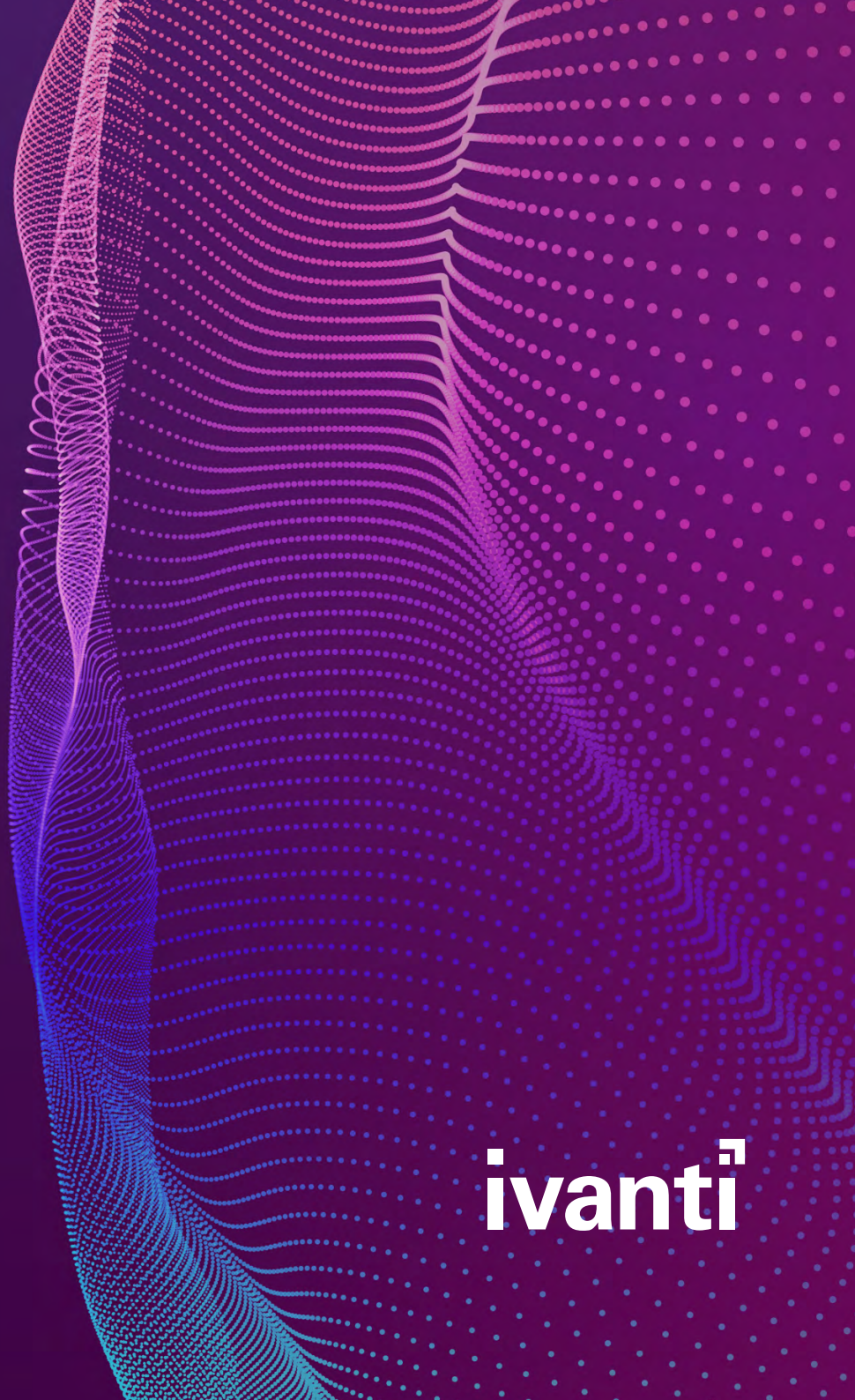
Wie das Exposure Management die Cybersicherheit verändern wird

Fünf strategische Veränderungen,
die neue Perspektiven eröffnen



ivanti

Das Konzept des Exposure-Management entwickelt sich zu einer **transformierenden Kraft in der Cybersicherheit.**

Im Gegensatz zu herkömmlichen Ansätzen, die Risiken oft isoliert betrachten, ermöglicht das Exposure-Management ein kontextbezogenes Verständnis von Bedrohungen und verknüpft diese mit den übergeordneten Unternehmenszielen. Dies ist nicht nur ein Perspektivwechsel, sondern eine tiefgreifende Neuausrichtung der Sicherheitsstrategie von Unternehmen.

Die Zahl und Komplexität der Bedrohungen, mit denen Unternehmen heute konfrontiert sind, wird weiter zunehmen, sodass sich auch die Art und Weise, wie Unternehmen Cyberrisiken wahrnehmen, ändern muss. Sicherheit darf nicht länger als alleinige Verantwortlichkeit der IT-Abteilung gesehen werden. Stattdessen sollte sie als gemeinsame Aufgabe verstanden werden, bei der alle Unternehmensbereiche zusammenarbeiten, um Risiken zu identifizieren, zu mindern und zu steuern. Dieser kollaborative Ansatz stärkt die Resilienz eines Unternehmens, fördert Innovationen und schafft Wettbewerbsvorteile.

Die kontinuierliche Weiterentwicklung des Exposure-Managements besitzt das Potenzial, die Cybersicherheit und ihre Bedeutung auf Unternehmensebene nachhaltig zu transformieren. Wir sind überzeugt, dass die folgenden fünf Szenarien nicht nur möglich, sondern als logische Konsequenz dieser Entwicklung eintreten werden.

Fünf strategische Veränderungen des Exposure-Managements

01

Unternehmen entwickeln eine ganzheitliche Perspektive auf Cybersicherheitsrisiken.

02

Der Begriff der „Angriffsfläche“ wird deutlich erweitert.

03

Die Bewertung von Cybersicherheitsrisiken wandelt sich von subjektiven Einschätzungen hin zu objektiven Analysen.

04

Cybersicherheitsstrategien werden künftig als zentrale Orientierung für betriebliche Investitionen fungieren.

05

Die C-Suite wird das informierte Management von Cybersicherheitsrisiken stärker in den Mittelpunkt rücken.

01

Unternehmen gehen zu einer allumfassenden Sichtweise des **Cybersicherheitsrisikos** über.

Heutzutage liegt das Risikomanagement größtenteils, wenn nicht sogar vollständig, in den Händen des IT-Teams. Diese isolierte Herangehensweise steht oft im Widerspruch zu einer umfassenden, unternehmensweiten Strategie, die das Kerngeschäft und seine Bedürfnisse berücksichtigt.

Zudem dreht es sich häufig um sogenannte Einzellösungen, d. h. Lösungen, die speziell entwickelt wurden, um einzelne Sicherheitsbedrohungen zu bewältigen, sobald sie auftreten. Dadurch entsteht eine Dynamik, die isolierte Spezialisierungen verstärkt und eine ganzheitliche Betrachtung von Cyberrisiken erschwert. Da diese Einzelprodukte oft nicht nahtlos miteinander integriert werden können, entstehen durch die fehlende Zusammenarbeit Lücken, die letztlich eine optimale Sicherheitsabdeckung gefährden können.

Umvon dieser problematischen Vorgehensweise wegzukommen, empfiehlt es sich, Ihre Risikodaten zu konsolidieren und eine umfassende, kontextbezogene Perspektive auf Cybersicherheitsrisiken einzunehmen. Nachfolgend finden Sie praktische Schritte, die Ihnen helfen, ein ganzheitliches Risikomanagement zu erreichen.

Datenerfassung und -integration

Führen Sie eine umfassende Inventarisierung aller im Unternehmen eingesetzten Cybersicherheits-Tools und -Plattformen durch und implementieren Sie eine zentrale Plattform, um die gewonnenen Risikodaten zentral zu erfassen.

Kontextbezogene Risikobewertung

Entwickeln Sie ein Risikobewertungsmodell, das den umfassenden Kontext des Unternehmens berücksichtigt, die potenziellen Auswirkungen von Risiken bewertet und ihnen entsprechende Priorität einräumt.

Integriertes Risikomanagement

Gewinnen Sie einen klaren Überblick über Ihre Risikosituation mithilfe einer integrierten Risikomanagement-Plattform, die Echtzeitüberwachung sowie automatisierte Workflows bietet, um Reaktionen und

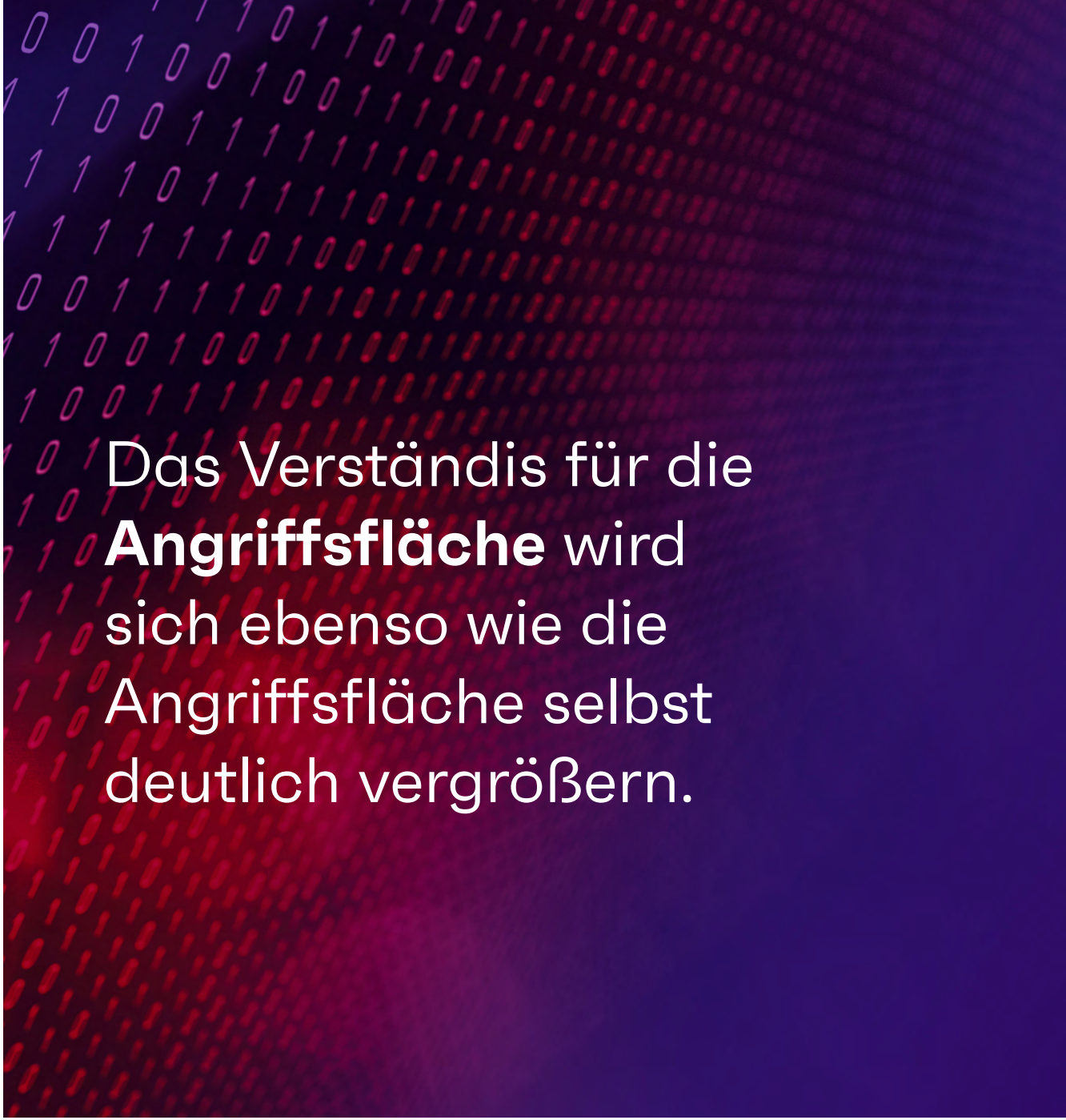
Strategische Ausrichtung

Entwickeln Sie Reports auf Führungsebene, die einen klaren, präzisen Überblick über die Risikolage des Unternehmens geben und die Cybersicherheit nahtlos in die Geschäftsplanung integrieren.

Mit diesem Ansatz können Unternehmen eine umfassendere, kontextbezogene Sicht auf Cybersicherheitsrisiken gewinnen, diese in die Ziele ihres Kerngeschäfts integrieren und dadurch ihre Resilienz sowie ihren Wettbewerbsvorteil steigern.

Die Angriffsfläche Ihres Unternehmens ist dynamisch und ständig im Wandel. Mit der rasanten Weiterentwicklung der IT-Landschaft stoßen die klassischen Parameter wie Software und Hardware an ihre Grenzen. Sie allein können die Vielzahl an entscheidenden Faktoren, die eine moderne Sicherheitsstrategie ausmachen, nicht mehr abdecken.

Mit der zunehmenden Vernetzung der Technologien, die moderne Unternehmen antreiben, wächst auch ihre Angriffsfläche. Neue Herausforderungen wie Cloud-Umgebungen, externe Dienstleister und eine stetig wachsende Zahl menschlicher Einflussfaktoren eröffnen spezifische Schwachstellen, die Unternehmen unbedingt berücksichtigen müssen.



Nachfolgend finden Sie einige der vielen Faktoren, die als Teil der Angriffsfläche betrachtet werden sollten.

Jenseits von Software und Hardware

Bedenken Sie, dass die Angriffsfläche über die traditionellen IT-Ressourcen hinausgeht. Sie umfasst auch Aspekte wie Cloud-Umgebungen, IoT-Geräte, Drittanbieter, Partner in der Lieferkette, menschliche Einflüsse und weitere kritische Bereiche.

Cloudsicherheit

Integrieren Sie Daten aus Cloud Security Posture Management (CSPM)-Tools, um Risiken im Zusammenhang mit Cloud-Diensten zu überwachen und zu verwalten. Stellen Sie sicher, dass Cloud-Umgebungen kontinuierlich auf Compliance sowie die Einhaltung bewährter Sicherheitspraktiken geprüft werden.

IoT-Geräte

Nutzen Sie Daten aus IoT-Sicherheitslösungen, um die spezifischen Schwachstellen vernetzter Geräte effektiv zu beheben. Implementieren Sie robuste Überwachungs- und Verwaltungspraktiken, um IoT-Geräte zu sichern und potenzielle Risiken zu minimieren.

Drittanbieter-Risiko

Verwenden Sie Daten aus Tools für das Drittanbieter-Risikomanagement (TPRM), um die Sicherheitslage Ihrer Lieferanten und Partner fundiert zu bewerten. Führen Sie regelmäßige Überprüfungen der Beziehungen zu Drittanbietern durch, um sicherzustellen, dass diese den Sicherheits- und Compliance-Standards Ihres Unternehmens entsprechen.

Menschliche Einflüsse

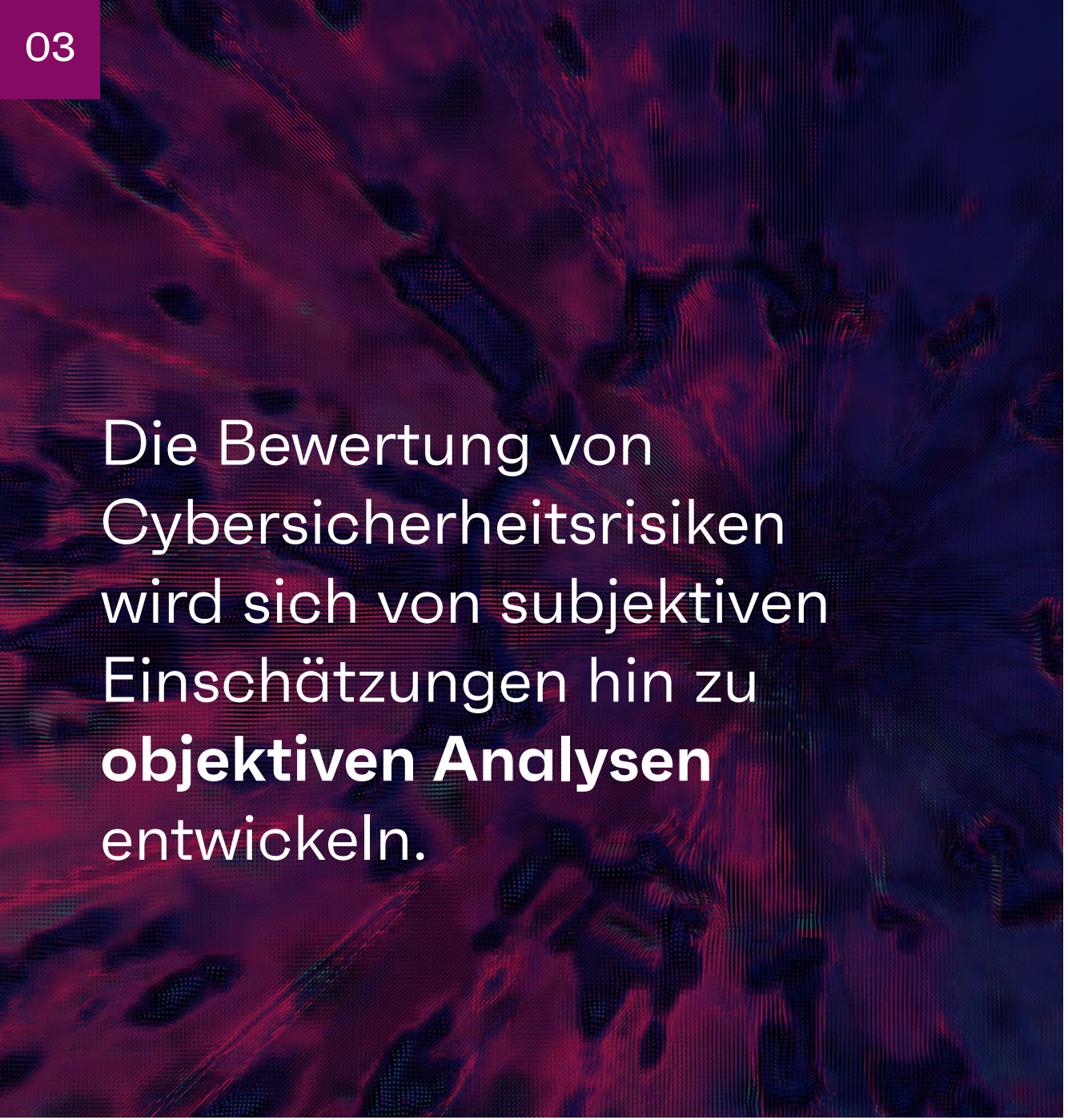
Berücksichtigen Sie Daten aus Programmen für Security-Awareness-Trainings und Phishing-Simulationen, um Risiken im Zusammenhang mit menschlichem Verhalten besser zu verstehen und zu minimieren.

Schutz vor digitalen Risiken

Nutzen Sie Daten aus Systemen zum Schutz vor digitalen Risiken, um Gefahren über verschiedene digitale Kanäle hinweg zu überwachen – von sozialen Medien über das Dark Web bis hin zu anderen Online-Plattformen. So können Bedrohungen wie Marken-Imitationen und Datenlecks frühzeitig erkannt und gezielt bekämpft werden.

Durch die Ausweitung der Angriffsfläche auf diese zusätzlichen Bereiche gewinnen Unternehmen eine umfassende und kontextbezogene Sicht auf Cybersicherheitsrisiken, was ihre allgemeine Resilienz stärkt.

03



Die Bewertung von Cybersicherheitsrisiken wird sich von subjektiven Einschätzungen hin zu **objektiven Analysen** entwickeln.

Die von Sicherheitsteams derzeit verwendeten Metriken sind für die strategische Planung nur bedingt geeignet, da es an allgemein anerkannten Standards mangelt. Sicherheitsrahmenwerke und -standards bieten zwar eine gewisse Orientierung, fokussieren sich jedoch meist darauf, was getan werden muss, statt darauf, wie dies konkret umzusetzen ist.

Das Exposure-Management wird eine präzisere Messung von Entscheidungsdaten ermöglichen und Führungskräften gleichzeitig die besseren Ergebnisse liefern: verwertbare, objektive Informationen, die Unternehmen dabei unterstützen, ihre angestrebte Sicherheitslage zu erreichen.

Nachfolgend finden Sie die Maßnahmen, die Sie ergreifen können, um dieses Ziel zu erreichen.

Asset-Wert analysieren

Um die mit Ihren Assets verbundenen Risiken effektiv verwalten zu können, sollten Sie zunächst den Wert jedes einzelnen Assets ermitteln. Nutzen Sie bei dieser Analyse organisationsspezifische Informationen – wie interne Daten, Risikobereitschaft und einzigartige Schwachstellen – anstelle von allgemeinen

Risikowahrscheinlichkeit abschätzen

Bewerten Sie anschließend die Häufigkeit und Schwere von Risiken, um relevante Szenarien für Ihre Organisation zu entwickeln. Dies hilft Ihnen, die Wahrscheinlichkeit und potenziellen Auswirkungen verschiedener Risikoevents

Kategorisierung nach Risikoeinfluss

Kategorisieren Sie Ihre Assets basierend auf ihrem Risikoprofil und nutzen Sie dabei quantitative Methoden wie Value-at-Risk (VaR) und Conditional Value-at-Risk (CVaR).

Die fortschreitende Entwicklung des maschinellen Lernens wird diesen Wandel vorantreiben, indem sie präzise, in Echtzeit verfügbare Risikobewertungen ermöglicht, die Unternehmen bei ihren Entscheidungen unterstützen.

Derzeit wird die Cybersicherheit überwiegend von technischen Spezialisten verwaltet, die oft Schwierigkeiten haben, ihre Bedürfnisse klar und überzeugend an die C-Suite zu kommunizieren. Gleichzeitig erkennen Führungskräfte die zentrale Bedeutung der Cybersicherheit und die damit verbundenen Risiken, sind jedoch nicht immer in der Lage, die Wissenslücke zwischen ihnen und ihren IT- oder Sicherheitsteams zu schließen.

Diese Diskrepanz erschwert es Unternehmen, ein „angemessenes“ Cybersicherheitsbudget oder eine effektive Strategie zu definieren. In der Folge werden Entscheidungen häufig eher von Ängsten oder Branchentrends geprägt, statt auf einer fundierten und datenbasierten Grundlage getroffen zu werden. Dieser Ansatz führt zu falsch gesetzten Prioritäten, ineffizienter Ressourcenzuweisung und einem Mangel an Verantwortlichkeit. Selbst Unternehmen, die überzeugt sind, die richtigen Maßnahmen zum Schutz zu ergreifen, können dadurch scheitern.

Um diese Herausforderungen zu bewältigen, sollten Unternehmen einen strategischen Ansatz für die Cybersicherheit verfolgen und ihre operativen Prioritäten mit messbaren Leistungskennzahlen verknüpfen. So funktioniert es:

Datengesteuerte Entscheidungen

Kontinuierliches Erfassen und Analysieren von Leistungsdaten hilft dabei, herauszufinden, welche Aktivitäten die aussagekräftigsten Ergebnisse liefern und welche keinen angemessenen ROI erzielen.

Umfassende Aufsicht

Die breitere C-Suite sollte eine umfassende Entscheidungs- und Feedbackschleife überwachen. Dadurch wird sichergestellt, dass Sicherheitsinitiativen mit den Geschäftszielen übereinstimmen und das Unternehmen seine Investitionen bedarfsgerecht ausrichten kann.

Förderung einer sicherheitsorientierten Unternehmenskultur

Integrieren Sie Sicherheit als strategischen Mehrwert und nicht nur als Kostenfaktor. Ein solcher kultureller Wandel führt zu klügeren Investitionen und nachhaltig besseren Ergebnissen.

Verbesserte Kommunikation

Schaffen Sie klare Kommunikationswege zwischen Cybersicherheitsspezialisten und der Geschäftsleitung. Regelmäßige Briefings, Workshops und Schulungen können dazu beitragen, die bestehende Wissenslücke effektiv zu schließen.

Leistungsmetriken

Erstellen und tracken Sie Key Performance Indicators (KPIs), um die Wirksamkeit Ihrer Cybersicherheitsinitiativen zu messen. Dadurch erhalten Sie ein klareres Bild davon, was ein „gutes“ und „angemessenes“ Cybersicherheitsbudget ausmacht.

Durch die Umsetzung dieser Strategien können Unternehmen fundiertere Entscheidungen über ihre Investitionen in die Cybersicherheit treffen, sie mit den Unternehmenszielen in Einklang bringen und so bessere Ergebnisse erzielen.

05

Die C-Suite wird dem **datengestützten Cybersicherheitsmanagement** Priorität einräumen.

Ohne gemeinsame und nachvollziehbare Metriken lässt sich das Cybersicherheitsrisiko nicht angemessen gegenüber den Entscheidungsträgern in der Führungsebene kommunizieren. Die C-Suite ist dadurch gezwungen, die Sicherheitsstrategie des Unternehmens weitgehend zu erraten, da eine objektive Messung der Ergebnisse fehlt.

Derzeit fehlen zuverlässige Verfahren, die sowohl Objektivität gewährleisten als auch eine direkte Verbindung zu datengestützten Entscheidungen herstellen. Die Integration der Cybersicherheit in die Geschäftsstrategie wird dadurch schwierig, wenn nicht gar unmöglich, was eine solide Bewertung der Risikobereitschaft des Unternehmens erschwert oder verhindert.

Exposure-Management ermöglicht der C-Suite, eine zentrale Kompetenz im Umgang mit Cybersicherheitsrisiken zu entwickeln. Es unterstützt sie dabei, fundierte, konsistente und nachvollziehbare Entscheidungen zu treffen. Durch den Einsatz robuster Daten und fortschrittlicher Analysemethoden können Risiken im geschäftlichen Kontext genauer bewertet werden. Dadurch wird die Kommunikation gestärkt und die Zusammenarbeit auf allen Ebenen des Unternehmens verbessert.

Um dies zu erreichen, sind nicht nur neue Kompetenzen seitens der Anbieter notwendig. Es ist auch ein kultureller Wandel innerhalb des Unternehmens erforderlich. Zudem ist die Bereitschaft gefragt, bestehende Entscheidungsprozesse grundlegend zu überdenken. Folgendes ist erforderlich und so können Sie vorgehen:

Einen Rahmen für die Risikobereitschaft schaffen

Definieren Sie die Risikotoleranz des Unternehmens und stimmen Sie sie mit den Unternehmenszielen ab. Dieser Rahmen dient als Leitlinie für die Entscheidungsfindung und gewährleistet Kohärenz.

Erweiterte Analysen implementieren

Nutzen Sie datengestützte Erkenntnisse, um Trends zu erkennen, Bedrohungen vorherzusagen und die Wirksamkeit von Sicherheitskontrollen mit einem ganzheitlichen Blick auf die Risikolandschaft zu messen.

Risiken in Geschäftsterminologie kommunizieren

Übersetzen Sie technische Risiken in geschäftliche Auswirkungen, um Stakeholder einzubinden und fundierte Entscheidungen zu fördern. Verwenden Sie eine einheitliche Risikosprache und verständliche Metriken, um eine klare Kommunikation sicherzustellen.

Eine funktionsübergreifenden Zusammenarbeit fördern

Bauen Sie Silos ab und fördern Sie die Zusammenarbeit zwischen Sicherheits-, IT- und Businessteams. Etablieren Sie regelmäßige Meetings und Workshops, um die Aktivitäten aufeinander abzustimmen und ein gemeinsames Ziel zu verfolgen.

Regelmäßige Überprüfung und Anpassung

Gestalten Sie die informierte Entscheidungsfindung als einen fortlaufenden Prozess. Überprüfen Sie regelmäßig Risiken, Kontrollen und Annahmen, um auf die dynamische Bedrohungslandschaft einzugehen und fundierte Anpassungen vorzunehmen.

Mit der weiteren Entwicklung des Exposure-Managements zeichnet sich ein Wandel ab, der weitreichende Auswirkungen auf den gesamten Cybersicherheitsmarkt haben wird.

Wenn Führungskräfte eine aktivere Rolle in der Cybersicherheit übernehmen, verspricht dies eine stärkere strategische Top-Down Unterstützung. Dies befähigt Sicherheitsteams, schneller und umfassender auf neue Bedrohungen zu reagieren. Durch eine bessere Ressourcenzuweisung und größere Transparenz auf Führungsebene gewinnt das Risikomanagement an Bedeutung und wird als höhere Priorität betrachtet.

Cybersicherheit kann zu einem strategischen Erfolgsfaktor werden, der die übergeordneten Unternehmensziele durch eine neue Ebene der Abstimmung und Unterstützung fördert. Wenn dieses Sicherheitsbewusstsein sich durch alle Ebenen des Unternehmens zieht, führt der entstehende kulturelle Wandel zu einer gestärkten Sicherheitslage – bis hin zu den alltäglichen Gewohnheiten und dem Bewusstsein jedes einzelnen Mitarbeitenden. Die Demokratisierung von Sicherheit ermöglicht es dem Unternehmen, dynamischer auf Bedrohungen zu reagieren, gestützt durch Echtzeit-Feedback einer informierten und sicherheitsbewussten Benutzergruppe.

Exposure-Management markiert schließlich den Übergang von subjektiven zu objektiven Ansätzen. Ein besserer Zugang zu quantifizierbaren Daten verringert die Abhängigkeit von qualitativen Einschätzungen und ermöglicht datengetriebene Entscheidungen, die auf messbaren Risikofaktoren basieren. Mit einem klaren, empirischen Verständnis der größten Risiken können Unternehmen gezielter reagieren und Maßnahmen priorisieren, die die gravierendsten Schwachstellen adressieren.

Dies bedeutet eine grundlegende Transformation der Cybersicherheit – sowohl als praktisches Arbeitsfeld als auch als strategisches Unternehmensziel. Das Exposure-Management wird diesen Wandel in naher Zukunft und darüber hinaus maßgeblich vorantreiben.

ivanti

Für weitere Informationen oder um Ivanti zu kontaktieren, besuchen Sie bitte ivanti.de