Catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel

aux termes de l'article 109 de la loi sur les télécommunications (loi TKG)

Version 2.0

Éditeur:

Bundesnetzagentur

Agence fédérale des réseaux d'électricité, de gaz,

de télécommunications, des postes et des chemins de fer

Version: 29.4.2020

---

* Notifié conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

Table des matières

1 Nomenclature, destinataire, contenu et proportionnalité de mesures de protection

La dépendance croissante de l'économie et de la société à l'égard des télécommunications, notamment compte tenu de la transformation numérique étendue de tous les domaines de la vie quotidienne, impose des exigences élevées concernant la sécurité et la disponibilité des réseaux et services de télécommunications.

Dans ce contexte, l'article 109 de la loi sur les télécommunications (abrégée «TKG» en allemand et ci-après) définit certains objectifs de protection et certaines obligations de protection. L'article 109, paragraphe 1, de la loi TKG définit la protection des données à caractère personnel et la confidentialité des télécommunications comme des objectifs de protection généraux. Il incombe à chaque prestataire de services de poursuivre ces objectifs de protection généraux. Les objectifs de protection particuliers visés à l'article 109, paragraphe 2, de la loi TKG portent en revanche sur la protection de l'infrastructure des télécommunications contre les dysfonctionnements et contre les risques, ainsi que sur la disponibilité des services de télécommunications. La poursuite d'objectifs de protection particuliers se limite aux opérateurs de réseaux publics de télécommunications et aux prestataires de services de télécommunications accessibles au public.

Pour atteindre les objectifs de protection, toutes les entreprises doivent mettre en place des mesures préventives techniques, ainsi que d'autres mesures. La poursuite les objectifs de protection particuliers nécessite également la mise en place de mesures destinées à protéger les systèmes de télécommunications et de traitement de données contre tout accès illicite afin de réduire au minimum les effets des atteintes à la sécurité pour les utilisateurs ou pour les réseaux interconnectés. Pour mieux maîtriser les risques menaçant l'infrastructure de télécommunications et la disponibilité des services de télécommunications, l'article 109, paragraphe 4, de la loi TKG prévoit l'établissement d'un programme de sécurité et la désignation de personnes chargées de la sécurité.

Les exigences de l'État sont soumises au principe de proportionnalité. Les entreprises peuvent donc uniquement être tenues de prendre les précautions techniques et autres mesures appropriées, nécessaires et raisonnables. L'état de la technique doit être pris en compte dans la nécessité de toute précaution ou mesure (article 109, paragraphe 1, phrase 2, de la loi TKG; article 109, paragraphe 2, phrase 3, de la loi TKG). Une précaution ou une mesure est raisonnable si les moyens techniques et économiques nécessaires qui sont mis en œuvre à cet effet ne sont pas disproportionnés par rapport à l'importance des réseaux ou services de télécommunications à protéger (article 109, paragraphe 2, phrase 5, de la loi TKG).

En remplissant ses obligations légales imposées en matière de télécommunications, l'entreprise doit également respecter les exigences générales applicables de protection des données fixées par la loi fédérale sur la protection des données (abrégée «BDSG» en allemand et ci-après) et du règlement général sur la protection des données (RGPD). Si les obligations légales imposées en matière de télécommunications aux termes de l'article 109 de la loi TKG sont remplies par d'autres personnes ou organismes au nom d'un responsable, et s'il en est de même pour le traitement des données, la personne responsable aux termes de l'article 109 de la loi TKG doit veiller au respect de la réglementation applicable en matière de télécommunications. Cela n'affecte en rien la responsabilité directe de la personne mandatée ou de l'organisme mandaté en matière de protection des données d'après la législation générale sur la protection des données.

2 Fonction et contenu de base du catalogue des exigences de sécurité

Les opérateurs de réseaux publics de télécommunications et les prestataires de services de télécommunications accessibles au public doivent décrire les mesures de protection techniques et organisationnelles qu'ils ont prises dans un programme de sécurité comme le prévoit l'article 109, paragraphe 4, de la loi TKG. Ledit programme de sécurité et les précautions techniques et autres mesures à prendre reposent sur le «Catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel conforme à l'article 109 de la loi TKG » que l'Agence fédérale des réseaux a dressé d'un commun

accord avec l'Office fédéral de la sécurité informatique et le commissaire fédéral à la protection des données et à la liberté d'information.

Les exigences de sécurité fondamentales pour l'exploitation des systèmes de télécommunications et de traitement de données, ainsi que pour le traitement des données à caractère personnel sont décrites au chapitre 3. Toutes les entreprises doivent respecter lesdites exigences de sécurité. Le chapitre 4 est destiné à donner un aperçu des exigences légales qui s'y rapportent dans la loi TKG (articles 88 à 109). Les préconisations relatives à l'établissement d'un programme de sécurité sont fournies au chapitre 5. L'annexe 1 décrit les mesures techniques et organisationnelles appropriées pour répondre aux exigences des prestataires de services de télécommunications dotés d'une infrastructure IP. L'annexe 2 contient les exigences de sécurité supplémentaires. Les exigences de sécurité supplémentaires visent les opérateurs de réseaux de télécommunications dont la menace est accrue.

La responsabilité de la mise en œuvre en bonne et due forme des mesures de protection incombe toujours à la partie obligée. Elle doit s'assurer qu'aucun affaiblissement de la sécurité n'est à prévoir, même lorsque des tâches sont transférées à des tiers.

Conformément à l'article 109, paragraphe 7, de la loi TKG, l'Agence fédérale des réseaux peut soumettre les opérateurs de réseaux de télécommunications publics ou les prestataires de services de télécommunications accessibles au public à un contrôle qui sera réalisé par un organisme indépendant qualifié ou par une autorité nationale compétente. Un tel contrôle a pour but de déterminer si les exigences de l'article 109, paragraphes 1 à 3, de la loi TKG ont été respectées. Pour cette raison, le catalogue des exigences de sécurité peut également constituer la base de l'audit de sécurité d'un organisme indépendant qualifié aux termes de l'article 109, paragraphe 7, de la loi TKG.

Les fabricants, les associations d'opérateurs de réseaux publics de télécommunications et les associations de prestataires de services de télécommunications accessibles au public ont participé à la rédaction du catalogue.

3 Exigences de sécurité pour l’exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel

Un programme global sert de base et de point de départ à l’établissement de tout système de gestion de la sécurité solide. La gestion de la sécurité informatique, ou gestion SI en abrégé fait partie intégrante de la gestion générale des risques destinée à garantir la confidentialité, l’intégrité et la disponibilité des informations, des processus de gestion, des applications et des systèmes informatiques. Cependant, la sécurité informatique n’est pas seulement une question de technologie. Pour atteindre un niveau de sécurité adapté aux besoins pour l’ensemble des processus de gestion, des informations et des technologies, des conditions-cadres appropriées doivent également être établies dans une large mesure sur le plan de l’organisation et des ressources humaines.

Les exigences de sécurité listées ci-dessous reprennent ces aspects. Les exigences s’appliquent à toutes les entreprises assujetties et sont de nature générale. À cet égard, elles constituent la base de toutes les mesures de protection à mettre en œuvre. Les mesures de protection découlant des exigences de sécurité doivent en outre être dûment prises en compte dans le programme de sécurité à établir. Il relève avant tout de la responsabilité de l’entreprise assujettie d’apprécier l’adéquation de toute mesure de protection du programme de sécurité. Il s’agit d’un processus d’évaluation continu dans lequel les stratégies et les mesures sont constamment vérifiées et adaptées à l’évolution des besoins. L’Agence fédérale des réseaux vérifie régulièrement que les exigences du catalogue de sécurité sont respectées et que le programme de sécurité est mis en œuvre.

Les exigences de sécurité du catalogue présenté ne sont donc ni finales ni fixes dans le temps. Il est possible que des exigences supplémentaires soient requises dans des cas isolés en fonction de la criticité d’un réseau ou service particulier ou de l’évolution de la technologie.

3.1 Organisation

Si l'entreprise assujettie est un commerçant ou une société unipersonnelle, les responsabilités et les processus sont faciles à attribuer. Cependant, dans de nombreux cas, l'obligation fixée par l'article 109, paragraphes 1 à 3, de la loi TKG repose sur la division du travail ou de l'offre. La personne dirigeant toute entreprise assujettie reposant sur une division du travail doit donc veiller à ce que la structure et les processus définis soient clairement organisés. Cela comprend également la désignation du chargé de la sécurité conformément à l'article 109, paragraphe 4, de la loi TKG.

3.1.1 Gestion de l'organisation et des risques

Toute entreprise doit veiller à mettre en place un processus contraignant pour identifier les risques menaçant les réseaux, les services et le traitement des données à caractère personnel. Les principales menaces identifiées (risques pour la sécurité) pour les réseaux, les services et les données doivent être consignés et les risques résiduels reconnus doivent être vérifiés en tenant compte de la proportionnalité.

3.1.2 Rôles et responsabilités en matière de sécurité

La responsabilité du personnel doit être définie pour la sécurité des informations, des processus de gestion, des applications, des tâches et de la réglementation. Tous les employés doivent être informés de ces responsabilités de manière appropriée. Des précisions doivent être envoyées concernant le moment où les chargés de la sécurité doivent participer et la manière dont ils doivent le faire.

- Lors de l'attribution des fonctions respectives en matière de sécurité, un certificat de nomination peut apporter clarté et transparence, ainsi qu'être publié. À ce propos, les tâches et les pouvoirs attribués peuvent également être définis.
- La désignation seule ne suffit pas. Les personnes responsables des incidents survenant en matière de sécurité doivent être joignables dans le cadre de l'exercice de leur fonction. Sous ce rapport, l'établissement d'une règle de représentation constitue une condition sine qua non importante.
- Les connaissances en matière de sécurité finissent par devenir caduques. Le personnel désigné doit donc être régulièrement formé.

3.1.3 Gestion des fournisseurs

La fourniture de services de télécommunications peut souvent uniquement se faire qu'en ayant recours à des tiers. Dans ce contexte, les fournisseurs et les personnes travaillant à son service jouent un rôle important. C'est la raison pour laquelle l'entreprise assujettie doit évaluer la fiabilité et la qualité de la personne travaillant à son service ou du fournisseur. Il faut vérifier que les dépendances vis-à-vis de tiers n'entravent pas la sécurité des réseaux ou des services et la sécurité des données à caractère personnel. Sous ce rapport, il y a lieu d'observer ce qui suit:

- la fiabilité du tiers peut uniquement être appréciée sur la base d'informations appropriées. Il faut donc: se procurer des informations avant de mandater un tiers,
- les tiers doivent être liés contractuellement. Sur ce point, il faut s'assurer que les exigences de sécurité sont incluses aux conditions contractuelles convenues avec les fournisseurs (par exemple lors de l'achat de produits informatiques ou de l'utilisation de services informatiques). Un soin particulier doit être apporté à cet égard si des processus de gestion entiers (assistance informatique, centres d'appels, connexions réseau) sont externalisés,
- le tiers doit agir dans le respect de la loi sur la protection des données. Cela peut s'effectuer au moyen de dispositions contractuelles appropriées. Les dispositions de l'article 28 du RGPD doivent être respectées pour traiter les commandes,
- les exigences de sécurité doivent non seulement être définies et actualisées, mais leur conformité doit également être vérifiée autant que possible. Cela doit par principe être fait à chaque commande traitée. Les contrôles doivent être répétés périodiquement.

3.2 Sécurité dans la gestion du personnel

Les employés apportent une contribution essentielle au respect des objectifs de protection mentionnés au départ. Les mesures de protection complexes et des programmes de redondance technique apportent uniquement l'efficacité escomptée, même si les employés ne constituent pas une vulnérabilité dans l'entreprise et sont conscients de la responsabilité intrinsèque de leur activité en matière de sécurité. Le présent chapitre expose les exigences de sécurité imposées au service du personnel, à la direction et au personnel de l'entreprise. Cela comprend également le personnel mis à disposition en externe pour effectuer certaines tâches (par exemple par des fournisseurs ou fabricants).

Les exigences suivantes doivent être prises en compte avant l'embauche et après le départ de l'employé de l'entreprise.

3.2.1 Contrôle de sécurité

Il peut être nécessaire d'effectuer un contrôle de sécurité raisonnable en fonction de la tâche et de la responsabilité. En ce qui concerne les employés et les fournisseurs, il est jugé opportun de valider l'identité et les références professionnelles, en particulier pour les personnes ayant des tâches et des responsabilités en matière de sécurité (par exemple les administrateurs système, les chargés de la sécurité ou les personnes de la sécurité). La technique de contrôle utilisée doit être consignée.

L'entreprise doit demander aux employés de présenter leur carte d'identité afin d'établir clairement leur identité. Les copies authentifiées de certificats, de certificats personnels ou de tout certificat officiel de bonne vie et de bonnes mœurs peuvent constituer d'autres preuves pertinentes. Dans certaines circonstances, il peut être judicieux de se procurer des références supplémentaires auprès d'employeurs précédents.

3.2.2 Connaissance en matière de sécurité et sensibilisation

Le personnel doit disposer des connaissances de sécurité appropriées et pertinentes et prendre conscience de la manière dont les données sensibles doivent être gérées.

Il faut donc s'assurer que le personnel employé et mandaté a suivi une formation appropriée et pertinente et veiller à mettre à disposition des supports traitant des questions de sécurité. La participation du personnel à la formation doit faire l'objet d'un rapport.

Les connaissances finissent par devenir caduques. Des formations et des sessions de sensibilisation régulières doivent donc être organisées régulièrement pour le personnel employé et mandaté pour les questions de sécurité concernées (par exemple, la protection des données, la confidentialité des télécommunications).

Les contenus de formation doivent également être vérifiés régulièrement en tenant compte des évolutions et le cas échéant être actualisés.

3.2.3 Changement de personnel

Tout changement de personnel s'accompagne de risques en matière de sécurité. Si les employés changent d'attribution ou quittent l'entreprise ou si de nouveaux employés sont intégrés, l'entreprise doit donc respecter certaines exigences de sécurité:

- les dispositions relatives à la gestion des changements de personnel ou des changements de compétences et de responsabilités doivent être respectées,

- après tout changement de personnel ou de mandataire, les droits d'accès aux systèmes, bâtiments ou installations concernés doivent être immédiatement adaptés ou suspendus. Les mots de passe délivrés doivent être gérés conformément à l'état de la technique,
- le nouveau personnel doit être informé et sensibilisé aux directives et procédures applicables.

3.2.4 Gestion des infractions

Il faut fixer des règles contraignantes sur la manière de gérer les atteintes à la sécurité à la suite d'infractions commises par ses propres employés.

3.3 Sécurité des données, des systèmes et des installations

Le présent chapitre traite de la sécurité matérielle et logique des données, des systèmes en réseau et des systèmes informatiques destinés à protéger les valeurs fondamentales (confidentialité, disponibilité et intégrité).

3.3.1 Gestion sécurisée des données et informations sensibles

Dans le domaine des télécommunications, il faut assurer la protection des données conservées à long terme et notamment des données hautement sensibles comme les données relatives à la fréquentation, au contrôle ou au contenu. Elles relèvent de la protection des données et de la protection de la confidentialité des télécommunications. Des dispositions doivent donc être prises afin que ces données et informations soient gérées de manière sûre. Il faut plus particulièrement:

- conserver les dossiers ou documents sensibles sous clé. Les meubles-classeurs verrouillables et les bureaux fermés doivent être envisagés comme des mesures possibles,
- les terminaux mobiles ou supports de données portatifs doivent être protégés en usant des technologies de cryptage appropriées. Il faut avoir recours à un système de gestion des appareils mobiles (Mobile Device Management),
- il faut prendre des dispositions relatives à l'élimination sûre des supports de données mobiles qui ne sont plus nécessaires ou qui sont défectueux,
- les disques durs contenant des données sensibles doivent être éliminés de manière à ce que les données ne puissent plus être restaurées.

3.3.2 Exigences de sécurité matérielle et élémentaire

Il existe également un risque pour la sécurité lié au vandalisme, au vol, au feu, à l'eau, à la poussière ou aux catastrophes naturelles. Des mesures de protection matérielles appropriées doivent être prises pour écarter autant que possible les risques de sécurité de ce type et ainsi maintenir la disponibilité du réseau et du service. Cela implique de prendre au moins les mesures suivantes:

- définir des dispositifs de sécurité matériels pour empêcher tout accès non autorisé, toute détérioration et toute dégradation des informations et des installations de traitement informatique (par exemple au moyen de verrous de sécurité, de détecteurs de mouvement, de systèmes de détection d'intrusion ou de vidéosurveillance),
- protéger les zones de sécurité par un dispositif de contrôle d'accès adéquat,
- entretenir les appareils et le matériel d'exploitation à intervalles réguliers ou aux intervalles recommandés par le fabricant,
- protéger correctement le câblage servant aux télécommunications et le câblage électrique contre toute coupure, tout dysfonctionnement et tout dégât; poser les lignes redondantes séparément les unes des autres; poser les câbles sous terre et les protéger par des gaines et en utilisant des espaces et placards verrouillés;
- éviter les conduites d'eau dans les salles de serveurs,
- prendre des mesures de protection contre les catastrophes naturelles et contre les accidents,
- évaluer régulièrement l'efficacité des mesures de protection matérielles et environnementales,
- utiliser des détecteurs d'incendie, de gaz et de fumée ou des systèmes d'extinction adaptés à la taille des locaux et les entretenir régulièrement,
- vérifier régulièrement que le règlement de prévention des incendies est respecté.

3.3.3 Protection de l'approvisionnement (disponibilité de l'ensemble du système)

Dans le domaine des télécommunications accessibles au public, il est essentiel d'assurer la sécurité de l'approvisionnement (télécommunications, électricité, climatisation, etc.). Les mesures de protection suivantes doivent être prises:

- les appareils et le matériel d'exploitation doivent être protégés contre les coupures de courant et les autres perturbations,
- les lignes redondantes doivent passer par différentes gaines et différents parcours,
- la climatisation et l'alimentation électrique doivent être dimensionnées de façon à être suffisantes et ce dimensionnement doit être contrôlé régulièrement,

- les installations de distribution électrique, les groupes électrogènes de secours, les batteries, etc. doivent être vérifiés régulièrement et testés si cela est possible,
- une procédure de mise en œuvre doit être établie pour la sécurité des approvisionnements, des installations d'approvisionnement et des aménagements auxiliaires critiques,
- des mesures destinées à protéger la livraison et la mise à disposition des installations d'approvisionnement doivent être mises en œuvre.

3.3.4 Contrôle d'accès au sein des systèmes en réseau et des systèmes informatiques

Sans mécanismes appropriés permettant un contrôle d'accès, il est impossible d'empêcher l'utilisation non autorisée d'appareils de télécommunications et de systèmes de télécommunication. Les personnes non autorisées peuvent également accéder à des informations confidentielles, les manipuler ou provoquer des dysfonctionnements. Accorder les droits adéquats a pour but de contrôler l'accès aux informations.

Les mesures de protection possibles sont les suivantes:

- délivrer aux utilisateurs des identifiants clairs et les authentifier avant de pouvoir accéder aux services ou aux systèmes,
- permettre l'enregistrement des mots de passe uniquement sous forme cryptée,
- définir les fonctions, les droits, les responsabilités et les procédures d'attribution et de révocation des droits d'accès,
- établir un protocole d'accès aux systèmes en réseau et des systèmes informatiques, enregistrer les écarts de procédure et établir un protocole pour lesdits écarts,
- sécuriser suffisamment les accès de maintenance à distance (propres accès VPN),
- faire accompagner les personnes étrangères dans des zones sécurisées ou leur permettre uniquement l'accès auxdites zones sécurisées après un contrôle de sécurité approprié et une initiation adéquate, les personnes étrangères sont dans ce cas les personnes provenant de sociétés externes, par exemple pour des travaux de maintenance, la transformation de bâtiments ou des travaux de nettoyage,
- vérifier régulièrement les mécanismes de contrôle d'accès et les ajuster si nécessaire,
- vérifier que seules les personnes autorisées ont accès aux installations techniques sécurisées.

3.3.5 Intégrité et disponibilité des systèmes en réseau et des systèmes informatiques

L'intégrité et la disponibilité des systèmes en réseau, des systèmes informatiques et de la protection contre les virus, les injections de codes et les autres logiciels malveillants susceptibles de modifier la fonctionnalité des systèmes doivent être garanties:

- il faut veiller à ce que les logiciels des systèmes en réseau et des systèmes informatiques ne soient pas manipulés ou modifiés sans autorisation (par exemple par une modification non autorisée de la configuration). Les modifications apportées doivent être consignées. Tout accès non autorisé doit être détecté. Les systèmes et les applications doivent toujours être équipés des dernières mises à jour de sécurité,
- des mesures appropriées doivent être mises en œuvre pour détecter les logiciels malveillants,
- des mesures de sensibilisation des employés doivent être établies et mises en œuvre,
- il faut s'assurer que les données critiques pour la sécurité (comme les mots de passe, les clés secrètes partagées, les clés privées, etc.) ne sont ni divulguées ni manipulées,
- l'efficacité des mesures destinées à protéger l'intégrité des systèmes doit être vérifiée et évaluée,
- les mots de passe doivent être authentifiés en toute sécurité et modifiés si nécessaire,
- des formations doivent donner aux employés les outils nécessaires pour identifier les e-mails ou les liens suspects.

3.3.6 Confidentialité de la communication

Il faut garantir la confidentialité et l'intégrité du contenu des communications et des métadonnées:

- des méthodes de cryptage appropriées doivent être employées pour garantir la protection adéquate de la confidentialité du contenu des communications et des métadonnées,
- des mécanismes d'authentification appropriés doivent être utilisés pour les réseaux de clients et de services,
- il faut examiner l'utilisation des réseaux et des services en continu et de manière appropriée afin de détecter les anomalies,
- des modes et moyens de transmission normalisés doivent être utilisés,

- les données du client critiques pour la sécurité doivent être particulièrement protégées (par exemple les données des cartes SIM, les IMEI, les mots de passe),
- l'efficacité des méthodes de protection de la confidentialité du contenu des communications et des métadonnées doit également être évaluée en continu et de manière appropriée. Les données de localisation comme les identifications de cellule font également partie des métadonnées et sont soumises à des exigences supplémentaires (voir paragraphe 4.2.4). Une évaluation appropriée peut consister à effectuer une contre-vérification ou un test (de résistance).

3.4 Gestion d'exploitation

La direction responsable de l'entreprise doit garantir son exploitation conforme et sûre. Les exigences de sécurité exposées ci-après portent sur la procédure d'exploitation opérationnelle, la gestion du changement et la gestion des valeurs de l'entreprise.

3.4.1 Procédures d'exploitation

Des procédures d'exploitation appropriées doivent être instaurées pour garantir le fonctionnement continu, sûr et en due forme des technologies de l'information et de la communication de l'entreprise assujettie concernée.

- Pour le garantir, il faut au moins définir la manière de procéder et la consigner. De plus, la responsabilité de l'exploitation des systèmes critiques doit être attribuée à un organe responsable.
- Les moyens disponibles et nécessaires doivent être connus. On entend par «moyens» entre autres le personnel, les systèmes, les applications et les locaux nécessaires et effectifs.
- Il faut constamment vérifier les moyens disponibles et nécessaires et le cas échéant les contrôler de manière appropriée.

3.4.2 Gestion du changement

Les changements peuvent présenter des risques pour la sécurité. Croissantes et en constante évolution, les exigences des utilisateurs accordent en outre de moins en moins de temps à toute entreprise assujettie d'un changement à l'autre, y compris pour ajuster les configurations de systèmes. À cet égard, les entreprises peuvent être confrontées à la tâche d'actualiser les éléments constitutifs des télécommunications rapidement et de façon adaptée aux besoins, mais aussi en toute sécurité. Les pratiques en matière de sécurité montrent que les risques ou les dysfonctionnements opérationnels sont souvent dus à une gestion incorrecte, précipitée ou

inexistante du changement. Pour éviter les dysfonctionnements ou les incidents de sécurité, les modifications apportées aux systèmes en réseau et aux systèmes informatiques, à l'infrastructure, à la documentation, aux processus, aux procédures et aux modes opérationnels doivent donc être planifiées, vérifiées, contrôlées et testées après mise en place.

- Les modifications apportées aux systèmes critiques doivent reposer sur des procédures prédéfinies et correctement consignées.
- Il faut évaluer toutes les répercussions potentielles directes et indirectes.
- Les modifications significatives effectives doivent être consignées de manière appropriée.
- Une fois les modifications apportées, il faut vérifier la fonctionnalité des systèmes de télécommunications de manière appropriée. Toutes les personnes concernées doivent être informées en détail des modifications nécessaires. Les anomalies identifiées doivent être signalées immédiatement à l'organe préalablement désigné.
- Il est recommandé de mettre en place des mesures de contrôle préventif, par exemple le principe des quatre yeux.

3.4.3 Gestion des actifs

La sécurité nécessite des connaissances. Il faut pouvoir identifier clairement au moins les installations, systèmes et équipements essentiels nécessaires au fonctionnement des différents réseaux ou à l'offre de services. Un inventaire et une gestion appropriés et individuels des installations et des systèmes peuvent le permettre. La gestion des actifs doit également comprendre le contrôle de la configuration des systèmes et réseaux de communication essentiels.

3.5 Interférences et incidents de sécurité

Il s'agit de détecter et de signaler la détection de dysfonctionnements et d'incidents de sécurité, ainsi que d'y répondre. Les incidents de sécurité peuvent être déclenchés par un seul évènement ou par un concours de circonstances différentes. Les incidents de sécurité peuvent compromettre la confidentialité, l'intégrité, la disponibilité ou l'authenticité des systèmes informatiques et des systèmes de télécommunication.

3.5.1 Identification des incidents de sécurité et des dysfonctionnements

Il faut établir une procédure d'identification des incidents de sécurité et des dysfonctionnements et la contrôler régulièrement.

À cet effet, il faut par exemple surveiller les paramètres d'exploitation prédéfinis comme la climatisation, l'électricité, le volume de données sur le réseau de télécommunications et donner l'alerte en cas d'incident de sécurité ou de dysfonctionnements.
Une fois que les dysfonctionnements et/ou les incidents sont connus, les systèmes concernés doivent être adaptés et/ou améliorés afin que ce problème soit évité à l'avenir.

3.5.2 Gestion des incidents de sécurité et des dysfonctionnements

Tout incident de sécurité peut avoir une origine singulière ou multiple. Tout type d'incident de sécurité peut compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes informatiques et des systèmes de télécommunication. Les entreprises assujetties doivent donc mettre en place une procédure permettant de définir et de gérer tout type d'incident de sécurité, et entre autres de les signaler aux personnes et autorités responsables. Il convient de vérifier régulièrement que la procédure fixée est adaptée aux circonstances actuelles et qu'elle est réellement mise en œuvre conformément à ce qui était prévu.

- Il faut désigner le personnel compétent devant être disponible pour les incidents de sécurité. En cas d'atteinte à la sécurité, il peut être nécessaire de gérer la sécurité ou de prendre des décisions en matière de sécurité dans l'urgence ou dans des circonstances atypiques. Le personnel doit donc non seulement être formé pour identifier les incidents de sécurité, mais aussi pour assurer leur gestion spécifique.
- La criticité de chaque dysfonctionnement ou atteinte à la sécurité doit être évaluée de manière appropriée. La méthode déclarative imposée pour le résultat de l'évaluation doit ensuite être appliquée.
- Les incidents de sécurité critiques doivent par principe faire l'objet d'une enquête. L'enquête et le résultat doivent faire l'objet d'un rapport. Le rapport doit indiquer les mesures prises ou prévues pour éviter des incidents de sécurité similaires et leurs effets à l'avenir ou pour limiter le risque pour la sécurité au minimum. Les mesures prises ou prévues à cet égard doivent être motivées. S'il s'agit d'atteintes graves de la sécurité aux termes de l'article 109, paragraphe 5, de la loi TKG, lesdites atteintes doivent être immédiatement signalées à l'Agence fédérale des réseaux et à l'Office fédéral de la sécurité informatique.

3.5.3 Communication et déclaration des incidents de sécurité

Des procédures déclaratives adéquates doivent être mises en place pour déclarer les incidents de sécurité afin de réduire les préjudices causés par les incidents de sécurité au minimum.

- Tout incident de sécurité peut déclencher une obligation légale de déclaration (par exemple aux termes de l'article 109a, paragraphe 5, de l'article 109a, paragraphe 1 de la loi TKG ou de l'article 33 du RGPD). Si cela est nécessaire, les incidents de sécurité actuels ou passés doivent être déclarés aux tiers, aux clients et/ou aux autorités.
- Des règles appropriées doivent être appliquées dans la manière de procéder de l'entreprise afin de garantir les éventuelles obligations déclaratives, ainsi que la communication et le signalement des incidents de sécurité.
- En cas d'atteinte de mots de passe, les clients concernés doivent être informés dans les plus brefs délais. Une procédure de notification appropriée doit être établie pour le garantir.

3.6 Gestion des urgences ou des coupures

Tout dysfonctionnement ou incident de sécurité peut entraîner une coupure du service ou de l'exploitation du réseau. Toute stratégie de prévention appropriée doit prendre en compte les évolutions de ce type et prévoir des programmes de défense appropriés en fonction de chaque cas. Dans ce contexte, il ne faut pas seulement réglementer les aspects techniques de la maintenance des services. Il faut également prévoir et définir des mesures organisationnelles en amont, ainsi que les contrôler en continu. Ce chapitre décrit les exigences relatives à la remise en état et au maintien des infrastructures opérationnelles.

3.6.1 Maintien des infrastructures de télécommunications et des services (gestion de la continuité des activités ou «business continuity management»)

Les règles de maintien des infrastructures et des services doivent contenir des instructions générales en matière de gestion et autant que possible des mesures d'urgence pratiques adaptées à chaque cas. Les coordonnées utiles doivent être décrites dans un manuel d'urgence et toujours à jour. Il faut garantir l'accès à ces règles et informations.

- La disponibilité de redondances adéquates au niveau du système et du service doit être garantie en amont.
- Lesdites redondances doivent être testées ou commutées à intervalles réguliers, dans la mesure du possible sans coupure.
- Il faut sauvegarder régulièrement les systèmes et les données critiques. Il faut en l'occurrence veiller à respecter les durées de suppression et de conservation imposées par la loi. La durée de conservation des sauvegardes doit plus particulièrement être

relativement proportionnelle à la durée de conservation des données à caractère personnel.

- Des plans d'urgence adaptés à l'exploitation des systèmes critiques doivent être élaborés, définis et mis en œuvre. Lesdits plans doivent être évalués régulièrement.
- Un responsable des urgences compétent doit être nommé. Ce dernier doit connaître et diriger toutes les activités de gestion des urgences.

3.6.2 Reprise d'activité après sinistre («disaster recovery management»)

Les temps d'arrêt jusqu'à ce que le réseau et les services de communication soient rétablis et à nouveau opérationnels doivent toutefois être maintenus aussi courts que possible en utilisant des moyens adéquats.

- Il faut établir et définir des politiques et procédures appropriées pour rétablir les services de réseau et de communication importants le plus rapidement possible. Lesdites politiques et procédures doivent être évaluées à intervalles réguliers.
- Les processus de gestion les plus importants pour la reprise d'activité doivent être classés par ordre de priorité.
- Il faut vérifier en amont que les contrats avec les fournisseurs prévoient un approvisionnement de substitution.
- Une mesure de protection appropriée peut consister en la fourniture d'appareils de remplacement appropriés pour l'infrastructure et les systèmes de télécommunication.
- La fourniture d'installations auxiliaires d'alimentation mobiles adaptées peut également constituer une mesure de protection appropriée dans des cas isolés.
- L'aménagement préventif de postes de travail d'urgence préventifs peut être utile pour les employés afin de maintenir les services.

3.7 Procédures de contrôle et de test

Des procédures de contrôle et de test doivent être introduites pour rendre les systèmes et les processus aussi sûrs que possible et pour les optimiser continuellement. Les exigences relatives à la surveillance et à la journalisation des systèmes en réseau et des systèmes de communication importants sont décrites ci-après.

3.7.1 Mesures de contrôle et de journalisation

Les évènements opérationnels et les évènements liés à la sécurité doivent être journalisés. Les données journalisées servent à évaluer et à contrôler certains évènements. Une journalisation détaillée et continue et aussi automatique que possible peut multiplier les possibilités d'évaluation. Dans le meilleur des cas, les données journalisées sur la base d'un examen médico-légal permettent une analyse de sécurité appropriée. Tous les évènements relatifs à la sécurité doivent donc être journalisés et enregistrés sous une forme évaluable. Si les données ne sont plus nécessaires à ces fins, elles doivent être immédiatement supprimées.

- Un ensemble adapté de règles de contrôle et de journalisation des systèmes opérationnels doit être introduit et mis en œuvre au cas par cas. Ces règles doivent être évaluées régulièrement.
- Dans des cas isolés, il est possible que le contrôle et la journalisation automatiques des systèmes opérationnels permettent d'obtenir des informations supplémentaires pertinentes pour l'évaluation.
- Les activités administratives ou les travaux réalisés sur les systèmes opérationnels doivent être consignés.

3.7.2 Exercices de simulation des situations d'urgence

Le chapitre 3.6 traitait des exigences de maintien et de reprise d'activité des infrastructures et des services après des situations d'urgence. Des exercices de simulation des situations d'urgence doivent être réalisés régulièrement afin que les plans d'urgence et les procédures puissent être mis en œuvre comme prévu dans des situations de stress. Une procédure de test et de mise en pratique des plans d'urgence destinés à permettre le maintien et la reprise d'activité des services et des infrastructures critiques doit être donc établie. Si cela est possible et nécessaire, cela doit également s'effectuer en collaboration avec des tiers.
Des scénarios aussi différents et réalistes que possible doivent être envisagés. L'objectif est de déterminer si les temps d'arrêt prévus ne sont pas dépassés et si l'équipe de gestion de crise en question accomplit ses tâches dans la pratique.

3.7.3 Test des systèmes en réseau et des systèmes informatiques

Les modifications ou les opérations de perfectionnement sur les systèmes en réseau ou les systèmes informatiques existants sont de possibles facteurs de risque. Il faut donc établir les règles d'autorisation et de test des systèmes en réseau et des systèmes informatiques en amont.

- Les systèmes en réseau ou les systèmes informatiques doivent être testés dans des environnements de test séparés avant d'être utilisés ou être connectés aux systèmes existants. Il en est de même pour les adaptations ou par exemple après les mises à jour.
- Les systèmes opérationnels doivent être soumis à des tests de sécurité réguliers. Cela est particulièrement vrai si de nouveaux systèmes sont introduits et si des modifications sont apportées.
- Il faut s'assurer que les tests n'ont aucun impact sur la sécurité des réseaux et des services. Il faut éviter toute utilisation de données sensibles.

3.8 Évaluation des mesures de protection

Toutes les mesures de protection doivent prendre en compte l'état de la technique. Cependant, la technologie évolue sans cesse. Parallèlement, la menace change également continuellement Dans ce contexte, les mesures de protection prises doivent être régulièrement réévaluées par l'entreprise assujettie. Une stratégie appropriée doit donc être élaborée pour évaluer les mesures de protection prises au cas par cas.

- Il faut au moins établir des règles d'évaluation pour les mesures de protection prises.
- Les analyses des risques régulières et les chiffres clés définis recueillis (par exemple, la durée des dysfonctionnements et les temps d'arrêt peuvent servir d'indicateur) peuvent être utilisés pour évaluer les mesures de protection.
- La réalisation de tests de résistance réguliers et réalistes peut éventuellement permettre d'identifier de nouveaux facteurs de risque.

3.9 Conformité aux exigences légales

Les dispositions légales, contractuelles ou facultatives doivent être respectées. Pour cela, un système de contrôle doit être intégré aux processus opérationnels et un organe responsable nommé. Tout comme la technologie ou les menaces, la loi subit également des évolutions constantes. Il faut donc examiner l'évolution de la loi de façon continue et appropriée et vérifier son application pour chaque cas. Le chapitre 4 ci-dessous donne un aperçu des dispositions légales qui s'y rapportent dans la loi TKG.

4 Exigences de sécurité légales issues de la réglementation spécifique au secteur

Les précautions techniques et autres mesures à prendre conformément à l'article 109, paragraphes 1 et 2, de la loi TKG visent la protection des données à caractère personnel, la confidentialité des télécommunications, la protection des infrastructures de télécommunications et la disponibilité des services. Ces biens protégés par des dispositions légales ne constituent pas l'objet exclusif de la loi TKG. À cet égard, dans certaines circonstances, l'entreprise assujettie doit également respecter d'autres dispositions européennes, constitutionnelles ou nationales.

Les explications fournies ci-après concernent exclusivement les exigences légales de la loi TKG spécifiques au secteur. Par exemple, les dispositions relatives à la protection de la confidentialité des télécommunications spécifiques au secteur se trouvent à l'article 88 et aux articles suivants de la loi TKG. L'article 91 et les articles suivants de la loi TKG s'appliquent à la protection des données à caractère personnel. L'article 100 et l'article 109, paragraphe 5, de la loi TKG ont pour objet la protection de l'infrastructure de télécommunications contre les dysfonctionnements et la disponibilité des services de télécommunications.

Les dispositions du droit européen, l'évolution constante de la situation en matière de sécurité et les évolutions techniques conduisent à modifier sans cesse la loi TKG. Pour se conformer à leurs obligations légales, les entreprises assujetties sont donc par principe tenues d'observer l'évolution de la législation et de la jurisprudence s'y rapportant et de vérifier leur application pour chaque cas. À cet égard, les préconisations formulées ci-après peuvent uniquement fournir un aperçu actuel des exigences spécifiques au secteur qui doivent être respectées.

4.1 Exigences de sécurité relatives à la protection de la confidentialité des télécommunications (article 88 de la loi TKG)

L'article 88 de la loi TKG représente la simple expression juridique de la protection de la confidentialité des télécommunications ancrée dans la Constitution de la République fédérale d'Allemagne en son article 10, paragraphe 1. La loi tient compte du fait qu'avec la libéralisation du marché des télécommunications, les services de télécommunications sont fournis par le secteur privé et ce dernier est souvent indirectement et donc uniquement relativement soumis aux principes constitutionnels. Dans ce contexte, il était nécessaire de compléter la protection prévue à l'article 10, paragraphe 1, de la Constitution de la République fédérale d'Allemagne par une réglementation purement juridique et de soumettre ainsi les prestataires privés et les autorités publiques directement liées à l'article 10, paragraphe 1, de la Constitution de la République fédérale d'Allemagne.

La confidentialité de l'utilisation du moyen technique servant à transmettre des messages est protégée par l'article 10 de la Constitution de la République fédérale d'Allemagne. Si les données des communications sont consultées, enregistrées, exploitées ou transmises par l'intermédiaire de l'État, cela constitue une atteinte dans les principes constitutionnels. Ladite réglementation possède un contenu similaire en raison de l'harmonie avec l'article 88 de la loi TKG. Contrairement à l'article 10 de la Constitution de la République fédérale d'Allemagne, la protection ne se déploie cependant pas vis-à-vis de l'État, mais vis-à-vis des prestataires de services.
Conformément à la jurisprudence constitutionnelle relative à l'article 10, paragraphe 1, de la Constitution de la République fédérale d'Allemagne, l'article 88, paragraphe 1, de la loi TKG couvre également les circonstances précises des télécommunications. Cela comprend toutes les informations sur l'heure et le lieu, ainsi que sur le mode de transmission immatériel dans la mesure où ils peuvent être à l'origine de risques pour la confidentialité du processus de transmission des informations.

En ce qui concerne le respect des exigences de sécurité destinées à protéger la confidentialité des télécommunications, il convient de souligner les points suivants:

- tout prestataire de services est tenu de préserver la confidentialité des télécommunications. L'obligation de confidentialité se poursuit même lorsque l'activité a pris fin,

- il faut éviter que les prestataires de services prennent connaissance ou permettent à d'autres de prendre connaissance du contenu ou des circonstances précises de la télécommunication au-delà de ce qui est nécessaire pour fournir à titre professionnel des services de télécommunication, qui comprennent la protection de leurs dispositifs techniques,
- il faut de même empêcher que des tiers non autorisés prennent connaissance du contenu ou des circonstances précises de la télécommunication,
- en l'occurrence, il faut prendre en compte les dispositifs techniques servant à la transmission directe et indirecte de contenus de messages, ainsi que les dispositifs servant à la collecte, au traitement et à l'exploitation de données de trafic (par exemple, ligne d'abonné, point terminal du réseau, équipements de commutation et de routage et réseau de connexion, ainsi que systèmes de facturation ou de fraude),
- pour ce qui est de la gestion et de la conservation de dossiers régies par la confidentialité des télécommunications, il faut utiliser des moyens de stockage suffisants pour protéger des données et des locaux appropriés dont l'accès est contrôlé de façon satisfaisante,
- seules les personnes suffisamment au fait de la sensibilité de ces données peuvent y avoir accès,
- il faut veiller à ce que, en cas de systèmes de messagerie avec enregistrement intermédiaire, par son consentement, seul l'abonné détermine le contenu, le volume et le type de traitement. Il est possible de mettre en œuvre des mesures de protection qui permettent exclusivement à l'abonné de décider lui-même des personnes qui peuvent saisir le contenu des messages et y accéder à l'aide de codes d'accès et de mots de passe appropriés. Ces derniers sont uniquement transmis à l'abonné de manière confidentielle et ledit abonné doit les modifier de façon autonome dès réception. L'abonné est libre de transmettre les identifiants aux personnes de son choix,
- la mise en place de systèmes de sauvegarde peut par exemple constituer une mesure de protection contre la suppression injustifiée de contenus de messages par le prestataire de services allant à l'encontre du lien juridique résultant du contrat conclu.

4.2 Exigences de sécurité relatives à la protection des données à caractère personnel (article 91 et articles suivants de la loi TKG)

La section 7, paragraphe 2, de la loi TKG régule la protection des données spécifique au secteur. Le règlement général sur la protection des données (RGPD) et les autres

réglementations de la loi allemande sur la protection des données (abrégée «BDSG» en allemand) sont également applicables.

On peut retenir que le RGPD n'impose aucune obligation supplémentaire aux personnes physiques ou morales en ce qui concerne le traitement dans le cadre de la fourniture de services de communication électroniques accessibles au public sur les réseaux de transmission publics si elles sont spécifiquement soumises à des obligations fixées par la directive 2002/58/CE (directive vie privée et communications électroniques) qui poursuivent le même objectif (article 95 du RGPD). Les dispositions du RGPD prévalent en conséquence, sauf en cas de divergence d'une disposition de la loi TKG résultant de la transposition de la directive vie privée et communications électroniques. Le RGPD supplante donc largement l'article 95 de la loi TKG, par exemple: à quelques exceptions près, la directive vie privée et communications électroniques ne contient en effet aucune disposition sur le traitement des données conservées à long terme. Les seules exceptions sont l'article 95, paragraphe 2, phrases 2 et 3, de la loi TKG transposant l'article 13, paragraphe 2, de la directive vie privée et communications électroniques. Aucune explication s'y rapportant n'a donc été fournie ci-dessous.

L'article 109 de la loi TKG transpose en revanche l'article 4, paragraphe 1, de la directive vie privée et communications électroniques et la directive 2002/21/CE (directive «cadre»): il prévaut donc sur les autres dispositions.

4.2.1 Obligations déclaratives (article 93 de la loi TKG)

Les obligations déclaratives ont pour but de garantir l'exercice du droit à l'autodétermination informationnelle, car:

«*Toute personne ne pouvant pas savoir avec une certitude suffisante quelles informations la concernant sont connues à certains niveaux de son environnement social et ne pouvant pas estimer dans une certaine mesure les connaissances d'éventuels partenaires d'échange électronique de données peut être considérablement entravée dans sa liberté de planifier ou de prendre des décisions en toute autonomie. Un ordre social et un ordre juridique qui le permet dans lesquels les citoyens ne peuvent plus savoir qui sait quoi sur eux, quand et à quelle occasion ne seraient pas compatibles avec le droit à l'autodétermination informationnelle.*» (Décision de la Cour constitutionnelle fédérale no 1, 44)

Cette argumentation de la Cour constitutionnelle fédérale intègre également clairement le fait que la protection constitutionnelle ne peut se limiter à l'intervention de l'État, mais doit par exemple également inclure la protection apportée par des entreprises de télécommunications privées.

La collecte, le traitement et l'exploitation des données conservées à long terme et des données de trafic des entreprises de télécommunications assujetties peuvent entre autres être effectués dans «Service à la clientèle et systèmes de facturation», dans «Systèmes de fraude (article 100, paragraphe 3, de la loi TKG)» ou dans «Dispositifs de notification des connexions entrantes (article 101 de la loi TKG)» ou dans «Systèmes à inclure dans les annuaires téléphoniques publics» (article 45m de la loi TKG).

En ce qui concerne le respect des obligations déclaratives applicables aux termes du droit régissant la protection des données, les dispositions applicables sont celles de l'article 13 du RGPD et de l'article 93 de la loi TKG. Les mesures suivantes doivent également être prises à cet égard:

- il est recommandé que les employés soient sensibilisés à la question de la protection des données en prenant des mesures appropriées en matière de formation. En outre, tous les employés concernés doivent remettre une déclaration d'engagement destinée à garantir la protection de leurs données,
- lors de la conclusion du contrat, le nom et les coordonnées de la personne responsable du traitement des données doivent être communiqués aux abonnés. De façon générale, les abonnés doivent être informés du type de données qui doit être traité, à quelles fins et sur quelle base juridique. Les destinataires ou catégories de destinataires auxquels les données à caractère personnel des abonnés sont transmises doivent également être nommés. S'il est prévu d'effectuer un transfert vers un pays tiers, c'est-à-dire vers un pays en dehors de l'UE et de l'Espace économique européen, cela doit également être indiqué aux abonnés. Les coordonnées du mandataire du gouvernement fédéral chargé du contrôle du traitement automatisé des informations nominatives au sein de l'entreprise doivent également être communiquées afin que les personnes concernées sachent qui est le bon interlocuteur dans l'entreprise pour les questions de protection des données. En outre, les droits des personnes concernées – comme le droit de rectification ou de suppression – et le droit de déposer une plainte auprès de l'autorité responsable de la protection des données doivent être indiqués. Les abonnés doivent être informés des possibilités de sélection et de configuration autorisées [par exemple, l'utilisation des données conservées à long terme pour conseiller les abonnés, pour personnaliser les offres publicitaires, pour étudier le marché (article 95, paragraphe 2, de la loi TKG) et pour fournir une facturation détaillée (article 99, paragraphe 1, de la loi TKG)], de la déclaration des connexions réglées au forfait (article 99, paragraphe 1, de la loi TKG), de l'enregistrement dans le répertoire des abonnés (article 104 de la loi TKG) et de la fourniture d'informations (article 105 de la loi TKG),

- les abonnés doivent être informés des éventuels risques particuliers encourus en cas d'atteinte à la sécurité du réseau et le cas échéant des solutions possibles.

4.2.2 Données de trafic (article 96 de la loi TKG)

Les données de trafic doivent être considérées comme des données à caractère personnel tout autant que les données conservées à long terme. Contrairement aux données conservées à long terme, les données de trafic sont toutefois soumises à la protection particulière prévue à l'article 10 de la Constitution de la République fédérale d'Allemagne ou à l'article 88 de la loi TKG.

La disposition réglemente la collecte et l'utilisation dans le cadre des droits à la protection des données et fixe en même temps les conditions de recevabilité pour les entreprises assujetties.
Les conditions suivantes figurent entre autres parmi lesdites conditions:

- la collecte de données sur le trafic peut uniquement être autorisée si cela est nécessaire à l'une des fins mentionnées au paragraphe 2 de la partie 7 de la loi TKG,
- dans certaines autres conditions, la détermination des profils d'échange électronique de données des différents abonnés et l'analyse des flots de données peuvent être autorisées aux termes de l'article 96, paragraphe 3, phrase 1, de la loi TKG,
- en règle générale, les données de trafic doivent être supprimées par le prestataire de services immédiatement après la fin de la connexion aux termes de l'article 96, paragraphe 1, phrase 3, de la loi TKG. Cela fait référence au guide du commissaire fédéral chargé de la protection des données (abrégé «BfDI» en allemand et ci-après) et de l'Agence fédérale des réseaux (abrégée «BNetzA» en allemand et ci-après) pour un enregistrement des données de trafic conforme aux droits à la protection des données (version du 19.12.2012) (disponible sur www.bundesnetzagentur.de).

4.2.3 Calcul et facturation des prix (article 97 de la loi TKG)

Les données de trafic servent généralement de base aux éléments constitutifs du traitement des données liés au calcul et à la facturation des prix. Sur ce point, la disposition constitue une autorisation spécifique au secteur d'utiliser les données de trafic (article 96, paragraphe 1, de la loi TKG, voir ci-dessus).

Il faut s’assurer de ce qui suit à cet égard:

- si des tiers sont impliqués dans l’établissement de factures de télécommunications ou la fourniture de services de télécommunications (par exemple par l’intermédiaire de prestataires de services n’ayant pas leur propre infrastructure de réseau), les relations d’interface techniques et organisationnelles entre le donneur d’ordre (prestataire de services) et le fournisseur (personne travaillant au service du donneur d’ordre) doivent être clairement régies,
- les données qui ne sont pas requises conformément à l’article 97, paragraphe 3, de la loi TKG doivent être supprimées immédiatement.

4.2.4 Données de localisation (article 98 de la loi TKG)

Les données de localisation (article 3, point 19, de la loi TKG) peuvent être regroupées en profils de déplacement qui permettent de déduire les relations ou habitudes sociales. Les données de localisation sont donc particulièrement importantes au point de vue de la législation sur la protection des données.

- Les données de localisation utilisées qui concernent les utilisateurs de réseaux de télécommunications publics ou de services de télécommunications accessibles au public peuvent uniquement être traitées dans les proportions nécessaires pour mettre à disposition des services à valeur ajoutée et pour la durée nécessaire à cet effet si elles ont été anonymisées ou si l’abonné a donné son accord au prestataire du service à valeur ajoutée.
- Il faut établir une procédure afin que l’utilisateur puisse interdire de manière simple et gratuite le traitement des données de localisation pour chaque connexion au réseau ou pour chaque transmission.
- La transmission de données de localisation pour les numéros de téléphone aux termes de l’article 98, paragraphe 3, de la loi TKG (numéros d’urgence 112 ou 110 ou numéro de téléphone 124 124 et 116 117) doit être assurée.
- Il faut veiller à ce que le traitement des données de localisation soit limité à ce qui est indispensable.

4.2.5 Facturation détaillée (article 99 de la loi TKG)

L'abonné doit être informé en détail des services de télécommunications facturés au moyen d'une facture détaillée. La facture détaillée sert ainsi à effectuer un contrôle. La facture détaillée doit toutefois être établie régulièrement sur la base des données de trafic. Ces dernières étant régies par la confidentialité des télécommunications, sous ce rapport, les dispositions spécifiques à la protection des données (article 99, paragraphe 1, de la loi TKG) doivent être respectées. Cela est particulièrement valable si certains droits des différents utilisateurs d'une ligne téléphonique sont concernés (article 99, paragraphe 2, de la loi TKG). En ce qui concerne l'article 99 de la loi TKG, il convient de souligner les points suivants:

- l'abonné doit uniquement être informé des données enregistrées pour les connexions pour lesquelles il paie s'il a demandé une facturation détaillée par écrit avant la période de facturation concernée. Les données des connexions payées au forfait peuvent uniquement lui être communiquées sur demande,
- la facture détaillée doit être fournie à l'abonné s'il en fait la demande,
- si l'abonné demande une facture détaillée, il doit avoir la possibilité d'obtenir les numéros de téléphone de son choix en entier ou leurs trois derniers chiffres,
- si la facture détaillée est envoyée par voie électronique, des mesures doivent être prises pour protéger la confidentialité des télécommunications et les données à caractère personnel,
- les réglementations applicables à la personne redevable doivent permettre de garantir que les connexions à la facture détaillée ne peuvent pas être identifiées aux termes de l'article 99, paragraphe 2, de la loi TKG. L'impossibilité d'identifier les connexions est assurée si la connexion n'apparaît pas dans la facture détaillée,
- la liste des organismes de conseil protégés conformément à l'article 99, paragraphe 2, phrase 4, de la loi TKG est consultable chaque trimestre par l'entreprise assujettie auprès de l'Agence fédérale des réseaux dans le cadre d'un processus automatisé,
- l'entreprise assujettie doit immédiatement prendre en compte les changements apportés à la procédure de facturation.

4.2.6 Notification des appels entrants (article 101 de la loi TKG)

Dans certains cas, la disposition accorde à l'abonné un droit d'information sur les appels entrants (procédure de localisation des communications téléphoniques) selon une procédure imposée. L'organisation de cette procédure de localisation des communications téléphoniques sur le plan légal doit permettre aux abonnés d'obtenir des informations sur la ligne à l'origine de l'appel en cas d'appels menaçants ou de harcèlement. La procédure est particulièrement intéressante pour les numéros supprimés et est souvent le seul moyen pour les personnes concernées d'entamer

des démarches juridiques convenablement. Il faut consulter le texte de loi pour plus de précisions.

L'Agence fédérale des réseaux et le commissaire fédéral chargé de la protection des données doivent être immédiatement informés de l'introduction et de la modification de la procédure visant à garantir la procédure de localisation des communications téléphoniques.

4.2.7 Renvoi automatique des appels (article 103 de la loi TKG)

Le but de la disposition est de protéger l'abonné contre le renvoi indésirable des appels d'un tiers vers sa ligne. Cependant, l'exigence de protection est soumise à sa faisabilité technique.

4.2.8 Systèmes de messagerie avec stockage provisoire (article 107 de la loi TKG)

Certains prestataires de services donnent aux clients la possibilité de stocker certains contenus utilisés dans le cadre de télécommunications pour une utilisation ultérieure. Pour cela, les systèmes de messagerie ne sont pas utilisés en temps réel. Cependant, le stockage de contenus utilisés dans le cadre de télécommunications peut également représenter un risque important pour les données à caractère personnel et la confidentialité des télécommunications. L'article 107 de la loi TKG a pour but d'éviter ce risque. À cet égard, il convient de souligner les points suivants:

- les prestataires de services de stockage temporaire doivent s'assurer que l'abonné est le seul à déterminer le contenu, le volume et le type de traitement,
- les prestataires de services doivent prendre les mesures techniques et organisationnelles nécessaires pour prévenir les transmissions incorrectes et la divulgation non autorisée du contenu des messages au sein de leur entreprise ou à des tiers.

4.3 Exigences de sécurité relatives à la protection de l'infrastructure de télécommunications et de la disponibilité des services de télécommunications

4.3.1 Dysfonctionnements des systèmes de télécommunications et emploi abusif des services de télécommunications (article 100 de la loi TKG)

Le prestataire de services peut collecter et utiliser les données conservées à long terme, les données de trafic et les données foncières requises pour identifier, limiter ou résoudre les dysfonctionnements. À cet égard, l'article 100, paragraphe 1, de la loi TKG réglemente les

éléments constitutifs de l'autorisation aux termes de la législation sur la protection des données. Dans certains cas, ces éléments constitutifs s'accompagnent d'une obligation déclarative. Des informations générales sur l'obligation déclarative visée à l'article 100, paragraphe 1, de la loi TKG et sur sa validité sont disponibles à l'adresse suivante: www.bundesnetzagentur.de disponible.

Pour détecter et limiter les dysfonctionnements, l'opérateur de tout système de télécommunications est également autorisé à intervenir sur les connexions existantes dans des conditions strictes. Tous les enregistrements qui ont pu être réalisés doivent cependant être immédiatement supprimés. Cette intervention dans le cadre de la législation relative à la protection des données s'accompagne d'une obligation déclarative envers le mandataire du gouvernement fédéral chargé du contrôle du traitement automatisé des informations nominatives au sein de l'entreprise (voir article 100, paragraphe 2, de la loi TKG).

En présence d'éléments indiquant une manœuvre dolosive ou une fraude, le prestataire de services peut utiliser les données conservées à long terme et les données de trafic sous certaines conditions pour protéger son droit. De ce point de vue, les obligations déclaratives par rapport à l'Agence fédérale des réseaux et au commissaire fédéral chargé de la protection des données doivent être respectées.

4.3.2 Atteintes graves à la sécurité (article 109, paragraphe 5, de la loi TKG)

Les opérateurs de réseau et les prestataires de services doivent immédiatement signaler tant les atteintes graves à la sécurité réellement survenues que potentiellement survenues à l'Agence fédérale des réseaux et à l'Office fédéral de la sécurité informatique. Cela fait référence au programme de mise en œuvre actuellement applicable pour déclarer les incidents (publication du: 10.11.2017, version: 4.0, JO de la BNetzA n° 22 du 22.11.2017).

4.3.3 Sécurité des données et des informations (article 109a de la loi TKG)

La disposition définit certaines obligations déclaratives en cas de non-respect de la protection des données à caractère personnel («non-respect de la protection des données» ou «atteinte à la sécurité»). Dans ce contexte, il incombe à l'entreprise assujettie de remplir certaines obligations de notification envers la personne concernée, mais également envers l'Agence fédérale des réseaux et le commissaire fédéral chargé de la protection des données. Cela fait référence aux conseils de l'Agence fédérale des réseaux disponibles sur www.bundesnetzagentur.de («Benachrichtigungspflichten im Fall einer Verletzung des

Schutzes personenbezogener Daten» ou exigences de notification en cas de non-respect de la protection des données à caractère personnel).

Si des atteintes à la sécurité informatique proviennent d'un système de traitement de données exploité par l'utilisateur, l'utilisateur est soumis à une obligation déclarative envers l'entreprise assujettie aux termes de l'article 109a, paragraphe 4, de la loi TKG. En passant par un renvoi au sein de ses propres réseaux, l'entreprise assujettie se donne la possibilité d'identifier d'abord l'utilisateur concerné, puis de lui permettre de remédier au problème (dit «sinkholing»).

La prestataire n'est pas dans l'obligation de réaliser une analyse personnalisée du système ou de fournir des conseils sur mesure. Dans les cas où il est techniquement impossible d'avertir les utilisateurs concernés en quelques jours, le prestataire est autorisé à informer et à indiquer un outil de protection uniquement à ses abonnés.

L'expression «dès qu'il en est informé» indique clairement que le prestataire a le droit de transmettre des données de trafic qu'il a déjà recueillies et enregistrées uniquement afin d'informer les utilisateurs. Il est donc interdit de recueillir d'autres données exclusivement afin d'avertir des utilisateurs (Bundestag, publication 18/4096, p. 37).

L'article 109a, paragraphe 5, de la loi TKG permet de restreindre, de rediriger ou de faire cesser la transmission de données en cas de dysfonctionnement. Compte tenu du nombre croissant d'incidents de sécurité informatique, ces pouvoirs ont pour but de permettre d'y remédier, notamment si un utilisateur dont les systèmes sont à l'origine du dysfonctionnement ne peut le résoudre alors qu'il en a été informé ou si l'on ne peut pas prévoir une élimination immédiate et si une intervention dans l'utilisation du service de télécommunications est nécessaire pour corriger ou bloquer l'atteinte.

L'entreprise assujettie peut de plus restreindre ou empêcher la transmission de données vers des sources de dysfonctionnement conformément à l'article 109a, paragraphe 6, de la loi TKG afin de contrer la survenue de dysfonctionnements dans les systèmes de télécommunications et de traitement des données des utilisateurs. Ce droit a été octroyé aux entreprises assujetties, car les pirates utilisent généralement des outils modulaires pour attaquer et ainsi infecter les systèmes de télécommunications et de traitement de données (Bundestag, publication 18/11808, p. 11).

5 Mise en œuvre des exigences de sécurité

L'article 109, paragraphe 4, de la loi TKG entraîne différentes obligations à remplir chronologiquement pour les opérateurs de réseaux publics de télécommunications et les prestataires de services de télécommunications accessibles au public. Fondamentalement, les opérateurs de réseau et les prestataires de services sont soumis à l'obligation d'établir un programme de sécurité. Un chargé de la sécurité doit également être nommé par les deux. La loi prévoit que seul l'opérateur de réseau se soumette à l'obligation de présenter à l'Agence fédérale des réseaux le programme de sécurité qu'il a établi au moment de la mise en exploitation. Le prestataire de services n'est pas légalement tenu de le présenter. Cependant, l'Agence fédérale des réseaux peut l'y obliger. En plus de ces obligations d'établir un programme de sécurité, de désigner un chargé de la sécurité et de présenter ledit programme, il faut également répondre à l'obligation de fournir des explications. Ladite obligation concerne la mise en œuvre effective des considérations du programme de sécurité. Si les circonstances évoluent, la loi oblige l'entreprise en question à s'adapter.

Les obligations liées au programme de sécurité aux termes de l'article 109, paragraphe 4, de la loi TKG servent à définir et à structurer des mesures appropriées et raisonnablement applicables pour protéger la confidentialité des télécommunications, les données et l'opérationnalité des réseaux et des services. Le catalogue des exigences de sécurité présenté constitue une condition préalable à l'exécution desdites obligations.

L'Agence fédérale des réseaux vérifie le projet et contrôle également régulièrement la mise en œuvre du programme de sécurité de l'entreprise. Si elle détecte un défaut de sécurité de ce point de vue, elle peut exiger que le défaut identifié soit éliminé. Ce contrôle doit être distingué de l'inspection réalisée par un organisme indépendant qualifié conformément à l'article 109, paragraphe 7, de la loi TKG. Ladite inspection ne se concentre ni sur le programme de sécurité de l'entreprise ni sur sa mise en œuvre. L'objet de cette inspection est uniquement la question de savoir au cas par cas si les exigences de sécurité de l'article 109, paragraphes 1 à 3, de la loi TKG, sont respectées. L'inspection effectuée conformément à l'article 109, paragraphe 7, de la loi TKG doit donc comparer l'évaluation de la sécurité de l'entreprise à celle d'un tiers. Le contenu du catalogue doit également être utilisé pour ce contrôle. Le catalogue sert donc de base à la fois pour les opérations et les contrôles.

5.1 Mise en œuvre des exigences de sécurité

La loi spécifie un certain contenu pour le programme de sécurité. Ces exigences découlent plus précisément de l'article 109, paragraphe 4, points 1 à 3, de la loi TKG. Le programme doit à cet égard inclure un rapport descriptif (article 109, paragraphe 4, point 1, de la loi TKG), une analyse des risques (article 109, paragraphe 4, point 2, de la loi TKG) et les mesures de protection correspondantes qui sont fixées pour chaque cas (article 109, paragraphe 4, point 3, de la loi TKG). Les bases de la mise en œuvre pratique de ces exigences sont traitées ci-dessous.

5.1.1 Description des réseaux publics de télécommunications exploités

L'établissement et la présentation d'un plan structurel du réseau suffit à respecter valablement l'exigence légale imposée par l'article 109, paragraphe 4, point 1, première partie de la phrase, de la loi TKG. Le plan établi doit décrire au moins les éléments structurels suivants:

1. tous les systèmes de télécommunications et de traitement de données (postes de commutation, serveurs des services, gestion de réseau) et tous les systèmes informatiques utilisés (gestion des données clients, facturation) qui sont intégrés au réseau;
2. toutes les liaisons qui relient les systèmes (connexions LAN, technologies dorsales et liaisons radio);
3. toutes les connexions externes (interfaces) des systèmes (type de connexion, Internet, à distance, itinérance);
4. taille et type de réseau (nombre d'abonnés, réseau d'antennes-relais de téléphonie mobile, faisceaux hertziens ou réseau câblé, etc.);
5. étendue géographique du réseau (locale, régionale, nationale ou internationale).

La complexité du plan de réseau peut être simplifiée en formant des groupes (par exemple par type, par configuration, par réseau, par emplacement, par conditions générales, par application, par service, etc.). Pour les réseaux plus importants, il peut également être judicieux d'établir des plans partiels séparés (par exemple pour le traitement des données des commandes, pour les systèmes de facturation, pour les réseaux dorsaux, etc.).

5.1.2 Description des services de télécommunications accessibles au public fournis

En principe, tous les services publics de télécommunications fournis par l'entreprise doivent être décrits en substance conformément à l'article 109, paragraphe 4, point 1, deuxième partie de la phrase, de la loi TKG. Pour établir l'analyse des risques, il est utile de préciser de façon théorique non seulement le contenu, mais aussi les différents groupes d'abonnés. Si seuls des

services sont fournis, il convient néanmoins d'indiquer les réseaux de télécommunications utilisés dans ce cas.

5.1.3 Classification de la criticité

Le programme de sécurité doit permettre de déduire les risques que l'on peut présumer aux termes de l'article 109, paragraphe 4, point 2, de la loi TKG. Pour présumer de ces risques, il est nécessaire de réaliser une analyse des risques; ce qui consiste normalement en une analyse des besoins de protection, des menaces et des risques. Les résultats descriptifs (paragraphes 5.1.1. et 5.1.2) déjà obtenus permettent en même temps une analyse théorique des risques et leur affectation à certaines criticités (postures de sécurité). Le facteur décisif pour déterminer la criticité est l'importance du réseau ou du service de télécommunications à protéger. En principe, les réseaux et services publics de télécommunications peuvent être classés aux niveaux de criticité suivants:

Criticité normale: tous les réseaux et services publics de télécommunications.

Criticité élevée: réseaux et services publics de télécommunications dans la mesure où ils sont plus importants pour l'intérêt général

Criticité extrême: réseaux et services publics de télécommunications dans la mesure où ils sont d'une importance capitale pour l'intérêt général.

Criticité normale

D'un point de vue constitutionnel, l'importance des biens protégés par l'article 109, paragraphes 1 et 2, de la loi TKG (confidentialité des télécommunications, protection des données et opérationnalité du réseau) doit au moins être prise en compte pour le particulier. Sur ce point, toute criticité normale (inférieure) doit se baser sur cette importance et garantir le respect des principes correspondants. Les exigences de sécurité de ce type découlent essentiellement de la partie principale du catalogue des exigences de sécurité.

Criticité élevée

Si le réseau ou service à protéger est utilisé par un plus grand nombre d'abonnés, l'importance du réseau ou service concerné est plus grande. Outre son importance pour le particulier, il est également important pour l'intérêt général. À partir d'un certain nombre d'abonnés, cet intérêt général peut devenir important. La loi sur la sécurité des services postaux et des services de télécommunications (abrégée «PTSG» en allemand et ci-après) fournit des éléments qui permettent de déterminer si un nombre d'abonnés est significatif. La loi PTSG sert entre autres à assurer le bon fonctionnement de la communauté en garantissant la fourniture fondamentale de services de télécommunication. Dans ce contexte de protection, le domaine d'application de la loi se rapporte à toute offre de services de télécommunications concernant plus de 100 000 abonnés. Le décret d'application relatif à la détermination des infrastructures critiques d'après la loi sur l'Office fédéral pour la sécurité des techniques de l'information (décret abrégé «BSI-KritisV» en allemand) utilise également les valeurs mentionnées dans la loi PTSG pour déterminer des valeurs seuils. Pour les offres de services de télécommunications ou l'exploitation de réseaux de télécommunications touchant un nombre proportionnel d'abonnés, il semble donc raisonnable de supposer qu'ils présument d'un réseau ou service d'une importance particulière au sens de l'article 109, paragraphe 2, phrase 5, de la loi TKG et qu'ils relèvent d'une criticité élevée.

Criticité extrême

Outre le nombre d'abonnés, les particularités du réseau ou service de télécommunications à protéger peuvent également indiquer qu'ils sont d'une certaine importance pour l'intérêt général ou au moins confirmer l'hypothèse qu'ils sont d'une importance particulière. Le réseau de téléphonie mobile public présente une originalité juridique de ce point de vue. Pour le réseau de téléphonie mobile, on peut en effet partir de la supposition qu'il est utilisé de manière transversale dans toutes les sphères de la vie publique. La disponibilité et la sécurité de ce réseau sont donc susceptibles de concerner non seulement le particulier, mais aussi l'État, l'économie et la société.

L'exploitation des réseaux 5G au sens de la recommandation (UE) 2019/534 du 26 mars 2019 présente une originalité juridique considérable. En ce sens, les réseaux 5G sont la future épine dorsale de nos économies nationales et de nos sociétés de plus en plus numériques. Ils traiteront des milliards d'objets et de systèmes les uns avec les autres et au sein des infrastructures critiques des secteurs de l'énergie, de l'eau, de l'alimentation, de la santé, des finances, des assurances, du transport et de la circulation, ainsi que du secteur des technologies de l'information et des télécommunications, et ils prendront en charge les systèmes de sécurité. Si des réseaux de téléphonie mobile 5G accessibles au public sont donc exploités avec plus de 100 000 abonnés, il est possible de classer l'importance de ces réseaux de télécommunications pour l'intérêt général comme capitale.

Si le nombre d'abonnés et/ou les spécificités du réseau ou service de télécommunications à protéger permettent de déduire qu'il est d'une importance capitale, on peut supposer que sa criticité est extrême. Actuellement, seuls les réseaux publics de télécommunications de la téléphonie mobile de la 5e génération au sein desquels les fréquences sont attribuées relèvent d'un niveau de criticité extrême.

5.1.4 Analyse pratique des risques

Indépendamment de l'affectation théorique préalable des risques à une certaine criticité, l'analyse pratique des risques réalisée par la suite consiste à déterminer et à évaluer les éléments qui sont réellement exploités au cas par cas.

Il faut donc d'abord déterminer tous les éléments constitutifs de la sécurité dans l'entreprise. Les éléments constitutifs de la sécurité dans ce sens peuvent être tous les sous-systèmes ou systèmes ou processus de gestion liés à la confidentialité des télécommunications, à la protection des données et à la disponibilité des réseaux de télécommunications et des services de télécommunications. Les éléments constitutifs de la sécurité peuvent également résulter de l'organisation. L'organisation de la sécurité de l'entreprise (paragraphe 3.1) doit sur ce point également faire l'objet d'une analyse de risque adéquate. Il faut anticiper la sécurité des données, des systèmes et des installations (paragraphe 3.3) ou de l'entreprise concernée (paragraphe 3.4) au cas par cas. Les normes de l'Office fédéral de la sécurité informatique (abrégé «BSI» en allemand et ci-après) et les piliers du compendium de la protection informatique de base du BSI fournissent des indications complémentaires sur ces sujets, entre autres concernant l'infrastructure, les systèmes informatiques, les réseaux et les applications.

Là encore, le compendium de la protection informatique de base du BSI fournit des précisions importantes sur les menaces élémentaires en ce qui concerne les cas de force majeure, les défauts organisationnels, les erreurs humaines, des défaillances techniques et les actes délibérés.

5.1.5 Analyse des risques de l'ensemble du système

Une situation dangereuse ne peut pas uniquement résulter d'éléments opérationnels isolés présentant des risques ou de l'affectation théorique d'un réseau à une criticité. L'interaction de divers sous-processus peut également entraîner certains risques et nécessiter des mesures de protection supplémentaires. Une évaluation supplémentaire de l'ensemble du système est donc nécessaire à cet égard.

Il n'est pas toujours possible d'identifier tout ce qui peut présenter des risques. Il faut donc considérer la présence d'une part d'inconnu en conséquence. La présence de ce risque résiduel

doit être décrite et évaluée plus en détail dans une évaluation finale des risques. L'objectif ne doit cependant pas être d'identifier toutes les menaces ou de les réduire à un niveau quantifiable et acceptable.

5.1.6 Définition et description des précautions techniques ou autres mesures de protection

1. Une fois l'analyse des risques terminée, l'entreprise assujettie doit sélectionner et mettre en œuvre les mesures de protection appropriées, nécessaires et raisonnablement applicables.
Il est toujours décisif d'évaluer le cas concerné pour les sélectionner et les définir.

L'état de la technique doit être pris en compte pour définir les mesures. L'obligation de tenir compte de l'état de la technique impose de s'adapter avec dynamisme à l'évolution des possibilités techniques et des risques. Sur ce point, l'évaluation des mesures de protection n'est pas définitive, mais continue. Dans ce cas, le recours à l'état de la technique n'inclut pas de méthodes n'ayant pas encore été employées dans la pratique. Les mesures correspondant à l'état de la technique doivent être à la fois commercialisables et éprouvées dans la pratique.

Les intérêts de l'entreprise jouent également un rôle dans la détermination des mesures. Les mesures de protection à prendre pour chaque cas conviennent uniquement si les moyens techniques et économiques sont proportionnels à l'importance des droits et des installations à protéger pour le grand public. Il ne doit pas y avoir de disproportion entre les moyens à déployer et l'utilité pour le grand public.

La protection existante peut être prise en compte au cas par cas pour les nouvelles mesures de protection à définir sous ce rapport. Les mesures de protection établies sur la base du «Catalogue des exigences de sécurité» (version 1.1 du 7.1.2016) peuvent donc continuer à être considérées comme appropriées au cas par cas. Cependant, il est indispensable qu'aucune modification actuelle sur les réseaux publics de télécommunications exploités ou dans les services de télécommunications accessibles au public, et donc aucune modification des situations risquées ne soit constatée. Il est également indispensable de pouvoir contrôler le cycle de vie de la technologie utilisée dans les réseaux exploités ou les services proposés. Dans les cas présents, le programme de sécurité établi ne doit pas être remplacé ou de nouveau présenté. Les écarts dus à la protection existante doivent en tout cas être consignés et il faut démontrer que les mesures existantes sont suffisantes.

2. Les principes suivants peuvent s'appliquer aux mesures de protection sélectionnées sur la base de l'analyse théorique des risques:

Criticité normale: les mesures techniques, organisationnelles, humaines et d'infrastructure à prendre doivent être adaptées pour assurer un niveau de sécurité communément admis. La protection informatique de base du BSI offre une sélection de recommandations concrètes. Les éléments constitutifs du compendium de la protection informatique de base sont divisés en dix strates et traitent d'une grande variété de sujets en matière de sécurité informatique; des applications (APP) à l'informatique industrielle (IND) en passant par la gestion de la sécurité (ISMS). Dans certains cas, un niveau de protection plus élevé peut être nécessaire pour protéger la confidentialité des télécommunications.

Criticité élevée: les mesures à prendre doivent être adaptées pour garantir une protection de base communément admise et une protection accrue dans les domaines d'importance pour la classification au niveau de criticité élevée. En outre, les mesures nécessaires et raisonnablement applicables doivent être prises contre les dysfonctionnements importants résultant de catastrophes naturelles, en particulier d'accidents graves, de destructions matérielles, d'attaques terroristes ou d'autres évènements comparables. Il faut également prévoir des mesures appropriées et raisonnablement applicables à cet égard en cas de tension ou d'un état de nécessité résultant d'une menace grave et immédiate pour les institutions ou pour l'intégrité du territoire. Cela concerne plus particulièrement les mesures de préparation aux situations d'urgence. Le compendium de la protection informatique de base du BSI offre une aide dans la sélection de mesures concrètes.

Criticité extrême: les mesures à prendre doivent être adaptées pour garantir une protection communément admise qui, outre le besoin général de protection (protection de base accrue), prend également en compte la criticité particulière. Les opérateurs de réseaux publics de télécommunications et les prestataires de services de télécommunications accessibles au public susceptibles de faire partie de cette catégorie doivent également se conformer aux exigences de sécurité et aux mesures spécifiées à l'annexe 2.

Les prestataires de services de télécommunications dotés d'une infrastructure IP doivent également prendre en compte les exigences et les instructions de l'annexe 1 «Exigences pour les prestataires de services de télécommunications dotés d'une infrastructure IP» lors de la définition des mesures de protection.

Ce n'est cependant pas l'affectation théorique à une criticité qui est décisive pour la définition des mesures de protection, mais toujours le résultat de l'analyse concrète et isolée des

risques. L'affectation d'un réseau ou d'un service à une certaine criticité peut toutefois être indicateur. De plus, la prévision globale doit être prise en compte dans tous les cas.

L'entreprise assujettie n'est généralement pas obligée d'établir des mesures de protection sur la base de l'analyse décrite ci-dessus. Il est également possible de déterminer des mesures sur la base de normes appropriées (par exemple les normes du BSI, la méthodologie de la protection informatique de base du BSI, les normes DIN ISO ou CEI).

5.1.7 Établir un programme de sécurité

Après avoir terminé l'analyse des risques et déterminé les mesures à prendre dans chaque cas, le programme doit être établi. Il doit s'agir d'un document cohérent par son contenu. Seules les communications orales ou les explications téléphoniques ne satisfont pas à ces exigences.

5.1.8 Désignation du chargé de la sécurité

La désignation du chargé de la sécurité ne constitue pas un élément directement constitutif du programme de sécurité. Cependant, comme l'établissement du programme, cette désignation doit être faite au début de l'exploitation ou au moment de l'offre de service. Sur ce point, il existe un lien temporel, mais aussi substantiel entre ces obligations. Il incombe au chargé de la sécurité d'effectuer entre autres certaines tâches de coordination, de contrôle et de sa spécialité. Le chargé de la sécurité ou le suppléant désigné doit en même temps être l'interlocuteur de l'Agence fédérale des réseaux.
Le poste doit préserver les connaissances spécifiques nécessaires et une compréhension des processus de l'entreprise proportionnellement à la fonction à remplir. La connaissance du poste des évolutions en matière de sécurité informatique, des processus de l'entreprise et des conditions juridiques générales doit être tenue à jour. Il faut établir les conditions préalables à tout contact direct avec la direction de l'entreprise.

5.1.9 Déclaration de mise en œuvre

Une déclaration doit être présentée avec le programme de sécurité. Elle doit attester que les précautions techniques et autres mesures de protection qui y figurent ont été mises en œuvre ou le seront au plus vite. La déclaration doit revêtir la forme écrite.

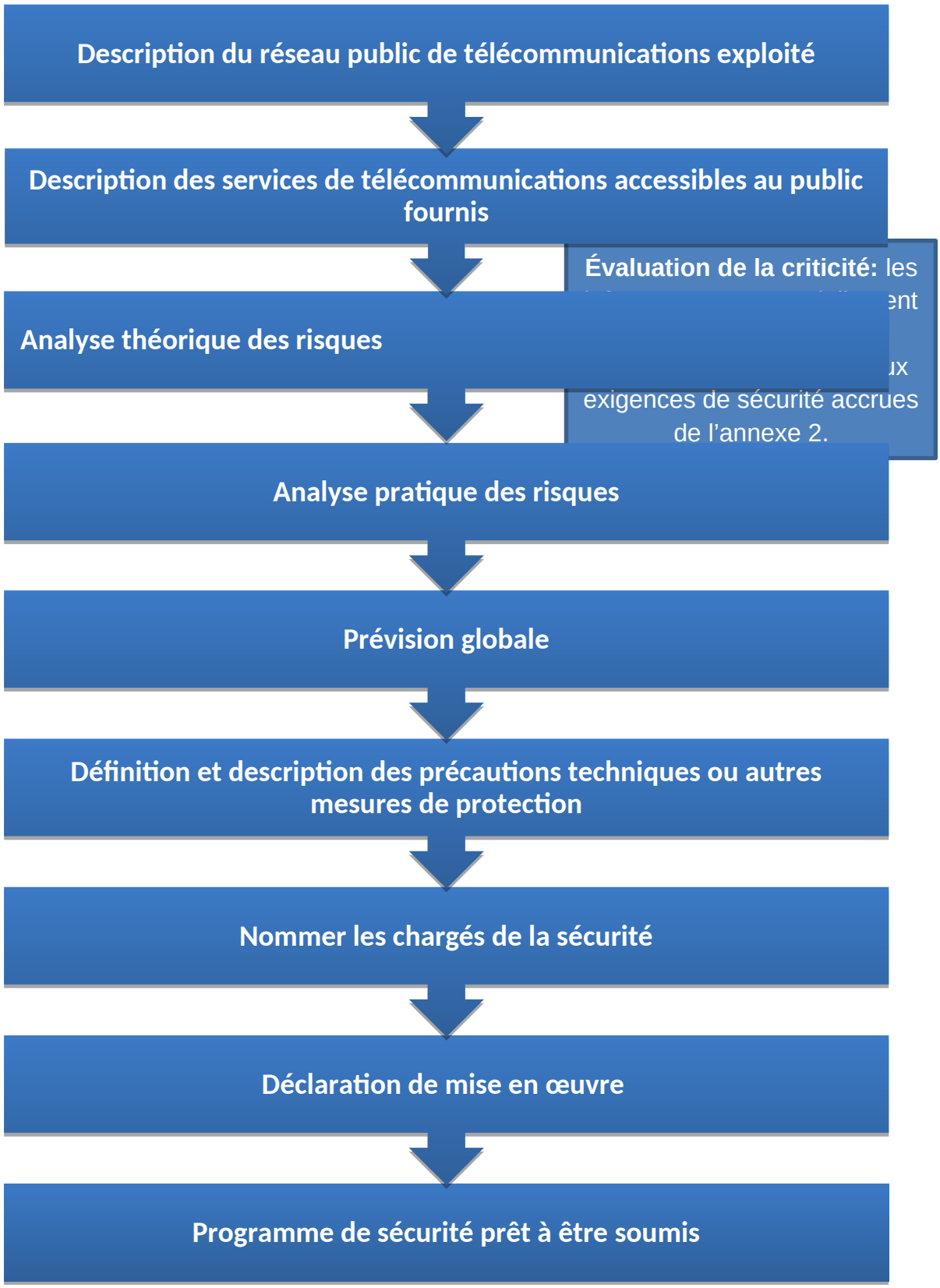
5.1.10 Adaptation du programme de sécurité aux changements

La sécurité des réseaux et services de télécommunications est un processus d'amélioration continue. Le programme de sécurité doit donc être contrôlé régulièrement et adapté aux

changements. Il faut veiller à réagir face aux progrès techniques, aux points faibles identifiés et aux vulnérabilités découvertes et à prendre des mesures de protection appropriées.

Pour garantir l'efficacité des mesures de protection dans un environnement en constante évolution (processus de gestions, paysages informatiques, lois et exigences, menaces, etc.), il faut veiller à déterminer et à évaluer l'efficacité des mesures de protection mises en œuvre à intervalles réguliers. Si des problèmes de sécurité sont identifiés, des mesures d'amélioration doivent systématiquement être prises, mises en œuvre et consignées. Si les circonstances à la base du programme de sécurité évoluent, l'entreprise obligée doit adapter le programme et le soumettre à nouveau à l'Agence fédérale des réseaux en se référant aux changements.

5.1.11 Procédure d'établissement du programme de sécurité



Beschreibung des betriebenen öffentlichen	Description du réseau public de

Telekommunikationsnetzes	télécommunications exploité
Beschreibung der erbrachten öffentlich zugänglichen Telekommunikationsdienste	Description des services de télécommunications accessibles au public fournis
Abstrakte Gefährdungsanalyse	Analyse théorique des risques
Kritikalität bewerten: Infrastrukturen mit erhöhtem Gefährdungspotenzial müssen erhöhte Sicherheitsanforderungen aus Anlage 2 erfüllen.	Évaluation de la criticité: les infrastructures potentiellement exposées à des risques accrus doivent répondre aux exigences de sécurité accrues de l'annexe 2.
Konkrete Gefährdungsanalyse	Analyse pratique des risques
Gesamtprognose	Prévision globale
Festlegung und Beschreibung der technischen Vorkehrungen oder sonstigen Schutzmaßnahmen	Définition et description des précautions techniques ou autres mesures de protection
Sicherheitsbeauftragten benennen	Nommer les chargés de la sécurité
Umsetzungserklärung	Déclaration de mise en œuvre
Sicherheitskonzept zur Vorlage bereit	Programme de sécurité prêt à être soumis

6 Entrée en vigueur et dispositions transitoires

Le catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel entre en vigueur dès sa publication au Journal officiel de l'Agence fédérale des réseaux. Les entreprises obligées doivent satisfaire aux exigences du catalogue au plus tard un an après son entrée en vigueur dans la mesure où aucune disposition transitoire particulière n'est mentionnée dans le catalogue.

Sources d'information:

ENISA Technical Guideline on Security measures for Article 4 and Article 13a:

https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a

Norme BSI 200-2:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html

Compendium de la protection informatique de base du BSI:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

Version allemande de la norme EN ISO/IEC 27001:2017

Version allemande de la norme EN ISO/IEC 27002:2017

7 Définitions

ENISA
European Agency for Cybersecurity/Agence européenne pour la cybersécurité (anciennement European Network, Information Security Agency/Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information).

Données de trafic selon l'article 3, point 30, de la loi TKG
Données collectées, traitées ou utilisées lors de la fourniture d'un service de télécommunications.

Prestataire de services selon l'article 3, point 6, de la loi TKG
Toute personne qui fournit en totalité ou partiellement

- des services de télécommunications ou qui
- contribue à la fourniture de tels services à titre professionnel.

Abonné selon l'article 3, point 20, de la loi TKG
Toute personne physique ou morale ayant conclu un contrat avec un prestataire de services de télécommunications **accessibles au public** pour la fourniture desdits services**.**

Données conservées à long terme selon l'article 3, point 3, de la loi TKG

Données d'un abonné qui sont collectées par l'intermédiaire de services de télécommunication pour établir, organiser les contenus, modifier ou résilier le lien juridique résultant d'un contrat.

Systèmes de télécommunications selon l'article 3, point 23, de la loi TKG

Installations techniques ou systèmes pouvant émettre, transmettre, envoyer, recevoir, régler ou contrôler des signaux électromagnétiques ou optiques identifiables sous la forme de messages.

Services de télécommunications selon l'article 3, point 24, de la loi TKG

Services généralement fournis moyennant rémunération qui consistent entièrement ou principalement en la transmission de signaux par l'intermédiaire de réseaux de télécommunications, entre autres de services de transmission sur les réseaux de radiodiffusion.

Données à caractère personnel

Toutes les informations concernant une personne physique identifiée ou identifiable (ci-après la «personne concernée»); on entend par personne «identifiable» toute personne physique pouvant être identifiée directement ou indirectement, principalement par l'identité (son nom, par exemple), par l'identifiant, par les données de localisation, par l'identifiant en ligne ou par une ou plusieurs caractéristiques particulières qui lui sont attribuées, lesdites caractéristiques étant l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de ladite personne physique.

Objectifs de protection

Les objectifs de protection généraux sont la protection des données à caractère personnel et la protection de la confidentialité des télécommunications. La protection de l'infrastructure des télécommunications contre les dysfonctionnements et les risques et la disponibilité des services de télécommunications sont des objectifs de protection particuliers.

Annexe 1: exigences imposées aux prestataires de services de télécommunications dotés d'une infrastructure IP

Annexe 2: exigences de sécurité supplémentaires relatives aux réseaux et services publics de télécommunications potentiellement exposés à des risques accrus

Catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel

aux termes de
l'article 109 de la loi sur les télécommunications (loi TKG)

Version 2.0

Annexe 1

Exigences imposées aux prestataires de services de télécommunications dotés d'une infrastructure IP

Version: 29.4.2020

Table des matière

s

1 Introduction

La connexion d'un système de télécommunications à Internet ou la fourniture de services de télécommunications sur Internet s'accompagne potentiellement de risques considérables pour les systèmes de télécommunications connectés, les systèmes informatiques connectés et leurs utilisateurs.

Il est par exemple possible d'avoir un aperçu des risques actuels dans les rapports annuels publiés par le BSI[1] et l'ENISA[2].

Les prestataires de services de télécommunications dotés d'une infrastructure IP doivent prendre des mesures de sécurité appropriées en raison de cette situation de risque spécifique et en raison de l'importance d'Internet dans les secteurs professionnels et privés. La présente annexe décrit les mesures techniques et organisationnelles destinées à améliorer la sécurité Internet. Ces mesures doivent être mises en œuvre conformément à l'état actuel de la technique.

Des recommandations supplémentaires sont entre autres disponibles dans la série sur la sécurité Internet (série ISi) et parmi les recommandations du BSI relatives à la cybersécurité destinées aux prestataires de services Internet.

2 Infrastructure

2.1 Routage et protocoles

S'il existe différentes normes ou différents autres protocoles pour la mise en œuvre d'un service, un examen attentif doit permettre de déterminer et de mettre en œuvre la solution qui semble la plus sûre selon l'état de la technique.

2.1.1 Technologie de cryptage

Le prestataire de services de télécommunications doit crypter les données conformément à l'état de la technique aux points qu'il est nécessaire de protéger. Les mots de passe doivent

[1] Rapport annuel du BSI (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html)
[2] «ENISA Threat Landscape Report» (rapport de l'ENISA concernant le panorama des menaces) (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape)

plus particulièrement au moins être traités par hachage et salage, ainsi qu'être enregistrés d'après l'état de la technique.
Outre le cryptage des données elles-mêmes, le cryptage sur l'itinéraire par l'intermédiaire du protocole TLS est également possible. Dans ce cas, le cryptage est transparent pour l'utilisateur (c'est-à-dire qu'il ne requiert pas son intervention). Les protocoles couramment utilisés qui sont compatibles sont les protocoles HTTPS et SMTPS. Le type de cryptage et la gestion des clés qui s'y rattachent doivent être adaptés aux besoins de protection. L'état de la technique doit à cet égard également être pris en compte. La directive technique TR-02102 du BSI offre une aide supplémentaire entre autres.

2.1.2 Protection contre les attaques DoS/DDoS

En général, le prestataire de services de télécommunications doit prendre des mesures pour se défendre (atténuation) contre les attaques DoS/DDoS (attaques par déni de service/déni de service distribué). De tels programmes d'atténuation peuvent être mis en œuvre et exploités soit par l'opérateur Internet lui-même soit par un prestataire de services spécialisé en la matière.

2.1.2.1 Résilience de l'infrastructure face aux attaques DoS/DDoS

L'infrastructure du fournisseur de télécommunications doit être dimensionnée de manière adéquate pour se protéger contre les attaques DDoS. Les capacités des systèmes susceptibles de faire l'objet d'attaques DDoS doivent être conçues de manière à ce que leur opérationnalité soit garantie sans prendre d'autres mesures, même en cas d'attaque moyennement grave.

2.1.2.2 Protection contre l'usurpation d'adresse IP

Pour éviter les attaques par réflexion, par exemple, les prestataires de services de télécommunications dotés d'une infrastructure IP doivent prendre des mesures qui empêchent ou rendent plus difficile la falsification des adresses des expéditeurs. Les exigences applicables sont celles des normes RFC2827 et RFC3704 de la série RFC de l'IETF.

2.1.2.3 Désactiver les services inutilisés

Les prestataires de services de télécommunications doivent protéger leurs propres serveurs contre toute usurpation, par exemple en désactivant les services qui ne sont pas nécessaires.

Leurs clients doivent être informés des ports ouverts et des services accessibles (autodéterminés ou à partir de sources externes) qui présentent potentiellement un risque pour les tiers.

2.1.2.4 Protection des services requis sur le plan opérationnel

Les services nécessaires à l'exploitation du réseau doivent être protégés contre les attaques DoS/DDoS par des mesures et des éléments appropriés.

Un exemple de mesure est l'utilisation de restrictions d'accès ou ACL (liste de droits d'accès).

Les composants peuvent être des routeurs filtrants ou des dispositifs d'atténuation DDoS, par exemple.

2.1.2.5 Détection des botnets (réseaux de machines-zombies)

Les prestataires de services de télécommunications dotés d'une infrastructure IP doivent exploiter un système de détection approprié afin de repérer les botnets en respectant les dispositions de l'article 100, paragraphe 1, de la loi TKG. Dans certains cas, la détection et la limitation de dysfonctionnements conformément à l'article 100, paragraphe 2, de la loi TKG s'effectuent également par une intervention sur les connexions existantes. Cependant, cela peut uniquement se produire s'il existe une nécessité opérationnelle et des moyens plus doux comme une évaluation des données de trafic ou de contrôle d'un protocole informatique ne permettent pas d'atteindre le but. Les dispositions relatives à la protection dans la législation sur la protection des données comme la suppression immédiate des données enregistrées et l'information du mandataire du gouvernement fédéral chargé du contrôle du traitement automatisé des informations nominatives au sein de l'entreprise doivent être respectées (voir article 100, paragraphe 2, de la loi TKG).

2.1.3 Principe de l'égalité de traitement

Le prestataire de services de télécommunications doit transmettre les ensembles de données provenant des clients et allant vers des clients sans les changer et avec les mêmes droits indépendamment de leur origine ou des applications qui ont généré lesdits ensembles. Une exception à cette règle est le service de VoIP (voix sur IP) du prestataire de services de

télécommunications, qui peut être exploité par l'intermédiaire de réseaux distincts et/ou avec une bande passante qui lui est réservée.

2.1.4 Routage interdomaine

Des mesures doivent être prises pour empêcher la manipulation des routes du protocole BGP. Dans le cas présent, il s'agit d'utiliser une RPKI, par exemple.

2.2 Suivi, établissement de rapports et coopération

Pour détecter des attaques ou des erreurs, les données de trafic doivent être régulièrement surveillées afin de détecter toute anomalie dans le cadre des possibilités offertes par la loi et dans la mesure où cela est nécessaire à la fourniture du service concerné. Si des irrégularités sont constatées, des mesures de protection appropriées doivent être prises (par exemple empêcher la communication sur le réseau ou restreindre ou empêcher la communication vers des personnes portant atteinte à la sécurité publique). Dans ce cas, les dispositions applicables sont plus particulièrement celles du RGPD et les dispositions de l'article 100, paragraphe 1, de la loi TKG, ainsi que les mesures de l'article 109a, paragraphes 4 à 6, de la loi TKG. Sur ce point, il faut suivre la recommandation du document d'orientation du BfDI et de la BNetzA pour un enregistrement des données de trafic conforme à la législation sur la protection des données[3] et supprimer les données au bout de 7 jours au plus tard en l'absence d'éléments indiquant des attaques ou erreurs.

Le contenu des télécommunications peut également être enregistré au cas par cas pour identifier et limiter les dysfonctionnements dans les conditions fixées à l'article 100, paragraphe 2, de la loi TKG (voir paragraphe 2.1.2.5 ci-dessus).

En outre, les mesures décrites dans la présente annexe doivent être mises en œuvre afin de pouvoir détecter ou exclure les modifications indésirables apportées par des fabricants, des prestataires de services de gestion ou des acteurs publics (par exemple des pays producteurs).

[3] Voir point B.I.2 du document d'orientation du 19.12.2012.

2.2.1 Mise en place d'une infrastructure de surveillance

2.2.1.1 Portée

Une infrastructure de surveillance appropriée doit être retenue. Elle doit permettre d'identifier et d'éviter les menaces en continu. Une infrastructure de surveillance appropriée doit également prévoir des mesures appropriées pour éliminer les dysfonctionnements qui apparaissent. Les mesures prévues doivent être mises en œuvre concrètement, le cas échéant même dans des délais serrés.

L'infrastructure de surveillance doit recenser tous les composants essentiels au fonctionnement du réseau, ainsi que les composants qui transmettent des données à caractère personnel (par exemple les identifiants d'utilisateurs) à des cocontractants externes, par exemple dans le cadre d'une signalisation entre différents réseaux. Il est possible d'inclure parmi les sources de données appropriées pour surveiller la sécurité les routeurs avec BGP, les serveurs DNS, l'e-mail, le protocole HTTP (S), le protocole SIP(S), le protocole SSH, le protocole IPsec.

Les écarts importants par rapport au fonctionnement normal du réseau (par exemple, les flux de données inhabituels, les ensembles de données atypiques sur certains ports, le comportement critique d'éléments critiques du réseau, etc.) doivent être continuellement enregistrés, analysés et consignés. De plus, il faut veiller à ce que les données soient uniquement enregistrées pour la durée requise. En l'absence d'éléments concrets indiquant la présence d'attaques ou d'erreurs, les données doivent être rendues anonymes au plus tard au bout de 7 jours (par exemple en réalisant des évaluations statistiques) ou supprimées.

2.2.1.2 Outils et documentation

Les outils utilisés à des fins de surveillance doivent enregistrer et évaluer continuellement et automatiquement les paramètres ou caractéristiques des opérations en cours qu'il convient d'enregistrer et d'évaluer. Le mode opératoire, l'association des outils de surveillance et tout traitement des données effectué le cas échéant doivent être consignés dans le programme de sécurité. Les seuils et les paramètres similaires utilisés pour ajuster l'infrastructure de surveillance (par exemple, la fréquence des évènements individuels survenant jusqu'à ce qu'une alarme soit déclenchée, l'ajustement du rapport vrais positifs-faux négatifs) doivent également être consignés.

Il faut également consigner la méthode de contournement des anomalies identifiées. Il convient d'identifier les mesures automatiquement déclenchées par l'infrastructure de surveillance et celles qui déclenchent une alarme entraînant une intervention manuelle.

En outre, l'infrastructure de surveillance doit générer des statistiques isolées pour chaque cas, ce qui permet de dégager le spectre d'un risque ou un mode opératoire spécifique. Si des classificateurs binaires sont utilisés, ils doivent être évalués en examinant les données de référence (TPR, FPR, TNR, FNR) ensemble et en analysant une représentation correspondante (par exemple, courbe ROC).

2.2.1.3 Perfectionnement technique

Les données générées par l'infrastructure de surveillance doivent être régulièrement revues pour optimiser le rapport vrais positifs-faux négatifs. Il faut utiliser des sources de données externes en plus pour identifier les faux négatifs. Dans ces cas, il faut également consigner les mesures prises en vue d'une optimisation (par exemple l'ajustement des seuils, l'enregistrement de paramètres supplémentaires, l'utilisation d'outils de surveillance supplémentaires ou la désactivation d'outils de surveillance qui ne sont plus appropriés) et les éventuelles modifications apportées à l'infrastructure de surveillance.

Une infrastructure de surveillance doit être légalement autorisée et conforme à la législation relative à la protection des données. Du point de vue des obligations légales imposées en matière de télécommunications, la recevabilité juridique d'une infrastructure de surveillance repose sur l'article 100, paragraphes 1 et 2, de la loi TKG.

2.2.2 Enregistrement/journalisation des activités de gestion

Toutes les activités de gestion portant sur les composants du réseau doivent être journalisées et archivées pendant une période suffisamment longue en fonction de leur importance pour la sécurité de l'infrastructure globale afin de pouvoir entre autres reconstituer les éventuels incidents de sécurité par la suite.

2.2.3 Journalisation des fichiers de configuration

La configuration théorique de chaque composant du réseau doit être consignée et mémorisée de façon à être protégée contre tout accès non autorisé.

2.2.4 Comparaison théorie-réalité des composants

L'infrastructure du réseau doit être révisée suffisamment fréquemment. Une telle révision comprend une comparaison théorie-réalité des fichiers de configuration actuels de tous les composants du réseau avec les fichiers de référence archivés conformément au paragraphe 2.2.3.

2.2.5 Test du comportement des composants

Au-delà de la comparaison théorie-réalité des fichiers de configuration, il faut comparer régulièrement le comportement réel et théorique de chacun des composants. Pour cela, il faut définir des scénarios de test décrivant le comportement conforme.

2.2.6 Identification des systèmes infectés et notification du client concernant les risques en cas de détection d'une infection

En plus des précautions susmentionnées pour assurer leur propre protection, les prestataires de services de télécommunications doivent également surveiller le réseau en tenant compte des systèmes infectés des clients. Les mesures nécessaires à cet effet doivent être définies d'après l'état de la technique et en tenant compte des exigences légales. Si le prestataire de services de télécommunications identifie des dysfonctionnements qui émanent des systèmes informatiques d'utilisateurs, il est tenu d'en informer immédiatement les utilisateurs aux termes de l'article 109a, paragraphe 4, de la loi TKG dans la mesure où cela est techniquement possible et raisonnable. Dans ce cas, il doit également indiquer aux utilisateurs les moyens techniques raisonnablement applicables, efficaces et accessibles qui leur permettront d'identifier et d'éliminer ces dysfonctionnements. Les obligations déclaratives imposées par la loi (voir paragraphe 3.5.3 du catalogue) doivent être remplies.

2.2.7 Coopération en cas de dysfonctionnement affectant différents prestataires de services de télécommunications

En cas de dysfonctionnements susceptibles d'affecter plusieurs prestataires de services de télécommunications, par exemple en raison d'attaques DDoS (voir paragraphe 2.1.2 également à ce sujet), il est nécessaire de mettre en place une coopération entre les différents prestataires de services de télécommunications. Cette coopération doit également comprendre un échange entre les différents fournisseurs en ce qui concerne les appareils infectés.

Pour ce faire, les interlocuteurs et les procédures doivent être convenus entre eux en amont. Cela implique également la désignation d'un interlocuteur pour les abus capable de réagir au moins pendant les heures d'ouverture du bureau et qui traitera les notifications entrantes (qui seront le cas échéant automatisées).

Il relève de la responsabilité du prestataire de services de télécommunications de contacter les fournisseurs du réseau afin de déterminer les interlocuteurs appropriés. En contrepartie, ce dernier doit informer immédiatement le premier prestataire de services de télécommunications de tout changement. Il faut toujours veiller à ce qu'un contact direct et immédiat soit possible entre les prestataires de services de télécommunications en cas d'urgence.

2.2.8 Coopération avec les fabricants d'antimalwares

Les fabricants d'antivirus doivent être soutenus pour améliorer les mesures de détection des logiciels malveillants (malwares) le plus rapidement possible grâce à la transmission immédiate d'échantillons des logiciels malveillants.

3 Services aux utilisateurs finaux

3.1 Mesures générales de sécurité

En plus de l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe, si cela est techniquement possible, les clients doivent se voir proposer des méthodes d'authentification forte comme des méthodes d'authentification cryptographique ou des méthodes d'authentification à deux facteurs (possession et connaissance).

3.2 Accès à Internet

3.2.1 Information des nouveaux clients

Les nouveaux clients doivent recevoir par écrit des informations sur les risques sur Internet et sur les protections possibles qu'il existe, ainsi que des indications sur la manière de traiter les logiciels malveillants.

3.2.2 Information du client en cas de suspicion d'infection par un logiciel malveillant

Le client doit être informé en cas de suspicion d'infection par un logiciel malveillant sur son terminal.

3.3 Voix sur IP (VoIP)

3.3.1 Bande passante, disponibilités de numéros d'urgence

Le prestataire de services de télécommunications doit réserver une partie de la bande passante mise à disposition à la communication à l'aide de la technologie de la VoIP. La disponibilité des numéros d'urgence doit avant tout être garantie.

3.3.2 Confidentialité de la communication

En plus du paragraphe 2.1.1, les données de la VoIP doivent être transmises cryptées dans la mesure où cela est techniquement possible et économiquement justifiable tant pour les transmissions entre les réseaux du fournisseur qu'entre l'équipement privé de l'abonné (abrégé CPE en anglais) et l'ordinateur monocarte (abrégé SBC en anglais et ci-après) du fournisseur; si l'équipement privé de l'abonné réunit les conditions techniques préalables à cette fin.

3.3.3 Transmission du numéro de téléphone

La signalisation utilisée pour la présentation de la ligne appelante (abrégée «CLIP» en anglais) ou le refus de présentation de la ligne appelante (abrégé «CLIR» en anglais) doit être correctement réglée pour les appels sortants et correctement prise en compte pour les appels entrants. En outre, le numéro fourni par le réseau (network provided number) et le numéro spécifique au client (user provided number) doivent être transmis correctement.

3.3.4 Protection contre les TDOS

Dans la mesure où cela est techniquement possible et économiquement raisonnable, les prestataires de services de télécommunications doivent être en mesure de détecter et d'empêcher les appels en masse automatisés vers une ligne ayant pour but de la paralyser (appelés des attaques TDOS), par exemple en effectuant une surveillance appropriée au niveau du SBC.

3.4 Services DNS

3.4.1 Protection contre l'usurpation et les complications d'attaques par réflexion/amplification

Pour se protéger contre les requêtes DNS usurpées, les prestataires de services de télécommunications doivent s'assurer que les résolveurs DNS, dans la mesure où ils sont sous leur propre responsabilité opérationnelle, ne sont pas ouvertement accessibles («open resolver»), mais que l'accessibilité est limitée à leur propre clientèle. Il faut assurer une surveillance permanente du serveur DNS afin de pouvoir détecter les attaques par réflexion/amplification suffisamment tôt. Cela permet d'en déduire des préconisations, par exemple, lors d'une multiplication des requêtes provenant de certaines sources, concernant certains enregistrements de ressources, des requêtes récursives non autorisées, entre autres. Dans ces cas, des contre-mesures doivent être prises, comme la restriction et le filtrage des requêtes. Cela s'applique également aux services comme le NTP, le SSDP, etc., qui sont également de plus en plus usurpés pour des attaques par réflexion.

3.4.2 Protection contre l'empoisonnement du cache DNS

Pour augmenter la résistance du serveur aux attaques par empoisonnement du cache DNS, il faut activer la randomisation des ports. Le volume du trafic doit être surveillé régulièrement afin de détecter les attaques par empoisonnement du cache DNS suffisamment tôt. Une attaque par empoisonnement du cache DNS est en outre possible malgré l'activation de la randomisation des ports, en particulier pour les résolveurs DNS connectés à large bande. Pour réduire le risque, il faut également définir des plafonds pour la durée de conservation des données mises en mémoire tampon dans le cache DNS.

3.4.3 Utilisation de DNSSEC

Les signatures DNSSEC doivent être validées à tous les niveaux au sein de l'infrastructure DNS de l'opérateur de réseau. Le prestataire de services de télécommunications doit expliquer les avantages des DNSSEC à ses clients et les encourager à les utiliser.

4 Acronymes

RFC Document RFC décrivant les normes relatives à Internet

TPR True Positive Rate (taux de vrais positifs)

FPR False Positive Rate (taux de faux positifs)

TNR True Negative Rate (taux de vrais négatifs)

FNR False Negative Rate (taux de faux négatifs)

ROC Receiver Operating Characteristic (fonction d’efficacité d’un récepteur)

Catalogue des exigences de sécurité pour l'exploitation des systèmes de télécommunications et de traitement de données et pour le traitement des données à caractère personnel

aux termes de
l'article 109 de la loi sur les télécommunications (loi TKG)

Version 2.0

Annexe 2

Exigences de sécurité supplémentaires relatives aux réseaux et services publics de télécommunications potentiellement exposés à des risques accrus

Version: 13.5.2020

Table des matières

1 Domaine d’application

Les exigences de sécurité supplémentaires pour les réseaux et services d’une criticité extrême sont décrites ci-après. La série d’exigences de sécurité supplémentaires décrites est basée sur le cycle de vie (production, livraison et mise en service) des éléments à évaluer.

2 Certification des éléments critiques

2.1 Principes fondamentaux

L’autorité nationale responsable de la certification de la sécurité informatique des éléments critiques est l’Office fédéral de la sécurité informatique (BSI). Le BSI est également responsable de l’homologation nationale des organismes de contrôle dans le cadre de la certification nationale de sécurité informatique.

Le BSI élabore et publie une directive technique en concertation avec l’Agence fédérale des réseaux pour les réseaux qui relève du domaine d’application de la présente annexe. Ladite directive contient les exigences applicables pour la certification des éléments critiques, dont les exigences en matière d’environnement d’exploitation et d’exploitation, qui constituent une condition préalable à la validité des certificats. En outre, il décrit les obligations de fourniture de pièces justificatives des certificats conformément au schéma européen de certification (CSA). Les sections ci-dessous décrivent le processus d’identification des éléments critiques et les dispositions réglementant leur utilisation en listant (voir ci-après) les fonctions critiques d’un réseau de télécommunications.

2.2 Liste des fonctions critiques

L’Agence fédérale des réseaux crée un document qui répertorie les fonctions critiques d’un réseau de télécommunications en collaboration avec le BSI.

Les fonctions critiques sont identifiées et ajoutées dans la liste par la BNetzA et le BSI sur la base d’une analyse conjointe des risques et sur la base de l’état actuel de la technique.

La liste est continuellement mise à jour après évaluation de la conformité par la BNetzA et le BSI, surtout si les principales conditions préalables ont changé. À cette occasion, les résultats

des analyses nationales ou internationales des risques comme celles de l'ENISA ou de l'Organe des régulateurs européens des communications électroniques (ORECE) sont pris en compte.

Le BfDI a la possibilité de participer à la création et à la mise à jour de la liste.

Les fabricants, les associations d'opérateurs de réseaux publics de télécommunications et les associations de prestataires de services de télécommunications accessibles au public ont la possibilité de formuler des observations. La liste est publiée au Journal officiel de l'Agence fédérale des réseaux.

2.3 Identification des éléments critiques

Les éléments qui servent partiellement ou totalement à la mise en place de fonctions critiques doivent être identifiés et consignés comme des éléments critiques. L'opérateur de réseau indique l'installation prévue pour l'élément critique au BSI et à la BNetzA.

Disposition transitoire: cette exigence doit être satisfaite au plus tard un an après la publication de la liste des fonctions critiques.

2.4 Certification des éléments critiques

I) Les éléments servant à la mise en place de fonctions critiques peuvent seulement être utilisés si leur sécurité informatique a été contrôlée par un organisme de contrôle et s'ils ont été certifiés par un organisme de certification habilité conformément au règlement (UE) 2019/881 (règlement sur la cybersécurité).

En l'absence de schéma de certification adéquat, les opérateurs de réseau et prestataires de services assujettis doivent prendre temporairement d'autres précautions techniques appropriées et raisonnablement applicables, ainsi que d'autres mesures de protection destinées à prévenir les risques pour toute utilisation d'éléments critique.

Des exigences sont souvent imposées dans le cadre de la certification des produits en ce qui concerne l'environnement d'exploitation ou la sécurité de l'exploitation des produits. Il est uniquement possible de garantir qu'une exploitation est sûre si les obligations décrites dans le certificat ou par le fabricant sont respectées.

Les exigences visées au paragraphe 2.4, en particulier par rapport aux schémas de certification à utiliser, sont précisées dans la directive technique du BSI qui les définit.

II) Dispositions:

Les dispositions applicables en ce qui concerne les exigences relatives à l'utilisation d'éléments critiques certifiés sont listées ci-après.

Mise en service des éléments après le 31.12.2025

Pour les éléments critiques qui sont mis en service après le 31.12.2025, les exigences applicables pour l'utilisation d'éléments critiques certifiés sont celles du paragraphe 2.4, point I.

Mise en service des éléments au plus tard le 31.12.2025

Les éléments critiques qui sont ou ont été mis en service au plus tard le 31.12.2025 doivent satisfaire aux exigences du paragraphe 2.4, point I, à partir du moment où deux produits appropriés dûment certifiés de fabricants différents sont disponibles sur le marché, mais au plus tard le 31.12.2025. Si des produits non certifiés sont utilisés à partir de ce moment et d'ici le 31.12.2025 (inclus), l'assujetti doit le justifier, ainsi que démontrer et prouver qu'aucun risque supplémentaire qui en découle n'est à prévoir et donc qu'aucune atteinte significative à la sécurité ne peut avoir lieu chez l'assujetti aux termes de l'article 109, paragraphe 5, de la loi TKG. Aucune certification ultérieure n'est requise pour les éléments existants qui ne sont plus nouvellement installés. Si un élément critique déjà utilisé sur le réseau ne reçoit pas ou perd la certification, l'élément doit être remplacé sur le réseau d'ici 2025. Il en est de même pour les éléments existants.

L'Agence fédérale des réseaux prend des mesures et d'autres dispositions aux termes de la loi TKG afin de garantir le respect desdites conditions.

3 Fiabilité des fabricants et des fournisseurs

La certification d'un composant ou d'une fonctionnalité critique n'est pas directement liée à la fiabilité de la source d'approvisionnement concernée (fournisseur). Cependant, l'utilisation d'éléments critiques provenant de sources inconnues ou non dignes de confiance peut présenter des risques considérables. Outre la certification, la source d'approvisionnement des éléments

critiques est donc particulièrement essentielle pour toute utilisation dans un environnement sensible.

Un élément critique peut provenir entre autres d'un fabricant (article 434, paragraphe 1, phrase 2, du Code civil) ou d'un vendeur ou fournisseur (article 445a, paragraphe 1, phrase 1, du Code civil). Dans ce contexte, les opérateurs de réseaux publics de télécommunications et les prestataires de services de télécommunications accessibles au public dont la criticité est extrême sont plus particulièrement tenus de sélectionner les fabricants et vendeurs ou fournisseurs d'éléments critiques convenablement avant tout achat. Sélectionner la source d'approvisionnement convenablement présuppose entre autres de vérifier comme il se doit si elle est digne de confiance. L'entreprise obligée doit obtenir une déclaration complète de la source d'approvisionnement comme preuve de fiabilité. La déclaration doit porter sur tous les éléments de sécurité et le cas échéant sur les fonctionnalités liées à la sécurité, ainsi que répertorier la source d'approvisionnement elle-même dans son ensemble (fabricant, dont les sous-traitants et le cas échéant le vendeur ou fournisseur).

Les éléments devant être contenus dans la déclaration de fiabilité d'une source d'approvisionnement sont répertoriés ci-après (liste non exhaustive). Les infractions à l'obligation déclarative doivent être sanctionnées par une pénalité conventionnelle. Les contenus spécifiques doivent être déterminés par l'entreprise assujettie au cas par cas.

1. Obligation de la source d'approvisionnement de coopérer pleinement avec le consommateur sur le plan des techniques de sécurité et en particulier de lui fournir des informations sur les nouveaux produits, les nouvelles technologies et les mises à jour des gammes de produits existantes suffisamment tôt.

2. Assurance fournie par la source d'approvisionnement de la non-transmission à des tiers d'informations provenant des liens juridiques résultant du contrat conclu avec le consommateur ou avec l'un de ses organes.

3. Obligation pour la source d'approvisionnement de garantir par des mesures organisationnelles et juridiques que les informations confidentielles de ou sur son (ses) client(s) ne seront pas transmises à l'étranger de sa propre initiative ou à l'instigation de tiers ou à des organismes étrangers en Allemagne.

4. Assurance fournie par la source d'approvisionnement de sa capacité légale et effective à refuser de transmettre des informations confidentielles de ou sur ses clients à des tiers. Au moment du dépôt de la déclaration, il n'y a plus particulièrement pas d'obligation de divulguer de telles informations à des tiers ou de les rendre accessibles de toute autre manière. Cela n'est pas applicable dès lors qu'il existe à cet effet des obligations légales de divulgation aux fins d'une poursuite pénale, à moins qu'il existe de telles obligations de divulgation vis-à-vis de services étrangers de renseignements ou de police. En cas de doute, la source d'approvisionnement indique l'obligation légale ou les obligations légales de divulgation avant de déposer la déclaration.

5. Obligation pour la source d'approvisionnement de notifier immédiatement l'utilisateur par écrit s'il devient impossible de continuer à garantir le respect de l'obligation déclarée, en particulier si une nécessité ou obligation s'impose à elle ou si elle aurait pu en identifier une qui pourrait l'empêcher de remplir cette obligation.

6. Obligation pour la source d'approvisionnement de fournir sur demande des informations concrètes sur la conception des produits des parties du système relevant des techniques de sécurité.

7. Obligation pour la source d'approvisionnement d'employer uniquement des salariés particulièrement dignes de confiance pour la conception et la fabrication des parties du système qui sont critiques sur le plan de la sécurité.

8. Déclaration pour la source d'approvisionnement affirmant sa disponibilité pour des contrôles de sécurité et des analyses de pénétration sur son produit à l'envergure requise et affirmant la fourniture d'une assistance d'une manière convenable.

9. Assurance fournie par la source d'approvisionnement de l'absence de vulnérabilité mise en œuvre délibérément pour le produit pour lequel la déclaration est délivrée, de la non-installation ultérieure de telles vulnérabilités et de la correction apportée ou qui sera dorénavant immédiatement apportée pour toutes les vulnérabilités involontaires connues.

10. Obligation pour la source d'approvisionnement de signaler immédiatement au consommateur les vulnérabilités ou manipulations connues ou découvertes afin que des mesures puissent être prises suffisamment tôt pour limiter et éliminer les conséquences subséquentes possibles des défauts de qualité. Si le fabricant obtient des informations qui affaiblissent la sécurité et la fonction de ses produits ou qui peuvent avoir une influence négative sur l'exploitation prévue par la disposition, le consommateur doit en être immédiatement notifié. Le fabricant s'engage en outre à proposer immédiatement des solutions.

11. Déclaration expliquant si la source d'approvisionnement peut apporter la garantie suffisante que l'élément critique ne possède aucune propriété technique susceptible d'influencer indûment la sécurité, l'intégrité, la disponibilité ou l'opérationnalité de l'infrastructure critique (par exemple par sabotage ou espionnage) et la manière dont cette garantie peut être apportée.

Les mesures et exigences décrites dans les chapitres suivants peuvent uniquement être mises en œuvre ou satisfaites si elles s'accompagnent de l'assurance que la source d'approvisionnement est digne de confiance.

Les explications s'appliquent mutatis mutandis aux déclarations des fournisseurs, ainsi que toute adaptation.

Sélectionner convenablement fabricants et fournisseurs se poursuit en effectuant un suivi convenable à leur sujet. Si l'entreprise assujettie prend connaissance d'éléments indiquant un non-respect de la déclaration sur l'honneur des fabricants ou fournisseurs, elle doit immédiatement demander que les faits lui soient expliqués et le cas échéant que des mesures appropriées soient prises pour prévenir tout risque. Le non-respect de la déclaration sur l'honneur des fabricants ou fournisseurs peut entraîner des atteintes graves à la sécurité. Cela fait référence à l'obligation de déclarer les atteintes graves réelles ou possibles à la sécurité (article 109, paragraphe 5, de la loi TKG).

4 Intégrité du produit

Tout produit est exposé à différents risques tout au long de son cycle de vie, au cours de différentes phases. Pour réduire ces risques au minimum, des exigences sont fixées ci-après pour les phases particulièrement critiques. Ces exigences concernent l'exploitant, mais également l'étendue fonctionnelle des éléments.

4.1 Généralités

L'opérateur doit être en mesure de vérifier l'intégrité des composants achetés à tout moment, et ce dès leur réception. L'opérateur doit demander les contrôles possibles et les consigner.
Pour que cela soit possible pour l'exploitant, des techniques ou modes opératoires doivent être intégrés au produit et l'approche retenue pour effectuer la vérification doit être correctement consignée.
Les zones présentant des risques pendant la livraison et jusqu'à la mise en service doivent être consignées explicitement et séparément dans le programme de sécurité par l'exploitant en soutien au fabricant. Les zones listées ci-après sont considérées comme particulièrement exposées à des risques.

4.2 Livraison

Il y a livraison dès lors que les éléments sortent du domaine d'action du fabricant. La livraison prend fin au moment de sa réception chez l'opérateur. Durant cette phase comportant des risques, les éléments livrés doivent être protégés contre d'éventuelles manipulations ou autres actions. Cette protection peut être assurée par des mécanismes externes ou propres au produit. Il existe actuellement certaines méthodes élémentaires ou certains modes opératoires de base pour garantir une telle protection. Pour les produits logiciels, une mesure appropriée consiste à utiliser des procédures cryptographiques afin de garantir l'intégrité des produits. Pour le matériel informatique, une protection matérielle appropriée doit être prévue, par exemple des boîtes de transport scellées, un transport surveillé ou une protection interne du produit (cela est par exemple possible pour les cartes SIM). La mise en place précise de ces mécanismes peut par principe être spécifique au fabricant.

4.3 Réception

Il y a réception au sens de la présente annexe 2 si un élément est opérationnel et exempt de défauts après contrôle par l'opérateur qui l'a réceptionné et si l'opérateur déclare expressément la réception de l'élément.

L'opérateur doit plus particulièrement vérifier si les composants en question ont subi des manipulations, des actions ou d'autres modifications durant la livraison. Pour cela, il existe généralement des contrôles adaptés dans le cadre des procédures déjà mentionnées.

4.4 Stockage

Le stockage désigne la partie de la chaîne d'approvisionnement entre la réception et la mise en service. L'intégrité des composants doit également être garantie par l'opérateur durant cette phase comportant des risques. Ceci peut là encore s'effectuer à l'aide de mécanismes externes et/ou propres au produit. Avant tout éventuel stockage, l'intégrité des composants doit être soumise à un test fonctionnel et un contrôle, au moins sur une base aléatoire.

4.5 Mise en service

Il y a mise en service lorsque les éléments sont transférés aux opérations du réseau. L'opérateur doit à nouveau effectuer un contrôle d'intégrité et l'inclure dans la gestion de la configuration. Par principe, des commandes appropriées sont également mises à disposition à cet effet dans le cadre des mécanismes déjà mentionnés.

4.6 Exploitation effective

Voir le chapitre 5 «Exigences de sécurité durant l'exploitation».

4.7 Mise hors service

Des exigences particulières (par exemple la suppression sécurisée des éléments clés, des configurations, des données à caractère personnel comme les données de trafic, etc.) doivent également être prises en compte pour la mise hors service. À cette fin, des techniques adaptées ou des modes opératoires appropriés doivent être intégrés au produit

et l’approche utilisée pour la mise hors service doit être correctement consignée par rapport à l’exploitant.

5 Exigences de sécurité durant l’exploitation

Une mise en service sûre ne garantit pas l’exploitation sûre du réseau public de télécommunications à long terme. Les risques qui surgissent durant l’exploitation sont plutôt d’origines différentes et nouvelles. Pour garantir le respect continu des dispositions de l’article 109, paragraphes 1 à 3, de la loi TKG, l’entreprise assujettie doit donc également prendre des précautions techniques raisonnablement applicables et autres mesures adaptées aux risques. Le recours à des procédures de surveillance est approprié en ce sens.

5.1 Surveillance de la sécurité

L’entreprise assujettie doit mettre en place et faire fonctionner une infrastructure de surveillance afin d’identifier, de limiter ou d’éliminer en permanence les dysfonctionnements ou erreurs des systèmes de télécommunication. Outre les exigences du paragraphe 2.2 de l’«Annexe: Exigences imposées aux prestataires de services de télécommunications dotés d’une infrastructure IP», les exigences listées ci-après sont applicables.

L’infrastructure de surveillance doit transmettre aux cocontractants externes tous les éléments critiques, ainsi que les éléments qui transmettent des données à caractère personnel (par exemple les IMSI, les EDA, les numéros RNIS d’abonnés mobiles, les IIEM), par exemple dans le contexte de la signalisation entre différents réseaux ou de l’itinérance. Les sources de données appropriées pour surveiller la sécurité sont entre autres les serveurs pour le SS7, les adresses poubelles, les projets pilotes d’échange de logiciels, l’échange de données d’itinérance en temps quasi réel et des éléments de l’infrastructure comme le centre de messagerie SMS ou le registre des abonnés nominaux.

Les dysfonctionnements ou erreurs dans les systèmes de télécommunications peuvent par exemple résulter d’attaques DoS et DDoS, de botnets, d’appels indésirables et manqués («Wangiri»), du piratage d’un autocommutateur privé, d’appels ou de SMS entrants en masse à un ou plusieurs abonnés (appel automatisé, pourriel téléphonique), appels ou SMS sortants en masse, falsification potentielle de l’identificateur d’appel, anomalies dans le cadre des

applications proposées (par exemple du domaine de la communication entre machines ou de l'IdO).

Les antennes-relais de téléphonie mobile falsifiées présentent également des risques. Ces risques doivent donc être identifiés par l'intermédiaire d'une infrastructure de surveillance appropriée n'impliquant pas les terminaux (matériel informatique ou logiciels) des utilisateurs.

5.2 Mécanismes cryptographiques et gestion des clés

L'entreprise obligée doit décrire sa gestion des clés dans son programme de sécurité. Le cycle de vie des clés cryptographiques et les mesures techniques et organisationnelles prises pour protéger ces clés doivent être consignés. La documentation doit par exemple englober le matériel clé:

- dans la carte de circuit intégré universel ou carte de circuit intégré universel embarqué, en plus de copies dans l'infrastructure,
- pour chiffrer le SUPI,
- pour l'exploitation dans le cadre du provisionnement à distance du module d'identification de l'abonné (SIM),
- pour le fonctionnement de l'interface N32 et DIAMÈTRE,
- pour l'exploitation de l'infrastructure SIP,
- pour protéger la communication entre les éléments du réseau et,
- pour protéger la communication entre les éléments du réseau et la gestion centrale du réseau

Cette liste fournit une orientation à suivre et ne prétend pas être exhaustive.

Si les clés sont générées par le fournisseur, le processus utilisé pour leur génération doit être consigné. Si des clés confidentielles ou des certificats à clé publique sont transmis à des cocontractants, les mesures de protection utilisées sur le plan technique et organisationnel doivent être consignées.

Le fournisseur doit consigner les algorithmes cryptographiques compatibles servant à protéger la confidentialité et l'intégrité sur l'interface radio en tenant compte de la

configuration adoptée. Si cela est possible, il faut à cette occasion distinguer la strate d'accès de la strate de non-accès, la signalisation des données utilisateur, et les différentes générations de réseau (2G/3G/4G/5G, etc.). S'il y a des différences selon la région géographique, les différences doivent également être consignées.

6 Personnel spécialisé initié

Le personnel spécialisé employé doit avoir les qualifications professionnelles requises pour remplir sa fonction. Cette exigence s'applique déjà par principe. Toutefois, une attention particulière doit être accordée à la détermination du niveau de compétence approprié pour gérer des éléments et fonctionnalités critiques. Il ne suffit pas de simplement connaître des processus techniques pour remplir une fonction liée aux techniques de sécurité avec le potentiel de risque existant. Il est plutôt nécessaire et approprié de disposer des connaissances minimales supplémentaires concernant les scénarios de menace les plus courants pour la confidentialité des télécommunications, la protection des données et l'opérationnalité du réseau.

L'état de la technique évolue aussi activement que les situations à risque qui s'y rattachent. L'entreprise assujettie doit donc non seulement veiller à toujours sélectionner son personnel convenablement, mais également à contrôler continuellement l'aptitude du personnel spécialisé. Le contenu des sessions de formation complémentaire à organiser doit au moins reposer sur l'état de la technique et porter sur l'évolution des situations à risque possibles et connues.

Tous les salariés employés dans le secteur des techniques de sécurité doivent donc être informés régulièrement des responsabilités qui leur incombent dans le cadre de sessions de sensibilisation et de formation.

Les sessions de formation et de sensibilisation doivent être consignées de manière appropriée.

Il faut veiller à ce que les responsabilités et les droits soient clairs et transparents pour tous. Cette transparence peut être obtenue par une description adéquate et accessible de l'organisation et des tâches.

Il faut également accorder une attention à l'adéquation particulière personnelle du personnel employé. En effet, l'exercice d'une fonction liée aux techniques de sécurité nécessite un comportement approprié, en particulier dans les situations exceptionnelles. Le personnel employé doit donc être aussi résilient que nécessaire pour assurer l'exercice de sa fonction

et la prise de décision dans des situations de stress. La participation à des exercices réguliers d'urgence ou de crise peut être utile de ce point de vue.

Le personnel employé doit être digne de confiance. Il faut au minimum donc établir l'identité du personnel concerné avant de l'employer dans le secteur des techniques de sécurité. Un curriculum vitæ pertinent, documenté et vérifié peut apporter une certitude quant à l'origine du personnel employé.

Si le personnel est employé dans des secteurs liés aux techniques de sécurité, il peut être raisonnable d'exiger la présentation d'un certificat de bonne vie et mœurs.

Les violations des règles et les informations inexactes fournies par le personnel de sécurité employé doivent être accompagnées d'une sanction appropriée et reconnue du point de vue du droit du travail. Les violations des règles qui constituent des infractions pénales doivent être signalées en conséquence.

7 Redondances

La compromission technique d'éléments critiques a de graves conséquences. Des précautions techniques appropriées ou d'autres mesures doivent donc être prises pour se prémunir contre les dysfonctionnements et pour maîtriser les risques. Une précaution technique appropriée peut consister à prévoir suffisamment de redondances. Cela est particulièrement vrai lorsque les éléments critiques doivent répondre à des exigences très élevées sur le plan de la disponibilité. Un objectif doit être d'éviter autant que possible les incidents ou du moins de réduire les temps d'arrêt au minimum. Si des manipulations sont détectées, une solution préventive peut être prise en prévoyant suffisamment de redondances.

Une analyse de risque appropriée doit, si possible, permettre de déterminer si la défaillance d'éléments critiques peut être responsable sans menacer les objectifs de protection imposés par la loi et dans quelle mesure. En outre, un contrôle doit être effectué pour déterminer si d'autres solutions techniques appropriées sont possibles en cas de défaillance. Il peut par exemple être utile d'identifier et de déterminer des itinéraires de réseau ou des antennes-relais de téléphonie mobile temporaires en remplacement. Il convient de spécifier et de décrire autant que possible dans le programme de sécurité les éléments du réseau et du système pouvant être activés

immédiatement (et automatiquement) par des éléments de remplacement opérationnels ou en cas de défaillance (hot standby). Il convient également de déterminer et de décrire les composants suffisamment disponibles à court terme parce qu'ils sont conservés adéquatement dans l'entrepôt ou grâce à des accords avec des fournisseurs. Il est à noter que certaines propriétés des réseaux modernes et certains scénarios d'application nécessitent une haute disponibilité des réseaux. Les communications ultra-fiables et à faible latence (abrégées «uRLLC» en anglais) sont par exemple des applications très critiques dans le temps avec une latence faible. Toute défaillance doit donc être exclue dans la mesure du possible. Le programme de sécurité doit prévoir des scénarios d'application adaptés à chaque cas.

Les unités de refroidissement peuvent constituer un exemple de redondance possible. Les armoires de serveurs et les boîtiers multifonctions doivent être surveillés comme il se doit. Les irrégularités doivent déclencher des mesures préventives prédéterminées. La conservation de systèmes de refroidissement redondants (mobiles, par exemple) peut convenir pour prévenir les dysfonctionnements.

8 Diversité

Lors de la planification et de l'installation des réseaux, il faut éviter les «monocultures» en utilisant des éléments critiques de différents fabricants pour le réseau et le système. Il faut donc utiliser des composants ou systèmes d'au moins deux fabricants différents pour le réseau central (réseau fédérateur et réseau central), pour le réseau de transport et pour les réseaux d'accès (réseaux d'accès radioélectrique/réseaux d'accès filaires) sauf si les propres développements de l'Organisation des réseaux multimédias (abrégée «MNO» en allemand) sont utilisés. Ceux-ci doivent être indépendants les uns des autres et au même titre ne pas dépendre d'un organe tiers. Les fonctions et éléments de réseau critiques ne doivent surtout pas dépendre d'un seul fournisseur d'éléments critiques en raison de la topologie de réseau utilisée. Les réseaux doivent être conçus topologiquement de manière à maintenir une diversité, même avec des fonctions et éléments de réseau critiques, c'est-à-dire particulièrement dignes d'être protégées. L'application de standards ouverts comme l'Open RAN pourrait y être favorable si l'état de la technique évolue en conséquence dans les années à venir.

Des mesures doivent être mises au point pour compenser l'indisponibilité à court terme des éléments d'un fabricant afin de maintenir l'opérationnalité du réseau.