PRÉPARATION AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

LIVRE BLANC

TABLE DES MATIÈRES

PRÉPARATION AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

INTRODUCTION

QU'EST-CE QUE LE RGPD ?

La numérisation et la mondialisation continues de notre économie dépend de plus en plus du contrôle et du traitement des données personnelles. S'il en résulte des opportunités considérables pour les entreprises, cette évolution s'accompagne également d'une prise de conscience et d'un intérêt croissants du public pour l'importance de la protection des données personnelles.

Selon une étude mondiale récente réalisée par KPMG International, plus de la moitié (55 %) des clients déclarent avoir abandonné des achats en ligne à cause de problèmes de confidentialité. Cette étude a également mis en avant que moins de 10 % des répondants pensent actuellement maîtriser la façon dont les entreprises gèrent et utilisent leurs données personnelles.

Le règlement général sur la protection des données (RGPD) de l'Union européenne constitue une réponse à ce problème. Reconnaissant la valeur de ces données, cette réglementation impose un coût de collecte, de stockage et d'utilisation en tenant les entreprises responsables de cette protection et en les contraignant à rendre le contrôle et la propriété aux individus.

Contrairement à la directive 95/46/CE sur la protection des données, qui a été traduite en lois individuelles nationales, le RGPD est une simple réglementation visant à renforcer, unifier et mettre en application la protection des données personnelles dans l'Union européenne. Imposant des critères plus stricts, des obligations supplémentaires et des pénalités plus élevées en cas de non-conformité (jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros, suivant la somme la plus élevée), le RGPD améliorera sans conteste les efforts de mise en conformité tout en augmentant les risques inhérents à la non-conformité. L'aspect positif pour la plupart des parties[1], c'est qu'il constituera une conjugaison d'efforts couvrant les responsabilités en matière de protection des données d'une entreprise au sein de tous les pays de l'union européenne.

[1] Les législateurs ont permis aux gouvernements locaux d'ajouter ou d'adapter les dispositions en fonction des besoins locaux en matière de protection des données.

Le **règlement général sur la protection des données (RGPD)** constitue la réponse de l'Union européenne au rôle considérablement accru que tient désormais la technologie dans notre quotidien. Le RGPD a été ratifié par les états membres en avril 2016 et **entrera en vigueur le 25 mai 2018.** Bien qu'il s'agisse d'un règlement de l'Union européenne, il s'applique également à toutes les entreprises, indépendamment de leur localisation physique, qui collectent des données personnelles sur les résidents de l'Union européenne.

Cette nouvelle réglementation vise à **garantir l'intégration d'une protection adéquate des données dans le processus de collecte des données personnelles « dès la conception et par défaut ».** Tout commence par la collecte des seules données requises pour un objet particulier et leur suppression une fois leur utilité passée. Autre aspect important du RGPD, l'intéressé (la source des données personnel) est le propriétaire des données personnelles le concernant. En tant que tel, il peut annuler son consentement à la collecte de données aussi facilement qu'il a donné son accord. L'intéressé bénéficie également du droit à l'oubli et de récupération de ses données personnelles.

Le RGPD définit également les conditions imposant l'envoi de notifications en cas de brèche de données, ainsi que deux niveaux de pénalités en fonction de la gravité de la brèche.

Du fait de l'évolution rapide des technologies, le RGPD fait portée à l'entreprise de collecte (contrôleur des données) la charge de l'« évaluation continue des risques » et exige que toute entreprise externe qui traite les données (mandataire de traitement des données) se conforme au RGPD.

QUI EST CONCERNÉ ?

Le RGPD s'applique à toutes les entreprises, dans tous les pays, qui collectent, conservent ou traitent les données personnelles des résidents de l'Union européenne. Ces données peuvent concerner les employés, les partenaires commerciaux ou les prospects et les clients. En termes de terminologie réglementaire, ces entreprises constituent des « contrôleurs » qui déterminent comment et pourquoi les données personnelles sont traitées ou des « transformateurs » qui agissent au nom du contrôleur. Elles sont toutes soumises aux obligations supplémentaires résultant du RGPD et peuvent se voir imposer des pénalités en cas de brèche.

QUELLES SONT LES IMPLICATIONS POUR LES ENTREPRISES MONDIALES ?

Pour la plupart des entreprises, les implications sont à la fois significatives et considérables. Elles nécessitent des modifications qui englobent les flux de traitement des données, la structure organisationnelle, les processus commerciaux et, enfin, les technologies d'informations et de sécurité.

DROITS INDIVIDUELS

Fondamentalement, le RGPD définit les droits des individus en matière de protection des données. Un bref récapitulatif de ces droits est présenté ci-après :

- **Consentement éclairé**
  Droit d'être clairement informé des raisons de la demande de données et de l'utilisation qui en sera faite. Le consentement doit être explicite et peut être annulé à tout moment.
- **Accès**
  Droit d'accès, gratuit, à toutes les données collectées et d'obtention d'une confirmation du traitement appliqué aux données.
- **Correction**
  Droit de corriger les données en cas d'imprécision.
- **Suppression et droit à l'oubli (RTBF)**
  Droit d'un individu à demander la suppression des données le concernant.
- **Portabilité des données**
  Droit de récupérer et de réutiliser les données personnelles, à ses propres fins, à travers plusieurs services.

Le premier défi inhérent à la conformité RGPD consiste, par conséquent, à auditer, et modifier si nécessaire, la façon dont l'entreprise collecte, conserve et traite les informations personnelles conformément à ces droits. Le simple fait, pour l'entreprise, de parvenir à localiser précisément toutes les instances des données personnelles d'un individu à l'échelle de son infrastructure (ce problème étant parfois résumé par l'expression « Où son mes données ? ») représentera une part majeure de ce défi.

Certaines entreprises y verront une opportunité de rationaliser les opérations, de supprimer la collecte inutile de données et de limiter le traitement aux informations essentielles à leurs principaux objectifs commerciaux. Pour d'autres, la transition vers la conformité constituera probablement une tâche considérable.

RESPONSABILITÉ ET GOUVERNANCE

L'entreprise doit pouvoir démontrer la conformité par le biais de mesures de gouvernance appropriées, y compris au moyen d'une documentation détaillée, de la journalisation et d'une évaluation continue des risques. Il en résulte une attente accrue en matière de « protection des données dès la conception et par défaut », de sorte que la sécurité doit, autant que possible, faire d'emblée partie intégrante de tous les systèmes plutôt qu'être appliquée rétrospectivement bien que cela constitue un défi considérable lorsque des systèmes existants sont impliqués. De telles situations mettent en exergue le rôle essentiel de la sécurité au niveau du réseau en tant que première couche de défense. En effet, il peut s'agir de la seule protection contre les brèches de données jusqu'à ce que le nombre considérable de systèmes existants toujours utilisés puisse être restructuré au moyen de mesures de protection de données intrinsèques.

Du fait de l'évolution rapide des technologies (Internet, appareils mobiles, applications et économie numérique, par exemple) et de l'évolution subséquente des cybermenaces qui continueront d'exploiter ces modifications, la législation est nécessairement vague quant aux mesures technologiques exactes à respecter. Au-delà des précautions les plus évidentes (chiffrement des données, anonymisation[2], etc.), le RGPD emploie des termes ou expressions comme « approprié » et « à la pointe de la technologie » pour communiquer les exigences en matière d'évaluation continue des risques et la mise à jour des mesures de conformité. Lorsque de nouvelles vulnérabilités sont détectées, les technologies de sécurité ou les pratiques en matière de protection des données actuellement considérées comme conformes peuvent nécessiter des modifications pour le rester à l'avenir. Bien que cela puisse sans conteste donner lieu à des contestations judiciaires en termes d'interprétation, les entreprises requerront néanmoins des mécanismes permettant de garantir que les efforts qu'elles déploient leur permettent de s'adapter aux dernières évolutions en matière de technologie et de menace.

[2] L'anonymisation est une procédure visant à remplacer les champs facilitant le plus l'identification dans un enregistrement de données par un ou plusieurs identifiants artificiels ou pseudonymes

NOTIFICATION DES BRÈCHES

Le RGPD introduit également une nouvelle obligation pour les entreprises. Ces dernières doivent notifier aux autorités compétentes toute brèche relative aux données personnelles[3] susceptible d'entraîner un risque relatif aux « droits et obligations des individus »[4]. Lorsque ce risque est considéré comme élevé, la notification doit également être étendue aux intéressés concernés. Les notifications doivent être exécutées « dans les meilleurs délais » et, lorsque la situation le permet, dans les 72 heures suivant la découverte de l'événement.

Même en l'absence de toute référence explicite aux technologies de protection des données et de sécurité du réseau, la transition vers la conformité doit commencer par s'assurer que le réseau sous-jacent est suffisamment protégé au niveau de tous les vecteurs d'attaque possibles.

DÉFIS LIÉS À LA SÉCURITÉ DU RÉSEAU

MAINTIEN D'UNE PROTECTION À LA POINTE DE LA TECHNOLOGIE

Suivre le rythme de l'évolution du paysage de menaces constitue un défi, y compris en l'absence de disposition du RGPD pour une protection à la pointe de la technologie. Les revenus considérables de la cybercriminalité, sans parler de son potentiel en matière de terrorisme parrainé par un État, garantit un niveau de ressources et d'innovation avec lequel une entreprise seule, voire même un gouvernement national, peut avoir du mal à rivaliser.

Le problème découle partiellement de l'évolution suivie par la cybersécurité, la découverte de chaque nouveau vecteur d'attaque nécessitant l'ajout d'une nouvelle solution de sécurité. Bien que chacun de ces ajouts puisse remplir l'objectif prévu, il le fait principalement de manière isolée, avec peu ou aucune interaction avec le reste de l'infrastructure de sécurité. Un tel processus, en plus d'être difficile à gérer, peut également se traduire par des lacunes et des incohérences en termes de réponse aux nouvelles menaces, notamment dans un environnement multi-fournisseurs.

Le problème est aggravé par l'adoption de tendances, comme la mobilité, le Cloud Computing et l'Internet des Objets, qui étendent toutes la surface d'attaque effective, exposant ainsi de nouvelles vulnérabilités tout en érodant le concept traditionnel de frontière du réseau.

L'une des réponses aux nouvelles menaces consiste à augmenter le traitement et les contrôles, mais quiconque connaît la sécurité aux aéroports/frontières peut témoigner que l'accroissement des contrôles peut rapidement conduire à des retards et à un désordre inacceptables. Un traitement supplémentaire accentue également la complexité en multipliant le nombre de points de données à agréger et à interpréter lors de l'évaluation de la meilleure réponse à apporter à un événement détecté.

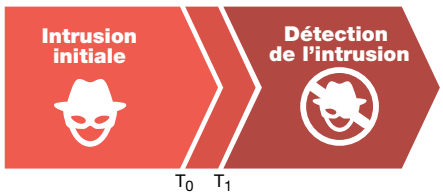
Toute solution digne de ce nom, à la pointe de la technologie, devra non seulement surmonter les difficultés ci-dessus mais également s'adapter continuellement à l'utilisation des technologies et au paysage évolutif des menaces.

SIGNALEMENT DES MENACES DANS LES 72 HEURES

La première difficulté relative à l'exigence de notification des brèches du RGPD consiste à détecter le moment d'apparition d'une brèche et à déterminer les actifs potentiellement en danger. Presque par définition, une brèche de sécurité externe effective a totalement échappé à la détection ou n'a pas été détectée suffisamment rapidement. Cela signifie qu'elle a exploité un mécanisme d'attaque différent de ceux rencontrés jusque-là ou que les signalements inhérents n'ont pas été réalisés.

En effet, en 2016, le délai moyen de prise de conscience par les entreprises de l'existence d'une brèche type s'élevait à presque cinq mois[5]. Heureusement, la fenêtre de notification de 72 heures du RGPD s'ouvre au moment de la détection, non de l'intrusion. Cependant, comme l'impact financier d'une brèche révèle une corrélation étroite avec la durée d'accès du pirate, réduire le délai de détection reste un impératif.

Comme il est clairement impossible de détecter l'indétectable, les administrateurs de sécurité doivent accepter et se préparer à une intrusion occasionnelle inévitable tout en s'efforçant de minimiser de telles occurrences et en accélérant leur détection par tous les moyens possibles. Comme indiqué précédemment, le RGPD n'exige pas de notification pour toutes les brèches de sécurité mais uniquement pour celles qui présentent un risque concernant les droits des individus. Par conséquent, si les données accessibles par le biais d'une brèche ont été correctement codées au moyen d'un chiffrement ou d'une anonymisation, et si la durée d'accès non autorisé reste brève, le risque d'infraction de ces droits devrait être minime.



[3] Une brèche de données personnelles est définie ici comment étant n'importe quelle infraction à la sécurité résultant en la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès aux données personnelles.
[4] RGPD, article 32, « Sécurité du traitement »
[5] Rapport M-Trends de 2016

Cependant, ce n'est pas parce qu'un profil d'attaque spécifique n'a pas encore été rencontré qu'il est nécessairement indétectable. En associant de manière appropriée l'analyse distribuée du trafic et les renseignements sur les menaces avec des technologies comme le sandboxing, il est toujours possible de bloquer des attaques inconnues. Le défi de ces techniques de détection avancée consiste à distinguer les signaux pertinents de tous les autres bruits.

Ce problème est similaire à celui rencontré par les organisations anti-terroristes dans le monde entier ; ces dernières doivent en effet extraire les signes suspects d'une attaque en cours des actions et communications de milliers de sujets surveillés à travers plusieurs juridictions et frontières nationales. Sans une étroite coopération et des technologies de reconnaissance automatique des modèles, ces efforts auraient peu de chance de donner des résultats.

De même, en matière de sécurité du réseau, l'approche traditionnelle qui repose sur plusieurs solutions isolées de reporting et l'aptitude décisionnelle d'un seul administrateur (humain), est rapidement devenue intenable. Du fait de l'augmentation de la complexité du réseau et de la fréquence des événements de sécurité, un certain niveau de collaboration et d'automatisation intelligente sur l'infrastructure de sécurité est essentielle.

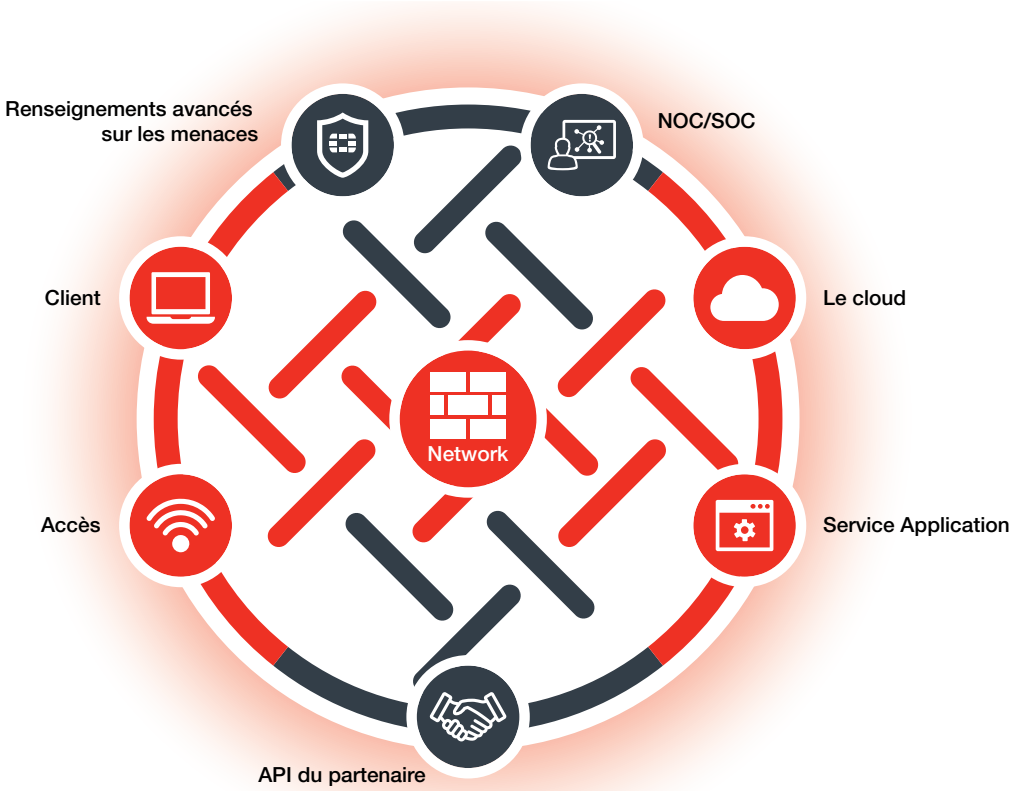
LA SOLUTION FORTINET — UNE SÉCURITÉ CONCEPTUELLE

Si la technologie seule ne permet pas de se conformer au RGPD, la mise en place d'une sécurité réseau de pointe constitue clairement une première étape essentielle. Pour réduire l'exposition à des implications potentiellement paralysantes d'une importante brèche de données, il est nécessaire de réduire le nombre d'intrusions sur le réseau et les délais de détection. C'est ici que Fortinet peut apporter une aide optimale aux efforts de conformité généraux d'une entreprise.

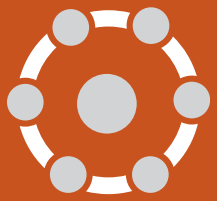
La solution Fortinet cache une nouvelle approche en matière de sécurité dans laquelle tous les composants principaux de l'infrastructure de sécurité sont intégrés à une solution homogène.

FORTINET SECURITY FABRIC

Cette solution repose sur trois propriétés principales : **extensivité, puissance et automatisme**. Fortinet Security Fabric offre une réponse unique aux défis inhérents à la protection des réseaux complexes, haut débit et sans frontières contre la menace de cyber-attaque qui évolue rapidement.



FORTINET SECURITY FABRIC



EXTENSIVITÉ

Conçue pour couvrir la surface d'attaque en expansion du réseau d'une entreprise moderne, la solution Fortinet Security Fabric garantit la protection, la visibilité et le contrôle sur tous les éléments constitutifs de l'environnement, des terminaux filaires et sans fil, à travers les actifs de cloud public et privé, au datacenter, sans oublier les applications elles-mêmes.

Associée à une segmentation dynamique du réseau qui sépare les données et les ressources de manière logique, la solution Fortinet Security Fabric peut sonder le réseau en profondeur pour découvrir de nouvelles menaces tandis qu'elles se déplacent d'une zone à une autre. Ce déploiement extensif et cette visibilité étendue constituent une étape cruciale vers la conformité en facilitant la surveillance des appareils et du trafic interne, en empêchant les accès non autorisés sur les actifs à accès restreint et en limitant la propagation des intrus et des malwares.

En outre, les avantages de Fortinet Security Fabric ne se limite pas au portefeuille de solutions de sécurité de Fortinet. Grâce à des API ouvertes, des technologies d'authentification ouvertes et des données télémétriques normalisées, un écosystème croissant de partenaires compatibles Fabric émerge et permet aux entreprises d'intégrer leurs investissements existants dans la sécurité et l'interconnexion réseau à leur propre solution Fortinet Security Fabric.

PUISSANCE

La puissance de traitement de nombreuses appliances de sécurité traditionnelles ne parvenant pas à suivre le rythme inhérent à la hausse de la bande passante du réseau et de la complexification des menaces, les entreprises sont souvent confrontées à un compromis inacceptable. Elles doivent soit réduire le niveau de protection, entraînant des risques d'intrusion par le biais d'un vecteur d'attaque non protégé ou une partie non sécurité du réseau, soit accepter une chute de performances des applications sur le réseau.

En déchargeant la sécurité et le traitement du contenu vers des unités de traitement de sécurité personnalisées et dédiées qui combinent une accélération matérielle à un micrologiciel hautement optimisé, les produits Fortinet sont devenus les plus rapides de l'industrie et permettent aux entreprises de mettre en place une sécurité complète sans compromettre les performances.

AUTOMATISATION

Outre une visibilité extensive à l'échelle de la surface d'attaque et la capacité de traitement permettant de sonder plus profondément chaque paquet, Fortinet Security Fabric permet également de rassembler les renseignements combinés de ses composants distribués pour corréler plus rapidement les événements et coordonner une réponse rapide, automatique et appropriée au niveau de risque.

Fortinet Security Fabric est en mesure d'isoler rapidement les appareils affectés, de partitionner les segments du réseau, de mettre à jour les règles, d'instaurer de nouvelles politiques et supprimer le malware aussi rapidement que les nouvelles menaces sont détectées. Et comme le réseau d'une entreprise est développé et adapté en fonction de l'évolution des besoins de l'entreprise, Fortinet Security Fabric évolue et s'adapte en conséquence, étendant automatiquement les dernières politiques de sécurité aux nouveaux appareils, charges de travail et services au fur et à mesure de leur déploiement, au niveau local, à distance ou sur le cloud.

SYNTHÈSE

Pour de nombreuses entreprises, la transition initiale vers la conformité au RGPD est probablement un processus lent et complexe. Cependant, la révolution numérique s'accompagnant d'avancées technologiques des deux côtés de la « course à l'armement » dans le domaine de la cybersécurité, cette conformité requerra une réévaluation régulière s'appuyant sur la reconsidération continue des risques.

Dans le cadre de cette démarche continue, la sécurité du réseau joue un rôle fondamental en prévenant les intrusions et en limitant les risques de brèche importante tout en réduisant le délai de détection des nouvelles menaces. Pour ce faire, l'approche en matière de sécurité doit être extensive, puissante et automatique.

Fortinet Security Fabric offre une vision de collaboration technologique qui s'appuie sur la puissance et l'intelligence collectives du portefeuille de solutions de sécurité de Fortinet pour conférer des avantages supérieurs à ceux de ses composants.

Les solutions de sécurité de Fortinet reposent sur une sécurité interconnectée et évolutive combinée à une forte sensibilisation, des renseignements exploitables sur les menaces et des normes API ouvertes. Elles offrent une protection homogène à la plupart des environnements d'entreprise les plus exigeants et ont obtenu la plupart des homologations indépendantes en matière de protection performante et efficace dans l'industrie. Ces solutions, qui découlent de la vision Fortinet Security Fabric, comblent les lacunes des produits individuels existants et offrent aux entreprises d'aujourd'hui la protection extensive, puissante et automatique qu'elles recherchent pour leurs environnements physiques, virtuels et de cloud.

"France
TOUR ATLANTIQUE
11ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33-1-8003-1655"

SIÈGE SOCIAL
INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1.408.235.7700
www.fortinet.com/sales

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tél. : +33.4.8987.0500

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65.6513.3730

AMÉRIQUE LATINE — SIÈGE SOCIAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tél. : +1.954.368.9990

67717 0 1 FR