5 questions pour comprendre le déchiffrement SSL

D'un côté les grands fournisseurs de services Web ou d'outils de connexion, qui soit pour se refaire une virginité après le scandale Prism, soit par réelle conviction, renforcent l'usage du chiffrement. Qu'on songe par exemple à l'annonce récente de Google affirmant sa volonté de privilégier le référencement des sites HTTPS. De l'autre, les responsables de la sécurité informatique des grandes entreprises que cette montée en puissance du cryptage peut déranger, car s'il est censé garantir la confidentialité des échanges des internautes, il **rend aussi aveugle les équipements de sécurité**. Et, au milieu, le déchiffrement SSL (ou plutôt TLS, le successeur du vieillissant SSL). Autrement dit, la mise en œuvre par l'entreprise d'une technique lui permettant d'**inspecter les flux que l'utilisateur pensait chiffrés** entre le serveur et son poste de travail.

Le sujet n'a rien de réellement neuf, à part qu'il prend aujourd'hui une autre dimension du fait de la généralisation du chiffrement sur les services Web. Au point que **l'Anssi**, l'Agence nationale de la sécurité des systèmes d'information, vient de publier une note technique portant sur ses recommandations en matière d'analyse de flux HTTPS. Ce document résume les objectifs assez légitimes de cette pratique tout en évoquant sa part d'ombre. « U*n contenu chiffré peut être source de comportement délictueux donnant lieu à la mise en jeu de la responsabilité de l'entité. Le déchiffrement, qui rend visible un contenu destiné à être confidentiel, permet de se prémunir contre ce risque mais parfois au prix des risques censés être couverts par le chiffrement* », écrit l'Anssi.

1) Comment ça marche ?

En fait, le déchiffrement SSL s'appuie sur une technique assez simple et bien connue. Comme l'écrit l'Anssi, la manœuvre consiste à duper le client (donc le navigateur de l'utilisateur) « *en interceptant la connexion TLS qu'il initie en direction du serveur Web cible* ». Une mission la plupart du temps confié à un proxy, serveur mandataire servant de point de passage unifié dans l'architecture. Ce proxy joue alors le rôle du serveur TLS pour les utilisateurs finaux. Il doit donc leur présenter un certificat valide lorsqu'ils initient une connexion HTTPS. La conséquence ? Ce dispositif **nécessite toujours une action sur le poste du salarié**, pour installer le certificat du proxy de l'entreprise. Bien entendu, ce dernier peut être préinstallé sur le poste fourni à l'employé, et donc ignoré de ce dernier. En somme, le déchiffrement SSL n'est ni plus ni moins que ce que les spécialistes de la sécurité appellent **une attaque de l'homme du milieu** (Man-in-the-middle), où un équipement vient s'interposer dans une communication afin d'intercepter les flux ou truquer un message.

Si la solution n'a donc rien de révolutionnaire, elle se heurte quand même à de nombreuses contraintes de mises en œuvre. « *Le déchiffrement SSL nécessite de configurer une autorité racine (ou une sous autorité) au niveau de ce proxy et de déployer les certificats correspondants sur les postes des utilisateurs* », souligne **Ary Kokos**, consultant senior chez Solucom. Pas forcément à la portée de toutes les organisations et très dangereux en cas de mauvaise manipulation. Comme l'a appris à ses dépens la Direction Générale du Trésor, en décembre dernier. « *Il s'agissait d'un déploiement interne pour faire du DLP (prévention de fuite de données, NDLR) et du filtrage sur les flux GMail, qui a été*

repéré et étiqueté par Chrome », rappelle **Hervé Schauer**, membre du conseil d'administration du Clusif (Club de la sécurité de l'information français) et dirigeant du cabinet de conseil HSC.

Le procédé pose aussi la question des postes amenés dans l'entreprise par les utilisateurs eux-mêmes. Une tendance de plus en plus prégnante avec les terminaux mobiles. « *Pour ces postes non maîtrisés par la DSI, la question est épineuse*, confirme Ary Kokos. *Signalons qu'une solution exploitant un HSM (appliance de chiffrement, NDLR), permettant de générer des certificats d'une sous-autorité d'une autorité publique, permet de les couvrir en déchiffrement. Mais cette solution s'avère très dangereuse juridiquement pour une entreprise qui se trouve alors en mesure d'intercepter des courriers ou des données confidentielles n'émanant pas de ses employés* ». La société Trustwave, qui proposait une offre de ce type, a d'ailleurs arrêté ce service.

Autre difficulté concrète : la définition du périmètre de déchiffrement. Pour des raisons de confidentialité des communications des salariés, **certains flux vont en effet échapper au déchiffrement**, et être placés sur ce qu'on appelle une **liste blanche** (regroupant les sites à priori de confiance). « *En pratique, cela s'avère très complexe, notamment pour la banque en ligne – car les financiers des entreprises s'en servent également – ou pour les services de messagerie dans le Cloud comme Gmail ou Yahoo mail*, note Ary Kokos. *Car ces services, relevant à priori de la sphère personnelle, peuvent aussi être utilisés par des assaillants pour exfiltrer discrètement des données* ». Selon le consultant, les assaillants utilisent d'ailleurs de plus en plus des flux chiffrés soit pour exfiltrer des données, via des messageries chiffrées par défaut, soit pour contrôler des malwares à distance.

Or, du fait du renforcement des mesures de sécurité des fournisseurs de service ou des éditeurs de logiciels, cette liste blanche tend à s'allonger. « *Elle sert également à exclure certains flux – les mises à jour d'antivirus, Windows Update, l'application Dropbox… – sur des technologies qui emploient des certificats clients qui font de l'authentification mutuelle avec le serveur*, explique **Jérémy D'Hoinne**, directeur de recherche chez Gartner. *Dans ces cas, en effet, la technique de l'homme du milieu ne fonctionne plus.* »

2) La pratique est-elle courante ?

« *Le sujet est très ancien pour moi*, dit Hervé Schauer, membre du conseil d'administration du Clusif. *Dans les entreprises, ce n'est pas une nouveauté, l'augmentation de site web utilisant SSL aboutit simplement à placer plus de sites en liste blanche.* » De facto, de nombreuses grandes entreprises ont déjà recours au déchiffrement SSL. Tant sur le trafic Web que sur les flux de messagerie SMTPS.

L'avocat **François Coupez**, du cabinet Atipic, suit le sujet depuis 2007 et confirme qu'il s'agit là d'une pratique courante dans les grandes entreprises. « *Mais elle n'a pas forcément été identifiée comme soulevant des problématiques juridiques, raison pour laquelle elle n'est pas particulièrement ni considérée ni encadrée. Les saisines sur le sujet ne sont pas si fréquentes.* »

Pour le Gartner, il faut distinguer le déchiffrement du trafic entrant (celui dirigé vers les sites Web internes de l'entreprise) et celui du trafic Internet des utilisateurs internes. Fin 2013, plus 90 % des entreprises déchiffraient le trafic Web entrant sur leurs propres applications Web. « *Tout simplement afin de protéger leurs serveurs* », dit Jérémy D'Hoinne, directeur de recherche au sein du cabinet d'études. Sur la navigation des utilisateurs, les niveaux de maturité seraient en revanche bien plus divers. Le directeur de recherche estime que moins de 10 % des grandes entreprises déchiffrent les

flux SSL au niveau des pare-feu. Moins encore en France. « *Plusieurs raisons à cela. Chez certaines, le sujet est mal compris et peu considéré. D'autres rencontrent des difficultés en matière de performances ou de législation.* » Par exemple, quand les entreprises sont déployées sur plusieurs pays, il faut se conformer à autant de législations locales.

Certaines études ont montré qu'ajouter le déchiffrement au niveau du pare-feu dégrade ses performances d'un facteur allant jusqu'à 90 %. « *Or, en passant au pare-feu applicatif, on a déjà grevé les coûts pour protéger un débit donné. Ajouter le déchiffrement ne ferait qu'alourdir la facture* », explique Jérémy D'Hoinne, ancien de NetAsq. Sur les proxy Web ou e-mail, les usages sont bien plus répandus, confirmant ainsi la domination de ce modèle d'architecture. Gartner estime que **40 à 50 % des grandes entreprises y pratiquent du déchiffrement SSL**, « *souvent partiellement* ». Les flux bancaires, les sites relatifs à la santé mais aussi les webmail rejoindront ainsi les listes blanches.

Si les grandes entreprises, dotées de spécialistes de la cyber-sécurité, sont en partie déjà équipées, il n'en va pas de même des entreprises plus petites. « *Dans les PME, la mise en œuvre du déchiffrement est évidemment plus rare, du fait du coût de ces solutions mais aussi du niveau de maturité nécessaire pour gérer une IGC interne (infrastructure de gestion de clefs, NDLR), déposer le certificat racine sur les postes utilisateur et maîtriser les questions relatives au cadre juridique* », note Ary Kokos.

3) Quels sont les risques du déchiffrement ?

Pour faire simple, ils sont de deux ordres : **techniques et juridiques**. Dans sa note, l'Anssi insiste sur les premiers. En toute logique car il ne s'agit pas là d'une opération anodine, puisqu'elle « *entraîne la rupture d'un canal sécurisé et expose les données en clair au niveau de l'équipement en charge de l'opération* », écrit l'Agence. Conséquence : le niveau de sécurité du tunnel TLS établi sur Internet avec le serveur cible ne dépend plus du navigateur web du client. « *La sécurisation des tunnels TLS établis avec le monde extérieur repose uniquement sur les possibilités offertes par le proxy en tant que client, celui-ci étant potentiellement plus laxiste au niveau TLS que les navigateurs web les plus récents* », écrit l'Agence. Une façon de souligner combien, dans cette architecture, **le proxy devient un équipement très critique**. Dont le fonctionnement devra être vérifié (par exemple en cas de présentation d'un certificat non valide) et l'administration encadrée. Pour Hervé Schauer (Clusif), la première des règles est de surtout ne pas conserver le contenu des pages consultées par les utilisateurs.

Dans ses recommandations, l'Anssi précise quelques autres bonnes pratiques essentielles, comme celle consistant à utiliser uniquement une autorité de confiance (AC) non publique (autrement dit limitée au système d'information) et à éviter les AC intégrée nativement aux proxy, génératrices de risques selon l'Agence (autorité identique sur différents équipements, utilisation de gabarits non appropriés…).

Ary Kokos (Solucom) confirme que la mise en place du déchiffrement au niveau du proxy fait naître de nouveaux risques : « *D'abord, cela signifie gérer une autorité générant des certificats. Si un attaquant venait à s'emparer de la clef, il pourrait intercepter toutes les communications de l'entreprise. Sur ce plan, un HSM fournit une réponse en protégeant la clef. Ensuite, le proxy devient lui-même un point sensible, toutes les communications y transitant par définition en clair. Enfin, il faut se montrer vigilant sur la*

configuration : si le proxy ne bloque pas les connexions non conformes, l'utilisateur final sera incapable de les détecter. » Un risque ici tant technique que juridique. Car si un employé venait à se faire dérober des informations personnelles du fait de leur déchiffrement sur le proxy de son entreprise, il pourrait incriminer la responsabilité de son employeur.

Si la pratique n'est **pas encadrée par un texte spécifique**, elle doit se conformer à un ensemble de textes, note l'avocat François Coupez : article 226-15 du Code pénal, article L. 1222-4 du Code du travail, loi Informatique et Libertés du 6 janvier 1978, principe de contrôle de l'activité du salarié, respect de l'obligation de sécurité des données à caractère personnel de l'entreprise, etc. « *Le principe doit être le même que celui mis en place pour le contrôle de l'utilisation des outils numériques par le salarié : d'abord un contrôle général, statistique et anonyme et puis (si la charte informatique le prévoit), en cas d'incident de sécurité ou d'utilisation non conforme, un contrôle personnalisé – dans un cadre strict – de ce flux* », explique l'associé du cabinet Atipic.

Car, comme le signale l'Anssi, le déchiffrement peut porter atteinte au secret des correspondances privées, à la protection des données à caractère personnel, à la vie privée des utilisateurs dans et au-dehors de leur travail ou encore à la sensibilité des informations (secret professionnel, informations classifiées…). Sans oublier les risques liés à une éventuelle sous-traitance, dont les pratiques doivent être encadrées par contrat.

Le traitement relatif au déchiffrement doit, en principe, faire l'objet d'**une déclaration à la CNIL**. Oui, mais comment ? « *Le flou en France réside dans le fait de savoir si la déclaration à la CNIL sur le déchiffrement doit être différente de celle concernant les logs et le filtrage d'URL ou s'il peut s'agir d'une même et unique déclaration* », souligne Jérémy D'Hoinne. Pour le directeur de recherche du Gartner, cette absence de démarche bien balisée pousse parfois les équipes de sécurité à limiter leurs opérations de déchiffrement aux seules catégories à risque, voire à bloquer le projet. « C*e qui limite l'efficacité du dispositif. En Europe, la plupart des entreprises décident ainsi de ne pas déchiffrer le webmail des employés pour respecter la vie privée* ». D'ailleurs, étonnamment, la CNIL a refusé de répondre à nos questions sur le sujet, arguant du fait qu'elle était en train de travailler sur ce dossier.

Pour Hervé Schauer, pourtant, le sujet est bien balisé en matière de formalités préalables : « *si les données sont collectées uniquement dans le but (la finalité) d'assurer la sécurité et le bon fonctionnement du SI, alors cela entre dans le cadre de la norme simplifiée n°46 (relative à la gestion du personnel, NDLR). Donc si l'entreprise a déjà utilisé cette norme pour déclarer son traitement RH, pas besoin de modifier sa déclaration. La norme simplifiée apparaît suffisamment large pour englober cette collecte.* » Par contre si la finalité du traitement dépasse la sécurité du SI pour englober un volet lié à la surveillance individuelle de l'activité des salariés, une nouvelle déclaration s'impose ou, si l'organisation comporte un CIL (Correspondant Informatique et Libertés), ce dernier devra ajouter une inscription à son registre recensant les traitements de données à caractère personnel.

4) Comment en informer les salariés ?

L'Anssi rappelle que le consentement individuel des utilisateurs est obligatoire, via la signature de la charte d'utilisation des moyens de communication électronique (ou tout autre nom que ce document peut revêtir), annexée au règlement intérieur. « *Elle doit être modifiée si les contrôles qu'elle prévoit ne permettent pas d'englober ce déchiffrement* », dit François Coupez. Qui précise : « *Il convient*

surtout d'éviter la rédaction de paragraphes dans la charte, donc dans le règlement intérieur, qui rendrait impossible tout contrôle, alors même qu'il serait fait en pratique pour les meilleures raisons du monde. La jurisprudence est très claire et rigoureuse en l'occurrence : la chambre sociale de la Cour de cassation a ainsi rappelé le 26 juin 2012 que face à une charte rédigée unilatéralement par l'employeur, celui-ci ne peut s'affranchir de limitations qu'il s'est imposé à lui-même, notamment concernant le cadre ou les conditions de contrôle. »

Voilà pour la règle. Reste à évaluer comment ces modifications, pouvant être perçues comme des mesures de flicage par les salariés, seront accueillies par les représentants du personnel. Jérémy D'Hoinne conseille aux entreprises d'**établir la discussion sur ce sujet avec les salariés en amont**, pour évaluer les risques : « *les organisations qui l'ont fait expliquent généralement qu'un accord sur les catégories placées en liste blanche suffit à avoir une discussion sereine* ». Une vision que confirme François Coupez. Qui explique : « *il faut garder en tête et savoir expliquer que ces outils ne sont pas mis en place pour décrypter les flux protégés entre le collaborateur et un tiers en tant que tels, mais pour appliquer les mêmes contrôles (antivirus, filtrage de flux, DLP, etc.) de sécurité que ceux appliqués au flux transitant en clair ou pour appliquer des contrôles qui sont rendus nécessaire par la loi (Hadopi) sur les flux en clair et sur les flux chiffrés. Rien de plus. En général et sous ces réserves, les représentants des salariés le comprennent.* »
L'avocat souligne également que la politique de sécurité des SI doit prévoir des « *procédures particulières quant à l'accès aux données déchiffrées* », l'employeur ne devant pas – fort logiquement – se mettre en capacité de connaître les mots de passe des espaces de banque en ligne de ses salariés, par exemple. L'Anssi rappelle également que l'organisation devra nommer un administrateur « *expressément autorisé à accéder aux contenus déchiffrés moyennant le respect d'une obligation de confidentialité qui le lie, y compris à l'égard de son employeur* ».

5) Pourquoi le sujet revient-il sur la table aujourd'hui ?

Plusieurs raisons expliquent que le sujet du déchiffrement SSL, qui n'a rien de neuf, revienne aujourd'hui au premier plan. D'abord, les révélations d'Edward Snowden sur les écoutes à grande échelle de la NSA américaine poussent les géants du Net à durcir leur défense. Donc à **généraliser le chiffrement des flux** émanant de leur service pour reconquérir la confiance de leurs utilisateurs. En août dernier, dans nos colonnes, Dominique Loiselet, directeur général de l'éditeur américain de solutions d'inspection de flux Blue Coat pour la France, expliquait que la généralisation du HTTPS était en train de rendre aveugles les équipements de sécurité dans lesquels les entreprises ont investi.

Ensuite, le déchiffrement SSL se heurte aujourd'hui à une difficulté : le **durcissement des défenses des navigateurs** vis-à-vis des interceptions à la volée (Man-in-the-Middle). Sur Google Chrome, la valeur du certificat de certains sites est désormais codée en dur, leur intégrité est donc validée depuis une liste intégrée au navigateur. Un certificat « local », émis par un proxy, sera donc détecté par le navigateur de Google et signalé à ce dernier. Depuis sa version 32, Firefox propose une option identique. « *Dans la plupart des cas, ces difficultés restent contournables, car les entreprises emploient souvent IE ou se tournent vers Firefox, sur lequel la vérification d'intégrité des certificats n'est qu'une option* », tempère toutefois Ary Kokos (Solucom).

Enfin, et c'est un facteur essentiel, si le déchiffrement SSL devient un sujet majeur, c'est tout simplement parce que **les assaillants utilisent de plus en plus les flux chiffrés** pour tenter de s'introduire dans les systèmes d'information des entreprises. Exploitant la faiblesse du taux de déploiement des solutions de déchiffrement et la propension des entreprises à faire grossir les listes blanches pour éviter tout conflit avec les salariés. Le cabinet d'études Gartner y voit d'ailleurs là une tendance majeure pour les années qui viennent : « *on pense que les assaillants vont de plus en plus exploiter les flux cryptés. Fin 2013, moins de 5 % des attaques exploitaient SSL directement. Avec la généralisation du chiffrement, ce taux pourrait monter à plus de 50 % d'ici 4 ans* », dit son directeur de recherche Jérémy D'Hoinne.

Les RSSI se trouvent donc **au centre d'un dilemme**. « *Il y a un conflit d'intérêt entre la volonté de sécuriser les systèmes de l'entreprise en pratiquant des inspections de flux et la volonté de bannir ces inspections pour préserver la confidentialité des échanges*, dit Jérémy D'Hoinne. *Avec les applications mobiles ou les dernières versions de navigateurs, à l'image de Firefox qui vient d'ajouter l'épinglage de certificats, le risque est de voir les listes blanches grossir. Donc de voir les flux intégrés au périmètre de déchiffrement se réduire* ». Le directeur de recherche de Gartner met toutefois en lumière quelques lueurs d'espoir, via l'utilisation de procédés complémentaires. Comme des techniques analytiques liées à du monitoring réseau – détectant par exemple de gros volumes transférés vers un serveur inconnu, une connexion vers un serveur connu pour héberger des botnet ou à un serveur créé dans les dernières 24 heures… – ou l'utilisation des informations échangées lors des phases de négociation des connexions SSL. « *Une façon de contourner en partie les limites du déchiffrement, tout en maintenant du filtrage sur des flux chiffrés* », dit Jérémy D'Hoinne.

Crédit photo : Maksim Kabakou / Shutterstock