Cloud Act, Patriot Act, RGPD
Comment sécuriser vos données sensibles ?

Entretien avec Philippe Anel,
CTO de Mediawen

Souvent, par « sécurité des données », on pense avant tout aux méthodes pour empêcher les intrusions et le vol par des personnes malveillantes. C'est une partie du sujet. Mais aujourd'hui plus qu'hier, la montée en puissance de l'analyse massive de données par ce qu'on appelle maladroitement « intelligence artificielle », ou plus justement « machine learning » pose un un autre problème.

En effet, les données à protéger ne sont plus seulement issues du travail d'une entreprise que l'on pourrait stocker dans un coffre-fort. Il ne s'agit plus de protéger par tous les moyens la formule chimique secrète qui va changer le monde.

Aujourd'hui, ce qui prend le plus de valeur, ce sont les données collectées sur les personnes et la façon dont ils utilisent, au quotidien, tel ou tel produit, tel ou tel service, telle ou telle donnée. Ces données valent de l'or et peuvent être utilisées pour nuire à la personne, voire à tout un groupe de personne.

Ces nouveaux algorithmes, boostés par la puissance de calcul et surtout l'extraordinaire quantité de données collectées, permettent de savoir « qui » vous êtes, statistiquement parlant, parfois mieux que vous-même [1].

Dès lors, il est essentiel pour une entreprise de savoir expliquer comment elle utilise les données collectées quand elle construit un service, à quelles fins. Nous entrepreneurs, utilisons ces données, et nous devons informer sur la manière dont on les protège. C'est une marque de respect et de confiance vis-à-vis de nos clients.

Mise aux normes, bonnes pratiques, RGPD.

La raison d'être d'une société est de vendre, si possible rapidement. Et parfois, parce qu'on n'en a pas saisi l'importance, cela se fait au détriment de la sécurisation des services : « on verra plus tard ». Mais ne nous y trompons pas, le client comprend de mieux en mieux l'importance de la protection de ses propres données. Et depuis les début de la RGPD, il le fait savoir.

Pourtant on se réveille, aujourd'hui encore en avril 2019, avec des informations inquiétantes concernant le fait, par exemple, que Facebook a conservé des millions de mots de passe de manière non-sécurisée [2] [3].

Et concernant Facebook, cela fait suite aux scandales qui ont accompagné les élections américaines ou bien les enquêtes pénales en cours concernant l'utilisation des données [4].

L'utilisateur ou le client a bien raison de se renseigner. Il utilisera alors la terminologie en vogue, comme « compliance » dont la signification la plus proche est la "conformité" des normes de sécurité. La prise de conscience des enjeux de sécurisation des données conduit à identifier toujours plus les bonnes pratiques et les meilleures méthodes. Et il y en a.

Cette démarche englobe plusieurs dimensions : la sensibilisation des collaborateurs de l'entreprise, une démarche contractuelle et une réflexion technique. Du côté des clients, les données sensibles peuvent

être de deux natures : la première donnée à protéger est la donnée brute, les contenus traités. Mais les données personnelles des clients ou des utilisateurs d'un service ne sont pas moins importantes. Et ça ne s'arrange pas quand les États s'en mêlent.

Cloud Act - Patriot Act, même combat ?

Le Patriot Act [5] permet aux agences gouvernementales américaines comme la NSA, la CIA ou le FBI d'obtenir des informations dans le cadre d'enquêtes liées au terrorisme. Cette loi ne concerne que les données stockées sur des serveurs aux États-Unis. Elle paraît légitime dans le contexte international que nous vivons.

Le Cloud Act [6], c'est autre chose. Ratifié par Donald Trump le vendredi 23 mars 2018 [7], il permet dans le cadre d'une enquête judiciaire, l'accès par les autorités américaines à des données électroniques stockées à l'étranger. Les autorités américaines bénéficiant d'un mandat peuvent alors demander à un fournisseur de service de droit américain de fournir vos données y compris sur des serveurs hébergés en Europe. Et ce sans même vous en informer !

La RGPD ne nous protège-t-elle pas contre le Cloud Act ?

La RGPD ne peut rien sur ce sujet. Une entreprise ou un fournisseur de service de droit américain, même répondant aux règles de la RGPD, se soumettra à la juridiction américaine. En théorie, il serait possible que cette entreprise, basée en Europe, s'y oppose. Mais dans les faits, cela est bien trop risqué pour son image : elle pourrait être désignée responsable en cas d'attaque terroriste par exemple, ou accusée de protéger des criminels. Et cela peut nuire à ses affaires. [8]

Bonnes pratiques pour sécuriser ses données d'entreprise

Pour sécuriser les données d'une entreprise, il faut d'abord prendre conscience que le plus grand risque vient de l'intérieur. L'idée n'est pas d'avoir de la défiance envers ses collaborateurs. Mais si on a conscience que nos données sont comme un trésor, il est facile de comprendre que limiter l'accès à celles-ci est pour le moins logique.

Valoriser les données inclut le risque de pouvoir les perdre. En général, on en prend pleinement conscience quand ça arrive: un vol d'ordinateur ou de téléphone, un disque dur qui refuse de redémarrer, une mauvaise manipulation qui efface tout... Contre la perte de vos données, la réponse est simple : backup et redondance des données dans des lieux géographiques distants.

Mais si on multiplie les sauvegardes et les espaces de stockage, on multiplie également les risques de vol. Pour accroître cette sécurisation des données, la cryptographie est un outil à considérer, en y mettant les moyens face à la puissance de calcul maintenant à la disposition de tous, et à l'arrivée prochaine des ordinateurs quantiques.

Si l'accès « légal » à vos données, autorisé par le Cloud Act ou le Patriot Act, est un frein pour vos clients, le mieux est de faire héberger vos données en Europe, par une société européenne. Il faudra en ce cas vous assurer qu'elle n'est pas rachetée ou financée par une société américaine qui permettrait ce droit extra-territorial d'accès à vos données. Cette souveraineté numérique est aujourd'hui un défi majeur pour les entreprises. Elles doivent maîtriser leurs données.

Il y a aussi l’aspiration illégale comme le Hacking ou le Sniffing. C’est un sujet compliqué. Il faut à mon avis inciter, voire imposer à vos clients et utilisateurs des navigateurs ou des systèmes d’exploitation à jour et sécurisés. Je sais combien cela peut s’avérer difficile. C’est une vraie contrainte et la mise à jour peut signifier parfois l’obsolescence des outils utilisés.

Ensuite, côté développement, j’ai un point de vue assez extrême. Il faut éviter d’utiliser des frameworks tous faits qui sont autant de vecteurs d’attaques possibles. Par exemple, en ce qui concerne l’authentification, si vous laissez un utilisateur s’authentifier grâce à son compte Facebook ou Google sur votre site, comment pouvez-vous prétendre pouvoir le protéger ? À n’en pas douter, C’est pratique et rapide à mettre en place. Mais à quel prix si vous subissez une attaque conséquente ?

Quand on a peu de moyens, il faut d’abord viser la simplicité. De nombreuses failles de sécurité informatique viennent de la complexité grandissante des outils disponibles. Pour les développeurs, l’article de Russ Cox au sujet des dépendances logiciels est très intéressant à lire [9].

À Mediawen, l’utilisation d’un serveur dédié pour garder les données importantes comme les données utilisateurs est une des réponses. Les machines virtuelles sont certes moins chères, mais elles sont aussi partagées avec d’autres machines virtuelles. Et ce qu’on sait aujourd’hui des failles de sécurités de type Meltdown [10] et Spectre [11] des processeurs actuels n’inspire pas vraiment confiance. La littérature ne manque pas le sujet. Les patchs non plus d’ailleurs !

D’ailleurs, il faut impérativement avoir des composants à jour, par exemple avec le protocole TLS amené à remplacer le SSL. Les failles de type heartbleed [12] ont fait d’énormes dégats ! N’hésitez pas non plus à suivre les informations concernant la vulnérabilité de toute la chaine de développement que vous utilisez. Il convient de mettre à jour ses compilateurs et ses outils régulièrement ! [13]

Globalement, la veille technologique est indispensable. L’indépendance technologique est indispensable ! Pouvoir écrire un code facile à maintenir, bien documenté et bien architecturé permettra de s’adapter aux nouveaux vecteurs d’attaques.

Quelles sont les questions posées par les clients ?

Les questions qui sont posées sont plus simples : « Où sont hébergées mes données ? », « avec qui travaillez-vous ? », « proposez-vous aussi du Saas privé ? », « proposez-vous de l’On Premise ? (c’est-à-dire la possibilité d’installer un service directement sur le serveur du client) », « comment assurez-vous la protection des données ? », « comment et quand la sauvegarde est-elle effectuée ? », « puis-je à chaque instant effacer mes données ? », « Puis-je obtenir les données collectées par votre service qui me concerne ? » …

Vous comprenez bien que dans ces conditions, répondre « on verra plus tard » n'est pas acceptable. La sécurité informatique, on doit y penser d’abord, c'est un socle sur lequel on développe des produits ou des services. Si cette attention vient trop tard, c’est beaucoup plus difficile et beaucoup plus coûteux. Et dans certains cas, c'est parfois trop tard.

La réponse n’est pas seulement technique, mais un peu quand même.

Il faut écrire du code avec des outils récents car il y a eu d’énormes progrès dans les langages de programmation et dans les outils mis à disposition, notamment pour simplifier le travail de test et de validation. Par exemple, dans le langage de programmation go [14], que j’utilise de plus en plus, il y a

toute une infrastructure pour le test. Vous pouvez en savoir plus, lire [15]. Ces outils sont de plus en plus présents dans tous les langages de programmation.

On en parle peu dans la presse, mais depuis quelques temps, de nouvelles attaques utilisent comme vecteurs des failles dans le hardware de certains microprocesseurs [10] [11] [16]. Ce sont des situations extrêmement graves. Là aussi il est possible de se protéger. Il faut s'en donner les moyens.

Je l'ai évoqué précédemment, l'utilisation de serveurs dédiés plutôt que des machines virtuelles, et le chiffrement sont de réelles solutions. Si les données sont chiffrées, il sera plus difficile de les lire, davantage si on réduit la surface d'intrusion de votre serveur.

Attention toutefois à la méthode employée. De fait, les données doivent être exploitées. Et pour cela elles doivent, à un moment où à un autre être décryptées. Si vous donnez à une entité malveillante la possibilité de récupérer vos clefs de cryptographie, alors vos efforts n'auront servi à rien.

La réponse est-elle aussi juridique ?

Mais il convient aussi de protéger aussi jurisiquement, nos données comme celles de nos utilisateurs. Cela commence par l'utilisation de ressources qui assurent le respect de la confidentialité des données. En Europe, la RGPD protège concrètement les données des utilisateurs. La souveraineté des données pour les entreprises est l'enjeu majeur aujourd'hui. La « compliance » ou conformité de la sécurisation des données que vous manipulez doit être mise en place et actualisée, dans un environnement qui évolue rapidement.

La réponse est au final humaine et culturelle.

Pourtant, je crains que la RGPD ne suffise pas à résoudre ces défis. Ce qui fait la force de la RGPD, c'est la prise de conscience des enjeux et parfois aussi des menaces. C'est désolant mais pragmatique.

La « compliance », c'est aussi sensibiliser les collaborateurs de l'entreprise ou de l'organisation avec des contenus de formation sur la confidentialité et la sécurisation des données. Sans cette pédagogie et cette prise de conscience par chacun dans l'entreprise, la mise en oeuvre sera compliquée, voire impossible.

La réponse a en fait aussi une dimension politique : elle viendra de la capacité de nos gouvernements en Europe à soutenir une direction commune et à créer des acteurs capables de concurrencer les leaders actuels. Aujourd'hui, nous sommes en retard. Mais demain ?

La sécurité, tout un programme.

Tout cela nous indique qu'il est préférable de travailler avec des sociétés européennes et dont les serveurs sont en Europe. Cela ne veut pas dire se fermer aux autres marchés, mais juste être capable de garantir aux clients qu'ils peuvent profiter d'une législation qui protège l'utilisateur.

Les clients doivent savoir quelles sont les données qu'ils veulent protéger et avoir suffisamment d'information pour les aider à réfléchir sur les compromis qu'ils sont prêts à faire. Notre rôle est d'expliquer les moyens à mettre en œuvre pour proposer la sécurité optimale et ses conséquences.

Pour cela, la première chose à faire est sans doute de concevoir une application facilement portable d’un fournisseur de ressources à un autre. La modularité et l’agilité sont indispensables, pour ne pas être entièrement dépendant d'un tiers et garder la maîtrise et de vos données et de l'avenir de votre entreprise.

Philippe Anel, 2019.

Addendum

Cet article fait suite à l'interview publiée sur le blog de Xperteam [17]

Philippe Anel, CTO de Mediawen, a travaillé plus de 10 années dans le domaine de la sécurité pour des sociétés américaines et israéliennes (Trustware/Bufferzone, LANDesk), en particulier en lien avec la prévention d’intrusion des machines lors d’attaques virales ou simplement malveillantes.

Liste des liens :

[1] https://www.europe1.fr/sciences/Facebook-vous-connait-beaucoup-mieux-que-vos-proches-761818

[2] https://www.lemonde.fr/pixels/article/2019/03/21/facebook-a-conserve-des-centaines-de-millions-de-mots-de-passe-de-maniere-non-securisee_5439366_4408996.html

[3] https://www.lemonde.fr/pixels/article/2019/04/04/les-donnees-de-540-millions-d-utilisateurs-de-facebook-librement-accessibles_5445690_4408996.html

[4] https://www.lemonde.fr/pixels/article/2019/03/14/facebook-enquete-penale-aux-etats-unis-sur-des-acces-partenaires-aux-donnees-des-utilisateurs_5435938_4408996.html

[5] https://fr.wikipedia.org/wiki/USA_PATRIOT_Act

[6] https://fr.wikipedia.org/wiki/CLOUD_Act

[7] https://www.lemonde.fr/pixels/article/2018/03/24/aux-etats-unis-une-loi-vise-a-encadrer-la-saisie-d-emails-a-l-etranger_5275736_4408996.html

[8] https://blog.httpcs.com/cloud-act-et-rgpd/

[9] https://research.swtch.com/deps

[10] https://fr.wikipedia.org/wiki/Meltdown_(vuln%C3%A9rabilit%C3%A9)

[11] https://spectreattack.com/spectre.pdf

[12] http://heartbleed.com/

[13] https://www.cvedetails.com/vendor/14185/Golang.html

[14] https://golang.org

[15] https://golang.org/pkg/testing/

[16] https://fr.wikipedia.org/wiki/Mart%C3%A8lement_de_m%C3%A9moire

[17] https://xperteam.net/cloud-act-patriot-act-rgpd-proteger-vos-donnees-sensibles/