TANIUM

Was Sie nicht wissen, kann Ihnen schaden: Expertentipps zur Risikomessung

Branchenexperten bieten Informationen und Empfehlungen zur Messung von Risiken in den schnelllebigen und stark verteilten Unternehmensumgebungen von heute.

TANIUM

Was Sie nicht wissen, kann Ihnen schaden: Expertentipps zur Risikomessung

Branchenexperten bieten Informationen und Empfehlungen zur Messung von Risiken in den schnelllebigen und stark verteilten Unternehmensumgebungen von heute.

Inhalt

EINFÜHRUNG

Expertentipps zur Risikomessung

Risikomanagement beginnt mit der Messung von Risiken.

Aber wie lassen sich Risiken sinnvoll messen? Sollten Sie sämtliche Softwareschwachstellen um Unternehmen ermitteln? Eine Liste aller Endpunktgeräte erstellen, die Softwarepatches erfordern? Sollten Sie die Zahlen zur Betriebszeit Ihrer wichtigsten Unternehmensanwendungen in Berichten erfassen?

Wenn Sie für die Risikomessung zuständig sind, sollten Sie sich auf die Bereiche konzentrieren, die für Ihr Publikum am relevantesten sind. Und für die wichtigsten Entscheidungen beim Thema Risiko besteht Ihr Publikum aus der Führungsetage und dem Vorstand Ihres Unternehmens.

In diesem E-Book teilen drei Experten aus der IT-Branche ihre Kenntnisse zu den praktischsten, umfassendsten und umsetzbarsten Methoden der Risikomessung.

Am Ende des E-Books finden Sie eine Checkliste mit einer Zusammenfassung der bereitgestellten Tipps. *Los gehts.*

KAPITEL 1:

Messen, was wichtig ist: Risikomessung an Unternehmenszielen ausrichten

Die meisten IT-Sicherheitsexperten sind der Ansicht, dass Risiken allgegenwärtig sind. Nicht gepatchte Endpunkte, neue Malware-Varianten, Phishing-Angriffe, Schatten-IT in der Cloud, im Zug vergessene Laptops – das Risiko ist überall. Da viele technische Details zum Risiko beitragen, fragt sich Ihr Risikoteam möglicherweise, wie es die wichtige Aufgabe der Risikomessung in Ihrem Unternehmen am besten angehen sollte.

Risikomessungen werden natürlich nicht zum Spaß durchgeführt. Mit Risikobewertungen sollen Entscheidungsträgern wichtige Informationen zur Verfügung gestellt werden. Daher lautet die entscheidende Frage: Wie messen Sie Risiken so, dass die Unternehmensleitung – das Führungsteam und der Vorstand – auf der Basis der Ergebnisse die richtigen Entscheidungen treffen kann, um die Risiken zu reduzieren?

Messen von Risiken, die Ihrer Unternehmensleitung wichtig sind

Um diese Frage zu beantworten, müssen wir ganz am Anfang beginnen. Das Führungsteam und der Vorstand sind für die strategische Ausrichtung Ihres Unternehmens verantwortlich. Ein Teil ihrer Aufgabe besteht darin, sicherzustellen, dass Entscheidungen und Investitionen in der gesamten Organisation den allgemeinen strategischen Zielen des Unternehmens zugutekommen.

Unabhängig davon, in welcher Branche Ihr Unternehmen tätig ist, beinhalten diese Ziele mit großer Sicherheit Folgendes:

- Geschäftskontinuität
- Vertraulichkeit, Integrität und Verfügbarkeit von Daten
- Einhaltung gesetzlicher Bestimmungen

Lassen Sie uns einzeln auf diese Aspekte eingehen.

Messung des Risikos im Zusammenhang mit der Geschäftskontinuität

Geschäftskontinuität bedeutet, den Betrieb, die Produktivität der Mitarbeiter sowie Produktions- und Versandvorgänge aufrechtzuerhalten und allgemein sicherzustellen, dass alle Abläufe jederzeit unterbrechungsfrei ausgeführt werden können.

Die Notfallwiederherstellung fällt in diese Kategorie, ebenso wie der Schutz geschäftskritischer Dienste vor Cyberbedrohungen.

Messung des Risikos im Zusammenhang mit der Vertraulichkeit, Integrität und Verfügbarkeit von Daten

Die Bedeutung von Daten ist branchenübergreifend bekannt – es ist das „neue Öl" der digitalen Wirtschaft. Entsprechend wichtig ist der Schutz von vertraulichen Daten.

Die Herausforderungen für die Sicherung dieser Daten sind gewachsen. In einer Zeit, in der Mitarbeiter zunehmend im Homeoffice arbeiten, werden sensible Daten beispielsweise von mehr Standorten als je zuvor abgerufen. Und die Mitarbeiter setzen zunehmend private Geräte ein, statt von der IT-Abteilung getestete und bereitgestellte Laptops und Desktop-Computer.

Letztlich spielt es jedoch keine Rolle, wo oder wie Mitarbeiter auf Daten zugreifen – Unternehmen müssen die Vertraulichkeit, die Integrität und die Verfügbarkeit aller Daten gewährleisten.

Messung des Risikos im Zusammenhang mit der Einhaltung gesetzlicher Bestimmungen

Beim Thema Datenschutz denken wir sofort an Vorschriften wie die DSGVO und HIPAA, die den Schutz personenbezogener Daten vorschreiben.

Aber es gibt auch Vorschriften für andere Bereiche, von der Rechnungslegung bis zur Rassendiskriminierung, die Unternehmen unbedingt einhalten sollten. Verstöße gegen diese Vorschriften können zu saftigen Geldstrafen, Vertragsauflösungen und negativer (und oft langfristiger) Publicity führen.

Um Risiken effektiv zu messen, müssen Sie wissen, welche Vorschriften für Ihr Unternehmen von Bedeutung sind. Dann erfassen Sie IT-Assets und -Prozesse, mit deren Hilfe Sie bestimmen können, ob Ihr Unternehmen diese Vorschriften einhält.

Risiko in Zusammenhang mit strategischen Zielen bringen

Die Aufgabe von Führungsteam und Vorstand besteht darin, dafür zu sorgen, dass das Unternehmen zentrale Ziele in den Bereichen Geschäftskontinuität, Datenschutz und Einhaltung gesetzlicher Bestimmungen erreicht. Natürlich spielen auch andere Ziele eine Rolle, etwa das Erreichen eines bestimmten prozentualen Wachstums oder die Etablierung einer bestimmten Unternehmenskultur.

Wenn Sie die Aufmerksamkeit dieser Führungskräfte gewinnen möchten, sollten Sie die Risikomessung in Bezug zu den auf Vorstandsebene erklärten Unternehmenszielen setzen. Anders ausgedrückt: Identifizieren und wägen Sie die verschiedenen technischen, gesetzlichen und anderweitigen Risiken Ihres Unternehmens ab und stellen Sie sie den allgemeinen strategischen Zielen Ihres Unternehmens gegenüber.

Sie werden feststellen, dass Sie Ihre Arbeit auf diese Weise besser ausrichten können und dass Sie von Seiten der Führungskräfte, die die Weichen für die Zukunft Ihres Unternehmens stellen, auf größeres Verständnis für Ihre Arbeit stoßen und mehr Anerkennung erhalten.

KAPITEL 2:

Risikomessung durch Identifizierung von Wertschöpfungsketten

In diesem Kapitel gehen wir ausführlicher auf die Messung von Risiken für Unternehmensziele ein. Ich bespreche die Bedeutung von gewichteten Skalen für verschiedene Risiken und für die Ziele selbst.

Identifizierung von Risiken im Zusammenhang mit strategischen Zielen

Die Aufgabe der Risikomessung beginnt mit der Identifizierung der strategischen Ziele Ihres Unternehmens und der anschließenden Untersuchung der Mitarbeiter, Prozesse und Technologien, die die Verfolgung dieser Ziele durch Ihr Unternehmen unterstützen.

Betrachten Sie es als Lieferkettenanalyse. Sie verfolgen den Fluss von Daten, Mitarbeitern und Betriebsabläufen von einem übergeordneten Ziel bis zu spezifischen IT-Systemen und -Prozessen, die dem Unternehmen dabei helfen, dieses Ziel zu erreichen. Diese Systeme und Prozesse agieren als eine Art Lieferkette für die jeweiligen Ziele.

Um das Risiko zu messen, identifizieren Sie Abhängigkeiten in der Lieferkette und verfolgen sie so weit nach, wie dies für die Ziele und die Leistung Ihres Unternehmens sinnvoll ist. Damit Sie Risiken innerhalb der Lieferkette vergleichen können, müssen Sie allen Elementen einer Lieferkette eine Punktzahl zuweisen.

Aufbau einer gewichteten Risikoskala

Selbst die strategischen Ziele selbst müssen verglichen und gewichtet werden. In der Regel werden unterschiedlichen strategischen Zielen eines Unternehmens auch unterschiedliche Prioritäten eingeräumt.

Sobald Sie diese Ziele identifiziert haben, weisen Sie ihnen Punktzahlen auf einer Skala zu, z. B. von 1 bis 10. Basierend auf Gesprächen mit dem Führungsteam könnten Sie dem kontinuierlichen jährlichen Umsatzwachstum von mindestens 10 % beispielsweise die Punktzahl 10 zuweisen und die Einhaltung gesetzlicher Bestimmungen mit 7 Punkten gewichten.

Als Nächstes ermitteln Sie die Mitarbeiter, Prozesse und Technologien, die an der Erreichung der individuellen strategischen Ziele beteiligt sind, und stufen die Bedeutung jedes dieser beteiligten Faktoren ein.

Für eine detailliertere Abstufung könnten Sie die Wahrscheinlichkeit schätzen, dass ein bestimmter Fehler oder Ausfall auftritt. Angenommen, Ihr Unternehmen betreibt einen Webserver, über den eine geschäftskritische App ausgeführt wird. Die Wahrscheinlichkeit, dass die Leistung des Servers in Spitzenzugriffszeiten untragbar schlecht ist, ist vermutlich größer als die Wahrscheinlichkeit, dass der gleiche Server einem Stromausfall erliegt, der sowohl das Haupt- als auch das Notfallstromsystem lahmlegt.

Durch die Multiplikation einer Punktzahl für die strategische Bedeutung des Servers (z. B. 7 von 10) mit der Wahrscheinlichkeit eines bestimmten Risikos (z. B. 50 % oder 0,5) können Sie dringliche Risiken identifizieren und einstufen.

Angenommen, der Server mit der schlechten Performance hat eine Wahrscheinlichkeit von 40 % und der Server, der bei einem katastrophalen Stromausfall zum Erliegen kommt, hat eine Wahrscheinlichkeit von 2 %. Wenn die Bedeutung des Servers bei 7 von 10 liegt, würde der Risikoscore für das Szenario mit der schlechten Performance 7 mal 40 betragen (was 2,8 ergibt). Der Risikoscore für das Stromausfallszenario würde 7 mal 0,02 betragen (was 0,14 ergibt). Das Szenario mit der schlechten Performance, das einen höheren Risikoscore aufweist, stellt offensichtlich das dringlichere Risiko dar.

Die Bedeutung der Zusammenarbeit bei der Risikomessung

Diese Art der Risikobewertung erfordert die Erfassung detaillierter Informationen über Menschen, Prozesse und Technologien im gesamten Unternehmen. Für das Zusammentragen dieser Daten ist die IT-Abteilung auf Hilfe angewiesen.

Am besten bitten Sie jede Abteilung, deren Prozesse und Technologien Sie bewerten, um Unterstützung. Wenn Sie zum Beispiel die Risiken im Zusammenhang mit den Anwendungen der Personalabteilung nachvollziehen wollen, sprechen Sie mit HR-Mitarbeitern. Sie können vielleicht etwas zur Bedeutung einer Anwendung sagen, die das IT-Betriebsteam übersehen hat.

Wenn Sie mit Personen außerhalb der IT-Abteilung sprechen, sollten Sie nach Möglichkeit auf technische Fachbegriffe verzichten. Außerdem sollten Sie Ihre Gesprächspartner immer erst nach ihren Lösungsvorschlägen für ein Problem fragen, bevor Sie Ihre eigenen Lösungen präsentieren. Andernfalls entgehen Ihnen möglicherweise kreative Alternativen. Darüber hinaus sträuben sich Menschen oft, eine neue Richtlinie zu befolgen, die direkte Auswirkungen für sie hat, wenn ihre eigenen Ideen nicht einmal in Betracht gezogen wurden.

Risikomanagement ist ein Problem, das nicht nur die IT betrifft, sondern das gesamte Unternehmen.

Wenn Mitarbeiter aus anderen Abteilungen merken, dass sie Ihnen vertrauen können und dass Sie sich aufrichtig dafür interessieren, was sie zu sagen haben, werden sie freier mit Ihnen kommunizieren. Sie fühlen sich dann auch mit größerer Wahrscheinlichkeit für die Risikomanagementlösungen verantwortlich, die Sie zusammen ausgearbeitet haben.

Diese andauernde Zusammenarbeit ist einer der Vorteile eines „Lieferketten-Ansatzes“ für die Risikomessung. So kommen Sie an die Details, die Sie zur genaueren Messung von Risiken benötigen. Gleichzeitig klären Sie Stakeholder in der gesamten Organisation über die Bedeutung von Risikomessung und Risikominderung auf. Und Sie erhalten die Möglichkeit, mit diesen Stakeholdern Lösungen zur Minderung der Risiken zu entwickeln, die Sie gemeinsam identifiziert haben.

KAPITEL 3:

Moderne Risikobewertung im verteilten Unternehmen

Früher war die Risikomessung ein besonderes Ereignis, für dessen Durchführung Berater herangezogen wurden. Dank Echtzeitdaten und Automatisierung messen Unternehmen Risiken jetzt genauer, kontinuierlicher und effektiver.

Der plötzliche Wechsel zum Homeoffice-Modell hat letztes Jahr viele Änderungen für die Unternehmens-IT bewirkt, unter anderem im Hinblick auf die Art und Weise, wie IT-Teams Risikobewertungen durchführen.

In diesem Kapitel untersuchen wir, wie Risikobewertungen im Unternehmen traditionell durchgeführt wurden. Dann betrachten wir, wie sich das Prozedere seit Beginn der Pandemie bei vielen Unternehmen geändert hat, und empfehlen Best Practices für die Modernisierung der Risikobewertung zur Anpassung an das stark verteilte Unternehmen von heute.

Wie sich Risiken und Risikobewertungen in der Pandemie verändert haben

Traditionell wurden Risikobewertungen in vielen Organisationen nur einmal im Jahr durchgeführt. Dazu erstellten Risikobewertungsteams detaillierte Berichte, in denen versucht wurde, alle Risiken einer Organisation in Bereichen wie IT-Sicherheit, Notfallwiederherstellung und Compliance zusammenzufassen.

Um Informationen für ihre Berichte zusammenzutragen, besuchten die Teams Rechenzentren und verteilten Fragebögen. Selbst wenn die Besuchstermine gewissenhaft durchgeführt wurden und die Fragebögen gründlich waren, spiegelten die Bewertungen immer nur ein zeitpunktspezifisches Risiko wider.

Wenn das Team gerade ein Rechenzentrum verlassen hatte und in diesem Moment ein neues Softwareupgrade plötzlich die Rechnungslegung des Unternehmens gefährdete, war von diesem erhöhten Risiko im Bewertungsbericht nichts zu finden.

Während der Pandemie wurden vielen Organisationen die Schwächen dieser Art der Risikobewertung aufgezeigt. Persönliche Besuche wurden durch E-Mail-Befragungen ersetzt. Die Stakeholder füllten die Fragebögen pflichtbewusst aus, auch wenn niemand mit Sicherheit sagen konnte, welche Geräte die Mitarbeiter im Homeoffice verwendeten oder welche Software auf diesen Geräten ausgeführt wurde.

Gibt es eine bessere Möglichkeit, Risikobewertungen durchzuführen? Ich habe mich in meiner Karriere ausgiebig mit der praktischen Durchführung von Risikobewertungen auseinandergesetzt und würde diese Frage bejahen.

Risikobewertung im Zeitalter von Cloud-Computing und Homeoffice

Das Erste, was sich an Risikobewertungen ändern muss, ist ihre Zeitlosigkeit. Wenn Berichte auf Daten basieren, die einmal im Jahr erfasst werden, sind sie zwangsläufig die meiste Zeit ungenau.

Die Geschäftswelt ist heute schnelllebiger als je zuvor. Daten, Geräte, Software, Geschäftsbeziehungen – all diese Dinge unterliegen einem ständigen Wandel. Risikobewertungen müssen diesen Wandel widerspiegeln.

Glücklicherweise verfügen IT-Abteilungen über neue Tools, die dazu beitragen können, die Genauigkeit von Risikobewertungen zu verbessern. Über die Endpunktüberwachung in Echtzeit können beispielsweise Berichte zum Standort, zur IT-Integrität und zu den Aktivitäten beliebiger Endpunkte ausgegeben werden, was auch im Homeoffice genutzte Geräte beinhaltet. Diese Überwachung funktioniert über Standard-Internetverbindungen, ohne VPN.

Mit diesen modernen Tools können IT-Organisationen heute immer umfassendere, aktuellere und präzisere Endpunktdaten sammeln, insbesondere im Vergleich zu Zeiten, in denen sich die meisten Endpunkte noch in internen Netzwerken befanden und nur sporadisch von herkömmlichen Endpunktmanagement-Tools überwacht wurden.

Der zweite Schritt in Richtung Modernisierung besteht darin, Risiken im Zeitverlauf zu messen. Führungskräfte wollen wissen, ob die eingeführten Maßnahmen zur Risikominderung funktionieren. Die Risikoteams sollten die Metriken nachverfolgen, an denen abgelesen werden kann, ob das Unternehmen seine Ziele für das Risikomanagement erreicht oder nicht.

Im dritten Schritt sollten datengestützte Gespräche zum Thema Risiken mit der Geschäftsleitung geführt werden. Hierbei zahlt es sich aus, über aktuellere und umfassendere Daten zu verfügen. Mit verbesserten Einblicken in Endpunkte und andere IT-Assets können Sie eine sinnvollere Diskussion darüber führen, welche Investitionen funktionieren und welche nicht.

Vier wichtige Elemente des Risikomanagements

Hier sind vier Schritte für das Risikomanagement in einem modernen Unternehmen unter Berücksichtigung der individuellen strategischen Ziele Ihrer Organisation.

Datensammlung

Dies beinhaltet die Sammlung aller Daten, die zur Messung der Risiken im Zusammenhang mit den strategischen Zielen Ihrer Organisation erforderlich sind. Zu diesen Daten gehören selbstverständlich Endpunktdaten sowie Umgebungs- und Benutzerdaten.

Analyse

Sobald Sie die Daten gesammelt haben, sollten Sie sie analysieren, vorzugsweise automatisiert. Die Analyse ist wahrscheinlich zeitaufwendiger und fehleranfälliger, wenn sie von mehreren Excel-Tabellen und Ausdrucken abhängt. Wenn Sie Scorecards zur Bewertung von Risiken erstellt haben, können Sie die Tabellarisierung automatisieren und die Analyse zu einem kontinuierlichen Prozess machen, anstatt einmal im Jahr eine Momentaufnahme zu erstellen.

Berichterstellung

In diesem Schritt werden Risikometriken und Analysen in Berichten für die Geschäftsleitung zusammengefasst. Diese Berichte dienen als Grundlage für Diskussionen über Risiken, Prioritäten, Investitionsentscheidungen und mehr in Ihrer Organisation. Sie sollten in diesen Berichten einen Bezug zwischen Risikoanalyse und den strategischen Zielen herstellen, mit denen sich Ihr Führungsteam und der Vorstand kontinuierlich auseinandersetzen.

Behebung

Es gibt zwei Arten von Risikobehebung. Zum einen gibt es Maßnahmen, die täglich von Mitarbeitern in den Bereichen IT-Sicherheit und -Betrieb ergriffen werden, um auf Bedrohungen wie Malware zu reagieren. Diese Maßnahmen erfordern keine Genehmigung seitens der Geschäftsführung. Zum anderen gibt es Maßnahmen, die von den Bereichsleitern aus IT- und Geschäftsabteilungen als Reaktion auf Berichte für die Geschäftsleitung ergriffen werden, die in den ersten drei Schritten dieses Prozesses erstellt wurden. Unternehmen sollten beide Formen der Risikobehebung anwenden.

Im Laufe des vergangenen Jahres haben sich viele Unternehmen als agilere, geografisch verteiltere Organisationen neu erfunden.

Jetzt haben sie die Möglichkeit, auch ihre Risikobewertungsprozesse neu zu gestalten. Mit Echtzeitdaten und Automatisierung können Unternehmen Risiken reduzieren und gleichzeitig die Sicherheit ihrer Remote-Mitarbeiter verbessern.

KAPITEL 4:

Die Bedeutung der Risikobewertung als kontinuierlicher Prozess

Das Messen von Risiken ist komplizierte Arbeit. Neue Technologien können allerdings dazu beitragen, die Risikobewertung zu automatisieren.

Risiken stellen für jede Organisation eine Bedrohung dar, aber die Bewertung dieser Risiken ist heute schwieriger als je zuvor. In diesem Kapitel erklären wir, was die Risikobewertung so schwierig macht und wie ein Top-Down-Ansatz bei der Risikomessung dazu beitragen kann, diese Arbeit zu optimieren und Organisationen zu helfen, bessere Entscheidungen zu treffen.

Warum das Messen von Risiken schwieriger geworden ist

Warum ist die Risikomessung heutzutage so schwierig? Hier sind vier Gründe.

Schwierigkeit Nr. 1: Unzusammenhängende, bunt gemischte IT-Assets

Vor zwanzig Jahren bestanden IT-Risikobewertungen hauptsächlich darin, die PCs der Mitarbeiter und die Server in Rechenzentren zu zählen, potenzielle Schwachstellen für verschiedene Hardwaremodelle zu untersuchen und am Ende einen Bericht zu erstellen.

Heute sind die IT-Assets, die es zu katalogisieren und zu analysieren gibt, mitunter über 50 Büros, 500 Rechenzentren (die zum Großteil anderen Unternehmen gehören) und 10.000 Heimnetzwerke verteilt. Und ein bedeutender Teil – wahrscheinlich mindestens 20 % – dieser verteilten Architektur besteht aus „Schatten-IT“, also aus Produkten und Diensten, die ohne offizielle Genehmigung und fortlaufende Überwachung durch die IT-Abteilung von den Mitarbeitern genutzt werden.

In dieser stark verteilten, schwer katalogisierbaren IT-Umgebung sind klassische Tools und Ansätze zur Risikomessung gar nicht anwendbar.

Schwierigkeit Nr. 2: Komplexität der IT

Ein zweiter Punkt, der die Risikobewertung erschwert, ist die Komplexität der IT. Es gibt mehr Geräte, Software ist anders konzipiert und Aufgabenschwerpunkte haben sich verändert. Doch das ist nicht alles.

Das Zeitalter der großen, monolithischen Anwendungen ist vorbei. Moderne IT-Infrastruktur bestehen aus vielen kleinen und mittelgroßen Komponenten, durch deren Zusammenarbeit ein größeres Ganzes entsteht.

Eine Banking-App kann beispielsweise auf die reibungslose Funktion von 75 verschiedenen IT-Komponenten angewiesen sein. Dabei kann es sich unter anderem um UI-Code oder mehrere Back-End-Datenbanken handeln. Die mit jeder dieser Komponenten verbundenen Risiken wirken sich auf das Gesamtrisiko der App aus.

Schwierigkeit Nr. 3: Raffinierte Sicherheitsangriffe

Unternehmen sind heutzutage einer wachsenden Anzahl von Cyberkriminellen ausgesetzt, die oft Zugang zu hochentwickelten Technologien haben.

Vor zwanzig Jahren waren Angreifer meist Störenfriede – Programmierer, die Spaß daran hatten, mithilfe ausgeklügelter Ideen Unruhe zu stiften. Unter den heutigen Angreifern befinden sich Nationalstaaten, kriminelle Syndikate und böswillige „Script-Kiddies“, die sich im Dark Web für 50 Dollar ein Malware- oder Credential-Stuffing-Skript und eine Liste mit gestohlenen Anmeldedaten kaufen.

Schwierigkeit Nr. 4: Geteilte Verantwortung

Eine letzte Hürde? Ein neuer Trend beim Risikomanagement erfordert eine breitere Aufteilung der Risiken auf Geschäftseinheiten. Die Risikobewertung einer Organisation mag zwar von der IT-Abteilung durchgeführt werden, doch Führungsteams und Vorstände fordern zunehmend, dass die Leiter von Geschäftseinheiten mehr Verantwortung für die Risiken übernehmen, die ihre Betriebsabläufe betreffen.

Zur Bewältigung dieser Schwierigkeiten sollten Sie einen Top-Down-Ansatz für die Risikomessung verfolgen, wie meine Kollegen in den vorangegangenen Kapiteln dieses E-Books beschrieben haben. Identifizieren Sie „Lieferketten“, die die verschiedenen strategischen Ziele unterstützen, und sammeln Sie möglichst viele Echtzeitinformationen über den Status jeder dieser Lieferketten.

Die Risikomessung ist eine fortlaufende strategische Aktivität

Ob Sie eine effektive Vorgehensweise für die Messung von Risiken gefunden haben, merken Sie, wenn die Aktivitäten kontinuierlich Informationen hervorbringen, die Ihnen helfen, geschäftliche Entscheidungen zu treffen. Damit Sie diese Informationen erhalten, sollten Sie folgende Best Practices für die Risikomessung beachten:

Kontinuierlich

Die Risikobewertungen Ihrer Organisation sollten kontinuierlich mit Informationen zum aktuellen Zustand Ihrer IT-Umgebung aktualisiert werden. Wenn die Risikodaten aktuell sind, können Sie Entscheidungen auf der Grundlage der Technologien und Anbieter treffen, die Sie aktuell nutzen bzw. mit denen Sie aktuell zusammenarbeiten. So müssen Sie nicht mit Daten arbeiten, die schon mehrere Monate alt sind.

Priorisiert

Ihre Vorgehensweise bei der Risikobewertung sollte es Ihnen erleichtern, Risiken und Risikominderungen je nach den strategischen Zielen Ihrer Organisation zu priorisieren. Sie verfügen über ein Risikobewertungsverfahren, damit Sie Risiken vergleichen können, wenn Sie überlegen, ein Daten-Repository aus einer lokalen Umgebung zu einem vertrauenswürdigen Cloud-Anbieter zu verschieben, um Geld zu sparen.

Zugänglich

Sie können bei Bedarf leicht auf Risikobewertungen zugreifen. Sie müssen sich nicht durch 43 Excel-Tabellen arbeiten, um die gesuchte Analyse zu finden. Sie haben eine Funktion zur Erstellung von Risikoberichten, auf die Sie im Rahmen der kontinuierlichen Entscheidungsfindung des Unternehmens schnell zugreifen können.

Die Geschäftswelt ist schnelllebiger als je zuvor. IT-Umgebungen sind groß und komplex. Mit einem Top-Down-Ansatz für die Risikomessung und den Vorteilen von Echtzeit-Datenerfassung und Automatisierung können Sie die erforderlichen Abläufe etablieren, um für langfristiges Wachstum zu sorgen und Ihre Organisation durch künftige Transformationen zu führen.

CHECKLISTE

Leitfaden für die Risikomessung

1. Führen Sie ein Meeting mit den Führungskräften Ihres Unternehmens durch, um einen Einblick in ihre langfristigen strategischen Ziele zu erhalten.
2. Weisen Sie diesen Zielen Punktzahlen zu, um ihre relative Bedeutung einzuordnen.
3. Ermitteln Sie die Mitarbeiter, Prozesse und Technologien, die an der Erreichung der individuellen Ziele beteiligt sind.
4. Erfassen Sie Ungewissheiten über jeden beteiligten Faktor in der „Lieferkette“ des jeweiligen Ziels.
5. Sammeln Sie Daten, z. B. zum Betriebsstatus von Endpunkten, und setzen Sie dabei nach Möglichkeit auf Automatisierung.
6. Setzen Sie sich mit Stakeholdern in verschiedenen Abteilungen zusammen, um zu erfahren, welche Bedenken sie bezüglich Risiken haben und welche Vorschläge sie zur Reduzierung dieser Risiken beitragen können.
7. Weisen Sie jeder Ungewissheit eine Punktzahl und einen Prozentsatz zu, die für ihre Bedeutung bzw. ihre Wahrscheinlichkeit stehen. Multiplizieren Sie die Punktzahlen mit der Wahrscheinlichkeit, um daraus einen Risikoscore für eine Person, ein bestimmtes Team, einen Prozess oder eine Technologie in der Lieferkette eines Ziels abzuleiten.
8. Rechnen Sie die Ergebnisse Ihrer Messungen zusammen und setzen Sie jedes Risiko in Bezug zu einem strategischen Ziel.
9. Setzen Sie sich noch einmal mit den Führungskräften Ihres Unternehmens zusammen, um eine datengestützte Diskussion zum Thema Risiken zu führen. Geben Sie ihnen einen Überblick über bestehende Risiken und die Entscheidungen, die zur jeweiligen Minderung getroffen werden können.
10. Das hierbei erstellte Rahmenwerk für die Risikomessung sollte kontinuierlich aktualisiert werden. Setzen Sie so oft wie möglich auf Automatisierung, damit Risiken jederzeit im Detail bewertet werden können.

Risiko, wie durch die Norm *ISO 31000* definiert, bedeutet Ungewissheit in Bezug auf Ziele. In diesem E-Book haben wir anhand unserer Kenntnisse beschrieben, welche Ziele wichtig sind und wie Sie die mit einem Ziel verbundene Ungewissheit messen können, um das bestmögliche Ergebnis zu erreichen: die Reduzierung von Risiken, die die Mission eines Unternehmens gefährden.

Die Endgeräte eines Unternehmens spielen beim Risikomanagement eine wichtige Rolle. Weitere Informationen zur Verwaltung, Überwachung und Sicherung von Unternehmensendpunkten mit der Tanium-Plattform finden Sie auf **Tanium.com**. **Fordern Sie jetzt eine Demo an**.

Tanium ist die Plattform, der Unternehmen vertrauen, wenn sie Visibilität und Kontrolle für alle Endpunkte in lokalen, Cloud- und hybriden Umgebungen erzielen möchten. Unser Ansatz bietet eine Lösung für die wachsenden Herausforderungen der heutigen IT. Durch die Bereitstellung präziser, vollständiger und aktueller Endpunktdaten erhalten Teams für IT-Betrieb, -Sicherheit und -Risiko die Möglichkeit, ihre Netzwerke schnell zu verwalten, zu sichern und zu schützen. Tanium verfolgt die Mission, Organisationen dabei zu helfen, jeden Endpunkt zu erfassen und zu kontrollieren. Das ist die Macht der Gewissheit.

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