FÉDÉRATION FRANÇAISE DES TÉLÉCOMS

Exigences de sécurité à destination des fournisseurs d'équipements d'infrastructure et plateformes de service

Fédération Française des Télécoms

29 mai 2018

Objet du document

Ce document décrit les exigences de sécurité demandées par les opérateurs membres de la Fédération française des télécoms à leurs fournisseurs d'équipements d'infrastructure et de plateformes de service, ainsi qu'à leurs prestataires.

Le périmètre d'application de ce document est l'ensemble des actifs de chaque opérateur de télécommunications. Il comporte des exigences sur les produits, ainsi que sur les prestations réalisées dans le cadre de l'intégration, l'exploitation et leur maintenance.

Les exigences de sécurité décrites dans le document sont la déclinaison du document cité en référence, en particulier celles concernant le poste d'administration des systèmes techniques qui devra faire l'objet d'une attention particulière de la part des fournisseurs.

Ces exigences sont un socle. Chaque opérateur pourra particulariser ce socle et ajouter ses propres exigences en fonction de son architecture et de ses prestations de SOC.

Par ailleurs, dans le contexte d'un système d'information d'importance vitale, il convient de s'assurer du respect par le fournisseur - ou son prestataire -, en tant que sous-traitants de l'opérateur, de l'ensemble des règles applicables du document de référence.

Référence

Ce document s'appuie sur l'arrêté du 28 novembre 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'impor-

tance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Communications électroniques et Internet » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, publié au J.O. n° 0282 du 04/12/2016.

Exigences de gouvernance

Cartographie

L'opérateur pourra demander au fournisseur de fournir les éléments nécessaires à la constitution de de la cartographie de l'actif, comme par exemple le schéma des flux internes de l'actif, la cartographie des applications implémentées sur l'actif, la liste des composants physiques constituant l'actif.

Il est rappelé au fournisseur que les éléments de cartographie des actifs sont des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal.

Il incombe au fournisseur de se mettre en conformité afin de protéger les données confidentielles de cartographie du système technique déployé chez l'opérateur par exemple lorsque l'actif est un composant d'un système d'information d'importance vitale de l'opérateur au sens de l'article R1332-41-2 du Code de la défense.

Si les données sont classifiées ou font l'objet d'un marquage, alors le fournisseur doit se doter des moyens de stockage adéquats - par exemple le fournisseur peut se référer à IGI 1300 pour les exigences de gestion des données classifiées Confidentiel Défense (CD) - et respecter le marquage du document (ex. Spécial France).

Maintien en condition de sécurité de l'actif

Journalisation

Les événements de sécurité relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité de l'actif, ainsi qu'au fonctionnement de l'actif, sont enregistrés dans un système de journalisation pendant une durée d'au moins 6 mois.

Pour ce faire, l'opérateur raccordera l'actif à un système de journalisation (log management) externe à l'actif.

L'actif devra donc implémenter des mécanismes comme SFTP ou syslog permettant d'envoyer les évènements de sécurité au système de journalisation de l'opérateur.

L'opérateur attend également du fournisseur qu'il documente les évènements de sécurité de l'actif, de façon à les rendre exploitables par un SIEM (Security Information and Event management).

Les logs correspondant à des évènements graves comme une détection d'intrusion sur l'actif sont détaillés. Le système d'horodatage des évènements doit être asservi à une source de temps externe à l'actif , via le protocole NTP par exemple.

Dans le cas où les évènements devraient être stockés localement sur l'actif, le fournisseur formalisera une justification en cas d'exception vis-à-vis de la période de rétention.

Gestion de vulnérabilités

L'opérateur demande au fournisseur de décrire dans une procédure les conditions permettant de maintenir le niveau de sécurité des ressources des actifs en fonction de l'évolution des vulnérabilités et des menaces. En particulier, le fournisseur décrira la politique d'installation de toute nouvelle version et mesure correctrice de sécurité d'une ressource et les vérifications à effectuer avant l'installation. Le fournisseur s'engage à mettre en oeuvre un processus permettant :

- d'identifier les vulnérabilités liées à l'Operating System (Windows, Linux) et aux applicatifs - sur les systèmes techniques composant l'actif, par exemple par une veille des alertes de différents CERT et des éditeurs ;
- d'analyser la criticité de la vulnérabilité et déterminer la priorité d'application d'un correctif ;
- de prévenir l'opérateur sans délai et par un canal dédié (messagerie chiffrée ou CERT par exemple) ;
- correction définitive dans les délais définis au contrat de maintenance selon la criticité de l'anomalie ouverte, convenue entre l'opérateur et le fournisseur.

Gestion des incidents de sécurité et gestion de crise

Le fournisseur mettra en oeuvre une procédure de traitement des incidents et de gestion de crise en concordance avec l'opérateur.

Cette procédure décrira les moyens techniques à appliquer en cas de crise, comme par exemple appliquer une configuration système afin d'éviter les at-

taques ou d'en limiter les effets, proscrire l'utilisation de supports de stockage amovibles connectés à l'actif, ou encore isoler l'actif du réseau internet en déconnectant physiquement ou logiquement ces interfaces réseau.

L'opérateur demande au fournisseur de mettre en place un service de permanence 24h/24 et 7j/7 en cas d'incident critique sur l'actif.

Cette permanence pourra être également sollicitée sur demande expresse de l'opérateur afin de demander un accompagnement du fournisseur dans le cadre d'analyse relatives à des incidents, des vulnérabilités et des menaces portant atteinte à la sécurité de l'actif comme par exemple la recherche de marqueurs de compromission sur l'actif.

L'opérateur demande au fournisseur d'indiquer un contact sécurité opérationnel sur l'actif, et de mettre en place des moyens d'échange sécurisés, validés par l'opérateur, à utiliser pendant la crise.

En cas d'incident de cybersécurité, le rapport d'analyse et traces ou preuves associées devront être stockés sur un réseau dédié, et l'accès doit y être restreint aux seules personnes ayant le besoin d'en connaître.

Indicateurs

L'opérateur évalue la sécurité de ses actifs par le suivi d'indicateurs de maintien en condition de sécurité, comme par exemple le pourcentage d'utilisateurs accédant aux actifs par type de comptes, le pourcentage de ressources systèmes de l'actif non mises à jour ou corrigées d'un point de vue sécurité, etc.

L'opérateur demandera au fournisseur de l'accompagner dans la définition et production des indicateurs mentionnés dans la règle (par exemple, l'opérateur pourra fournir un template à remplir par le fournisseur).

Accès et administration de l'actif

Le fournisseur s'assure de la probité de son personnel et de ses prestataires, en particulier lorsque ceux-ci disposent d'un droit à fort privilège et sensibilise son personnel aux problématiques de sécurité.

L'opérateur souhaite pouvoir identifier les intervenants, systèmes d'information ou processus ayant réalisé une opération sur l'actif (pour rappel : toute action de consultation, ajout, modification ou suppression d'un élément de l'actif). Ce qui implique du fournisseur :

— que l'exploitation et la maintenance de l'actif soient réalisées via des comptes nominatifs uniquement (pas de compte générique), et que les opérations nécessitant des privilèges élevés soient réalisées uniquement

via des comptes d'administration individualisés, que le principe du moindre privilège soit respecté dans l'attribution des droits,
— qu'il produise et maintienne dans le temps la liste des comptes nominatifs/individualisés (d'administration et autres) qu'il utilise, qu'il renouvelle les secrets des comptes nominatifs/individualisés au moins une fois par an,
— qu'il désactive et supprime les comptes inutilisés,
— qu'il formalise une justification en cas d'exception à ces exigences, comme par exemple lorsqu'il est dans l'impossibilité de créer des comptes nominatifs/individualisés sur l'actif,
— qu'il fasse appliquer les mêmes directives à ses sous-traitants opérant ou maintenant l'actif.

Le processus d'accès à l'actif par un utilisateur ou par un processus automatique s'appuie sur un mécanisme d'authentification basé sur un élément secret.

Le fournisseur fournira à l'opérateur les règles de gestion des éléments secrets d'authentification mis en oeuvre dans l'actif :
— processus de modification des secrets, dont ceux par défaut, avant la mise en service de l'actif,
— processus de renouvellement des secrets dans la vie de l'actif,
— mécanismes de protection des secrets mis en oeuvre afin de réduire l'accès aux secrets aux seules personnes ayant droit d'en connaître (chiffrement, droits d'accès, mots de passe différents entre les différents comptes privilégiés et non privilégiés,),
— mesures de traçabilité qu'il est possible de mettre en oeuvre afin de réduire le risque lié à l'utilisation d'un élément secret d'authentification, en particulier si celui-ci ne peut pas être renouvelé.

Le fournisseur et ses sous-traitants utiliseront exclusivement des postes d'administration sous maîtrise du fournisseur ou d'un prestataire mandaté pour opérer et maintenir l'actif. Ces postes d'administration seront durcis et déconnectés d'Internet ou de serveurs de messagerie sur internet. Ces postes d'administration devront disposer d'antivirus, de mémoires de stockage chiffrées, et être à jour du point de vue de la sécurité autant que nécessaire (systèmes d'exploitation, applications, etc.).

Toutefois, si pour des raisons opérationnelles ou organisationnelles, le fournisseur utilise ce poste d'administration pour d'autres opérations que des opérations d'administration, alors il devra mettre en place un cloisonnement pour isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel utilisé pour les opérations d'administration. Pour cela, un accès à distance à un environnement bureautique depuis un environnement d'administration peut être mis en oeuvre mais non l'inverse.

Les postes d'administration doivent être hébergés sur un réseau dédié aux activités d'administration de systèmes (accès à privilèges sur des actifs d'opérateurs Réseau), et cloisonné du reste du SI du fournisseur. Le poste devra être prioritairement utilisé dans des locaux professionnels, dont le fournisseur a la maîtrise. En cas d'utilisation hors des locaux professionnels, une solution d'accès distants au SI du fournisseur peut être utilisée, et devra assurer l'intégrité, l'authenticité et la confidentialité des flux (chiffrement IPsec de préférence, TLS à défaut) et l'authentification forte de l'administrateur. Le poste distant doit être configuré de manière à ne pas pouvoir constituer une passerelle entre le SI du fournisseur et des réseaux non maîtrisés (ex : Internet).

Si des annuaires d'identification et d'authentification sont utilisés pour les ressources d'administration (postes d'administration et outils utilisés pour l'exploitation ou la maintenance de l'actif), ces annuaires doivent être dédiés à ces ressources et déployés dans des zones de confiance, réservées aux ressources d'administration.

L'ensemble de l'outillage technique du prestataire permettant l'administration des postes d'administration (maintien en conditions opérationnelle et de sécurité, configuration) doit être dédié à ces ressources et déployés dans des zones de confiance, réservées aux ressources d'administration.

Le fournisseur doit mettre en place une authentification forte de l'ensemble de ses ressources accédant au SI de l'opérateur sur son environnement permettant l'accès aux matériels et/ou logiciels fournis.

Les flux d'administration de l'actif seront chiffrés depuis le poste d'administration du fournisseur, même si un VPN relie le fournisseur à l'opérateur. L'opérateur attend du fournisseur qu'il documente et présente la solution technique du poste d'administration mise en place.

Installation, cloisonnement et durcissement

Afin de limiter la propagation des attaques informatiques, le fournisseur implémentera des dispositifs de cloisonnement (ACL, règles firewall,) de l'actif et de ses sous-systèmes vis-à-vis des systèmes concomitants, afin de séparer les différents plans (utilisateur, données, contrôle) de l'actif. Les flux entrants et sortants de l'actif seront documentés dans une matrice et réduits au strict nécessaire. Il en sera de même des flux internes de l'actif, c'est-à-dire entre ses différents sous-systèmes.

Le fournisseur implémentera des mécanismes de durcissement des matériels et logiciels composant l'actif. Pour ce faire, le fournisseur :

— listera l'ensemble des services actifs sur l'actif,

— désactivera les services et fermera les ports inutilisés de l'actif,
— installera les derniers niveaux de patch de sécurité et antivirus sur l'actif avant sa mise en service, et proposera un mécanisme d'installation des mises à jour des patchs de sécurité et antivirus.

L'opérateur pourra demander à raccorder l'actif à ses plateformes d'authentification, de traçabilité, d'accès (bastion), d'antivirus, de scans de ports et vulnérabilité, de patchs management et de journalisation. Si, pour des raisons opérationnelles, l'actif ne peut pas être raccordé à de telles plateformes, alors l'opérateur pourra demander au fournisseur de proposer un plan de mise en conformité et le délai nécessaire à son implémentation.

Les supports amovibles utilisés par le fournisseur pour les opérations d'intégration, d'exploitation et de maintenance de l'actif, feront l'objet d'une inspection approfondie avant utilisation afin d'éviter par exemple l'exécution de code malveillant sur l'actif et pourront être notariés.

Exigences techniques liées au RGPD

Un actif manipulant ou stockant des données à caractères personnels est soumis au règlement général de protection des données (RGPD) à partir du 25 mai 2018, ce qui implique du fournisseur de l'actif :

— de proposer à l'opérateur un mécanisme permettant de pseudonymiser les données à caractère personnel collectées sans nuire au bon fonctionnement de l'actif,
— de proposer à l'opérateur un mécanisme permettant de rendre les données traitées au-delà d'une durée paramétrable. Les données ne doivent pas pouvoir être ré-identifiées,
— de proposer à l'opérateur un mécanisme permettant de supprimer à la demande des données
— de proposer à l'opérateur un mécanisme permettant d'extraire à la demande les données,
— de proposer à l'opérateur un mécanisme permettant d'exclure un abonné d'un traitement.