IBM Security

IBM

L'entrée en vigueur du RGPD approche à grands pas. Etes-vous prêts ?

L'adoption du Règlement général sur la protection des données a des répercussions au niveau mondial

Livre blanc IBM Security

La nouvelle législation impose d'importantes mesures de protection des données personnelles

Impossible d'y échapper : c'est la loi. Voté en mai 2016, le Règlement général de l'Union européenne (UE) sur la protection des données (RGPD) remplace la directive sur la protection des données, moins contraignante, qui permettait depuis 21 ans aux 28 Etats-membres de l'UE de fixer leurs propres règles de protection de la confidentialité et de la sécurité des données. Avec l'ancienne directive, la validité et la puissance des lois variaient d'un pays d'Europe à l'autre. Ce ne sera plus le cas à compter du 25 mai 2018.

A partir de cette date, toutes les organisations devront respecter les mêmes obligations en matière de protection des données. Ou s'exposer à de fortes amendes. Pourquoi avoir adopté le RGPD ?

- **Evolution des utilisateurs et des données.**
Les utilisateurs sont de plus en plus nombreux et divers et leurs actions se multiplient. C'est vrai aussi pour les données. La quantité et la diversité des informations collectées et stockées par les organisations montent en flèche. Les informations stratégiques devraient être protégées, mais on ignore souvent où elles se trouvent, quels utilisateurs y ont accès et à quel moment, ou ce qu'il advient des données après les avoir consultées.

- **Evolution de l'accès aux données et de leur traitement.**
Le cloud, les réseaux sociaux, les cartes à puce et les divers appareils numériques et mobiles ont ouvert la voie à de nombreuses menaces pour la sécurité des données. Face à ces changements qui concernent la planète entière, l'UE a reconnu dans ses textes que « la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. »[1]

« Les entreprises qui exercent leur activité en Europe ou qui ciblent une clientèle européenne doivent s'organiser et commencer à se préparer au nouveau système. »
—The Register, *UK*[2]

▸ Lire l'introduction au RGPD par un spécialiste de la législation sur le respect de la vie privée.

1 Article 1. « Règlement (UE) 2016/679 du Parlement européen et du Conseil, » 27 avril 2016.

2 John Leyden, « Enfin approuvées, les nouvelles mesures de protection de la confidentialité doivent s'appliquer aux pays de l'UE d'ici 2018, » *The Register*, 14 avril 2016.

Conséquences du RGPD à l'échelle mondiale et sur le plan financier

Si l'Europe se préoccupe depuis longtemps déjà du respect de la vie privée, ce n'est pas le cas dans d'autres régions du monde où les contrôles sont nettement moins contraignants. Désormais, un tel laxisme n'aura plus cours, le RGPD s'appliquant à toutes les sociétés qui collectent les données personnelles de résidents de l'Union européenne comme à celles qui font des affaires dans l'UE. Pour elles, la mise en conformité avec le RGPD est une obligation, quelle que soit leur situation géographique. Peu importe le lieu où les données sont envoyées, traitées ou enregistrées : le RGPD impose que les informations personnelles soient protégées. L'objectif premier est de permettre à chaque individu de mieux contrôler et connaître les données personnelles qui le concernent.

Pour permettre un tel contrôle, le RGPD inclut deux éléments essentiels :

- ***Non-conformité :***
  Application d'une amende administrative pouvant atteindre 20 millions d'euros (soit près de 22,3 millions de dollars) ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.[1]

- ***Notification :***
  En cas de détection d'une violation des données, la société doit la signaler à l'autorité de contrôle « dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après en avoir pris connaissance. »[2]

Dit simplement, le RGPD inclut des exigences importantes en matière de sécurité et d'opérations informatiques et son non-respect entraîne un risque d'impact financier important pour l'entreprise.

Des informations concernant 157 000 clients ont été piratées lors d'une attaque visant un fournisseur britannique de téléphonie et de services haut débit.[3]

▸ Afficher le webinaire IBM sur le RGPD.

1 Article 83, 5. « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016.

2 Article 85. « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016.

3 Sean Farrell, « Nearly 157,000 had data breached in TalkTalk cyber-attack, » (Près de 157 000 personnes se font pirater des données dans une cyberattaque contre TalkTalk) *The Guardian*, 3 novembre 2015.

Augmentation du nombre et du coût des violations de données

Seulement 72 heures pour détecter une violation des données et la signaler aux autorités ?

Pas facile ! Selon certaines études, le délai moyen nécessaire pour identifier une violation des données est de 201 jours, et le délai moyen de résolution du problème de 70 jours.[1] Et plus il faut de temps pour détecter et endiguer une violation, plus l'opération risque d'être coûteuse.

Entre 2015 et 2016, le coût moyen d'une violation des données est passé de 3,79 à 4 millions de dollars.[1] Si l'on ajoute à cela l'amende pour non-respect d'une disposition du RGPD ayant conduit à la violation, les conséquences peuvent être vertigineuses.

Les risques pour les données personnelles, financières ou autres, ne faiblissent pas. Chaque jour, des cybercriminels inventent, développent et introduisent inlassablement de nouvelles menaces toujours plus sophistiquées. En fait, une enquête mondiale a montré que les sociétés étudiées présentaient 26 % de risque de subir une ou plusieurs violations impliquant la perte ou le vol de 10 000 enregistrements dans les 24 prochains mois.[1]

Et pourtant, nombreuses sont les organisations qui n'ont pas conscience de la vulnérabilité de leurs données, ni des conséquences d'une violation. Faute de prendre la mesure de la menace, elles ne prennent pas la peine d'identifier les risques et de réparer les failles.[2] Une erreur de jugement qui peut s'avérer coûteuse.

100 banques de 30 pays ont perdu 1 million de dollars en deux ans dans des attaques coordonnées.[2]

- Pour plus d'informations sur l'impact d'une violation des données, lire le dernier rapport Ponemon.

1 « 2016 Cost of Data Breach Study: Global Analysis, » (Etude 2016 sur le coût des violations des données : analyse mondiale), enquête de référence commanditée par IBM, *Ponemon Institute*, juin 2016.

2 « IBM X-Force Threat Intelligence Report 2016, » (Rapport 2016 IBM X-Force sur la connaissance des menaces) *IBM Corp.*, février 2016.

Mise en conformité avec le RGPD : c'est le moment d'agir

Toutes les sociétés ont besoin d'une stratégie de protection des données. La correction des failles de sécurité des référentiels de données, selon le service de R&D IBM® X-Force®, doit être incluse dans les bonnes pratiques élémentaires de toute organisation.[1] Cela passe par la mise en œuvre d'un plan multiniveau détaillé permettant de connaître la façon dont les données sont acquises, consultées, enregistrées et protégées. Il faut aussi intégrer et utiliser les meilleures connaissances et les meilleures solutions possibles. Le temps et l'argent consacrés à la mise en œuvre d'une solide stratégie de protection à l'échelle de l'entreprise constituent également un bon investissement en vue de la mise en conformité avec le RGPD.

Partout dans le monde, les autorités ont adopté une règlementation sur la protection des données dans divers secteurs, notamment la santé, la gestion financière et les entreprises de consommation. L'objectif est le même que celui du RGPD : protéger les données sensibles[1]. Les organisations qui ont alloué le budget, le temps et les solutions nécessaires au respect des réglementations existantes pourront s'appuyer sur les programmes de protection déjà en place pour faire face à leurs obligations en vertu du RGPD.

Dès aujourd'hui, les entreprises européennes, mais aussi les sociétés internationales qui travaillent dans l'UE ou pour des habitants des Etats-membres de l'UE, doivent comprendre qu'il est nécessaire d'agir. En effet, toute organisation traitant des données personnelles (ne serait-ce que celles de ses salariés) est concernée par le RGPD.

96 000 failles de sécurité ont été documentées dans la base de données IBM X-Force au niveau mondial.[1]

▶ Regarder la vidéo IBM sur les dix pratiques de sécurité essentielles.

1 « IBM X-Force Threat Intelligence Report 2016, » (Rapport 2016 IBM X-Force sur la connaissance des menaces) *IBM Corp*., février 2016.

Une compagnie d'assurance italienne garantit la conformité des accès

Dotée d'énormes magasins de données, l'une des plus importantes compagnies européennes d'assurance, de services bancaires et de gestion des investissements était confrontée à un dilemme. Elle avait mis en place une solution de gestion des identités pour attribuer et supprimer les privilèges d'accès, mais son outil « sur mesure » d'accès et de recertification ne suivait pas. Il était incapable d'évoluer pour prendre en charge de nouvelles applications ou de nouveaux utilisateurs, et peu d'employés savaient l'utiliser.

Pour faire face à ses obligations en matière de confidentialité et de réalisation d'audits internes et respecter de la loi italienne 196 sur la confidentialité des données, la société a commencé à rechercher une solution avec de puissantes fonctions de certification des identités et des accès.

Après avoir examiné les solutions possibles, elle a déployé pour ses 75 000 utilisateurs une solution IBM Security Identity Governance and Intelligence intégrée. L'interopérabilité de la solution avec les applications SAP (et autres) existantes et le système mainframe a permis de répondre aux besoins de la société en termes de gain de temps et d'argent, de conformité et de sécurité.

En reliant plusieurs perspectives (conformité, gestion et TI) et en simplifiant les processus de certification des rôles et des accès utilisateur, la solution IBM Security Identity Governance and Intelligence a permis de réduire la vulnérabilité aux risques et de limiter les violations de la stratégie de la société. Elle contribue au respect de la loi italienne 196 sur la confidentialité et de la loi 262 (l'équivalent de la loi Sarbanes-Oxley aux Etats-Unis) sur la gouvernance d'entreprise.

Avantages de la solution IBM pour la compagnie d'assurance :

- *Amélioration du contrôle des processus de réduction du risque et de conformité des accès*
- *Respect accru des obligations en matière de confidentialité*

Lire le livre blanc IBM sur l'importance de la gestion des identités pour la mise en conformité.

Une banque verrouille l'accès de ses employés aux données des clients

Lorsqu'un audit avait conclu qu'elle ne protégeait pas suffisamment les informations confidentielles de ses clients, cette banque régionale avait compris qu'il lui fallait des fonctionnalités plus puissantes pour limiter les accès et éviter toute violation des données. Il était impératif qu'elle restreigne, et même qu'elle fasse cesser, certaines pratiques : pour les administrateurs informatiques, le partage de l'accès aux applications des clients, et pour les différentes branches, l'utilisation de feuilles de calcul différentes pour le suivi des informations. Les failles qui existaient dans le contrôle des accès avaient même permis à un ancien salarié d'accéder aux données d'un client et de les récupérer.

Pour protéger les informations d'identification et gérer l'accès des administrateurs aux données sensibles, la banque a déployé la solution IBM Security Privileged Identity Manager. Avec ce système, lorsqu'un administrateur a besoin d'accéder aux données, l'agent intégré à la solution vérifie les informations d'identification et, si l'utilisateur est approuvé, le connecte automatiquement à l'application sans jamais dévoiler le mot de passe. A la fin de la session, le mot de passe est modifié.

La banque a également déployé IBM Security Guardium® afin de pouvoir suivre en temps réel l'accès aux données par les utilisateurs dotés de privilèges, et vérifier que les accès avec un identifiant partagé entraient dans le cadre des permissions définies pour l'utilisateur en question. S'il détecte une violation des règles d'accès, Guardium envoie une alerte à IBM QRadar® SIEM, qui intègre la gestion des informations et des événements de sécurité à des fins de détection des anomalies inter-entreprises, le diagnostic des incidents, la résolution des incidents et la gestion des vulnérabilités.

Avantages d'IBM pour la banque :

- *Simplifie le contrôle et le suivi des accès avec ID partagé*
- *Réduit les coûts d'exploitation*
- *Evite les violations de données préjudiciables*
- *Simplifie les audits par des enregistrements d'audit consolidés*

▸ Plus d'informations sur IBM Security Privileged Identity Manager et Guardium sur le Web.

Des solutions IBM Security garantes de la conformité au RGPD

Le RGPD change la donne pour les entreprises du monde entier. A minima, les obligations prévues sont :

- **Obligation de rendre des comptes sur la protection des données.** Les sociétés doivent pouvoir démontrer que d'importantes mesures de sécurité sont en place pour protéger les données personnelles des utilisateurs. La barre est placée plus haut pour les entreprises qui opèrent dans des secteurs à hauts risques.
- **Droit d'accès, de rectification et de portabilité, et droit à l'effacement des données pour la personne concernée.** Les organisations sont tenues de vérifier l'identité de la personne, de produire rapidement les données personnelles traitées, et de corriger, effacer et transférer les données sur simple demande.
- **Notification d'une violation de données.** Toute violation de données à caractère personnel « entraînant, de manière illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données » doit être signalée dans un délai de 72 heures.[1]

Pour assurer la conformité au RGPD, vous devez :

- Connaître vos utilisateurs et les données auxquelles ils ont accès.
  C'est le rôle d'IBM Security Identity Governance and Intelligence.
- Savoir où se trouvent vos données critiques et qui y accède.
  C'est le rôle d'IBM Security Guardium.
- Savoir comment utiliser ces informations pour faire face aux attaques.
  C'est le rôle d'IBM QRadar Security Intelligence Platform.
- Connaître les raisons des violations et les solutions pour réduire les risques.
  C'est le rôle d'IBM Resilient Incident Response Platform.
- Appliquer une solution d'authentification de l'utilisateur pour les appareils mobiles, le cloud et le Web.
  C'est le rôle d'IBM Security Access Manager.
- Utiliser des outils de mise en conformité avec le RGPD préconfigurés et prêts à être déployés.
  C'est le rôle d'IBM Security Guardium GDPR Accelerator.

« Jusque dans leurs moindres détails, nos identités en ligne sont de plus en plus exposées au monde physique. C'est pourquoi nous devons donner plus de responsabilité... à ceux en qui nous avons confiance »
—Ponemon Institute[2]

▸ Découvrir comment IBM X-Force Exchange peut vous aider à relever les défis liés à la sécurité des données.

1 Article 83. « Règlement (UE) 2016/679 du Parlement européen et du Conseil », 27 avril 2016.

2 « 2016 Cost of Data Breach Study: Global Analysis, » (Etude 2016 sur le coût des violations des données : analyse mondiale), enquête de référence commanditée par IBM, *Ponemon Institute*, juin 2016.

Contrôle des points d'accès utilisateur et détection des risques de conformité

IBM Security Identity Governance and Intelligence

Cette solution est une plateforme unique qui permet d'analyser et de contrôler les accès utilisateur et les risques. Elle gère les identités et les accès et comble les lacunes au niveau de la conformité, des opérations de gestion et des opérations informatiques, afin de :

- Contrôler les accès et garantir le respect de la réglementation
- Centraliser et automatiser les tâches d'administration des identités utilisateur, des informations d'identification, des comptes et des permissions d'accès
- Faciliter la communication entre auditeurs et personnel informatique et déterminer les violations de l'obligation de séparation des tâches

IBM Security Access Manager

Pour respecter le RGPD, les droits d'accès des utilisateurs doivent se limiter aux éléments nécessaires à l'exécution des tâches qui leur sont dévolues. Cette obligation est assurée par IBM Security Access Manager qui s'appuie sur un accès en fonction du risque, l'authentification multifacteur, la fédération des identités pour les applications exécutées en interne et à l'extérieur de l'entreprise, etc.

IBM Security Guardium

Guardium réalise des analyses automatiques qui permettent de détecter les risques internes et externes auxquels sont exposées les données : un avantage pour respecter le délai de 72 heures prévu par le RGPD pour le signalement des violations. La solution prend en charge toute la chaîne de protection des données, de la mise en conformité à la protection de bout en bout des données, avec une même infrastructure et une même approche. Avec Guardium, les sociétés peuvent :

- Identifier et classer les données sensibles et détecter automatiquement les risques de mise en conformité
- Savoir qui accède aux données, identifier les anomalies et stopper la perte de données par la surveillance des activités sur les données
- Analyser les données pour identifier les signes d'une attaque contre une base de données, qu'elle émane de l'intérieur ou de l'extérieur
- Se mettre à l'abri en adoptant des fonctions de mise en conformité des données et d'audit sur les données statiques et en mouvement
- Localiser les données personnelles concernées par le RGPD et mieux comprendre la portée de la conformité au RGPD avec Guardium GDPR Accelerator.

En 2015, 60 % des attaques provenaient de l'intérieur, contre 55 % seulement en 2014.[1]

1 « Reviewing a year of serious data breaches, major attacks and new vulnerabilities » (Un an de graves violations de données, d'attaques d'envergure et de nouvelles failles), *IBM X-Force Research: 2016 Cyber Security Intelligence Index,* Avril 2016.

Anticiper les violations pour les éviter et réagir rapidement quand elles surviennent

IBM QRadar Security Intelligence Platform

Simple à utiliser et économique, le moteur IBM Sense Analytics Engine™ de la plateforme QRadar détecte les menaces les plus sophistiquées. Cette plateforme permet aux sociétés de :

- Collecter et analyser les données d'identification et les vulnérabilités, et consigner les événements, les flux réseau et les paquets réseau
- Prendre des mesures en cas d'incident et assurer la conformité réglementaire par la collecte de données, leur corrélation et l'établissement de rapports
- Identifier les menaces à haut risque, les attaques et les violations de sécurité via une corrélation en temps réel avec Sense Analytics
- Privilégier les incidents jugés prioritaires parmi les milliards de points de données reçus chaque jour

IBM Resilient Incident Response Platform

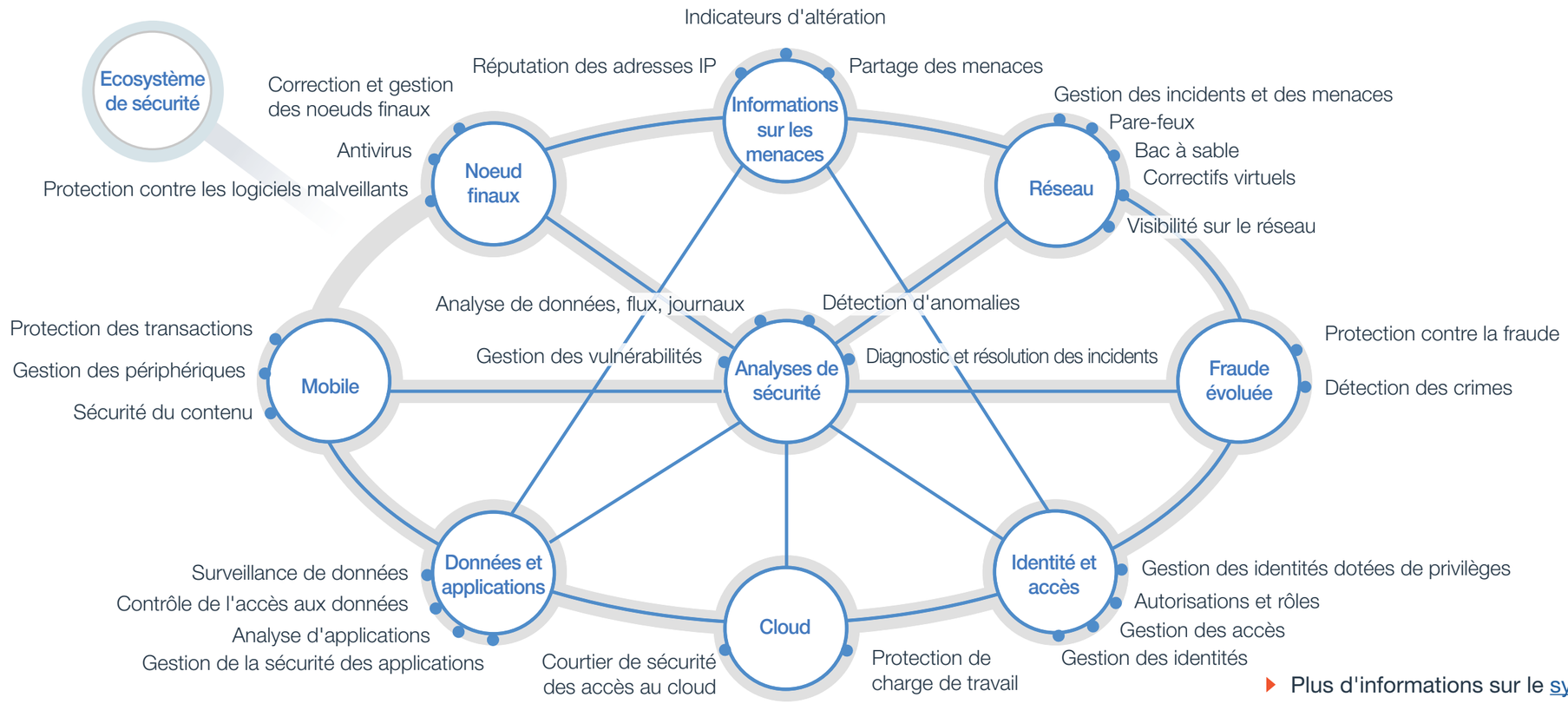
Cette plateforme permet de réagir presque instantanément aux alertes, fournit des informations sur le contexte de l'incident et permet aux équipes chargées de la sécurité d'éliminer ou de simplifier certaines étapes critiques. Elle permet à la société de :

- Réagir rapidement et en toute confiance par des plans d'action dynamiques et instantanés reposant sur de bonnes pratiques et sur une base de connaissances complète sur la règlementation en matière de notification des violations de données
- Adapter les plans de réponse en fonction du déroulement des incidents, grâce à une gestion souple et personnalisable des priorités et des tâches
- Accéder rapidement aux informations stratégiques grâce à des outils complets et personnalisables d'établissement de rapports, de tableaux de bord et d'analyse
- Réagir intelligemment grâce à une diffusion en temps réel d'informations sur les menaces

600 millions d'enregistrement ont fuité dans le monde en 2015, d'après les rapports publiés sur les violations signalées.[1]

1 « IBM X-Force Threat Intelligence Report 2016 » (Rapport 2016 IBM X-Force sur la connaissance des menaces), *IBM Corp.*, février 2016.

Un système immunitaire intégré et intelligent pour assurer la sécurité



Les solutions IBM Security forment un « système immunitaire », une solution complète et intégrée dont l'efficacité est renforcée par les synergies entre composants. Centré sur des fonctions d'analyse, ce système immunitaire apporte un niveau de maturité qu'il serait impossible d'atteindre avec une seule solution de sécurité.

▸ Plus d'informations sur le système immunitaire IBM pour la cybersécurité.

Faire appel à l'expertise mondialement reconnue d'IBM en matière de services de conseils sur la confidentialité des données

Cliquer sur l'image pour l'agrandir.
Cliquer dessus une seconde fois pour revenir aux dimensions initiales.

IBM Privacy Consulting Practice

IBM Privacy Consulting Practice aide les organisations à accélérer la création et le déploiement de stratégies de confidentialité complètes, de normes, de directives et de procédures d'exploitation conformes aux bonnes pratiques et destinées à mieux gérer les exigences en matière de conformité réglementaire. IBM propose une approche globale, appelée Total Privacy Management Framework (cadre de gestion totale de la confidentialité) qui permet d'établir une passerelle entre les différentes structures (LOB, juridique, informatique et gestion). Cette approche permet aux clients de renforcer l'efficacité de leur programme de protection de la confidentialité et de mieux gérer la conformité à la réglementation locale et internationale.

Evaluation de préparation au RGPD par IBM

IBM Data Privacy Consulting Services est l'offre de base qui permet d'identifier les secteurs de l'entreprise qui seront impactés par les exigences et les obligations du RGPD. Une évaluation personnalisée détaillée de l'état de préparation au RGPD permet de comparer les pratiques actuelles de l'entreprise aux nouvelles exigences du RGPD, notamment en matière de développement de processus, de bonnes pratiques et de besoins organisationnels. Dans le cadre de ce service, IBM propose un modèle de maturité du RGPD et un plan de correction des lacunes destiné à faciliter l'élaboration et la mise en œuvre d'une feuille de route de mise en conformité. L'évaluation de l'état de préparation au RGPD propose, pour chacune des exigences du RGPD, des produits et services IBM : le client bénéficie d'un interlocuteur unique pour l'achat des logiciels et/ou des services nécessaires à la mise en conformité.

Un modèle de maturité du RGPD et un plan de correction des lacunes facilitent l'élaboration et la mise en œuvre d'une feuille de route de mise en conformité.

- Plus d'informations sur les services IBM Data Privacy Services de mise en conformité avec le RGPD.

Pourquoi IBM ?

IBM aide les entreprises à protéger leurs données stratégiques et leur infrastructure mainframe (sans oublier leurs utilisateurs) contre les menaces et autres violations. En matière de solutions de sécurité, IBM propose une approche intégrée et à plusieurs niveaux. Elle répond ainsi non seulement aux préoccupations spécifiquement liées au système mainframe, mais aussi aux problèmes de sécurité plus généraux tels que la gestion des identités et des accès, la communication d'informations de sécurité et la sécurité des données au sein de l'entreprise.

IBM propose tout un éventail de solutions de protection offrant une vue à 360° de l'activité réseau (y compris les comportements anormaux) et des failles éventuelles du système. Ces solutions permettent aussi d'identifier les menaces et d'alerter les administrateurs afin qu'ils prennent les mesures nécessaires pour éviter les problèmes ou réparer les dommages.

Les entreprises qui déploient dès maintenant une solution IBM Security prendront de l'avance pour la mise en conformité avec le GRPD lorsque celui-ci entrera en vigueur en 2018. Les solutions IBM Security reposent sur de bonnes pratiques qui créent une base solide pour la sécurité globale de l'entreprise et permettent de protéger à la fois les données des clients et de l'entreprise contre le vol, l'utilisation frauduleuse ou l'altération.

Pour en savoir plus

Pour découvrir en quoi les solutions IBM Security peuvent vous aider à vous mettre en conformité avec le RGPD et, plus généralement, à protéger votre entreprise, contactez votre interlocuteur ou votre partenaire IBM, ou rendez-vous sur le site **ibm.com/**security

- Regarder la vidéo IBM sur la protection de l'univers numérique contre les cyberattaques.

A propos des solutions IBM Security

IBM Security offre l'un des portefeuilles les plus avancés et intégrés de produits et de services de sécurité d'entreprise. Ce portefeuille, qui s'appuie sur la recherche et le développement X-Force de renommée mondiale, fournit des renseignements de sécurité qui aident les entreprises à assurer une protection globale de leur personnel, de leurs infrastructures, de leurs données et de leurs applications, grâce à des solutions de gestion des identités et des accès, de sécurité des bases de données, de développement d'applications, de gestion du risque, de gestion des nœuds finaux, de sécurité du réseau, etc. Ces solutions permettent aux organisations de gérer efficacement les risques et de mettre en œuvre une sécurité intégrée pour le mobile, le cloud, les médias sociaux et les autres architectures métier de l'entreprise.

IBM exploite l'une des plus vastes organisations au monde de recherche, de développement et de diffusion de solutions de sécurité, surveille 15 milliards d'événements de sécurité par jour dans plus de 130 pays et détient plus de 3000 brevets de sécurité.

En outre, IBM Global Financing propose de nombreuses options de paiement pour financer vos investissements informatiques stratégiques et faire progresser votre activité. De leur acquisition à leur utilisation, nous proposons une gestion complète du cycle de vie des produits et services informatiques. Pour en savoir plus, rendez-vous sur : **ibm.com/**financing

IBM

IBM Security
Route 100
Somers, NY 10589

Produit aux Etats-Unis d'Amérique
Janvier 2017

WGW03247-USEN-03