ivanti

Cinq stratégies de sécurité pour la conformité au GDPR

Table des matières

Introduction

Aujourd'hui, les consommateurs ne sont pas satisfaits. Le cybercrime s'étend et gagne de l'argent, alimenté par des criminels qui apprennent sans cesse de nouvelles astuces créatives pour profiter de l'exploitation de précieuses données client. Les exigences de sécurisation du stockage des données personnelles secouent les gouvernements du monde entier. Ils réalisent l'importance de la protection des données et sont contraints de traiter le problème via des solutions législatives toujours plus strictes. Mais ces lois de protection augmentent la charge de travail des personnes chargées de collecter les données client. C'est pourquoi, une fois de plus, les départements IT d'entreprise doivent trouver un moyen de résoudre le conflit entre conformité aux réglementations et productivité de l'entreprise. Ce document examine l'exemple le plus significatif parmi les lois récemment promulguées, et suggère au département IT des solutions pratiques et innovantes pour alléger les efforts et les coûts de la mise en conformité avec ces réglementations.

Aïe !

C'est un fait. Sur le plan des réglementations, difficile de faire mieux que l'Union européenne (UE). En mai 2016, l'UE (célèbre pour sa loi sur l'arc de courbure toléré pour les bananes) a mis en place la réglementation 2016/679[1] « relative à la protection des personnes physiques concernant le traitement des données personnelles et la libre circulation de ces données... ». Appelée GDPR (General Data Protection Regulation, Règlement Général sur la Protection des Données), cette mesure remplace les réglementations précédentes de l'UE, et standardise et renforce les lois sur la sécurité des données client. Nouveautés du GDPR :

- Exigences strictes pour une meilleure prise de contrôle personnel des données par les citoyens européens
- Exigences de notification détaillée en cas de fuite de données
- Obligation pour les entreprises d'embaucher des « responsables de la protection des données » (DPO) chargés de protéger les données données
- Amendes beaucoup plus lourdes pour les entreprises non conformes aux conditions du GDPR

Bien que le GDPR ne prenne effet qu'en mai 2018, il nécessite des changements substantiels dans l'infrastructure de l'entreprise et du département IT, longs et complexes à mettre en place. Et le coût de la non-conformité au GDPR inclut de très lourdes amendes, des pénalités[2], et des dommages et intérêts en cas de non-respect[3]. Les amendes administratives pour non-conformité à certaines conditions du GDPR, à elles seules, peuvent atteindre jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'entreprise. Aïe, vraiment ! Le potentiel de ce fantastique impact financier ne fait pas seulement saliver les financiers de l'UE. Les courtiers en assurance d'entreprise prennent très au sérieux leur évaluation de la conformité au GDPR comme source de risque potentiel, lorsqu'ils calculent les primes d'assurance d'une entreprise. Les entreprises n'ont pas le choix : si elles travaillent avec des pays membres de l'UE, il faut très rapidement se mettre en conformité avec le GDPR. Les enjeux sont très élevés. Et il ne reste plus beaucoup de temps.

Les 5 défis de sécurité qui vous empêchent de dormir

Le GDPR spécifie très clairement qu'il faut protéger la sécurité des données client, mais le texte est beaucoup moins clair sur les mesures exactes à prendre pour y parvenir. Bien que le chemin de la mise en conformité puisse varier d'une entreprise à l'autre, la plupart doivent chercher à implémenter de nouvelles méthodes pour éliminer les vulnérabilités de sécurité que provoquent les 5 difficultés suivantes pour les départements IT :

1. Collaborateurs mobiles qui veulent se connecter partout et à tout moment
2. Utilisateurs avec privilèges qui ont besoin de droits Admin sur une incroyable variété de systèmes
3. Impact (coûteux et dommageable) des ransomwares et des malwares
4. Risques liés à l'embauche et à la fin de contrat des collaborateurs
5. Pistes d'audit : suivi et reporting de l'accès aux données personnelles

C'est assez pour en perdre le sommeil, non ? Heureusement, la technologie peut, par nature, trouver des solutions à toutes les difficultés, même complexes. Nous voulons partager avec vous 5 stratégies de sécurité faciles à mettre en place et rapides à implémenter, qu'il serait judicieux d'ajouter à vos plans de mise en conformité au GDPR.

Stratégie 1 : Réduire l'exposition de sécurité représentée par les collaborateurs mobiles.

Mobilité = productivité. Avec l'aide des connexions sans fil disponibles partout et des applis/services de Cloud, les collaborateurs mobiles dominent le paysage des entreprises... et les feuilles de route des départements IT. Cependant, chaque périphérique et point d'accès mobile augmente sérieusement les risques d'intrusion dans l'infrastructure de l'entreprise par des opérateurs malveillants. Depuis des années, le département IT a développé d'incroyables technologies de sécurité statiques, fondées sur le périmètre... pour les voir maintenant totalement dépassées par les collaborateurs trop zélés qui utilisent leur smartphone alors qu'ils sont connectés au café du coin. Pour protéger les entreprises de ces nouvelles menaces et assurer la conformité au GDPR, il est indispensable d'opter pour les nouveaux contrôles de sécurité et de stratégie avec reconnaissance du contexte. Les contrôles avec reconnaissance du contexte s'adaptent dynamiquement à l'espace de travail numérique de chaque collaborateur, ainsi qu'au niveau de risque de sécurité que cette personne présente à tout moment, sur la base de critères de travail spécifiques :

- L'utilisateur est-il connecté avec un périphérique connu ou un périphérique inconnu ?
- Est-il connecté via un réseau de confiance ou non ?
- Utilise-t-il des lecteurs USB ou des périphériques autorisés par l'entreprise ou non reconnus ?
- Essaie-t-il d'accéder à des informations sensibles pendant ses heures de travail ou à un moment inhabituel de la journée ?

En mettant en place ces contrôles avec reconnaissance du contexte, le département IT contrôle et suit facilement les accès des collaborateurs, et peut créer des pistes d'audit qui serviront à respecter les exigences de conformité au GDPR.

Stratégie 2 : Reprendre le contrôle de l'accès utilisateur avec privilèges.

Les entreprises doivent être à même d'octroyer ou de retirer les droits d'accès IT élevés des utilisateurs, en fonction de ce dont ils ont besoin pour rester productifs. Cependant, les utilisateurs avec privilèges ne sont pas seulement les administrateurs IT ; il peut aussi s'agir, par exemple, de personnes qui ont besoin de télécharger des applications et reçoivent des droits complets sur un domaine au lieu d'un accès limité aux seules ressources dont ils ont besoin. Pour aller plus vite, certaines entreprises accordent des droits d'accès élevés à presque tout le monde dans l'entreprise, simplement parce qu'elles n'ont pas les ressources ou la capacité nécessaires pour gouverner plus prudemment ces accès. Dans la plupart des entreprises, les stratégies d'accès « utilisateur à moindres privilèges » incluent souvent des droits inappropriés. Pourtant, chaque utilisateur doté de privilèges est une cible de choix pour les pirates ; leurs droits d'accès élevés renforcent les

vulnérabilités, car ils permettent aux pirates de naviguer plus facilement dans les réseaux, les systèmes et les applications des entreprises. Les contrôles d'accès dynamiques permettent d'augmenter ou de réduire les niveaux d'accès selon les besoins, de manière automatique, afin que les utilisateurs puissent travailler efficacement sans augmenter les risques de sécurité. Avec ce type de contrôle dynamique, vous pouvez réduire immédiatement les droits des utilisateurs dotés de privilèges, dès que l'administrateur concerné (ou autre utilisateur avec privilège) a fini d'utiliser une application ou signale qu'il a achevé une tâche. Chaque réduction des privilèges utilisateur limite les risques de failles dans la sécurité. La mise en place de contrôles dynamiques peut avoir un impact significatif sur la mise en conformité avec le GDPR.

Stratégie 3 : Contenir les attaques par ransomware et malware.

Les ransomwares et autres malwares n'auront aucun impact sur votre entreprise... s'ils ne peuvent y entrer. Et leur chemin d'entrée le plus courant est l'attaque par e-mail d'hameçonnage. Les pirates utilisent également des sites Web, des lecteurs externes et des périphériques pour transmettre du code malveillant à vos périphériques et obtenir un accès aux données personnelles. Les périphériques sont infectés lorsque l'utilisateur clique sur un lien dans un e-mail, visite des sites Web infectés ou se connecte à un lecteur USB fourni par un tiers. En appliquant des mesures proactives telles que les listes blanches, et en verrouillant l'accès aux sites Web et aux fichiers, les entreprises peuvent limiter leur exposition aux attaques. Les listes blanches permettent d'interdire l'ouverture des exécutables non autorisés. La plupart des entreprises disposent déjà d'un type de liste blanche. Toutefois, en ajoutant un contrôle granulaire au niveau du hachage, qui utilise des signatures pour ouvrir les fichiers ou exécuter les applications, vous ferez un grand pas car les utilisateurs ne pourront plus lancer involontairement une attaque en cliquant sur un lien ou une pièce jointe d'e-mail. Les entreprises peuvent également mettre en place des contrôles permettant de bloquer dynamiquement les utilisateurs afin d'interdire l'accès à des sites Web ou fichiers spécifiques. Cela évite que l'utilisateur enregistre un fichier malveillant sur un lecteur ou un disque local. Il est aussi possible de verrouiller les périphériques externes afin que seuls les fichiers protégés ou chiffrés puissent être ouverts ou enregistrés. Les contrôles proactifs permettent aux entreprises de garantir que les données personnelles sont protégées, et de prouver leur conformité aux exigences de sécurité du GDPR.

Stratégie 4 : Sécuriser l'embauche et la fin de contrat des collaborateurs.

De nombreuses entreprises s'appuient toujours sur des processus manuels pour gérer l'arrivée d'une personne dans l'entreprise ou le départ d'un collaborateur, ce qui provoque souvent des inexactitudes, et des retards de plusieurs jours ou plusieurs semaines. Une étude récente de l'Institut Ponemon a montré que plus de 24 % des personnes ayant quitté leur entreprise avaient conservé l'accès aux données de cette entreprise, parfois des semaines après leur départ[4]. Les processus IT peuvent provisionner automatiquement l'accès des collaborateurs aux applications et services nécessaires pour leur travail, en fonction de leur rôle. Et la même technologie peut servir à déprovisionner ces personnes dès qu'elles quittent l'entreprise, ou lorsqu'elles sont mutées ou changent de rôle. Les stratégies d'application du provisioning et du déprovisioning automatisées sont plus sûres, et elles facilitent grandement le travail de préparation aux audits du département IT. Les processus de provisioning et de déprovisioning doivent être étroitement intégrés à vos applications existantes de ressources humaines, vos systèmes de gestion de projets ou autres magasins d'identités de l'entreprise, afin que les changements d'accès puissent être déclenchés automatiquement lorsqu'un collaborateur change d'état d'identité dans l'un de ces systèmes. Cette approche plus holistique de la gestion du cycle de vie des identités permet aux entreprises de réellement améliorer la productivité et la sécurité, tout en respectant les exigences de conformité au GDPR.

Stratégie 5 : Consigner et suivre l'accès aux données personnelles, pour un reporting précis.

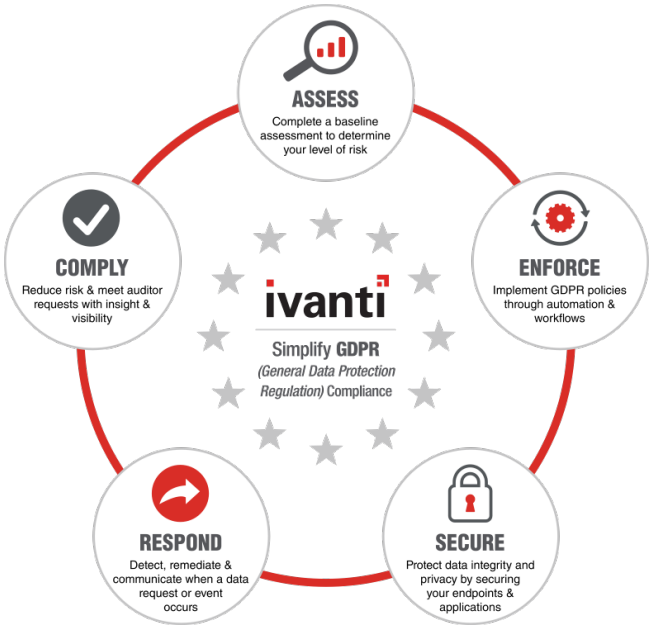
Les entreprises doivent conserver des enregistrements de toutes leurs activités de traitement, afin de générer facilement des rapports sur l'utilisation des données personnelles et la conformité des traitements. Il faut consigner le nom des personnes qui ont accédé aux données et les

entreprises doivent pouvoir prouver que les contrôles appropriés ont été mis en place pour protéger les données personnelles. Les technologies de consignation peuvent suivre les activités et répondre aux demandes des chargés d'audit sans aucun stress. Il faut également pouvoir générer facilement des rapports sur les détails des espaces de travail déployés, avec les changements, les utilisations, les périphériques, les applis et les configurations. Le suivi des journaux et le reporting permettent aux entreprises d'apporter la preuve de leur conformité au GDPR, et de préparer rapidement les informations nécessaires pour signaler toute fuite aux autorités et individus responsables.

Comment Ivanti soutient votre stratégie de GDPR

Pour développer une stratégie de conformité, commencez par évaluer les processus existants et par estimer le niveau de risque en fonction des principes de base du GDPR. Pour certaines exigences, la technologie seule ne suffit pas : il faut effectuer le changement à l'échelle de l'entreprise. C'est notamment le cas de l'embauche d'un DPO (Data Protection Officer, Responsable de la protection des données) ou du développement de votre processus de notification en cas de fuite. Pour être complète, une stratégie de GDPR doit combiner la création de processus en interne, l'implémentation de changements de stratégie et la mise en place de nouvelles technologies. Ivanti vous aide à mettre en œuvre vos solutions de mise en conformité avec le GDPR (General Data Protection Regulation, Règlement Général sur la Protection des Données) afin d'évaluer les risques, d'appliquer des stratégies, de sécuriser les données, de réagir aux incidents et aux demandes, et de prouver votre conformité. Ivanti unifie les opérations IT et de sécurité, ce qui permet de mesurer les risques pour l'ensemble de l'entreprise, afin de faciliter l'implémentation d'un plan complet de mise en conformité au GDPR.

Contactez Ivanti dès aujourd'hui



La date limite de mise en conformité approche à grands pas. Ne perdez pas plus de temps : lancez immédiatement votre projet de conformité au GDPR. Il faut du temps pour mettre en place les processus, les stratégies et les technologies appropriés. Si vous êtes en train de développer votre stratégie de GDPR, contactez Ivanti pour trouver la meilleure façon de limiter les risques grâce à nos solutions d'IT unifiée.

www.ivanti.com/GDPR

+33 (0)1 49 03 77 80

contact@ivanti.fr

[1] http://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Articles 83 & 84
[3] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Article 82
[4] http://media.techtarget.com/Syndication/NATIONALS/Data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf