance.

5. Next Level Cybersecurity: Orchestrierung und Automatisierung von Sicherheitsvorfällen

Cyberangriffe nehmen in Frequenz, Geschwindigkeit und Komplexität kontinuierlich zu. Unternehmen stehen vor der Herausforderung, nicht nur immer mehr Vorfälle zu erkennen, sondern auch in kürzester Zeit konsistente und nachweisbare Reaktionen einzuleiten. Klassische SOC-Strukturen stoßen hier zunehmend an ihre Grenzen.

Mit SOAR entsteht ein Ansatz, der genau an dieser Stelle ansetzt: Vorfälle werden nicht nur erkannt, sondern systematisch und automatisiert bearbeitet – in einer Geschwindigkeit und Konsistenz, die mit rein manuellen Prozessen nicht erreichbar wäre.

Das Zusammenspiel von SOC, SIEM, CERT und War-Gaming bildet bereits heute das Fundament moderner Cyberabwehr. SOAR baut darauf auf: Es ist kein Zukunftskonzept, sondern wird bereits von vielen Unternehmen eingesetzt – als nächster Reifegrad, der bestehende SOC-Strukturen konsequent weiterentwickelt.

5.1. Von SOC zu SOAR – wo liegt der Unterschied?

Das SOC ist darauf ausgerichtet, Bedrohungen zu überwachen, Vorfälle zu analysieren und koordinierte Gegenmaßnahmen einzuleiten. Es bringt Menschen, Prozesse und Technologien zusammen, um handlungsfähig zu bleiben. In der Praxis bedeutet das allerdings oft auch, dass viele Routineaufgaben sich wiederholen, und Analysten so einen Großteil ihrer Zeit mit manuellen Tätigkeiten verbringen, anstatt sich auf die wirklich kritischen Vorfälle konzentrieren zu können.

SOAR erweitert diese Basis. Es geht nicht mehr allein um das Sichtbarmachen und manuelle Bearbeiten von Vorfällen, sondern darum standardisierte Reaktionen automatisch und orchestriert auszuführen. Alerts werden in Sekunden mit relevanten Informationen angereichert, IP-Adressen blockiert oder kompromittierte Accounts gesperrt, während Analysten ihre Aufmerksamkeit auf komplexere Szenarien richten können.

Der entscheidende Unterschied: Während SOC Strukturen und Prozesse etabliert, führt SOAR sie auf einer Plattform zusammen und beschleunigt sie durch Automatisierung.

Zusammensetzung: Was für SOAR erforderlich ist

Damit SOAR seine Wirkung entfalten kann, braucht es drei eng verzahnte Komponenten:

// Technologien

Neben SIEM-Systemen spielen vor allem offene Schnittstellen (APIs) eine Rolle, die es ermöglichen Security-Tools wie Firewalls, Endpoint-Schutz oder Ticketing-Systeme miteinander zu verbinden. Auch Cloud-Dienste und SaaS-Anwendungen werden zunehmend eingebunden – ein wesentlicher Faktor, da Angriffe heute häufig hybride IT-Landschaften betreffen.

// Playbooks

Sie sind das Herzstück von SOAR: kodifizierte Reaktionsmuster, die Angriffsszenarien wie Phishing, Malware-Ausbreitung oder Insider-Vorfälle abbilden. Ein Playbook legt fest, welche Datenquellen genutzt werden, wie eine Entscheidung getroffen wird und welche Aktionen automatisch folgen. Durch die Wiederverwendbarkeit solcher Playbooks entsteht ein wachsender Katalog, der das Unternehmen Schritt für Schritt resilienter macht.

// Menschen

Analysten und Security-Architekten definieren die relevanten Use Cases, entwickeln Playbooks und stellen sicher, dass Automatisierungen regelmäßig überprüft und verbessert werden. Ihre Aufgabe ist es, den richtigen Grad an Automatisierung zu wählen: nicht alles kann oder sollte vollständig automatisiert werden, doch manche Szenarien erfordern weiterhin eine bewusste menschliche Entscheidung.

Diese Zusammensetzung macht deutlich: SOAR ist kein Ersatz für SOC, sondern eine Erweiterung, die bestehende Fähigkeiten systematisch skaliert und beschleunigt.

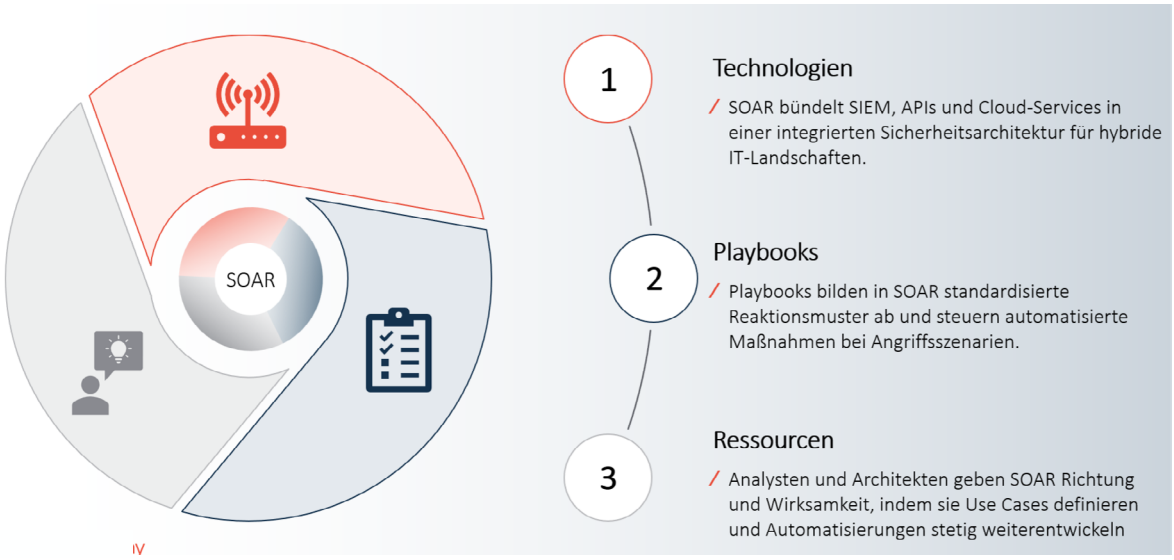

Abbildung 7: Zentrale Komponenten zur Etablierung einer SOAR-Plattform zur modernen Cyberabwehr.

5.2. Vorgehensmodell: Vom Use Case zur Skalierung

Die Einführung von SOAR sollte idealerweise schrittweise erfolgen:

1. Use Cases definieren

Auswahl und Priorisierung relevanter Bedrohungsszenarien, abgestimmt auf das jeweilige Risikoprofil.

2. Playbooks entwickeln

Standardisierte Abläufe, die beschreiben, wie Daten analysiert, Maßnahmen ergriffen und Eskalationen angestoßen werden.

3. Automatisieren und integrieren

Umsetzung der Playbooks in der SOAR-Plattform. Routinetätigkeiten laufen automatisiert und komplexere Fälle bleiben beim Analysten.

4. Lernen und optimieren

Erfahrungen aus Vorfällen fließen in die Weiterentwicklung der Playbooks ein. Wichtige Kennzahlen sind z. B.

// Mean Time to Detect (MTTD) – die durchschnittliche Zeit, bis ein Vorfall erkannt wird.

// Mean Time to Respond (MTTR) – die durchschnittliche Zeit, bis auf einen Vorfall reagiert wird. Erfolgreiche SOAR-Implementierungen zeichnen sich dadurch aus, dass diese Kennzahlen nicht einmalig gemessen, sondern kontinuierlich überprüft und verbessert werden.

5. Skalieren

Schrittweise Ausweitung auf weitere Use Cases, Teams und Unternehmensbereiche. Dabei gilt: Lieber mit wenigen, relevanten Szenarien starten und iterativ erweitern, als gleich die gesamte Organisation zu überfrachten.

5.3. Wo SOAR seinen größten Mehrwert entfaltet

Nicht jedes Unternehmen benötigt sofort eine SOAR-Lösung. Besonders sinnvoll ist der Einsatz dort, wo:

// eine große Zahl von Alerts anfällt, die manuell kaum noch zu bewältigen sind,

// komplexe IT- und Sicherheitslandschaften bestehen, in denen viele Tools und Datenquellen integriert werden müssen,

// regulierte Branchen wie Finanzdienstleistungen, Versicherungen oder kritische Infrastrukturen tätig sind, bei denen Geschwindigkeit und Nachweisbarkeit entscheidend sind,

// Fachkräftemangel spürbar ist und Automatisierung die Effizienz des Security-Teams erhöht.

Gerade in Unternehmen mit hohen Compliance-Anforderungen oder einer global verteilten IT ist SOAR mehr als nur Effizienzsteigerung, es wird zur Voraussetzung, um überhaupt noch mit der Geschwindigkeit der Bedrohungen Schritt zu halten. In kleineren Organisationen mit überschaubaren Strukturen reicht dagegen häufig ein gut organisiertes SOC aus.

5.4. Technologische Basis und Marktüberblick

Damit SOAR seine Stärke entfalten kann, braucht es mehrere ineinandergreifende Bausteine. Im Zentrum stehen Integrationen und APIs, die unterschiedliche Sicherheitswerkzeuge miteinander verbinden – etwa Firewalls wie Palo Alto oder Endgerätesicherheit (EDR) wie CrowdStrike Falcon. Darauf aufbauend sorgt eine Playbook-Engine dafür, dass wiederkehrende Schritte automatisch und konsistent ablaufen, vom Blockieren verdächtiger IPs bis zum Sperren kompromittierter Konten. Viele Plattformen setzen dabei inzwischen auf Low-Code- oder No-Code-Designer, mit denen Playbooks ohne tiefgehende Programmierkenntnisse erstellt und angepasst werden können. Ergänzend kommen Case-Management-Funktionen hinzu, die Vorfälle strukturiert abbilden, Threat-Intelligence-Anbindungen, die Alerts mit Kontextinformationen anreichern, sowie Dashboards und Reporting, die Geschwindigkeit und Nachvollziehbarkeit in den Mittelpunkt stellen.

Im Markt haben sich Plattformen wie Palo Alto Cortex XSOAR, Splunk SOAR, IBM QRadar SOAR, Fortinet FortiSOAR oder ServiceNow Security Operations etabliert. Ergänzt werden sie durch spezialisierte Anbieter wie Swimlane oder Siemplify (Google Cloud). Die Unterschiede liegen vor allem in Integrationsbreite, Playbook-Ansätzen oder Cloud-Native-Fähigkeiten – das gemeinsame Ziel bleibt jedoch gleich: vorhandene Security-Tools orchestriert zusammenzuführen und schnelle, konsistente Reaktionen zu ermöglichen.

5.5. Automatisierung als nächster Entwicklungsschritt der Cyberabwehr

SOAR schließt die Lücke zwischen klassischen SOC-Strukturen und den Anforderungen einer immer komplexeren Bedrohungslandschaft. Es automatisiert wiederkehrende Aufgaben, orchestriert das Zusammenspiel von Tools und Teams und erhöht die Geschwindigkeit in der Reaktion. Damit wird es zu einem wichtigen Baustein für Unternehmen, die ihre Cyberabwehr gezielt auf den nächsten Reifegrad weiterentwickeln wollen und die sicherstellen müssen, auch in Zukunft handlungsfähig zu bleiben.

6. Zero Trust: Architektur der Zukunft oder überschätzter Hype?

In Zeiten verschärfter Cyberregulatorik und zunehmender Digitalrisiken rückt das Prinzip „Zero Trust" in den Fokus der Sicherheitsstrategien vieler Unternehmen. Dabei gilt ein zentraler Grundsatz: Vertraue niemandem – weder intern noch extern – ohne vorherige Prüfung. Das klassische Sicherheitsverständnis, wonach Benutzer und Systeme innerhalb des eigenen Netzwerks automatisch als vertrauenswürdig gelten, ist damit obsolet.

Stattdessen setzt Zero Trust auf kontinuierliche Verifizierung, feingranulare Zugriffskontrollen und Echtzeitüberwachung. Angriffe wie Ransomware, Credential Stuffing oder Insider Threats sollen so bereits in der Entstehung unterbunden werden. Das Konzept basiert auf der Annahme, dass Systeme jederzeit kompromittiert sein könnten – und verlangt daher bei jedem Zugriff Identitätsnachweise, Integritätsprüfungen und Kontextanalysen.

6.1. Kernelemente einer ZTA:

// **Kein Vertrauen:** Authentifizierung mittels MFA und kontextsensitiver Autorisierung. Minimal notwendige Zugriffsrechte, situativ und zeitlich beschränkt. Zugang nur für verifizierte Endgeräte.

// **Annahme des erfolgreichen Angriffs:** Kontinuierliches Monitoring und Anomalie-Erkennung durch KI und verhaltensbasierte Analytik. Begrenzung von Bewegungen innerhalb des Netzwerks durch Mikrosegmentierung.

// **Test- & Auditierbarkeit:** Zero Trust-Systeme liefern lückenlose, standardisierte Zugriffsnachweise. Systematische Testbarkeit und dokumentierte Wirkungskontrolle von Sicherheitsmaßnahmen sind Pflicht.

Im Unterschied zur traditionellen IT-Sicherheit, die stark perimeterorientiert denkt, bietet ZTA ein adaptives, risiko-orientiertes Sicherheitsmodell – besonders geeignet für hybride Umgebungen, Remote Work und digitale Ökosystemex.

Schöne neue ZTA-Welt: Von der Theorie zur Umsetzung

Moderne Umsetzungen zeigen, wie sich traditionelle Sicherheitsansätze durch Zero-Trust-Prinzipien ablösen lassen – oft mit höherer Effizienz, Sicherheit und Transparenz. Folgende Umsetzungsbeispiele aus der Projektpraxis stehen für diese neue Welt:

1. Adaptive Authentifizierung statt statischer Logins über VPN

Klassische statische Passwörter werden durch kontextbasierte MFA ersetzt. Während VPNs Zugang zu breiten Netzwerkkontext gewähren prüfen Identity-Aware Proxies (IAP) hingegen Identität, Gerätestatus und Kontext bei jedem Zugriff und lassen nur spezifische Anwendungen zu. Adaptive Authentifizierung bestimmt anhand von Verhalten, Geostandort und Nutzungsverhalten dynamisch das erforderliche Authentifizierungsniveau, was auch als Attribute-Based Access Control (ABAC) bezeichnet wird. Dies vermeidet zusätzlichen Login-Aufwand für den Benutzer, da nur bei verdächtigen Versuchen eine komplexe Authentifizierung nötig wird. Außerdem reduziert es die Erfolgschancen auch fortgeschrittener Angriffe (Credential Stuffing, Phishing) und schafft zugleich bessere Auditierbarkeit der Zugangsvorgänge.

2. Mikrosegmentierung statt große Netzwerkzonen

Segmentierung auf Anwendungs-, Container- oder sogar Prozessebene begrenzt potenzielle Angriffsflächen und erlaubt gezielte Reaktionsmechanismen. So lassen sich etwa sensible Backend-Server untereinander isolieren: Ein kompromittierter Prozess kann dann nicht einfach seitlich ins nächste System vordringen. Moderne Lösungen machen Segmentierung dabei automatisierbar: Erreicht ein System eine neue Bedrohungslage, schiebt die Plattform Quarantäneregeln nach, ohne dass Administratoren manuell in die Firewall eingreifen müssen.

3. KI-gestützte Echtzeitanalyse statt Schwellenwertalarme

Lernende Systeme erkennen feinste Verhaltensabweichungen und stoppen potenzielle Angriffe früher und präziser als klassische SIEM-Systeme. Die KI lernt die Normalzustände in operativen Systemen und erkennen sofort, wenn abweichendes Verhalten auftritt – sei es ein unerwarteter Traffic-Peak in der Zahlungsabwicklung oder ein unautorisiertes Leseversuch an sensiblen Kundendaten. Erkennt die KI etwa einen ungewöhnlichen Vorgang, initiiert sie automatisch Gegenmaßnahmen: Benutzerzugriffe werden gesperrt oder betroffene Geräte isoliert, noch bevor ein menschlicher Analyst reagieren kann.

Das Jahr 2025 hat gezeigt, dass diese Methoden bereits verstärkt eingesetzt worden sind und bemerkenswerte Erfolge bei Reaktionsgeschwindigkeit und Risikoreduktion erzielt haben.

6.2. Die Herausforderungen für Unternehmen

Trotz der Überzeugungskraft moderner Sicherheitsansätze sehen sich viele Unternehmen mit erheblichen Hindernissen konfrontiert.

Abbildung 8: Kernelemente einer Zero Trust Architektur zur Absicherung moderner IT-Umgebungen.

Fünf typische Hemmnisse für die Zero-Trust-Umsetzung:

1. **Monolithische Legacy-Systeme:** Kernsysteme wurden oft ohne Modularität oder Schnittstellenstrategie entwickelt.
2. **Mangelnde Sichtbarkeit:** Viele Unternehmen kennen ihre eigenen Zugriffspfade, Privilegien und Datenflüsse nur unzureichend.
3. **Komplexität im Betrieb:** Zero Trust verlangt eng getaktete Zusammenarbeit zwischen IT, Risk, CISO und Fachbereichen.
4. **Kosten und Ressourcen:** Transformation benötigt Budget, Spezialwissen und oft externe Unterstützung.
5. **Kultureller Wandel:** Fachbereiche müssen Zugangskontrollen als Notwendigkeit akzeptieren, nicht als Bremse.

In der Praxis helfen oft Übergangslösungen, den Einstieg risikoorientiert zu erleichtern. Beispielsweise ermöglichen IAPs selektive Kontrolle vor monolithischen Legacy-Systemen und Virtualisierung von Zugriffspfaden trennt veraltete Kernsysteme von modernen Frontends und durch Just-in-Time-Zugriffssteuerung erhalten speziell Administratoren oder Systeme anstatt dauerhafter Vollzugriffsrechte nur befristete, kontextabhängige Berechtigungen. Aus unseren Projekten wissen wir: Es gibt kein One-Size-Fits-All sondern die Lösungen müssen der individuellen Realität der IT-Landschaft des Kunden folgen. Das kann insbesondere auch den Einsatz von hybriden Modellen bedeuten, in denen Zero-Trust-Prinzipien selektiv eingeführt werden – beispielsweise zuerst für privilegierte Nutzer oder Drittanbieter.

6.3. Zero Trust trifft DORA: Zwischen Konformität und Übererfüllung

Mit DORA erhalten IT-Sicherheit und digitale Resilienz erstmals eine europäisch einheitliche Regulierungsgrundlage. Viele der zentralen Forderungen wie Echtzeit-Detection, Zugriffskontrolle, Rechenschaftspflicht und Lieferkettensteuerung lassen sich durch Zero-Trust-Konzepte direkt umsetzen – und in manchen Fällen sogar übertreffen.

DORA-Kernanforderungen und ZTA-Antworten:

// **Schutz kritischer Funktionen:** Mikrosegmentierung schützt gezielt geschäftskritische Prozesse und Systeme.
// **Incident Response**: KI-gestützte Anomalieerkennung ermöglicht frühzeitiges Erkennen und Eingrenzen.
// **Business Continuity:** Isolierte Zugriffspfade verhindern Dominoeffekte bei Kompromittierungen.
// **Drittparteiensteuerung:** Zugriff wird nicht nur eingeschränkt, sondern zeitlich und funktional begrenzt.
// **Testing und Kontrolle:** Zero Trust erzwingt systematische Testbarkeit und dokumentierte Wirkungskontrolle von Sicherheitsmaßnahmen.

ZTA liefert also nicht nur ein Instrument zur DORA-Umsetzung – es ermöglicht ein proaktives Risikomanagement, zum Teil über regulatorische Mindestanforderungen hinaus.

Warum sich Zero Trust trotzdem rechnet

Angesichts des Umfangs scheint Zero Trust für viele Unternehmen wie ein überdimensionierter Kraftakt. Aber, die Investition lohnt sich:

1. Vermeidung technischer Schulden: Wer heute reaktiv Sicherheitsinseln baut, zahlt morgen doppelt für Umbau und Integration. Eine stringente Zielarchitektur spart langfristig Kosten und Zeit.

2. Automatisierung reduziert Betriebskosten: Finanzdienstleister berichten von bis zu 35% geringeren Kosten durch gezielte Automatisierung, insbesondere in Prozessen mit hohem regulatorischem Dokumentationsaufwand.

3. Minimierung regulatorischer und operativer Risiken: Angesichts der potenziellen Bußgelder (z. B. bei DORA-Verstößen) und der immensen Kosten bei Sicherheitsvorfällen ist Zero Trust ein effektives Schutzinstrument – auch für die Bilanz.

ZERO TRUST IST KEINE OPTION – SONDERN EINE STRATEGISCHE NOTWENDIGKEIT.

Wer frühzeitig handelt, spart sich langfristig operative und regulatorische Umwege.

7. Cybersecurity im Fokus: Metriken statt Bauchgefühl

„Wie gut sind wir denn geschützt?" – diese Frage gehört zu den Klassikern, wenn das Management das Thema Cybersecurity adressiert. Die ehrliche Antwort lautet: Cyber-Security leicht interpretierbar zu vereinfachen, ist eine gewagte, aber erforderliche Übung – Cyber-Metriken sind hierfür ein zentraler Baustein.

7.1. Mehrwert von Cybersecurity-Metriken

Cybersecurity-Metriken sind quantifizierbare Messgrößen bzw. KPIs, die die Wirksamkeit von Sicherheitsmaßnahmen abbilden. Dadurch stellen sie eine datenbasierte Grundlage dar, die Wirksamkeit von Cybersecurity-Maßnahmen zu bewerten. Sie liefern Einblicke für Entscheidungsfindung, Risikomanagement und den Nachweis von Sicherheitsleistungen gegenüber Stakeholdern. Gemessen werden u. a. Reaktionsgeschwindigkeit bei Vorfällen, Patch-Zeiten, Erkennungsraten von Bedrohungen oder die Einhaltung von Richtlinien. Mit sauber austarierten Metriken kann man:

// Fundierte Entscheidungen treffen: Metriken schaffen Transparenz über Risiken und Fortschritte – und ermöglichen faktenbasierte Entscheidungen statt Bauchgefühl.
// Wertbeitrag belegen: KPIs zeigen, welche Maßnahmen wirken und wo Ressourcen den höchsten Nutzen stiften.
// Compliance nachweisen: Kennzahlen machen regulatorische Erfüllung messbar und zeigen frühzeitig, wo Handlungsbedarf besteht.

Welche Metriken aber verwendet werden sollen, hängt dabei unter anderem von Branche, Unternehmensgröße und regulatorischen Anforderungen ab. Als Orientierung bietet sich ein Überblick über zentrale Themenfelder und typische Kennzahlen an:

// Threat Detection & Exposure Monitoring

Aussagekräftige Kennzahlen zeigen, wie gut echte Angriffe erkannt und priorisiert werden – über alle relevanten Dimensionen hinweg. Dazu gehören die Abdeckung kritischer Use Cases im Monitoring (z. B. MITRE ATT&CK-Taktiken), das Verhältnis von geblockten zu erfolgreichen Angriffen bei Phishing, Malware oder Credential-Attacken sowie die True-Positive- bzw. False-Negative-Rate im SIEM/EDR. Ergänzend geben Kennzahlen wie die Time to Triage (MTTT) oder der Analysten-Workload pro Incident Hinweise darauf, wie effizient die Detection-Pipeline arbeitet.

// Incident Response Performance

MTTD, MTTC und MTTR sind weiterhin die zentralen Messgrößen für die Reaktionsgeschwindigkeit und Effektivität der Sicherheitsorganisation. Eine schrittweise Reduktion des Incident-Impact über die Zeit zeigt dabei, dass Maßnahmen nicht nur schnell, sondern auch wirksam sind. Ergänzend kann die Rate vollständig gelöster Vorfälle ohne Re-Opening bewertet werden, um nachhaltigen Lernerfolg sicherzustellen.

// Identity & Access Security

Im Fokus stehen die Sicherheit privilegierter Zugriffe und die konsequente Minimierung von Identitätsrisiken. Kennzahlen wie die Abdeckung mit Multi-Faktor-Authentisierung, die Anzahl risikobehafteter Aktivitäten privilegierter Accounts sowie das fristgerechte Entziehen überflüssiger Berechtigungen (Joiner-Mover-Leaver) sind dabei aussagekräftig. Weitere Indikatoren sind verwaiste Accounts oder „toxic combinations" in sensiblen Rollen, die im Idealfall eliminiert werden.

// Vulnerability & Configuration Management

Hierzu zählen die durchschnittliche Verweildauer kritischer Schwachstellen sowie der Anteil rechtzeitig geschlossener High-Risk-Vulnerabilitäten. Ebenso relevant ist die Anzahl unbekannter oder nicht inventarisierter Systeme („Shadow IT"), da nur bekannte Assets geschützt werden können. Eine steigende Secure-Configuration-Coverage, etwa anhand etablierter Benchmarks, belegt, dass Prävention nicht nur reaktiv, sondern strukturell verankert ist.

// Resilience & Recovery

Mit Blick auf Ransomware und Supply-Chain-Angriffe gewinnt die Fähigkeit zur schnellen Wiederherstellung zunehmend an Bedeutung. KPIs wie die Wiederherstellungszeit kritischer Services, die Erfolgsrate regelmäßig getesteter Backups sowie die Abdeckung getesteter Wiederanlaufpläne zeigen, wie robust das Unternehmen bei erfolgreichen Angriffen aufgestellt ist. Eine kontinuierliche Verbesserung dieser Werte reduziert den realen Schaden im Ernstfall deutlich.

// Governance, Risk & Compliance

Wirksame Governance misst sich an der Einhaltung definierter Kontrollen über alle kritischen Assets hinweg. Dazu gehören die Policy-Compliance-Rate, die Rezertifizierungsquote privilegierter Berechtigungen sowie die Anzahl signifikanter Findings aus Audits oder Third-Party-Assessments. Die Entwicklung zentraler Kontroll-Maturity-Scores macht Fortschritte messbar – und zeigt, ob Security-Regeln im Alltag tatsächlich gelebt werden.

// Security Awareness & Human Defense

Neben Trainingsquoten zählen vor allem konkrete Verhaltensmetriken, die reale Risiken abbilden. Dazu gehören eine niedrige Klickrate bei simulierten Phishing-Angriffen, eine kurze Time-to-Report verdächtiger Nachrichten sowie die Anzahl wiederholt auffälliger Nutzer. Diese Werte zeigen, ob Sicherheitsbewusstsein im Arbeitsalltag verankert ist und ob Mitarbeitende zur aktiven Verteidigung beitragen.
Der Überblick zeigt, wie vielfältig Security-Metriken sind – und wie anspruchsvoll ihre praktische Umsetzung ist.

7.2. Vorgehensmodell für Cybersecurity Metriken & Reporting

Die Dauer bis zur letztendlichen Messung und Interpretation von KPIs hängt stark vom Reifegrad der Organisation und den definierten Zielvorstellungen ab. Ein Minimum Viable Product (MVP) lässt sich erfahrungsgemäß oft innerhalb weniger Wochen umsetzen. In unseren Projekten folgen wir dabei einem konzeptionellen Vorgehen in drei Stufen.

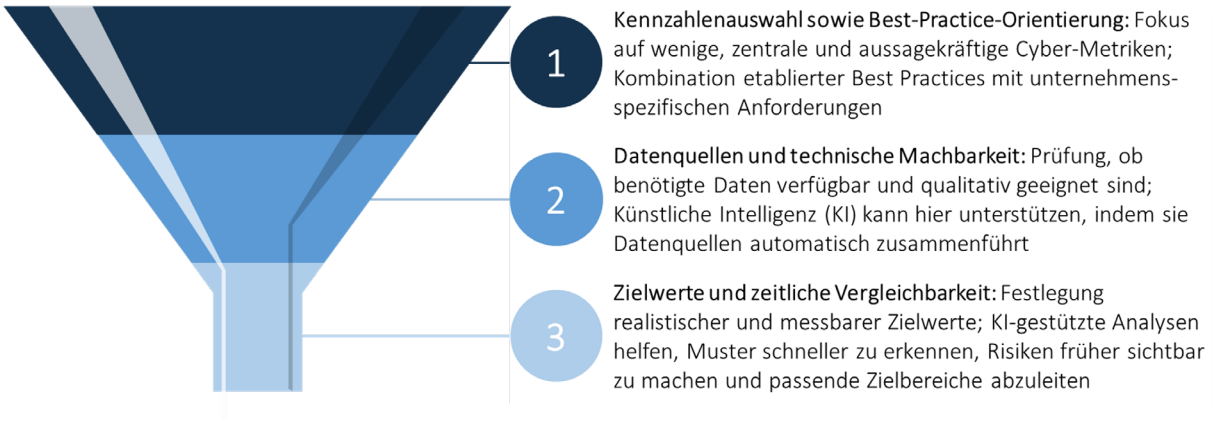

Abbildung 9: Typisches Vorgehensmodell zur Etablierung und dem Reporting von Cybersecurity-Metriken

1. Kennzahlenauswahl sowie Best-Practice-Orientierung

Um geeignete Metriken für jedes Themenfeld festzulegen, lohnt es sich zunächst, ggf. bereits im Einsatz befindliche Kennzahlen bzw. Best Practices (siehe Auflistung oben) zu prüfen und daraus eine konzentrierte Auswahl zu treffen. Entscheidend ist der Fokus auf wenige KPIs, die tatsächlichen Mehrwert liefern, statt eine breite und schwer überschaubare Sammlung anzubieten. Kennzahlen erfüllen ihren Zweck genau dann, wenn sie den aktuellen Status klar vermitteln und gleichzeitig Orientierung für das weitere Vorgehen liefern. Darauf aufbauend lassen sich konkrete Maßnahmen definieren, z. B. mehr Awareness-Trainings mit klaren Verantwortlichkeiten und regelmäßigen Fortschritts-Reviews.

2. Datenquellen und technische Machbarkeit

Eine Cyber-Metrik entfaltet jedoch nur dann Wirkung, wenn die zugrunde liegenden Daten verlässlich sind. In vielen Projekten zeigt sich: bestehende Systeme, etwa Security Information, Event Management oder Ticketsysteme, liefern zwar Daten, konsolidieren oder priorisieren sie aber nicht zu handlungsfähigen Erkenntnissen – oft fehlt hierbei ein definierter Standard an Datenqualität. Verfügbarkeit, Aktualität, Schätzungen und viele andere Phänomene führen in der Erhebung und Prozessierung zu Unschärfe. Schwerwiegender ist aber, dass oft Begriffe und Ereignisse unterschiedlich definiert sind oder unterschiedlich verstanden werden. Somit wird eine konstante Bedeutung der Metrik über die Zeit nicht gewährleistet. Ein Data Dictionary zu jeder KPI mit eindeutigen Definitionen ist daher erforderlich, um Interpretationsunschärfe zu begegnen. Zudem kann der Einsatz von KI die Datenkonsolidierung und ihre automatische Bereitstellung deutlich vereinfachen. Entscheidend ist jedoch, diese Möglichkeiten bereits in der Projektkonzeption einzuplanen, um späteren Mehraufwand zu vermeiden.

3. Zielwerte und zeitliche Vergleichbarkeit

Zuletzt besteht die Frage, wie nun Ziel- und Referenzwerte festgelegt werden können. In unserer Projekterfahrung hat sich ein pragmatisches Vorgehen bewährt: historische Werte analysieren, technische Rahmenbedingungen berücksichtigen und anschließend Zielbereiche mit relevanten Fachbereichen definieren. Unterstützend können KI-gestützte Analysen eingesetzt werden, die große Datenmengen schneller auswerten, Muster zuverlässig identifizieren und aufkommende Risiken frühzeitig sichtbar machen. Dadurch entstehen fundierte Analyseergebnisse, die helfen, Zielbereiche präziser abzuleiten und klar zu bestimmen, ab wann eine Kennzahl als unkritisch, verbesserungsbedürftig oder kritisch einzustufen ist. Ebenso wichtig ist die langfristige Vergleichbarkeit. Wie schon angedeutet, verändern sich Systeme oder Messmethoden im Zeitverlauf auch naturgemäß bzw. zwangsläufig. Frühere Messungen der gleichen Kennzahl können nicht als gleiche Kennzahl interpretiert werden. Ein möglichst stabiles bzw. langfristig ausgerichtetes Messkonzept hilft, Trends verlässlich zu interpretieren. Ergänzend empfiehlt sich ein kurzer regelmäßiger Abgleich der zentralen KPIs. So lassen sich Ausreißer, technische Messfehler oder veränderte Rahmenbedingungen frühzeitig erkennen.

7.3. Kernprinzipien für wirksames Cybersecurity Reporting

Damit Metriken akzeptiert werden und im Idealfall „für sich selbst sprechen", braucht es mehr als nur Zahlen. Erfolgreiches Reporting verbindet Klarheit, Kontext und konsequente Visualisierung – damit die Organisation jederzeit versteht, wo sie steht und was zu tun ist.

// Zielgruppenorientierung & Relevanzfokus Ein CFO hat andere Informationsbedürfnisse als ein SOC-Lead. Deshalb sollte jede Metrik auf das Wesentliche reduziert und so präsentiert werden, dass der Nutzen für die jeweilige Zielgruppe sofort erkennbar ist. Ein klarer Management-Fokus auf Risiko, Trend und Handlungsnotwendigkeiten verhindert Detailüberlastung – „Data Diet statt Data Dump"

// Kontext & Interpretation liefern – Story statt Zahlenfriedhof

Eine Zahl ohne Einordnung beantwortet keine Fragen. Erst Trends, Benchmarks, Risikobewertungen und Ursachen liefern Bedeutung. Gute Reports zeigen, warum sich ein Wert verändert hat, welche Maßnahmen daraus folgen und welchen Effekt diese künftig haben. Erfolgreiches Security Reporting ist immer auch Business Storytelling: Wie ist der aktuelle Stand? Was wurde erreicht? Was ist als Nächstes notwendig?

// Visualisierung mit System – Konsistent, intuitiv, wiedererkennbar

Dashboards, Heatmaps oder Ampel-Visualisierungen helfen, komplexe Sachverhalte schnell zu erfassen. Wichtig sind einheitliche Skalen, klare Farben und konsistente Darstellungslogik – so wird Reporting lesbar, vergleichbar und langfristig akzeptiert. Ein gutes Visual vermittelt auf einen Blick die Antwort auf die Kernfrage: Wie gut sind wir gegen Cyberrisiken geschützt – und wohin entwickeln wir uns?

8. FAZIT

Die in dieser Unterlage zusammengefassten Beiträge machen es deutlich: Cybersecurity befindet sich in einem grundlegenden Wandel. Steigende Bedrohungen, neue Technologien wie Künstliche Intelligenz und Quantencomputing sowie eine wachsende Datenabhängigkeit zwingen Unternehmen dazu, Sicherheitsstrategien neu zu denken. Reaktive Einzelmaßnahmen reichen längst nicht mehr aus – gefragt sind integrierte, vorausschauende und messbare Sicherheitsansätze.

Themen wie Cryptoagilität, datenzentrierte Sicherheit (DSPM und CSM), KI-gestützte Risikoerkennung sowie die Orchestrierung und Automatisierung von Sicherheitsvorfällen zeigen, wie moderne Cybersecurity heute aussehen muss: vernetzt, skalierbar und eng an den Geschäftsanforderungen ausgerichtet. Gleichzeitig unterstreicht die Diskussion um Zero Trust, dass Sicherheitsarchitekturen kein Selbstzweck sind, sondern konsequent am individuellen Risikoprofil und Reifegrad eines Unternehmens ausgerichtet werden müssen. Verlässliche Metriken schaffen dabei Transparenz und bilden die Grundlage für fundierte Entscheidungen.

DIE AUTOREN

Dr. Oliver Laitenberger

Dr. Carsten Woltmann

Robert Tippmann

Dr. David Bauder

Dr. Moritz Pleintinger

Dr. Thomas Kurz

Markus Ettenauer

Timothy Borrell

Christoph Halwachs

ÜBER HORN & COMPANY

HORN & COMPANY ist eine im Kern auf Banken und Versicherungen sowie Industrie und Handelsunternehmen spezialisierte Top-Management-Beratung. Der Fokus der über 160 BeraterInnen liegt auf Strategieprozessen, GuV-orientierte Performance-Verbesserung und der digitalen Transformation. Mit Gründung der „Horn & Company Data Analytics GmbH" und Kooperationen mit Software-Entwicklern und IT-Lösungsanbietern hat Horn & Company ein Consulting-Ökosystem für die digitale Transformation etabliert. Für die Jahre 2026/27 wurden die BeraterInnen von Horn & Company zum wiederholten Mal als „Hidden Champion des Beratermarktes" ausgezeichnet.

Das Unternehmen mit Hauptsitz in Düsseldorf hat Büros in Berlin, Frankfurt am Main, Hamburg, München, Wien und Zürich. www.horn-company.de HORN & COMPANY ist Mitglied im exklusiven Beraterpool für Stabilisierungsmaßnahmen des Wirtschaftsstabilisierungsfonds (WSF). Für unsere Auswahl waren insbesondere die großen Erfahrungen in Sanierung und Turnaround sowie die Kenntnisse von Schlüsselbranchen und mittelständischen Unternehmen ausschlaggebend.

Horn & Company wird zudem in unabhängigen Beratervergleichen regelmäßig ausgezeichnet, unter anderem als „HIDDEN CHAMPION", als „TOP CONSULTANT/BERATER DES JAHRES" und „BESTE BERATER".

HORN & COMPANY
Kaistraße 20 | 40221 Düsseldorf
Telefon +49 (0)211 30 27 26-0 | info@horn-company.de
www.horn-company.com