Les données au service de la souveraineté européenne

Thierry LEBLOND, Timothée REBOURS

Cet article est une retranscription de l'audition de Timothée Rebours, cofondateur de SEALD, éditeur du logiciel éponyme et de Thierry Leblond, cofondateur de SCILLE, éditeur du logiciel PARSEC, deux logiciels de cybersécurité « zero trust », par chiffrement de bout-en-bout, des données sensibles sur le *Cloud*.[1]

Qu'est-ce que le chiffrement ?

Timothée REBOURS – Tout le monde utilise tous les jours le chiffrement, par exemple en étant connecté à une visioconférence Teams : la connexion qu'on a entre nous et les serveurs de Microsoft est chiffrée, dans une technologie que l'on appelle TLS[2], qui est une sorte de « tuyau ».

Microsoft de son côté centralise la visioconférence et redistribue notre image et notre son à tous les autres participants.

C'est une technologie qui prend une donnée et permet de la transformer en quelque chose qui n'est lisible que par les seuls détenteurs d'un secret qu'on l'appelle « une clé ». La principale question qui se pose est : qui détient la clé ? Toute personne ayant en sa possession la clé de chiffrement d'une donnée chiffrée, est en mesure de la lire. Si l'on reprend le cas de Microsoft sur une visioconférence à laquelle nous sommes tous connectés via Teams, Microsoft nous indique que tout est chiffré, mais Microsoft détient la clé de chiffrement, et donc est capable de lire, d'entendre, et de voir tout ce que l'on se dit pendant une conférence.

Donc chiffrer ne veut pas forcément dire sécuriser. L'enjeu du chiffrement réside dans la maîtrise de celui qui détient les clés de (dé) chiffrement, plutôt que dans le chiffrement proprement dit. La question du chiffrement des données se résume à deux questions :

1. Que veut-on chiffrer ?

2. Qui détient la clé de chiffrement ?

Schématiquement, les algorithmes de chiffrement sont soit « robustes » quand il n'existe pas de technique pour les casser, soit « vulnérables » quand ils sont faciles à casser par des mathématiciens. Il n'y a pas de chiffrement « moyen fort ». La seule faiblesse qui peut exister dans du chiffrement utilisant des algorithmes « robustes » réside donc dans le transfert de la confiance à celui « qui détient les clés ».

(1) Cet entretien est intervenu dans le cadre du rapport de La Villa Numéris intitulé Les données au service de la souveraineté européenne, paru le 28 septembre 2021 : https://www.lavillanumeris.com/210928_datatransfer). Think tank indépendant, La Villa Numeris promeut un modèle européen du numérique affirmant la primauté de l'humain. La maîtrise de notre destin numérique est un impératif au risque, sans cela, du déclassement économique et géopolitique.

(2) TLS (Transport Layer Security) : protocole de sécurisation des échanges par réseau informatique, notamment par Internet.

Thierry LEBLOND

Thierry Leblond est membre du conseil EuroDéfense France et président de SCILLE, éditeur du logiciel de cybersécurité des données PARSEC, certifié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dédié au partage *Zero Trust* et anti-*ransomware* des données sensibles sur le *cloud* public. Il est également ingénieur général de l'armement.

Timothée REBOURS

Timothée Rebours est cofondateur de Seald depuis 2016, société qui permet le chiffrement de données de l'entreprise par un kit de développement logiciel certifié par l'ANSSI. Il a suivi une double formation en parallèle comme ingénieur à Polytechnique et à l'Université de Californie à Berkeley en 2015-2016.

D'un point de vue juridique, le chiffrement est un peu analogue à un coffre-fort, qui ne peut être ouvert que par la personne qui possède la clef. Mais l'analogie s'arrête là, car on peut forcer le coffre-fort mais pas le chiffrement, à moins d'avoir conçu à l'avance une clef disponible pour quelqu'un d'autre : une porte dérobée ou *backdoor*.

Par exemple, quand un juge ordonne le déchiffrement des données gérées par une personne, si l'entreprise visée n'a pas la clé, elle ne pourra pas le lire, et le mandat du juge n'aura donc pas de sens.

Peut imaginer un déchiffrement possible avec un ordinateur extrêmement puissant, par exemple à l'aide de technologies quantiques ?

Timothée REBOURS – Il y a en effet une simplification qui est faite ici. Une clé c'est une chaîne de caractères aléatoires. On peut tout à fait imaginer une attaque par force brute[3], qui va essayer toutes les combinaisons possibles ; mais il y a tellement de possibilités qu'il est impensable de construire une telle machine dans les X prochaines années. Ce X varie selon la taille de la clé et l'algorithme utilisé. Il est estimé en fonction des connaissances actuelles par des autorités comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou le National Institute of Standard and Technology (NIST[4]). Sur des algorithmes type AES[5], ordinateur quantique[6] ou pas, cela ne changera rien.

Il y a d'autres algorithmes qui sont dits « à cryptographie asymétrique » qui sont sensibles à l'émergence d'un ordinateur quantique, qui, si l'on arrivait à en fabriquer un, permettrait de rendre plus vulnérable l'algorithme. Il passerait donc du range de « robuste » à « vulnérable ».

Un algorithme peut être déclassé : par exemple, demain, il peut y avoir un mathématicien, un chercheur ou des services de renseignement qui vont trouver une manière d'attaquer tel algorithme. À partir de ce moment-là, on va déclasser l'algorithme.

Les autorités gouvernementales, par exemple, si elles détiennent un ordinateur quantique qui peut casser du RSA[7], vont alerter en disant qu'on va arrêter d'utiliser des algorithmes vulnérables à ce genre d'attaque, car cela met en péril l'usage sécurisé d'Internet. Si un ordinateur quantique émergeait et permettait de casser un algorithme de type RSA, plus rien sur Internet aujourd'hui ne serait résistant.

(3) Attaque par force brute : méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.
(4) Agence du département du commerce des États-Unis promouvant l'économie en développant les technologies, la métrologie et des normes de concert avec l'industrie.
(5) Algorithme AES (Advanced Encryption Standard) : algorithme de chiffrement avancé.
(6) Ordinateur quantique : il travaille sur des données quantiques dont l'état peut posséder une infinité de valeurs.
(7) Algorithme RSA : algorithme de cryptographie asymétrique utilisé pour échanger des données confidentielles sur Internet

Lors d'une réunion précédente, nous avons échangé autour de la souveraineté numérique[8] avec une personne qui soutenait fortement une protection européenne parce que disait-il, tout était déchiffrable.

Timothée REBOURS - Si on n'a pas la clé on ne peut pas déchiffrer une donnée chiffrée. Mais cela ne préjuge en rien de « ce qu'on pourra décrypter (c'est-à-dire obtenir la donnée en clair, sans la clé) dans 50 ans ».

L'ANSSI émet des recommandations sur le dimensionnement et les choix d'algorithmes à faire à ce sujet-là pour qu'une attaque par force brute ne soit pas envisageable avant un certain temps, mais elle ne va pas au-delà de 2030, car elle considère qu'au-delà il est difficile de prédire de façon absolue ce qui sera robuste. On peut noter que pour des usages militaires, les données peuvent transiter par Internet avec une couche de chiffrement spécifique (typiquement des données « diffusion restreinte »), ils recommandent l'usage d'algorithmes de chiffrement identiques au monde civil, soulignant la robustesse aujourd'hui des méthodes utilisées.

Mais il est vrai que tout ce qui peut être chiffré pourrait être décrypté, si demain un cryptanalyste réussissait à casser l'algorithme de chiffrement utilisé ; c'est un risque faible, mais c'est un risque.

Thierry LEBLOND – Quand on parle de sécurité sur Internet, il faut bien comprendre qu'il y a 3 niveaux de sécurité :

1. La sécurité de l'authentification, qui permet de savoir à qui on a affaire et de prouver qu'on est bien la personne qu'on prétend être. On peut considérer que la sécurité de l'authentification est parfaitement maîtrisée, avec la double authentification forte MFA[9] ou d'une façon générale les technologies de gestion des identités et des accès ou IAM[10] ;

2. La sécurité du transport : c'est le chiffrement TLS, dont on vient de parler, qui consiste pour un terminal informatique à communiquer avec un serveur par un canal étanche de manière qu'un tiers ne puisse pas accéder à l'information. Ce canal est sécurisé par un chiffrement qu'on appelle le HTTPS ou le TLS et qui n'apporte pas la garantie de sécurité et d'étanchéité, car il est accessible sur le plan gouvernemental. Cependant, en première approximation, pour la sécurité du transport, on peut considérer que le HTTPS[11] et le TLS résolvent le problème ;

3. la sécurité du partage : c'est le vrai sujet, car il est très difficile de partager des informations chiffrées, donc par conception non partageables. En effet, cela pose la question de la sécurité et paradoxalement de l'ergonomie de l'opération de transfert des clés, généralement complexe. C'est ce qui est le plus difficile à faire ; ce sont les technologies sur lesquelles on travaille actuellement.

> SCHÉMATIQUEMENT, LES ALGORITHMES DE CHIFFREMENT SONT SOIT « ROBUSTES » QUAND IL N'EXISTE PAS DE TECHNIQUE POUR LES CASSER, SOIT « VULNÉRABLES » QUAND ILS SONT FACILES À CASSER PAR DES MATHÉMATICIENS. IL N'Y A PAS DE CHIFFREMENT « MOYEN FORT ». LA SEULE FAIBLESSE QUI PEUT EXISTER DANS DU CHIFFREMENT UTILISANT DES ALGORITHMES « ROBUSTES » RÉSIDE DONC DANS LE TRANSFERT DE LA CONFIANCE À CELUI « QUI DÉTIENT LES CLÉS ».

Timothée REBOURS – quand tu dis que TLS est accessible niveau gouvernemental, il faut nuancer le propos. Le protocole lui-même n'est pas attaquable ni par le gouvernement ni par un attaquant, en revanche le point d'entrée et le point de sortie sont maîtrisables par le gouvernement, notamment le point de sortie du serveur

(8) La souveraineté numérique désigne l'application des principes de souveraineté au domaine des technologies de l'information et de la communication (TIC), c'est-à-dire à l'informatique et aux télécommunications.
(9) Le MFA (Multi Factor Authentification) consiste à demander au moins deux facteurs d'authentification (je possède un token, je connais un pin ou un mot de passe, je suis une empreinte digitale, une reconnaissance faciale ou une signature acoustique de voix).
(10) IAM : en sécurité des systèmes d'information, la gestion des identités et des accès (GIA) (en anglais Identity and Access Management : IAM) est l'ensemble des processus mis en œuvre par une entité pour la gestion des habilitations de ses utilisateurs à son système d'information ou ses applications. Il s'agit donc de gérer qui a accès à quelle information à travers le temps. Cela implique ainsi d'administrer la création, la modification, et les droits d'accès de chaque identité numérique interagissant avec les ressources de l'entité. La gestion des identités et des accès s'intéresse par exemple au contrôle de la façon dont les utilisateurs acquièrent une identité, la protection de cette identité et les technologies permettant cette protection (source Wikipedia).
(11) HTTPS : Hypertext Transfer Protocol Secure ou protocole de transfert hypertexte sécurisé.

qui peut être saisi par un gouvernement. Le protocole en lui-même, TLS n'est pas attaquable.

Thierry LEBLOND – Oui. Tu évoques les 2 niveaux de chiffrement possibles ; il faut bien comprendre qu'il y a deux types de chiffrement :

1. Le chiffrement symétrique : la clé qui permet de chiffrer est la même que celle qui permet de déchiffrer. J'insiste bien sur le terme « chiffrer » et pas « crypter », car décrypter, c'est arriver à lire une information chiffrée dont on ne possède pas la clé. Chiffrer, c'est donc brouiller une information à partir d'une clé que l'on possède. Et déchiffrer, c'est, à partir de cette même clé que l'on possède, lire l'information en clair ;

2. Le chiffrement asymétrique : il s'appuie sur des algorithmes, notamment le fameux RSA. On chiffre avec la clé publique du destinataire et le destinataire déchiffre avec sa clé privée. On parle de bi-clés (un binôme clé publique/clé privée). Cet algorithme repose sur le principe qu'il est impossible (sauf en faisant des calculs de brute force très chronophages) de factoriser un nombre en ses facteurs premiers, à partir du moment où les nombres en question sont suffisamment gigantesques.

Le jour où l'on est en mesure de casser ces algorithmes asymétriques, comme le promettent les technologies d'ordinateurs quantiques, ce ne sera pas si grave, car, dans les applications bien faites, on remplacera juste la bibliothèque de chiffrement par une autre basée sur les algorithmes post-quantiques qui se fondent sur d'autres principes mathématiques, donc des algorithmes qui ne peuvent pas être cassés par un ordinateur quantique.

Timothée REBOURS – On attend d'ailleurs une standardisation qui sera faite (sûrement l'année prochaine) par l'ANSSI, le NIST et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), à l'échelle européenne, qui va produire une spécification des algorithmes qu'il faudra utiliser pour être résistant à un ordinateur quantique.

Thierry LEBLOND – Il y a d'autres éléments qui entrent en ligne de compte, ce sont les questions de latence, parce que faire du chiffrement cela oblige à faire plus de calculs. Il faut avoir une approche scientifique pour choisir les bons algorithmes en fonction de ce que l'on veut faire pour que l'expérience utilisateur ne soit pas éloignée de ce qu'il a l'habitude de faire.

Timothée REBOURS – D'un point de vue technique, il serait intéressant de rebondir sur le sujet des KMS[12] (*Key Management System*), systèmes qui sont présents chez tous les hébergeurs *Cloud*.

AWS[13], Google Cloud, Azure, Atos, etc. proposent tous des KMS pour gérer les clés. Un KMS, c'est une sorte de coffre-fort dans lequel on peut stocker ses clés, et dans lesquelles les hébergeurs vous assurent qu'elles sont protégées.

Ce type de solution ne répond pas à un problème fondamental, car ces services sont obligatoirement confiés à des tiers de confiance et ce sont eux qui ont la clé de nos données qui leur permettra de tout déchiffrer : on n'a fait que repousser le problème de la détention de la clé vers un autre tiers de confiance. Le problème de fond c'est que le service de KMS détient les clés.

L'arrêt Schrems II, qui a invalidé le *Privacy Shield* en 2020, a été fait sur le fondement que les États-Unis s'appuient sur le *Foreign Intelligence Surveillance Act* (FISA), article 1881 A, sur le *Cloud Computing* et le *Cloud Act*, qui permettent à l'administration étasunienne d'aller faire une perquisition dans les data centers de n'importe quel hébergeur *Cloud* US, indépendamment de l'endroit où est hébergée la donnée. FISA permet donc d'aller perquisitionner des données européennes dans des data centers d'entreprises américaines où que ce soit dans le monde et ce sans le consentement de la justice européenne.

L'arrêt Schrems II a invalidé le *Pricavy Shield*, car il n'est pas conforme au du règlement général sur la protection des données (RGPD).

La CNIL a dit que l'on pourrait tout à fait utiliser le même argument pour invalider l'utilisation d'AWS en France parce que « FISA » a une portée extraterritoriale et leur donne la capacité d'aller utiliser la clé protégée dans un de leurs data centers pour déchiffrer les données qu'ils veulent.

Il faut faire très attention à cette notion de KMS, car c'est un tiers de confiance. Avec Thierry, on a la conviction qu'il faut pousser le contrôle de la clé privée au niveau de l'utilisateur final qui doit chiffrer lui-même ses données ; ce que permettent de faire nos technologies. Faire en sorte que l'utilisateur final soit le seul détenteur de sa clé.

(12) KMS : système de gestion des clés qui comprend la gestion, la génération, l'échange, le stockage, l'utilisation, le déchiffrement cryptographique et le remplacement des clés.
(13) AWS : Amazon Web Services.

On est au cœur du sujet, c'est là que les côtés techniques et juridiques se rejoignent. Si la clé est détenue par l'hébergeur et que ce dernier a accès à l'ensemble des clés de ses clients, dès lors le chiffrement perd toute sa finalité. Ne pas comprendre où se trouve la faiblesse du raisonnement alors que l'hébergeur gère l'ensemble du trousseau de clés font que c'est tout le chiffrement qui se trouve discrédité.

Timothée REBOURS - Dans les KMS fournis par tous les hébergeurs *Cloud*, il y a une subtilité, c'est qu'ils ne peuvent pas lire la clé. Il faut cependant comprendre qu'une réglementation qui interdirait aux hébergeurs de lire les clés stockées dans un KMS ne répondra pas au problème, car s'ils ne peuvent pas lire la clé, ils peuvent utiliser (une carte bleue fonctionne sur le même principe).

Comment s'en sortir ? Par exemple, dans la recommandation de l'European Data Protection Board[14] suite à Schrems II, on indique qu'il faut utiliser des moyens particuliers pour que l'hébergeur vers lequel on fait un transfert de données n'ait pas la capacité de déchiffrer les données en faisant en sorte que la clé ne soit pas mise en tiers de confiance chez un hébergeur soumis à une réglementation intrusive. Si vous prenez un KMS qui est chez Atos, il sera soumis à la justice française. Alors, si un juge français dit qu'il veut perquisitionner la clé, il peut.

On peut prendre un KMS chez Atos, l'utiliser pour chiffrer des données, et le data center qui sera chez AWS pourra déchiffrer les données. Il y a un point très critique dans ce que je viens de dire : si c'est AWS qui peut faire la requête à l'HSM[15] Atos pour déchiffrer les données, cela veut dire que le serveur sur AWS a les données en clair à un moment. En effet, le serveur qui dispose de la donnée chiffrée en mémoire va renvoyer cette donnée au service de KMS qui est sur un autre hébergeur ; par exemple, Atos fera l'opération de déchiffrement et renverra la donnée en clair sur le serveur d'AWS. AWS connaîtra au cours de l'exécution la donnée en clair, ce qui laisse la porte ouverte à un scénario malveillant.

La seule façon de véritablement régler le problème, c'est de faire le chiffrement/déchiffrement non pas côté serveur, mais sur le terminal du client. C'est ce que l'on appelle du chiffrement de bout en bout. Et lorsque c'est le terminal du client, de l'utilisateur final, qui fait les opérations de chiffrement, il envoie la donnée déjà chiffrée à un hébergeur considéré comme malveillant qui n'a pas la clé. À ce moment, la sécurité des données est garantie.

Il faut faire très attention à cette histoire de KMS : sous quelle réglementation est le KMS (américaine/européenne) et où transite la donnée en clair ? Si elle arrive sur un data center américain, ne serait-ce qu'au cours de l'exécution, la finalité de protection des données européenne n'est pas atteinte. Ce sont des concepts extrêmement complexes, ténus et susceptibles de manipulation de langage. Le diable est dans les détails.

Si on reprend cet exemple, et que la donnée en clair n'est pas stockée chez Atos mais y transite seulement ?

Timothée REBOURS – il y a deux façons d'être malveillant.

Prenons AWS qui va stocker des données chiffrées avec une clé qu'il n'a pas et qui est chez Atos. Comment AWS peut-il être malveillant dans un tel scénario ?

1. Attaque passive : puisque le serveur hébergé sur AWS va déchiffrer la donnée par la clé qui est chez Atos, il va récupérer la donnée en clair à un moment pour pouvoir travailler dessus, et donc le serveur d'AWS a en mémoire, à un instant précis, les données en clair. Pour espionner, le fournisseur de *cloud* peut lire la mémoire jusqu'à ce que les données en clair apparaissent ;

2. Attaque active : qui peut être menée à la fois par le développeur, qui code le serveur sur AWS ou par un attaquant qui arrive à modifier le code du serveur. L'attaquant peut prendre la donnée chiffrée sur AWS, la faire déchiffrer via le KMS de chez Athos puis va lire le résultat, qui est la donnée en clair.

Est-ce que FISA peut donner l'injonction à AWS de faire une attaque active ?

Timothée REBOURS – il y a un flou juridique, il faut examiner précisément comment sont rédigés et appliqués FISA, le *Cloud Act*[16]. On peut penser que la rédaction est suffisamment floue pour qu'une attaque active soit possible.

(14) European Data Protection Board : comité européen de la protection des données.
(15) HSM (Hardware Security Module) : matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clefs cryptographiques.
(16) Cloud Act : ensemble de textes de loi permettant notamment aux États-Unis d'exploiter librement des données personnelles d'individus étrangers. Cette utilisation s'oppose donc directement au RGPD.

AVEC L'ARRIVÉE DE LA 5G, TOUT VA COMMUNIQUER AVEC TOUT. ON N'EST PLUS DANS UNE LOGIQUE PÉRIMÉTRIQUE DE TYPE CHÂTEAU FORT OÙ LA SÉCURITÉ PASSERAIT PAR UNE SIMPLE PROTECTION DU RÉSEAU, DES PARE-FEU, DES SONDES QUI PERMETTENT DE DÉTECTER DES FLUX, ETC. LES MILLIARDS D'OBJETS CONNECTÉS QUI VONT ARRIVER, CE SONT AUTANT DE POINTS D'ATTAQUE POSSIBLES. IL FAUT DONC CHANGER LE PARADIGME DE SÉCURITÉ.

Thierry LEBLOND– Il ne faut pas se contenter d'une analyse qui constaterait que juridiquement parlant ils n'auraient pas le droit de faire une intrusion dans des données chiffrées par des clés européennes ; il faut rendre cela techniquement impossible.

Parler de chiffrement de bout en bout, cela ne veut rien dire, car comme on l'a dit tout dépend de qui a la clé.

Ce qu'on qualifie généralement de chiffrement de bout en bout est une configuration où c'est le serveur central qui détient la clé[17] (le plus mauvais cas de figure), donc où le prestataire dispose techniquement des capacités d'accéder aux données.

Il existe également un principe appelé « Bring Your Own Key » (BYOK) : par exemple, Microsoft propose une offre Azure en partenariat avec Thalès. BYOK, cela veut dire qu'on génère ses clés et qu'elles sont confiées à ces fameux HSM (coffres-forts des clés), mais le problème c'est que ces coffres-forts sont forcément opérés par quelqu'un. Dans le cas de Microsoft, c'est Thalès qui opère les HSM. On met donc le doigt sur un élément très important évoqué plus haut. La sécurité c'est toujours faire confiance à un tiers.

L'approche qui nous semble la plus forte est celle qui consiste à dire que cette clé, il ne faut la confier à personne. La bonne façon de le faire c'est de repousser le niveau de sécurité au niveau le plus fin possible, le plus loin possible de l'opérateur de *Cloud*, c'est-à-dire au niveau du terminal. Il devient infiniment plus compliqué d'attaquer des milliers de terminaux sur lesquels la donnée est micro-segmentée plutôt que de pénétrer un serveur qui dispose des droits pour accéder à l'ensemble du système d'information.

Pourtant, même là ce n'est pas encore gagné, car il est encore possible d'attaquer les terminaux à travers des fameuses failles « zero day » (des failles que les fabricants des systèmes d'exploitation ou même des *hardwares* peuvent laisser, volontairement ou pas).

Dans l'idéal, même en repoussant le chiffrement des données au niveau des terminaux informatiques, il faut ajouter une fonction de maîtrise du terminal soit par un EDR[18], soit, mieux, par un système d'exploitation souverain, mais cela coûte de plus en plus cher à chaque fois.

Un antivirus traditionnel parce qu'il analyse des signatures de code malveillant ne suffit plus : l'heuristique de l'EDR analyse en temps réel les comportements anormaux par une sorte d'intelligence artificielle.

Le terminal, à partir du moment où il a un accès à Internet, n'est-il pas un point de faiblesse ?

Thierry LEBLOND – Le meilleur système protégé, c'est le carnet de prise de notes du boucher. Mais ce temps est révolu ; pour simplifier, il existe trois technologies d'environnement extérieur qui s'imposent à nous, quoi que l'on fasse :

1. Le *Cloud* ;

2. Le Réseau notamment la 5G ;

3. La Mobilité.

Ces trois technologies caractérisent la modernité de notre monde de données. Si l'on n'a plus de terminal, comment peut-on échanger nos données à un niveau international ? Le terminal numérique, c'est un moindre mal, un passage obligé. Donc la question devient : comment fait-on pour éviter de faciliter la tâche aux organisations qui font de l'espionnage institutionnalisé des données souveraines ?

Avec l'arrivée de la 5G, tout va communiquer avec tout. On n'est plus dans une logique périmétrique de type château fort où la sécurité passerait par une simple protection du réseau, des pare-feu, des sondes qui permettent de

(17) Comprendre pour « serveur central » : un info-géreur, un fournisseur de Cloud, un tiers de confiance opérant le service (Google, Amazon, etc.).
(18) EDR (Endpoint Detection and Response) : technologie émergente de détection des menaces sur les EndPoints (ordinateurs, serveurs).

détecter des flux, etc. Les milliards d'objets connectés qui vont arriver, ce sont autant de points d'attaque possibles. Il faut donc changer le paradigme de sécurité. Si on reste sur un paradigme de sécurité de type protection réseau, on ne s'en sort pas.

Thierry LEBLOND – En parlant de « protection réseau », il ne suffit même plus de déconnecter ses ordinateurs d'Internet. Les centrifugeuses d'uranium iraniennes étaient déconnectées d'Internet et pourtant elles ont été attaquées par le virus Stuxnet.

Donc même en étant déconnecté d'Internet, on arrive quand même à faire une cyberattaque ?

Thierry LEBLOND – Connecté ou pas, il faut parler maintenant d'une notion fondamentale : celle de *zero trust*[19]. C'est une approche de plus en plus pertinente, même si le concept n'est pas nouveau.

Le Zero Trust consiste à ne faire confiance qu'à son terminal et à rien d'autre. Le réseau, le *Cloud*, l'infogéreur et l'administrateur ne sont plus considérés comme des acteurs de confiance.

L'administrateur, c'est quand même un point de faiblesse, car il y a certes des logiciels qui permettent de gérer ce que l'on appelle les « comptes à privilège », mais il est quand même dans une position très intéressante pour l'évasion de la donnée, on l'a vu avec le cas Snowden[20] par exemple.

Timothée REBOURS – On pourrait convertir la notion de « zero trust », qui est une notion très informatique, très « sécurité », en une notion plus juridique qui est le principe du moindre privilège[21]. C'est-à-dire que si quelqu'un n'a pas besoin de lire une donnée, il ne faut pas lui donner la capacité de le faire.

Thierry LEBLOND – le moindre privilège, je l'attribue plutôt à la notion de « sécurité de l'authentification », mais peut-être que l'on peut l'étendre à quelque chose de plus large quand on parle de *zero trust* : au-delà du « moindre privilège ». La question de la distribution de la confiance, par exemple est un point qui me semble très important. Il faut bien penser que la distribution de la confiance s'est souvent faite sous le mode pyramidal, hiérarchique des armées : on part du chef en haut qui va donner l'accès aux subalternes et ainsi de suite.

Mais on peut se dire qu'il y a une autre manière de regarder le problème, avec la technique du « réseau de résistance ». Cette fois-ci, on va considérer que la confiance ne part plus du haut, mais vient du bas. C'est un concept qui est souvent mis en avant par les combattants opérationnels qui risquent leur vie : une fois les objectifs désignés, ce sont eux qui décident des modes d'action et pas l'état-major.

En matière de sécurité informatique, celui qui est en bout de chaîne a un avantage par rapport à tout le monde, c'est qu'il n'a pas besoin d'un tiers pour certifier son identité, il sait qui il est. Il a un autre avantage, c'est qu'il est supposé très bien connaître les gens avec lesquels il veut échanger en confiance.

En articulant le paradigme de la distribution de la confiance sur l'extrémité de la chaîne, il y a un avantage clair.

La notion de micro-segmentation[22] est implicite à celle du *zero trust*. C'est un moindre privilège mais qui va au-delà du simple droit d'accès, de telle sorte que si un segment de données tombe, il ne compromet pas l'ensemble du système d'information. L'ennemi en sécurité des données, c'est la centralisation de la donnée.

Nous avons organisé en 2021 un webinaire intitulé « Santé et *zero trust* » où nous expliquions que mettre des données de santé, personnelles et sensibles, sur un serveur central, c'était de la pure folie en l'absence de technique de « chiffrement homomorphe[23] ».

Enfin, une dernière notion essentielle est celle de WORM (*Write Once Read Many*). Si malgré toutes les précautions précédentes, un terminal est attaqué par un rançongiciel,

(19) Le Zero Trust (ou zéro confiance) est un modèle de sécurité qui repose sur le principe qu'aucun acteur n'est digne de confiance. Voir notamment la fiche éditée par l'ANSSI : https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/

(20) Edward Snowden : informaticien américain, qui a rendu publiques (entre autres) des informations classées top secret de la NSA.

(21) Le principe de moindre privilège est un principe qui stipule qu'une tâche ne doit bénéficier que de privilèges strictement nécessaires à l'exécution du code menant à bien ses fonctionnalités.

(22) La micro-segmentation est une technique de sécurité du réseau qui permet aux architectes de sécurité de subdiviser le datacenter en sections de sécurités logiques distinctes jusqu'au niveau des charges de travail individuelles, puis de définir des contrôles de sécurité et de fournir des services pour chaque segment.

(23) Chiffrement homomorphe : techniques de calcul qui permettent de ne manipuler que des données chiffrées, c'est-à-dire que le serveur n'a accès à aucune information en clair.

une façon de couper l'arbre sous le pied, c'est de faire en sorte que la donnée soit immortelle, que sa modification n'entraîne qu'une mise en indice sans perdre l'historique de la donnée complète. Voilà comment je poserai en termes synthétiques la question de la sécurisation des données sensibles sur Internet sur les dix prochaines années.

Timothée REBOURS – Il a un point que tu as soulevé Thierry, qui me semble intéressant à souligner, c'est le chiffrement homomorphe.

Quand je disais que c'est intéressant d'empêcher AWS (ou tout autre serveur *Cloud*) de lire des données en faisant un chiffrement qui n'est pas effectué par ce serveur, il y a des cas où on veut exécuter des actions sur ce serveur, par exemple faire un algorithme de *machine Learning*[24], exécuter des opérations et, dans ce cas, on ne peut pas faire de chiffrement de bout en bout.

Ce problème se pose quand il existe une partie des données sur lesquelles on veut atteindre ce niveau de sécurité particulièrement robuste (impliquant du chiffrement) et une autre partie pour laquelle on a besoin de déléguer la capacité de calcul à un serveur tiers pour effectuer les opérations. C'est un problème que le chiffrement, hormis le chiffrement homomorphe, ne permet pas de régler. Aujourd'hui, le chiffrement homomorphe opérationnel est encore en devenir et il y a assez peu d'utilisation réelle.

Et encore une fois, la souveraineté du serveur est importante.

Le chiffrement est peut-être un moyen pour faire du transfert de données transfrontalier dans certaines circonstances, mais il existe des cas où il va falloir trouver un entre-deux.

Selon vous, les autorités de contrôle ont-elles conscience de cette limite ?

Timothée REBOURS - les autorités ont bien conscience de cette limite, c'est pour cela qu'AWS n'est pas interdit aujourd'hui en France. Elles ont conscience qu'à travers Schrems II, FISA, etc., les États-Unis ont la capacité de lire les données sur des serveurs AWS, Google Cloud et Azure, hébergés en France, mais la raison pour laquelle ce n'est pas interdit d'un point de vue RGPD sur le territoire européen, c'est que cela bloquerait tous les usages. La question reste donc en suspens pour le moment.

Thierry LEBLOND - pour revenir au chiffrement homomorphe, l'idée de faire travailler un serveur sur des données chiffrées, c'est aujourd'hui un peu tôt compte tenu du fait que le chiffrement homomorphe est extrêmement coûteux en puissance de calcul, typiquement un facteur 10 000 en 2021.

Timothée REBOURS - La difficulté est de limiter au maximum ses droits sans compromettre les fonctionnalités. Mais si on doit se méfier d'un serveur qui est en permanence malveillant et qui lit tout ce qui se passe, il n'y a pas trop de solutions.

Il existe des techniques pour limiter l'exposition d'un serveur qui centraliserait les droits en faisant un octroi temporaire de droit. Ce n'est pas toujours possible, mais l'idée de moindre privilège, c'est de restreindre le plus possible les droits…

Une autre remarque : il y a une autre classe de solutions pour limiter le risque, c'est l'anonymisation profonde[25]. Il ne faut pas confondre l'anonymisation et la pseudonymisation qui, elle, est réversible.

Par exemple, prenons les habitants de Paris : le nom, le prénom, la date de naissance et la taille d'une personne. La pseudonymisation va consister à couper le jeu de données en deux échantillons, garder la taille sur une colonne dans un fichier, y mettre un identifiant unique aléatoire à chaque ligne et dans une autre base de données, mettre les noms, prénoms, dates de naissance associés au même pseudonyme.

Quelqu'un qui n'a accès qu'à la table « pseudonyme – taille » n'a que ces deux informations, mais quelqu'un qui a les deux moitiés de la base de données est capable de revenir à la base de données initiale. Il a des techniques de chiffrement qui peuvent compléter la pseudonymisation pour faire en sorte que cette table ne soit accessible que par des personnes habilitées. La pseudonymisation n'est pas une alternative au consentement, cela reste de la donnée personnelle ! La donnée personnelle disparaît à partir du moment où on a effectué une anonymisation profonde.

(24) Les algorithmes de Machine Learning apprennent de manière autonome à effectuer une tâche ou à réaliser des prédictions à partir de données et améliorent leurs performances au fil du temps.

(25) Anonymisation profonde : procédé qui assure une protection totale des données personnelles et le respect intégral des libertés publiques. Par une anonymisation immédiate et complète, il rend impossible, même par corrélation, toute ré-identification des utilisateurs et toute reconstitution de parcours individuel ou de points de rencontre spécifiques

Quelles sont les motivations principales de vos clients pour adopter le chiffrement ?

Thierry LEBLOND - nous avons compris qu'il fallait beaucoup d'évangélisation pour arriver à faire prendre conscience du risque sur les données de l'entreprise. C'est pourquoi, aujourd'hui, on inverse l'approche. Cela ne sert à rien d'aller vers des gens qui n'ont pas compris le risque auquel ils sont confrontés. Il vaut mieux travailler avec des gens qui ont bien compris le sujet. Les grands comptes parce qu'ils ont des équipes dédiées au sujet ont le bon niveau de compétence et de connaissance pour bien poser le problème en termes de cas d'usage.

Prenez un grand compte qui travaille sur un environnement périmétrique sécurisé, éventuellement avec des extensions via des VPN[26] et qui doit sous-traiter le plan d'une installation sensible à un sous-traitant. Comment fait-il aujourd'hui pour partager cette donnée sensible directement sur Internet avec des gens qui ne sont pas dans son périmètre de confiance ?

On peut aussi prendre le cas de la crise cyber : vous avez un problème majeur qui arrive niveau cyber et vous devez vous méfier de votre système d'information. Comment faites-vous pour gérer une crise cyber avec des techniques de sécurité potentiellement partout ? Et bien il faut être en mesure de construire directement sur Internet une infrastructure de confiance.

Si quelqu'un travaille sur un serveur web central très ergonomique, mais si je ne veux pas qu'il puisse échanger l'information sensible à travers ce serveur central, nous allons devoir imaginer une manière d'hybrider ce serveur avec nos technologies *zero trust* PARSEC pour qu'il puisse accéder à ses données sensibles à partir d'interfaces intuitives, tout en mettant en œuvre des techniques de chiffrement complexes. Parce que si vous faites de la sécurité en compliquant la vie des gens, les gens vont la contourner. Ce n'est pas simple de faire de la sécurité simplement !

Timothée REBOURS – Je partage ton dernier constat Thierry. Mes clients ont différentes motivations :

1. Des motivations réglementaires. Notre réglementation nous oblige à avoir des techniques de chiffrement. Plusieurs entreprises de télémédecine anticipent soit un engouement réglementaire, soit une mauvaise presse du fait qu'ils stockent des données médicales dans AWS. Ils doivent donc utiliser une surcouche de chiffrement fournie par SEALD qui assure qu'AWS, même malveillant, ne pourra pas y arriver. Dans ce cas d'usage précis, on utilise non pas une technique de chiffrement de bout en bout, mais une technique de secret réparti, ou la moitié du secret est stockée chez AWS, et l'autre moitié chez nous, mais la reconstitution n'est faisable que sur le terminal du client et sur authentification du client par nos soins. Même si AWS devient malveillant de manière active, il ne peut pas récupérer la donnée. En revanche, si la justice française nous perquisitionne ainsi que le client, elle aura accès aux données de l'utilisateur ;

2. Des usages plus industriels. Par exemple, travailler avec une entreprise qui fait de l'aérospatial et qui fonctionne sur un réseau déconnecté d'Internet, et aimerait migrer vers le *Cloud*, tout en maîtrisant le chiffrement sur une infrastructure de fusion restreinte. L'idée c'est de faire le chiffrement avec notre technologie depuis les terminaux clients avec la partie serveur qui est sur leur réseau ,mais que le serveur sur lequel on fait le chiffrement, lui soit dans le Cloud. Un peu particulier, mais c'est une façon pour eux d'essayer d'encourager le télétravail ■

Entretien réalisé par Jean-Christophe Le TOQUIN
et Quentin ROLAND

(26) VPN (Virtual Private Network) : le réseau privé virtuel est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.