FICHE 8

CYBERSÉCURITÉ : QUELS CRITÈRES PRENDRE EN COMPTE POUR CHOISIR VOS OFFRES DE CONNECTIVITÉ ?

Disponibilité et confidentialité : des enjeux bien réels pour vos communications électroniques.

Dans son CyberDico, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit la « cybersécurité » comme l'état qui permet de résister à des événements à la fois i) issus du cyberespace, et ii) susceptibles de compromettre notamment la disponibilité, l'intégrité ou la confidentialité des données transmises, traitées ou stockées et des services connexes. Pour y parvenir, la cybersécurité s'appuie sur un ensemble de mesures destinées à protéger les systèmes d'information.

Les services proposés par les opérateurs ont pour principal objectif de permettre les échanges à distance. Ils n'intègrent pas systématiquement des mécanismes de protection contre d'éventuelles atteintes à la disponibilité, à l'intégrité ou à la confidentialité des données transmises, et ne sont pas nécessairement conçus pour faire face à tous types de menaces. Pour une entreprise utilisatrice des réseaux, il est d'autant plus important d'avoir conscience de ces limites que le secteur des télécommunications est particulièrement ciblé par les attaquants, comme l'illustrent plusieurs publications récentes de l'ANSSI[1]. Soyez attentifs aux garanties de cybersécurité fournies par défaut dans les offres des opérateurs, et assurez-vous d'en comprendre les limites (par exemple, les types de perturbations couverts, les zones géographiques couvertes, le type de chiffrement mis en œuvre, etc.) afin de gérer convenablement les risques correspondants.

DISPONIBILITÉ DES SERVICES : COMMENT ÉVALUER ET SÉLECTIONNER LES BONNES GARANTIES CONTRACTUELLES ?

Pour assurer une disponibilité optimale de vos communications électroniques, il convient, en premier lieu, de disposer d'une connexion dont le niveau de robustesse est adapté à vos besoins. Il existe différents types de garanties contractuelles relatives à la disponibilité, qui peuvent porter aussi bien sur la **qualité des services fournis** (par exemple, un débit[2] minimum garanti) que sur le **rétablissement des services** en cas de défaillance totale (par exemple, les garanties de temps d'intervention ou de temps de rétablissement). Pour choisir une offre de connectivité, il est important de sélectionner les niveaux de garanties adaptés à vos besoins. En fonction des spécificités de votre activité, il peut être préférable de souscrire à des offres proposant certaines options qualitatives complémentaires (par exemple, disposer d'une garantie de temps de rétablissement de 4h en heures non ouvrées (HNO), 7j/7). Vous pouvez vous référer à : FICHE 23 : Quelle qualité de service pour les offres fixes proposées aux entreprises ? pour plus de détails sur les garanties proposées par les opérateurs, et notamment leurs limites.

Enfin, lorsque la disponibilité d'un service de connectivité représente un enjeu de résilience particulièrement important, vous pouvez souscrire à des **services de secours** (par exemple, une bascule automatique des liens sur un réseau alternatif de type 4G/5G fixe ou satellite), ou mettre en place une **architecture de** connectivité **redondante multi-opérateurs**, en souscrivant par exemple un même service d'accès fixe auprès de différents fournisseurs. Dans ce dernier cas, il est important de déterminer dans quelle mesure les infrastructures des opérateurs sont partagées (par exemple au niveau des équipements ou des chemins de fibre optique), pour assurer qu'une même perturbation (comme une coupure physique localisée par exemple) n'affecterait pas l'ensemble des liens simultanément.

1. État de la menace ciblant le secteur des télécommunications
Panorama de la cybermenace 2024
Panorama de la cybermenace 2025
2. Les termes surlignés sont définis dans le glossaire en page 122.

De façon générale, il est recommandé de faire l'inventaire de vos besoins en matière de connectivité (ceux de vos utilisateurs, de vos applications, de vos infrastructures) lors de la souscription de services de communications électroniques. Il convient de tenir à jour une liste de vos prestataires de connectivité, d'évaluer régulièrement les conséquences associées à la perte d'un service, et de vous assurer que les garanties de disponibilité offertes à titre standard répondent à vos besoins. Le cas échéant, vous pouvez souscrire à des services de communications électroniques à qualité de service renforcée (garantie de débit ou de temps de rétablissement), et prévoir des moyens de substitution (par exemple, redondance, secours). Tous ces éléments peuvent être formalisés au sein d'un plan de continuité d'activité.

Connaissez-vous les attaques dites par « déni de service distribué » (DDoS[1]) ? Il s'agit d'un type d'attaque informatique qui vise à rendre indisponible un service en sollicitant les ressources sur lesquelles il repose jusqu'à son épuisement. Pour vous protéger contre ce type d'attaques, dans la mesure où la protection n'est pas nécessairement incluse dans les offres standard des opérateurs, il peut être important de souscrire à une option complémentaire dédiée. Pour en savoir plus à ce sujet, vous pouvez consulter les guides 🌐 Les Essentiels de l'ANSSI - Les dénis de service distribués et 🌐 Comprendre et anticiper les attaques DDoS.

CONFIDENTIALITÉ DES DONNÉES : COMMENT ASSURER LA SÉCURITÉ DE VOS COMMUNICATIONS ?

Les services de communications électroniques ne garantissent pas, de manière systématique et par défaut, la protection des données transmises. C'est notamment le cas de nombreux services de réseaux virtuels, qui permettent avant tout l'interconnexion entre des sites, des réseaux, ou des équipements distants. À titre d'exemple, le tableau ci-dessous illustre, pour cinq types de services de connectivité choisis, différentes variantes technologiques proposées habituellement sans mécanisme de chiffrement moderne et/ou de bout en bout.

Type de service	Exemples non exhaustifs de technologies de connectivité habituellement proposées sans chiffrement moderne et/ou de bout en bout
Téléphonie fixe	RTC[2]
Téléphonie mobile	2G, 3G, 4G, 5G
Accès à internet fixe	ADSL, FttO
Messages textes mobile	SMS
Réseaux privés virtuels[3]	MPLS
Connectivité par satellite (par exemple pour l'accès à internet)	DVB-S2/RCS2, protocoles propriétaires

1. *Distributed Denial of Service*, en anglais.
2. *Réseau Téléphonique Commuté*
3. L'appellation « réseau privé virtuel » (VPN) est ambigüe et peut recouvrir des réalités différentes selon les contextes. D'une part, dans le domaine des télécommunications, le terme « privé » renvoie essentiellement à l'isolation des flux d'un client donné de ceux d'autres usagers ou de l'Internet, sans protection effective du point de vue de la cybersécurité. D'autre part, dans le domaine de la cybersécurité, un service « VPN » désigne souvent, par simplification, des solutions intégrant par défaut un mécanisme chiffrement. Cette ambiguïté exige d'examiner précisément les mécanismes de protection mis en œuvre avant de choisir une offre.

Si vos communications électroniques (par exemple, la voix, les messages, les données, les mots de passe) reposent sur un service ne bénéficiant pas de mécanisme de chiffrement moderne et de bout en bout, alors elles sont exposées à un plus grand risque d'interceptions malveillantes par des attaquants cybercriminels ou étatiques.

Ce risque est d'autant plus important si vous produisez ou manipulez des données sensibles (notamment en tant qu'entreprise de la base industrielle et technologique de défense, etc.). En fonction des spécificités de votre activité, il peut donc être important de se renseigner sur les mécanismes de chiffrement mis en œuvre à titre standard sur les réseaux des opérateurs, et de les compléter le cas échéant pour obtenir un chiffrement moderne et de bout en bout (par exemple en souscrivant à d'éventuelles options auprès des opérateurs, en déployant des mécanismes complémentaires côté client).

Pour illustration, **la technologie** VoIP[5] peut être habituellement proposée par les opérateurs avec un mécanisme de chiffrement moderne et de bout en bout des conversations si les protocoles DTLS-SRTP[6] et SIP TLS sont mis en œuvre ensemble et à l'état de l'art (quant aux informations techniques de signalisation permettant la gestion des appels, celles-ci ne peuvent être en général chiffrées que de proche en proche).

Enfin, pour bénéficier d'une garantie de sécurité, il est parfois possible de souscrire à des offres s'appuyant sur des technologies qui disposent d'un visa de sécurité délivré par l'ANSSI. Cela peut s'avérer particulièrement adapté à vos besoins télécoms les plus sensibles.

De façon générale, il est recommandé, pour assurer la confidentialité des communications, de :

- **identifier les points d'interconnexion avec des réseaux externes (entre les implantations de votre entreprise, avec internet) ;**
- **cartographier les flux de données non chiffrés transitant sur les infrastructures des opérateurs, en prenant soin d'identifier d'éventuelles données sensibles (comme certaines données métier ou techniques) ;**
- **protéger le cas échéant les données sensibles au sein de canaux renforcés cryptographiquement, de bout en bout (comme par exemple, via un tunnel IPsec[7] ou TLS configuré à l'état de l'art) ;**
- **anticiper les conséquences d'une exposition de données sensibles, ainsi que la gestion d'éventuelles crises[8] en cas de divulgation ;**
- **sensibiliser vos collaborateurs aux enjeux relatifs à la protection des données sensibles lorsque celles-ci sont en transit sur les réseaux.**

5. *Voice over IP*, en anglais.
6. *Secure Real-Time Transport Protocol*, en anglais.
7. En ce qui concerne la protection des flux en confidentialité, l'ANSSI a mis en place des guides détaillés pour la mise en place de tunnels IPsec TLS, pour l'architecture de passerelles de connexions à internet, et pour le nomadisme numérique.
8. Pour vous accompagner, l'ANSSI a également publié un ensemble de guides permettant d'anticiper et gérer une crise d'origine cyber.

POUR ALLER PLUS LOIN

Pour vous accompagner dans l'établissement d'une démarche de gestion des risques de cybersécurité, plusieurs sources de bonnes pratiques existent, comme le guide de l'ANSSI relatif à l'hygiène informatique, celui produit à destination des TPE/PME, ou encore le service numérique MesServicesCyber. Ces références, qui rappellent d'importants principes généraux de gestion du risque cyber, recommandent en particulier la mise en place de plans d'assurance sécurité (ou « PAS ») avec les fournisseurs, ainsi que l'intégration systématique de clauses d'audit dans les contrats.

En outre, la directive européenne dite « NIS2 » vise à élever le niveau de sécurité numérique de secteurs considérés comme critiques et hautement critiques dans l'ensemble de l'Union européenne. Sa mise en œuvre contribuera notamment à ce que les fournisseurs de réseaux et de services de communications électroniques mettent en place de nouvelles obligations adaptées aux enjeux de cybersécurité actuels. Néanmoins, ce nouveau dispositif ne remplace pas la nécessité, pour votre entreprise, d'identifier et de formaliser ses propres besoins en matière de cybersécurité et de résilience des communications et, le cas échéant, de compléter d'éventuels mécanismes de protection mis en place par votre opérateur par un ou plusieurs mécanismes côté client.

Il est toutefois important de rappeler que :

- **le risque zéro n'existe pas : un service moderne protégé cryptographiquement et redondé n'est pas invulnérable et peut faire l'objet d'attaques, qui peuvent être réussies selon le niveau de l'attaquant et les ressources engagées par lui ;**

- **cette courte fiche de sensibilisation ne saurait aborder de façon exhaustive l'ensemble des enjeux de cybersécurité en matière de télécommunications ; à titre d'exemple, celle-ci n'évoque ni tous les types de services télécoms (comme la connectivité IoT, les messages RCS, les services SD-WAN), ni toutes les caractéristiques à préserver (comme la latence ou le taux de perte de paquets), ni toutes les menaces contre lesquelles se défendre (comme la propagation d'une attaque entre sites distants, les attaques sur les terminaux mobiles et postes nomades, les menaces internes aux opérateurs, ou encore la menace quantique), ni les propriétés de sécurité à assurer (comme l'intégrité), ou encore toutes les façons d'y porter atteinte (par exemple, l'absence d'authentification mutuelle entre un équipement utilisateur et le réseau de l'opérateur).**