Positives Risiko im Bereich Cybersicherheit

AWS Prescriptive Guidance

AWS Prescriptive Guidance: Positives Risiko im Bereich Cybersicherheit

Table of Contents

Positives Risiko im Bereich Cybersicherheit

Greg Bell, Amazon Web Services (AWS)

Mai 2022 (Dokumentverlauf)

Die meisten Menschen betrachten Risiken aus einer negativen Perspektive, z. B. wenn sie einem Verlust ausgesetzt sind oder mit einem unerwünschten Ereignis umgehen. Die Internationale Organisation für Normung (ISO) definiert Risiko jedoch als „Auswirkung von Unsicherheit auf Ziele“. In diesem Fall kann der Effekt positiv oder negativ sein.

Die tatsächlichen Risiken können je nach Branche variieren, aber diese Standarddefinition gilt für alle, und jede Branche birgt sowohl negative als auch positive Risiken. In der Cybersicherheitsbranche bezieht sich negatives Risiko auf potenziellen Verlust und positives Risiko bezieht sich auf den potenziellen Gewinn von Komponenten, Wissen, Verbesserungen oder Daten.

Die Domains Projektmanagement und IT verfolgen die Strategie, positive Risiken in Geschäftsberichten und Geschäftsentscheidungen zu bewerten. Die Cybersicherheitsbranche hat dies jedoch noch nicht als gängige Praxis übernommen und viele Risikomanagementmethoden konzentrieren sich weiterhin auf negative Risiken. Wenn sie überhaupt über positive Risiken sprechen, dann nur kurz.

Traditionell betrachtet Cybersicherheit Risiken ausschließlich aus einer negativen Perspektive. Im Folgenden sind die beiden häufigsten Arten negativer Risiken im Bereich der Cybersicherheit aufgeführt:

- Abwärtsrisiko – Risiko von Verlusten aufgrund externer Faktoren, wie z. B. einer Bedrohung. Cyberkriminelle könnten beispielsweise einen Sicherheitsvorfall herbeiführen oder dessen Wahrscheinlichkeit erhöhen.
- Aufwärtsrisiko – Risiko von Verlusten bei gleichzeitiger Gewinnerzielung, wie z. B. eine Schwachstelle, die sich aus Veränderungen ergibt. Wenn Sie beispielsweise eine IT-Strategie implementieren, könnten Sie versehentlich das Risiko eines Sicherheitsvorfalls erhöhen. Ein Aufwärtsrisiko ist nicht dasselbe wie ein positives Risiko. Auch wenn es auf der Suche nach einem Gewinn auftritt, konzentriert sich das Aufwärtsrisiko auf das Verlustpotenzial.

Bis vor Kurzem wurden in der Cybersicherheit nur negative Risiken berücksichtigt, und die Definition von Risiko konzentrierte sich auf potenzielle negative Folgen. Positive Risiken konzentrieren sich auf das potenzielle positive Ergebnis zu Beginn der Risikoidentifikation. Der Ausschluss positiver Risiken

führt dazu, dass die positiven Ergebnisse im Bereich der Cybersicherheit nicht erkannt werden. Aufgrund der Fokussierung auf negative Risiken nimmt die Unternehmensleitung Cybersicherheit häufig eher als reaktiv denn als proaktiv wahr und unterschätzt den Beitrag der Cybersicherheit zu positiven Geschäftsergebnissen.

In diesem Dokument werden positive Risiken für die Cybersicherheitsbranche definiert und die Vorteile und die Bedeutung der Einbeziehung positiver Risiken in Ihre Cybersicherheitsstrategie erörtert.

Vorteile eines positiven Risikos

Insbesondere in einer Branche wie der Cybersicherheit, die sich darauf konzentriert, das Unternehmen vor potenziellen Verlusten zu schützen, ist es einfach, Risiken aus einer negativen Perspektive zu betrachten. Die Neuausrichtung von Cybersicherheitsrisiken auf der Grundlage ihrer potenziellen Vorteile kann der Organisation zugute kommen, indem positive Ergebnisse erzielt, die Sicherheitslage der Organisation verbessert und das Vertrauen der Kunden gestärkt wird.

Förderung positiver Ergebnisse

Die Übernahme positiver Risiken ermöglicht es der Organisation, den Beitrag, den die Domain zu positiven Geschäftsergebnissen leistet, zu bewerten und anzuerkennen. Laut Cybersicherheit in der C-Suite und im Sitzungssaal(Forschungsbericht der Enterprise Strategy Group):

- 69 % der Geschäfts- und Technologieführer glauben, dass Cybersicherheit ganz oder größtenteils ein Technologiebereich ist, der kaum oder gar nicht mit dem Unternehmen verknüpft ist.
- 11 % der Geschäfts- und Technologieführer setzen Cybersicherheit mit der Einhaltung gesetzlicher Vorschriften gleich.
- 82 % der Organisationen geben an, dass die Cybersicherheitsrisiken in den letzten zwei Jahren aufgrund von Faktoren wie zunehmenden Cyberbedrohungen, einer stärkeren Integration von Technologie in die Organisation und einer wachsenden Angriffsfläche zugenommen haben.

Wenn Führungskräfte im Bereich Cybersicherheit positive Risiken in Gespräche und Berichte integrieren, trägt dies dazu bei, den Wert eines sicheren IT-Betriebs innerhalb des Unternehmens zu fördern.

Nehmen wir zum Beispiel an, ein Unternehmen hatte vor einigen Jahren eine Datenschutzverletzung, und die Datenschutzverletzung wurde durch das Fehlen eines Patch-Management-Prozesses verursacht. Der Vorfall wird immer noch in den Medien thematisiert und beeinträchtigt die Wahrnehmung und Interaktion der Kunden mit dem Unternehmen. Das Unternehmen möchte den Vorfall hinter sich lassen und sein Serviceangebot erweitern, aber das Kundenvertrauen blockiert den Vertrieb. Cybersicherheit nutzt positive Risiken, um Führungskräfte davon zu überzeugen, in einen Patch-Management-Prozess zu investieren, der Anwendungen kontinuierlich aktualisiert. Der neue Prozess reduziert das Risiko einer Datenschutzverletzung drastisch und verbessert so die Sicherheitslage des Unternehmens. Neuigkeiten über den up-to-the-minute Patch-Management-

Prozess erreichen die Medien und potenzielle Kunden. Die Kunden fühlen sich jetzt wohl dabei, bei dem Unternehmen einzukaufen, und der Umsatz steigt auf ein beeindruckendes Niveau.

Wenn positive Risiken bei der Risikoidentifikation nicht berücksichtigt werden, kann dies zu einer unvollständigen Bewertung führen und die Geschäftsentscheidung beeinflussen. Konkrete Beispiele für positive Risiken, die sich auf Geschäftsentscheidungen auswirken könnten, finden Sie unter Beispiele für positive Risiken.

Erhöhung der Sicherheitslage und des Kundenvertrauens

Cybersicherheit ist ein wesentlicher Bestandteil der Sicherheitslage des Unternehmens. Datenschutzverletzungen können sich negativ auf das Kundenvertrauen auswirken, aber eine starke Sicherheitslage und ein guter Ruf können auch das Vertrauen der Kunden stärken und Geschäftschancen eröffnen.

Wie in Förderung positiver Ergebnisse beschrieben, zeigen Untersuchungen, dass Führungskräfte zwar die negativen Risiken im Zusammenhang mit Cybersicherheit verstehen, aber häufig nicht die positiven Risiken oder den Geschäftswert verstehen. Untersuchungen zeigen jedoch, dass Führungskräfte im Bereich Cybersicherheit verstehen, wie ein starkes Sicherheitskonzept der Organisation zugute kommen kann.

In Cybersicherheitsforschung: Der Innovationsbeschleuniger (Vodafone-Whitepaper) hat Vodafone 1 434 weltweite Entscheidungsträger im Bereich Cybersicherheit interviewt. Deren Daten zeigten:

- 73 % der Befragten waren der Ansicht, dass starke Sicherheitsvorkehrungen neue Geschäftsmöglichkeiten eröffnen.
- 89 % gaben an, dass Verbesserungen ihrer Sicherheit die Kundenbindung und das Vertrauen stärken würden.
- 90 % gaben außerdem an, dass sie in der Lage waren, ihr Image zu verbessern, neue potenzielle Kunden zu erreichen und sie auch zu echten Kunden zu machen.
- 89 % glauben, dass eine effektive Cybersicherheit ein relevanter Wettbewerbsvorteil ist, der ihnen hilft, sich von ihren Mitbewerbern abzuheben.
- 24 % meldeten einen Umsatzanstieg durch den Einsatz von Cloud-Technologien und dem Internet der Dinge (IOT), sowie durch gezielte IT-Sicherheitskontrollen.
- Anstatt potenzielle negative Ergebnisse bei der Kommunikation mit der Geschäftsleitung zu nutzen, können Sie auch positive Risiken nutzen, um den Geschäftswert einer Verbesserung des Kundenvertrauens zu kommunizieren. Führungskräfte können bei der Finanzierung von

Programmen vorsichtig sein. In einigen Fällen wird die Cybersicherheit nur auf das Nötigste beschränkt, das für den Betrieb erforderlich ist. Die interne Kommunikation positiver Risiken bei Finanzierungsanträgen kann Ihrer Unternehmensleitung helfen, den geschäftlichen Wert der Cybersicherheit zu verstehen. Dies kann zu einer erhöhten Finanzierung von Cybersicherheitsinitiativen führen und den Umsatz des Unternehmens steigern.

Änderung der Sprache für Cybersicherheitsrisiken

Ein Teil der Herausforderung bei der Einführung positiver Risiken für die Cybersicherheit besteht darin, dass sich die technische und domainspezifische Terminologie auf negative Risiken konzentriert, wie Bedrohungen, Schwachstellen, und Sicherheitskontrollen. Die Cybersicherheitsbranche muss ihr Vokabular weiterentwickeln und erweitern, um Formulierungen einzubeziehen, die die positiven Geschäftsergebnisse (oder positiven Risiken) hervorheben, die Cybersicherheit für das Unternehmen mit sich bringt. Begriffe wie Geschäftsvorteil, Vorteile und Geschäftswert heben Sie den Beitrag der Cybersicherheit für die Organisation hervor.

Eine Änderung der Sprache der Cybersicherheit trägt dazu bei, die Auffassung zu ändern, dass Cybersicherheit ein Technologiebereich ist, der sich ausschließlich auf Bedrohungen und Schwachstellen konzentriert und unabhängig vom Geschäft ist. Die Unternehmensführung unterschätzt häufig den Beitrag der Cybersicherheit zu positiven Geschäftsergebnissen. Weitere Informationen über die Wahrnehmung von Cybersicherheit durch die Führung finden Sie unter Förderung positiver Ergebnisse.

Zunehmende Verbreitung in verwandten Bereichen

In vielen Bereichen besteht ein wachsendes Interesse an der Einbeziehung positiver Risiken, da dadurch der Beitrag der Domain zu den Geschäftsergebnissen anerkannt wird. Das Konzept des positiven Risikos wurde vor Kurzem in allgemeine Projektmanagementprozesse und Definitionen aufgenommen.

Im Jahr 2013 hat das Project Management Institute (PMI) die Definition des positiven Risikos (auch bekannt als Möglichkeiten) in die fünfte Ausgabe des Project Management Body of Knowledge (PMBOK) eingefügt. PMBOK definiert individuelles Risiko als „ein ungewisses Ereignis oder eine unsichere Bedingung, die sich, falls sie eintritt, positiv oder negativ auf ein oder mehrere Projektziele auswirkt“. Es definiert insgesamt Projektrisiko als „die Auswirkung der Unsicherheit auf das Projekt… als Ganzes mehr als die Summe der Einzelrisiken innerhalb eines Projekts, da sie alle Quellen der Projektunsicherheit einbezieht... bedeutet, dass die Stakeholder den Auswirkungen sowohl positiver als auch negativer Schwankungen des Projektergebnisses ausgesetzt sind“.

Leider gilt die Tatsache, dass PMI positive Ergebnisse in seine Risikodefinitionen einbezieht, noch nicht für die Cybersicherheitsbranche.

Beispiele für positive Risiken

Im Folgenden finden Sie einige Beispiele für positive Risiken in den Bereichen Technologie, Projektmanagement und Cybersicherheit.

Positives Technologierisiko

Ein Beispiel für ein positives Technologierisiko ist, dass die Einführung einer Technologie zu niedrigeren Lohnkosten führen könnte. Zum Beispiel:

1. Die Implementierung der Technologie könnte zu einer höheren Geschäftseffizienz führen.
2. Diese Effizienzsteigerungen könnten zu einer Reduzierung des Arbeitsaufwands führen.
3. Ein geringerer Arbeitsaufwand könnte zu niedrigeren Lohnkosten führen.

Positives Risiko für das Projektmanagement

Ein Beispiel für ein positives Risiko für das Projektmanagement ist die Fehlkalkulation eines Projektbudgets, die zu Kosteneinsparungen oder zur Finanzierung zusätzlicher Projekte führen könnte. Zum Beispiel:

1. Die frühzeitige Umsetzung eines Technologieprojekts könnte dazu führen, dass der Projektmanager die Projektkosten falsch berechnet.
2. Eine Fehlkalkulation der Projektkosten könnte zu überhöhten Projektmitteln führen.
3. Zu hohe Projektmittel könnten zu Kosteneinsparungen oder zur Finanzierung zusätzlicher Projekte führen.

Positives Risiko für die Cybersicherheit

Ein Beispiel für ein positives Risiko für die Cybersicherheit ist die Implementierung von Patch-Management, das das Vertrauen der Kunden stärken könnte. Zum Beispiel:

1. Durch die Implementierung von Patch-Management könnten Schwachstellen in der Anwendung reduziert werden.
2. Die Beseitigung von Schwachstellen könnte die Anwendungsrisiken verringern und die Anwendung sicherer machen.

3. Eine verbesserte Anwendungssicherheit könnte den Datenverlust reduzieren.
4. Ein geringerer Datenverlust könnte das Vertrauen der Kunden stärken.

Ein weiteres Beispiel für positive Risiken im Zusammenhang mit Cybersicherheit ist die Implementierung von Vorfallsreaktion, die die Produktivität der Mitarbeiter steigern könnte. Zum Beispiel:

1. Die Implementierung von Vorfallsreaktion könnte dazu führen, dass ein erhöhter Netzwerkverkehr erkannt wird.
2. Ein erhöhter Netzwerkverkehr könnte dazu führen, dass der Missbrauch von Ressourcen durch Mitarbeiter erkannt wird, indem sie auf Inhalte zugreifen, die nichts mit der Arbeit zu tun haben, wie Musik- und Videostreaming-Services. Diese Aktivitäten verbrauchen Netzwerkbandbreite und können sich negativ auf die Netzwerk- und Anwendungsleistung auswirken.
3. Die Entdeckung des Missbrauchs von Unternehmensressourcen durch Mitarbeiter könnte zur Sperrung dieser Services führen.
4. Das Blockieren dieser Services könnte den Verbrauch von Netzwerkbandbreite reduzieren und die Produktivität der Mitarbeiter steigern.

Das letzte Beispiel für positive Risiken im Bereich Cybersicherheit ist schließlich die Implementierung eines Notfallplans, der die Geschäftsmöglichkeiten und die Einhaltung der Datenschutzgesetze verbessern könnte. Zum Beispiel:

1. Die Umsetzung eines Plans zur Vorfallsreaktion könnte dazu führen, dass Malware und Ransomware schnell erkannt und identifiziert werden können.
2. Die Identifizierung von Malware und Ransomware könnte die Auswirkungen minimieren und die Bedrohung der Unternehmensressourcen mindern.
3. Die Minderung der Bedrohung der Unternehmensressourcen könnte zu neuen Geschäftsmöglichkeiten führen und dem Unternehmen helfen, die Datenschutzgesetze einzuhalten.

Reaktion auf Cybersicherheit-Risiken

Die Reaktionen auf positive und negative Risiken sind sehr unterschiedlich. Bei negativen Risiken ergreifen Sie Maßnahmen, um die Auswirkungen auf das Ergebnis zu minimieren, aber bei positiven Risiken ergreifen Sie Maßnahmen, um die Auswirkungen auf das Ergebnis zu maximieren. Die folgende Tabelle zeigt mögliche Reaktionen auf positive und negative Risiken.

Risikotyp	Antwort	Definition
Positives Risiko	Ausnutzung	Maximierung der Wahrschei nlichkeit, dass das Risiko eintritt, um seine positiven Auswirkungen zu realisieren.
	Freigeben	Übertragung eines Teils des Eigentums an oder der Verantwortung für das Risiko auf eine andere Partei. Dies ist derselbe Ansatz wie bei einem negativen Risiko, und es wird versucht, den potenziel len Verlust oder Gewinn zu kontrollieren.
	Verbessern	Erhöhung der Bedingungen, die das Risiko schaffen, um die Chance zu maximieren.
	Ignore	Ignorierung der Möglichke it des Risikos und keine Maßnahmen ergreifen. Diese Reaktion ist üblich, wenn die Wahrscheinlichkeit eines Risikos sehr gering ist oder wenn die Vorteile eines potenziellen positiven Ergebnisses minimal sind.

Risikotyp	Antwort	Definition
Negatives Risiko	Abschwächen	Minimiert die Wahrschei nlichkeit oder Wahrschei nlichkeit des Eintretens des Risikos.
	Übertragung	Verlagerung der Verantwor tung oder Haftung für das Risiko auf eine andere Partei, z. B. durch den Abschluss einer Versicherungspolice, um das Risiko auf eine Versicher ungsgesellschaft zu übertrage n.
	Vermeiden	Beseitigung der Bedingungen, die das Risiko darstellen.
	Accept	Erkennung der Existenz des Risikos an, jedoch werden keine Maßnahmen ergriffen.

Bei negativen Risiken vermeiden, übertragen, mindern oder akzeptieren Organisationen das Risiko auf der Grundlage ihrer Risikobereitschaft und Risikobereitschaft. Sie versuchen, das Eintreten des Risikos zu verhindern, und wenn doch, versuchen sie, seine Auswirkungen auf die Gesamtmission zu minimieren.

Die positiven Reaktionen auf Risiken lassen sich am besten anhand von Beispielen veranschaulichen:

- Ausnutzen – Ein Sicherheitsbeauftragter erfährt, dass ein gut qualifizierter Sicherheitsexperte vor Kurzem beschlossen hat, eine neue Anstellung zu suchen, und arrangiert einen großzügigen Unterzeichnungsbonus, um den potenziellen Mitarbeiter in sein Team zu locken.
- Teilen – Der Leiter einer Geschäftseinheit möchte die Sicherheit durch den Einsatz eines Produkts zur Verwaltung privilegierter Zugriffe verbessern, verfügt jedoch nicht über ein ausreichendes Budget, um die Tools und Services im laufenden Haushaltsjahr zu erwerben. Der Leiter

arbeitet mit einem Leiter aus einer anderen Geschäftseinheit zusammen, der das Tool als Pilotprojekt erwerben und implementieren und später die Installation erweitern wird, um beide Geschäftsbereiche zu unterstützen.

- Verbessern – Ein Mitarbeiter hat eine Möglichkeit erkannt, einen bestehenden Geschäftsprozess zu automatisieren, um Cybersicherheitsbedrohungen zu reduzieren. Dies erfordert jedoch Investitionen in Zeit und Ausrüstung. Angesichts der positiven Vorteile eines solchen Prozesses genehmigt der Manager Überstunden, um die Kapazitäten auszubauen, und verwendet vorhandene Hard- und Softwareressourcen, die den Fortgang des Projekts ermöglichen, für neue Zwecke.
- Ignorieren – Ein Finanzmanager erfährt, dass ein Mitarbeiter der Vertriebsabteilung eine neue Anwendung entwickelt hat, die eine mühsame und manuelle Aufgabe automatisiert. Die Anwendung wurde kürzlich nur für die Verwendung in der Verkaufsabteilung autorisiert. Der Finanzmanager erhält ohne ausdrückliche Genehmigung eine Kopie der neuen Anwendung, um sich in seiner Abteilung einen ähnlichen Vorteil zu verschaffen.

Nächste Schritte

Die Domains Technologie und Projektmanagement haben positive Risiken in ihre Risikobewertungsprozesse aufgenommen, aber die Cybersicherheitsbranche hat sie in der Vergangenheit ausgeschlossen. Positive Risiken können zu positiven Geschäftsergebnissen führen, und die Cybersicherheitsbranche muss sich darauf einstellen, positive Risiken einzugehen und die Vorteile zu nutzen.

Sie können sofort damit beginnen, positive Risiken in allen Mitteilungen zu kommunizieren. Risikobewertungen, Sicherheitsbeurteilungen oder Statusberichte sollten z. B. einen Abschnitt über positive Risiken enthalten. Finanzierungsanträge an die Geschäftsführung sollten positive Risiken beinhalten, die potenziellen Vorteile für das Unternehmen darlegen und alle potenziellen Geschäftsvorteile hervorheben, die sich aus der Genehmigung des Antrags ergeben.

Häufig gestellte Fragen

Was ist der Unterschied zwischen dem Aufwärtsrisiko und dem positiven Risiko?

Obwohl Aufwärtsrisiko und positives Risiko ähnlich klingen, sind sie tatsächlich sehr unterschiedlich. Innerhalb des Risikos gibt es entweder ein positives oder ein negatives Ergebnis, und innerhalb des negativen Ergebnisses gibt es entweder eine positive oder eine negative Seite.

Positives Risiko ist der potenzielle Gewinn von Komponenten, Wissen, Verbesserungen oder Daten. Sie implementieren beispielsweise Patch-Management und einen Prozess zur schnellen Beseitigung von Schwachstellen z. B. innerhalb einer Woche. Im Laufe des nächsten Jahres gab es keine Sicherheitsvorfälle.

Aufwärtsrisiko ist das Risiko, Verluste zu erleiden, während man einen Gewinn anstrebt. Beispielsweise führt das Unternehmen eine neue Anwendung ein, und Sie implementieren eine Patch-Verwaltung und einen Prozess zur schnellen Beseitigung von Schwachstellen, z. B. innerhalb einer Woche. Das Risiko von Verlusten (der Zeitraum, in dem Sie Schwachstellen entfernen) dient der Erzielung eines Gewinns (einer sichereren Anwendung), weshalb dies als Aufwärtsrisiko angesehen wird. Sie können das Aufwärtsrisiko erhöhen, indem Sie den Prozess zur Beseitigung von Schwachstellen auf einen Tag ändern, oder das Aufwärtsrisiko verringern, indem Sie den Zeitraum auf einen Monat ändern. Grundsätzlich ist das Aufwärtsrisiko die unsichere Möglichkeit eines Gewinns bei gleichzeitigem Versuch, den Verlust zu minimieren.

Warum ist es wichtig, positive Risiken in die Cybersicherheit einzubeziehen?

Die Integration positiver Risiken in Bewertungen und Gespräche zu Cybersicherheitsrisiken trägt dazu bei, den Wert der Cybersicherheit für das Unternehmen zu fördern. Weitere Informationen finden Sie unter Vorteile eines positiven Risikos.

Ressourcen

- Cybersicherheit in der C-Suite und im Sitzungssaal (Forschungsbericht der Enterprise Strategy Group):
- Cybersicherheitsforschung: Der Innovationsbeschleuniger (Vodafone-Whitepaper)
- Integration von Cybersicherheit und Unternehmensrisikomanagement (ERM) (NIST-Publikation)
- Erläuterung von „Aufwärtstrends“ und „positiven“ Risiken (Blogbeitrag des FAIR-Instituts)

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	27. Mai 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.