Les outils de sécurisation d'applications web dans l'informatique en nuage (cloud)

22 janvier 2024

Anti-DDoS, WAF, load balancers, CDN : ces outils sont devenus indispensables pour sécuriser un service cloud. Comment fonctionnent-ils et quelles problématiques soulèvent-ils vis-à-vis de la protection des données

À retenir

- Différents fournisseurs proposent des outils pour sécuriser les services cloud ou améliorer leur performance (Anti-DDoS, WAF, *load balancers*, CDN).
- **Ces outils collectent des données personnelles.**
- Ces outils peuvent soulever des problématiques au regard de la protection des données : ils peuvent entraîner des transferts de données vers des pays ne garantissant pas un niveau de protection suffisant, ou des risques en matière de sécurité (déchiffrement TLS).

Une protection nécessaire face à la menace de cyberattaques

Le web est incontournable pour tout type de services et d'organismes (e-commerce, divertissements, actualités, communications, interactions avec les services publics, etc.) et ses usagers se sont habitués dans ce contexte à une qualité de service très élevée. Il est donc attendu que les sites et applications web soient :

- **performants** à tout moment ;
- **disponibles** à tout moment ; et
- **protégés** des attaques informatiques.

Cependant, les menaces contre ces sites et applications n'ont jamais été aussi présentes :

- les attaques par déni de service distribuées (« *Distributed Denial of Service* » ou **DDoS**) sont très fréquentes, notamment du fait de la relative simplicité de leur mise en œuvre, et de leur efficacité contre une cible non préparée ;
- les **attaques dirigées contre les applications web**, telles que les « injections SQL » (SQLi) et les injections dites de « *cross-site scripting* » (XSS) profitent de vulnérabilités des sites et applications web et conduisent souvent à la compromission de la confidentialité de données personnelles.

Outils et services pour la sécurité et la performance de services web

Certains fournisseurs proposent une gamme d'outils combinant des services pour améliorer la performance des sites et applications web et des outils pour les sécuriser et garantir leur disponibilité. Ces outils sont répertoriés dans le tableau ci-dessous.

Type d'outils	Outils/Services	Définitions

Outils pour la sécurité	**Anti-DDoS**	**Anti attaques par déni de service distribuées - Anti-distributed denial of service**	Les solutions anti-DDoS ont pour objet de protéger les systèmes d'information contre les attaques du type DDoS. Celles-ci se matérialisent par l'envoi répété et en quantité importante de requêtes, via Internet, à un serveur ou à un équipement réseau, dans le but d'entraver son fonctionnement ou d'empêcher les utilisateurs légitimes d'un service de l'utiliser (saturation de la bande passante, des connexions d'un équipement, etc.). Les attaques DDoS sont menées à partir de nombreuses machines compromises, d'où le terme d'attaque « distribuée », car le nombre d'adresses IP à filtrer devient très important, jusqu'à dépasser les capacités des outils de filtrage. Les solutions anti-DDoS fonctionnent de différentes façons : par **filtrage du trafic en bordure du système d'information** (attaques dont le volume n'excède pas la capacité des liens réseau), via les équipements pare-feux ; par **filtrage du trafic en amont**, par l'intermédiaire des opérateurs de transit ou des fournisseurs d'accès ; par **répartition de charge**, via la distribution du trafic entrant sur plusieurs serveurs, empêchant un seul serveur d'être submergé par un grand volume de requêtes ; par **l'intermédiaire de certains prestataires** qui proposent des solutions anti-DDoS dans le cloud ou en ligne hébergées sur leurs propres infrastructures (par exemple, via des réseaux dédiés de distribution de contenus, ou CDN). Ces solutions agissent alors tel qu'un proxy pour le trafic réseau des clients.

	WAF	**Pare-feu pour application Web - Web application firewall**	Le pare-feu d'application web est une solution de sécurité permettant de protéger les applications web **en analysant les flux web** (HTTP et HTTPS) et en **bloquant les flux suspects et malveillants**, entre les clients et les serveurs de destination qui hébergent les applications web. Le WAF peut se présenter sous forme matérielle, logicielle ou comme un service SaaS (« software as a service »). Le WAF applique un mécanisme de filtrage, à base de règles sur les échanges HTTP(S), permettant de protéger les applications web contre des attaques sophistiquées et ciblées, telles que le « cross-site scripting » (XSS) et l'« injection SQL » (SQLi) qui pourraient entraîner une violation de données. Un WAF peut être considéré comme un « proxy » inverse (serveur mandataire inverse).
			Les réseaux de distribution de contenus sont des réseaux

Ces solutions sont susceptibles de traiter des données personnelles et d'engendrer des risques pour les droits et libertés des personnes.

Données personnelles traitées par ces services

Les données collectées et traitées par ces briques de sécurité dépendent des techniques de protection utilisées (surveillance et classification du trafic réseau selon l'origine géographique des paquets, selon le contenu des paquets, selon le nombre de paquets reçus en un temps donné, etc.).

Néanmoins, de manière générale, les données personnelles potentiellement traitées sont les suivantes (liste non exhaustive) :

- des adresses IP et/ou MAC ;
- des données permettant l'identification de l'origine des attaques (horodatage, géolocalisation, taille des paquets, etc.) et notamment les IOC (indicateurs de compromission) lorsqu'elles se rapportent à une personne identifiable ;
- si les paquets qui transitent sur le réseau ne sont pas chiffrés ou si l'équipement de sécurité est configuré en « rupture de chiffrement » (c'est-à-dire que les données sont déchiffrées sur l'équipement avant d'être rechiffrées pour réémission) : le contenu des requêtes HTTP, l'URL des pages web visitées par la personne concernée, les données personnelles transmises au serveur web, etc.

Pour des besoins d'analyses à postériori, afin de détecter de nouvelles tendances de cybermenaces, les fournisseurs (notamment de WAF et d'anti-DDos) peuvent prélever aléatoirement des échantillons du trafic de données, contenant des captures réseau pouvant contenir des données personnelles.

Le tableau ci-dessous récapitule les données traitées en fonction des outils considérés.

Type d'outils	Outils	Données personnelles traitées
Outils pour la sécurité	**Anti-DDoS**	Des adresses IP et/ou MAC et/ou des cookies ; des captures réseau complètes pour analyse postérieure, qui peuvent comprendre des données personnelles, y compris des données sensibles, contenues dans les paquets échangés ; de manière générale, des données permettant l'identification de l'origine des attaques (horodatage, géolocalisation, etc.).
	WAF	Toutes les requêtes de données et de pages envoyées à un serveur web, incluant le contenu des requêtes HTTP/HTTPS ; échantillons du trafic de données prélevés aléatoirement pour analyse postérieure, qui peuvent contenir des données personnelles.

	CDN	**Données personnelles collectées par le CDN lors de la fourniture du service :** des données personnelles incluses dans les journaux d'administration ; les adresses IP des utilisateurs ainsi que leur géolocalisation ; les pages visitées par la personne concernée (leur URL, un horodatage, le contenu des pages, etc.) ; des données de télémétrie et autres données techniques (information sur le navigateur, le système d'exploitation et le terminal utilisés, les clics, etc.). Ces données sont traitées notamment afin de fournir des indicateurs au client concernant les performances de son site web ou de son application ainsi que pour calculer les frais à facturer au client. **Données personnelles potentiellement traitées par le CDN à la demande du client :** les données mises en cache : à priori, le type et la quantité de données mises en cache sont sous le contrôle du client du fournisseur de CDN ; le contenu des requêtes HTTP de type POST (p. ex. : envoi de données d'un formulaire) et de leurs réponses.
Outils pour la sécurité et la performance		Des données personnelles incluses dans les journaux d'administration ;

Les problématiques RGPD des outils de sécurité

Problématiques liées aux transferts et accès par les autorités de pays tiers

Pour un client recourant à un fournisseur d'informatique en nuage (cloud), les outils de sécurité et de performance doivent être pris en compte dans l'analyse des transferts et accès potentiels. Il est ainsi essentiel d'obtenir du fournisseur de service une description précise des outils et technologies appliqués d'office sur les services souscrits, de lui demander toutes les informations et données personnelles que ces outils manipulent, afin de déterminer les éventuels transferts et accès qu'ils induisent.

Les transferts liés aux outils de sécurité et de performance

À l'instar des services de cloud, les fournisseurs des outils de sécurité précités sont affectés par la question des transferts ou d'accès par les autorités de pays tiers.

Premièrement, les traitements de données, notamment à caractère personnel, qui transitent sur Internet et passent par les CDN, WAF ou outils anti-DDoS offerts par des **fournisseurs non européens**, peuvent engendrer des transferts hors de l'UE.

Deuxièmement, les données traitées par ces outils de sécurité et de performance peuvent, en raison du fonctionnement du réseau internet, **transiter dans des pays ne garantissant pas les principes de protection des données personnelles dans l'UE**. Cette situation est susceptible de se produire même lorsque l'utilisateur et le fournisseur du service recourant au cloud sont tous deux basés en Europe, et même lorsque le fournisseur de cloud propose une « localisation en Europe » des données : en effet, ces outils de sécurité ne sont pas nécessairement fournis selon les mêmes règles de localisation que les prestations de *cloud* achetées par le client (IaaS, PaaS et SaaS). Par exemple, dans le cas des CDN, le besoin de positionner les données sur des serveurs adossés aux grands axes de circulation des données peut conduire à ce qu'elles soient recopiées sur des matériels tiers hors UE, au débouché des câbles transocéaniques (voir ci-dessous).

Il semble donc nécessaire pour chaque client recourant à un fournisseur de cloud de vérifier auprès de ce dernier si d'éventuels transferts peuvent être réalisés par les outils de sécurité intégrés nativement avec les prestations fournies. Sur son site web, la CNIL propose un guide pratique pour vérifier la légalité des transferts de données hors UE. Sur la base de ce guide, les questions qu'un client pourrait poser à son fournisseur pourraient être les suivantes :

Étape 1 : recensement des transferts de données personnelles

- Votre offre comprend-t-elle des outils de sécurité ou d'optimisation des performances réseau (WAF, CDN, Anti-DDoS, LB) qui analysent le trafic ?
- Si oui, où ces outils et équipements sont-ils localisés ?
- Existe-t-il des flux de données vers le fournisseur ?
- Existe-t-il des accès distants accordés au fournisseur ?
- Que prévoit le contrat en matière de transferts de données hors UE (y compris concernant les lieux de support technique) ?

Étape 2 : définition d'un plan d'action en cas de transferts hors UE

- Est-ce que les données personnelles sont transférés vers un pays bénéficiant d'une décision d'adéquation de la Commission européenne ?
- S'il n'existe pas de décision d'adéquation, comment sont encadrés ces transferts et quels outils de transferts sont mis en place pour garantir la protection des données ?
- Des mesures supplémentaires de protection des données sont-elles nécessaires, en fonction du pays visé ?

Les possibilités d'accès par des autorités de pays tiers

En outre, d'autres considérations techniques sont à prendre en compte pour évaluer les possibilités d'accès par des autorités de pays tiers non conformes au RGPD :

- les fournisseurs de ces services de sécurité collectent et stockent des **journaux de traçabilité** sur un territoire hors de l'UE, journaux qui peuvent contenir des données personnelles (notamment l'adresse IP ou la géolocalisation) ;
- les **administrateurs de la solution de sécurité peuvent avoir accès à tous les trafics** et donc toutes les données qui transitent ;

- les briques techniques nécessaires à la délivrance du service traitent également des données personnelles (p. ex. : pour la gestion de la facturation ou l'amélioration du service ou le diagnostic de problèmes).

Ainsi, les organismes qui traitent des données d'une sensibilité particulière et souhaitent se garantir contre ce type d'accès sont amenés à utiliser des briques de sécurité offertes par **un fournisseur européen, immunisé aux lois extracommunautaires**, afin d'exclure de fait tout accès non autorisé aux données par des entités non-européennes, même en cours de transit.

La question des flux de données hors UE et du fonctionnement d'Internet : le cas particulier du CDN

L'étendue mondiale d'Internet et de son fonctionnement impliquent que les données circulent hors de l'Union européenne : c'est le cas notamment quand un échange de courriels a lieu entre une personne située dans en France et un interlocuteur hors de l'UE ou lorsque des données sont mises en cache sur des serveurs situés en dehors de l'UE pour être servies plus rapidement à un internaute.

Si les outils d'anti-DDoS, d'équilibrage de la charge (LB) et les pare-feux applicatifs (WAF) peuvent être placés au sein de l'UE pour éviter des transferts hors UE du fait de leur utilisation, le service de réseau de distribution de contenus (CDN) présente les mêmes limites que le fonctionnement traditionnel d'Internet : un tel réseau est conçu pour offrir au plus près de chaque internaute une copie du service / contenu demandé. Si la copie est mise en cache sur un serveur situé hors UE, il est possible que des données transitent depuis un serveur au sein de l'UE vers un serveur situé hors UE. L'ampleur de la transmission des données hors de l'UE dépendra de divers facteurs, et notamment de la portée des opérations du fournisseur de CDN, des types de contenus diffusés et de l'emplacement des serveurs utilisés par le fournisseur de CDN. Si cette transmission de données est effectuée dans le cadre d'un traitement soumis au RGPD, il peut s'agir d'un transfert de données à caractère personnel, sous réserve que les critères applicables soient remplis, qui doit donc être conforme au chapitre V du règlement.

Il est recommandé en tant que bonne pratique que le client et son fournisseur de CDN s'assurent d'une configuration appropriée limitant la circulation de données hors UE :

- **d'une part, en sélectionnant les données étant placées dans le cache du CDN** : il est recommandé de se limiter à des données dites « statiques » de contenus particulièrement lourds (vidéos, images) ne contenant pas d'informations personnelles, et de ne pas y placer des données personnelles dynamiques (bases de données, fichiers clients, etc.) ;
- **d'autre part, en configurant le CDN de sorte à ne pas faire circuler plus de données que dans le cadre d'un accès simple via Internet au service demandé** (c.-à-d. sans le recours à un CDN). En particulier :
    - si le service web ne vise pas particulièrement d'utilisateurs en dehors de l'Union européenne, il n'est pas pertinent de configurer un CDN en dehors de l'UE ;
    - de même, il est recommandé de configurer le service de CDN de sorte que les différents équipements utilisés soient situés dans des pays considérés comme adéquats.

De nombreux fournisseurs de services lient les outils : il n'est pas toujours possible, dans leurs offres, de traiter différemment le CDN des autres services offerts.

Différentes modalités de déchiffrement TLS

Le protocole TLS (pour « *Transport Layer Security* », c'est-à-dire : « sécurité de la couche transport » du modèle OSI, voir ci-dessus) est un protocole de sécurité que l'on peut mettre en œuvre sur les réseaux non sûrs (tels qu'Internet). Il est notamment utilisé pour sécuriser l'échange des flux de données des services web. Il opère suivant le paradigme client-serveur et réalise les objectifs de sécurité suivants :

- **l'authentification** du serveur (via le processus d'entrée en relation appelé « *handshake* », qui permet l'échange de certificats électroniques) ;
- **la confidentialité** des données échangées (chiffrement du trafic à l'aide d'un algorithme de chiffrement symétrique dont la clé temporaire de session est partagée au moment du « *handshake* ») ;
- **l'intégrité** des données échangées (via des fonctions de hachage et des codes d'authentification de message, ou MAC) ;
- parfois également, l'authentification du client.

Dans la phase de *handshake*, TLS permet au client et au serveur d'effectuer un échange authentifié de clés, afin d'établir un secret partagé à partir duquel la clé de chiffrement symétrique de la session sera dérivée.

TLS est largement utilisé pour fournir des communications sécurisées, en particulier chiffrées, entre les clients et les serveurs. Cependant, le chiffrement TLS, s'il a pour objectif de garantir la confidentialité des échanges, rend **aveugles** les outils de sécurité qui agissent en tant qu'**intermédiaires** entre les clients et les serveurs (voir figure 1 ci-dessous). En effet, nombre de ces intermédiaires opérant au niveau du réseau (outils de surveillance du réseau, d'optimisation de performance, de mise en cache, de prévention des fuites de données, etc.) ont été conçus sur la base du fait que les données en transit étaient en clair et donc facilement accessibles pour être analysées.

Figure 1 - Flux sans déchiffrement TLS : l'intermédiaire n'a pas accès aux données en clair

Les cas où le chiffrement TLS entrave les objectifs de sécurité (c'est-à-dire que l'objectif de sécurité ne peut en principe pas être réalisé sur des flux chiffrés) sont :

- l'inspection des flux web (WAF et anti-DDoS applicatif) ;
- la répartition de la charge au niveau applicatif (LB7) ;
- la mise en cache (CDN).

À l'inverse, le chiffrement TLS n'entrave pas a priori les objectifs de sécurité suivants :

- anti-DDoS réseau ;
- la répartition de charges au niveau réseau/transport (LB 4).

Néanmoins, en pratique, de plus en plus de produits de sécurité combinent les différentes fonctions ci-dessus et encouragent les utilisateurs à activer le déchiffrement TLS.

En conséquence, pour pouvoir inspecter les flux de données, analyse qui aujourd'hui ne peut être opérée que sur des **données en clair**, le service de sécurité doit intercepter le trafic chiffré et effectuer un **déchiffrement à la volée des flux chiffrés**. L'intermédiaire se comporte ainsi fonctionnellement comme un « homme au milieu » (« *man-in-the-middle* ») de la communication chiffrée entre le serveur et le client. Ce déchiffrement introduit par nature des faiblesses vis-à-vis de la sécurité et la protection de la

vie privée des communications sur le web. En effet, étant donné que l'accès par un intermédiaire aux données en clair échangées dans un communication TLS est normalement considéré comme une attaque contre TLS, au moins l'une des extrémités de la communication TLS doit s'entendre (on parle informatiquement de « collusion ») avec cet intermédiaire pour que ce déchiffrement puisse avoir lieu (voir ci-dessous).

Plusieurs solutions sont mises en œuvre afin de « contourner » le chiffrement opéré par TLS :

- en fragmentant la liaison TLS (« homme au milieu ») ou ;
- en partageant les clés et secrets TLS.

La fragmentation TLS

La technique dite de « l'homme au milieu » (*man-in-the-middle*) fragmente la session TLS entre le client et le serveur en deux sessions : le client est redirigé vers l'intermédiaire, qui agit vis-à-vis de lui comme un serveur, et lui-même agit à son tour comme un client vis-à-vis du serveur d'origine. L'intermédiaire émet également son propre certificat racine, ce qui nécessite que le navigateur du client ait été configuré de façon à accepter les certificats émis par l'intermédiaire (voir figures 2 et 3). Le client doit donc faire confiance à l'intermédiaire pour effectuer la phase d'entrée en relation (« *handshake* ») TLS.

Le partage de la clé privée du certificat

Dans ce modèle, la clé privée correspondant au certificat du serveur est partagée avec l'intermédiaire de sécurité (voir figures 4 et 5) qui, par ce biais, usurpe l'identité du serveur. Cette solution revient à faire de la fragmentation TLS, mais en utilisant le matériel cryptographique du serveur d'origine. Cette technique remet en cause à la fois la notion de « clé privée », dans le sens où celle-ci est partagée avec un tiers, mais aussi celle de chiffrement de bout en bout (ce pour quoi le protocole TLS a été conçu), dans le sens où l'une des extrémités de la communication chiffrée n'est pas l'extrémité cible (le client s'attend à communiquer avec le serveur final et non pas avec l'intermédiaire).

Dans les deux cas, le flux chiffré arrive au niveau du service de sécurité intermédiaire. Celui-ci déchiffre le flux, l'inspecte et filtre les utilisateurs et les requêtes malveillantes. Pour les visiteurs et les requêtes légitimes, l'intermédiaire transmet le flux au serveur d'origine. Dans ce cas, deux modes sont possibles :

- l'intermédiaire transmet la requête légitime dans un flux non chiffré, ce qui affaiblit considérablement la sécurité des communications et n'est donc pas recommandé (voir figures 2 et 4) ;
- l'intermédiaire chiffre le flux de données à l'aide des éléments cryptographiques du serveur d'origine (voir figures 3 et 5).

Figure 2 - Déchiffrement de flux avec le certificat du CDN sans rechiffrement subséquent

Figure 3 - Déchiffrement de flux avec le certificat du CDN et rechiffrement subséquent

Figure 4 - Déchiffrement de flux avec le certificat du serveur d'origine et sans rechiffrement subséquent

Figure 5 - Déchiffrement de flux avec le certificat du serveur d'origine et avec rechiffrement subséquent

Problématiques du déchiffrement des flux TLS et risques associés

La pratique du déchiffrement des flux TLS pose un risque pour la sécurité et la protection des données personnelles qui transitent dans ces flux, mais aussi la sécurité globale du système informatique serveur, qui expose des données de connexion censées rester confidentielles. Or, cette problématique découle du

besoin de certains acteurs de déchiffrer les flux chiffrés pour des raisons de sécurité en surveillant et analysant ces derniers. Par conséquent, l'analyse des risques et la mise en œuvre de mesures appropriées pour la protection des données supposent une mise en balance des différents facteurs.

Les risques associés au déchiffrement des flux TLS

- **Un risque pour la confidentialité des données déchiffrées** : les données initialement protégées par le chiffrement sont exposées en clair au niveau du point de déchiffrement des flux. Cela implique qu'elles sont potentiellement accessibles aux acteurs impliqués dans le déchiffrement (à savoir, les dispositifs de sécurité et de performance cités dans la présente note). Si ces points ne sont pas correctement sécurisés ou s'ils sont compromis par des acteurs non autorisés, le déchiffrement TLS peut entraîner une violation de la confidentialité des données.
- **Un risque d'augmentation de la surface d'attaque** : lorsque le déchiffrement TLS est effectué au niveau d'un système informatique, celui-ci constitue un point d'entrée supplémentaire pour d'éventuels attaquants. Si ce point d'entrée est compromis, les données qui étaient chiffrées deviennent accessibles en clair à un attaquant, qui contourne ainsi le chiffrement initial.
- **L'introduction d'un point de défaillance unique** (« *single point of failure* », ou « SPOF ») : si le point de déchiffrement est indisponible ou si le déchiffrement échoue, les flux dépendants de ce point seront affectés, entraînant potentiellement une interruption de service ou une diminution de la performance.
- **Des possibilités de transferts hors UE et/ou d'accès par des autorités de pays tiers** : le déchiffrement des flux TLS peut engendrer les possibilités, exposées à la section 1 ci-dessus, sur les données en clair. Par exemple, les données déchiffrées peuvent être transmises à des destinataires situés dans un pays ne garantissant pas le même niveau de protection de données que dans l'UE.

Avant l'adoption du nouveau cadre de protection des données UE-États-Unis (« *Data Privacy Framework* »), cette considération avait conduit l'autorité de protection des données portugaise à ordonner à l'INE, l'institut portugais de la statistique, de cesser tout transfert de données de recensement vers un prestataire américain d'outils de sécurité et de performance web. L'INE avait notamment recours aux services de CDN et de WAF offerts par ce prestataire qui pratique un déchiffrement des flux HTTPS, en utilisant les certificats du prestataire (figures 2 et 3). L'autorité a ainsi relevé que :

- le prestataire détenait les clés de chiffrement et de déchiffrement des flux lui permettant d'avoir accès aux données en clair ; et
- rien ne garantissait que les données étaient traitées dans l'UE car, étant donnée la distribution géographique des serveurs du prestataire, des transferts de données vers des pays ne pouvant pas assurer le niveau de protection équivalent à celui requis par le RGPD pouvaient avoir lieu.

Ces risques s'appliquent également au déchiffrement appliqué à des fonctions de sécurité fournies dans le cadre de l'informatique en nuage.

Les mesures d'atténuation des risques

Pour minimiser les risques associés au déchiffrement des flux TLS tout en préservant l'objectif de sécurité initialement prévu lors de la mise en place de dispositifs de sécurité, des solutions appropriées doivent être envisagées.

Mise en balance des objectifs sécurité du SI vis-à-vis de la protection des données : une analyse approfondie des risques et des avantages du déchiffrement TLS doit être effectuée avant d'y recourir. Cette analyse doit prendre en compte la nécessité de cette pratique pour prévenir les menaces

identifiées. Le client doit se poser la question de savoir si le déchiffrement est évitable en envisageant des mesures alternatives pour assurer la sécurité des applications et des systèmes informatiques. En particulier, les anti-DDoS « réseau » reposant sur le filtrage au niveau de la couche réseau (liste noire d'adresses IP, par exemple) et sur la limitation de requêtes entrantes peuvent éviter que les données soient déchiffrées en transit. De manière similaire, les répartiteurs de charge (*load balancers*) opérant sur la couche 4 ne déchiffrent pas et n'inspectent pas le contenu des données chiffrées. Dans la mesure du possible, le chiffrement de bout en bout pour garantir la confidentialité des données pendant leur transmission peut être une solution à prendre en compte.

Lorsque le déchiffrement des flux TLS est nécessaire :

- **Mise en œuvre de mesures de sécurité au niveau des points de déchiffrement** : il est nécessaire de garantir la sécurité des points de déchiffrement des flux TLS. Pour atténuer les risques de sécurité identifiés ci-dessus, une note de l'ANSSI publiée en 2014 présente des recommandations d'ordre technique à suivre lorsque l'analyse des flux HTTPS nécessite un déchiffrement. En particulier, il est recommandé de mettre en place des mesures telles que des contrôles d'accès stricts aux données déchiffrées, une authentification forte pour accéder aux données déchiffrées, la configuration d'un bastion pour le déchiffrement, la pseudonymisation des données en transit, etc.
- **Mise en œuvre des recommandations énoncées dans la section 1 pour répondre aux problématiques liées aux transferts hors UE et accès par les autorités de pays tiers** : il s'agit notamment d'évaluer la juridiction du pays tiers, la mise en place de mesures supplémentaires complétant les instruments de transferts, la mise en place d'un chiffrement de bout en bout lorsque cela est possible, etc.
- Minimisation des données **faisant l'objet d'un déchiffrement** : il est nécessaire de s'assurer que les données faisant l'objet d'un déchiffrement sont minimisées vis-à-vis de la finalité de garantir la sécurité d'une application ou d'un système informatique. Si la minimisation lors du déchiffrement n'est pas possible, les informations déchiffrées et non nécessaires à l'objectif de sécurité devront être supprimées immédiatement, tandis que les informations déchiffrées utiles et nécessaires pour l'objectif de sécurité devront être supprimées après leur traitement.
- Durée de conservation limitée : dans le cas où les données déchiffrées sont conservées pour analyse postérieure, elles devront être conservées pendant une durée n'excédant pas celle nécessaire au regard de l'objectif de sécurité. Lorsque cela est possible, les données seront pseudonymisées, voire anonymisées.
- Information aux personnes concernées : dans un but de transparence, les personnes concernées devront être informées du fait que leurs données sont susceptibles d'être déchiffrées, accédées et analysées à des fins de sécurité. Cette information devra respecter les exigences de transparence posées par le RGPD.

En 2015, la CNIL a publié sur son site web une communication sur la question du déchiffrement des flux HTTPS.

Pour aller plus loin

Dans certains cas, le déchiffrement des flux TLS peut être déconseillé en raison des risques pour la confidentialité et la protection des données personnelles.

Cela inclut les cas suivants :

- les traitements de données faisant intervenir des catégories particulières de données (articles 9 et 10 du RGPD) ;
- les traitements de données personnelles dont la compromission de la confidentialité engendrerait un impact significatif pour les personnes concernées ;

- les transferts hors de l'UE, impliquant la possibilité d'accès étendus aux données/communications par des autorités de pays tiers.

Un travail sur une partie de ces questions va être lancé dans le cadre des travaux de la CNIL sur la conformité des solutions de cybersécurité avancées.

Vous souhaitez contribuer à l'amélioration de cette fiche ?

Écrivez à retours-cloud[@]cnil.fr

Articles en relation

- Responsables de traitement : comment identifier et traiter des transferts de données hors UE ?
- Transferts de données hors UE : le cadre général prévu par le RGPD
- Cybersécurité : la CNIL agit pour le développement de solutions respectueuses du RGPD
- ANSSI – Comprendre et anticiper les attaques DDoS.
- ANSSI - Recommandations de sécurité concernant l'analyse des flux HTTPS
- Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE
- Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD

< Les pratiques de chiffrement dans l'informatique en nuage (cloud) public
Sommaire
Les actualités sur le cloud >