Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

JORF n°0225 du 29 Septembre 2018

Le Premier ministre,
Vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ;
Vu le code de la défense, notamment ses articles L. 2321-1, R. * 1132-3 et R. 2321-1 ;
Vu le code général des collectivités territoriales, notamment son article L. 1212-2 ;
Vu le code monétaire et financier, notamment son article L. 614-2 ;
Vu le code de la mutualité, notamment son article L. 411-1 ;
Vu la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, notamment son article 6 ;
Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;
Vu le décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information ;
Vu le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, notamment son article 10 ;
Vu l'avis du conseil national d'évaluation des normes en date du 13 septembre 2018 ;
Vu l'avis du comité consultatif de la législation et de la réglementation financières en date du 12 juillet 2018 ;
Vu l'avis du conseil supérieur de la mutualité en date du 12 juillet 2018,
Arrête :

Article 1

Les règles de sécurité mentionnées à l'article 10 du décret n° 2018-384 du 23 mai 2018 susvisé figurent à l'annexe I du présent arrêté.
Les opérateurs de services essentiels appliquent ces règles de sécurité aux réseaux et systèmes d'information mentionnés à l'article 7 du décret précité, à compter de la date de leur désignation en tant qu'opérateurs de services essentiels dans les délais figurant à l'annexe II du présent arrêté.

Article 2

Le présent arrêté est applicable sur l'ensemble du territoire de la République.

Article 3

Le présent arrêté entre en vigueur le 1er octobre 2018.

Article 4

Le présent arrêté sera publié au Journal officiel de la République française.

ANNEXES

Annexe I

Régles de sécurité

Les présentes règles de sécurité sont applicables aux réseaux et systèmes d'information mentionnés à l'article 7 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique. Ces réseaux et systèmes d'information sont dénommés « systèmes d'information essentiels » dans la présente annexe.

Chapitre Ier : Règles relatives à la gouvernance de la sécurité des réseaux et systèmes d'information

Règle 1. Analyse de risque

L'opérateur de services essentiels effectue et tient à jour, dans le cadre de l'homologation de sécurité prévue à la règle 3, une analyse de risque de ses systèmes d'information essentiels (SIE).
Cette analyse de risque prend notamment en compte l'analyse que l'opérateur a menée pour identifier ses systèmes d'information en tant que SIE.

Règle 2. Politique de sécurité

L'opérateur de services essentiels élabore, tient à jour et met en œuvre une politique de sécurité des réseaux et systèmes d'information (PSSI).
La PSSI décrit l'ensemble des procédures et des moyens organisationnels et techniques mis en œuvre par l'opérateur afin d'assurer la sécurité de ses systèmes d'information essentiels (SIE).
Dans le domaine de la gouvernance de la sécurité, la PSSI définit :
- les objectifs et les orientations stratégiques en matière de sécurité des SIE ;
- l'organisation de la gouvernance de la sécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe (prestataires, fournisseurs, etc.) à l'égard de la sécurité des SIE ;
- les plans de sensibilisation à la sécurité des SIE au profit de l'ensemble du personnel ainsi que des plans de formation à la sécurité des SIE au profit des personnes ayant des responsabilités particulières, notamment les personnes en charge de l'administration et de la sécurité des SIE et les utilisateurs disposant de droits d'accès privilégiés aux SIE ;
- la procédure d'homologation de sécurité des SIE ;
- les procédures de contrôle et d'audit de la sécurité des SIE, notamment celles mises en œuvre dans le cadre de l'homologation de sécurité.
Dans le domaine de la protection, la PSSI définit :
- les mesures de sécurité générales, notamment en matière de gestion et de sécurité des ressources matérielles et logicielles des SIE, de contrôle d'accès aux SIE, d'exploitation et d'administration des SIE et de sécurité des réseaux, des postes de travail et des données ;
- les procédures et les mesures de sécurité physique et environnementale applicables aux SIE ;
- la procédure de maintien en conditions de sécurité des ressources des SIE.
Dans le domaine de la défense, la PSSI définit :
- la procédure de détection des incidents de sécurité ;
- la procédure de traitement des incidents de sécurité.
Dans le domaine de la résilience des activités, la PSSI définit :

- la procédure de gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur les services essentiels de l'opérateur ;
- les procédures de continuité et de reprise d'activité.
La PSSI et ses documents d'application sont approuvés formellement par la direction de l'opérateur.
L'opérateur élabore au profit de sa direction, au moins annuellement, un rapport sur la mise en œuvre de la PSSI et de ses documents d'application. Ce rapport précise notamment l'état des lieux des risques, le niveau de sécurité des SIE et les actions de sécurisation menées et prévues.
L'opérateur tient à la disposition de l'Agence nationale de la sécurité des systèmes d'information la PSSI, ses documents d'application et les rapports sur leur mise en œuvre.

Règle 3. Homologation de sécurité

L'opérateur de services essentiels procède à l'homologation de sécurité de chaque système d'information essentiel (SIE), en mettant en œuvre la procédure d'homologation prévue par sa politique de sécurité des réseaux et systèmes d'information.
L'homologation d'un système est une décision formelle prise par l'opérateur qui atteste que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'opérateur.
Dans le cadre de l'homologation, un audit de la sécurité du SIE doit être réalisé conformément à la règle 5.
L'opérateur prend la décision d'homologuer un SIE sur la base du dossier d'homologation comportant notamment :
- l'analyse de risques et les objectifs de sécurité du SIE ;
- les procédures et les mesures de sécurité appliquées au SIE ;
- les rapports d'audit de la sécurité du SIE ;
- les risques résiduels et les raisons justifiant leur acceptation.
La validité de l'homologation est réexaminée par l'opérateur au moins tous les trois ans et lors de chaque événement ou évolution de nature à modifier le contexte décrit dans le dossier d'homologation. Chaque réexamen de l'homologation est consigné dans le dossier d'homologation.
L'opérateur procède au renouvellement de l'homologation dès qu'elle n'est plus valide.
L'opérateur tient à la disposition de l'Agence nationale de la sécurité des systèmes d'information les décisions et dossiers d'homologation.

Règle 4. Indicateurs

L'opérateur de services essentiels évalue et tient à jour, pour chaque système d'information essentiel (SIE), les indicateurs suivants :
- des indicateurs relatifs au maintien en conditions de sécurité des ressources :
- le pourcentage de postes utilisateurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
- le pourcentage de serveurs dont les ressources systèmes ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
- des indicateurs relatifs aux droits d'accès des utilisateurs et à l'authentification des accès aux ressources :
- le pourcentage d'utilisateurs accédant au SIE au moyen de comptes privilégiés ;
- le pourcentage de ressources dont les éléments secrets d'authentification ne peuvent pas être modifiés par l'opérateur ;
- des indicateurs relatifs à l'administration des ressources :
- le pourcentage de ressources administrées dont l'administration est effectuée à partir d'un compte non spécifique d'administration ;
- le pourcentage de ressources administrées dont l'administration ne peut pas être effectuée au travers d'une liaison réseau physique ou d'une interface d'administration physique.

L'opérateur précise pour chaque indicateur la méthode d'évaluation employée et, le cas échéant, la marge d'incertitude de son évaluation. Lorsqu'un indicateur évolue de façon significative par rapport à l'évaluation précédente, l'opérateur en précise les raisons.
L'opérateur communique à l'Agence nationale de la sécurité des systèmes d'information, à sa demande, les indicateurs mis à jour sur un support électronique.

Règle 5. Audits de la sécurité

L'opérateur de services essentiels réalise, dans le cadre de l'homologation de sécurité prévue à la règle 3, un audit de la sécurité de chaque système d'information essentiel (SIE). L'audit doit aussi être réalisé lors de chaque renouvellement de l'homologation en prenant notamment en compte les résultats de la mise à jour de l'analyse de risque du SIE.
Cet audit vise à vérifier l'application et l'efficacité des mesures de sécurité du SIE et notamment le respect des présentes règles de sécurité. Il doit permettre d'évaluer le niveau de sécurité du SIE au regard des menaces et des vulnérabilités connues et comporte notamment la réalisation d'un audit d'architecture, d'un audit de configuration et d'un audit organisationnel et physique.
L'opérateur ou le prestataire mandaté à cet effet réalise cet audit en s'appuyant sur les exigences du référentiel en matière d'audit de sécurité des systèmes d'information pris en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.
A l'issue de l'audit, l'opérateur ou, le cas échéant, le prestataire élabore un rapport d'audit qui expose les constatations sur les mesures appliquées et sur le respect des présentes règles de sécurité. Le rapport précise si le niveau de sécurité atteint est conforme aux objectifs de sécurité, compte tenu des menaces et des vulnérabilités connues. Il formule des recommandations pour remédier aux éventuelles non-conformités et vulnérabilités découvertes.

Règle 6. Cartographie

L'opérateur de services essentiels élabore et tient à jour, pour chaque système d'information essentiel (SIE), les éléments de cartographie suivants :

- les noms et les fonctions des applications, supportant les activités de l'opérateur, installées sur le SIE ;
- le cas échéant, les plages d'adresses IP de sortie du SIE vers internet ou un réseau tiers, ou accessibles depuis ces réseaux ;
- le cas échéant, les plages d'adresses IP associées aux différents sous-réseaux composant le SIE ;
- la description fonctionnelle et les lieux d'installation du SIE et de ses différents sous-réseaux ;
- la description fonctionnelle des points d'interconnexion du SIE et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ;
- l'inventaire et l'architecture des dispositifs d'administration du SIE permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- la liste des comptes disposant de droits d'accès privilégiés au SIE (appelés « comptes privilégiés »). Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés, notamment les comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de messagerie, comptes de processus, etc.) ;
- l'inventaire, l'architecture et le positionnement des services de résolution de noms d'hôte, de messagerie, de relais internet et d'accès distant mis en œuvre par le SIE.

L'opérateur communique à l'Agence nationale de la sécurité des systèmes d'information, à sa demande, les éléments de cartographie mis à jour sur un support électronique.

Chapitre II : Règles relatives à la protection des réseaux et systèmes d'information

Section 1 : Sécurité de l'architecture

Règle 7. Configuration

L'opérateur de services essentiels respecte les règles suivantes lorsqu'il installe des services et des équipements sur ses systèmes d'information essentiels (SIE) :

- l'opérateur installe sur ses SIE les seuls services et fonctionnalités qui sont indispensables à leur fonctionnement ou à leur sécurité. Il désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'opérateur le mentionne dans le dossier d'homologation du SIE concerné en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre ;
- l'opérateur ne connecte à ses SIE que des équipements, matériels périphériques et supports amovibles dont il assure la gestion et qui sont indispensables au fonctionnement ou à la sécurité de ses SIE ;
- les supports amovibles inscriptibles connectés aux SIE sont utilisés exclusivement pour le fonctionnement, y compris la maintenance et l'administration, ou la sécurité des SIE ;
- l'opérateur procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de code malveillant. L'opérateur met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de code malveillant provenant de ces supports.

Règle 8. Cloisonnement

L'opérateur de services essentiels procède au cloisonnement de ses systèmes d'information essentiels (SIE) afin de limiter la propagation des attaques informatiques au sein de ses systèmes ou ses sous-systèmes. Il respecte les règles suivantes :

- chaque SIE est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes d'information de l'opérateur et des systèmes d'information de tiers ;
- lorsqu'un SIE est lui-même constitué de sous-systèmes, ceux-ci sont cloisonnés entre eux physiquement ou logiquement. Un sous-système peut être constitué pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIE ou encore pour isoler des ressources d'un SIE nécessitant un même besoin de sécurité ;
- seules les interconnexions strictement nécessaires au bon fonctionnement et à la sécurité d'un SIE sont mises en place entre le SIE et les autres systèmes ou entre les sous-systèmes du SIE.

Dans le cas particulier d'une interconnexion entre internet et un SIE nécessaire à la fourniture de services d'hébergement de noms de domaine, d'hébergement de zones de premier niveau, de résolution de noms de domaine ou d'interconnexion par appairage pour l'échange de trafic internet, l'opérateur n'est pas tenu d'assurer un cloisonnement physique ou logique au niveau de cette interconnexion mais met en œuvre des mesures de protection appropriées telles que celles préconisées par l'Agence nationale de la sécurité des systèmes d'information.
Par ailleurs, lorsqu'un service essentiel nécessite que le SIE nécessaire à sa fourniture soit accessible via un réseau public, l'opérateur organise ce SIE, selon le principe de la défense en profondeur, en au moins deux sous-systèmes comme suit :

- un premier sous-système correspondant à la partie du SIE directement accessible via ce réseau public, auquel l'opérateur applique des mesures de cloisonnement appropriées telles que celles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;

- un deuxième sous-système correspondant à la partie interne du SIE auquel l'opérateur applique la présente règle sur le cloisonnement.

L'opérateur décrit dans le dossier d'homologation de chaque SIE les mécanismes de cloisonnement qu'il met en place.

Règle 9. Accès distant

L'opérateur de services essentiels protège les accès à ses systèmes d'information essentiels (SIE) effectués à travers des systèmes d'information tiers.
En particulier, lorsqu'un service essentiel nécessite que le SIE nécessaire à sa fourniture soit accessible via un réseau public, l'opérateur protège cet accès au moyen de mécanismes cryptographiques conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information.
Par ailleurs, lorsque l'opérateur ou un prestataire qu'il a mandaté à cet effet accède à un SIE via un système d'information qui n'est pas sous le contrôle de l'opérateur ou du prestataire, l'opérateur applique ou fait appliquer à son prestataire les règles suivantes :

- l'accès au SIE est protégé par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;
- lorsque l'accès au SIE est effectué depuis un site extérieur à celui de l'opérateur, le mécanisme d'authentification est renforcé en mettant en œuvre une authentification à double facteur (authentification impliquant à la fois un élément secret et un autre élément propre à l'utilisateur), sauf si des raisons techniques ou opérationnelles, précisées dans le dossier d'homologation du SIE, ne le permettent pas ;
- les équipements utilisés pour accéder au SIE sont gérés et configurés par l'opérateur ou, le cas échéant, par le prestataire. Lorsque l'accès au SIE est effectué depuis un site extérieur à celui de l'opérateur, les mémoires de masse de ces équipements sont en permanence protégées par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information.

L'opérateur décrit dans le dossier d'homologation de chaque SIE les mécanismes de protection des accès au SIE qu'il met en place.

Règle 10. Filtrage

L'opérateur de services essentiels met en place des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information essentiels (SIE) afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques. Il respecte les règles suivantes :

- l'opérateur définit les règles de filtrage des flux de données (filtrage sur les adresses réseau, sur les protocoles, sur les numéros de port, etc.) permettant de limiter la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIE ;
- les flux entrants et sortants des SIE ainsi que les flux entre sous-systèmes des SIE sont filtrés au niveau de leurs interconnexions de manière à ne permettre la circulation que des seuls flux strictement nécessaires au fonctionnement et à la sécurité des SIE. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués par défaut ;
- l'opérateur établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées depuis moins d'un an. Cette liste précise pour chaque règle :
- le motif et la date de la mise en œuvre, de la modification ou de la suppression de la règle ;
- les modalités techniques de mise en œuvre de la règle.

Dans le cas particulier d'un SIE nécessaire à la fourniture de service d'interconnexion par appairage pour l'échange de trafic internet, l'opérateur ne met en place de mécanismes de filtrage que pour les

flux de données autres que ceux correspondant au trafic internet proprement dit.
L'opérateur décrit dans le dossier d'homologation de chaque SIE les mécanismes de filtrage qu'il met en place.

Section 2 : Sécurité de l'administration

Règle 11. Comptes d'administration

L'opérateur de services essentiels crée des comptes (appelés « comptes d'administration ») destinés aux seules personnes (appelées « administrateurs ») chargées d'effectuer les opérations d'administration (installation, configuration, gestion, maintenance, supervision, etc.) des ressources de ses systèmes d'information essentiels (SIE).
L'opérateur définit, conformément à sa politique de sécurité des réseaux et systèmes d'information, les règles de gestion et d'attribution des comptes d'administration de ses SIE, et respecte les règles suivantes :

- l'attribution des droits aux administrateurs respecte le principe du moindre privilège (seuls les droits strictement nécessaires sont accordés). En particulier, afin de limiter la portée des droits individuels, ils sont attribués à chaque administrateur en les restreignant autant que possible au périmètre fonctionnel et technique dont cet administrateur est responsable ;
- un compte d'administration est utilisé exclusivement pour se connecter à un système d'information d'administration (système d'information utilisé pour les opérations d'administration des ressources) ou à une ressource administrée ;
- les opérations d'administration sont effectuées exclusivement à partir de comptes d'administration, et inversement, les comptes d'administration sont utilisés exclusivement pour les opérations d'administration ;
- lorsque l'administration d'une ressource ne peut pas techniquement être effectuée à partir d'un compte spécifique d'administration, l'opérateur met en place des mesures permettant d'assurer la traçabilité et le contrôle des opérations d'administration réalisées sur cette ressource et des mesures de réduction du risque lié à l'utilisation d'un compte non spécifique à l'administration. Il décrit dans le dossier d'homologation du SIE concerné ces mesures ainsi que les raisons techniques ayant empêché l'utilisation d'un compte d'administration ;
- l'opérateur établit et tient à jour la liste des comptes d'administration de ses SIE et les gère en tant que comptes privilégiés.

Règle 12. Systèmes d'information d'administration

L'opérateur de services essentiels applique les règles suivantes aux systèmes d'information (appelés « systèmes d'information d'administration ») utilisés pour effectuer l'administration de ses systèmes d'information essentiels (SIE) :

- les ressources matérielles et logicielles des systèmes d'information d'administration sont gérées et configurées par l'opérateur ou, le cas échéant, par le prestataire qu'il a mandaté pour réaliser les opérations d'administration ;
- les ressources matérielles et logicielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des opérations d'administration. Cependant, lorsque des raisons techniques ou organisationnelles le justifient, le poste de travail physique de l'administrateur peut être utilisé pour réaliser des opérations autres que des opérations d'administration. Dans ce cas, des mécanismes de durcissement du système d'exploitation du poste de travail et de cloisonnement doivent être mis en place pour permettre d'isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel utilisé pour les opérations d'administration ;
- un environnement logiciel utilisé pour effectuer des opérations d'administration ne doit pas être

utilisé à d'autres fins, comme l'accès à des sites ou serveurs de messagerie sur internet ;
- un utilisateur ne doit pas se connecter à un système d'information d'administration au moyen d'un environnement logiciel utilisé pour d'autres fonctions que des opérations d'administration ;
- les flux de données associés à des opérations autres que des opérations d'administration doivent, lorsqu'ils transitent sur les systèmes d'information d'administration, être cloisonnés au moyen de mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;
- les systèmes d'information d'administration sont connectés aux ressources du SIE à administrer au travers d'une liaison réseau physique utilisée exclusivement pour les opérations d'administration. Ces ressources sont administrées au travers de leur interface d'administration physique. Lorsque des raisons techniques empêchent d'administrer une ressource au travers d'une liaison réseau physique ou de son interface d'administration physique, l'opérateur met en œuvre des mesures de réduction du risque telles que des mesures de sécurité logique. Dans ce cas, il décrit ces mesures et leurs justifications dans le dossier d'homologation du SIE concerné ;
- lorsqu'ils ne circulent pas dans le système d'information d'administration, les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information. Si le chiffrement et l'authentification de ces flux ne sont pas possibles pour des raisons techniques, l'opérateur met en œuvre des mesures permettant de protéger la confidentialité et l'intégrité de ces flux et de renforcer le contrôle et la traçabilité des opérations d'administration. Dans ce cas, il décrit ces mesures et leurs justifications dans le dossier d'homologation du SIE concerné ;
- les journaux enregistrant les événements générés par les ressources des systèmes d'information d'administration ne contiennent aucun mot de passe ou autre élément secret d'authentification en clair ou sous forme d'empreinte cryptographique.

Section 3 : Gestion des identités et des accès

Règle 13. Identification

L'opérateur de services essentiels crée des comptes individuels pour tous les utilisateurs (y compris les utilisateurs ayant des comptes privilégiés ou des comptes d'administration) et pour les processus automatiques accédant aux ressources de ses systèmes d'information essentiels (SIE).
Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, l'opérateur met en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes. Dans ce cas, l'opérateur décrit ces mesures dans le dossier d'homologation du SIE concerné et les raisons justifiant le recours à des comptes partagés.
Par ailleurs, lorsqu'un service essentiel nécessite de diffuser de l'information au public, l'opérateur n'est pas tenu de créer de comptes pour l'accès du public à cette information.
L'opérateur désactive sans délai les comptes qui ne sont plus nécessaires.

Règle 14. Authentification

L'opérateur de services essentiels protège les accès aux ressources de ses systèmes d'information essentiels (SIE), que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification impliquant un élément secret.
L'opérateur définit, conformément à sa politique de sécurité des réseaux et systèmes d'information, les règles de gestion des éléments secrets d'authentification mis en œuvre dans ses SIE.
Lorsque la ressource le permet techniquement, les éléments secrets d'authentification doivent pouvoir être modifiés par l'opérateur chaque fois que cela est nécessaire. Dans ce cas, l'opérateur respecte les règles suivantes :

- l'opérateur doit modifier les éléments secrets d'authentification lorsqu'ils ont été installés par le fabricant ou le fournisseur de la ressource, avant sa mise en service. A cet effet, l'opérateur s'assure auprès du fabricant ou du fournisseur qu'il dispose des moyens et des droits permettant de réaliser ces opérations ;
- l'élément secret d'authentification d'un compte partagé doit être renouvelé régulièrement et à chaque retrait d'un utilisateur de ce compte ;
- les utilisateurs qui n'en ont pas la responsabilité, ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair ;
- lorsque les éléments secrets d'authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre comptes privilégiés ou entre un compte privilégié et un compte non privilégié;
- lorsque les éléments secrets d'authentification sont des mots de passe, ceux-ci sont conformes aux règles de l'art telles que celles préconisées par l'Agence nationale de la sécurité des systèmes d'information, en matière de complexité (longueur du mot de passe et types de caractères), en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de renouvellement.

Lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'opérateur met en place un contrôle d'accès approprié à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe. L'opérateur décrit dans le dossier d'homologation du SIE concerné ces mesures et les raisons techniques ayant empêché la modification de l'élément secret d'authentification.
Par ailleurs, lorsqu'un service essentiel nécessite de diffuser de l'information au public, l'opérateur n'est pas tenu de mettre en place de mécanismes d'authentification pour l'accès du public à cette information.

Règle 15. Droits d'accès

L'opérateur de services essentiels définit, conformément à sa politique de sécurité des réseaux et systèmes d'information, les règles de gestion et d'attribution des droits d'accès aux ressources de ses systèmes d'information essentiels (SIE), et respecte les règles suivantes :

- l'opérateur n'attribue à un utilisateur ou à un processus automatique les droits d'accès à une ressource que si cet accès est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique ;
- l'opérateur définit les accès aux différentes fonctionnalités de chaque ressource et en attribue les droits uniquement aux utilisateurs et aux processus automatiques qui en ont strictement le besoin ;
- les droits d'accès sont révisés périodiquement, au moins tous les ans, par l'opérateur. Cette révision porte sur les liens entre les comptes, les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet ;
- l'opérateur établit et tient à jour la liste des comptes privilégiés. Toute modification d'un compte privilégié (ajout, suppression, suspension ou modification des droits associés) fait l'objet d'un contrôle formel de l'opérateur destiné à vérifier que les droits d'accès aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège (seuls les droits strictement nécessaires sont accordés) et en cohérence avec les besoins d'utilisation du compte.

Section 4 : Maintien en conditions de sécurité

Règle 16. Procédure de maintien en conditions de sécurité

L'opérateur de services essentiels élabore, tient à jour et met en œuvre une procédure de maintien en conditions de sécurité des ressources matérielles et logicielles de ses systèmes d'information

essentiels (SIE), conformément à sa politique de sécurité des réseaux et systèmes d'information. Cette procédure définit les conditions permettant de maintenir le niveau de sécurité des ressources des SIE en fonction de l'évolution des vulnérabilités et des menaces et précise notamment la politique d'installation de toute nouvelle version et mesure correctrice de sécurité d'une ressource et les vérifications à effectuer avant l'installation. Elle prévoit que :

- l'opérateur se tient informé des vulnérabilités et des mesures correctrices de sécurité susceptibles de concerner les ressources matérielles et logicielles de ses SIE, qui sont diffusées notamment par les fournisseurs ou les fabricants de ces ressources ou par des centres de prévention et d'alerte en matière de cyber sécurité tels que le CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) ;
- sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur installe et maintient toutes les ressources matérielles et logicielles de ses SIE dans des versions supportées par leurs fournisseurs ou leurs fabricants et comportant les mises à jour de sécurité ;
- préalablement à l'installation de toute nouvelle version, l'opérateur s'assure de l'origine de cette version et de son intégrité, et en analyse l'impact sur le SIE concerné d'un point de vue technique et opérationnel ;
- dès qu'il a connaissance d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur en planifie l'installation après avoir effectué les vérifications mentionnées à l'alinéa précédent, et procède à cette installation dans les délais prévus par la procédure de maintien en conditions de sécurité ;
- lorsque des raisons techniques ou opérationnelles le justifient, l'opérateur peut décider, pour certaines ressources de ses SIE, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'opérateur met en œuvre des mesures techniques ou organisationnelles prévues par la procédure de maintien en conditions de sécurité pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues. L'opérateur décrit dans le dossier d'homologation du SIE concerné ces mesures de réduction des risques et les raisons techniques ou opérationnelles ayant empêché l'installation d'une version supportée ou d'une mesure correctrice de sécurité.

Section 5 : Sécurité physique et environnementale

Règle 17. Sécurité physique et environnementale

L'opérateur de services essentiels définit et met en œuvre, conformément à sa politique de sécurité des réseaux et systèmes d'information, les procédures et les mesures de sécurité physique et environnementale applicables à ses systèmes d'information essentiels (SIE). Ces procédures et mesures portent notamment sur le contrôle du personnel interne et du personnel externe, le contrôle d'accès physique aux SIE et, le cas échéant, la protection des SIE contre les risques environnementaux tels que les catastrophes naturelles.

Chapitre III : Règles relatives à la défense des réseaux et systèmes d'information

Section 1 : Détection des incidents de sécurité

Règle 18. Détection

L'opérateur de services essentiels élabore, tient à jour et met en œuvre, conformément à sa politique de sécurité des réseaux et systèmes d'information, une procédure de détection des incidents de

sécurité affectant ses systèmes d'information essentiels (SIE).
Cette procédure prévoit des mesures organisationnelles et techniques destinées à détecter les incidents de sécurité affectant les SIE. Les mesures organisationnelles comprennent les modalités d'exploitation des dispositifs de détection et décrivent la chaîne de traitement des événements de sécurité identifiés par ces dispositifs. Les mesures techniques précisent la nature et le positionnement des dispositifs de détection.
L'opérateur met en œuvre des dispositifs de détection capables d'identifier des événements caractéristiques d'un incident de sécurité notamment d'une attaque en cours ou à venir et de permettre la recherche de traces d'incidents antérieurs. A cet effet, ces dispositifs :

- collectent les données pertinentes sur le fonctionnement de chaque SIE (notamment des données « réseau » ou des données « système ») à partir de capteurs positionnés de manière à identifier les événements de sécurité liés à l'ensemble des flux de données échangés entre les SIE et les systèmes d'information tiers à ceux de l'opérateur ;
- analysent les données issues des capteurs notamment en recherchant des marqueurs techniques d'attaques connus, dans le but d'identifier les événements de sécurité et de les caractériser ;
- archivent les métadonnées des événements identifiés afin de permettre une recherche a posteriori de marqueurs techniques d'attaques ou de compromission sur une durée d'au moins six mois.

Dans le cas particulier d'un SIE nécessaire à la fourniture de service d'interconnexion par appairage pour l'échange de trafic internet, l'opérateur ne met en œuvre de dispositifs de détection que pour les flux de données autres que ceux correspondant au trafic internet proprement dit.
L'opérateur ou le prestataire mandaté à cet effet exploite les dispositifs de détection en s'appuyant sur les exigences du référentiel en matière de détection des incidents de sécurité pris en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.
L'opérateur veille en particulier à ce que l'installation et l'exploitation des dispositifs de détection n'affectent pas la sécurité et le fonctionnement de ses SIE.

Règle 19. Journalisation

L'opérateur de services essentiels met en œuvre sur chaque système d'information essentiel (SIE) un système de journalisation qui enregistre les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SIE ainsi qu'au fonctionnement du SIE. Le système de journalisation contribue à la détection d'incidents de sécurité en collectant les données de journalisation.
Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés au premier alinéa :
- les serveurs applicatifs supportant les services essentiels ;
- les serveurs d'infrastructure système ;
- les serveurs d'infrastructure réseau ;
- les équipements de sécurité ;
- les postes d'ingénierie et de maintenance des systèmes industriels ;
- les équipements réseau ;
- les postes d'administration.

Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées. Ils sont, pour chaque SIE, centralisés et archivés pendant une durée d'au moins six mois. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

Règle 20. Corrélation et analyse de journaux

L'opérateur de services essentiels met en œuvre un système de corrélation et d'analyse de journaux qui exploite les événements enregistrés par le système de journalisation installé sur chacun des systèmes d'information essentiels (SIE), afin de détecter des événements susceptibles d'affecter la sécurité des SIE. Le système de corrélation et d'analyse de journaux contribue à la détection d'incidents de sécurité en analysant les données de journalisation.
Le système de corrélation et d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection d'événements susceptibles d'affecter la sécurité des systèmes d'information.
L'opérateur ou le prestataire mandaté à cet effet installe et exploite ce système de corrélation et d'analyse de journaux en s'appuyant sur les exigences du référentiel en matière de détection des incidents de sécurité pris en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

Section 2 : Gestion des incidents de sécurité

Règle 21. Réponse aux incidents

L'opérateur de services essentiels élabore, tient à jour et met en œuvre, conformément à sa politique de sécurité des réseaux et systèmes d'information, une procédure de traitement des incidents de sécurité affectant ses systèmes d'information essentiels (SIE).
L'opérateur ou le prestataire mandaté à cet effet procède au traitement des incidents en s'appuyant sur les exigences du référentiel en matière de réponse aux incidents de sécurité pris en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.
Un système d'information spécifique doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système est cloisonné vis-à-vis du SIE concerné par l'incident.
L'opérateur conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'au moins six mois. Il tient ces relevés techniques à la disposition de l'Agence nationale de la sécurité des systèmes d'information.

Règle 22. Traitement des alertes

L'opérateur de services essentiels met en place un service lui permettant de prendre connaissance, dans les meilleurs délais, d'informations transmises par l'Agence nationale de la sécurité des systèmes d'information relatives à des incidents, des vulnérabilités et des menaces. Il met en œuvre une procédure pour traiter les informations ainsi reçues et le cas échéant prendre les mesures de sécurité nécessaires à la protection de ses systèmes d'information essentiels (SIE).
L'opérateur communique à l'Agence nationale de la sécurité des systèmes d'information les coordonnées (nom du service, numéro de téléphone et adresse électronique) tenues à jour du service prévu à l'alinéa précédent.

Chapitre IV : Règles relatives à la résilience des activités

Règle 23. Gestion de crises

L'opérateur de services essentiels élabore, tient à jour et met en œuvre, conformément à sa politique de sécurité des réseaux et systèmes d'information, une procédure de gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur les services essentiels de l'opérateur.
Cette procédure décrit l'organisation de la gestion de crises mise en place par l'opérateur et prévoit notamment l'application des mesures techniques suivantes aux systèmes d'information essentiels (SIE) :
- configurer les SIE de manière à éviter les attaques ou à en limiter les effets. Cette configuration peut viser :
- à proscrire l'utilisation de supports de stockage amovibles ou la connexion d'équipements nomades aux SIE ;
- à installer une mesure correctrice de sécurité sur un SIE particulier ;
- à restreindre le routage ;
- mettre en place des règles de filtrage sur les réseaux ou des configurations particulières sur les équipements terminaux. Cette mesure peut viser :
- à effectuer des restrictions d'accès sous forme de listes blanches et de listes noires d'utilisateurs ;
- à bloquer les échanges de fichiers d'un type particulier ;
- à isoler de tout réseau des sites internet, des applications, ou des équipements informatiques de l'opérateur ;
- isoler du réseau internet les SIE de l'opérateur. Cette mesure impose de déconnecter physiquement ou logiquement les interfaces réseau des SIE concernés.

La procédure précise les conditions dans lesquelles ces mesures peuvent être appliquées compte tenu des contraintes techniques et organisationnelles de mise en œuvre.

Annexe II

Délais d'application des règles de sécurité

REGLES DE SECURITE	DELAIS D'APPLICATION (à compter de la date de désignation de l'opérateur en tant qu'opérateur de services essentiels)
Règle 1. Analyse de risque	Délai prévu pour l'homologation de sécurité (délai de la règle 3)
Règle 2. Politique de sécurité	1 an
Règle 3. Homologation de sécurité	3 ans pour un système d'information essentiel (SIE) mis en service antérieurement à la date de désignation de l'opérateur de services essentiels. 2 ans pour un SIE mis en service dans un délai de 2 ans à compter de la date de désignation de l'opérateur de services essentiels. Avant sa mise en service pour un SIE mis en service dans un délai supérieur à 2 ans à compter de la date de désignation de l'opérateur de services essentiels.
Règle 4. Indicateurs	2 ans
Règle 5. Audits de la sécurité	Délai prévu pour l'homologation de sécurité (délai de la règle 3)
Règle 6. Cartographie	1 an
Règle 7. Configuration	1 an
Règle 8. Cloisonnement	2 ans
Règle 9. Accès distant	2 ans

Règle 10. Filtrage	**2 ans**
Règle 11. Comptes d'administration	**2 ans**
Règle 12. Systèmes d'information d'administration	**2 ans**
Règle 13. Identification	**1 an**
Règle 14. Authentification	**1 an**
Règle 15. Droits d'accès	**1 an**
Règle 16. Procédure de maintien en conditions de sécurité	**1 an**
Règle 17. Sécurité physique et environnementale	**1 an**
Règle 18. Détection	**2 ans**
Règle 19. Journalisation	**1 an**
Règle 20. Corrélation et analyse de journaux	**2 ans**
Règle 21. Réponse aux incidents	**1 an**

Règle 22. Traitement des alertes	**3 mois**
Règle 23. Gestion de crises	**1 an**

Faite le 14 septembre 2018.