Lignes directrices « gestion sécuritaire de la chaîne d'approvisionnement » - Supply Chain Proces - 2020

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be

Table des matières

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

1 Introduction

1.1 Objectif

Le présent document a pour but de décrire des objectifs de contrôle afin de protéger la confidentialité, l'intégrité et la disponibilité (« confidentiality, integrity, availability », triade CIA) au sein de la chaîne d'approvisionnement des actifs et services de réseau pour les opérateurs de services essentiels (OSE) en vertu de la législation NIS (cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, date de publication 3/5/2019, NUMAC 2019011507).

1.2 Contribution

Ce document a été écrit avec la contribution de l'IBPT(Institut Belge des services Postaux et des Télécommunications), de plusieurs autres services publics et experts en (Cyber)sécurité.

1.3 Chaîne d'approvisionnement des actifs et services de réseau

Le recours de plus en plus fréquent à des partenaires tiers pour optimiser la fourniture de services et la réduction des coûts, accroît l'importance d'aborder les risques en matière de sécurité à l'égard de ces partenaires tiers et de leurs sous-traitants. Les partenaires tiers désignent notamment les intégrateurs, les prestataires de services (p.ex. : pour la maintenance des composants réseau), l'infogérance (« managed services ») ou encore les fournisseurs de matériel et de logiciels.

La sécurité de la chaîne d'approvisionnement consiste en la sécurisation des actifs et des services tout au long du cycle de vie d'un système (conception, développement, élaboration, conditionnement, assemblage, distribution, intégration au système, gestion opérationnelle, entretien et mise hors service).

Selon le type de prestataire de services, la chaîne d'approvisionnement et le recours à des partenaires tiers par le prestataire de services lui-même sont plus ou moins complexes et opaques. Tant l'opérateur de services essentiels que les prestataires de services proprement dits se doivent de faire preuve de professionnalisme dans leur gestion de la chaîne d'approvisionnement et des risques connexes et veiller à l'implémentation de mesures de réduction des risques identifiés.

Étant donné que ces mesures entraînent des coûts tant pour l'opérateur de services essentiels que pour les partenaires tiers, ces mesures doivent reposer sur une évaluation des risques étayée et ce, tant pour le fournisseur de services que pour le partenaire tiers.

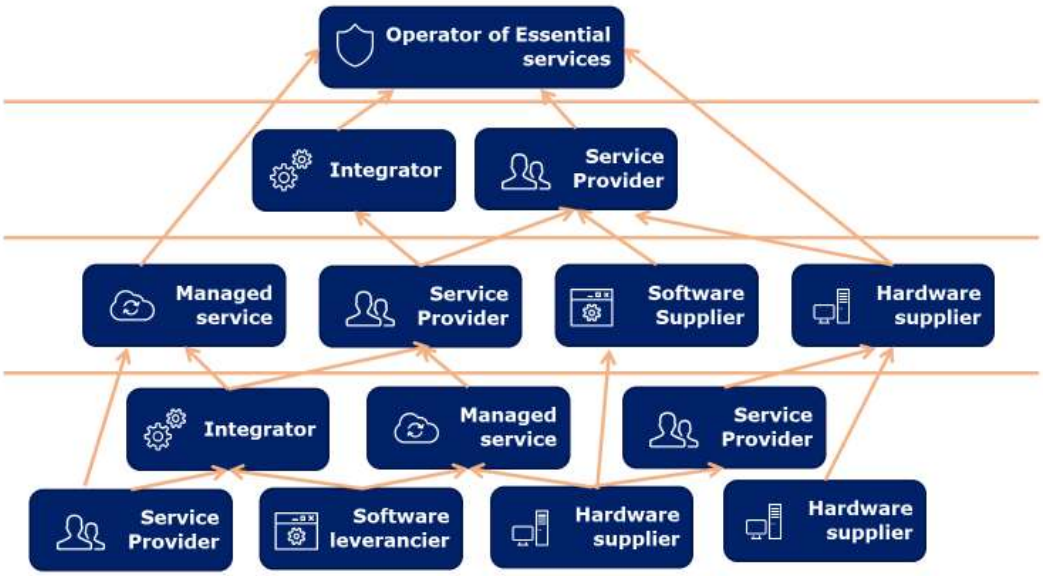

FIGURE 1 - COMPLEXITÉ DE LA CHAÎNE D'APPROVISIONNEMENT POUR LES OPÉRATEURS DE SERVICES ESSENTIELS

1.4 Structure du document

Le présent document s'articule autour des différents domaines de contrôle du processus de la chaîne d'approvisionnement. Chaque domaine de contrôle est assorti d'objectifs de contrôle généraux, liés à la sécurité des informations dans le domaine en question. Un ou plusieurs sous-domaines décrivant des objectifs de contrôle plus spécifiques peuvent compléter un domaine de contrôle. Pour satisfaire objectivement à un contrôle, il est possible d'implémenter une ou plusieurs mesures. Si ce document n'a pas pour objet de proposer une liste exhaustive de mesures, il fait cependant référence aux normes internationales en vigueur, lorsque c'est possible.

Dans ce document, le cycle de vie d'un service ou d'un actif est divisé en cinq domaines et la «gestion des risques» est considérée comme le sixième domaine central.

Les différents chapitres reprennent les différentes étapes du cycle de vie d'un actif ou d'un service.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

1.5 Documents connexes

Ce document s'inspire notamment de la norme ISO 28000 « systèmes de management de la sûreté de la chaîne d'approvisionnement », qui a pour objet le contrôle de la sécurité de la chaîne d'approvisionnement. La portée de ce document se limite cependant à la sécurisation des informations des actifs relatifs aux composants et services réseau. Les normes de la famille ISO 27000 ou les « Baseline Information Security Guidelines » (BSG) du CCB proposent des objectifs de contrôles plus généraux ou des mesures plus spécifiques.

Le texte a été rédigé sur base des documents suivants :

- ISO/IEC 27000 – 27001 – 27002 – 27005
- ISO/IEC 27017 Cloud Security
- ISO/IEC 27036 Information security for supplier relationships
- ISO/IEC 28000
- NIST SP 800 161
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation
- ISO/IEC 20243:2015 Open Trusted Technology Provider Standard
- NIST Cybersecurity Framework Version 1.1 (2018)
- Baseline Information Security Guidelines (CCB édition 2019)

1.6 Termes et définitions

Terme	Définition
OSE	Opérateur de services essentiels Selon la définition de la loi « établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique », article 6, § 11 (date de publication 3/5/2019, NUMAC 2019011507)
CERT	Cyber Emergency Response Team. Voir CSIRT
Triade CIA	CIA signifie « Confidentiality, Integrity & Availability ». Dans ce document, nous faisons référence à sa traduction française : confidentialité, intégrité et disponibilité.
Contrôle	Mesure qui agit sur le risque auquel il est associé (conforme à la norme ISO).
Domaine de contrôle	Un domaine de contrôle décrit un sujet pour lequel des objectifs de contrôle ont été identifiées.
Objectif de contrôle	Un objectif de contrôle décrit un objectif spécifique à la lumière duquel l'efficacité des mesures à implémenter peut être évaluée (conformément à la norme ISO).
CSIRT	Computer Security Incident Response team. Voir CERT
RGPD	Il s'agit du Règlement général sur la protection des données ou « General Data Protection Regulation » (GDPR) en anglais. C'est un règlement qui vise à uniformiser les règles relatives au traitement des données à caractère personnel.
Fournisseur non UE	Ce terme désigne aussi les services fournis dans un pays hors de l'UE.
KPI	KPI est le diminutif de « Key Performance Indicator » Il s'agit d'une mesure d'évaluation des prestations fournies.
Directive NIS	Renvoie à la directive européenne 2016/1148 concernant des mesures destinées à assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information au sein de l'Union. Cette directive a été transposée dans la législation belge le 7 avril 2019.
RTO	RTO signifie « Recovery Time Objective » Il s'agit du temps maximum nécessaire pour revenir à une prestation de services normale après un incident.
SLA	SLA signifie « Service Level Agreement » Il s'agit de la détermination de la prestation de services et de la qualité minimale que le client peut en attendre.
Chaîne d'approvisionnement	La chaîne d'approvisionnement des services et des actifs.

Les termes non définis dans le tableau ci-dessus respectent les définitions des normes usuelles (voir ISO 27000 et NIST).

2 Gestion des risques (Risk management)

Identification et analyse des risques au sein de l'organisation en ce qui concerne la chaîne d'approvisionnement des actifs et des services de réseau.

2.1 Détermination du contexte

2.1.1 Registre des actifs et des services (asset and service inventory)

Objectif: Élaborer et tenir à jour un aperçu de tous les actifs et services de réseau et de leur niveau critique.

Ligne Conductrice: les OSE élaborent un processus permettant de conserver dans un registre l'inventaire des actifs et des services. Cet inventaire constitue une vue d'ensemble centrale et globale. Cette vue d'ensemble permet également de tenir à jour des caractéristiques telles que la propriété («ownership»).

2.1.2 Évaluation de la dépendance à l'égard d'autres fournisseurs de services

Objectif: Évaluer le service en fonction de la dépendance à d'autres fournisseurs de services.

Ligne Conductrice : les opérateurs de services essentiels doivent évaluer dans quelle mesure leur prestation de services est tributaire d'autres services vitaux (comme la fourniture d'électricité), l'impact de cette dépendance en cas de panne ou de perturbation, ainsi que la manière dont des mesures (préventives) pourraient minimiser cet impact.

2.1.3 Scénarios et représentation de la menace

Objectif: Déterminer, évaluer et suivre les menaces associées aux actifs et services de réseau.

Ligne Conductrice : l'évolution de l'image de la menace pesant sur la sécurité informatique fera l'objet d'un suivi et donnera lieu à des communications périodiques ainsi que des recommandations (bulletins de sécurité des fournisseurs ou des CERT nationaux). En cas de modification de la menace, telle que l'apparition de nouveaux scénarios par exemple, il peut s'avérer nécessaire de procéder à une réévaluation des risques.

2.2 Analyse des risques (Risk analysis)

2.2.1 Analyse des risques de la chaîne d'approvisionnement

Objectif : Identifier et analyser les risques liés à la sécurité de la chaîne d'approvisionnement dans le cadre de la gestion plus large des risques au sein de l'organisation.

Ligne Conductrice : les OSE mettent au point une méthode d'analyse des risques, en ce compris les échelles d'impact et de probabilité afférentes.

Il est défini ici quels actifs font partie de la prestation de services essentiels dans la chaîne d'approvisionnement, ainsi que les risques associés qu'il y a lieu d'examiner. Il est important d'intégrer l'évaluation des risques de la chaîne d'approvisionnement dans une gestion plus large des risques (Entreprise Risk Management).

La réalisation d'une grille d'évaluation d'impact tient au minimum du nombre d'utilisateurs touchés par la perturbation du service essentiel, la durée de l'incident et l'étendue de la zone géographique touchée par l'incident.

Sur la base d'une analyse des risques, les mesures à implémenter sont déterminées pour un actif ou un service. En cas d'actif ou service dont le risque est élevé, il s'agira de prendre des mesures plus strictes qu'en cas d'actif ou service dont le risque est faible.

2.3 Communication et surveillance des risques

2.3.1 Communication des risques

Objectif : Partage des informations sur les risques avec les parties prenantes concernées.

Ligne Conductrice : la communication des risques est indispensable si l'on entend assurer la veille sur l'évolution de la menace et déterminer les mesures à implémenter par les tiers concernés.

2.3.2 Surveillance des risques

Objectif : Suivi des risques existants au sein de l'organisation.

Ligne Conductrice : les risques au sein d'une organisation ne sont pas statiques. Les types de menaces évoluent en permanence, ce qui peut dès lors modifier les risques courus au sein de l'organisation ou, en créer de nouveaux. Une réévaluation périodique de la menace et des risques associés est indispensable pour assurer une surveillance de qualité. En outre, des adaptations au sein de l'organisation peuvent également entraîner une modification des risques encourus.

3 Gestion de la sécurité et architecture (Security management and architecture)

Gestion générale de la sécurisation des informations pour les actifs et services de réseau et architecture de sécurisation des actifs et services de réseau.

3.1 Gestion

3.1.1 Rôles et responsabilités

Objectif : Formaliser les principales responsabilités et la structure de gouvernance du sous-traitant et du donneur d'ordre en ce qui concerne la chaîne d'approvisionnement.

Ligne Conductrice : en cas de sous-traitance, il y a un certain nombre de responsabilités importantes à attribuer, tant au sein de l'organisation du sous-traitant que dans celle du donneur d'ordre.

Identifier les partenaires devant être impliqués dans le processus décisionnel, la personne qui prend la décision définitive et celle qui est responsable d'une action/d'un résultat, celle qu'il faut consulter ou informer, comme défini dans le modèle RACI (par exemple le service juridique, les RH, les finances, l'enterprise risk management, le service IT, le service marchés publics, le program management, etc.).

Allouer les ressources nécessaires à la mise en œuvre des processus et des mesures pertinents en matière de sécurisation des informations pour la chaîne d'approvisionnement.

3.1.2 Stratégie d'achat (Procurement strategy)

Objectif : Définir une stratégie d'achat soutenue par le management et qui couvre les exigences internes, opérationnelles, juridiques, architecturales et réglementaires.

Ligne Conductrice : l'OSE doit définir la stratégie d'achat entourant les services essentiels et la développer dans des modèles de contrat et des procédures d'achat.

Les organisations doivent inciter les partenaires tiers à implémenter des mesures de sécurisation des informations, à assurer la transparence des processus organisationnels, à utiliser leurs propres partenaires tiers et les pratiques concernant la sécurisation des informations, à instaurer un contrôle supplémentaire des collaborateurs et des tiers liés à des prestations de services essentiels.

3.1.3 Définition et suivi des KPI pour la sécurité de la chaîne d'approvisionnement

Objectif : Définir et assurer le suivi des KPI pour la sécurité de la chaîne d'approvisionnement.

Ligne Conductrice : L'OSE définit des KPI internes et externes pour assurer le suivi des exigences en termes de sécurité de la chaîne d'approvisionnement.

3.1.4 Traitement des risques (Risk Treatement)

Objectif : Traiter les risques liés à un actif ou un service de réseau.

Ligne Conductrice : L'analyse des risques permet de déterminer le niveau de rigueur requis des mesures à implémenter pour un actif ou un service.

3.1.5 Gestion des incidents (Incident management[1])

Objectif : Être prêt à traiter et à suivre les incidents.

Ligne Conductrice : La définition d'une procédure formelle de traitement des incidents contribue à l'efficacité de la réaction aux incidents. Cette procédure comprend a minima les phases suivantes : Préparation (Prepare) ; Détection et analyser (Detection and Analysis) ; Confinement, éradication et résolution (Contain, eradicate and recover); Activités post-incident (Post-incident activities).

Lorsqu'il s'agira de définir cette procédure, l'OSE devra également assigner aux parties internes ou externes les différents rôles et responsabilités lors du traitement des incidents. En outre, l'OSE devra définir par contrat avec ses partenaires tiers les moments où il souhaite que ses partenaires tiers l'informent d'incidents les concernant.

L'OSE intègrera aussi dans sa procédure de traitement des incidents l'obligation légale de signaler des incidents au CSIRT national, le centre de crise National et l'autorité sectorielle.

3.2 Architecture de sécurisation du réseau

3.2.1 Schéma de l'architecture du réseau

Objectif : Élaborer et tenir à jour un aperçu schématique de tous les actifs de réseau et services associés, et de leurs interconnexions.

Ligne Conductrice : L'OSE conserve un aperçu de la manière dont les différents actifs et services de réseau communiquent et interagissent entre eux.

[1] https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-FR.pdf

3.2.2 Mesures de sécurisation des informations du réseau

Objectif : Déterminer les mesures de sécurisation des informations du réseau sur la base d'une analyse des risques (en tenant au moins compte des différents flux d'informations et de la sensibilité des données).

Ligne Conductrice : Le schéma de l'architecture du réseau servira de base pour évaluer les risques et les mesures pertinentes à implémenter au niveau de la couche réseau. L'analyse des risques doit au moins inclure les différents flux d'informations, les vulnérabilités connues et la sensibilité des données.

3.3 Solutions Cloud

Les solutions de type « Cloud » comme Software as a Server (SaaS), Platform as a Service (PaaS) ou Infrastructure as a Service (IaaS)sont de plus en plus utilisées. Dans ces cas de figures, il y a lieu d'appliquer des objectifs de contrôle spécifiques.

3.3.1 Niveau critique du Cloud

Objectif : Cartographier les flux de données vers le fournisseur du service Cloud et le niveau critique des prestation de services que cela supporte.

Ligne Conductrice : L'OSE détermine l'impact potentiel d'un service Cloud sur l'ensemble de la chaîne d'approvisionnement et les prestations des services essentiels concernés. Ceci donne une indication des mesures de mitigation que doivent prendre le fournisseur de service Cloud et l'OSE. Les risques liés aux solutions Cloud devront être gérés et mitigés différemment des risques classiques que l'organisation contrôle.

3.3.2 Mesures de sécurisation des informations dans le Cloud

Objectif : Définir les mesures nécessaires pour stocker des données dans le Cloud de manière à assurer une protection adéquate et en tenant compte d'éventuelles autres directives et législations.

Ligne Conductrice : Le stockage de données dans le Cloud doit respecter les mêmes contrôles d'accès que les données stockées localement. En outre, il convient de vérifier si la localisation géographique des données et les sauvegardes éventuelles sont conformes à ce que d'autres directives ou législations (par exemple le RGPD) autorisent.

3.3.3 Souveraineté des données en cas de prestation de services par un fournisseur hors UE

Objectif : Protéger la souveraineté des données vis-à-vis de fournisseurs hors UE

Ligne Conductrice : L'utilisation de services IT, y compris les services Cloud, par des fournisseurs hors UE présente des risques pour la souveraineté des données. Cela signifie que toutes les données stockées, traitées ou envoyées par le service sont soumises aux lois et réglementations des pays dans lesquels les données sont stockées, traitées et transmises.

De même, un fournisseur hors UE qui exploite un service en Belgique peut être soumis aux lois du pays où est établi son siège social. Par exemple, un prestataire de services peut être contraint par une instance de sécurité d'un pays hors UE à fournir des données de ses clients, sans en informer le client. Il est donc important qu'un OSE identifie les règles juridiques applicables à ses données stockées, traitées ou transmises.

L'OSE doit par ailleurs comprendre comment les lois en vigueur dans ces pays peuvent influencer la confidentialité, l'intégrité, la disponibilité et le caractère privé des informations. Lorsqu'un prestataire de services sous-traite à un partenaire tiers un pan de la fourniture du service, l'OSE doit également déterminer si cette sous-traitance comporte des risques supplémentaires de souveraineté des données.

4 Achat (Procurement)

Gestion des relations du fournisseur et achat d'actifs et de services de réseau jusqu'à la fourniture et au stockage.

4.1 Gestion des relations (Relationship Management)

La gestion des relations avec les fournisseurs démarre premier contact et se maintient jusqu'à la résiliation.

4.1.1 Échange d'informations

Objectif : Échanger en toute connaissance de cause des informations avec des fournisseurs (potentiels) durant le processus d'achat.

Ligne Conductrice : Pendant le processus d'achat, l'organisation et les fournisseurs (potentiels) échangeront des informations.

Cet échange d'informations débute lors de l'établissement d'un cahier des charges ou d'une « Request for Proposal » (RFP). Au cours de cet échange, il conviendra de préciser quelles informations seront partagées. Si nécessaire, une solution serait de conclure un accord contraignant concernant le partage d'informations avec le fournisseur (potentiel) et ce, afin de protéger par contractuellement les informations partagées. Cela comprend, entre autre, le partage d'informations avec des sous-traitants ou des partenaires tiers de fournisseurs (potentiels), ou également la durée autorisée de conservation des informations.

4.1.2 Nécessité contractuelle de mesures de sécurisation des informations des fournisseurs

Objectif : Collecter, analyser et signaler les mesures de sécurisation des informations liées à l'achat d'actifs ou de services dans le but de démontrer la maturité du dispositif de sécurisation des informations dans la relation avec le fournisseur, avant de démarrer une nouvelle relation et à répéter à intervalles réguliers pour les relations déjà existantes.

Ligne Conductrice : Lors de la sélection d'un fournisseur pour un actif ou un service, il est possible d'imposer un certain niveau de maturité de la sécurisation des informations. Un tel statut devrait également encadrer les relations existantes. Pour ce faire, il existe une solution dite active (via l'audit) ou passive (via rapports). En cas de changement des besoins en sécurité, il conviendra éventuellement de réviser les mesures de sécurisation des informations en collaboration avec le partenaire tiers.

4.1.3 Maturité de la sécurisation du fournisseur (Suppliers Security maturity)

Objectif : Choisir des fournisseurs ayant un niveau de maturité adéquat en matière de sécurisation des informations et en assurer régulièrement le suivi.

Ligne Conductrice : Le choix du fournisseur sera arrêté à la lumière de différents paramètres. L'un de ces paramètres est le niveau souhaité de sécurisation des informations. L'OSE peut également déterminer lui-même le niveau de maturité de la sécurisation des informations au moyen d'un audit ou d'une analyse de maturité.

4.1.4 Respect des réglementations européenne et nationale par les fournisseurs

Objectif : Choisir les fournisseurs qui respectent les réglementations européenne et nationale.

Ligne Conductrice : Le fournisseur doit être évalué et il conviendra d'évaluer s'il est dans l'obligation de se soumettre à une réglementation qui serait contraire à la réglementation européenne ou belge.

4.1.5 Cartographie de tous les partenaires et parties impliqués dans la prestation de services des fournisseurs.

Objectif : Identifier tous les partenaires et parties (stratégiques), tels que les sous-traitants, leurs prestations de services et leur relation avec les services essentiels.

Ligne Conductrice : L'OSE présente ses partenaires et parties (stratégiques) ainsi que les services qu'ils fournissent et leur relation avec la prestation de services essentiels de l'OSE. Cet inventaire permettra de présenter une vue d'ensemble des risques.

4.1.6 L'OSE tient compte des informations relatives à la menace

Objectif : Intégrer les informations relatives à la menace pesant sur les fournisseurs hors UE dans le processus d'analyse des risques de l'OSE.

Ligne Conductrice : Dans le cadre des informations relatives à la menace qui sont nécessaires à leur analyse des risques, les OSE ont accès à la plateforme centrale de renseignement sur les menaces (CTI/EWS). Les services de renseignement compétents partagent leurs analyses de menaces relatives à certains risques techniques et géopolitiques par l'intermédiaire de cette plateforme CTI. Le CCB coordonne les analyses spécifiques, en concertation avec les services de sécurité et de renseignement compétents.

4.2 Envoi, livraison et stockage

Lors des activités d'envoi, de livraison et de stockage, les actifs peuvent être exposés à des menaces externes. Les téléchargements ou les dossiers numériques peuvent aussi être compromis lors de leur transmission sur le réseau ou lors de leur stockage.

4.2.1 Protéger l'intégrité, la confidentialité et la disponibilité d'un actif

Objectif : Protéger les actifs contre les modifications malveillantes pendant l'envoi, la livraison et le stockage.

Ligne Conductrice : Les actifs seront contrôlés afin de détecter toute anomalie pendant l'envoi, la livraison ou le stockage. Une possibilité serait d'exiger des plis scellés lors du transport et du stockage. Il sera par ailleurs nécessaire de procéder au contrôle des actifs numériques envoyés, livrés et stockés. L'intégrité des téléchargements numériques et des fichiers enregistrés devra également être validée, si nécessaire, avant leur utilisation.

4.3 Déclaration d'auto-évaluation pour les fournisseurs de services ou de systèmes de sécurisation IT

Objectif : Faire respecter les directives qui entourent le processus de chaîne d'approvisionnement par les sous-traitants ou les partenaires tiers de l'OSE.

Pour la fourniture ou l'achat de services ou systèmes de sécurisation IT, le fournisseur transmettra une déclaration d'auto-évaluation dans laquelle il affirmera respecter les différents objectifs de contrôle de la présente directive.

L'annexe 1 du présent document donne un exemple de déclaration d'auto-évaluation.

5 Gestion opérationnelle (Operational Management)

La gestion opérationnelle comprend les tâches récurrentes de gestion et d'entretien effectuées par un tiers ou via des services achetés auprès d'un prestataire de services.

5.1 Mesures générales de sécurisation

5.1.1 Sensibilisation

Objectif : Sensibilisation des collaborateurs concernant le partage d'informations de l'entreprise avec des tiers et, aux éventuels risques pour la chaîne d'approvisionnement.

Ligne Conductrice : Les informations peuvent être partagées avec des tiers sur une base « besoin de savoir » (need-to-know).

5.1.2 Procédures opérationnelles

Objectif : Élaborer et gérer les « Security Operating Procedures » liées aux actifs et services de réseau.

Ligne Conductrice : L'organisation élaborera et assurera le suivi d'un ensemble de « Security Operating Procedures » afin de maintenir à un niveau acceptable les risques résiduels liés à la sécurisation des informations.

5.1.3 Contrats

Objectif : Protéger les informations des entreprises contre le vol et les abus perpétrés par des personnes externes.

Ligne Conductrice : L'élaboration d'accords contraignants entre toutes les parties concernées pour protéger les informations de manière adéquate (voir risk assessment) et l'assurance d'une CIA, sera intégré dans les contrats conclus avec des tiers et ce, afin de garantir une protection juridique contre le vol et l'utilisation abusive d'informations commerciales.

5.1.4 Accès aux actifs de réseau

Objectif : Prévenir et surveiller l'accès non autorisé aux actifs de réseau.

Ligne Conductrice : Les collaborateurs, internes et externes, ont besoin d'un cycle de vie « Identity en Access Management (IAM) » clair. Les accès aux actifs de réseau ne peuvent leur être octroyés que si c'est nécessaire à l'exécution de leur fonction. Cet accès devrait dès lors leur être retiré une fois qu'il n'est plus nécessaire.

5.1.5 Connexion et surveillance

Objectif : L'enregistrement des accès et la surveillance des actifs et services de réseau pour la détection des incidents liés à la sécurité de l'information.

Ligne Conductrice : Les différents actifs du réseau doivent être sécurisés par un dispositif d'identification et de surveillance afin de détecter les incidents de sécurité de l'information (pour identifier les accès non autorisés, par exemple).

5.1.6 Cryptage des informations

Objectif : Veiller à une utilisation correcte et efficace de la cryptographie afin de protéger la confidentialité, l'intégrité et la disponibilité (CIA) des informations.

Ligne Conductrice : Utiliser le cryptage end-to-end et en tunnels pour la communication effectuée à partir d'appareils qui ne sont pas gérés par l'organisation ou dont la sécurité ne peut être suffisamment garantie.

5.1.7 Échange d'informations

Objectif : Maintenir la sécurité des informations échangées au sein d'une organisation et avec un partenaire tiers.

Ligne Conductrice : Élaborer des règles et mesures claires concernant les e-mails échangés avec des partenaires tiers ainsi que le partage de documents.

5.1.8 Dépendance au fournisseur

Objectif : Limiter la dépendance à l'égard d'un seul fournisseur.

Ligne Conductrice : L'OSE doit veiller à ne pas dépendre d'un seul fournisseur ou fabricant pour des actifs ou services de réseau.

Une solution serait par exemple d'héberger le code source des applications développées par le sous-traitant auprès d'un tier de confiance (« Escrow »), ou de louer les services d'un deuxième centre de données auprès d'un autre fournisseur, etc.

L'architecture du réseau et du Cloud doit suffisamment tenir compte du niveau de dépendance d'un fournisseur ou d'un fabricant. Une architecture modulaire dont les composantes sont fournies par plusieurs fournisseurs et/ou fabricants réduira la dépendance de l'organisation vis-à-vis d'un partenaire tiers.

5.2 Consultants/Externes

Dans le cadre du présent document, tous les collaborateurs externes, de longue et de courte durée, sont considérés comme consultants. Voir les mesures supplémentaires visées au point 5.1.

5.2.1 Accès physique

Objectif : Empêcher l'accès physique non autorisé aux informations et aux installations de traitement des informations de l'organisation, de sorte de prévenir les dommages et l'interférence avec celles-ci.

Ligne Conductrice : Un collaborateur extérieur ne peut accéder qu'aux locaux et bâtiments nécessaires à l'exercice de sa fonction. Cet accès peut être prévu sur une base autonome ou sous surveillance.

5.3 Partenaire tier en charge de gestion

Un partenaire tiers peut gérer différents pans de l'organisation. À titre d'exemple, on peut citer la gestion du réseau, du serveur ou du centre de données. Voir les mesures supplémentaires visées au point 5.1.

5.3.1 Accès limité dans le temps

Objectif : Limitation de l'accès aux systèmes et applications dans des intervalles de temps précis.

Ligne Conductrice : L'accès d'un gestionnaire tiers sera limité dans le temps. L'accès peut être octroyé pour une fenêtre temporelle (p. ex. les heures de bureau) ou sur la base d'une demande (p. ex. un ticket support).

5.4 Fournisseurs de services d'infogérance (Managed service providers)

Un service externalisé. En sus des mesures visées au point 5.1.

5.4.1 Echange d'informations

Objectif : Maintenir la sécurité des informations échangées au sein d'une organisation et avec une entité externe.

Ligne Conductrice : Lors de l'achat d'un service d'infogérance ayant accès au réseau central de l'organisation ou pouvant le contrôler, il y a lieu de veiller à partager les informations avec une protection adéquate.

5.4.2 L'OSE tient compte des informations relatives à la menace

Objectif : Intégrer les informations relatives à la menace liées aux fournisseurs hors UE dans le processus d'analyse des risques de l'OSE.

La même règle s'applique ici que celle prévue pour la section Achat (4.1.6)

6 Restauration après un incident et changements majeurs (Recovery & Major Changes)

Interventions exceptionnelles sur des actifs et services de réseau, modification de la prestation de services et remplacement d'actifs de réseau qui ne relèvent pas de la gestion opérationnelle courante.

6.1 Généralités

6.1.1 Protection de l'accès pour des interventions exceptionnelles

Objectif : Fournir une autorisation temporaire d'accès aux actifs et services de réseau dans le cadre d'interventions exceptionnelles.

Ligne Conductrice : Les équipes de support externes doivent avoir la possibilité d'accéder temporairement aux actifs ou aux services de réseau qui leurs sont nécessaires.

6.1.2 Plans d'urgence

Objectif : Prévoir des plans d'urgence élaborés afin restaurer les actifs et les services critiques.

Ligne Conductrice : Implémenter des plans d'urgence qui intègrent les aspects de la chaîne d'approvisionnement afin de garantir son intégrité et sa fiabilité pendant les incidents (p. ex. en cas de cyberattaque ou de grève).

6.1.3 Accès sécurisés

Objectif : Prévoir des canaux de communication sécurisés pour les équipes de support à distance.

Ligne Conductrice : Pendant les restaurations et les changement majeurs, il est possible d'accorder l'accès à distance à certaines parties de l'infrastructure réseau de base. Il existe différentes solutions pour installer l'accès à distance, comme des services de type RDP ou SSH.

L'octroi d'un accès à distance aux équipes de soutien externes sera assuré via des canaux de communication sécurisés (par exemple, protégés par VPN et la nécessité d'authentification à plusieurs facteurs).

6.1.4 Zones sécurisées

Objectif : Empêcher l'accès physique non autorisé aux informations et aux installations de traitement des informations propriétaire de l'organisation, ainsi que de prévenir les dommages et l'interférence avec celles-ci.

Ligne Conductrice : Lors de restaurations ou de changements majeures, il peut être nécessaire d'accéder à certains locaux ou installations pour réparer ou remplacer des composantes du réseau.

Il convient d'éviter d'octroyer un accès trop important ou inopiné. Comment octroyer l'accès physique ? A la demande, ad hoc, en cas d'urgence ? Un accompagnement est-il nécessaire ?

6.2 Renvoi

Il peut arriver qu'il faille renvoyer les actifs au fournisseur pour réparation, également appelé Renvoi avec autorisation (RAA).

6.2.1 Renvoi en toute sécurité

Objectif : Protéger les données de l'entreprise que contiennent les actifs renvoyés au fournisseur ou au fabricant.

Ligne Conductrice : En cas de renvoi, il conviendra de surveiller les parties (service de coursier, poste, etc.) qui ont accès à ces actifs et sur les informations qu'ils contiennent.

7 Mise hors service sécurisée (Secure disposal)

Mise hors service d'appareils et clôture ou transition de services.

7.1 Supports de données

7.1.1 Prévention des fuites d'informations

Objectif : Protéger les données contre la perte lors de la mise hors service d'actifs de réseau.

Ligne Conductrice : Lors de la mise hors service d'appareils, on peut se renseigner pour savoir si ces appareils peuvent être réutilisés ou s'ils doivent être détruits. Une analyse de risques peut venir appuyer une telle décision. Lorsqu'un appareil peut être réutilisé, qu'il soit vendu ou réutilisé au sein de l'organisation, la première chose à faire est de supprimer correctement toutes les données de l'appareil.

7.2 Plan de transition services

7.2.1 Gestion des données auprès des fournisseurs en cas de cessation

Objectif : Protéger les informations de l'entreprise partagées avec un fournisseur en cas de cessation d'un contrat de services.

Ligne Conductrice : Lorsqu'un service touche à sa fin, tous les transferts de données en provenance/à destination d'un fournisseur seront clôturés. Le fournisseur devra supprimer les informations de l'entreprise qui sont en sa possession et, le cas échéant, les restituera à l'OSE.

En cas de transfert d'un service vers un autre fournisseur, les informations de l'entreprise nécessaires devront également être transférées du fournisseur initial vers le nouveau. Ce transfert sera assuré en toute sécurité.

Annexe 1 : Exemple de déclaration d'auto-évaluation de la chaîne d'approvisionnement

[Fournisseur]

Par la présente, je certifie en qualité de [Fournisseur] que la sécurité de la chaîne d'approvisionnement du produit [Produit] a fait l'objet d'une évaluation au regard des exigences fixées par [OSE].

Je confirme par cette déclaration de sécurité de la chaîne d'approvisionnement pour le produit [Produit] que les aspects suivants sont traités comme décrit par [OSE] :

- Gestion des risques
- Sécurisation et architecture
- Achat
- Gestion opérationnelle
- Restauration après un incident et grandes extensions
- Mise hors service sécurisée

Je suis en mesure de produire les preuves nécessaires, le cas échéant.

Fournisseur :

Signature

Date

Editeur responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépot légal
D/2020/14828/002

Lignes directrice « gestion sécuritaire de la chaine d'approvisionnement » - Supply Chain Proces – Décembre 2019

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 18 – Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be