BITSIGHT

Das Risikomanagement mit Sicherheitsbewertungen effektiver gestalten

ORGANISATIONALES BENCHMARKING UND BERICHTE FÜR DEN VORSTAND

DRITTPARTEI-RISIKOMANAGEMENT

ABSCHLUSS VON CYBERVERSICHERUNGEN UND BEWERTUNG DES GESAMTEN CYBERRISIKOS

ÜBERSICHT

Angesichts der zunehmenden Anzahl und Komplexität von Cyberbedrohungen und den täglichen Meldungen über Sicherheitsverstöße, steht das Cyberrisiko auf der Liste der bedeutendsten Risiken für Organisationen weit oben. Tatsächlich wurde Cybersicherheit (speziell Cybercrime, Datensicherheitslücken und IT-Ausfälle) laut einer Umfrage, die Allianz 2016 unter Sicherheitsexperten durchführte, als drittgrößtes Risiko für Organisationen identifiziert[1]. Das überrascht nicht, wenn man bedenkt, dass das Identify Theft Resource Center im Jahr 2016 980 schwerwiegende Verstöße registrierte,[2] bei denen Millionen Datensätze gefährdet oder kompromittiert wurden.

Auch wenn Cybersicherheit bei Führungskräften und Gesetzgebern höchste Priorität hat, ist es nach wie vor schwierig, Risikoniveaus zu bemessen und zu verwalten. Angesichts eines kontinuierlichen Stroms sich weiterentwickelnder Bedrohungen, geben viele Unternehmen jedes Jahr Millionen von Dollar für Mitarbeiter, Prozesse und Technologien aus, um sich gegen das Cyberrisiko zu schützen. Jedoch ist es außerordentlich schwierig festzustellen, wie effektiv diese Investitionen sind.

Die Lage ist noch schwieriger, wenn es darum geht, das Risiko beim Austausch sensibler Daten mit Dritten zu bemessen. Indem Funktionen wie Fertigung, Recht, Gehaltsabrechnung, Zahlungsabwicklung und Kundendienst häufig ausgelagert werden, können Unternehmen hunderte Geschäftspartner haben, mit denen sie zu jedem beliebigen Zeitpunkt zusammenarbeiten. Da sich der Trend zum Outsourcing so bald nicht ändern dürfte, wird das Drittpartei-Risikomanagement voraussichtlich noch an Bedeutung gewinnen.

In diesem Beitrag werden einige der Strategien in Bezug auf das Sicherheitsrisikomanagement besprochen, auf die Organisationen bisher zurückgreifen, sowie eine neue Strategie zu diesem zunehmenden Problem: BitSight Security Ratings. Risiko- und Sicherheitsexperten in mehr als 600 Organisationen setzen heute BitSight Security Ratings ein, um das Risiko in ihrem Ökosystem zu identifizieren, zu bemessen und zu mindern. Die folgenden drei spezifischen Anwendungsfälle werden in diesem Beitrag besprochen und so zusammengefasst.

1. Organisationales Benchmarking und Berichte für den Vorstand

Organisationen setzen BitSight Security Ratings ein, um ihr Cyberrisiko zu quantifizieren, die Wirkung von Initiativen zur Risikominderung zu messen und ihre Leistung mit anderen Unternehmen der Branche zu vergleichen. Viele Unternehmen setzen BitSight Security Ratings jetzt außerdem dafür ein, den Vorstand über Fortschritt und Ergebnisse in Bezug auf die Sicherheit in einer Sprache zu informieren, die Sicherheit und Risiko in den geschäftlichen Zusammenhang stellt.

[1] Allianz-Risikobarometer der größten Unternehmensrisiken im Jahr 2016
[2] Identity Theft Resource Center 2016 Übersicht über die Kategorien von Datensicherheitsverstößen

2. Drittpartei-Risikomanagement

BitSight Security Ratings helfen Organisationen das laufende Risiko beim Austausch von sensiblen Daten mit Drittparteien wie Geschäftspartnern, Lieferanten und Übernahmezielen schnell und kostengünstig zu identifizieren.

3. Abschluss von Cyberversicherungen und Bewertung des gesamten Cyberrisikos

Viele führende Anbieter von Cyberversicherungen setzen heute BitSight Security Ratings ein, um sich ein genaueres und kontinuierliches Bild des Cyberrisikos zu machen, dem Antragsteller wie auch Inhaber von Policen ausgesetzt sind.

„FRÜHER DAUERTE DIE BEWERTUNG VON LIEFERANTEN MEHRERE WOCHEN. HEUTE BRAUCHEN WIR DAFÜR NUR STUNDEN. BITSIGHT SECURITY RATINGS UNTERSTÜTZEN SICHERHEITSGESPRÄCHE MIT POTENZIELLEN LIEFERANTEN. SIE SIND EIN INTEGRALER BESTANDTEIL UNSERES PROGRAMMS FÜR DAS LIEFERANTENRISIKO-MANAGEMENT."

MICHAEL CHRISTIAN, INFORMATION SECURITY MANAGER OF CYBER RISK & COMPLIANCE BEI CABELA'S

MODERNER ANSATZ FÜR DAS RISIKOMANAGEMENT

Wie man der Häufigkeit und dem Umfang von Datensicherheitsverstößen entnehmen kann, ist niemand gegen einen Cyberangriff gefeit. Da sich Cyberbedrohungen schnell weiterentwickeln, kann ein Sicherheitsniveau, das heute hoch ist, morgen schon niedrig sein. So hat BitSight herausgefunden, dass fast 80 Prozent der Organisationen aller Branchen durch POODLE oder Logjam verwundbar sind, beides schwerwiegende SSL/TLS-Schwachstellen. Selbst wenn eine Organisation ein hohes Sicherheitsniveau hat, wird es häufig durch einen Drittanbieter oder einen Geschäftspartner gefährdet.

Die meisten Unternehmen managen das Sicherheitsrisiko heute im Rahmen ihrer allgemeinen IT-Praxis, häufig ohne dass andere Teile des Unternehmens daran beteiligt sind. Sie beschaffen Sicherheitsprodukte wie Firewalls, Einbruchserkennungssysteme sowie Security-Information- und Event-Management-Werkzeuge, um ihre Organisation zu schützen. Sie stellen interne Richtlinien für Mitarbeiter auf und helfen, sie darin zu schulen, sich selbst und die Organisation vor Phishing-Angriffen zu schützen. Sie verwenden Zeit und Ressourcen, um sicherzustellen, dass sie alle nötigen Branchenzertifizierungen erhalten und Konformitätsanforderungen der Branche erfüllen, wie zum Beispiel HIPAA, PCI und NIST oder die Europäische Datenschutzrichtlinie. Die Sicherheitsausgaben steigen weltweit von Jahr zu Jahr. Und doch nimmt trotz all dieser Anstrengungen die Häufigkeit von Cyberangriffen zu. Es gibt nur wenige objektive Kennzahlen, um den Sicherheitsstatus eines Unternehmens kontinuierlich zu messen und somit einschätzen zu können, ob er sich verbessert oder verschlechtert hat.

Es ist zudem eine Herausforderung, das Drittparteirisiko zu identifizieren, zu bewerten und darauf zu reagieren. Auch wenn immer mehr Unternehmen um das Risiko beim Austausch sensibler Daten mit Geschäftspartnern wissen, um dieses Risiko auch proaktiv und kontinuierlich zu identifizieren und zu verwalten fehlen oft die Mittel.

Ohne quantifizierte Basis, kontinuierliche Messung und Vergleichsdaten können Führungskräfte die Wirkung von Initiativen zur Risikominderung nicht messen und die Leistung im Vergleich zu anderen Unternehmen der Branchen nicht bewerten.

Führende Sicherheitsteams von Organisationen messen normalerweise heute den IT-Sicherheitsstatus von Partnern und Lieferanten, indem sie anhand von Anforderungschecklisten oder Fragebögen Daten erheben oder indem sie um die Bestätigung der Konformität mit einem branchengemäßen Standard durch eine Prüfstelle bitten. Indem diese Standards als Kompendium von Best Practices dienen, können sie als Grundlage für eine Messung gute Hinweise darauf geben, wo Ressourcen eingesetzt werden müssen. Sie sind auch ein guter Ausgangspunkt für die Beurteilung einer Drittpartei. Die Schwierigkeit liegt darin, dass die Verwendung allein dieser Methoden zur Bewertung eines Sicherheitsrisikos nicht ausreicht, wie die wachsende Zahl öffentlich gemachter Sicherheitsverstöße in Verbindung mit Geschäftspartnern zeigt.

Ein Unternehmen mag zwar alle einschlägigen Vorschriften einhalten und über ausgezeichnete Sicherheitsrichtlinien verfügen, schafft es aber eventuell nicht, diese Richtlinien im Alltag effektiv umzusetzen. Nur selten fällt bei einer Sicherheitsbewertung auf, wie viele kompromittierte Server ein Unternehmen zurzeit in seinem Netzwerk betreibt. Außerdem stellen die Ergebnisse einer Checkliste oder Prüfung nur den Status zum jeweiligen Zeitpunkt dar und können nicht den dynamischen Aspekt des Cyberrisikos erfassen, ganz egal, wie umfassend die Checkliste oder Prüfung ist. Selbst wenn ein Penetrationstest oder ein Schwachstellen-Scan durchgeführt wird, haben dessen Ergebnisse in der folgenden Woche schon keine Gültigkeit mehr.

Den Regulierungsbehörden ist die Schwäche der aktuellen Risikomanagementansätze nicht verborgen geblieben. 2014 hat das National Institute of Standards and Technology das Regelwerk „Framework for Improving Critical Infrastructure Cybersecurity“ herausgegeben, um Organisationen zu helfen, ihre Cyberrisiken besser verstehen, kommunizieren und managen zu können. Dieses freiwillige Regelwerk setzt auf die Verwendung von Geschäftsfaktoren zur Orientierung von Risikomanagement-Aktivitäten und geht auch auf die Notwendigkeit ein, das Drittparteirisiko zu bewältigen.

In seiner Semiannual Risk Perspective von 2016 äußerte das Office of the Comptroller of Currency (OCC) erneut seine Besorgnis in Bezug auf das Dritt- und Viertpartei-Cyberrisiko. Die Regulierungsbehörde, die 2013 eine Orientierungshilfe zum Drittpartei-Risikomanagement herausgegeben hatte, bezeichnete die Bewertung der Wirksamkeit von Drittpartei-Cyberrisikoprogrammen von Banken als „aufsichtsbehördliche Priorität“. Die Securities and Exchange Commission (SEC) hat ebenfalls Cybersicherheit als eine ihrer Prüfprioritäten für 2016 bezeichnet. SEC-Prüfer habe große Lücken in den Drittpartei-Risikomanagement-Initiativen von Organisationen festgestellt und machen dies bei künftigen Prüfungen eventuell zu einem Schwerpunkt. Die Regulierung nimmt nicht nur in der Finanzdienstleistungsbranche zu. Regulierungsbehörden wie das U.S. Department of Health & Human Services (HHS), die Federal Trade Commission und die Federal Energy Regulatory Commission (FERC) haben allesamt Durchsetzungsmaßnahmen besprochen oder verfolgt, wenn Programme zum Drittpartei-Risikomanagement nicht ordnungsgemäß umgesetzt wurden.

Die Durchführung einer Sicherheitsbewertung mit einer kontinuierlichen Beurteilung der Wirksamkeit der Sicherheitsmaßnahmen ermöglicht es den Unternehmen, ihre Einsicht in die Sicherheitsrisiken des erweiterten Unternehmens zu verbessern und die neuen Richtlinien und Vorschriften einzuhalten. Neben dem Einblick in die Schwachpunkte eines Netzwerks, kann eine datengestützte, evidenzbasierte Bewertung es den Unternehmen ermöglichen, neu auftretende Risiken proaktiv zu mindern und Probleme zu identifizieren, für deren Erfassung eine aufsichtsbehördliche Prüfung nicht ausgelegt wurde. Mit diesen

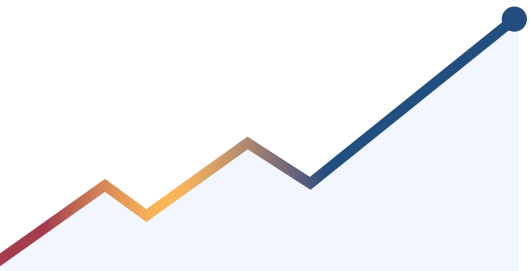
WAS GEHT IN EINE SICHERHEITSBEWERTUNG EIN?

KOMPROMITTIERTE SYSTEME (60 %)
+
SORGFALT (30 %)
+
BENUTZERVERHALTEN (10 %)
+
DATENSICHERHEIT-SVERSTÖSSE
=
BITSIGHT® SECURITY RATINGS

Schritten können Organisationen sich in Richtung eines reifen, risikobasierten Sicherheitsmodells zu bewegen und die simplere Auswahlkästchen-Mentalität aufgeben.

SICHERHEITSBEWERTUNGEN: EIN NEUER ANSATZ FÜR DAS RISIKOMANAGEMENT

Seit Jahren genießen Kreditrisikomanager die Vorteile, die Bonitätsbewertungen durch Auskunfteien bei Entscheidungen über Kreditvergabe, Investitionen oder Partnerschaften bieten. Diese Bewertungen sind standardisiert, verständlich und leicht zu verwenden, und sie basieren zumeist auf zuverlässigen Daten. Ebenso wie Kreditrisikomanager benötigen auch Sicherheitsrisikomanager datengestützte, objektive und vergleichbare Bewertungen, damit sie das Risiko besser verwalten können. Und hier kommen Sicherheitsbewertungen ins Spiel.



VIELE ORGANISATIONEN SIND SICH ÜBER DAS SICHERHEITSRISIKO, DEM SIE IN IHREN EIGENEN NETZWERKEN AUSGESETZT SIND, UND ÜBER DAS RISIKO, DAS IHRE GESCHÄFTSPARTNER EINFÜHREN, NOCH IMMER NICHT IM KLAREN.

BitSight Technologies hat den Branchenstandard für Sicherheitsbewertungen entwickelt. BitSight Security Ratings bieten ein objektives, datengestütztes Maß für den Sicherheitsstatus eines Unternehmens und geben Risikomanagern somit die Möglichkeit, Risiko im Zeitverlauf zu messen. Und hier kommen Sicherheitsbewertungen ins Spiel.

BitSight Security Ratings werden täglich erzeugt und liegen zwischen 250 und 900, wobei höhere Werte ein höheres Sicherheitsniveau bedeuten. Um diese Bewertungen zu erzeugen, erfasst und bewertet BitSight Terabytes allgemein verfügbarer Daten zum Sicherheitsverhalten an rund um die Welt verteilten Erfassungspunkten. Zur Bewertung eines Unternehmens werden unterschiedliche Datentypen verwendet, wie Daten zu kompromittierten Systemen, zur Sorgfalt in Bezug auf die Sicherheit, zum Benutzerverhalten und zu Datensicherheitsverstößen. Sämtliche Daten, die zur Erstellung einer Sicherheitsbewertung verwendet werden, sind extern verfügbar und werden ohne Einbruchstests bei einer Organisation erhoben.

Kompromittierte Systeme sind ein Beweis für erfolgreiche Cyberangriffe. Aufgrund der Offenheit und Vernetzung des Internets ist eine riesige Menge von Informationen verfügbar, aus denen man etwas über Sicherheitsniveaus erfahren kann. Kompromittierte Systeme, wie Malware-Verbreitung, Beteiligung an Distributed Denial of Service Attacks und Kommunikation mit einem bekannten Command-and-Control-Server eines Botnets können viel über die Dinge sagen, die in einer Organisation möglicherweise vor sich gehen. Viele dieser Bedrohungen wurden mit einer höheren Wahrscheinlichkeit für Datenverlust in Verbindung gebracht, und jede ist ein Hinweis darauf, dass die Organisation in irgendeiner Weise kompromittiert wurde und eingehender untersucht werden sollte.

Konfigurationsinformationen sind ein Maß dafür, wie sorgfältig ein Unternehmen bei der Risikominderung vorgeht. Eine ordentliche Konfiguration und frühzeitige Patches und Updates sind gut, um Sicherheitslücken zu vermeiden. Beispiele für Belege, die in dieser Kategorie gesammelt werden, sind etwa Sender-Policy-Framework-Datensätze, die Stärke der Verschlüsselung, offene Proxies und die Konfiguration des Netzwerks.

BITSIGHT SECURITY RATINGS ERMÖGLICHEN ES ORGANISATIONEN, IHR CYBERRISIKO ZU QUANTIFIZIEREN, DIE WIRKUNG VON INITIATIVEN ZUR RISIKOMINDERUNG ZU MESSEN UND IHRE LEISTUNG MIT DER ANDERER UNTERNEHMEN DER BRANCHE ZU VERGLEICHEN.

Benutzerverhalten repräsentiert jegliches mögliche Risiko, das mit den Aktionen von Benutzern in Unternehmensnetzwerken einhergeht. Ein Beispiel für riskantes Benutzerverhalten ist etwa die Nutzung von Peer-to-Peer-Tauschbörsen, wobei bösartige Software durch das Herunterladen einer kompromittierten Datei in das Netzwerk gelangen kann. Offengelegte Zugangsdaten von Mitarbeitern können ebenfalls ein Hinweis darauf sein, ob die privaten oder geschäftlichen Informationen der Mitarbeiter eines Unternehmens im Rahmen einer öffentlich bekannt gemachten Lücke kompromittiert wurden.

Datensicherheitsverstöße sind öffentlich bekannt gemachte Fälle von Datenverlust oder -diebstahl. Dazu zählen Daten, die aufgrund von erfolgreichen Angriffen, der Nachlässigkeit von Mitarbeitern oder des Diebstahls von Hardware verloren gegangen sind.

BitSight erhebt diese Daten kontinuierlich und analysiert sie auf Schwere, Häufigkeit, Dauer und Zuverlässigkeit. Die Sicherheitsbewertungen von Unternehmen und Branchen werden täglich aktualisiert und im BitSight-Kundenportal präsentiert. Wenn sich die Bewertung eines Unternehmens bedeutend ändert, werden Alarmmeldungen ausgegeben.

DREI WEISEN, AUF DIE MANAGER SICHERHEITSBEWERTUNGEN ZUR RISIKOMINDERUNG NUTZEN KÖNNEN

BitSight Security Ratings können im Rahmen des allgemeinen Risikomanagements auf vielerlei Weise verwendet werden. Viele Organisationen sind sich über das Sicherheitsrisiko, dem sie in ihren eigenen Netzwerken ausgesetzt sind, und über das Risiko, das ihre Geschäftspartner einführen, noch immer nicht im Klaren. Sie verfügen nicht über die Möglichkeiten, Risiko zu messen oder eine Strategie für kontinuierliches Risikomanagement umzusetzen. Glücklicherweise bieten BitSight Security Ratings einen kostengünstigen und kontinuierlichen Einblick in sich entwickelnde Risikoprofile.

Im Folgenden werden drei wichtige Weisen dargestellt, auf die Organisationen BitSight Security Ratings nutzen, um Risiken proaktiv zu verwalten:

1. Sicherheitsniveau bewerten

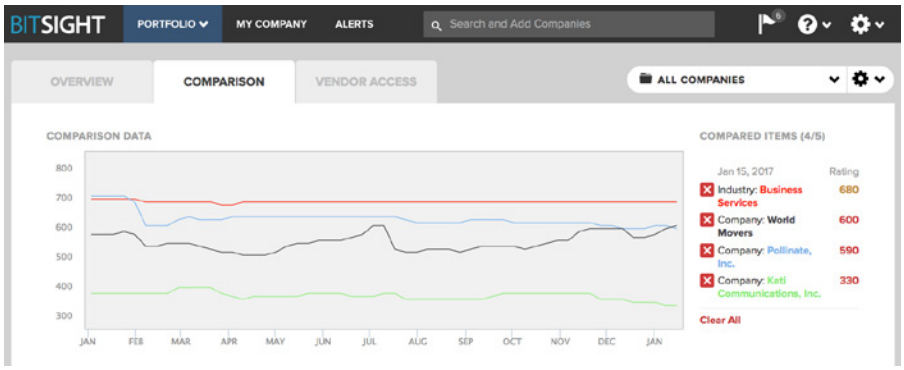
Im Finanzbereich wird die Unternehmensleistung mit Kennzahlen wie Bruttomarge, Gewinn pro Aktie und Kundenbindungsraten gemessen. Operative Abteilungen messen die Leistung anhand von Kennzahlen wie Betriebszeit, Latenz und für die Lösung von Kundendienstproblemen benötigte Zeit. Risikomanager hingegen haben keine standardisierten Kennzahlen für die Messung des Cyrerrisikos. Natürlich können sie sich die Zahlen zu Datensicherheitsverstößen und kompromittierten Rechnern ansehen. Sie können aber nicht erkennen, ob die Gesamtzahl kompromittierter Rechner weltweit ebenfalls gestiegen ist. Trotz der jüngsten Schlagzeilen werden nur sehr wenige Datensicherheitszwischenfälle öffentlich gemacht. Viele werden gar nicht erst erkannt.

BitSight Security Ratings ermöglichen es Organisationen ihr Cyberrisiko zu quantifizieren, die Wirkung von Initiativen zur Risikominderung zu messen und ihre Leistung mit der anderer Unternehmen der Branche zu vergleichen. Fragen, die anhand von BitSight Security Ratings beantwortet werden können, sind zum Beispiel:

- Wie hat sich mein Sicherheitsniveau in den letzten zwölf Monaten verändert?
- Wird mein Sicherheitsniveau besser oder schlechter?
- Wie stellt sich meine Leistung im Vergleich zum Branchendurchschnitt dar?
- Wie kann ich im Vergleich zu anderen Unternehmen der Branche und Wettbewerbsteilnehmern besser werden?

BitSight bietet eine detaillierte Sicht auf die eigenen Sicherheitsereignisse und -konfigurationen eines Unternehmens. Diese Einzelheiten können dazu dienen, Risikoquellen besser zu identifizieren und schnell Maßnahmen zu deren Abschwächung zu ergreifen. Alarmmeldungen zu bedeutenden Änderungen bei der eigenen Bewertung eines Unternehmens sind häufig frühe Warnhinweise für ein größeres Problem.

OB EINE ORGANISATION EINE HOHE ZAHL VON DRITTANBIETERN, POTENZIELLEN NEUKUNDEN, GESCHÄFTSPARTNERN ODER ÜBERNAHMEZIELEN VERWALTEN MUSS, EINE KONTINUIERLICHE MESSUNG IST VON ENTSCHEIDENDER BEDEUTUNG FÜR DAS VERSTÄNDNIS DES RISIKOS, DAS DAMIT EINHERGEHT, WENN MAN MIT IHNEN GESCHÄFTE MACHT.



Mit BitSight Security Ratings for Benchmarking erhalten Unternehmen Einblick in ihr Sicherheitsniveau im Vergleich zu anderen Unternehmen derselben Branche im Zeitverlauf.

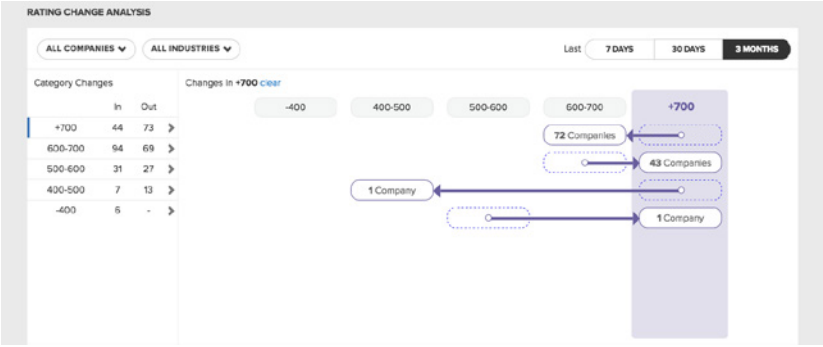
2. Durch Drittparteien bedingtes Risiko verwalten

Ob eine Organisation eine hohe Zahl von Drittanbietern, potenziellen Neukunden, Geschäftspartnern oder Übernahmezielen verwalten muss, eine kontinuierliche Messung ist von entscheidender Bedeutung für das Verständnis des Risikos, das damit einhergeht, wenn man mit ihnen Geschäfte macht.

BitSight Security Ratings helfen Organisationen, ein Risiko schnell und kostengünstig zu identifizieren, bevor ein Vertrag geschlossen wird und in der Folge dieses Risiko über die Dauer der Partnerschaft zu überwachen. Organisationen setzen Sicherheitsbewertungen ein, um zu bestimmen, welche Anbieter zuerst beurteilt werden müssen, welche eingehender beurteilt werden müssen sowie welche Partnerschaft beendet werden muss, da das Risiko unakzeptabel hoch ist. Durch die Unterstützung bei der Priorisierung können Organisationen ihre Ressourcen effizienter verwalten und somit durch Drittparteien bedingtes Risiko besser identifizieren, quantifizieren und mindern. Darüber hinaus können BitSight Security Ratings dabei helfen, die zunehmende Zahl von Vorschriften zum Drittpartei-Risikomanagement, wie HIPAA, OCC und PCI-DSS, durch eine proaktive und kontinuierliche Überwachung der Wirksamkeit der Sicherheitsvorkehrungen eines Drittanbieters einzuhalten. Schließlich kann das Portfolio Quality Dashboard von BitSight Einblick in das Gesamtrisiko Ihrer Drittparteien bieten und eine detaillierte Analyse davon liefern, welche Unternehmen sich in einer jüngeren Zeitspanne verbessert oder verschlechtert haben.

Sicherheitsrisikobewertungen sind immer häufiger auch Teil des Due-Diligence-Prozesses bei Fusionen und Übernahmen. In Bezug auf Übernahmeziele helfen BitSight Security Ratings, die Risiken zu identifizieren und die mit ihnen verbunden Kosten zur Risikominderung in die Gesamtkosten einer Übernahme und in den Integrationszeitplan einzubeziehen.

Organisationen können für Lieferanten auch den Zugang zum BitSight Security Ratings-Portal aktivieren und damit Drittparteien in die Lage versetzen, latente Probleme in ihren Netzwerken selbst zu beheben. Jedes Unternehmen erhält 14 Tage zusätzlichen Zugang zum BitSight-Portal mit forensischen Informationen, die es ihm erleichtern, Cyberbedrohungen in Netzwerken abzuwenden.



Anhand der Analyse von Bewertungsänderungen (Rating Change Analysis) können Sie feststellen, wie sich die Bewertungen eines Unternehmens in der letzten Woche, im letzten Monat oder in den letzten drei Monaten verändert haben. Kunden können Gruppen von Unternehmen bestimmen, die erhebliche Verschlechterungen der Bewertungen um mehr als eine Bewertungskategorie verzeichneten.

3. Das Bewusstsein vom Vorstand abwärts steigern

Viele CEOs und Unternehmensvorstände verlangen heute einen regelmäßigen Einblick in das Sicherheitsrisiko, das mit dem Ökosystem eines Unternehmens verbunden ist, daher benötigen die Praktiker im Bereich Datensicherheit eine Möglichkeit, ein Sicherheitsrisiko in geschäftlichen Begriffen zu kommunizieren. BitSights Dashboards für die Führungsebene dienen zunehmend der Schulung von Leitungsteams und liefern Daten als Grundlage für risikobasierte Entscheidungen. Sicherheitsbewertungen bieten Führungskräften eine leicht verständliche Sicht auf das Risikoniveau eines Unternehmens im Zeitverlauf und dazu, wie sich dieses Unternehmen im Vergleich mit anderen Unternehmen der Branche darstellt. Sie bieten ebenfalls eine Sicht auf das Risiko, das mit dem Austausch sensibler Daten mit Geschäftspartnern einhergeht. Mittels Sicherheitsbewertungen kann das Sicherheitsrisiko zu einem bedeutenden Element aller Geschäftsentscheidungen werden.

Darüber hinaus helfen detaillierte Berichte über die Aktivität, die einer Sicherheitsbewertung zugrunde liegt, das Bewusstsein bei IT-Sicherheitsmanagern zu erhöhen. Diese Berichte helfen, Ereignisse und Konfigurationsprobleme zu bestimmen, sodass Praktiker schnell reagieren und die Bedrohung mindern können.

SCHLUSS

Niemand ist vor einem Datensicherheitsverstoß gefeit, doch ist die effektive und kontinuierliche Überwachung von Cybersicherheitsrisiken ein wichtiger Schritt für Unternehmen jeder Größe und Branche zur Risikominderung. Die gute Nachricht ist, dass Unternehmen Cybersicherheit heute zu einem Thema für die Führungs- und die Vorstandsebene machen und die Notwendigkeit eines besseren Risikomanagements erkennen. Indem Cybersicherheit mehr Gewicht erhält und beim Risikomanagement mehr proaktive Sorgfalt herrscht, verzeichnen Organisationen, die BitSight Security Ratings nutzen, Verbesserungen bei ihrer Cybersicherheit. Kontinuierliche und datengestützte Sicherheitsbewertungen schließen eine Lücke, indem sie eine kontinuierliche Einsicht in die Risiken bieten, denen Organisationen ausgesetzt sind, und bringen sie bei der künftigen Risikoverwaltung und -minderung ein gutes Stück weiter.

ÜBER BITSIGHT TECHNOLOGIES

BitSight transformiert anhand von objektiven, nachprüfbaren und umsetzbaren Sicherheitsbewertungen die Weise, in der Unternehmen Datensicherheitsrisiken verwalten. Das 2011 gegründete Unternehmen hat seine Security Ratings Platform dafür entwickelt, immense Mengen externer Daten zu Sicherheitsproblemen zu analysieren. Sieben der zehn größten Anbieter von Cyberversicherungen, 80 Fortune-500-Unternehmen sowie drei der fünf größten Anlagebanken vertrauen bei der Verwaltung von Cyberrisiken auf BitSight.

FOR MORE INFORMATION

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com
sales@bitsighttech.com

„Wir können unsere Sicherheit mit der unserer Wettbewerber vergleichen. Wir können diese Informationen an unsere oberste Führung und den Vorstand weitergeben und sie dahingehend beruhigen, dass unser Programm planmäßig läuft.“