ivanti

Leitfaden für Exposure-Management-Metriken

Exposure Management gewinnt zunehmend an Bedeutung – und mit diesem Wandel verändert sich auch die Art und Weise, wie Unternehmen Cyber-Risiken messen. Dieser Leitfaden stellt eine Auswahl an Metriken vor, mit denen sich sämtliche Aspekte eines Exposure-Management-Programms analysieren und steuern lassen.

Mithilfe dieser Metriken können Sicherheitsteams die Effizienz und Wirksamkeit ihrer Maßnahmen steigern, indem sie Risiken gezielter priorisieren. Zudem können sie Risiken besser quantifizieren und gegenüber der Geschäftsleitung, dem Vorstand sowie anderen involvierten Fachbereichen klar kommunizieren.

Operative Metriken

Diese Metriken werden von den Sicherheitsteams verwendet, um die täglichen Exposure-Management-Aktivitäten zu steuern.

Sichtbarkeit der Angriffsfläche	
Beschreibung	Die Sichtbarkeit von Cyber-Assets ist die Grundlage für das Exposure-Management. Unternehmen haben drei Arten von Cyber-Assets: ■ Bewusste Kenntnis: Cyber-Assets, die Ihnen bekannt sind und die nachweislich Teil Ihrer Angriffsfläche sind. ■ Bewusste Unkenntnis: Cyber-Assets, von denen Sie wissen, dass sie zu Ihrer Angriffsfläche gehören, die Sie jedoch möglicherweise nicht aktiv überwachen oder verwalten. ■ Unbewusste Unkenntnis: Cyber-Assets, die möglicherweise Teil Ihrer Angriffsfläche sind – oder auch nicht. Sie haben darüber keine gesicherten Informationen. Eine Metrik zur Sichtbarkeit der Angriffsfläche gibt an, wie umfassend Sie Ihre eigene Angriffsfläche überblicken. Indem Sie diesen Anteil messen, können Sie gezielt jene Bereiche identifizieren, in denen Blindspots bestehen – und gezielt Maßnahmen ergreifen, um diese Sicherheitslücken zu schließen. Idealerweise sollte 100 % Sichtbarkeit angestrebt werden – auch wenn dieses Ziel kaum erreichbar ist.
Messmethode	Ermitteln Sie den Prozentsatz der Cyber-Assets, die Sie über die von Ihnen zur Bewertung Ihrer Exposures genutzten Produkte oder Plattformen einsehen können. Teilen Sie dazu die Anzahl dieser einsehbaren Assets durch die geschätzte Gesamtanzahl aller Assets, die mit „bewusste Kenntnis“ und „bewusste Unkenntnis“ in Ihrer Umgebung eingeordnet wurden. Multiplizieren Sie das Ergebnis anschließend mit 100, um den Wert als Prozentsatz anzugeben.

Beachten Sie, dass Assets der Kategorie „unbewusste Unkenntnis“ bei der Sichtbarkeit der Angriffsoberfläche nicht berücksichtigt werden, da sie die Berechnung der Metrik unmöglich machen, aber Sie können sie nicht einfach ignorieren. Verwandeln Sie diese „unbewusste Unkenntnis“ in „bewusste Unkenntnis“ und kommen Sie der 100%igen Sichtbarkeit der Angriffsoberfläche einen Schritt näher – mit Ivantis Checkliste für Angriffsflächen.

Verwaltetes Vermögen (Assets Under Management)	
Beschreibung	Nachdem die Sichtbarkeit der Angriffsfläche berechnet wurde, folgt die Berechnung des verwalteten Vermögens (Assets Under Management). Diese Metrik wird traditionell verwendet, um den Prozentsatz der Geräte zu ermitteln, die aktiv über ein Unified Endpoint Management (UEM)-Tool verwaltet werden – ein Tool, mit dem IT-Administratoren Geräteeinstellungen und Sicherheitsrichtlinien zentral steuern können. Beim Exposure Management versteht man unter dem verwalteten Vermögen die Assets, die Ihrem Sicherheitsteam Erkenntnisse zu den Exposures liefern. Denken Sie daran: Die Sichtbarkeit von Assets ist nur der erste Schritt – für die Berechnung des Risikos sind Erkenntnisse zu den Exposures erforderlich.
Messmethode	Teilen Sie die Anzahl der Assets, von denen Sie Erkenntnisse zu den Exposures erfassen, durch die Anzahl der sichtbaren Assets (verwenden Sie hierfür den oben genannten Wert zur „Sichtbarkeit der Angriffsfläche“). Multiplizieren Sie ihn mit 100, um einen Prozentsatz zu erhalten.

Nutzen Sie die Checkliste für die Exposure Management-Strategie von Ivanti, um festzulegen, welche Technologien Sie Ihrer Cybersecurity-Architektur hinzufügen müssen, damit 100 % Ihrer Cyber-Assets erfasst und verwaltet werden.

Bewertung des Gefährdungsrisikos	
Beschreibung	Sobald Sie Ihre Cyber-Assets und deren Exposures identifiziert haben, können Sie die zugehörigen Exposures systematisch bewerten. Anhand von Bewertungen des Gefährdungsrisikos können Sicherheitsteams diejenigen Bedrohungen identifizieren, die mit hoher Wahrscheinlichkeit gegen das Unternehmen ausgenutzt werden – und diese gezielt priorisieren, um frühzeitig Gegenmaßnahmen zu ergreifen. Zugleich lässt sich einschätzen, welche Bedrohungen die Aufmerksamkeit der Geschäftsführung, des Vorstands oder anderer Stakeholder im Bereich Exposure Management erfordern.
Messmethode	Produkte und Plattformen zur Bewertung von Exposures automatisieren den Prozess der Berechnung von Risikobewertungen für Schwachstellen, Fehlkonfigurationen, Lücken in der Sicherheitskontrolle und andere Exposures anhand diverser Faktoren: ■ Schweregrad (z. B. CVSS und/oder Hersteller-Score) ■ Ausnutzbarkeit (z. B. Schwachstellenanalysen und/oder EPSS-Wert) ■ Potenzielle Auswirkungen (z. B. Asset-Kontext und/oder geschäftliche Auswirkungen) Umfassende Risikobewertungen unterscheiden das Exposure Management wesentlich vom traditionellen Schwachstellenmanagement – letzteres berücksichtigt lediglich den Schweregrad. Auch risikobasiertes Schwachstellenmanagement greift zu kurz, da es zwar den Bedrohungskontext einbezieht, nicht aber die geschäftlichen Auswirkungen.

Metriken für die Entscheidungsfindung

Diese Metriken ermöglichen es Führungskräften, Vorständen und anderen Stakeholdern, fundierte Entscheidungen über das Exposure Management zu treffen.

Cyber-Risikolevel	
Beschreibung	Das Cyber-Risikolevel ist einfach ein numerischer Wert für die Cybersicherheitslage eines Unternehmens. In Kombination mit der Risikobereitschaft des Unternehmens – also dem Maß an Cyber-Risiken, das im Sinne der Geschäftsziele in Kauf genommen wird – liefert das aktuelle Cyber-Risikolevel einen wichtigen Kontext für alle Entscheidungen zum Exposure Management auf Führungsebene.
Messmethode	Produkte und Plattformen zur Bewertung von Exposures berechnen das Cyber-Risikolevel eines Unternehmens auf Basis der Risiken durch einzelne Assets. Sie weisen jedem Asset in der IT-Umgebung eines Unternehmens einen Risiko-Score zu – basierend auf Faktoren, wie zum Beispiel: ■ Risikobewertungen der mit dem Asset verbundenen Exposures (wie oben beschrieben) ■ Zugänglichkeit des Assets (wie einfach ein Asset über einen externen oder internen Weg erreicht werden kann). ■ Kritikalität eines Assets (die Bedeutung eines Assets für das Unternehmen im Hinblick auf die potenziellen Auswirkungen eines Verlusts oder einer Gefährdung). Die Risiko-Scores einzelner Assets können anschließend aggregiert werden, um fundierte Entscheidungen auf der jeweils relevanten Ebene zu ermöglichen – sei es für das gesamte Unternehmen, eine bestimmte Geschäftseinheit oder eine Vertriebsregion. Die Skalen und Bedeutungen der Risiko-Scores unterscheiden sich je nach Anbieter, doch viele verwenden eine Skala von 0 bis 100 – ähnlich wie bei Tests oder Quizzen: Niedrigere Werte stehen für ein höheres Risiko und eine schwächere Sicherheitslage, höhere Werte hingegen für ein geringeres Risiko und eine solidere Sicherheitslage.

Verschaffen Sie Stakeholdern im Exposure Management zunächst ein Grundverständnis von Cyber-Risikolevel und Risikobereitschaft – bevor Sie offizielle Daten präsentieren. Nutzen Sie dazu diese Einführung in das Thema Exposure Management.

Prognostiziertes Cyber-Risikolevel	
Beschreibung	Das aktuelle Risikolevel eines Unternehmens ist nur ein Teil des Entscheidungsprozesses. Ebenso wichtig ist es, zu prognostizieren, wie sich eine bestimmte Entscheidung auf dieses Risikolevel auswirken könnte. ■ Liegt Ihr Cyber-Risiko über Ihrer Risikobereitschaft und würde die Behebung eines bestimmten Exposures Ihr Gesamtrisiko voraussichtlich in diesen Bereich (oder dessen Nähe) verschieben, lohnt sich eine genauere Prüfung dieser Maßnahme. ■ Eine Risikominderung sollte man auch dann erwägen, wenn ein Exposure – ohne entsprechende Maßnahmen – dazu führen könnte, dass das Risikolevel unterhalb der Risikobereitschaft des Unternehmens liegt. ■ Wenn ein Exposure keine wesentlichen Auswirkungen auf das Risiko hat – weder positiv noch negativ – kann es in der Regel akzeptiert und später neu bewertet werden. Während Metriken zum Cyber-Risikolevel für die Analyse auf einen Blick hilfreich sind – sie ermöglichen es Unternehmen, ihre aktuelle Situation schnell zu verstehen und zu signalisieren, wann Maßnahmen erforderlich sein könnten –, erfordern wichtige Entscheidungen eine weitergehende Analyse. Metriken wie die Annual Loss Expectancy (Jährliche Verlusterwartung) (siehe unten) können dabei helfen.
Messmethode	Die Prognose von Änderungen des Risikolevels auf der Grundlage empfohlener Abhilfemaßnahmen ist eine innovative Funktion, die in einigen Produkten und Plattformen zur Bewertung von Exposures zu finden ist. Prognosen werden erstellt, indem abgeschätzt wird, wie sich die Behebung eines Exposures auf die Faktoren auswirken würde, die in die Berechnung des aktuellen Cyber-Risikolevels eines Unternehmens einfließen (wie oben beschrieben).

Annual Loss Expectancy (Jährliche Verlusterwartung) (ALE)	
Beschreibung	Für Führungskräfte zählt eine klare Kommunikation in betriebswirtschaftlich nachvollziehbaren Begriffen. Die jährliche Verlusterwartung erfüllt genau diesen Zweck: Sie übersetzt das Risiko einer Gefährdung in konkrete monetäre Auswirkungen.
Messmethode	ALE wird durch Multiplikation der folgenden Variablen berechnet: ■ Single Loss Expectancy (Einzelverlusterwartung) (SLE) – ist ein Maß für die potenziellen Auswirkungen eines einzelnen Cyberangriffs auf das Unternehmen. Sie weist einem Angriff einen konkreten Geldwert zu, indem der Wert des betroffenen Assets mit dem prozentualen Verlust multipliziert wird, den eine Bedrohung verursachen könnte. ■ Die Annualized Rate of Occurrence (Jährliche Eintrittswahrscheinlichkeit) (ARO) – ein Maß für die Wahrscheinlichkeit – schätzt die Häufigkeit, mit der die Bedrohung innerhalb eines Jahres auftritt. Durch den Vergleich der aktuellen Annual Loss Expectancy (ALE) mit der verbleibenden ALE – also der geschätzten Verlusterwartung nach Umsetzung einer Risikominderungsmaßnahme – können Führungskräfte eine fundierte Kosten-Nutzen-Analyse vornehmen. Auf dieser Grundlage lässt sich entscheiden, ob ein Risiko aktiv angegangen oder bewusst akzeptiert werden soll. Wie bei den meisten Entscheidungen im Exposure Management sollte dabei stets die Risikobereitschaft des Unternehmens mitberücksichtigt werden.

In Ivantis E-Book Evaluating Cyber Risk Objectively: A Guide to Data-Driven Risk Assessments erhalten Sie eine Schritt-für-Schritt-Anleitung zur Verwendung von ALE und anderen Metriken, um fundierte Exposure-Management-Entscheidungen in Ihrem Unternehmen zu treffen. Anhand dieser Folien zum Risiko-Reporting können Sie Ihren Stakeholdern Ihre Bewertungen präsentieren.

Leistungsmetriken

Diese Metriken machen die Ergebnisse der Exposure-Management-Aktivitäten sichtbar. Ein nachweislich positiver Einfluss kann die Akzeptanz im Unternehmen stärken – und damit auch die Bereitschaft erhöhen, weiter in Exposure Management zu investieren.

Abgebaute Bedrohungsschulden (Threat Debts)	
Beschreibung	Sicherheitsteams erhalten nur selten Anerkennung für ihre proaktive Arbeit zum Schutz des Unternehmens. Viel zu häufig zeigt sich Wertschätzung erst in negativer Form – nämlich dann, wenn ein Sicherheitsvorfall eintritt und das Team im Krisenmodus reagieren muss. Exposure Management bietet das Potenzial, die Führungsebene stärker in Entscheidungen zur Cybersicherheit einzubinden – auch wenn dies typischerweise nur bei strategisch wichtigen Themen geschieht, etwa bei der Frage, ob eine „prominente“ Schwachstelle behoben oder in neue Sicherheitsmaßnahmen investiert werden soll. Über das Reporting zu abgebauten Bedrohungsschulden lässt sich zudem der volle Umfang der bereits geleisteten Arbeit im Bereich Exposure Management transparent darstellen. Bei den Metriken zu abgebauten Bedrohungsschulden ist ein wichtiger Punkt zu beachten: Sie sind aktivitätsbasiert, während es im Exposure Management vorrangig um Ergebnisse geht. Zwar zeigen sie auf, wie viel Arbeit ein Team geleistet hat – entscheidend ist jedoch, welche konkreten Resultate daraus entstanden sind.
Messmethode	Produkte und Plattformen zur Bewertung von Exposures sollten Daten liefern, die Sie zur Erstellung von Metriken für die abgebauten Bedrohungsschulden verwenden können. Diese Daten können in der Regel gefiltert werden, um bestimmte Aspekte zu verdeutlichen. Einige Beispiele: ■ Im 2. Quartal wurden 9.423 Malware-Instanzen beseitigt. ■ Im ersten Quartal wurden 399 Schwachstellen im Zusammenhang mit Ransomware behoben. ■ Verringerung der Zahl der kritischen Schwachstellen um 40 % im letzten Quartal.

Änderungen des Cyber-Risikolevels	
Beschreibung	Während die aktuellen und prognostizierten Cyber-Risikolevels als Richtschnur für kurzfristige Entscheidungen darüber dienen können, ob eine Gefährdung beseitigt werden soll, zeigen Veränderungen des Cyber-Risikolevels im Laufe der Zeit die langfristigen Auswirkungen dieser Entscheidungen. Ein messbarer Nachweis für die Effektivität des Exposure Managements ist die Fähigkeit, das Cyber-Risiko im Einklang mit der unternehmerischen Risikobereitschaft zu steuern und bei Bedarf zu minimieren. Die regelmäßige Überprüfung aktueller und zukünftiger Cyberrisiken gemeinsam mit Entscheidungsträgern auf Führungsebene sorgt dafür, dass Veränderungen – oder deren Ausbleiben – nachvollziehbar sind. Reports über Veränderungen des Cyberrisiko-Niveaus bieten zudem die Gelegenheit, zu zeigen, dass das Exposure Management wie vorgesehen greift.
Messmethode	Änderungen des Cyber-Risikolevels lassen sich auf unterschiedliche Weise messen und darstellen: ■ Absolute Veränderung (der genaue numerische Unterschied zwischen den Cyber-Risikolevels zu zwei unterschiedlichen Zeitpunkten – wenn das Cyber-Risikolevel beispielsweise am 1. Januar 72 und am 31. Dezember 83 betrug, ist das eine Veränderung von +11 im Laufe eines Kalenderjahres). ■ Prozentpunkte (der prozentuale Unterschied zwischen den Cyber-Risikolevels zu zwei verschiedenen Zeitpunkten – um beim obigen Beispiel zu bleiben, würde die Veränderung 15,3 % betragen, wenn die Risikolevels auf einer Skala von 0 bis 100 gemessen werden). ■ Liniendiagramm (zeigt das Cyber-Risikolevel zu verschiedenen Zeitpunkten und gibt Aufschluss über etwaige Trends, z. B. ob das Niveau generell steigt oder fällt). Einige Produkte und Plattformen zur Bewertung von Exposures stellen diese Daten automatisch auf Dashboards dar.

Return on Security Investment (Rentabilität der Sicherheitsinvestitionen) (ROSI)	
Beschreibung	Auch hier gilt: Führungskräfte möchten Dinge in betriebswirtschaftlichen Begriffen erklärt bekommen. Und kaum eine Metrik hat im Business-Kontext einen höheren Stellenwert als der Return on Investment (ROI). Return on Security Investment (ROSI) ist die Version des Sicherheitsteams, und es ist vielleicht das leistungsstärkste Tool in der Toolbox des Exposure Management Reporting. Durch die Zuordnung von Geldwerten zu den Exposure-Management-Maßnahmen können die Sicherheitsteams sowohl über den Wert einzelner Investitionen als auch über den kumulativen Wert aller Maßnahmen zum Exposure Management in einem bestimmten Zeitraum berichten.
Messmethode	Im Gegensatz zum traditionellen ROI, der die finanziellen Gewinne einer Investition ins Verhältnis zu ihren Kosten setzt, bewertet der ROSI die voraussichtlichen finanziellen Verluste, die durch eine Investition abgewendet wurden, relativ zu den entstandenen Kosten. Diese prognostizierten Verluste lassen sich mit angemessener Genauigkeit anhand einer Kombination aus unternehmensinternen historischen Daten und branchenspezifischer Forschung schätzen. Der traditionelle ROI wird berechnet, indem die Kosten einer Investition von ihrem aktuellen Wert abgezogen, durch die Kosten geteilt und dann mit 100 multipliziert werden, um einen Prozentsatz zu erhalten. Durch eine Änderung dieser Gleichung – die Änderung des aktuellen Werts einer Investition in den Wert der prognostizierten Verluste, die aufgrund einer oder mehrerer Investitionen abgewendet wurden – können Unternehmen den Return on Security Investment (ROSI) berechnen, um die finanziellen Auswirkungen von Investitionen in das Exposure Management zu messen.

Über Ivanti

Ivanti ist ein Anbieter von Unternehmenssoftware und bietet eine umfassende cloudbasierte Plattform für IT- und Sicherheitslösungen. Mit skalierbaren Softwarelösungen unterstützt Ivanti seine Kunden dabei, die Effizienz in IT und Sicherheit zu steigern, Kosten zu senken und Sicherheitsrisiken proaktiv zu minimieren. Die cloudnative Plattform Ivanti Neurons bildet das Fundament für einheitliche, wiederverwendbare Dienste und Tools. Sie ermöglicht eine konsistente Transparenz, hohe Skalierbarkeit und eine sichere Bereitstellung von Lösungen. Mehr als 34.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen mit den eigenen End-to-End-Lösungen zu meistern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter ivanti.com und folgen Sie @GoIvanti.

ivanti

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