LIVRE BLANC

RGPD : ÊTES-VOUS PRÊT ?

Les MSP qui traitent les données issues de clients européens doivent se préparer à la mise en conformité dès maintenant.

Kaseya ACCELERATE Online!

Quand il s'agit de se mettre en conformité avec un règlement de cette portée, il faut s'y prendre tôt pour être dans les délais ; si vous attendez la date fixée, il sera trop tard.

Le Règlement général sur la protection des données de l'UE (RGPD) est le changement le plus important apporté à la réglementation sur la confidentialité des données en 20 ans

Le règlement général sur la protection des données (RGPD), ensemble de règles créées par le Parlement européen, le Conseil européen et la Commission européenne, vise à renforcer la protection des données des personnes physiques dans l'Union européenne (UE). Le règlement traite également de l'exportation de données personnelles hors de l'UE.

Tous les fournisseurs de services gérés (MSP) qui traitent les données de clients situés en Europe doivent commencer à se préparer à se conformer au RGPD dès maintenant. En adoptant une approche proactive, les MSP peuvent non seulement garantir leur mise en conformité et, par conséquent, éviter de lourdes amendes, mais ils peuvent également renforcer leur position en matière de cybersécurité à un moment où les menaces sont plus sophistiquées et répandues que jamais.

L'essentiel de cette approche proactive concerne le déploiement des solutions de sécurité qui répondent spécifiquement aux exigences du RGPD.

RGPD – POURQUOI VOUS PRÉPARER AUJOURD'HUI

Le RGPD, qui remplace une directive de 1995 sur la protection de données, ne prendra officiellement effet qu'au 25 mai 2018, après une période de transition de deux ans.

Quand il s'agit de se mettre en conformité avec un règlement de cette portée, il faut s'y prendre tôt pour être dans les délais ; si vous attendez la date fixée, il sera trop tard.

« Les entreprises doivent comprendre qu'il s'agit d'une réforme majeure de la loi sur la protection des données ; elle reconsidère tout ce qui concerne la sécurité des données », a déclaré Joanne Bone, partenaire du cabinet juridique Irwin Mitchell LLP, qui conseille les entreprises de tous les secteurs sur les questions informatiques, avec une spécialisation dans la protection des données et le RGPD.

Selon elle, « toutes les organisations qui pensent que le RGPD constitue juste un simple ajustement des exigences en matière de protection de données n'ont pas compris jusqu'où cette loi pourra influencer un si grand nombre de domaines ». « Compte tenu de l'étendue de la législation, si vous ne commencez pas assez tôt à réfléchir sur les moyens de vous mettre en conformité, cela sera beaucoup plus pénible et coûteux par la suite ».

La préparation au RGPD chez les clients de Bone varie considérablement en fonction de la nature de leur entreprise et de leur taille. Certaines entreprises, telles que les entreprises de services financiers ayant des environnements lourds de données, se préparent à la mise en conformité depuis un certain temps. D'autres par contre ne savent toujours rien du tout des nouvelles règles de protection de données.

« Le fait de ne pas en prendre conscience et de ne pas s'y préparer est inquiétant. YouGov a réalisé un sondage pour notre compte auprès de plus de 2 000 décideurs principaux dans des entreprises au Royaume-Uni, afin de déterminer leur niveau de préparation et les mesures qu'ils ont prises à ce jour. « Les résultats ont montré que moins de la moitié des décideurs principaux (38 %) connaissaient les nouvelles règles du RGPD, et seulement 29 % disent avoir commencé à se préparer pour le RGPD malgré le délai de mise en conformité qui se situe actuellement à moins de 12 mois », explique Bone.

Les fournisseurs de services ne devraient pas considérer le RGPD comme une grosse charge. En fait, il offre une bonne occasion aux MSP de réévaluer la sécurité des données de leurs clients.

Il y a longtemps que les MSP ont compris le besoin de techniques de défense en sécurité informatique permettant de gérer le risque de cyber-attaques, et ils ont adopté des outils de sécurité en conséquence. Ils auront ainsi fait de grands progrès vers la mise en conformité avec le RGPD. Mais dans de nombreux cas, ils devraient davantage s'investir pour se mettre en conformité et échapper à de lourdes amendes.

Les fournisseurs de services ne devraient pas considérer le RGPD comme une grosse charge. En fait, il offre une bonne occasion aux MSP de réévaluer la sécurité des données de leurs clients.

« Beaucoup de clients de fournisseurs de services vont poser plus de questions à ces derniers au sujet de leur sécurité et de leur mise en conformité en général », déclare Hazel Grant, associé et responsable du groupe de confidentialité et d'information du cabinet d'avocats Fieldfisher spécialisé en droit de l'information et de la protection des données.

Selon Grant, « il existe une énorme publicité autour du RGPD ». Les fournisseurs de services verront leur responsabilité augmenter face à des violations de données. Cela signifie que la pression pour améliorer la sécurité sera plus grande que jamais – tant de la part des clients que des chefs d'entreprise au sein de l'organisation. « Il existe une perception du marché selon laquelle la protection des données est importante », dit-elle. « Les entreprises ne veulent pas de cette publicité négative découlant d'une violation de données ».

REPENSER LA SÉCURITÉ

Les efforts de sécurité doivent être menés de manière intégrale. L'adoption d'une approche fragmentaire pour la protection des systèmes et des données (comme l'installation de logiciels antivirus au besoin, le déploiement des correctifs ici et là et la mise en œuvre de processus de sauvegarde de données non suivis de manière cohérente) ne la réduira pas dans ce nouvel environnement.

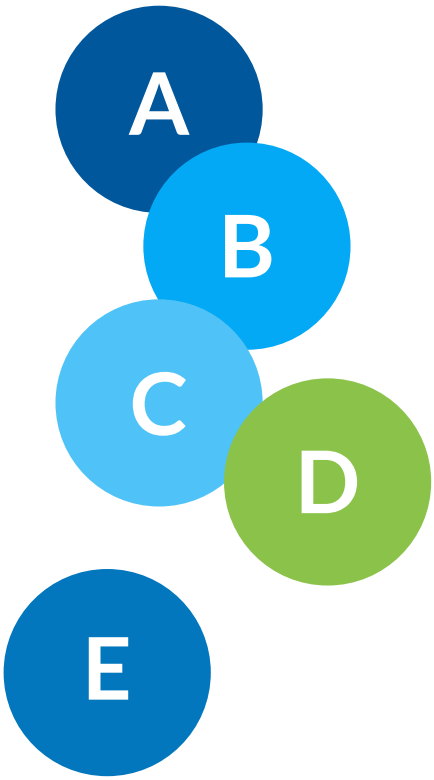
Les menaces à la sécurité aujourd'hui et les nouvelles réglementations visant à renforcer la sécurité comme jamais auparavant nécessitent une approche cohérente et en couches de la sécurité. Les MSP, tirant parti de cette approche en couches, peuvent offrir des services de sécurité plus complets à leurs clients et, en même temps, mieux protéger leurs propres ressources informatiques contre les attaques – et éviter les amendes prévues par la réglementation.

Qu'apporterait une approche en couches de la sécurité ? D'une part, elle devrait donner aux MSP une visibilité complète de leur environnement technologique.

Un bon début consiste à recueillir les informations sur les flux de données dans l'ensemble de l'organisation, puis à créer des documents décrivant le type de données détenues par l'entreprise, l'utilisation qui en est faite, le lieu où elles sont stockées et où elles pourraient être acheminées.

Grant affirme que la responsabilisation est essentielle pour prouver la mise en conformité, de sorte que les entreprises doivent disposer de la documentation sur la localisation et l'utilisation des données, la façon dont elles sont protégées, la façon dont les gens sont formés pour utiliser les données en toute sécurité, etc.

L'une des exigences du RGPD est que les entreprises avertissent rapidement les clients des violations de données et fournissent des détails précis sur la violation. Sans une bonne visibilité des systèmes et réseaux, il est beaucoup plus difficile de le faire en temps opportun.



Pour protéger véritablement les données, les entreprises ont besoin d'une méthode pour identifier facilement et continuellement tous les appareils connectés à leurs réseaux ainsi qu'à ceux de leurs clients. Il s'agit notamment d'avoir une vue des serveurs, des ordinateurs de bureau, des appareils mobiles et d'autres produits pour utilisateurs finaux.

L'une des exigences du RGPD est que les entreprises avertissent rapidement les clients des violations de données et fournissent des détails précis sur la violation. Sans une bonne visibilité des systèmes et réseaux, il est beaucoup plus difficile de le faire en temps opportun.

Une approche en couches devrait également inclure la collecte continue et automatisée des rapports d'état, en temps réel, sur tous les détails d'exploitation des appareils, afin de les tenir à jour. De cette façon, les gestionnaires peuvent savoir si les logiciels anti-programmes malveillants et les correctifs de sécurité sont à jour, et les mettre à jour automatiquement et rapidement au besoin.

TROUVER LES SOLUTIONS APPROPRIÉES

Les solutions disponibles sur le marché aujourd'hui peuvent aider les MSP à tendre vers la conformité au RGPD et à améliorer leur position globale en matière de cybersécurité. Lors de l'évaluation des produits, les décideurs informatiques et de sécurité devraient rechercher certaines caractéristiques qui fournissent des capacités spécifiques de réseau, de systèmes et de protection de données. Et ils doivent s'assurer que les solutions intègrent la mise en conformité dans leurs fonctionnalités.

Par exemple, les produits devraient intégrer le suivi et la gestion à distance, afin de permettre aux entreprises de surveiller de manière proactive les serveurs, les postes de travail, les ordinateurs distants et les applications, ce qui est essentiel à la sécurité. Les MSP doivent avoir un système de surveillance avec notification instantanée des problèmes ou des changements d'état, et recevoir des alertes lorsque des serveurs clés sont défaillants, lorsque les utilisateurs modifient leurs configurations ou lorsqu'une éventuelle violation à la sécurité se produit.

Une autre caractéristique principale est la gestion des correctifs qui maintient automatiquement les serveurs, les postes de travail et les ordinateurs et périphériques distants à jour avec les derniers correctifs de sécurité requis et les mises à jour logicielles. Il est difficile de suivre et d'appliquer les modifications de sécurité ou de logiciel d'une infrastructure informatique, en particulier si les réseaux couvrent divers emplacements et comprennent de nombreux domaines.

La gestion automatisée des correctifs réseau permet aux MSP d'appliquer les politiques et de résoudre facilement les difficultés liées au déploiement des logiciels et des correctifs de sécurité.

Les MSP devraient également surveiller la variété de systèmes d'exploitation utilisés dans leur environnement, y compris Windows, VMware et Linux, ainsi que d'autres systèmes qui couvrent une gamme d'appareils connectés au réseau, des serveurs de base de données et de messagerie, des hyperviseurs, des routeurs, des pare-feux et d'autres composants. Toute plate-forme de surveillance utilisée devrait permettre d'y parvenir.

En déployant les solutions les plus efficaces, les MSP peuvent faciliter leur mise en conformité avec le RGPD. Parallèlement, ils peuvent renforcer leurs moyens de défense contre l'éventail croissant de menaces à la sécurité.

Il est également important de rechercher des solutions qui fournissent des services de routine en matière de sauvegarde et de récupération. La sauvegarde et la récupération fiables et cryptées constituent une partie essentielle de l'approche de sécurité en couches. Des sauvegardes complètes et régulières peuvent constituer un moyen de défense efficace contre les attaques de ransomware, qui sont de plus en plus fréquentes ces dernières années.

Les MSP devraient aussi principalement assurer une gestion complète de l'identité et de l'accès (IAM). Cette fonctionnalité comprend l'authentification multi-facteurs (AMF), notamment la gestion des informations d'identification centralisées, les règles de politiques et l'ouverture d'une session unique pour les utilisateurs finaux, qui vise à protéger les systèmes internes et les systèmes de clients.

Enfin, lorsque vous cherchez un fournisseur pour des solutions de sécurité, dans le cadre d'un effort de mise en conformité avec le RGPD, assurez-vous que le fournisseur comprend les exigences de la réglementation et peut expliquer dans quelle mesure ses produits respectent le RGPD.

CONCLUSION

La mise en application du RGPD est très proche et son impact sera significatif pour tous les MSP qui traitent les données des citoyens européens. Il s'agit notamment des fournisseurs de services qui font des offres de nuage public ou via leur propre centre de données où ils hébergent des applications. Quoi qu'il en soit, ils sont responsables de la protection des données des clients.

Les conséquences de la non-conformité sont élevées et comprennent notamment des amendes potentiellement lourdes. Le règlement stipule que les pénalités pour non-conformité peuvent représenter jusqu'à 4 % du chiffre d'affaires annuel mondial de l'entreprise coupable de violation ou 20 millions d'euros, la valeur la plus élevée étant retenue, en fonction de la nature de l'infraction.

Par-dessus tout, il y a la publicité négative qui pourrait résulter de cette non-conformité et l'impact que cela pourrait engendrer sur la réputation et la marque d'une entreprise, ainsi que sur sa capacité de trouver de nouveaux clients ou de conserver les clients actuels.

Les MSP doivent commencer à se préparer maintenant – s'ils ne l'ont pas déjà fait. Les responsables de l'informatique et de la sécurité doivent travailler avec des représentants issus de divers départements (commercial, juridique, de gestion des risques, des ressources humaines et d'autres domaines de l'organisation liés à la planification). « Il doit s'agir d'une approche collaborative », affirme Bone.

En déployant les solutions les plus efficaces, les MSP peuvent faciliter leur mise en conformité avec le RGPD. Parallèlement, ils peuvent renforcer leurs moyens de défense contre l'éventail croissant de menaces à la sécurité.

Liste de contrôle pour la préparation RGPD

- Avoir une connaissance approfondie des exigences du RGPD, y compris ses différentes composantes, le type de protection de données nécessaire et les délais de conformité.
- Recueillir les informations sur les flux de données dans l'ensemble de l'organisation et créer des documents décrivant le type de données détenues par l'entreprise, l'utilisation qui en est faite, le lieu où elles sont stockées et où elles pourraient se retrouver. Évaluer si la collecte et l'utilisation des données sont autorisées dans la liste définie des fondements juridiques liés à leur utilisation, contenue dans le RGPD. Une part essentielle de toute préparation RGPD consiste à comprendre et à pouvoir apporter la preuve des données en votre possession ainsi que la base juridique de leur utilisation. Si vous n'y parvenez pas, vos autres activités de conformité seront compromises.
- Effectuer une évaluation complète des politiques et des technologies actuelles en matière de sécurité des données, et la comparer aux exigences du RGPD pour une « analyse des lacunes ». S'efforcer à combler toute éventuelle lacune relevée.
- Adopter une approche en couches pour la sécurité des données et assurer ainsi aux clients des services de sécurité plus complets associés à une meilleure protection des ressources informatiques internes contre les attaques.
- Cette approche en couches devrait fournir une visibilité complète de l'environnement technologique et un moyen d'identifier facilement et continuellement tous les appareils connectés aux réseaux de l'entreprise et à ceux des clients.
- Disposer des mécanismes permettant de comprendre rapidement s'il y a eu une violation des données, et d'une procédure facilitant la décision de notifier ou non. Il est également nécessaire d'adopter une procédure qui traite de la réponse à une violation et de la solution potentielle à offrir aux clients.
- Lorsqu'il s'agit de trouver des solutions technologiques pour la mise en conformité, rechercher des fonctionnalités telles que la surveillance et la gestion à distance qui permettent aux entreprises de surveiller de manière proactive les serveurs, les postes de travail, les ordinateurs distants et les applications ; la gestion des correctifs qui maintient les serveurs, les postes de travail et les ordinateurs et périphériques distants à jour par rapport aux derniers correctifs de sécurité requis ; fournir des services de sauvegarde et de récupération de routine ; et fournir une gestion complète de l'identité et des accès.
- Documentez votre mise en conformité et vos décisions en matière de conformité. La responsabilisation sous-tend le RGPD. Vous devez non seulement faire le bon choix, mais également pouvoir le démontrer.

À PROPOS DE KASEYA

KASEYA EST LE FOURNISSEUR LEADER DE LOGICIELS DE GESTION INFORMATIQUE BASÉS SUR LE CLOUD. LES SOLUTIONS KASEYA PERMETTENT AUX PRESTATAIRES DE SERVICES GÉRÉS (MSP) ET AUX ORGANISATIONS IT DE GÉRER ET DE SÉCURISER EFFICACEMENT LES TECHNOLOGIES DE L'INFORMATION EN VUE DE PROPULSER LES SERVICES INFORMATIQUES ET LE SUCCÈS DES ENTREPRISES. PROPOSÉES AUSSI BIEN EN TANT QUE SOLUTION DE POINTE EN MATIÈRE DE CLOUD QUE LOGICIELS SUR SITE, LES SOLUTIONS KASEYA PERMETTENT AUX MSP ET AUX ENTREPRISES DE TAILLE MOYENNE DE CONTRÔLER TOUT LEUR SYSTÈME INFORMATIQUE DE MANIÈRE CENTRALISÉE, DE GÉRER AISÉMENT LES ENVIRONNEMENTS DISTANTS ET DISTRIBUÉS, ET D'AUTOMATISER LES FONCTIONS DE GESTION INFORMATIQUE DANS LEUR ENSEMBLE. À L'HEURE ACTUELLE, LES SOLUTIONS KASEYA SONT UTILISÉES PAR PLUS DE 10 000 CLIENTS DANS LE MONDE, LESQUELS SONT ISSUS DE NOMBREUX SECTEURS D'ACTIVITÉ, NOTAMMENT LE COMMERCE AU DÉTAIL, L'INDUSTRIE MANUFACTURIÈRE, LA SANTÉ, L'ÉDUCATION, L'ADMINISTRATION, LES MÉDIAS, LA TECHNOLOGIE, LES FINANCES ET AUTRES. KASEYA EST UNE ENTREPRISE PRIVÉE AYANT UNE PRÉSENCE DANS PLUS DE 20 PAYS. POUR EN SAVOIR PLUS, VEUILLEZ VISITER LE SITE WWW.KASEYA.COM

Kaseya ACCELERATE