FORTINET

SÉCURITÉ DES DONNÉES CONFORMÉMENT AU RGPD : COMMENT SE PRÉPARER À L'INÉVITABLE

SOMMAIRE

INTRODUCTION

Le règlement général sur la protection des données (RGPD) de l'Union européenne (UE), qui entrera en vigueur le 25 mai 2018, accroît radicalement les pénalités en cas de protection insuffisante des données personnelles des utilisateurs. Les amendes maximales pouvant être requises à l'encontre d'une organisation remplacent les pénalités qui pouvaient être imposées par le passé; elles peuvent représenter jusqu'à 4% du chiffre d'affaires international de la société en infraction ou 20 millions d'euros, selon la somme la plus élevée.

Malgré cet enjeu énorme, le RGPD offre peu d'indications aux entreprises sur ***la manière*** de garantir leur conformité. Mais, pas de panique, la bonne nouvelle c'est que les sociétés qui ne sont pas encore en conformité avec le règlement ont la possibilité de limiter les amendes encourues, voire de les éviter totalement, en démontrant qu'elles ont pris les bonnes décisions en matière de gestion des données personnelles. Cela s'applique notamment en cas de potentiels vols de données.

Des politiques et pratiques de protection des données bien pensées et proactives peuvent aider à renforcer une organisation, non seulement face à d'éventuelles pénalités du RGPD, mais aussi face aux conséquences que peuvent entraîner des vols de données en termes juridiques et de réputation. Ainsi, la consolidation des processus liés à la protection contre la perte de données et à la détection des menaces est plus importante que jamais.

En développant des politiques de protection des données, les organisations doivent garder à l'esprit les trois points clés suivants :

- Les intrusions sont inévitables.
- L'architecture de sécurité peut nécessiter pseudonymisation et segmentation.
- Une sécurité de pointe est indispensable.

1 LES INTRUSIONS SONT INÉVITABLES

Il n'existe aucune garantie dans le domaine de la protection des données. Tandis que les sociétés de sécurité informatique continuent d'améliorer les défenses des entreprises, les criminels s'efforcent sans cesse de garder un temps d'avance. Les cybercriminels sont de plus en plus créatifs et leur motivation à innover est énorme.

La rapidité et la complexité des attaques d'aujourd'hui signifient que quelles que soient les sommes qu'une société consacre à sa sécurité informatique, elle ne peut que réduire la probabilité d'une intrusion criminelle dans ses systèmes, mais elle ne pourra jamais éliminer totalement la possibilité d'une intrusion. Par conséquent, outre l'attribution de ressources à la prévention des menaces, les organisations doivent aussi envisager des moyens de réduire la fenêtre d'opportunité offerte au criminel en cas d'intrusion.

En moyenne, un cybercriminel qui viole un réseau d'entreprise dispose de 65 jours pour semer le chaos avant que l'intrusion ne soit détectée.[1] Plus cette fenêtre d'opportunité est large, plus le criminel aura le temps de chercher, trouver et dérober des données importantes. À l'inverse, plus la société identifie vite une menace, plus elle a de chances d'atténuer, voire d'empêcher le vol de données.

Le programme de sécurité informatique d'une entreprise doit en partie se concentrer sur la minimisation de la durée écoulée entre le vol de données, sa détection et sa réparation. Les directeurs de la sécurité informatique doivent :

[1] « 2017 Trustwave Global Security Report », Trustwave, juin 2017.

COMPRENDRE LES DONNÉES QUE LEUR SOCIÉTÉ COLLECTE ET CONSERVE

Chaque organisation devrait examiner de près les données personnelles identifiables (DPI) qu'elle collecte ou qu'elle manipule. Certaines de ces données appartiennent-elles à des résidents de l'UE ? Si c'est le cas, la société doit déterminer si elle utilise ces données dans le but initialement recherché et si elle doit continuer à collecter ou à conserver ces informations.

Si les réponses à ces questions sont positives, l'organisation doit alors comprendre où elle conserve les données personnelles des individus, comment elle les protège et comment ces informations se déplacent au sein des systèmes de l'entreprise et sont transmises à des tiers, le cas échéant.

SE PRÉPARER À L'INÉVITABLE

Si une société découvre un vol de données personnelles régi par le RGPD, elle a 72 heures pour signaler l'événement à l'autorité de contrôle compétente, à moins que ce vol « soit peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ». Cela signifie que, dans les trois jours, la société doit déterminer à qui appartiennent les DPI concernées, quels

aspects des DPI ont été exposés et dans quelle mesure la violation est susceptible d'affecter ces personnes.

Les exigences de signalement sont amplifiées lorsque le vol de données personnelles est susceptible « d'engendrer un risque ***élevé*** pour les droits et libertés des personnes physiques ». Dans ce cas, la société doit aussi informer du vol, les résidents de l'UE dont les données ont été affectées.

Pour satisfaire à ces obligations, une organisation qui découvre un vol de données doit très rapidement déterminer les systèmes affectés par le pirate. Cela implique habituellement d'examiner le trafic réseau et de vérifier individuellement chaque appareil et chaque application.

[2] Règlement général sur la protection des données, Article 33 : « Notification à l'autorité de contrôle d'un vol de données à caractère personnel. »
[3] Règlement général sur la protection des données, Article 34 : « Communication à la personne concernée d'un vol de données à caractère personnel. »

Outre le recueil des informations nécessaires pour signaler le vol de données, l'équipe informatique doit éliminer la brèche ayant permis au criminel de pénétrer dans le réseau. Cela permet d'éviter de futurs vols et aide l'équipe de sécurité informatique à s'assurer que le pirate n'a plus de point d'accès au réseau. Il est également crucial pour l'entreprise de bien comprendre le but et l'impact du vol, afin que les informations transmises à l'autorité de protection des données (APD) et/ou aux personnes dont les données ont été affectées, inspirent confiance. À l'inverse, si la société ne signale pas en externe le vol de données, elle doit être parfaitement sûre que l'incident remplit les critères du RGPD la dispensant de signalement.

Quoi qu'il en soit, la rapidité de la réponse est essentielle. En fait, les sociétés qui répondent très vite aux attaques criminelles de leur réseau peuvent être capables de si bien contenir la menace qu'elles minimisent les conséquences possibles de l'incident vis-à-vis du RGPD.

Les entreprises doivent avoir soigneusement documenté leurs plans de réponse à l'incident, plans qui couvrent les procédures de détection et de compréhension des intrusions dans le réseau. Elles doivent déterminer qui sera chargé de ces processus en cas de vol de données. Dans la plupart des cas, les réponses à ces vols impliquent le directeur de la sécurité informatique, le conseiller juridique et un administrateur ou membre du conseil d'administration. Il incombe à ce dernier de prendre la décision finale concernant la réaction publique de la société.

Ensuite, comme pour toutes les procédures de cybersécurité, les plans de réponse aux menaces doivent être testés régulièrement.

S'ASSURER DE LA MISE EN PLACE DE PROCESSUS ET SYSTÈMES DE SAUVEGARDE ET DE RÉCUPÉRATION

Une sauvegarde et une récupération sérieuses de tous les systèmes clés de l'entreprise sont un autre élément nécessaire dans le cadre de la préparation à une potentielle intrusion du réseau. Les fichiers récupérés peuvent être utiles pour tracer l'attaque jusqu'à son point d'origine. Ils peuvent en outre s'avérer inestimables en cas d'attaque par ransomware, dans laquelle les criminels menacent de détruire de façon permanente les données chiffrées exfiltrées de l'entreprise si une rançon ne leur est pas versée.

S'ASSURER DE LA COORDINATION DES SYSTÈMES ET PROCESSUS SUR L'ENSEMBLE DE LA SURFACE D'ATTAQUE

De solides capacités de prévention et de détection des menaces exigent que les informations, les plans et les procédures soient coordonnés sur l'ensemble du réseau de l'entreprise. Des systèmes complexes et décousus ébranlent la capacité de l'organisation à trouver les failles de sécurité et à y répondre, notamment dans l'infrastructure de sécurité réseau. La situation est exacerbée si les mises à jour de renseignements sur les menaces proviennent de fournisseurs multiples. Un correctif peut stopper une attaque particulière le jour-même, tandis qu'il faudra plusieurs semaines pour répondre à une autre alerte de sécurité du système.

L'une des mesures les plus importantes que puisse prendre un directeur de la sécurité informatique pour se préparer à une potentielle faille de sécurité, consiste à évaluer le niveau d'intégration des systèmes de sécurité mis en place par l'entreprise. De nombreuses sociétés possèdent différentes technologies de sécurité remplissant chacune une fonction spécifique au sein de l'infrastructure de sécurité. Le problème est que ces systèmes ne sont pas conçus pour fonctionner ensemble. Lorsque les technologies ne communiquent pas entre elles, l'équipe informatique dispose d'une vision cloisonnée des menaces et manque de transparence sur l'intégralité de la surface d'attaque. Rassembler des données issues de différents systèmes prend du temps et accroît le risque de lacunes de l'analyse.

Dans un tel environnement, les pirates peuvent exploiter les défauts de visibilité entre systèmes. Et si un vol de données est détecté, l'éparpillement des données et des systèmes amplifie la difficulté à déterminer si le vol remplit les critères de signalement du RGPD. Pour toutes ces raisons, les sociétés ont besoin d'une infrastructure de sécurité informatique dans laquelle les systèmes partagent les informations sur les menaces et offrent une totale transparence en temps réel.

2 L'ARCHITECTURE DE SÉCURITÉ PEUT NÉCESSITER UNE PSEUDONYMISATION ET SEGMENTATION

En plus de l'évaluation du degré d'intégration des systèmes de sécurité de l'ensemble de l'infrastructure du réseau, les directeurs de la sécurité informatique qui se préparent au RGPD doivent se poser la question de savoir si, et comment, des données chiffrées sont conservées sur le réseau de l'entreprise.

Certaines organisations choisissent de protéger les données personnelles en les anonymisant, processus qui consiste à supprimer de façon permanente les informations personnelles identifiables. Par exemple, une organisation de santé peut rayer les noms des patients de ses enregistrements afin que les données médicales ne puissent pas être reliées à un individu. Il s'agit là d'un moyen efficace de supprimer les DPI à des fins de sécurité informatique, mais qui peut évidemment poser problème le jour où la société a besoin d'accéder à ces informations. Les données anonymisées ne peuvent en effet jamais être restaurées à leur état d'origine.

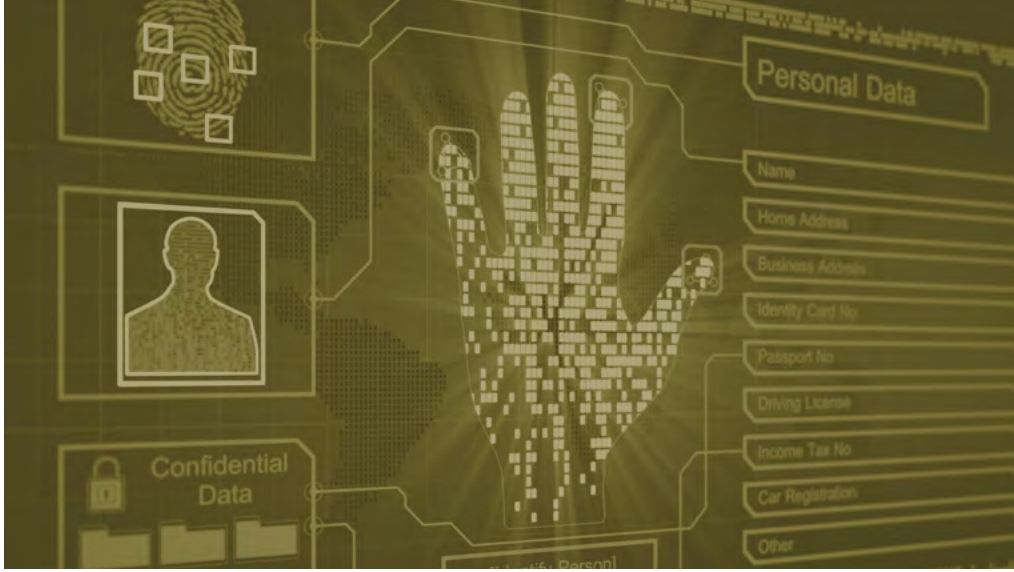
La pseudonymisation peut être une alternative. Comme son nom l'indique, ce processus consiste à remplacer les identifiants personnels comme les noms, par une chaîne de caractères cohérents réversible servant de pseudonyme. Un fichier séparé est utilisé comme clé reliant chaque identifiant personnel au pseudonyme qui lui a été attribué. Si un cybercriminel accédait à un dossier médical pseudonymisé, rien dans le fichier ne relierait les données du patient à un individu particulier. Le pirate devrait aussi accéder au fichier clé pour pouvoir obtenir les identifiants personnels.

LES PSEUDONYMES SONT ESSENTIELS À UNE SÉCURITÉ PLUS PRATIQUE

En fait, le RGPD fait spécifiquement référence à la pseudonymisation en tant que l'une des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».[4] En cas de vol de données, la pseudonymisation démontre aussi aux APD compétentes que la société a fourni un effort significatif pour en minimiser l'impact sur leurs propriétaires. Les exigences de signalement dans le cadre du RGPD sont moins coûteuses pour les sociétés qui utilisent la pseudonymisation que pour celles dont les DPI sont conservées en texte clair, car elle minimise la probabilité de perte de données personnelles.

LA SEGMENTATION DU RÉSEAU MET LES CLÉS HORS D'ATTEINTE

Lorsqu'une société a créé un fichier servant de clé pour un ensemble d'enregistrements pseudonymisés, l'étape suivante logique consiste à séparer la clé des enregistrements en la plaçant sur un segment de réseau différent. Pour accroître encore la protection de ces fichiers, l'organisation peut renforcer la sécurité des segments en déployant des pare-feux internes afin de prévenir tout déplacement d'un éventuel pirate d'un segment à l'autre.



Par exemple, une société peut conserver les dossiers de son personnel dans le service RH, mais utiliser la pseudonymisation afin qu'aucun de ces enregistrements ne puisse être directement lié à un individu. Elle peut ensuite conserver la clé qui relie les pseudonymes aux noms des employés dans le service financier, et placer un pare-feu sur le réseau interne entre ces deux fonctions. Même si un criminel accède au segment du réseau contenant les dossiers RH, il ne pourra pas combler les vides sans accéder aussi au segment financier du réseau. Le pare-feu interne réduira de façon significative sa capacité à naviguer entre ces deux segments du réseau.

[4] Règlement général sur la protection des données, Article 32 : « Sécurité du traitement ».

3 UNE SÉCURITÉ DE POINTE EST INDISPENSABLE

Les termes du RGPD encouragent aussi les sociétés à intégrer des technologies de sécurité de pointe. L'article 25 commence ainsi : **« Compte tenu de l'état des connaissances … le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données… »**[5]

Le règlement ne définit pas « l'état des connaissances » et cite seulement spécifiquement la pseudonymisation. Clairement, l'état des connaissances évoluera avec les technologies de pointe au fur et à mesure de l'évolution du marché de la sécurité informatique. Pour l'instant, on peut supposer que les organisations doivent s'assurer que leur environnement de sécurité utilise des technologies modernes pour protéger les données qu'elles conservent, utilisent et déplacent.

[5] Règlement général sur la protection des données, Article 25 : « Protection des données dès la conception et protection des données par défaut. »

Tout comme elle ébranle les efforts de détection des menaces, la complexité est aussi l'ennemi de la technologie de pointe. Les produits de sécurité individuels ne peuvent pas rester cloisonnés. L'intégration est essentielle à l'efficacité dans une infrastructure de sécurité informatique et indispensable pour satisfaire aux exigences de modernité du RGPD. De la même manière, l'automatisation des activités de neutralisation des menaces est cruciale à la fois pour assurer la sécurité de la société et pour répondre aux exigences de technologies de pointe du RGPD.

Des évaluations des risques en continu sont également nécessaires. Les solutions qui intègrent automatiquement des informations sur les menaces émergentes réduisent le risque de vol de données tout en minimisant l'exposition à des amendes en cas de vol. Ainsi, les solutions et services de sécurité doivent intégrer des renseignements sur les menaces mis à jour en continu afin de tenter de garder un coup d'avance sur les cybercriminels.

CONCLUSION

Tant que le RGPD n'est pas entré en vigueur, personne ne sait vraiment comment chaque pays va appliquer ces instructions. Le Commissariat à l'information du Royaume-Uni (ICO)[6] fournit d'excellentes ressources, y compris une récente publication de blog de la commissaire à l'information Elizabeth Denham qui indique : « il serait alarmiste de suggérer que nous sanctionnerons pour l'exemple des organisations qui commettraient des infractions mineures ou que les amendes maximales seront appliquées le plus souvent ».[7] Même si le RGPD s'imposera en se concentrant sur l'objectif de protection des données plutôt que sur une analyse détaillée des technologies, il mettra l'accent sur tous les aspects de la position et de la philosophie des entreprises en matière de sécurité.

La panique n'est donc pas à l'ordre du jour. L'ordre du jour consiste pour chaque société dans le monde en contact avec les données personnelles de résidents de l'UE, à réévaluer son infrastructure de sécurité informatique. Ses technologies sont-elles à la pointe ? Son réseau inclut-il des mesures de protection des données sophistiquées telles que la prévention et la détection des menaces, la pseudonymisation et la segmentation interne ? Un plan de réponse au vol de données a-t-il été documenté et testé ? Toutes les solutions de sécurité informatique communiquent-elles d'une manière qui protège les données de façon optimale et offre toute la visibilité nécessaire sur le réseau ?

Les directeurs de la sécurité informatique qui peuvent répondre « oui » à toutes ces questions sont en bonne voie pour se préparer à l'inévitable.

[6] Commissariat à l'information (ICO)
[7] Elizabeth Denham, « GDPR—sorting the fact from the fiction » 9 août 2017.

www.fortinet.fr

Copyright © 2017 Fortinet, Inc. Tous droits réservés. 14.12.2017

143874-C-0-FR