Télécommunications par satellite

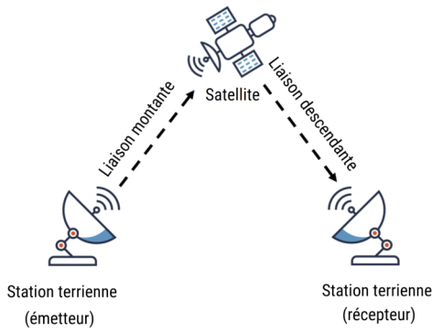
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mars 2023 | ITSAP.80.029

Dans un monde où la communication est primordiale, les télécommunications par satellite (SATCOM pour *Satellite Communications*) fournissent la connectivité aux personnes de communautés éloignées dans lesquelles les réseaux cellulaires ou les connexions câblées ne sont pas disponibles. Les technologies SATCOM offrent d'importantes fonctionnalités, comme des canaux de communications essentiels en période de conflits ou de catastrophes naturelles, lorsque les infrastructures de communications traditionnelles sont endommagées ou inaccessibles. Le présent document énumère des conseils sur la façon d'atténuer les risques et est conçu pour les fournisseurs de réseau SATCOM, les exploitants d'infrastructures essentielles et les organisations dépendant d'une connectivité par satellite pour offrir leurs services.

Que sont les télécommunications par satellite?

SATCOM consistent en l'utilisation de satellites artificiels pour relier au moins deux points sur Terre. L'un des nombreux avantages des SATCOM est de permettre les communications entre des points géographiquement très éloignés. Les SATCOM se servent d'une station terrienne pour transmettre des signaux au satellite (liaison montante). Ensuite, le répéteur intégré au satellite amplifie les signaux et les transmet à une station terrienne réceptrice (liaison descendante). Il peut s'agir de signaux vocaux, vidéo ou de données. Un groupe de satellites, appelé une constellation de satellites, assure la disponibilité des services tels que l'accès Internet par satellite et la téléphonie par satellite partout sur Terre.



Quels sont les risques?

Les cybermenaces visant les réseaux SATCOM peuvent avoir des répercussions considérables sur place. Les menaces peuvent se propager dans de multiples secteurs et systèmes, causant des dommages collatéraux aux infrastructures essentielles utilisées sur Internet et sur les réseaux mobiles, ou aux services d'électricité. Les auteures et auteurs de menace peuvent cibler les SATCOM de différentes manières.

- Brouiller les signaux afin de bloquer les communications entre un satellite et une station terrienne, ce qui peut mener à une perturbation délibérée des communications essentielles.
- Intercepter les transmissions montantes et descendantes du satellite au moyen de protocoles de communications non chiffrés.
- Attaquer la chaîne d'approvisionnement en créant des portes dérobées lorsque le matériel ou les logiciels de tiers non approuvés ne sont pas examinés ni vérifiés adéquatement avant de conclure des partenariats.
- Cibler les petits satellites comme les CubeSats qui sont généralement moins coûteux, plus légers et assemblés en utilisant des logiciels et du matériel commerciaux sur étagère (COTS pour Commercial-off-the-shelf). En raison du faible coût et des contraintes de ressources, il est possible que ce type d'équipement n'ait pas la capacité de mettre en œuvre des mesures de sécurité robustes.
- Exploiter des appareils SATCOM non sécurisés, dont les émetteurs connectés à Internet et les récepteurs de station. Les auteures et auteurs de menace dotés de moyens sophistiqués peuvent tirer parti des vulnérabilités connues ou du jour zéro sur ces systèmes pour causer des dommages ou accéder à d'autres parties du réseau.
- Utiliser des systèmes satellites pour géolocaliser les bornes de terre afin de trouver des satellites précis à des fins malveillantes, ce qui peut avoir des répercussions sur la confidentialité et la sécurité opérationnelle de la population en général et des forces armées.

À quoi servent les SATCOM ?

L'utilisation des technologies SATCOM continue d'augmenter afin d'aider à répondre à la demande croissante de connectivité mondiale et d'information en temps réel. Ces technologies sont utilisées le plus couramment dans les domaines suivants:

Télécommunications mobiles. Les téléphones satellites sont des types d'appareils mobiles qui représentent un outil indispensable pour de nombreux secteurs, dont le gouvernement (lors d'interventions en cas d'urgence et de situations de reprise après sinistre), le secteur minier (afin de surveiller le personnel et l'équipement), ainsi que le secteur pétrolier et gazier (pour se connecter aux sites de distribution, de production et d'exploration).

Radiodiffusion. Les télédiffuseurs et les radiodiffuseurs utilisent les SATCOM pour distribuer une grande variété de contenu à la clientèle. Le contenu diffusé inclut les nouvelles, les sports et les divertissements, ainsi que les flux de diffusion en direct. La clientèle peut accéder à ce contenu de la maison et du bureau ou pendant des déplacements en région urbaine ou rurale.

Accès Internet par satellite. Il s'agit d'un type de connexion Internet sans fil permettant aux personnes de régions éloignées et de nouveaux quartiers d'accéder à des réseaux de communication, pour les écoles ou des services de télémédecine en milieu rural, par exemple. Tout comme les téléphones satellites, il permet aux organisations de maintenir une connectivité avec leur personnel en télétravail et leurs opérations à distance. Certains ministères et organismes du gouvernement du Canada (GC) utilisent des routeurs connectés à un satellite dans les régions éloignées comme solution de rechange pour obtenir un accès Internet, conformément à leur stratégie de continuité des activités.

Forces armées. Les technologies SATCOM permettent aux forces armées de communiquer avec leur personnel déployé partout dans le monde, dans des environnements maritimes, terrestres et aériens. Ces communications incluent la transmission d'information essentielle sur la reconnaissance et la surveillance dans le but d'appuyer les missions opérationnelles des forces armées.

Connexion satellite à un appareil sans intermédiaire. Cette technologie émergente fournit une connectivité directement au téléphone mobile ou à l'appareil de l'Internet des objets (IdO) d'une utilisatrice ou d'un utilisateur. La fonctionnalité initiale est limitée aux services de localisation d'urgence, à la messagerie et aux applications à faible débit. Une intégration complète aux scénarios d'utilisation des reseaux 5G est en cours de développement.

Terminal à très petite ouverture (TTPO)

Un TTPO est une technologie qui s'applique à une station terrienne de télécommunication par satellite bidirectionnelle utilisant de petites antennes paraboliques (généralement moins de trois mètres) pour transmettre et recevoir des signaux sur les réseaux SATCOM. Les systèmes TTPO sont couramment utilisés lors de transactions par cartes de crédit de point de vente dans des commerces, de la transmission des transactions bancaires entre le bureau central et les succursales, de la transmission des télémesures provenant de systèmes de technologies opérationnelles (TO) et de la prestation d'accès Internet dans les régions éloignées. Les TTPO sont faciles à déployer comme leur configuration et leur utilisation exigent peu d'infrastructures.

Pour en savoir plus, consultez la publication *Protecting VSAT Communications* (en anglais seulement) de la National Security Agency (NSA).

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Télécommunications par satellite

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mars 2023 | ITSAP.80.029

Comment protéger l'écosystème des SATCOM

Les **fournisseurs de réseau SATCOM** doivent protéger l'équipement satellite déployé en orbite contre les dommages physiques causés par des menaces malveillantes ou non intentionnelles. De plus, les mesures d'atténuation suivantes peuvent réduire les risques de compromission visant l'écosystème des SATCOM:

- ☐ Surveiller les activités du réseau pour détecter le trafic anormal aux points d'entrée et de sortie. Le trafic non autorisé et les incidents de sécurité doivent faire l'objet d'une enquête le plus tôt possible par le personnel qualifié du centre des opérations de sécurité (COS) afin d'intervenir rapidement et d'empêcher qu'une compromission se propage dans le reste du réseau.
- ☐ Veiller à la séparation logique ou physique de toutes les communications de plan d'utilisation, de gestion et de contrôle. Elles doivent également être isolées, chiffrées et authentifiées dans le réseau et lorsqu'elles sont transmises au moyen de liaisons par satellite.
- ☐ Mettre en œuvre des mesures de sécurité physique pour protéger l'infrastructure principale et les stations terriennes des satellites contre des attaques malveillantes, des pannes d'équipement ou des catastrophes naturelles. Certains exemples de mesures de sécurité physique incluent l'utilisation de caméras de surveillance, de verrous, de contrôles d'accès et de protection contre les incendies et les inondations. Ces mesures peuvent prévenir l'accès non autorisé et la perte d'accès de gestion à l'équipement du réseau principal essentiel, ou la réduction de la capacité du centre d'exploitation du réseau.
- ☐ Éviter que les appareils SATCOM se connectent inutilement à Internet ou aux réseaux publics. Au besoin, mettre en place des mesures de protection des réseaux comme des pare-feu et des réseaux privés virtuels (RPV) pour veiller à ce que l'accès soit limité aux communications de confiance.
- ☐ Utiliser des faisceaux étroits et des méthodes de sauts de fréquence pour réduire les interférences de signaux et éviter les interceptions. Les faisceaux étroits concentrent les signaux satellites pour couvrir des zones géographiques limitées sur Terre. Les sauts de fréquence consistent à basculer rapidement la fréquence porteuse pendant la transmission.
- ☐ Veiller à ce que l'infrastructure réseau principale des satellites soit conçue et construite en prenant en compte la résistance et la redondance, y compris, par exemple, la mise en place de sites de sauvegarde à chaud et à froid, de l'écriture miroir ou de la réplication du stockage. Utiliser les stratégies et les protocoles adéquats pour minimiser l'instabilité de la table de routage Internet principale. Ces mesures permettent de garantir le flux des données en cas de panne ou de prévenir la perte complète de la plateforme d'authentification des abonnés.

Les exploitants d'infrastructures essentielles, les entreprises et les organisations peuvent contribuer à la protection de l'écosystème des SATCOM en mettant en place les mesures suivantes:

- ☐ Utiliser les outils contenant des mesures de protection liées à la sécurité des transmissions pour dissimuler le volume de trafic, cacher la provenance et la destination du trafic et confirmer que les sessions d'accès aux terminaux distants sont autorisées.
- ☐ Installer des appareils de filtrage sur les antennes pour réduire l'interférence localisée des brouillages de signaux terriens non malveillants (non intentionnels) provenant d'autres appareils sans fil.
- ☐ Collaborer avec les opérateurs de satellites ou les fournisseurs de services de réseau pour comprendre les scénarios de fuites de données possibles et atténuer le risque d'exposition de l'information de géolocalisation.
- ☐ Configurer les appareils de communications mobiles et SATCOM connectés à Internet en se servant de conventions d'affectation des noms et d'identifiants. Ainsi, les auteures et auteurs de menace auront de la difficulté à identifier les appareils sur le réseau et les appareils ayant des vulnérabilités exploitables.
- ☐ Veiller à ce que les développeurs de logiciels et d'équipement SATCOM utilisent les pratiques de développement de logiciels sécurisés (p. ex. éviter l'utilisation de portes dérobées codées en dur ou de mécanismes d'authentification et de chiffrement faibles).

À titre de pratiques exemplaires générales, les fournisseurs de réseau SATCOM et leur clientèle devraient mettre en place les mesures d'atténuation suivantes pour protéger leurs réseaux et l'ensemble de l'écosystème des SATCOM:

- ☐ Appliquer le principe du droit d'accès minimal, c'est-à-dire accorder aux utilisatrices et aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir leurs tâches autorisées.
- ☐ Activer les mises à jour automatiques sur l'équipement TI et corriger les vulnérabilités exploitables connues le plus tôt possible.
- ☐ Utiliser des systèmes de détection d'intrusion pour surveiller et relever le trafic indésirable (p.ex. balayages des ports) sur le réseau. Des services ou outils d'évaluation des vulnérabilités devraient être utilisés pour analyser les vulnérabilités sur le réseau.
- ☐ Isoler le réseau TI organisationnel des réseaux de technologies opérationnelles (TO) et d'Internet des objets (IdO) afin de réduire le risque de compromission de l'information sensible en cas de brèche de sécurité.
- ☐ Sécuriser les appareils de communications connectés à un satellite en modifiant les justificatifs d'identité par défaut offerts par le fournisseur, en utilisant une authentification multifacteur et en chiffrant les données qui en découlent.
- ☐ Élaborer un plan de reprise informatique dans le cadre de la stratégie de continuité des activités au cas où les services SATCOM ne sont pas disponibles.
- ☐ Établir une stratégie robuste de gestion des risques liés à la chaîne d'approvisionnement afin de réduire les risques d'acquisition et de déploiement de produits possiblement vulnérables dans l'écosystème des SATCOM. Cette stratégie doit inclure l'application de clauses liées à la sécurité lors des contrats d'approvisionnement et lors de l'achat d'équipement et de services de télécommunications provenant de fournisseurs de confiance.

Renseignements supplémentaires

- Pratiques exemplaires en matière de cybersécurité à intégrer dans votre organisation (ITSAP.10.102)
- Isoler les applications Web (ITSAP.10.099)
- Considérations en matière de sécurité pour les infrastructures essentielles (ITSAP.10.100)
- Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)
- Clauses contractuelles visant l'équipement et les services de télécommunications (TSCG-01L)

Consultez la publication *Strengthening cybersecurity of SATCOM network providers and customers* (en anglais seulement) de la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

 No de cat.D97-1/80-029-2023F-PDF ISBN 978-0-660-47754-1