BITSIGHT

Cybersel

Une gestion des risques plus efficace grâce aux notations de sécurité

ANALYSE COMPARATIVE ET INFORMATION DU CONSEIL D'ADMINISTRATION

GESTION DES RISQUES RELATIFS AUX TIERS

CYBER-ASSURANCE ET EVALUATION DU CYBER-RISQUE GLOBAL

RESUME ANALYTIQUE

Alors que les cyber-menaces se font de plus en plus nombreuses et sophistiquées et que les atteintes à la sécurité deviennent quotidiennes, le cyber-risque figure dans le peloton de tête des menaces qui planent sur les entreprises. En fait, selon le baromètre 2016 des risques d'entreprise établi par Allianz[1], la cyber-sécurité (et notamment la cybercriminalité, les atteintes aux données et les pannes informatiques) a été identifiée comme le troisième risque le plus important pour l'entreprise. Rien de surprenant à cela : l'Identify Theft Resource Center a enregistré 980 violations majeures[2] en 2016, se traduisant par des millions d'enregistrements exposés ou compromis.

Si la cyber-sécurité se place désormais au centre des préoccupations des dirigeants et des autorités de contrôle, mesurer et gérer les niveaux de risque reste pourtant une tâche difficile. Face à un flux ininterrompu de menaces changeantes, de nombreuses entreprises dépensent chaque année des millions de dollars pour se protéger des cyber-risques à grands renforts de spécialistes, processus et technologies. Cependant, elles n'ont que peu de visibilité sur l'efficacité de ces investissements.

Et la situation se complique encore lorsqu'il s'agit de quantifier le risque que présente le partage de données sensibles avec des tiers. En effet, des fonctions telles que la production, le service juridique, la paie, le traitement des paiements et le service clients sont souvent externalisées ; les entreprises travaillent alors avec des centaines de partenaires distincts. Comme la tendance à l'externalisation n'est pas près de s'inverser, la gestion des risques liés aux tiers ne peut que gagner en importance.

Ce document présente certaines des méthodes de gestion des risques que les entreprises ont adoptées à ce jour, ainsi qu'une nouvelle approche du problème : les notations de sécurité BitSight Security Ratings. Aujourd'hui, les professionnels du risque et de la sécurité de plus de 600 entreprises font appel à BitSight Security Ratings pour identifier, quantifier et atténuer les risques dans leur environnement. Nous nous pencherons sur trois cas d'utilisation spécifiques, résumés ci-après.

1. Analyse comparative et information du conseil d'administration

Des entreprises utilisent BitSight Security Ratings pour quantifier leur cyber-risque, évaluer l'impact des actions de gestion des risques mises en œuvre et comparer leurs performances à celles de la concurrence. Nombre d'entre elles se servent également de BitSight Security Ratings pour informer leur conseil d'administration de l'évolution de la sécurité et des résultats obtenus dans des termes qui placent la sécurité et le risque dans un contexte opérationnel.

2. Gestion des risques relatifs aux tiers

BitSight Security Ratings permet aux entreprises d'identifier rapidement et à

[1] Allianz Risk Barometer Top Business Risks 2016
[2] Identity Theft Resource Center 2016 Data Breach Category Summary

moindre coût le risque permanent que représente le partage de données sensibles avec des tiers, qu'il s'agisse de partenaires commerciaux, de fournisseurs ou d'acquisitions potentielles.

3. Cyber-assurance et évaluation du cyber-risque global

De nombreux cyber-assureurs de premier plan utilisent maintenant BitSight Security Ratings pour évaluer de façon plus précise et en continu le cyber-risque identifié tant par les demandeurs que par les assurés.

APPROCHE ACTUELLE DE LA GESTION DES RISQUES

Comme le démontrent la fréquence et l'étendue des atteintes aux données, personne n'est à l'abri d'une cyber-attaque. En raison de l'évolution rapide des cyber-menaces, un système de sécurité aujourd'hui solide pourrait s'avérer insuffisant dans un futur proche. En fait, BitSight a découvert que près de 80 % des entreprises, tous secteurs confondus, n'étaient pas protégées contre les failles POODLE ou Logjam, qui sont des vulnérabilités SSL/TLS majeures. Même si les procédures de sécurité internes sont rigoureuses, le risque provient souvent d'un fournisseur ou d'un partenaire.

A l'heure actuelle, la plupart des entreprises gèrent les risques pour la sécurité dans le cadre de procédures informatiques globales, et souvent avec peu d'interaction de la part de leurs autres divisions opérationnelles. Dans le but de protéger leur activité, elles achètent des produits, tels que des pare-feu, des systèmes de détection d'intrusion et des outils de gestion des événements et des informations de sécurité (SIEM). Elles définissent des règles internes pour leurs collaborateurs et apprennent à ces derniers à se protéger et à protéger l'entreprise contre les tentatives d'hameçonnage. Elles consacrent également du temps et des ressources à s'assurer qu'elles disposent de toutes les certifications appropriées et qu'elles respectent les normes de conformité du secteur, telles que HIPAA, PCI et NIST, ou à la directive de l'Union européenne sur la protection des données. En conséquence, les dépenses de sécurité augmentent chaque année. Cependant, malgré tous ces efforts, la fréquence des cyber-attaques fait de même. Peu d'indicateurs objectifs permettent de mesurer l'éventuelle dégradation ou amélioration du système de sécurité d'une entreprise.

L'identification, l'évaluation et la résolution des risques imputables aux tiers posent également problème. Si de plus en plus d'entreprises sont conscientes des risques qu'elles encourent à partager leurs données sensibles avec des associés, et de la nécessité d'identifier et de gérer ces risques, les ressources pour le faire de façon proactive et continue leur font souvent défaut.

Sans base de référence quantifiée, ni mesures continues et données comparatives, il est impossible aux dirigeants d'évaluer l'incidence des procédures de réduction des risques, ou de mesurer la performance leur mode opératoire par rapport à la concurrence.

A l'heure actuelle, l'approche suivie par les équipes de sécurité les plus performantes dans les entreprises pour mesurer la situation de leurs partenaires et fournisseurs en la matière, consiste généralement à recueillir des renseignements par le biais

« AUTREFOIS, IL FALLAIT DES SEMAINES POUR EVALUER ENTIEREMENT NOS FOURNISSEURS. MAINTENANT, QUELQUES HEURES SUFFISENT. BITSIGHT SECURITY RATINGS FACILITE LES DISCUSSIONS SUR LA SECURITE AVEC DES FOURNISSEURS POTENTIELS. L'APPLICATION FAIT PARTIE INTEGRANTE DE NOTRE PROGRAMME DE GESTION DES RISQUES LIES AUX FOURNISSEURS. »

MICHAEL CHRISTIAN, RESPONSABLE DE LA SECURITE INFORMATIQUE CHARGE DU CYBER-RISQUE ET DE LA CONFORMITE CHEZ CABELA'S

d'une liste de critères ou d'un questionnaire, ou à demander une attestation de conformité aux normes du secteur établie par un auditeur. Certes, une comparaison établie sur la base d'un tel recueil de bonnes pratiques peut donner de précieuses indications pour allouer des ressources et établir le point de départ de l'évaluation d'un partenaire. Il n'en reste pas moins que ces seules méthodes ne suffisent pas à mesurer les risques pour la sécurité, comme en témoigne le nombre croissant de violations de la confidentialité impliquant des partenaires.

Une entreprise peut très bien respecter toutes les réglementations en vigueur et se doter d'excellentes règles de sécurité, mais se montrer inefficace dans la mise en œuvre de ces règles au quotidien. Il est rare qu'une évaluation de la sécurité permette de dénombrer les serveurs compromis présents sur le réseau d'une entreprise. En outre, aussi exhaustifs soient-ils, les résultats d'une liste de contrôle ou d'un audit ne sont qu'un reflet ponctuel de la situation et ne tiennent pas compte de la nature dynamique des cyber-risques. Même en cas de test d'intrusion ou d'analyse de vulnérabilité, les résultats peuvent ne plus être valables la semaine suivante.

La faiblesse des méthodes actuelles de gestion des risques n'a pas échappé aux autorités de contrôle. En 2014, le National Institute of Standards and Technology (NIST) a publié un cadre pour l'amélioration de la cyber-sécurité des infrastructures stratégiques (Framework for Improving Critical Infrastructure Cybersecurity). Ce cadre est destiné à aider les entreprises à mieux comprendre, décrire et gérer leurs cyber-risques. Ce système volontaire s'appuie sur le recours à des facteurs opérationnels pour orienter les tâches de gestion des risques. Il se penche également sur la nécessité de gérer les risques liés aux tiers.

Dans son rapport 2016 intitulé « Semiannual Risk Perspective », l'OCC (Office of the Comptroller of Currency, le bureau du Contrôleur de la monnaie des Etats-Unis) a réaffirmé ses inquiétudes concernant les cyber-risques liés aux prestataires externes. L'autorité de contrôle, qui avait formulé des directives sur la gestion des risques liés aux tiers en 2013, a indiqué que l'évaluation de l'efficacité des programmes bancaires pour la gestion des cyber-risques liés aux tiers constituait une priorité. La SEC (Securities and Exchange Commission) a également identifié la cyber-sécurité comme l'une de ses principales cibles d'examen en 2016. Ayant constaté de graves lacunes dans les actions des entreprises en matière de gestion des risques liés aux tiers, les vérificateurs de la SEC pourraient faire porter leurs efforts sur ce point lors de leurs futurs contrôles. Cependant, le secteur des services financiers n'est pas le seul à connaître un durcissement de la réglementation. Aux Etats-Unis, des autorités de contrôle telles que le ministère de la santé et des affaires sociales (HHS, U.S. Department of Health & Human Services), la Federal Trade Commission (FTC) et la Federal Energy Regulatory Commission (FERC), ont toutes envisagé ou exercé des mesures exécutoires en cas de non-application des programmes de gestion des risques liés aux tiers.

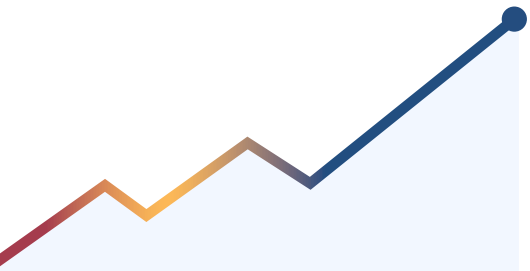
En complétant leur analyse de la sécurité par une évaluation continue de son efficacité, les entreprises pourront mieux cerner les risques qu'elles encourent dans un cadre étendu, et satisfaire aux nouvelles directives et réglementations. Outre le gain de visibilité sur les faiblesses d'un réseau, une évaluation effectuée à partir des données et reposant sur des éléments concrets peut aider les entreprises à limiter de façon proactive les nouveaux risques dès leur apparition et à identifier les problèmes qu'un audit réglementaire n'aura pas permis de détecter. C'est en appliquant ces mesures que les entreprises pourront s'affranchir de l'approche simpliste qui consiste à cocher des cases dans un formulaire pour passer à un modèle de sécurité évolué, fondé sur les risques.

QU'EST-CE QUI ENTRE DANS LA COMPOSITION D'UNE NOTATION DE SECURITE ?

SYSTEMES COMPROMIS (60 %)
+
DILIGENCE (30 %)
+
COMPORTEMENT DES UTILISATEURS (10 %)
+
ATTEINTE AUX DONNEES
=
BITSIGHT® SECURITY RATINGS

NOTATIONS DE SECURITE : UNE NOUVELLE APPROCHE DE LA GESTION DES RISQUES

Depuis des années, les gestionnaires du risque de crédit s'appuient sur les notations des agences d'évaluation du crédit pour prendre des décisions en matière de prêts, d'investissements et de partenariats. Normalisées, ces notations sont faciles à comprendre et à utiliser et reposent en général sur des données fiables. A l'instar de ces gestionnaires, leurs homologues chargés de la sécurité ont besoin de notations objectives et comparables, fondées sur les données, pour mieux gérer les risques. C'est là que les notations de sécurité entrent en jeu.



En termes de notations de sécurité, c'est BitSight Technologies qui a mis au point la norme du secteur. BitSight Security Ratings fournit une évaluation objective et fondée sur les données des performances d'une entreprise en matière de sécurité. Cette évaluation permet ainsi aux gestionnaires du risque de mesurer ce dernier dans le temps. C'est là que les notations de sécurité entrent en jeu.

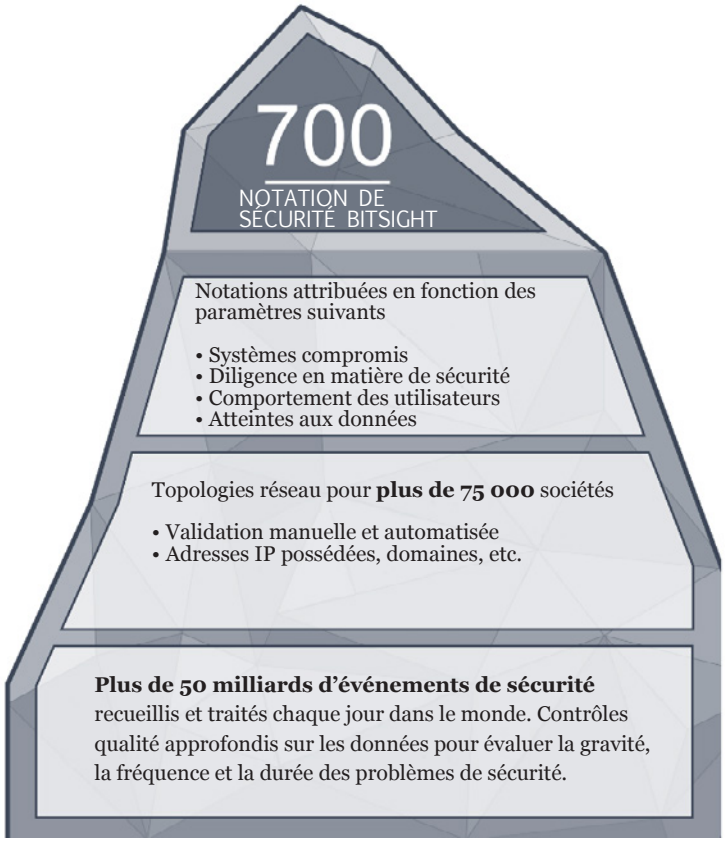
Générées quotidiennement, les notations BitSight Security Ratings s'échelonnent de 250 à 900, les notations les plus élevées traduisant de meilleures performances de sécurité. Pour générer ces notations, BitSight recueille et évalue des téraoctets de données publiques sur les comportements de sécurité, à partir de points de collecte disséminés sur la planète. Divers types de données sont utilisés pour évaluer une entreprise : données sur les systèmes compromis, diligence en matière de sécurité, comportements des utilisateurs et atteintes aux données. Toutes les données utilisées pour générer une notation de sécurité sont disponibles en externe et collectées auprès d'une l'entreprise de façon non intrusive.

DE NOMBREUSES ENTREPRISES IGNORENT ENCORE TOTALEMENT LE NIVEAU DE RISQUE AUQUEL SONT CONFRONTES LEURS PROPRES RESEAUX, AINSI QUE LES RISQUES INTRODUITS PAR LEURS PARTENAIRES.

Les systèmes compromis sont la preuve de cyber-attaques réussies. Etant donné la nature ouverte et interconnectée d'Internet, une quantité considérable d'informations est disponible sur les comportements de sécurité. Les systèmes compromis, notamment via la diffusion de logiciels malveillants, la participation à une attaque par déni de service distribué (DDoS, Distributed Denial of Service) et la communication avec le serveur de commande et de contrôle d'un botnet, témoignent des types d'activité susceptibles d'avoir lieu au sein même d'une organisation. Un grand nombre de ces menaces est associé à un risque élevé de perte de données et chacune dénote que l'entreprise a été compromise d'une manière ou d'une autre, et doit donc être soumise à un examen plus approfondi.

Les informations de configuration permettent d'évaluer la diligence d'une entreprise pour réduire les risques. De fait, une configuration appropriée ainsi que des correctifs et mises à jour réguliers constituent de bonnes pratiques dans la lutte contre les failles de sécurité. Les éléments objectifs réunis dans cette catégorie comprennent, par exemple, les enregistrements SPF (Sender Policy Framework), le niveau de chiffrement, les serveurs proxy ouverts et la configuration du réseau.

BITSIGHT SECURITY RATINGS FOR BENCHMARKING PERMET AUX ENTREPRISES DE QUANTIFIER LEUR CYBER-RISQUE, D'EVALUER L'INCIDENCE DES ACTIONS DE GESTION DES RISQUES MISES EN PLACE ET DE COMPARER LEURS PERFORMANCES A CELLES DE LA CONCURRENCE.



Le comportement des utilisateurs représente les risques potentiels découlant des actions des employés sur les réseaux de l'entreprise. Ainsi, les comportements à risque incluent le partage de fichiers de pair à pair, qui peut introduire des logiciels malveillants dans les réseaux via le téléchargement d'un fichier infecté. La divulgation de certains identifiants peut également être le signe que les informations personnelles ou professionnelles des employés d'une société ont été dévoilées à la suite d'une fuite dans le domaine public.

Les événements d'atteinte aux données sont des incidents publiquement divulgués qui impliquent la perte ou le vol de données. Il peut s'agir de données perdues à la suite d'attaques ayant abouti, d'une négligence des employés ou d'un vol de matériel.

BitSight recueille des données de ce type en continu et les analyse pour déterminer leur gravité, leur fréquence, leur durée et leur fiabilité. Les notations de sécurité des entreprises et des secteurs d'activité sont mises à jour quotidiennement sur la base des données les plus récentes, et sont présentées sur le portail clients BitSight Customer Portal. Des alertes sont générées en cas de variations importantes de la notation d'une société.

TROIS USAGES DES NOTATIONS DE SECURITE A LA DISPOSITION DES RESPONSABLES POUR REDUIRE LES RISQUES

Les notations BitSight Security Ratings peuvent être utilisées de diverses façons dans le cadre d'une gestion globale des risques. De nombreuses entreprises ignorent encore totalement le niveau de risque auquel sont soumis leurs propres réseaux, ainsi que les risques qu'induisent leurs partenaires. Elles ne disposent pas des

ressources nécessaires pour mesurer le risque ou pour mettre en œuvre une stratégie de gestion continue en la matière. Fort heureusement, BitSight Security Ratings constitue une méthode économique et stable de renseignement sur des profils de risque fluctuants.

Voici trois axes majeurs de gestion proactive des risques pour les entreprises qui adoptent BitSight Security Ratings :

1. Analyser les performances de sécurité

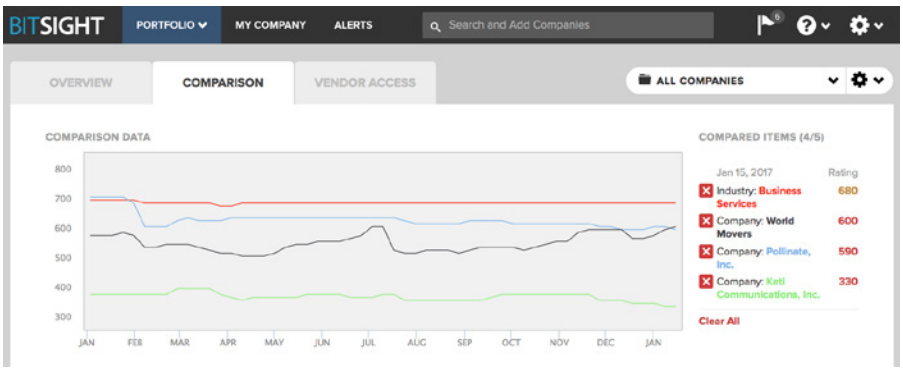
Les groupes financiers mesurent les performances d'une entreprise à l'aide d'indicateurs tels que la marge brute, le bénéfice par action et le taux de fidélisation de la clientèle. Les services opérationnels, eux, basent leurs mesures sur des indicateurs tels que la disponibilité, la latence et le délai de résolution des problèmes des clients. En revanche, les gestionnaires des risques ne disposent d'aucune métrique standard pour évaluer les cyber-risques. Certes, ils peuvent prendre en compte le nombre d'atteintes aux données et de machines compromises. Mais ils n'ont aucun moyen de savoir si le nombre total de machines compromises au niveau mondial a également augmenté. En effet, malgré l'actualité récente, très peu de violations de la sécurité sont rendues publiques. Un grand nombre ne sont même jamais détectées.

BitSight Security Ratings for Benchmarking permet aux entreprises de quantifier leur cyber-risque, d'évaluer l'impact des efforts de gestion des risques mis en place, et de comparer leurs performances à celles de la concurrence. BitSight Security Ratings apporte une réponse aux questions suivantes, entre autres:

- Comment mes performances de sécurité ont-elles évolué sur les 12 derniers mois ?
- Mes performances de sécurité sont-elles en hausse ou en baisse ?
- Où se situent mes performances par rapport à la moyenne du secteur ?
- Comment mon entreprise se classe-t-elle par rapport à ses homologues et concurrents ?

BitSight permet à une entreprise de visualiser dans le détail ses événements et configurations de sécurité. De telles informations peuvent alors servir à mieux identifier les sources de risque et à prendre rapidement des mesures pour y remédier. Les alertes déclenchées par des variations importantes de la notation d'une entreprise constituent souvent le signe avant-coureur d'un problème plus grave.

LORSQU'UNE ENTREPRISE DOIT GERER UNE PLETHORE DE FOURNISSEURS, DE NOUVEAUX CLIENTS POTENTIELS, DE PARTENAIRES OU DE CIBLES D'ACQUISITION, UNE EVALUATION CONTINUE S'AVERE ESSENTIELLE POUR COMPRENDRE LES RISQUES ASSOCIES A TOUTES CES RELATIONS COMMERCIALES.



BitSight Security Ratings for Benchmarking permet aux entreprises de se faire une idée de leurs performances de sécurité par rapport à la concurrence.

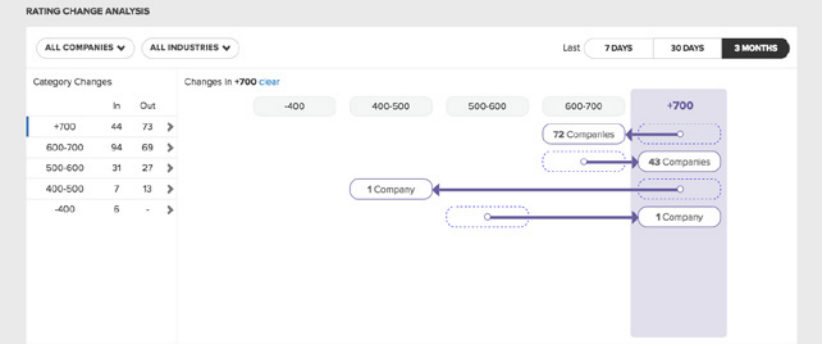
2. Gérer les risques induits par les tiers

Lorsqu'une entreprise doit gérer une pléthore de fournisseurs, de nouveaux clients potentiels, de partenaires ou de cibles potentielles d'acquisition, une évaluation continue s'avère essentielle pour comprendre les risques associés à toutes ces relations commerciales.

BitSight Security Ratings aide les entreprises à identifier les risques rapidement et au meilleur coût, avant la signature d'un contrat, puis à exercer une surveillance continue pendant toute la durée du partenariat. Les entreprises utilisent ainsi les notations de sécurité pour déterminer les fournisseurs à évaluer en premier, ceux à examiner de façon plus détaillée et les partenariats auxquels elles doivent mettre un terme en raison de niveaux de risque inacceptables. En établissant un ordre de priorité, les notations permettent aux entreprises de gérer plus efficacement leurs ressources afin de mieux identifier, quantifier et réduire les risques associés aux tiers. En outre, BitSight Security Ratings contribue à se mettre en conformité avec le nombre croissant de réglementations relatives à la gestion des risques liés à des tiers (HIPAA, OCC et PCI-DSS, par exemple), grâce à une surveillance proactive et constante de l'efficacité de leur sécurité. Enfin, le Portfolio Quality Dashboard de BitSight peut donner un aperçu des risques cumulés que posent vos partenaires, avec une analyse détaillée des entreprises ayant récemment connu une amélioration ou un recul.

Les évaluations des risques pour la sécurité font également de plus en plus partie intégrante du processus d'obligation de vigilance des fusions-acquisitions. Pour les acquisitions potentielles, BitSight Security Ratings contribue à identifier les risques et à intégrer au coût global du processus d'acquisition et d'intégration les coûts des mesures de gestion et réduction des risques nécessaires.

Les entreprises peuvent également autoriser l'accès de leurs prestataires et partenaires au portail BitSight Security Ratings, leur permettant ainsi de remédier eux-mêmes aux problèmes non encore résolus sur leurs réseaux. Chaque société bénéficiera alors de 14 jours d'accès gratuit au portail BitSight, notamment à des informations analytiques facilitant la lutte contre les cyber-menaces qui touchent les réseaux.



La fenêtre Rating Change Analysis vous permet de repérer toute modification des notations au cours de la semaine, du mois ou du trimestre précédent. Les clients peuvent ainsi identifier les groupes d'entreprises dont les notations ont considérablement chuté.

A PROPOS DE BITSIGHT TECHNOLOGIES

La société BitSight révolutionne la façon dont les entreprises gèrent les risques pour la sécurité de leurs informations. Pour ce faire, elle leur fournit des notations de sécurité objectives, vérifiables et exploitables. Fondée en 2011, la société a développé sa plateforme Security Ratings dans le but d'analyser en continu d'énormes quantités de données externes portant sur les problèmes de sécurité. Sept des dix plus grandes compagnies de cyber-assurance, 80 entreprises du classement Fortune 500 et trois des cinq plus importantes banques d'investissement font confiance à BitSight pour la gestion des cyber-risques.

3. Sensibiliser tous les échelons de l'entreprise à la gestion des risques

De nombreux PDG et conseils d'administration exigent désormais d'être régulièrement informés des risques pour la sécurité dans tout l'écosystème de leur entreprise. Les spécialistes de la sécurité doivent donc être capables de communiquer sur ces risques selon un point de vue opérationnel. Les tableaux de bord de BitSight destinés aux dirigeants sont de plus de plus utilisés pour éduquer les équipes de direction et leur fournir les données qui leur permettront de prendre des décisions en fonction des risques. Avec les notations de sécurité, les cadres peuvent bénéficier d'une vision facilement compréhensible du niveau de risque de leur société dans le temps, et de sa position par rapport à la concurrence dans le même secteur d'activité. Ils bénéficient également d'un aperçu des risques induits par le partage de données sensibles avec des partenaires commerciaux. Ainsi, grâce aux notations de sécurité, les risques deviennent une composante essentielle à toutes les décisions métier.

En outre, des rapports détaillés présentant l'activité fondamentale à une notation de sécurité contribuent à sensibiliser les responsables de la sécurité informatique. Ces rapports font ressortir les événements et problèmes de configuration, et permettent ainsi aux spécialistes de réagir rapidement pour combattre la menace.

CONCLUSION

Personne n'est à l'abri d'une atteinte aux données, mais une surveillance continue efficace constitue, quels que soient la taille et le secteur d'activité de l'entreprise, une étape importante dans la lutte contre les risques pour la cyber-sécurité. Point positif, aujourd'hui les dirigeants et conseils d'administration des entreprises sont conscients de l'importance d'une meilleure gestion des risques, et placent désormais la cyber-sécurité en tête des priorités. En mettant davantage l'accent sur la cyber-sécurité et en s'attaquant à bras-le-corps à la gestion des risques, les entreprises qui utilisent BitSight Security Ratings constatent des améliorations de leur santé informatique. Menées en continu et fondées sur les données, les notations de sécurité comblent une lacune en fournissant des informations régulières sur les risques actuels encourus par les entreprises, et contribuent largement à gérer et à réduire les risques à venir.

« Nous sommes en mesure de comparer notre niveau de sécurité à celui de nos concurrents. Nous pouvons partager ces informations avec nos dirigeants et notre conseil d'administration, leur donnant ainsi l'assurance que notre programme est sur la bonne voie ».

FOR MORE INFORMATION

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com
sales@bitsighttech.com

A propos de Cybersel

Cybersel est un leader de solutions de Cyber Sécurité. Cybersel a supporté le projet BitSight dès le début et est actuellement un des partenaires de BitSight Security Ratings les plus expérimentés dans la zone EMEA.

Contact France :
Alain Melamed - Tel : +33 6 80 74 13 16
Email : alain.melamed@cybersel.eu

Contact Italie :
Davide Turina Tel :+39 3494603846
Email : davide.turina@cybersel.eu

Cybersel Srl
Via Lessolo 3
10153 TORINO - ITALY
tel: +39 011 2481121
www.cybersel.eu