Point de vue

Gigamon et le Règlement général sur la protection des données de l'Union européenne

Exploiter la visibilité complète pour garantir la conformité

Devant entrer en vigueur le 25 mai 2018, le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE) est un règlement conçu pour garantir la confidentialité des données et la protection de l'ensemble des citoyens de l'UE en renforçant et en unifiant la législation relative à la protection des données à travers l'Europe. Le nouveau règlement, qui remplacera la Directive sur la protection des données 95/46/UE, adoptée en 1995 pour réguler le traitement des données personnelles, a été conçu afin d'améliorer la confiance dans l'économie numérique émergente en offrant aux individus plus de transparence et de contrôle sur l'utilisation de leurs données personnelles. Il s'applique à toute entreprise - indépendamment de la localisation géographique - rassemblant ou traitant des données personnelles sur des résidents de l'UE, et établit des amendes élevées en cas de non-conformité - jusqu'à 4 pour cent des ventes annuelles globales totales ou 20 millions d'euros (EUR) par violation de données.

Aux termes de la Directive sur la protection des données actuelle, les données personnelles constituent toute information concernant une personne physique identifiée ou identifiable pouvant être identifiée, en particulier, en se référant à un numéro d'identification ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, mentale, économique, culturelle ou sociale. Reflétant l'évolution des technologies et des moyens dont les entreprises rassemblent des informations sur les personnes, le RGPD étend cette définition pour inclure des identificateurs en ligne comme :

- Adresses de protocole Internet (IP), dans certains cas.
- Données pseudonymisées, en fonction du site attribuant le pseudonyme à un individu.

Contrôleurs de données, processeurs de données et délégués à la protection des données

Le RGPD s'applique aux activités de traitement des données des entreprises qui agissent comme contrôleurs de données et processeurs de données avec un établissement en UE. Ayant la responsabilité première de la conformité, un contrôleur de données décide de la façon dont des données personnelles sont traitées et de la raison pour laquelle elles le sont ; il peut s'agir tout autant d'entreprises à but lucratif que d'organismes de bienfaisance ou de gouvernements. Un processeur de données, tel une entreprise TI, procède au traitement réel des données pour le compte du contrôleur.

Les contrôleurs de données doivent s'assurer que les données personnelles sont recueillies et traitées légalement, et pour un but spécifique et légitime, par exemple, dans le but d'assurer la sécurité d'un réseau et des informations ou de signaler des menaces criminelles possibles. Les individus peuvent demander à une entreprise d'effacer leurs données sans délai injustifié lorsque l'une des raisons suivantes s'applique :

- Les données personnelles ne sont plus nécessaires relativement aux fins pour lesquelles elles ont été collectées ou autrement traitées.
- La personne concernée retire le consentement sur lequel le traitement se fonde conformément au point (a) de l'Article 6(1), ou au point (a) de l'Article 9(2), et lorsque n'existe plus d'autre justification légale pour le traitement.
- La personne concernée s'oppose au traitement conformément à l'Article 21(1) et il n'existe aucune raison légitime supérieure justifiant le traitement, ou la personne concernée s'oppose au traitement conformément à l'Article 21(2).
- Les données personnelles ont été illégalement traitées.
- Le contrôleur de données doit se conformer à une obligation légale énoncée dans les lois de l'Union européenne ou d'un État membre.
- Les données personnelles ont été collectées en relation à l'offre de services de l'entreprise informatique ainsi que référé dans l'Article 8(1).

Non seulement les contrôleurs de données doivent supprimer l'ensemble des copies ou liens vers les données personnelles lorsque la personne retire son consentement, mais ils doivent également prendre des mesures raisonnables aux fins d'informer les autres entreprises traitant lesdites données. Ceci est connu comme le « droit à l'oubli. » De même, en vertu d'une disposition désignée le « droit à la restriction, » les données doivent également être supprimées - enquête en cours - si une personne conteste l'exactitude de ses données personnelles.

43 % des répondants ne disposent pas d'une visibilité complète de toutes les données circulant à travers leurs réseaux

66 % des répondants pensent qu'un manque de visibilité des données rend difficile de se conformer au RGDP

67 % des répondants conviennent que les angles morts au niveau des réseaux constituent un obstacle majeur en matière de protection des données au sein de leurs entreprises

Source : "Hide and Seek : Cybersecurity vs. the Cloud, » (Cache-cache : Cybersécurité versus Cloud), enquête de la société d'étude de marché indépendante, Vanson Bourne, août 2017.

Il est de la responsabilité des contrôleurs de données de s'assurer que leur processeur respecte les lois sur la protection des données et les processeurs de données doivent eux-mêmes se conformer aux règles afin de maintenir des archives de leurs activités de traitement. Si des processeurs de données sont impliqués dans une violation de données, ils sont également bien plus exposés en vertu du RGPD qu'aux termes de la Directive sur la protection des données actuelle.

Les contrôleurs de données sont également responsables de nommer un Délégué à la protection des données (DPD), dont la tâche est d'informer et de conseiller afin de satisfaire aux exigences du RGDP. Un DPD doit prévoir un plan afin de conduire un audit des informations à travers l'entreprise pour cartographier les flux de données et pour documenter quelles données personnelles sont conservées, quelle est leur provenance et avec qui elles sont partagées. Un DPD doit également s'assurer que les procédures et les technologies adéquates sont en place aux fins de détecter, signaler et enquêter sur une violation de données personnelles. Dans le même temps, un DPD doit surveiller la conformité aux politiques de protection des données et régulièrement passer en revue l'efficacité des activités et des contrôles de traitement des données.

Comment garantir protection et conformité à l'aide de Gigamon

Bien que le RGPD soit techniquement normatif et n'identifie pas les outils ou les technologies requis, la réalité est que de nombreux outils de sécurité réseau nouveaux et existants seront nécessaires, y compris des systèmes de prévention d'intrusion (intrusion prevention systems, IPS), des systèmes de détection d'intrusion (intrusion detection systems, IDS), des anti-malware, des solutions d'informatique réglementaire et des pare-feux prochaine génération destinés à l'application des politiques axées sur les contenus. C'est également, plus ou moins, une certitude que le RGPD encouragera de nouveaux investissements dans des ensembles d'outils existants mais utilisés de façon moindre, tels que :

- Prévention des pertes de données (DLP) : pour identifier et empêcher une utilisation abusive de données et la perte de données en mouvement (data in motion, DIM), ainsi qu'aux fins d'audit et de classification des données au repos (data at rest, DAR) et des données utilisées (data in use, DIU).
- Surveillance d'accès aux fichiers (File Access Monitoring, FAM) : pour détecter les accès non autorisés aux fichiers.
- Surveillance d'accès aux bases de données (Database Access Monitoring, DAM) : pour détecter les accès non autorisés aux bases de données d'entreprise.

Ces ensembles d'outils ont deux points communs : Ils requièrent un accès complet au réseau d'entreprise et ils opèrent généralement à des vitesses inférieures à celles des réseaux centraux modernes. Par exemple, la plupart des outils DLP orientés contenu opèrent à 300 - 500 Mbps, en raison de la nécessité pour eux d'effectuer extraction de fichiers à forte intensité de calcul et analyse de contenu. Par comparaison, un réseau central moderne opère à 10 Gbps ou à 40 Gbps.

Traditionnellement, les entreprises ont déployé des outils DLP à la périphérie des réseaux, où ils voient uniquement les données sortantes. Cependant, la plupart des incidents de perte de données sont non malveillants et correspondent à des échecs de processus opérationnel ou à des erreurs de bonne foi de la part du personnel. Les entreprises peuvent mieux voir et remédier à ces types d'incidents au sein du réseau central, et non à la périphérie du réseau. Par exemple, comment un outil DLP en périphérie de réseau voit-il un utilisateur télécharger des données sensibles, en vertu du RGPD, vers son poste de travail et sur une clé USB ? L'outil DLP doit disposer d'une visibilité du trafic central.

Pour maximiser la visibilité du trafic réseau et optimiser les performances des outils de cybersécurité - incluant des outils DLP - Gigamon offre la plateforme de sécurité GigaSECURE®. Avec sa capacité à surveiller et à transmettre le trafic adéquat aux outils appropriés en temps opportun, la plateforme de sécurité GigaSECURE® peut constituer l'épine dorsale de tout exercice de conformité au RGDP.

Par exemple, la plateforme de sécurité GigaSECURE peut extraire des applications, telles que le trafic vidéo ou de maintenance Windows, qu'un DLP n'a pas besoin de voir ou d'analyser. Au lieu de cela, en transmettant des données appropriées au DLP uniquement, telles que des messages email avec pièces jointes, la plateforme accroît l'efficacité et les chances de l'outil de détecter tout partage de données injustifié ou toute exfiltration de données en temps opportun. Un IPS recourt à une architecture Representational State Transfer (REST) pour indiquer à une solution DLP de terminaison qu'elle doit appliquer un contrôle des périphériques amovibles afin de prévenir un événement potentiel d'exfiltration de données - par exemple, en bloquant toute écriture sur des périphériques USB.

En exploitant la plateforme de sécurité GigaSECURE, les entreprises peuvent connecter ces outils plus lents, mais néanmoins puissants en matière d'inspection, aux réseaux d'entreprise plus rapides et leur transmettre uniquement le trafic qu'ils doivent voir et analyser pour une efficacité maximale.

Le RGPD n'a pas de tolérance pour des protections « juste assez suffisantes ». Il exige des entreprises de faire preuve d'un niveau d'efficacité et d'efficience élevé en matière de sécurité, qui peut être atteint grâce à la plateforme de sécurité GigaSECURE. La solution de Gigamon introduit la visibilité complète du trafic réseau requise pour éliminer les angles morts en termes de surveillance, pour améliorer considérablement l'exactitude et la précision de la détection des risques relatifs aux données et d'aider les entreprises à répondre aux défis posés par le RGDP.

1063-01 08/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 États-Unis | +1 (408) 831-4000 | www.gigamon.com