Le Règlement général sur la protection des données de l'UE et son application

www.netwrix.com
www.netwrix.fr

Téléphone : 33 975 18 11 19

Comprendre et respecter le Règlement général sur la protection des données de l'UE

Le General Data Protection Regulation (GDPR) de l'Union européenne, Règlement général sur la protection des données (RGPD) en français, revêt une grande importance pour les entreprises. Néanmoins, de nombreux responsables ne se préoccupent que très peu, voire aucunement des nouvelles règlementations destinées à renforcer la protection des données. Cette erreur pourra leur coûter davantage à partir de 2018 (au plus tard).

L'utilisation des données à caractère personnel et l'utilisation abusive des données sont régies par des réglementations. Déjà depuis le début de l'année 2016, les entreprises sont tenues de mettre en adéquation leurs infrastructures IT avec le RGPD. Ces infrastructures ont jusqu'à 2018 pour remplir les conditions fixées par le RGPD, faute de quoi, les entreprises s'exposent à des sanctions draconiennes. L'autorité compétente peut infliger des amendes d'un montant pouvant atteindre un million d'euros ou 2 % du chiffre d'affaires annuel si une entreprise ne se conforme pas au RGPD. Il est ainsi grand temps pour les entreprises de s'y intéresser.

Les objectifs du Règlement général sur la protection des données

Le RGPD précise par exemple que les données à caractère personnel de citoyens de l'UE ne peuvent être archivées au sein de l'entreprise que sous certaines conditions. Chaque enregistrement de données doit d'abord faire l'objet d'un consentement éclairé selon lequel une entreprise est autorisée à stocker les données concernées. Les infrastructures IT doivent ainsi être en mesure de stocker et de fournir ces informations.

Les données qui ne sont plus nécessaires aux relations d'affaires doivent être supprimées par l'entreprise. Il n'est plus utile de conserver dans le système de l'entreprise les données d'un client ayant acheté un produit cinq ans auparavant, une fois la vente conclue. Selon le principe de « Privacy by Design » (respect de la vie privée dès la conception), les données à caractère personnel ne doivent être stockées que si elles sont indispensables au processus commercial. En outre, le RGPD est constitué de quatre éléments :

Obligation d'information - Le RGPD vise à renforcer l'information des personnes. Celles-ci doivent pouvoir accéder plus facilement aux données qui ont été collectées à leur sujet et les recueillir sans contraintes. Les infrastructures IT doivent également se conformer au règlement. La façon dont l'entreprise accède aux données importe peu. Chaque citoyen de l'UE doit avoir le droit de consulter les données enregistrées à son égard. De plus, la communication de ces données doit être intelligible. Les services marketing ainsi que le service d'informations de l'entreprise doivent également être en mesure de consulter et de transmettre les données d'un client en tout temps au sein des systèmes informatiques internes. Les employés sont en outre tenus de connaître l'ensemble des systèmes informatiques pertinents à cet égard.

Portabilité des données - La seconde finalité du RGPD consiste à faciliter le transfert des données d'une personne d'une entreprise à une autre. Lorsqu'un citoyen de l'UE demande un transfert des relations commerciales d'une entreprise à une autre, les données qui le concernent doivent elles aussi faire l'objet d'un déplacement. Ces données doivent pouvoir être effacées du système à l'issue du transfert.

Effacement complet des données - Si des personnes souhaitent que leurs données ne soient plus traitées, celles-ci doivent ainsi pouvoir être supprimées du système de l'entreprise. Les infrastructures IT ne doivent plus contenir aucune trace électronique de la personne en question (le

droit à l'oubli). Les entreprises sont également tenues d'effacer l'ensemble des données qui ne présentent plus d'utilité aux relations d'affaires. Si un client exige la suppression de ses données, celle-ci doit être effectuée dans les plus brefs délais. Le réseau de l'entreprise ne doit alors contenir plus aucune trace de données. Il est de ce fait essentiel de savoir où sont stockées les données des clients. Pour cela, il existe des outils tels que Netwrix Auditor qui permettent aux entreprises de localiser précisément l'emplacement hébergeant les données des clients et de connaître l'identité des personnes pouvant y accéder.

Notification des failles de sécurité des données - Il devient désormais obligatoire à toute société de notifier aux personnes compétentes toute faille de sécurité des données ou toute perte de données dans un délai de 72 heures après sa découverte. Le RGPD définit clairement les procédures à suivre dans une telle situation. Les infrastructures IT doivent également satisfaire aux exigences du RGPD. La perte ou le vol de données constitue un problème grave qui expose la société à des répercussions. L'entreprise doit en informer aussi bien ses utilisateurs que les autorités nationales compétentes. Des mesures doivent être prises afin d'améliorer la protection des données des utilisateurs. Par ailleurs, les entreprises sont chargées de définir des processus et de mettre en place un système de gestion des incidents. Il existe des outils destinés à l'inventorisation des actifs informatiques.

Le RGPD précise en outre que les données des clients doivent être protégées. Les systèmes informatiques doivent être efficacement protégés contre les attaques indésirables. Le service informatique est également chargé de mettre en place ces protections. Le relevé des données existantes par l'intermédiaire d'un outil comme Netwrix Auditor revêt une importance considérable. Cette plateforme fournit des indications précises sur l'emplacement des données et l'identité des personnes qui y ont accès. De plus, elle indique les modifications apportées aux droits d'accès, leur auteur et leur date. Sans outil de ce type, il sera très difficile pour les entreprises de se conformer au RGPD à partir de 2018.

Qui est chargé de veiller au respect du RGPD ?

De manière générale, chaque entreprise est tenue de respecter le RGPD. Il est de leur responsabilité de se conformer aux directives, du fait qu'elles détiennent un grand nombre de données propres à leurs clients et à leurs employés. Les entreprises évoluant dans le secteur grand public et détenant des données sur leurs clients sont d'autant plus concernées. Plus le volume de données enregistré et traité des employés et des clients est élevé, plus l'ampleur du travail de mise en œuvre du RGPD est conséquente. Cette mise en œuvre n'épargne aucune entreprise d'une manière générale. En effet, chacune d'elles stocke des informations sensibles sur ses clients qui nécessitent une protection.

Exigences relatives à la mise en œuvre du RGPD.

Un nombre croissant d'utilisateurs travaillent en déplacement ou chez eux. C'est là qu'intervient l'utilisation de services cloud qui n'est quant à elle pas directement du ressort de l'entreprise, même si ces services abritent d'importantes données à caractère personnel. Le cloud n'est pas épargné par le RGPD. Il peut arriver, au sein de grandes entreprises, que des services louent de nouveaux services informatiques comme le cloud, sans en informer le service informatique. Cette situation peut se produire aussi dans une entreprise de plus petite taille et entraîne de gros risques. En effet, lorsqu'un service enregistre des données à caractère personnel sans en informer le service informatique, les responsables de l'entreprise ou encore le personnel des services de sécurité informatiques, il est alors très difficile d'identifier une faille de sécurité. Une fois de plus, les solutions telles que Netwrix Auditor s'avèrent très efficaces puisqu'elles facilitent le processus d'inventorisation et permettent de connaître les utilisateurs ayant accès aux données. Netwrix

Auditor aide également à chercher de manière ciblée les actifs informatiques au sein de l'entreprise et à les répertorier. La plateforme permet donc de les rassembler et de les sécuriser de manière optimale.

Le RGPD s'applique également de plein droit aux services informatiques sur le cloud. Pour un service informatique, il n'est donc pas simple de savoir où sont stockées précisément les données à caractère personnel. Toutes ces données sont soumises au RGPD, mais il est possible que les divers services ne disposent pas des connaissances nécessaires ou que ses membres n'aient pas été sensibilisés à la protection des données. Les entreprises, en particulier leur service informatique, doivent être en mesure de mettre la main sur les actifs informatiques et de les localiser de manière précise. Les outils semblables à Netwrix Auditor sont parfaitement adaptés à la situation.

Netwrix Auditor permet de vous assister dans la mise en œuvre du RGPD.

Il est nécessaire de trouver des solutions permettant d'établir un relevé des données existantes et d'identifier d'éventuelles lacunes. Il convient également de remédier à ces insuffisances. Les outils précités permettent d'obtenir une vue d'ensemble précise. Ils sont les seuls à donner les moyens aux responsables de veiller à ce que le système informatique de l'entreprise soit conforme aux nouvelles prescriptions du règlement. Netwrix Auditor aide à établir un inventaire des actifs informatiques et à les superviser. Pour localiser précisément l'emplacement des données à caractère personnel, le service informatique doit d'abord connaître les logiciels et le matériel exploités au sein de l'entreprise. Ce n'est qu'une fois cette liste établie que l'emplacement des données à caractère personnel peut être vérifié tout comme leur protection.

Les données répandues dans toute l'entreprise dont les responsables informatiques ignorent l'existence sont très difficiles à effacer, si cela s'avère nécessaire. Le transfert des données prévu par le RGPD devient alors presque impossible, tout comme la mise en place d'une protection optimale. Il est alors indispensable d'éviter autant que possible la profusion et le contrôle des données.

Netwrix permet de satisfaire les exigences du RGPD

La plupart des entreprises disposent de différentes structures informatiques et d'un nombre encore plus important d'administrateurs qui ont accès au système. Sans outils complémentaires tels que Netwrix Auditor, Il est très difficile de discerner les administrateurs qui détiennent l'accès aux systèmes ainsi que les modifications qu'ils effectuent à différents moments. Grâce à Netwrix Auditor, l'ensemble des systèmes informatiques sont répertoriés de manière centralisée et les modifications opérées par les administrateurs enregistrés. Ces opérations permettent aussi de prévenir l'utilisation abusive des données ou de détecter très tôt un tel problème. La plateforme offre un système de gestion de sécurité et de configuration et un accès aux données sur l'ensemble des systèmes informatiques pertinents via un système de gouvernance.

Netwrix Auditor garantit la transparence des systèmes informatiques, de la configuration en matière de sécurité et de l'accès aux données. Toutes les infrastructures IT et les données sont ainsi répertoriées. Les rapports fournissent des réponses aux questions suivantes : qui, quand et quoi ? Ils indiquent également la nature des données enregistrées ainsi que le nom des personnes qui y ont accès. Les rapports mentionnent aussi les modifications effectuées au sein même des infrastructures informatiques et les changements relatifs aux droits d'accès des données. Par ailleurs, il est intéressant de savoir par exemple quels utilisateurs de l'entreprise disposent d'un accès aux différentes données et à quel moment un accès ou une tentative d'accès a eu lieu.

Netwrix Auditor vous fait bénéficier des données d'audit essentielles et met à la disposition des responsables des rapports prenant en considération l'ensemble des principaux secteurs ayant trait à l'informatique et leurs accès. Ces rapports peuvent être créés pour des administrateurs informatiques, des responsables informatiques, mais aussi pour certains postes clés comme le dirigeant principal de l'information, le chef du service de sécurité ou d'autres responsables de l'entreprise. De plus, Netwrix met à disposition son « Auditor Client ». Celui-ci permet à différents employés d'obtenir les données d'audit essentielles. Le client est accessible sur le poste de travail de chaque employé.

Netwrix Auditor garantit le respect des règlements

Les rapports contribuent par défaut au respect des exigences du RGPD et à la réduction des coûts. Netwrix Auditor propose également plus de 200 rapports prédéfinis que vous pouvez bien entendu compléter ou enrichir de vos propres rapports. Les rapports State-in-time en font partie. Ils affichent les paramètres de configuration ainsi que les droits d'accès à des périodes données. Ces rapports permettent même aux employés responsables de l'entreprise de retracer les droits d'accès ou les adhésions aux groupes octroyé(e)s par le passé. Il en va de même pour le paramétrage des mots de passe tel qu'il était un an auparavant par exemple.

Netwrix Auditor permet ainsi d'éviter les pénalités de non-conformité au RGPD. La plateforme est adaptée à toutes les entreprises, quelle que soit leur taille. Dans le cadre du respect du RGPD et de la protection des données des clients, elle permet de garantir la protection des données des détenteurs de carte, ce qui revêt une importance majeure notamment pour les banques, mais aussi pour les détaillants.

Les rapports de l'outil donnent lieu à la mise au point et à la maintenance de systèmes et d'applications davantage sécurisées. Limiter l'accès aux données des détenteurs de carte en fonction des besoins d'informations commerciales constitue une autre action essentielle, tout comme l'identification et l'authentification de l'accès aux composantes des systèmes.

Le suivi et le contrôle de l'ensemble des accès aux ressources réseau et aux données des détenteurs de carte peuvent être pris en charge par Netwrix Auditor. Aussi, il est indispensable de tester régulièrement les systèmes et processus de sécurité en place. Netwrix Auditor offre à l'ensemble du personnel la possibilité de mettre en place une gestion de la politique en matière de sécurité des informations.

La plateforme aide les entreprises à se conformer au RGPD, mais aussi au COBIT (Objectifs de contrôle de l'Information et des Technologies Associées) ou encore à la norme ISO27001. Netwrix Auditor aide à la mise en œuvre des normes de conformité PCI DSS 3.0, HIPAA, SOX, FISMA / NIST800-53 et ISO / IEC 27001.

Les principaux avantages offerts par Netwrix Auditor

Le recours à la plateforme garantit une conformité continue en vérifiant de manière permanente les directives et processus mis en place au sein de l'entreprise. Cette solution permet d'éviter les coûts importants résultant de la violation de la protection de données et de la perte accidentelle d'informations. Ce point fait partie des éléments fondamentaux du RGPD.

Les rapports très détaillés fournis par Netwrix Auditor sont les seuls à assurer une transparence complète sur toutes les infrastructures informatiques et les données qu'elles contiennent. Le dépistage et l'identification de cas de violation du règlement sont ainsi rendus possibles, tout

comme l'analyse des modifications non autorisées dans les configurations du système ou les accès non autorisés à des données.

Les rapports établis par Netwrix Auditor aident à détecter et prévenir les failles et lacunes en matière de protection des données sensibles par la surveillance des modifications apportées aux contenus et droits d'accès propres aux utilisateurs. Netwrix Auditor supprime les restrictions à l'audit natif et améliore la gestion des événements et des informations de sécurité (SIEM) en comblant les lacunes et en remédiant aux perturbations qui touchent les données d'audit par le biais de la technologie AuditAssurance. Voilà autant de raisons qui ont poussé de grandes entreprises comme KPMG, CreditSuisse, Ing Diba et bien d'autres à faire confiance à Netwrix Auditor pour garantir leur conformité.

Supervision de services spécifiques fournis par des serveurs - SharePoint et autres

L'un des points forts de la solution Netwrix Auditor est sa prise en charge des solutions Microsoft courantes, car un grand nombre de sociétés enregistrent les données de leurs clients sur des serveurs Microsoft SQL, mais aussi sur SharePoint ou Exchange. Netwrix Auditor peut, entre autres, superviser les serveurs Windows, Active Directory, Exchange, les serveurs de fichiers ainsi que les serveurs SharePoint et SQL. L'outil assure une couverture complète de tous les systèmes. Les administrateurs peuvent mettre la main sur toutes les modifications apportées aux structures informatiques ou aux accès aux données par le biais d'une recherche interactive sur Netwrix Auditor. Pour cela, il suffit de rechercher des journaux d'évènements ou des protocoles. L'ensemble de ces tâches reviennent aux administrateurs dans la console Auditor. De plus, Netwrix Auditor détecte chaque tentative d'accès aux données, fructueuse ou non, que le système aurait certes fait échouer, mais signale les tentatives abusives d'interception de données de la part de cyber pirates.

Netwrix Auditor dispose de rapports efficaces.

Netwrix Auditor met à disposition des centaines de rapports qui fournissent une aide précieuse aux entreprises pour la mise en œuvre du RGPD. Les tableaux suivants vous donnent quelques exemples :

Rapport	Rôle
All Changes by Audited System	Affiche toutes les modifications apportées aux structures informatiques qui sont regroupées par système contrôlé.
Windows Server Overview	Affiche toutes les modifications apportées aux serveurs Windows et les ajustements au niveau des droits d'accès.
Administrative Group Membership Changes	Affiche toutes les modifications relatives à l'adhésion aux groupes d'administrateurs dans Active Directory.
All Logon Activity	Affiche l'ensemble des tentatives d'accès fructueuses au réseau, mais également celles indiquant qu'un cyberpirate cherche à s'y introduire.
Mailbox Delegation and Permissions Changes	Affiche les modifications en matière de droits d'accès pour les boites aux lettres Exchange. Ce rapport est particulièrement utile aux employés qui détiennent un accès aux données importantes de l'entreprise.
All File Server Activity by Action Type	Affiche l'ensemble des actions réalisées sur les serveurs de fichiers. Parmi elles notamment, les opérations de lecture et d'écriture, les ajustements accomplis et non-accomplis. Il est possible de filtrer ces opérations. Le rapport affiche également les opérations de copie/d'effacement de données.
Files Copied	Dresse une liste des fichiers copiés avec leurs dossiers source et de

	destination.
SharePoint Activity Summary	Affiche les actions effectuées par les utilisateurs dans SharePoint et détecte également les tentatives suspectes d'accès à des fichiers sur les bibliothèques SharePoint.
SharePoint Read Access	Affiche les documents consultés par les utilisateurs pour lecture.
All SQL Server Data Changes	Affiche les modifications de données sur un serveur SQL. Ces rapports sont également mis à disposition pour les bases de données Oracle.
VMware Virtual Machine Permissions Changes	Affiche les modifications propres aux droits d'accès des VM.
Access to Archive Data	Affiche les accès aux données des archives ainsi que l'identité des utilisateurs qui en sont à l'origine de leur attribution.
File Names Containing Sensitive Data	Détecte les fichiers laissant à penser qu'ils contiennent des données sensibles. Par exemple, « Mot_de_passe.txt ».

Bilan

Les entreprises n'auront aucun autre choix que de respecter dans son intégralité le General Data Protection Regulation (GDPR) de l'Union européenne, règlement général sur la protection des données (RGPD) dès 2018. Elles ont fort intérêt à se préparer sans tarder à établir un inventaire des actifs informatiques de l'entreprise et obtenir une vision claire des accès sur les systèmes. Un outil tel que Netwrix Auditor parait alors indispensable puisqu'il permet d'obtenir une vue d'ensemble précise et de documenter l'ensemble des modifications effectuées.

Seul l'établissement d'une documentation d'audit claire et convaincante accompagnée d'un inventaire d'audit permet aux entreprises d'être en conformité avec le RGPD. La taille de l'entreprise n'a aucune importance. PME et grandes sociétés multinationales peuvent avoir recours à Netwrix Auditor. Avec Netwrix Auditor, les incidents de sécurité de tout genre qui surviennent au sein de l'entreprise peuvent être détectés suffisamment tôt et faire l'objet d'une analyse complète précoce. L'ensemble des violations de conformité et des accès non autorisés sont identifiés et même contrés. Ainsi, il est possible avec cette plateforme de corriger dans les plus brefs délais les manipulations malencontreuses et dangereuses.