TANIUM

Was Sie nicht kennen, kann Ihnen schaden

Ein Leitfaden zur Risikomessung für Hersteller

2023 könnte ein entscheidendes Jahr werden für das herstellende Gewerbe im Bezug auf das Risikomanagement.

Energie- und Rohstoffpreise in noch nie dagewesener Höhe, verbunden mit anhaltendem Rohstoffmangel, behindern weiterhin den Sektor.

Der perfekte Sturm zieht seit geraumer Zeit auf und kein Teilsektor in der gesamten EU scheint immun gegen die sinkende Nachfrage und die anhaltenden Lieferkettenprobleme.

Für Unternehmen, die diese Effekte bekämpfen möchten, bieten sich scheinbar zwei Kernstrategien. Diese betreffen in erster Linie abgestimmte Bestrebungen um finanzielle Nachhaltigkeit mit Fokus auf die Verbesserung von Eigenkapital, Bonität und Liquidität. Fertigungsunternehmen sind auf hohe Investitionen angewiesen, sodass der einfache Zugang zu erschwinglichen Finanzierungen für sie in den kommenden Jahren entscheidend sein wird.

Zudem wird erwartet, dass viele von ihnen stärker in die Digitalisierung investieren werden, um ihre Kosten zu senken und die Produktivität zu verbessern, insbesondere in Bezug auf Industrie 4.0/IoT, Robotik und Automatisierung.

Natürlich sind finanzielle Stabilität und betriebliche Effizienz[1]für deutsche [2]Hersteller keine Fremdwörter, aber das Risikomanagement wird angesichts bedeutender strategischer Veränderungen erheblich erschwert.

Nehmen wir zum Beispiel den Verkauf einer Tochtergesellschaft, um den Cashflow zu verbessern: Wie entkoppelt sich ein Hersteller von den Cybergefahren aller veralteten Infrastrukturen, Anwendungen und Endpunkte?

Oder umgekehrt, wie sorgt ein Hersteller, der neue digitale Prozesse integrieren möchte, für Konformität und zwar ganz ohne über eine Referenzarchitektur und Rahmenkonzepte für die Interoperabilität zu verfügen? Veränderungen sind zwar gut, aber stets mit Risiken verbunden.

Risiken, die sorgfältig gehandhabt und gemessen werden müssen. Die CIOs, CEOs und CFOs von Unternehmen erkennen zunehmend, dass sie eine viel bessere Chance haben, die Nullen im Betriebsergebnis zu sichern, wenn sie sich auf das Risiko konzentrieren. Schließlich ist „Profitabilität“ in jeder Rezession das Schlüsselwort.

In diesem E-Book geht es um das Konzept „Was gemessen wird, lässt sich auch verwalten“. Wir zeigen, wie eine effektive Risikomessung dazu beitragen kann, Ihre Risikoexposition einzudämmen.

Wir beginnen damit, die vier Hauptprobleme zu untersuchen, mit denen Technologieführer konfrontiert werden, wenn sie versuchen, ihre Risiken unternehmensweit zu quantifizieren und zu messen.

Risikomanagement beginnt mit der Messung von Risiken

Aber wie lassen sich Risiken sinnvoll messen?

Sollten Sie wirklich sämtliche Software-Schwachstellen im Unternehmen und seinen Tochterfirmen ermitteln? Müssen Sie tatsächlich eine Liste aller Endpunktgeräte erstellen die die Software-Patches erfordern? Sollten Sie die Betriebszeit Ihrer wichtigsten Unternehmensanwendungen in Berichten erfassen?

Schwierigkeit Nr #1: **Verteilte, unterschiedliche Assets**

Heutzutage muss der IT-Bestand mitunter über 50 Büros, 500 Rechenzentren (die zum Großteil anderen Unternehmen gehören) und 10 000 Heimnetzwerken hinweg analysiert und katalogisiert werden. Und ein bedeutender Teil – wahrscheinlich mindestens 20 % – dieser verteilten Architektur besteht aus „Schatten-IT", also aus Produkten und Diensten, die ohne offizielle Bestätigung und fortlaufende Überwachung durch die IT-Abteilung von den betrieblichen Funktionen genutzt werden.

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

Schwierigkeit Nr #2: **IT-Komplexität**

Es gibt nicht nur mehr Geräte, sondern dazu noch geänderte Software-Konzepte und neue Aufgabenschwerpunkte. 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 E-Commerce-Anwendung kann beispielsweise auf das reibungslose Funktionieren 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: **Intelligente Cyberangriffe**

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

Zu Beginn gingen Cyberbedrohungen meistens von Störenfrieden und Programmierern aus, die Spaß daran hatten, mithilfe ausgeklügelter Ideen Unruhe zu stiften. Heutzutage treten als Angreifer Nationalstaaten, kriminelle Syndikate und böswillige Script-Verfasser auf, die sich im Dark Web für 50 Dollar ein Malware- oder Credential-Stuffing-Skript und eine Liste mit gestohlenen Zugangsdaten kaufen.

Schwierigkeit Nr #4: **Gemeinsame Verantwortung**

Ein neuer Trend beim Risikomanagement erfordert eine breitere Aufteilung der Risiken auf die Geschäftseinheiten.

Die Risikobewertung einer Organisation mag zwar von der IT-Abteilung durchgeführt werden, doch Management-Teams und Vorstände fordern zunehmend, dass die Leiter von Geschäftseinheiten mehr Verantwortung für die Risiken übernehmen, die ihre Betriebsabläufe betreffen. Um diese Probleme anzugehen, verfolgen Sie einen Top-Down-Ansatz zur Risikomessung. Identifizieren Sie „Lieferketten“, die die verschiedenen strategischen Ziele unterstützen, und sammeln Sie möglichst viele Echtzeitinformationen über den Status jeder dieser Lieferketten.

Risiko in Zusammenhang mit strategischen Zielen bringen

Die Aufgabe von Management-Team und Vorstand besteht darin, dafür zu sorgen, dass das Unternehmen zentrale Ziele in den Bereichen Geschäftskontinuität, Datenschutz und Einhaltung gesetzlicher Bestimmungen erreicht.

Wenn Sie die Aufmerksamkeit Ihrer Kollegen im Führungsteam gewinnen möchten, sollten Sie beim Erörtern der Risikomessung den Bezug zu den auf Vorstandsebene erklärten Unternehmenszielen herstellen.

Anders ausgedrückt: Identifizieren und wägen Sie die verschiedenen technischen, gesetzlichen und anderweitigen Risiken Ihres Unternehmens ab und stellen Sie diese den allgemeinen strategischen Zielen Ihres Unternehmens gegenüber.

Sie werden feststellen, dass ein solches Framing Ihrer Risikomessungen Ihnen dabei hilft, Ihre Arbeit zu fokussieren, und den Führungskräften der Geschäftsbereiche das Verständnis und die Entscheidungsfindung erleichtert.

Aufbau einer gewichteten Risikoskala

Es ist selten, dass ein Unternehmen alle strategischen Ziele gleich behandelt. Sobald Sie aber diese Ziele identifiziert haben, weisen Sie ihnen auf einer Art von Skala Punktzahlen zu, z. B. von 1 bis 10. Basierend auf Gesprächen mit dem Management könnten Sie dem kontinuierlichen, jährlichen Umsatzwachstum von mindestens 10 % beispielsweise die Punktzahl 10 zuweisen und die regulatorische Compliance 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 beteiligten Faktors ein.

Für eine detailliertere Abstufung könnten Sie die Wahrscheinlichkeit[1]schätzen, mit der ein bestimmter Fehler auftritt. Angenommen, Ihr Unternehmen betreibt einen Webserver, über den eine geschäftskritische App ausgeführt wird.

Die Wahrscheinlichkeit, dass die Leistung des Servers in Spitzenzugriffszeiten unzumutbar niedrig ist, ist sicherlich größer als die Wahrscheinlichkeit, dass der gleiche Server von einem Stromausfall[2]betroffen ist, der gleichzeitig das Haupt- und das Notfallstromsystem lahmlegt.

In all diesen Fällen werden die [g1]Wahrscheinlichkeit und Schwere basierend auf der Zuverlässigkeit der Daten bestimmt. Wenn ein gewisses Maß an Kenntnissen vorhanden ist, werden

Risiken akzeptabler. Wenn Sie sich ihrer Kenntnisse sicher sind, können Sie besser erkennen, was Sie nicht wissen. Dadurch lassen sich extreme Risiken im Vergleich zu geringen Risiken deutlicher fokussieren. Die besten Risikoentscheidungen erfordern stets auch die besten Informationen. Vom Mittelwert mehrerer Datenquellen auszugehen, führt zu Ableitungen dieser Quellen, die unzuverlässig und falsch sind.

Wahrheit kennt keinen Mittelwert.

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.

Um entsprechende Handlungsempfehlungen geben zu können, sollten Sie Ihre Best Practice zur Risikomessung kontinuierlich an den Informationen über den aktuellen Zustand Ihrer IT-Umgebung ausrichten.

Wenn die Risikodaten aktuell sind, können Sie Entscheidungen auf Grundlage der Technologien und Anbieter treffen, die Sie im Moment nutzen bzw. mit denen Sie derzeit zusammenarbeiten. So müssen Sie nicht mit Daten arbeiten, die schon mehrere Monate alt sind.

Proaktives Risikomanagement beginnt mit einem umfassenden Überblick über die Risikolage

Risiko, wie durch die Norm ISO 31000 definiert, bedeutet Ungewissheit in Bezug auf Ziele.

Die Endgeräte und Fertigungsinfrastruktur des Unternehmens spielen eine integrale Rolle beim Risikomanagement, wie in diesem E-Book beschrieben.

Tanium bietet eine kostenlose Risikobewertung, die Ihnen helfen kann, einen Überblick über Ihre Gefährdungslage zu erhalten und gleichzeitig einen umsetzbaren Verbesserungsplan zu liefern.

Als branchenweit einziger Anbieter von konvergentem Endpunktmanagement (XEM) führt Tanium den Paradigmenwechsel bei herkömmlichen Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an. Nur Tanium schützt jedes Team, jeden Endpunkt und jeden Arbeitsablauf vor Cyber-Threats, 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.

Besuchen Sie uns auf www.tanium.de