Simplifiez votre mise en conformité RGPD
En utilisant les solutions de sécurité Oracle

LIVRE BLANC ORACLE | JUILLET 2017

Avertissement

L'objectif de ce document est d'aider les entreprises à comprendre comment les solutions de sécurité Oracle peuvent être utilisées pour les aider dans leur mise en conformité avec certaines exigences du règlement général sur la protection des données de l'Union européenne. Certaines des solutions de sécurité décrites dans le présent document peuvent ne pas être pertinentes au vu de l'environnement et des besoins spécifiques d'une entreprise. Oracle recommande systématiquement de tester les solutions de sécurité au sein de votre propre environnement afin de vous assurer que la performance, la disponibilité et l'intégrité sont au niveau requis.

De plus, les informations contenues dans ce document ne doivent pas être interprétées ni utilisées comme un avis juridique sur le contenu, l'interprétation ou l'application de toute législation, réglementation ou directive réglementaire. Les clients existants et prospects doivent s'adresser à leur propre conseiller juridique pour comprendre l'applicabilité des lois ou réglementations à leurs traitements de données personnelles, y compris lors de l'utilisation de produits ou services de fournisseur tiers.

Introduction

Avec toute l'effervescence autour du Règlement Général sur la Protection des Données (RGPD), certaines organisations s'efforcent d'en comprendre les impacts, parmi lesquels :

- Des amendes allant jusqu'à 4% du chiffre d'affaires annuel, auxquelles s'ajoutent les frais de justice et autres recours
- La révision et la modification des processus organisationnels, des applications et des systèmes
- La prise en compte de nouvelles exigences plus strictes en matière de confidentialité et de sécurité

Le projet de mise en conformité avec le RGPD nécessite une stratégie coordonnée impliquant différentes entités organisationnelles parmi lesquelles le département juridique, les ressources humaines, le marketing, la DSI, la sécurité… En effet, peuvent être concernées par le sujet de la protection des données des informations recueillies auprès de différentes personnes (clients, employés, …), ainsi que via des technologies et canaux de communication adaptés.

Les organisations devraient donc disposer d'une stratégie et d'un plan d'action clairs pour répondre aux exigences du RGPD en vue de la date d'entrée en vigueur, fixée au 25 mai 2018.

Grâce à son expérience acquise au fil des ans et à ses capacités technologiques, Oracle s'engage à aider les clients à mettre en œuvre une stratégie destinée à se conformer aux points du RGPD liés à la sécurité. Ce livre blanc a donc pour objectif d'expliquer comment les solutions de sécurité Oracle peuvent être utilisées pour aider à mettre en œuvre un cadre de sécurité conforme au RGPD.

Une stratégie Sécurité pour faire face aux menaces, réduire les risques et maintenir une conformité constante

Le RGPD n'est probablement pas la seule règlementation en matière de confidentialité et de sécurité à laquelle votre organisation doit se conformer. En effet, de nombreuses entreprises doivent respecter de multiples lois et règlementations, ainsi que des normes et standards de l'industrie. Ces lois et règlementations visent, notamment, à protéger les citoyens, le gouvernement, l'économie et l'industrie, pour ne citer que ces exemples. Il est donc important d'avoir une stratégie globale qui s'adapte facilement à un cadre réglementaire en constante évolution.

Le recours à de plus en plus de règles de sécurité peut s'expliquer en partie par l'augmentation des violations de données et des incidents de cyber sécurité. Qu'il s'agisse d'espionnage, de crime organisé ou de malveillance interne, les cybercriminels tirent profit illicitement de systèmes d'information mal conçus. Cela a pour conséquence de compromettre la libre circulation de l'information qui est l'une des clés d'une économie et d'une société prospères.

Afin d'établir une stratégie appropriée qui réponde à l'exigence de conformité au RGPD et à une réduction des risques, les organisations ont besoin d'un cadre de conformité global qui incorpore les meilleures pratiques de l'industrie internationale, telles que la norme ISO 27000 et autres.

Le RGPD préconise l'utilisation des meilleures pratiques et des concepts de sécurité bien établis. Il exige que les « responsables de traitement » (par exemple, des entreprises achetant des services pour traiter les données de leurs clients) et les « sous-traitants » (tels que les fournisseurs de services Cloud) adoptent des mesures de sécurité appropriées, conçues pour assurer un niveau de sécurité adapté au niveau de risque pouvant affecter les droits et les libertés des individus dont les données sont collectées et utilisées par le responsable de traitement (les « personnes concernées »). La loi insiste donc sur l'analyse des risques et la mise en œuvre de mesures de sécurité (également appelées contrôles de sécurité) pour pallier ces risques.

Dans l'ensemble, le RGPD adresse les principaux principes de sécurité : confidentialité, intégrité et disponibilité des systèmes et des données. Oracle dispose d'une grande expérience et a démontré ses capacités en matière de sécurité des systèmes et données. L'offre de sécurité Oracle comprend un ensemble complet de solutions Cloud et hybrides, sécurisées en profondeur, qui aident à prévenir, détecter, répondre et prédire les menaces de sécurité. Ces solutions peuvent être utile dans des projets de mise en conformité avec des règlementations comme le RGPD.

Une implémentation stratégique de la bonne technologie, avec des contrôles de sécurité efficaces, peut apporter des bénéfices importants :

- Se mettre en conformité avec les exigences réglementaires
- Réduire les risques (qu'ils soient juridiques ou d'autres natures)
- Développer un avantage concurrentiel en apportant une flexibilité accrue et des délais de commercialisation plus rapides
- Accélérer la transformation digitale

En fin de compte, la mise en œuvre de mesures organisationnelles de sécurité efficaces offrira aux entreprises l'opportunité d'améliorer leur sécurité informatique et, par voie de conséquence, la sécurisation de leur système d'information.

Les articles clés qui impactent la sécurité informatique

Avec 99 articles et 173 considérants, le RGPD intègre des exigences clés qui impactent directement la manière dont les organisations mettent en pratique la sécurité informatique.

La protection des individus dont les données à caractère personnel sont collectées et traitées est un droit fondamental qui intègre nécessairement la sécurité informatique. De nos jours, les systèmes informatiques sont omniprésents et les exigences du RGPD appellent une bonne sécurité informatique.

Pour protéger et sécuriser les données personnelles, il est notamment nécessaire de :

- Savoir où sont localisées les données (inventaire des données)
- Comprendre les risques auxquels elles sont exposées (sensibilisation aux risques)
- Passer en revue et, si nécessaire, modifier les applications existantes (revue des applications)
- Placer la sécurité au cœur des problématiques d'architecture IT (architecture sécurité)

Le tableau suivant met en évidence les articles du RGPD les plus pertinents qui traitent de la sécurité IT :

THEMATIQUE SECURITE ET ARTICLE DU RGPD

Thématique sécurité	RGPD Référence de l'article
Inventaire des données	» *Art. 30 : Registre des activités de traitement*
Sensibilisation aux risques	» *Art. 35 : Analyse d'impact relative à la protection des données*
Revue d'application	» *Art. 15 : Droit d'accès de la personne concernée* » *Art. 16 : Droit de rectification* » *Art. 17 : Droit à l'effacement (« droit à l'oubli »)* » *Art. 18 : Droit à la limitation du traitement* » *Art. 19 : Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement* » *Art. 20 : Droit à la portabilité des données*
Architecture sécurité	» *Art. 32 : Sécurité du traitement* » *Art. 5 : Principes relatifs au traitement des données à caractère personnel* » *Art. 24 : Responsabilité du responsable de traitement* » *Art. 25 : Protection des données dès la conception et protection des données par défaut* » *Art. 28 : Sous-traitant* » *Art. 34 : Communication à la personne concernée d'une violation de données à caractère personnel*

La création et la mise à jour d'un inventaire des données est une exigence de l'article 30 (Registre des activités de traitement) du RGPD. C'est aussi, plus généralement, le point de départ de toute activité liée à la collecte et au traitement des données personnelles.

La limitation des risques représente un point important de tout bon plan de sécurité informatique. Les entreprises doivent faire en sorte d'éliminer les risques conduisant à une atteinte aux de données à caractère personnel et doivent, pour cela, mettre en œuvre une évaluation régulière des risques de cyber sécurité. Pour en savoir plus sur la façon dont Oracle peut vous aider dans ces évaluations, nous vous invitons à contacter votre représentant local Oracle.

Pour permettre à l'individu d'exercer ses nouveaux droits (articles 15 à 20, par exemple, le « droit à l'oubli »), il peut être nécessaire de procéder à des évolutions structurantes. Dans la mesure où celles-ci concernent des applications qui peuvent contenir des données à caractère personnel, il est nécessaire de connaître spécifiquement le modèle de données et la logique métier afin de réaliser les modifications requises par le RGPD.

Des mesures complémentaires peuvent être mise en œuvre dans l'architecture. C'est le cas, par exemple, du chiffrement des flux réseau et de la base de données. Des évolutions portant sur l'architecture sont normalement plus faciles et moins coûteuses à mettre en œuvre que la modification des applications et s'avèrent généralement plus fiables, car elles ne sont pas conditionnées par la nécessité de connaître le modèle de données et la logique métier de l'application. Dans les entreprises de grande taille, où le système d'information est relativement cloisonné et où on constate assez souvent un manque de

connaissances des applications, il est alors plus simple d'adopter une approche généraliste de protection des données personnelles par de telles mesures.

Les solutions de Sécurité Oracle et le RGPD

Oracle a une large proposition de valeur pour adresser les exigences du RGPD qui impacte l'inventaire des données, la sensibilisation aux risques, la modification des applications et l'architecture sécurité. La figure ci-dessous illustre le positionnement des solutions de sécurité proposé par Oracle, soit une large gamme de produits on premise et de services Cloud.

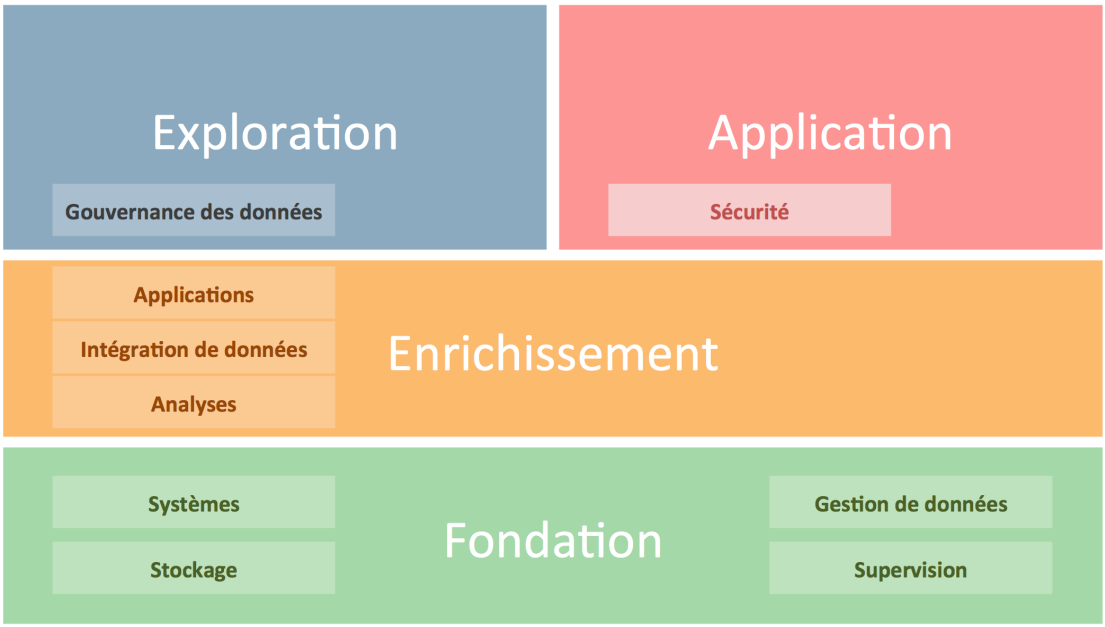

Figure 1. Le positionnement des solutions de sécurité Oracle pour le RGPD.

Exploration. Produits on premise et services Cloud qui peuvent aider à identifier les données à caractère personnel et à cartographier les flux de données. La gouvernance des données en est une partie intégrante, fournissant des capacités d'exploration, d'inventaire et de traçabilité des données.

Enrichissement. L'enrichissement concerne les évolutions applicatives qui peuvent être nécessaires afin de se conformer aux droits de l'individu (articles 15 à 20). De plus, il peut être nécessaire de consolider les données des clients pour obtenir une vue unique des personnes concernées à travers l'organisation.

Fondation. Un ensemble complet de technologies ayant fait leur preuve, partie intégrante de l'ADN d'Oracle, qui garantissent un bon niveau de sécurité en mettant l'accent sur la disponibilité et la performance des services. Ce sont des solutions hybrides (Cloud et on premise) qui couvrent des sujets allant de l'architecture à très haute disponibilité aux systèmes d'exploitation et aux processeurs. Elles sont utiles pour fournir « *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement; des moyens permettant de rétablir la disponibilité des*

données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique » (article 32).

Application. Technologies hybrides (Cloud et on premise) Oracle qui impose des règles et des contrôles de sécurité pour protéger les identités, les logiciels et les systèmes. Ces technologies englobent des produits et service de sécurité qui offrent des contrôles de sécurité basés sur la prédiction, la prévention, la détection et la réactivité pour la sécurisation des base de données, la gestion des identités et des accès, le monitoring, la supervision ainsi que l'analyse comportementale des utilisateurs.

La suite de ce livre blanc détaille ce dernier point : l'**application**. Des informations additionnelles sur le RGPD peuvent être trouvées ici : https://www.oracle.com/goto/gdpr

Les solutions de Sécurité (Application)

Les responsables de traitement et les sous-traitants doivent mettre en œuvre des mesures de sécurité appropriées conçues pour garantir que le niveau de sécurité est adapté aux risques associés aux données traitées, comme indiqué dans l'article 32 du RGPD (« Sécurité du traitement »).

L'article 32 cite la pseudonymisation et le chiffrement comme exemples de possibles mesures de sécurité appropriées. **Le RGPD laisse finalement la décision et la responsabilité aux organisations en charge de la mise en œuvre d'un cadre de sécurité de choisir les mesures appropriées qui garantissent la confidentialité, l'intégrité, la disponibilité et la résilience des données et des systèmes.** Une fausse idée reçue, souvent répandue par les fournisseurs de sécurité, est que le RGPD liste les technologies spécifiques à appliquer. En réalité, le RGPD tient le responsable de traitement et le sous-traitant pour responsables et exige qu'ils prennent en considération les risques associés aux données qu'ils manipulent et mettent en place des contrôles de sécurité appropriés pour réduire les risques. Les organisations n'intègrent pas systématiquement les contrôles de sécurité même les plus élémentaires tels que :

- Chiffrer les données sensibles au repos et en transit
- Patcher (corriger) les systèmes dans un délai raisonnable
- Collecter les journaux système pour y repérer toute activité anormale
- Appliquer le principe du «moindre privilège» ou la « séparation des tâches » pour les comptes à privilèges
- Contrôler l'accès, ou le partage, des comptes de production
- Masquer les données de production lorsqu'elles sont copiées vers des environnements de développement

La section « Application » du cadre de sécurité proposé par les solutions Oracle comprend quatre groupes qui regroupent les mesures de sécurité de base que les organisations devraient envisager de mettre en œuvre.

Protéger les données. Déployer le chiffrement pour les données au repos et en mouvement est l'une des premières étapes les plus courantes mises en œuvre pour la protection des données, car elle est relativement simple et efficace. Le chiffrement est souvent implémenté car il est conçu pour empêcher tout accès non autorisé, il est transparent pour les applications et les utilisateurs, il offre un contrôle préventif fort et les méthodes modernes de chiffrement ont généralement un faible impact sur les

performances. Les technologies supplémentaires de protection des données incluent la gestion des clés de chiffrement, la rédaction des données de la couche applicative et le masquage des données de production sensibles pour une utilisation dans des environnements non destinés à des fins de test et de développement.

Contrôler les accès. Le chiffrement des données sans contrôle de sécurité qui vérifient qui disposent de droits n'a aucun sens. Par conséquent, il est nécessaire de mettre en œuvre une technologie de gestion des identités et des accès pour les utilisateurs d'applications et le personnel informatique, y compris les administrateurs système.

Surveiller, bloquer et vérifier. Avec le niveau d'innovation des nouvelles menaces de sécurité, il est essentiel de mettre en œuvre un monitoring intelligent et automatisé des incidents de sécurité et de la performance. Les composants logiciels et les applications produisent des journaux et des pistes d'audit. Pour réduire le risque d'atteinte aux données, il est essentiel de collecter et d'analyser les flux internes et externes et les journaux pour détecter et atténuer les menaces.

Sécuriser les configurations. Pour une bonne hygiène de sécurité, les logiciels doivent être mis à jour, bien configurés et régulièrement patchés (corrigés). Une gestion de la sécurité des configurations est de plus en plus présentée comme étant l'une des bonnes pratiques internationales de sécurité, car les cybercriminels profitent souvent des vulnérabilités des logiciels non patchés pour voler des données sensibles.

Ces quatre exigences de sécurité font partie d'un ensemble d'exigences réglementaires mondiales et de bonnes pratiques de sécurité bien connues (telles que la famille des normes ISO 27000, NIST 800-53, PCI-DSS 3.2, OWASP et les contrôles CIS). Pour développer la figure 1, nous explorons plus en détail la section « Application » du cadre de sécurité proposé par les solutions Oracle qui permettent d'aborder le RGPD.

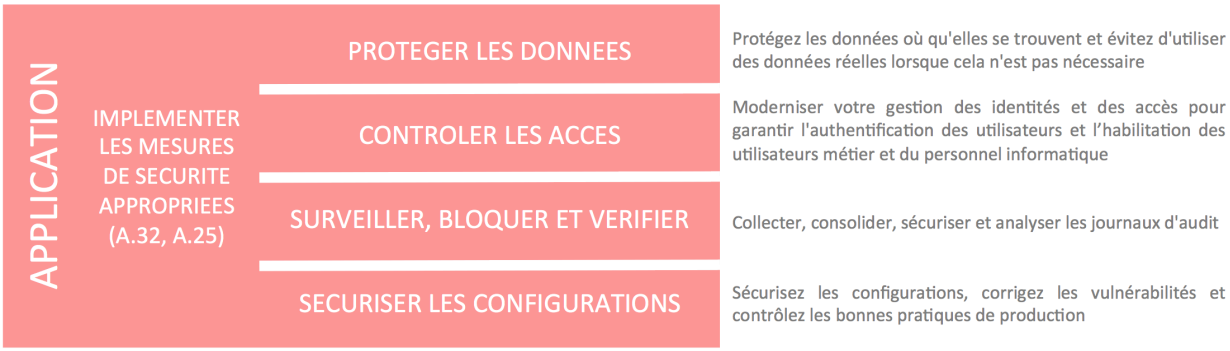

Figure 2. Vue détaillée de la section « Application » du cadre de sécurité proposé par les solutions Oracle.

Les outils de Sécurité Oracle qui peuvent aider à se mettre en conformité avec le RGPD

Oracle fournit des produits de sécurité on premise et Cloud pour des environnements hybrides conçus pour protéger les données, gérer les identités des utilisateurs, surveiller et auditer les environnements informatiques. Le tableau suivant fournit une brève description des produits, organisée par type de mesure de sécurité. Chaque produit fournit plus de fonctionnalités que celles décrites, penser donc à demander à votre contact commercial Oracle pour obtenir plus de détails.

LES OUTILS DE SECURITE ORACLE QUI PEUVENT AIDER A SE CONFORMER AU RGPD

Produit Oracle	Mesure de sécurité	Service Cloud	Brève description
Advanced Security	Protéger les données		Chiffrement des bases de données Oracle de manière transparente et ré écriture à la volée les données sensibles.
Key Vault	Protéger les données		Gestion en toute sécurité du cycle de vie des clés de chiffrement, ainsi que les mots de passe, certificats…
Data Masking and Subsetting	Protéger les données		Anonymisation des données de production pour les environnements de test et de développement.
Database Vault	Contrôler les accès		Contrôle d'accès des utilisateurs à privilège en utilisant les principes de moindres privilèges et de séparation des tâches.
Identity Cloud Service	Contrôler les accès	X	Gestion des identités en mode Cloud hybride pour contrôler les accès, les autorisations, l'authentification, le provisioning et l'authentification unique (SSO).
Identity Governance	Contrôler les accès		Gestion du cycle de vie de l'identité: administration des utilisateurs, gestion des comptes à priviléges et gouvernance des identités.
Access Management	Contrôler les accès		Contrôle des accès aux applications et fédération d'identité.
Directory Services	Contrôler les accès		Gestion des annuaires à grosses volumétries et fortes contraintes en lecture/écriture
Label Security	Contrôler les accès		Etiquetage individuel des enregistrements de données avec des métadonnées qui décrivent les caractéristiques des données, puis contrôle d'accès à ces enregistrements en fonction des métadonnées.
Audit Vault and Database Firewall	Surveiller, bloquer et vérifier		Audit centralisé, suivi, reporting et alerte de détection d'activités anormales pour les bases de données.
Security Monitoring and Analytics Cloud Service	Surveiller, bloquer et vérifier	X	Monitoring des incidents de sécurité dans des environnements Cloud hétérogènes et hybrides.
CASB Cloud Service	Surveiller, bloquer et vérifier	X	Découverte des usages de services Cloud non autorisés et implémentation des stratégies de sécurité cohérentes dans les environnements SaaS, PaaS et IaaS approuvés.
Configuration and Compliance Cloud Service	Sécuriser les configurations	X	Implémentation et maintien d'une configuration et une conformité continues pour les ressources informatiques.
Enterprise Manager: Configuration Mgmt.	Sécuriser les configurations		Vérification de la bonne installation des ressources informatiques et la sécurisation de leur configuration.

Comme première étape, Oracle suggère d'implémenter Oracle Advanced Security avec un chiffrement transparent des données en raison de deux facteurs importants : le chiffrement est considéré comme une bonne pratique et les bases de données contiennent souvent des données importantes pouvant tirer profit d'un chiffrement fort.

« Protection des données par défaut »

Un concept important intégré dans le RGPD est la « Protection des données dès la conception et protection des données par défaut » (article 25) qui stipule « *le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées* ». Le concept

de protection des données dès la conception est proche du concept de « Security By Design », que la technologie Oracle supporte très bien en poussant les politiques et les contrôles au plus près des données.

Parmi les avantages du déploiement de solutions de sécurité Oracle (référencées dans le tableau précédent) dans le cadre d'une architecture globale figurent :

- Protection simplifiée grâce à des mécanismes de sécurité éprouvés implémentés dans les technologies Oracle ;
- Mises à jour logicielles et correctifs ;
- Suppression des risques liés aux développements spécifiques, qui peuvent être sources d'erreur de programmation, ou systèmes, qui peuvent exposer au risque de violation des données personnelles.

Un cas d'usage exemple

Le cas d'usage métier suivant est destiné à illustrer la manière dont les produits Oracle peuvent être utilisés pour sécuriser les systèmes informatiques et aider à se conformer au RGPD.

Cas d'usage métier : le domaine de la Santé

L'organisation fictive est un grand hôpital privé. Le marché privé de la santé se consolide et cette organisation a récemment acquis une autre société qui fournit des services de diagnostic médical et d'hospitalisation de courte durée dans plusieurs villes. La société acquise s'est elle-même développée grâce à des acquisitions, mais à plus petite échelle.

Ils ont démarré un projet d'envergure avec les objectifs opérationnels suivants :

- Consolider les bases de données clients pour permettre des activités discrètes de marketing en vue de la commercialisation de diagnostics préventifs.
- Améliorer l'expérience client liée aux réservations (en ligne, mobiles) et au retrait des rapports médicaux.
- Garantir le respect des lois nationales et régionales, y compris du RGPD.
- Être perçu comme une entreprise sûre et moderne, respectueuse de la vie privée des patients.

Ainsi que les objectifs informatiques suivants :

- Moderniser les systèmes informatiques hétérogènes (résultat de multiples fusions) sans perturber l'activité.
- Gérer les identités des employés (médecins, infirmières, administration, etc.) et fournir des fonctionnalités d'authentification unique (SSO) pour réduire le risque de fraude et la multiplication des tâches d'administration.

Pour des raisons techniques, ils ne veulent pas changer tous les systèmes à la fois. Donc certains systèmes hérités seront traités plus tard, d'autres seront modifiés en plusieurs étapes. Ils utilisent également certaines applications packagées d'un éditeur de logiciel indépendant, et l'une de leurs trois applications importantes a été développée par une entreprise qui n'est plus en activité, donc qu'ils ne sont plus en mesure de maintenir ni de faire évoluer le code du logiciel. Enfin, ils externalisent des services auprès d'hébergeurs locaux (qui doivent être maintenus au moins pour les deux prochaines années), notamment du matériel, des réseaux, des systèmes d'exploitation et des bases de données Oracle.

Construction d'un plan projet

A l'origine, ils considéraient le RGPD comme un obstacle à leurs objectifs métier, mais leur PDG a réalisé que ces objectifs métier étaient alignés sur la nécessité de mettre en place de bons systèmes informatiques et une bonne sécurité. Ayant une vision suffisante du projet, l'organisation a commencé à déployer la sécurité au sein de l'architecture et à atteindre progressivement les objectifs métier et informatiques.

Technologies utilisées

Le premier challenge était de trouver où les données personnelles sensibles étaient stockées. Pour les bases de données Oracle, ils ont consolidé les informations avec Application Data Model (ADM). ADM répertorie la liste des applications, des tables et des relations entre colonnes, qu'elles soient déclarées dans le dictionnaire de données, importées à partir des métadonnées de l'application ou spécifiées par un utilisateur.

Le deuxième défi consistait à évaluer la posture des différents services en terme de Sécurité. Pour l'évaluation de la sécurité des bases de données Oracle, l'entreprise a eu recours aux services de consulting d'Oracle ; l'entreprise a interviewé des informaticiens et des sous-traitants, mis en place des outils de mesure (« Database Security Assessment Tool » ainsi qu'un programme bêta de Configuration and Compliance Cloud Service) et produit un rapport qui a permis de planifier les projets et l'adoption de nouvelles technologies – tout cela en une semaine. Ce rapport a été stocké comme un élément clé du projet d'ajustement au RGPD, pour démontrer la responsabilisation de l'entreprise (conformément à l'article 24 du RGPD) et a été présenté au Conseil d'administration par le délégué à la protection des données.

Les éléments suivants ont été mis en évidence parmi les actions de remédiation les plus importantes:

- **Migrer vers Oracle Database 12c à partir des versions 10 et 9 plus supportées.** Ils ont dû demander à leurs fournisseurs d'applications de certifier le support de la nouvelle version, mais pour le cas où le fournisseur est en faillite, ce n'était pas possible. La base de données n'a pas pu faire l'objet d'une migration, mais une mesure de compensation a été mise en œuvre grâce à la technologie de pare-feu de base de données Oracle fournie par Oracle Audit Vault et Database Firewall.
- **Déployer le chiffrement et les contrôles d'accès.** L'organisation, évoluant dans le domaine de la santé, a décidé qu'elle devait chiffrer les données de la base de données avec Oracle Advanced Security (suggéré dans l'article 32). À l'aide d'Oracle Database Vault, ils ont effectué une analyse des privilèges pour vérifier tous les comptes à privilèges et ils ont créé des comptes personnels avec un accès restreint en utilisant le principe du « besoin de savoir ». Ils ont constaté que les mots de passe de l'administrateur système n'avaient pas été modifiés depuis de nombreuses années.
- **Centraliser les comptes des bases de données.** L'organisation a centralisé tous les comptes de base de données dans un annuaire à l'aide de la fonctionnalité de la base de données « Enterprise User Security » et d'une instance existante d'un annuaire Oracle.
- **Masquer les données dans des environnements de non-production.** L'organisation a jugé nécessaire l'utilisation de données réelles qui étaient copiées des environnements de production vers les environnements de développement et de test. Cela a été réalisé de deux manières : en fournissant des systèmes vierges aux développeurs et en déployant la technologie d'anonymisation de Oracle Data Masking and Subsetting.
- **Réactiver les mécanismes de journalisation qui n'avaient pas été utilisés depuis plusieurs années.** La production et l'analyse des journaux (log) sont la base de toute stratégie de sécurité. L'organisation a choisi de collecter les journaux de base de données avec Oracle Audit Vault et les journaux système avec Oracle Log Analytics Cloud Service. Oracle Storage Cloud Services a ensuite été utilisé pour réduire la place occupée sur les serveurs en local par Audit Vault et le stockage des

journaux d'applications. Certaines applications ont été modifiées pour transmettre les données de l'utilisateur de l'application à la base de données, ce qui permet une meilleure traçabilité et améliore l'analyse des journaux.

Parallèlement, cet organisme de santé a intégré son portail actuel avec IDCS (Oracle Identity Cloud Service) pour obtenir une meilleure expérience utilisateur pour ses clients et offrir un sentiment de sécurité (SSO, authentification forte, accès adaptatif). Ils ont utilisé cette même technologie (IDCS) pour fournir une authentification multi-facteur et l'authentification unique (SSO) pour les utilisateurs internes. Les identités ont été synchronisées avec un Active Directory existant on premise. Enfin, un projet de réduction et de centralisation des identités on premise a été lancé.

L'entreprise utilise également le service Cloud Oracle CASB (Cloud Access Security Broker) pour superviser l'utilisation de services Cloud non autorisés depuis le réseau de l'entreprise. Ce service permet d'éviter la perte de données personnelles dans le Cloud et de surveiller les services de messagerie Microsoft. Son déploiement et sa mise en production ont pris une semaine. Afin de progresser sur le monitoring de leur Sécurité, Oracle a suggéré la mise en œuvre d'un Identity SOC, en se basant sur une solution plus moderne qui permet une remédiation rapide, tout en conservant leur prestataire de service. Ils ont donc décidé d'adopter la technologie Identity SOC (combinaison des produits Identity Cloud Services, CASB Cloud Services, Security Monitoring and Analytics Cloud Services, and Configuration and Compliance Cloud Services) proposée par Oracle en remplacement de la solution externalisée limitée à la supervision du réseau.

Conclusion

Le non-respect du RGPD peut entraîner de lourdes amendes et des mesures réglementaires accrues. Plus important encore, toute atteinte significative aux données peut altérer la marque, la valeur et la réputation d'une organisation. Pour protéger sa marque, une organisation qui collecte des données personnelles doit être en mesure de prouver qu'elle est conforme de manière constante et fiable aux principes de confidentialité et de sécurité du RGPD.

Le chemin vers la conformité RGPD nécessite une stratégie coordonnée impliquant différentes entités organisationnelles : juridique, ressources humaines, marketing, sécurité, informatique et autres. Les organisations doivent donc avoir une stratégie claire et un plan d'action pour répondre aux exigences du RGPD en vue de la date butoir du 25 mai 2018.

Se basant sur son expérience et ses capacités technologiques, Oracle s'engage à aider ses clients avec une stratégie conçue pour atteindre la conformité au niveau de sécurité requis par le RGPD. Pour en savoir plus sur la façon dont Oracle peut vous y aider, contactez votre représentant local et visitez le site https://oracle.com/goto/gdpr.

Oracle Corporation, Siège Social Monde
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Demandes mondiales
Téléphone : +1 650 506 7000
Fax : +1 650 506 7200

CONNECT WITH US

blogs.oracle.com/oraclesecurity
facebook.com/oraclesecurity
twitter.com/oraclesecurity
oracle.com/security

Integrated Cloud Applications & Platform Services

Simplifiez votre mise en conformité RGPD en utilisant les solutions de sécurité Oracle
Juillet 2017
Auteur : Alessandro Vallega, Troy Kitch
Contributeurs : Angelo Bosis