TANIUM

CHIEF DISRUPTOR

Management von Informationsrisiken – Erwartung und Realität

Ein Bericht zu Taniums *Standpunkt* Bericht in Partnerschaft mit Chief Disruptor.

BERICHT ZUM STANDPUNKT

CONTENTS

Einführung

Informations- und Sicherheitsmanagement wurden oft an den anfallenden Kosten gemessen, anstatt an den erzielten Geschäftsergebnissen. Das ändert sich, da unsichere Betriebsbedingungen für Unternehmen das kommerzielle Wachstum zunehmend an ein genaues Verständnis der Risiken binden. Aber die digitale Transformation stellt Unternehmen vor neue Herausforderungen, die sich einen besseren Überblick über IT-Assets, Technologierisiken und Schwachstellen verschaffen möchten.

> **„Cybersicherheit zählt zu den drei größten Risiken. Wir erkennen das als Führungsteam und als Unternehmen an, daher wird sie 2023 große Bedeutung haben."**
>
> **Chief Information and Security Officer**
> FTSE-100-Verpackungsunternehmen

Für den Umgang mit dieser Herausforderung entwickeln Führungskräfte neue Strategien, um das Management von Informationsrisiken in die Art und Weise der Geschäftstätigkeit einzubetten. Inmitten dieser Veränderung wollten wir herausfinden, ob noch Lücken zwischen den Gedanken hinter diesen Strategien und der tatsächlichen Reife ihrer Umsetzung bestehen.

In diesem Bericht untersuchen wir kontextabhängige Push-and-Pull-Faktoren, die den Reifegrad des Informations- und Sicherheitssektors beeinflussen. Wir skizzieren dann häufig erwähnte Lücken zwischen den Erwartungen und der Realität, in Bezug auf das Management von Informationsrisiken. Der Bericht schließt mit Leitprinzipien ab, um die Erwartungslücke zwischen Strategie und Umsetzung zu schließen.

Anerkennungen

Die Autoren bedanken sich bei den leitenden Mitgliedern der Chief Disruptor Community, die sich im vierten Quartal 2022 Zeit für ein Interview für diesen Bericht genommen haben. Ihre Ansichten, von denen einige auf den folgenden Seiten zitiert sind, dienten als Richtschnur für diesen Bericht. Wir danken ihnen für ihre wertvollen Beiträge und Erkenntnisse.

Befragte

- Erik Gaston, VP Executive Engagement, Tanium
- Zac Warren, Chief Security Advisor, Tanium
- Barry Panayi, Chief Data & Insight Officer, John Lewis
- James Tomkins, Chief Architect, Met Office
- Jon Roughley, Director of Data Strategy and Innovation, Experian
- Paul Curtis, Chief Technology Officer, Easyjet Holidays
- Matthew Wilmot, Group Head of Enterprise IT & Information Security, Fraser Group
- Chief Information and Security Officer, Dienststelle des Ministeriums
- Chief Information and Security Officer, FTSE-100-Verpackungsunternehmen
- Senior Manager, CERT, Vodafone
- Que Tran, Regional Chief Information Officer, DP World
- Ketan Patel, Group Chief Information Officer, WH Smith

ABSCHNITT 1

Die aktuelle Situation

Die sich verändernde Gestalt der IT

Unsere Befragten bestätigten, dass sich die IT-Infrastruktur in den letzten Jahren schnell entwickelt hat. Der Wechsel von lokalen Rechenzentren zu öffentlichen und hybriden Clouds wirkte sich disruptiv auf die bisherigen Prozesse aus. Die Umstellung hat betriebliche Vorteile gebracht, darunter die schnelle Markteinführung, Skalierbarkeit und die Möglichkeit zur Sammlung und Speicherung größerer Datenmengen.

Vom Standpunkt der Sicherheit aus gesehen machten diese Entwicklungen einen neuen Ansatz für das Management von Informationsrisiken erforderlich. Mit physischer Speicherung vor Ort sind die Technologie-Assets eines Unternehmens greifbar und IT-Assets können mit traditionellen Ansätzen für die Bestandsverwaltung bewertet werden.

Mit der Verbreitung von Software- und Cloud-Lösungen nahm die Komplexität der IT-Landschaft exponentiell zu. Die Umstellung auf Remote-Arbeit und die Nutzung persönlicher Geräte bedeutet, dass die Grenze einer Organisation nicht mehr physisch definiert ist und die Angriffsvektoren zugenommen haben.

> „Wir haben Mitarbeiter, die ihre eigenen Geräte verwenden oder an verschiedenen Standorten auf der ganzen Welt arbeiten möchten. All diese Faktoren erhöhen die Komplexität des Netzwerks."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

> „Es geht nicht darum, eine von einem hoch spezialisierten Team verwaltete Grenze zu sichern, da Angriffsvektoren jetzt die Verwendung von WhatsApp oder das Öffnen einer E-Mail beinhalten."

James Tomkins
Chief Architect, Met Office

Da Unternehmen verstärkt strukturell auf Technologie aufbauen, wirkt sich eine Verletzung oder ein Angriff direkt auf die Betriebsfähigkeit eines Unternehmens sowie auf das Kundenerlebnis und das Markenkapital aus.

> „Das Risiko trat vor etwa 3 Jahren auf und wir hatten eine große Datenschutzverletzung mit starker Auswirkung in der Öffentlichkeit. Sie hat unseren Ruf massiv beeinträchtigt. Ab diesem Zeitpunkt haben wir beschlossen, unsere Investitionen in Risikomanagement und Cybersicherheit deutlich zu erhöhen."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

Die Risiken, die mit schlechtem Management von IT-Assets verbunden sind, können für ein Unternehmen erhebliche Verluste bedeuten. Für jede Stunde, die eine Website ausfällt, muss ein Unternehmen ggf. erhebliche Einbußen bei den Einnahmen hinnehmen. Zu beachten sind auch die mit einem Verstoß verbundenen Gebühren und Strafen. Negative Berichterstattung in der Presse und Social-Media-Diskussionen können sich auch auf zukünftige Umsätze auswirken. In Hinblick auf diese Faktoren wird das Geschäftsszenario für Investitionen in Tools, Prozesse und Mitarbeiter deutlich, um über die Compliance hinaus Schritte in Richtung Cyber-Resilienz zu unternehmen.

> „Die Sicherheit gewinnt Jahr für Jahr an Priorität. Es gibt mehr Geschichten als je zuvor über Unternehmen, die schwerwiegende Verstöße hatten. Infolgedessen gewinnen Sicherheitslösungen das Rennen um die Finanzierung, weil das neue Risiken birgt und die Ergebnisse katastrophal sein könnten."

Barry Panayi
Chief Data & Insight Officer, John Lewis

> „Langsam ist mittlerweile fast schon mit ‚down' gleichzusetzen. Ihre Website muss nicht ausfallen, um Ihrem guten Ruf zu schaden. Eine langsame Website kann in einem Social-Media-Feed negativ bewertet werden."

Erik Gaston
VP Executive Engagement, Tanium

Viele unserer Befragten prognostizierten, dass sich die organisatorischen Grenzen 2023 und darüber hinaus weiter auflösen werden. Da Unternehmen immer enger mit Partnern zusammenarbeiten, um gemeinsame Herausforderungen wie den Klimawandel, die Unterbrechung der Lieferkette und den Inflationsdruck zu bewältigen, müssen die Unternehmen ihre Daten und Informationen über die Betriebsgrenzen hinweg teilen. Das alles führt zu einem überzeugenden Argument für die vermehrte Priorisierung und Investitionen in Informationsmanagement- und Sicherheitslösungen.

„Wir haben standardisierte Protokolle eingeführt, die festlegen, wie alle unsere Partnerorganisationen in unser Netzwerk integriert werden, um die Risiken zu reduzieren, die wir tragen." Das steht im Gegensatz zu unseren Handlungsweisen in der Vergangenheit, nämlich der individuellen Zusammenstellung für jeden Partner. Ehe Sie sich's versehen, verwalten Sie viele verschiedene Systeme nur für das Management der ein- und ausgehenden Daten", sagt Paul Curtis, Chief Technology Officer bei Easyjet Holiday

Ein Mandat des Vorstands

Da Informationen und Technologie zu wichtigen Bestandteilen der Geschäftsfähigkeit eines Unternehmens geworden sind, hat sich die Rolle des Chief Information Officer entsprechend der wachsenden Bedeutung dieses Themas weiterentwickelt. Da die IT im Allgemeinen stark mit dem Geschäft verwachsen ist, steht die Rolle des CIO nun im Mittelpunkt.

> „Die Sicherheit fand ihren Platz bisher immer an der Seite in einer Nische. In den meisten Unternehmen sehe ich, dass sich die Rolle des CIO verändert und sich stärker am Geschäft orientiert. Hier taucht die Sicherheit dort wieder auf, wo sie eigentlich hingehört – direkt im Zentrum."

Erik Gaston
VP Executive Engagement, Tanium

Da die Sicherheit des Informations- und Technologie-Stacks eines Unternehmens zu einer der obersten Prioritäten für den Vorstand geworden ist, stiegen die Sicherheitsbudgets. Im Hinblick auf diese Priorität entwickelt sich auch die Rolle des CISO weiter. Der CISO muss sich zunehmend strategisch mit dem CIO und dem Vorstand abstimmen, damit effektive Investitionen in das Informationsmanagement und die Sicherheit realisiert werden.

> „Zusammen mit dem CIO ist dem CISO nun der Platz am Tisch mit dem Vorstand sicher – eine sehr positive Entwicklung."

Zac Warren
Chief Security Advisor, Tanium

Da CIOs und CISOs jedoch ein klares Bild erhalten möchten, um dem Vorstand ein Risikoprofil zu liefern, kann sie mangelnde Klarheit und Visibilität in ihrer IT behindern. Viele haben ausgedehnte IT-Landschaften mit Daten aus veralteten Infrastrukturen, lokalen, Cloud- und SaaS-Quellen übernommen. Dies kann CIOs und CISOs Schwierigkeiten bereiten, welche die Bedrohungslandschaft ansprechen oder eine deutliche Kapitalrendite demonstrieren möchten.

Zusammenführen von IT und Sicherheit

> „Wir versuchen, den alten Ansatz hinter uns zu lassen, bei dem für die Sicherheit verschiedene Schutzgeländer vorgesehen waren. So lässt sich zwar in acht Wochen eine Lösung entwickeln, dann heißt es aber drei bis sechs Monate auf die Sicherheitsgenehmigung warten, bevor die Lösung in Betrieb gehen kann."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

Viele der von uns Befragten wenden sich SecOps-Modellen zu, um das Informationsrisiko besser zu verwalten und die Visibilität und Nutzbarkeit von IT-Assets zu erhöhen. SecOps beinhaltet das Zusammenführen von Sicherheits- und IT-Betrieb. Indem die Sicherheit zum frühesten Zeitpunkt der Einführung eines neuen Produkts oder einer neuen Dienstleistung Beachtung findet, können Unternehmen später Sicherheitssperren beseitigen.

> „Das Designen ohne Einbindung des Sicherheitsteams direkt von Anfang an wäre kurzsichtig."

Barry Panayi
Chief Data & Insight Officer, John Lewis

Obwohl die Bemühungen zur Einführung und Erweiterung von SecOps positiv zu bewerten sind, werden viele Organisationen davon abgehalten, diese Strategie vollständig umzusetzen, da ihnen ein grundlegendes Verständnis der Tools, Prozesse und Technologien der jeweiligen Fachrichtungen fehlt. Ohne dieses Verständnis wird es schwierig, zwischen IT-Operations- und Sicherheitsteams die Effizienz, Innovationskraft und Effektivität zu erhöhen.

> „Die nachträgliche Wiederherstellung der Sicherheit ist in der Regel teurer und dauert länger."

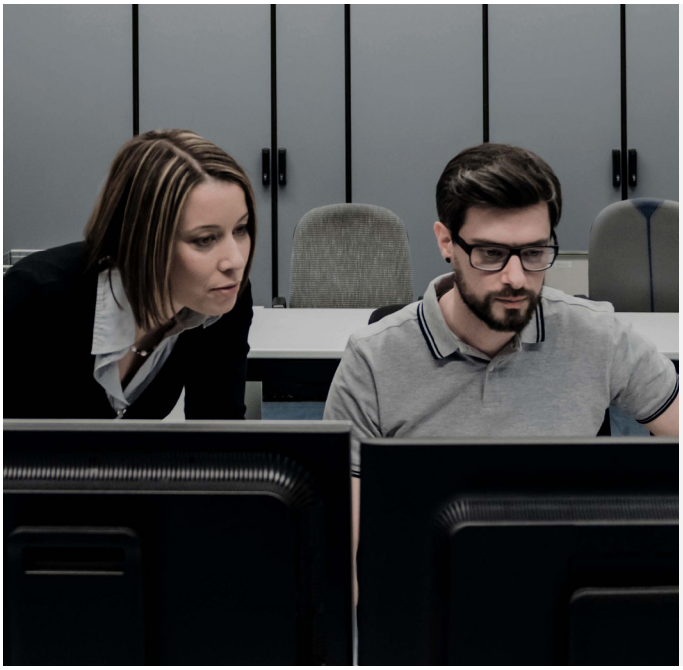
Que Tran
Regional Chief Information Officer, DP World

ABSCHNITT 2

Erwartung und Realität

Wenn Unternehmen von der Strategieplanung zur Implementierung übergehen, entstehen oft Erwartungslücken. Durch Interviews mit Informations- und Sicherheitsexperten in leitenden Positionen und Führungskräften aus verschiedenen Branchen haben wir die häufigsten Missverständnisse ermittelt, mit denen Führungskräfte auf ihrem Weg zur Zusammenführung und Innovation von IT-Betrieb und -Sicherheit konfrontiert waren. Im nächsten Abschnitt dieses Berichts legen wir die Erwartungen und die Realitäten so dar, wie sie von unseren Befragten beschrieben werden. Wir erläutern auch eine Reihe von Prinzipien, die Führungskräfte für ein besseres Management des Technologierisikos anwenden können.

„Vielen Unternehmen mangelt es an Visibilität, weil sie Architekturen und Umgebungen geerbt haben, die von den Vorgängern implementiert wurden. Sie trafen die besten Entscheidungen, die sie mit den damals verfügbaren Technologien, Prozessen und Mitarbeitern treffen konnten, aber jetzt erkennen wir, dass Sicherheitslücken bestehen“, sagt Zac Warren, Chief Security Advisor bei Tanium.



„Es gibt immer eine Lücke zwischen Bestrebung und Umsetzung. Das selbst ist ein anerkanntes Risiko, mit dem angemessen umzugehen ist.“

Chief Information and Security Officer
FTSE-100-Verpackungsunternehmen

Werkzeugvermehrung gegenüber Werkzeugoptimierung

Die Angriffsfläche ist durch die Erweiterung der Informationsökonomie und die Entwicklung immer ausgefeilterer Tech-Stacks exponentiell gewachsen. In diesen komplexen Umgebungen können Sicherheitsschwachstellen über Nacht erscheinen, erneut auftreten und sich vermehren. Da Firewall- und VPN-Lösungen allein unzureichend für den Schutz moderner Unternehmen sind, reagierten viele Organisationen damit, eine breite Palette neuer Cybersicherheitstools zu erwerben.

„Die Cybersicherheitsfähigkeiten sind eigentlich sehr gut. Die mangelnde Integration dieser Fähigkeiten ist jedoch genau der Punkt, an dem viele Unternehmen Lücken haben“, so Erik Gaston, VP Executive Engagement bei Tanium.

Obwohl damit die allgemeine Sicherheitslage in Bezug auf Risiken gereift ist, hat dies auch die Komplexität des ohnehin schon komplizierten IT-Ökosystems erhöht. Im Gegensatz könnte eine Zunahme der Tools zur Bekämpfung von Sicherheitsbedrohungen das Problem verschlimmern, wenn sich diese Tools nicht zusammen integrieren lassen. Daher hatten viele Organisationen Schwierigkeiten, ihre bestehenden Informations- und Sicherheitsökosysteme zu überwachen, zu verwalten und zu optimieren. Viele Organisationen haben doppelte Funktionen und nicht ausgelastete Anwendungen.

> „Ich verwende die bereits verfügbaren Werkzeuge nach besten Kräften, bevor ich die Lücken markiere."

Matthew Wilmot
Konzernleiter Enterprise IT & Information Security, Fraser Group

Für Unternehmen in dieser Position könnte die Konzentration auf die Tool-Optimierung, um das Beste aus den vorhandenen Werkzeugen herauszuholen, eine effektivere Strategie sein. Der Ausgangspunkt ist, eine klare Visibilität der verwendeten Assets zu erhalten und Möglichkeiten zur Optimierung und Integration dieser Tools zu identifizieren. Von diesem Standpunkt aus können Schwachstellen effektiver identifiziert und schneller behoben werden.

> „Finden Sie heraus, wie Sie die vorhandenen Tools vollständig nutzen können. Befreien Sie sich von all den Störgeräuschen, der zusätzlichen Software und den zusätzlichen Programmen, die Sie nicht nutzen, und überprüfen Sie dann, wo sich Ihre Lücken befinden. Für mich geht es dabei um die Vereinfachung."

Zac Warren
Chief Security Advisor, Tanium

Eine einheitliche Oberfläche im Vergleich zu einer mit mehreren Fenstern

> „Es ist unglaublich schwierig, eine einheitliche Oberfläche zu erreichen, aber dennoch möglich, das zu schaffen, was wir als „Oracles of Truth" bezeichnen."

Chief Information and Security Officer
FTSE-100-Verpackungsunternehmen

Eine einheitliche Oberfläche ist eine Managementstrategie, bei der die Daten über mehrere Quellen hinweg vereinheitlicht und in einer einzigen Ansicht präsentiert werden. Da Unternehmen zunehmend auf große Datenmengen setzen und von Daten abhängig sind, müssen Führungskräfte die Informationen konsolidieren, die aus verschiedenen Quellen im Unternehmen landen und davon gesendet werden. Es besteht die Erwartung, dass dieser Informationsfluss über ein einziges Dashboard verwaltet werden kann.

In unseren Interviews haben wir festgestellt, dass das Erreichen einer einheitlichen Oberfläche zur Konsolidierung der Informationen, die zur Beantwortung geschäftskritischer Fragen erforderlich sind, nicht immer effektiv ist. Viele Unternehmen haben zu viele Informationen und zu viele kritische Geschäftsfragen für eine schnelle Beantwortung, und dadurch wird eine einheitliche Oberfläche unrealistisch.

Stattdessen entwickeln Führungskräfte mehrere Fenster, um verschiedene wichtige Geschäftsprobleme zu lösen. Dazu werden verschiedene Tools integriert und kombiniert und Informationen in einem Fenster pro Geschäftsproblem zusammengefasst. Durch die Zusammenführung von Daten aus verschiedenen Bereichen der Geschäftsumgebung erhalten Führungskräfte ein realistisches Bild und einen ganzheitlichen Überblick über die Risiken, die mit geschäftskritischen Daten und Anwendungen verbunden sind.

> „Korrelieren Sie Ihre Arbeit direkt, um geschäftliche Probleme zu lösen. Fassen Sie dann Informationen auf Bedienfeldern zusammen, die sich direkt auf die Lösung dieser Geschäftsprobleme beziehen. Das ist transformativ. Die Transformation sollte einfach, nicht komplex sein."

Erik Gaston
VP Executive Engagement, Tanium

Compliance gegenüber einem risikobasierten Ansatz

> „Konzentrieren Sie sich auf Ihr Budget, da niemand ein Blankoscheckbuch für die Sicherheit hat und es nur begrenzt Personen mit dem entsprechenden Know-how gibt."

Zac Warren
Chief Security Advisor, Tanium

Organisationen können sich durch Compliance vor zahlreichen Risiken schützen.

Aber die Erwartung, dass die Einhaltung von Vorschriften mit Cyber-Widerstandsfähigkeit gleichzusetzen ist, trifft größtenteils nicht zu. Compliance und Vorschriften konzentrieren sich oft auf enge Bereiche und fördern einen taktischen Ansatz im Kontrollkästchenstil. Bei diesem können Schwachstellen bei der Sicherheit und andere Lücken außen vor bleiben.

> „Am wichtigsten sind unsere wirtschaftlich sensiblen Daten und unsere Kundendaten. Für den Rest haben wir ein anderes Sicherheitsniveau."

Barry Panayi
Chief Data & Insight Officer, John Lewis

Unter den Experten, mit denen wir gesprochen haben, wollten viele gerade die Lücke zwischen Compliance und einem risikobasierten Ansatz schließen, der Risiken vorbeugt und mindert.

Unsere Befragten nannten häufig die Notwendigkeit, Risikobewertungen durchzuführen, um ihre Ressourcen und ihr Know-how auf kritische Daten in Geschäftsbereichen mit hoher Priorität zu konzentrieren.

Sobald diese erstellt wurden, können Daten aus mehreren Quellen abgerufen, analysiert und gemäß einer Risikobewertung geschützt werden. Dies bietet einen ganzheitlichen Blick und die Möglichkeit, sich dynamisch auf geschäftskritische Daten und Anwendungen zu konzentrieren, je nach den Bedürfnissen des Unternehmens und der sich entwickelnden Bedrohungslandschaft. Dieser Ansatz schafft auch Effizienzen und hilft zu zeigen, wie Sicherheitsmaßnahmen den Umsatz steigern können.

> „Wir beschäftigen uns jetzt viel stärker mit abgestuften Kontrollen und „Rightsizing" für Betriebs- und Forschungsumgebungen."

James Tomkins
Chief Architect, Met Office

Damit Unternehmen jedoch einen risikobasierten Ansatz realistisch umsetzen können, müssen sie wissen, wo sich ihre geschäftskritischen Daten und Anwendungen befinden. Sie müssen über Visibilität in ihren IT-Ökosystemen und organisatorischen Prozessen verfügen, um die Ausbreitung von Tools und Informationen einzuschränken.

Komplexität gegenüber Einfachheit

> „Es wurden erhebliche Anstrengungen unternommen, um die Richtlinienlandschaft zu vereinfachen, da Sicherheit oft als zu komplex angesehen wurde."

James Tomkins
Chief Architect, Met Office

Viele Unternehmen akzeptieren, dass zusätzliche Komplexität auf dem Weg von der lokalen Infrastruktur zur Public Cloud unvermeidlich ist. Da die digitale Transformation jedoch nicht abzuschwächen scheint, erkennen Unternehmen, dass sich unkontrollierte Komplexitätsstufen nicht bewältigen lassen.

Mit dem Tempo und Ausmaß der digitalen Transformation erkennen Unternehmen, dass sie durch eine zu große Komplexität davon abgehalten werden, Innovationen zu entwickeln und Schwachstellen zu verstehen. Um dem entgegenzuwirken, hatten viele unserer Befragten Programme zur Vereinfachung der IT-Ökosysteme gestartet.

Während Unternehmen risikobasierte Ansätze für das Informations- und Sicherheitsmanagement implementieren möchten, wird die Fähigkeit als wichtiger Ausgangspunkt immer deutlicher, Daten, Vermögenswerte und Informationen kohärent zu katalogisieren und im gesamten Unternehmen nachzuverfolgen.

> „Wenn Sie diese grundlegende Visibilität nicht haben, können Sie Ihre Schwachstellen nicht verstehen. Und das ist für mich die größte Lücke, die bei den meisten Unternehmen zwischen Erwartungen und Realität besteht."

Zac Warren
Chief Security Advisor, Tanium

„Beobachtbarkeit im Unternehmen mit Blick auf die Ereignisse hat für uns eine Priorität. Auf der Ebene sinnvoller Geschäftstätigkeit wollen wir sehen, was im Unternehmensalltag passiert", so James Tomkins, Chief Architect im Met Office

> **„Wir vereinfachen unseren Gesamtbestand. Aus Sicherheits- und Datensicht gestaltet es sich viel einfacher, einen einzigen, skalierbaren Ressourcensatz zu verwalten, anstatt viele verschiedene Systeme zu verwenden. Diese Vereinfachung reduziert die Komplexität tatsächlich und verringert die Wahrscheinlichkeit unterschiedlicher Lücken."**

Paul Curtis
Chief Technology Officer, Easyjet Holiday

ABSCHNITT DREI

Leitprinzipien für ein besseres Informationsrisikomanagement

Während Unternehmen versuchen,alte Erwartungen zu überwinden und realistische Strategien für ein effektives Informationsrisikomanagement umzusetzen, können einige Leitprinzipien hilfreich sein. Im nächsten Abschnitt fassen wir die am häufigsten zitierten Ratschläge der für diesen Bericht befragten führenden Informations-, Daten- und Technologieleiter zusammen.

IT-Ordnung

> „Die IT-Ordnung ist wirklich das grundlegende Element. Sobald Sie diese geschaffen haben, können Sie stärker zum Risikomanagement, Kulturwandel und letztendlich zur Cyber-Resilienz übergehen."

Chief Information and Security Officer
FTSE-100-Verpackungsunternehmen

Unternehmen, die ihre Cyber-Resilienz sinnvoll weiterentwickeln möchten, müssen schnellen oder Hype-basierten Lösungen widerstehen. Oftmals können mehr Werkzeuge, die ein Patentrezept versprechen, zum Problem beitragen, indem sie im Ökosystem für zusätzliche Komplexität sorgen.

„Eine Kernkomponente der Sicherheit ist eine gute Ordnung. Der Elefant im Raum in Bezug auf den Cyber-Space ist die mangelnde IT-Ordnung, was bedeutet, dass alle Assets sichtbar sind und die Schwachstellen bewertet werden können. Es besteht leider eine große Lücke", sagt Zac Warren, Chief Security Advisor bei Tanium.

Für das Ziel der Cyber-Resilienz müssen sich Unternehmen für die IT-Ordnung doppelt so stark anstrengen Um die nötige Klarheit für strategische Fortschritte zu erlangen, ist ein genauer Überblick über den gesamten IT-Bereich eines Unternehmens erforderlich. Es ist wichtig, Cloud-, On-Premises- und SaaS-Assets effektiv zu organisieren, bevor genaue Daten zum Risiko gewonnen werden können.

Dazu müssen IT-Assets aufgeräumt und ordentlich gehalten werden, indem die Bestände aktuell und vollständig sind. Die Bedeutung dieser grundlegenden Schritte kann nicht überbewertet werden. Durch die Minimierung der allgemeinen Bedenken in Bezug auf den Zustand und die Ordnung des IT-Bestands lassen sich die vorhandenen Risiken und Schwachstellen einfacher bestimmen.

Automation

> „Wir untersuchen derzeit, wie wir Standardbestände verstärkt automatisieren können."

Barry Panayi
Chief Data & Insight Officer, John Lewis

Obwohl die Implementierung und Aufrechterhaltung der IT-Ordnung unerlässlich sind, kann sie sehr zeitaufwändig sein. Der manuelle Aufwand bei der Aufnahme von IT-, Anwendungs- und Datenbeständen kann auch ineffizient und mit menschlichen Fehlern behaftet sein. Selbst für die erfahrensten Sicherheitsexperten behindert das Sammeln von Daten aus einer Vielzahl von spezialisierten Tools mit begrenzter Interoperabilität die Fähigkeit, zeitnahe und kontextreiche Informationen zu sammeln.

Durch die Automatisierung von Prozessen in Bezug auf die IT-Ordnung und Sicherheitswartung kann ein Unternehmen seine Personalressourcen freisetzen, damit sich diese auf strategische Projekte für das Erreichen der Geschäftsziele konzentrieren können. Das unterstützt dabei, sicherheitsbezogene Aktivitäten von einer Kostenstelle in einen Umsatzgenerator zu verwandeln.

> „Wir möchten, dass unsere Entwickler uneingeschränkt arbeiten und wissen, dass ihre gesamte Arbeit automatisierte Qualitätsprozesse und -verfahren durchläuft. Wir heben mit dem Build-Prozess alles hervor, was unsere Sicherheitsstandards nicht erfüllt."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

„Ein wesentlicher Bestandteil der erfolgreichen Umsetzung ist die Betrachtung der Mechanismen, die wir für die Automatisierung nutzen können. Denn das Verlassen auf große manuelle Anstrengungen bringt keinen Geschäftswert. Wir müssen also viel davon mit Automatisierung aufbauen, um diese Beobachtbarkeit zu erreichen. Ansonsten gestaltet es sich sehr schwierig, weil sich die Dinge so schnell bewegen“, so James Tomkins, Chief Architect, im Met Office

> „Die reine Erweiterung unserer Sicherheitsteams ist keine langfristige Lösung. Im Moment können wir Bedrohungen nicht schnell genug erkennen oder mit Lichtgeschwindigkeit verteidigen. Automatisierung, Integration und Interoperabilität sind unsere Mittel, um die langfristigen Sicherheitsziele des Unternehmens nachweislich zu realisieren und zu erreichen.“

Chief Information und Security Officer
Regierungsbehörde

Wenn ein Endpunkt gefährdet sein könnte, ermöglicht die Automatisierung Incident-Teams auch beschleunigte Reaktionszeiten, indem ein schnelles und genaues Bild der Umgebung in Minuten statt Tagen bereitgestellt wird.

> „Die Automatisierung unserer täglichen Arbeit hilft uns dabei, ein Unternehmen zu festigen und zu schützen.“

Ketan Patel
Group Chief Information Officer, WH Smith

Zusammenarbeit

Neben der Verbesserung von Prozessen und Technologien ist die Unternehmenskultur eine Schlüsselkomponente für ein besseres Management des Informationsrisikos. Für den Erfolg ist die Fähigkeit von zentraler Bedeutung, die Sicherheit von einem Silo zu einem integralen Bestandteil des Unternehmens zu verlagern.

Das beginnt an der Spitze der Organisation, mit einer stärkeren Zusammenarbeit zwischen CIOs, CISOs und dem Vorstand. Es erweitert sich auf Arbeitsweisen, indem dafür gesorgt wird, dass Sicherheitsexperten nicht nur Teil der gesamten IT-Agenda, sondern auch der gesamten Geschäftsagenda sind.

> „SecOps-Modelle sind wichtig, weil sie eine andere Art der Denkweise zeigen, wie Sicherheit zum Gesamtbetrieb des Unternehmens passt."

Que Tran
Regional Chief Information Officer, DP World

Durch die Einführung von SecOps-Modellen soll dieses Ziel erreicht werden, indem eine stärkere Zusammenarbeit zwischen Sicherheitsteams und IT-Betrieb gefördert wird. Damit SecOps-Modelle erfolgreich von der Strategie zur Implementierung übergehen können, müssen Unternehmen die Tools tiefgreifend verstehen, die traditionell jede Disziplin untermauert haben, und Wege für deren sinnvolle Integration finden, sodass isolierte Teams wirkungsvoll zusammenarbeiten können.

> „Es ist kurzsichtig, zu versuchen, Innovationen voranzutreiben, ohne das Sicherheitsteam von Anfang an einzubeziehen."

Barry Panayi
Chief Data & Insight Officer, John Lewis

Durch die Förderung einer stärkeren Zusammenarbeit zwischen Sicherheits- und IT-Betriebsteams können Unternehmen die Visibilität sowohl der Sicherheitsrisiken als auch der IT-Prioritäten erhöhen, um das Geschäftswachstum und die Belastbarkeit gleichermaßen zu unterstützen. Durch die Integration und Automatisierung von Sicherheits- und IT-Operationen können weitere Vorteile in Form von Agilität und Effizienz erreicht werden.

> „Die Zusammenarbeit mit Ihrem Team und der Unternehmensleitung zahlt sich wirklich aus. Durch die Zusammenarbeit auf diesem Weg gestaltet sich die Bereitstellung viel termingerechter und kostengünstiger."

Leitender Manager
CERT, Vodafone

> „Sicherheit wurde als ein Thema angesehen, mit dem sich die Mitarbeiter nicht einfach beschäftigen konnten und deshalb nicht weiter verfolgt wurde. Infolgedessen fiel es in die Hände weniger Spezialisten. Um dem entgegenzuwirken, haben wir breit gefächerte Kommunikations- und Fortbildungsprogramme im gesamten Unternehmen eingeführt, damit alle für die Sicherheit verantwortlich sind."

James Tomkins
Chief Architect, Met Office

FAZIT

Das Ganze ist größer als die Summe seiner Teile

> „Viele Unternehmen versuchen, komplexe Bedrohungen der Cybersicherheit mit linearen Lösungen zu bekämpfen. Aber die Risikolandschaft stellt sich nicht als eine Reihe linearer Probleme dar. Für ein dynamisches Problem wie die Sicherheit müssen Unternehmen mehr auf integrierte Plattformen schauen, die ein vollständiges Bild vermitteln."

Erik Gaston
VP Executive Engagement, Tanium

Während sich das Informations- und Sicherheitsmanagement weiterentwickelt und ausreift, wird den Erwartungen der Fachleute in diesem Bereich weiterhin getrotzt. Aber indem sie sich auf Leitprinzipien stützen, können Unternehmen risikobasierte Ansätze und kollaborative Modelle einführen, die Sicherheit zu einem integralen Bestandteil der Geschäftstätigkeit machen und somit die Lücke zwischen Erwartungen und Realität schließen.

Dynamische, sich ständig ändernde Probleme wie die Sicherheit benötigen eine Lösung, die größer als die Summe ihrer Teile ist. Keine einzige Lösung, kein Team oder keine Methodik wird eine schnelle Lösung bieten, da Sie zur Lösung dynamischer Probleme integrierte Lösungen benötigen. Um einen strategischen und präventiven Ansatz zu erreichen, müssen sich Unternehmen darauf konzentrieren, die vorhandenen Tools zu optimieren und zu integrieren und sie zu konsolidieren, damit eine bessere Sicht auf die Bedrohungslandschaft aus der Vogelperspektive möglich ist.

> „Durch das Erreichen von Visibilität gewinnt ein Unternehmen mehr, als man vermuten könnte. Das reduziert nicht nur das Risiko massiv, was ein enormer Faktor ist, sondern beschleunigt auch die Innovationen, weil die Datenbestände im Unternehmen sichtbar werden."

Jon Roughley
Director of Data Strategy and Innovation, Experian

CHIEF DISRUPTOR

Chief Disruptor ist die Community für Führungskräfte in den Bereichen Wirtschaft und Technologie.

Disruptive Führungskräfte glauben, wie wir, dass Disruption ein Katalysator für Chancen ist, und unser Name, Chief Disruptor, verkörpert und feiert diese Denkweise stolz. Seit 2005 hat unsere Mitgliedergemeinschaft für Führungskräfte aus den Bereichen Wirtschaft und Technologie Innovatoren, Change Maker und disruptive Denker für den Austausch von Fachwissen, Strategien und umsetzbaren Erkenntnissen zusammengebracht.

Unser Ziel war es schon immer, den Hype zu durchbrechen und unseren Mitgliedern die Nutzung dieser disruptiven Trends und Technologien über unsere durch Mitglieder geführten Insight-Berichte, Inhalte und Community-Aktivitäten zu ermöglichen.

Angesichts der anhaltenden geopolitischen Unruhen und der düsteren Realität der Rezession am Horizont benötigen Unternehmen heute mehr denn je eine agile, zielgerichtete Führung, welche die Chancen erfasst und die Bedrohungen von Disruption proaktiv handhabt. Es wird nicht einfach sein, aber wir sind hier, um Ihnen zu helfen. Connect. Learn. Disrupt.
chiefdisruptor.com

TANIUM

Als branchenweit einziger Anbieter von konvergentem Endpunktmanagement (Converged Endpoint Management, XEM) führt Tanium den Paradigmenwechsel bei herkömmlichen Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an.

Nur Tanium vereint Teams und Arbeitsabläufe, um jeden Endpunkt vor Cyberbedrohungen zu schützen, indem es IT, Compliance, Security und Risk in eine einzige Plattform integriert, die umfassende Visibilität über alle Geräte hinweg, einen einheitlichen Satz von Kontrollen und eine gemeinsame Taxonomie für einen einzigen gemeinsamen Zweck bietet: den Schutz kritischer Informationen und Infrastruktur. Tanium wurde sieben Jahre in Folge in die Forbes Cloud 100-Liste aufgenommen und steht auf der FORTUNE-Liste der „Best Workplaces in Technology". Tatsächlich vertrauen mehr als die Hälfte der Fortune-100-Unternehmen und die US-Streitkräfte auf Tanium, um Einzelpersonen zu schützen, Daten zu verteidigen, Systeme zu sichern und jeden Endpunkt, jedes Team und jeden Workflow überall zu identifizieren und zu steuern. Das ist die Power of Certainty.

Besuchen Sie uns unter www.tanium.com und folgen Sie uns auf LinkedIn und Twitter.