Nations Unies ECE/TRANS/WP.30/GE.1/2021/34

Conseil économique et social

Distr. générale
18 mai 2021
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des problèmes douaniers intéressant les transports

Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR

Deuxième session
Genève, 25-28 mai 2021
Point 6 d) de l'ordre du jour provisoire
Version 4.3 de la documentation sur les concepts, les fonctions et les techniques eTIR : Spécifications techniques du système eTIR

Sécurité du système eTIR*

Note du Secrétariat

I. Mandat

1. À sa quatre-vingt-deuxième session (23-28 février 2020), le Comité des transports intérieurs a approuvé la création du Groupe d'experts des aspects théoriques et techniques de l'informatisation du régime TIR (WP.30/GE.1) (ECE/TRANS/294, par. 84[1]) et approuvé son mandat[2] (ECE/TRANS/WP30/2019/9 et ECE/TRANS/WP.30/2019/9/Corr.1), sous réserve de l'accord du Comité exécutif de la Commission économique pour l'Europe (CEE). Lors de la réunion informelle qu'il a tenue à distance le 20 mai 2020, le Comité exécutif a approuvé la création du WP.30/GE.1 et son fonctionnement jusqu'en 2022, sur la base du cahier des charges énoncé dans le document ECE/TRANS/WP.30/2019/9 et Corr.1, tel qu'il figure dans le document ECE/TRANS/294 (ECE/EX/2020/L.2, par. 5(b))[3].

2. Le mandat du Groupe dispose que celui-ci doit concentrer ses travaux sur le développement d'une nouvelle version des spécifications eTIR, en attendant la mise en place officielle de l'Organe de mise en œuvre technique (TIB). Plus précisément, le Groupe est

* Le présent document a été soumis tardivement aux services de traitement de la documentation en raison de contretemps liés à sa mise au point.

[1] Décision du Comité des transports intérieurs, ECE/TRANS/294, par. 84 − www.unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294f.pdf.

[2] Mandat du Groupe nouvellement créé, approuvé par le Comité des transports intérieurs et le Comité exécutif de la CEE − https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09f.pdf et rectificatif ; www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09c1f.pdf.

[3] Décision du Comité exécutif, ECE/EX/2020/L.2, par. 5 b) − www.unece.org/fileadmin/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/Item_4_ECE_EX_2020_L.2_ITC_Sub_bodies_E.pdf.

Merci de recycler

chargé : a) d'établir une nouvelle version des spécifications techniques de la procédure eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications fonctionnelles de la procédure eTIR ; b) d'établir une nouvelle version des spécifications fonctionnelles du système eTIR, avec les modifications à y apporter, en veillant à assurer leur conformité avec les spécifications conceptuelles du système eTIR ; c) d'élaborer des amendements aux spécifications conceptuelles du système eTIR, à la demande du Groupe de travail des problèmes douaniers intéressant les transports (WP.30).

3. Le texte du présent document, qui présente tous les aspects de la sécurité du système eTIR, fera partie des spécifications techniques eTIR.

II. Sécurité du système eTIR

4. Le présent chapitre décrit tous les aspects du système eTIR ayant trait à la sécurité informatique. Il y est en particulier question des objectifs et des exigences, ainsi que des mesures et des contrôles mis en place à cet égard. La sécurité étant, en raison de l'importance qu'elle revêt pour les systèmes informatiques d'aujourd'hui, considérée comme un axe fondamental de la conception du système international eTIR, la CEE entend prendre correctement en compte cette question. L'objectif est de préciser de façon exhaustive tous les aspects fondamentaux de la sécurité informatique. Ces éléments devront ensuite être régulièrement examinés et actualisés par le TIB.

5. La sécurité informatique ne concerne pas seulement les logiciels, mais tous les domaines qui peuvent jouer un rôle dans la sécurité d'un système. C'est pourquoi il sera ici question des domaines suivants : la sécurité et la gestion des risques ; la sécurité des biens ; l'architecture et l'ingénierie de la sécurité ; la sécurité des communications et des réseaux ; la gestion des identités et des accès ; l'évaluation et la mise à l'épreuve de la sécurité ; les activités liées à la sécurité ; la sécurité du développement des logiciels.

6. Comme il a été dit au chapitre précédent, qui porte sur les aspects techniques du système international eTIR, le niveau de détail des sections suivantes dépend des éléments décrits et toutes les informations ne peuvent être divulguées pour des raisons de sécurité.

A. Objectifs et principes de la sécurité

1. Classification de l'information et politiques de sécurité

7. Il importe, en préambule à toute discussion relative à la sécurité informatique, de déterminer la sensibilité des informations gérées par les systèmes informatiques. Aux Nations Unies, ces aspects sont régis par la circulaire du Secrétaire général intitulée « Informations sensibles ou confidentielles : classification et maniement »[4]. Les données échangées entre les acteurs du système eTIR ou entre les utilisateurs de la banque de données internationale TIR (ITDB) sont classées dans la catégorie « Confidentiel », telle que définie dans la section 2 de la circulaire.

8. Il est question du niveau de confidentialité, ou il y est fait référence, dans d'autres documents des Nations Unies précisant les règles, les directives et les bonnes pratiques applicables. Ainsi, plusieurs circulaires du Bureau de l'informatique et des communications (OICT) portant sur la sécurité informatique décrivent les contrôles de sécurité qui doivent être effectués pour un niveau donné[5]. Les mesures et les contrôles de sécurité définis dans les spécifications techniques eTIR sont à cet égard aussi stricts que l'exigent les circulaires portant sur la gestion des informations confidentielles.

[4] Voir le document ST/SGB/2007/6.

[5] On trouvera une liste de ces circulaires à l'adresse iseek.un.org/nyc/department/policies.

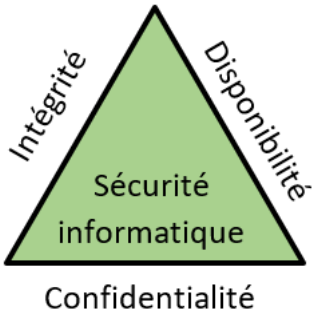
2. Les objectifs de la sécurité

9. La sécurité informatique consiste à atteindre les trois objectifs fondamentaux suivants[6] :

- **L'intégrité** : l'information conserve sa véracité et n'est modifiée intentionnellement que par des sujets autorisés ;
- **La disponibilité** : les sujets autorisés bénéficient d'un accès rapide et permanent aux informations ;
- **La confidentialité** : les informations ne sont pas divulguées à des sujets non autorisés.

10. Ces trois objectifs fondamentaux, tels que représentés dans la figure ci-après, sont les principales composantes de la sécurité informatique. Ils impliquent l'observation de certaines règles lors du développement des systèmes informatiques.

Figure I
Les objectifs fondamentaux de la sécurité informatique

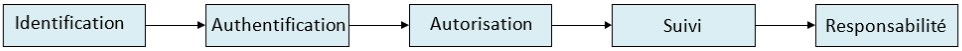


11. Dans le cas du système eTIR, l'atteinte de ces trois objectifs impose des règles strictes. En effet, les données traitées relevant de la catégorie « Confidentiel », leur confidentialité doit être garantie par des contrôles de sécurité appropriés. Étant donné le grand nombre d'acteurs impliqués dans un transport international de marchandises effectué selon la procédure eTIR, le système doit toujours être disponible pour ses utilisateurs. Enfin, il convient de préserver l'intégrité des données transférées entre les différents acteurs pour créer la confiance et pour assurer la non-répudiation.

3. Faire en sorte que les acteurs assument la responsabilité de leurs actions et assurer la non-répudiation

12. Après avoir présenté les notions d'intégrité, de disponibilité et de confidentialité, il est également important de préciser le mode d'identification d'un sujet[7] dans un système et de déterminer de quelle manière on fait en sorte que les acteurs assument la responsabilité de leurs actions et comment est assurée la non-répudiation. On peut résumer cela à une série de cinq étapes, qui est schématisée dans la figure ci-après et présentée dans la suite du document.

Figure II
De l'identification au respect du principe de responsabilité



a) **L'identification**, première étape de la procédure permettant l'application du principe de responsabilité, permet à un sujet de décliner son identité. Un sujet doit s'identifier pour être authentifié par un système. Pour s'identifier, il peut par exemple saisir son nom

[6] On trouvera la définition complète de ces trois termes dans le glossaire technique.
[7] On entend ici par « sujet » une personne ou un système informatique qui tente d'accéder à un système informatique.

d'utilisateur ou positionner un doigt à proximité d'un dispositif de lecture. Le fait que chaque sujet doive posséder une identité unique est un principe fondamental de l'authentification ;

b) **L'authentification** consiste à vérifier ou à mettre à l'essai la validité d'une identité déclarée. Pour être authentifié, un sujet doit fournir des informations supplémentaires correspondant à l'identité qu'il revendique, par exemple un mot de passe ou un certificat numérique. L'authentification consiste à vérifier l'identité du sujet en comparant un ou plusieurs éléments à ceux enregistrés dans la base de données des identités valides (par exemple les comptes utilisateurs) ;

c) **L'autorisation** est le processus qui consiste à accorder l'accès à une ressource ou à un objet, une fois son identité authentifiée. Dans la plupart des cas, le système évalue une matrice de contrôle d'accès qui compare le sujet, l'objet et l'activité prévue. L'autorisation n'est accordée au sujet que si l'action en question est permise ;

d) **Le suivi** permet de connaître et d'enregistrer l'activité d'un sujet afin de pouvoir le tenir responsable de ses actes lorsqu'il est authentifié par un système. Le dispositif de suivi permet également au système de détecter toute activité non autorisée ou anormale ;

d) **La responsabilité** est le principe en vertu duquel les sujets doivent assumer les conséquences de leurs actions. Pour que les sujets puissent être efficacement tenus responsables de leurs actions, il faut être en mesure de prouver leur identité et de suivre leur activité. La responsabilité est avérée lorsqu'on établit un lien entre une personne et les activités d'une identité en ligne au moyen des fonctions de sécurité et des mécanismes de suivi, d'authentification et d'identification.

13. **La non-répudiation** est un objectif de sécurité dérivé important reposant sur le principe selon lequel le sujet à l'origine d'une activité ou d'un événement ne peut pas contester le fait d'être à l'origine de ladite activité. En vertu de ce principe, un sujet ne peut pas prétendre qu'il n'a pas envoyé un message, accompli une action ou été à l'origine d'un événement. Cet objectif est important parce que les informations stockées dans le système international eTIR peuvent être demandées par les Parties contractantes en cas de réclamation[8]. Lorsque sont atteints les objectifs relatifs à la responsabilité des sujets et à l'intégrité des données stockées dans le système international eTIR, l'objectif de non-répudiation est également atteint.

4. Principes relatifs à la sécurité

14. Comme dans le cas des principes directeurs arrêtés pour le développement du système international eTIR, la CEE a fait siens et adopté des principes reconnus et largement appliqués par la communauté des experts en sécurité informatique.

15. Le premier de ces principes est celui de la **diligence raisonnable**. Dans le contexte de la sécurité informatique, cela signifie l'obligation de prendre les précautions qui s'imposent pour protéger les biens d'une organisation de manière continue. Le respect de ce principe exige un niveau élevé d'anticipation et l'instauration d'une culture de la sécurité. La mise en œuvre des principes et des procédures de sécurité dont il est question dans cette partie, ainsi que la réalisation d'audits et d'examens périodiques de la sécurité, garantissent aux acteurs du système eTIR que la CEE prend les mesures qui s'imposent pour respecter son obligation de diligence.

16. Le deuxième principe est celui du **moindre privilège**, en vertu duquel un élément d'une couche d'abstraction donnée d'un environnement informatique (qu'il s'agisse d'un processus, d'un utilisateur ou d'un programme, selon le sujet) ne peut accéder qu'aux informations et ressources correspondant à ses besoins légitimes[9]. Ce principe s'applique également aux fonctionnaires de la CEE chargés d'élaborer et de faire fonctionner le système international eTIR : les autorisations et les accès ne leur sont accordés que de manière sélective pour leur permettre de faire leur travail et un système de contrôle passe régulièrement en revue la liste des autorisations et supprime ces dernières lorsqu'elles ne sont plus nécessaires. À cela s'ajoute le fait que toutes les personnes (fonctionnaires, consultants,

[8] Conformément au paragraphe 3 de l'article 12 de l'annexe 11 de la Convention TIR.

[9] Voir : en.wikipedia.org/wiki/Principle_of_least_privilege.

stagiaires, etc.) cessant de travailler pour la CEE se voient retirer les accès dont elles disposaient. Enfin, des contrôles d'accès physiques et techniques sont également mis en place pour que seules les personnes autorisées aient accès aux informations et aux systèmes leur permettant de faire leur travail.

17. Le troisième principe est celui de la **défense en profondeur**, qui consiste à prévoir des contrôles de sécurité (défenses) à plusieurs niveaux du système informatique. L'idée est de maintenir un niveau de sécurité adéquat dans l'éventualité d'une défaillance d'un contrôle de sécurité ou de l'exploitation d'une vulnérabilité, en ce qui concerne par exemple la sécurité du personnel, des procédures et des aspects techniques ou la sécurité physique[10]. Il est fait usage de ce principe à plusieurs reprises. Ainsi, dans le système international eTIR il existe plusieurs niveaux de validation pour la saisie des données (reçues dans les messages eTIR), l'objectif étant de vérifier leur qualité et leur conformité aux spécifications eTIR.

18. Le quatrième principe est celui de la **partition des tâches**, en vertu duquel une tâche ne peut être effectuée par une seule personne. Pour les activités sensibles, la partition, qui consiste à confier l'exécution d'une même tâche à plus d'une personne, est une mesure de contrôle interne destinée à empêcher les fraudes et les erreurs[11]. Ce principe est utilisé par les développeurs du système international eTIR, par exemple lorsqu'un informaticien examine des lignes de code entrées et validées précédemment par un collègue. Il permet de repérer les omissions et les erreurs éventuelles, qui pourront être immédiatement corrigées par l'auteur du code.

B. Exigences relatives à la sécurité

1. Exigences techniques mentionnées précédemment

19. Comme expliqué au chapitre précédent, la sécurité informatique porte sur un large éventail d'exigences non fonctionnelles (techniques) applicables à un système informatique, car beaucoup jouent un rôle en ce qui concerne un ou plusieurs des trois objectifs principaux que sont l'intégrité, la disponibilité et la confidentialité. En particulier, il est à noter que les exigences suivantes, dont il a déjà été question ailleurs[12], jouent un rôle en dans la sécurité informatique du système eTIR :

- En ce qui concerne la **disponibilité**, qui est l'un des trois principaux objectifs en matière de sécurité et donc l'un des plus importants, les informaticiens doivent accorder une attention particulière aux exigences suivantes : AV.1, AV.2, AV.3 et AV.4 ;
- La **sauvegarde**, avec ses deux exigences (BK.1 et BK.2), est une composante de l'objectif de disponibilité, puisqu'il s'agit de rétablir l'accès des sujets autorisés aux informations en cas de perte de données ;
- La première exigence relative à la **capacité**, CP.1, contribue également à la réalisation de l'objectif de disponibilité, puisqu'elle consiste à faire en sorte que le système international eTIR puisse traiter à tout moment les messages envoyés par les différents acteurs. Il en va de même pour les autres exigences (CP.2, CP.3 et CP.4), quoique dans une moindre mesure ;
- Toutes les exigences relatives à la **gestion de la configuration** (CM.1, CM.2, CM.3, CM.4 et CM.5) ont une incidence sur les trois objectifs (disponibilité, intégrité et confidentialité) dans la mesure où elles ont trait à des aspects importants du développement et de la gestion du système international eTIR ;
- Les exigences relatives à la **conservation des données** (RE.1 et RE.2) ont un lien avec certains aspects précis de l'objectif de disponibilité puisqu'elles permettent de savoir combien de temps les données échangées dans le système eTIR doivent être conservées et comment y accéder ;

[10] Voir : en.wikipedia.org/wiki/Defense_in_depth_(computing).
[11] Voir : en.wikipedia.org/wiki/Separation_of_duties.
[12] Voir le document ECE/TRANS/WP.30/GE.1/2021/31.

- Les exigences en matière de **reprise après sinistre** (DR.1 et DR.2) sont aussi manifestement liées à l'objectif de disponibilité. En effet, elles concernent la remise en marche du système international eTIR en cas de sinistre ;
- Les exigences en matière de **tolérance aux pannes** (FT.1, FT.2, FT.3 et FT.4) qui portent sur certains aspects techniques précis liés aux solutions de secours du système international eTIR, jouent également un rôle en ce qui concerne l'objectif de disponibilité ;
- Les deux premières exigences relatives à la **maintenabilité**, qui concernent la dette technique (MT.1 et MT.2), font partie des mesures préventives mises en place pour éviter les problèmes de sécurité informatique dans le système international eTIR ;
- Comme pour la CP.1, les deux exigences relatives à la **performance** PE.2 et PE.3 relèvent aussi de l'objectif de disponibilité, puisqu'il s'agit de faire en sorte que l'échange de messages entre le système international eTIR et une autre partie prenante eTIR soit toujours effectué dans un délai raisonnable. Les deux dernières exigences relatives à la **performance** (PE.4 et PE.5) font également partie des mesures préventives visant à éviter un éventuel problème du système international eTIR susceptible de compromettre sa disponibilité ;
- La plupart des exigences relatives à la **fiabilité** (RL.1, RL.2, RL.3, RL5 et RL.7) sont également des mécanismes mis en place pour éviter dans la mesure du possible que le système international eTIR connaisse des problèmes susceptibles de compromettre sa disponibilité.

20. Il est évident que la sécurité informatique est un sujet transversal et omniprésent qui ne peut être traités de manière fragmentaire et qu'il est nécessaire, si l'on veut que cette dimension soit prise en compte à toutes les étapes du cycle de développement des logiciels, d'adopter une démarche homogène. Les exigences non fonctionnelles (et pas nécessairement techniques) dont il est question ci-après sont propres à la sécurité informatique. Elles sont généralement applicables à tous les composantes du système eTIR, à savoir le système international eTIR, les systèmes informatiques de toutes les autres Parties prenantes au système eTIR (y compris ceux mis à la disposition des titulaires pour soumettre des renseignements anticipés) et les connexions réseau entre tous ces systèmes. Il est toutefois important de noter que plusieurs de ces exigences peuvent ne s'appliquer qu'à un sous-ensemble desdites composantes.

21. Dans les sections suivantes, on entend par « compte utilisateur » un compte ouvrant à une personne ou à un système informatique l'accès à un système informatique donné (qui utilise et gère ces comptes).

2. Suivi

22. Le tableau ci-après porte sur les exigences liées à l'étape du suivi représentée dans la figure II. Bien que cette exigence s'applique principalement au système international eTIR, il est recommandé de l'appliquer également aux autres systèmes informatiques du système eTIR.

Tableau 1
Exigences relatives au suivi

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AU.1	Toutes les informations envoyées au et reçues par le système international eTIR sont liées à un compte utilisateur et peuvent être vérifiées.	La totalité des messages transmis vers ou reçus par le système eTIR sont entièrement enregistrés, y compris la signature numérique. Ces journaux, qui sont conservés et gérés en toute sécurité dans l'espace de stockage des journaux eTIR, peuvent ensuite être réclamés par les autorités douanières en cas de réclamation.

3. Authentification

23. Le tableau ci-après énumère les exigences liées à l'étape de l'authentification représentée dans la figure II. Seule la première (AE.1) s'applique à l'authentification des acteurs eTIR dans le système international eTIR. Les autres exigences s'appliquent aux autres systèmes informatiques en lien avec le système eTIR.

Tableau 2
Exigences relatives à l'authentification

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AE.1	Choisir pour le système international eTIR un mécanisme d'authentification rigoureux afin d'empêcher tout accès non autorisé.	Les acteurs du système eTIR qui souhaitent accéder aux services Web du système international eTIR doivent s'authentifier à l'aide d'un certificat numérique. La clé privée de ce certificat doit être stockée en toute sécurité par chaque acteur du système eTIR.
AE.2	Activer le verrouillage de la session après une période d'inactivité pour protéger l'accès aux comptes utilisateurs.	Pour les comptes utilisateurs attribués à des personnes uniquement : sur les interfaces mises à la disposition des utilisateurs pour accéder à un système informatique (que ce soit sur une page Web ou sur une application mobile), une période d'inactivité de quinze minutes doit entraîner l'interruption de la session.
AE.3	Gérer les mots de passe de manière sécurisée pour éviter tout accès non autorisé.	Les mots de passe doivent être stockés en toute sécurité dans des bases de données utilisant des fonctions de hachage cryptographiques modernes. Les mots de passe doivent être conformes aux meilleures pratiques en la matière, notamment en ce qui concerne leur longueur minimale et leur complexité.
AE.4	Recommander l'authentification multifactorielle pour l'accès au système afin de protéger les comptes utilisateurs.	S'il y a lieu, les comptes utilisateur attribués à des personnes doivent être dotés d'un système d'authentification multifactorielle, qui peut par exemple reposer sur les deux éléments suivants : « quelque chose que l'utilisateur connaît » (un mot de passe) et « quelque chose que l'utilisateur possède » (une carte de sécurité ou un téléphone mobile).

4. Autorisation

24. Le tableau suivant énumère les exigences liées à l'étape de l'autorisation représentée dans la figure II, pour les systèmes informatiques associés au système eTIR.

Tableau 3
Exigences relatives à l'autorisation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AO.1	N'accorde que l'accès ou les droits strictement nécessaires, de façon à empêcher tout accès non autorisé.	On n'attribuera à un compte utilisateur que l'accès ou les autorisations qui lui sont strictement nécessaires pour obtenir les informations qu'il est habilité à obtenir et pour effectuer les actions qu'il est habilité à accomplir.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AO.2	Utiliser le contrôle d'accès en fonction des rôles pour améliorer la gestion des comptes utilisateur.	S'il y a lieu, les comptes utilisateur doivent se voir accorder des accès et des autorisations en fonction des rôles ou des groupes. Il s'agit d'une façon pérenne de gérer les listes de contrôle d'accès. En effet, l'examen et la mise à jour de l'ensemble des accès et des autorisations est plus facile et présente moins de risques d'erreur lorsqu'ils portent sur tous les membres d'un groupe que sur chaque compte utilisateur.
AO.3	Retirer aux employés l'accès au système à la fin de leur contrat pour empêcher toute intervention non autorisée.	Lorsque le contrat d'un employé se termine, il convient de prévoir des procédures assurant la suppression de ses accès et autorisations à un compte utilisateur. Le compte utilisateur en question doit ensuite être désactivé.
AO.4	Passer en revue les comptes utilisateur au moins une fois par an afin d'éviter le cumul des autorisations d'accès.	Il convient de mettre en place une procédure prévoyant l'examen de tous les comptes utilisateur au moins une fois par an afin de vérifier et de valider que les accès et les autorisations attribués sont justifiés.

5. Sensibilisation et formation

25. Il a déjà été démontré à plusieurs reprises que l'homme est le maillon le plus faible de la chaîne de la sécurité informatique. Il est donc essentiel de sensibiliser et de former le personnel qui doit utiliser les systèmes informatiques en lien avec le système eTIR à la sécurité informatique et aux meilleures pratiques et menaces courantes en la matière. Les humains étant la cible d'attaques spécifiques comme le hameçonnage, le harponnage et le piratage psychologique, il est important d'insister sur ces aspects. Il est donc recommandé à toutes les Parties prenantes au système eTIR de mettre en place de telles mesures.

26. Le tableau suivant énumère les exigences liées aux processus mis en place pour sensibiliser et former l'ensemble du personnel concerné.

Tableau 4
Exigences en matière de sensibilisation et de formation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
AW.1	Sensibiliser l'ensemble du personnel concerné en lui dispensant des formations sur les fondamentaux de la sécurité informatique.	Il convient de proposer au personnel utilisant les systèmes informatiques liés au système eTIR des formations sur les fondamentaux de la sécurité informatique (portant sur les meilleures pratiques et les menaces courantes). Des procédures doivent être mises en place pour faire en sorte que tout le personnel utilisant les systèmes informatiques liés au système eTIR ait suivi ces formations.
AW.2	Tenir des registres de participation aux formations obligatoires.	Ces registres doivent être tenus et gérés de telle façon qu'il soit possible de vérifier que la totalité du personnel utilisant les systèmes informatiques liés au système eTIR a bénéficié d'une formation sur les fondamentaux de la sécurité informatique. L'idéal serait que ces formations soient dispensées périodiquement (tous les trois ans, par exemple).

6. Confidentialité

27. Les informations échangées avec le système eTIR et stockées dans celui-ci sont confidentielles. Il convient par conséquent de mettre en place des mesures de contrôle pour faire en sorte que les données soient à l'abri de tout accès non autorisé lorsqu'elles sont échangées avec le système international eTIR (données échangées) et lorsqu'elles y sont stockées (données stockées). On trouvera dans le tableau ci-dessous la liste des exigences relatives à la confidentialité dans le système international eTIR.

Tableau 5
Exigences relatives à la confidentialité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
CO.1	Les informations transférées entre les systèmes informatiques du système eTIR restent confidentielles.	Tous les messages échangés entre les systèmes informatiques du système eTIR sont cryptés à l'aide de protocoles et de mécanismes de cryptage considérés comme sécurisés par la communauté des professionnels de la sécurité informatique[13]. Ces protocoles et mécanismes doivent être mentionnés dans les spécifications techniques eTIR et leur liste doit être régulièrement examinée pour que ceux qui ne sont plus considérés comme sûrs soient retirés et remplacés par des dispositifs plus sécurisés.
CO.2	L'accès aux informations stockées dans le système international eTIR est restreint.	L'accès aux informations enregistrées dans les trois espaces de stockage du système international eTIR (base de données eTIR, documents eTIR et journaux eTIR) est limité aux seuls comptes utilisateur autorisés. Ces espaces de stockage sont situés dans un environnement sécurisé protégé par des contrôles de sécurité physiques et logiciels.

7. Identification

28. Le tableau qui suit énumère les exigences liées à l'étape de l'identification représentée dans la figure II, pour les systèmes informatiques associés au système eTIR.

Tableau 6
Exigence relative à l'identification

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
ID.1	L'identification d'une personne ou d'un système informatique bénéficiant d'un compte utilisateur est unique, ce qui permet de tenir le détenteur du compte responsable de ses actions.	Un compte utilisateur doit être attribué et lié à une seule personne et non à un groupe d'utilisateurs (s'il s'agit de personnes) ou à un système d'information unique (dans le cas des systèmes). Un même système informatique doit avoir une identité différente dans chaque environnement utilisé (développement, tests d'acceptation et production).

[13] Cette « communauté » comprend les organismes nationaux spécialisées dans la sécurité informatique qui publient régulièrement sur le sujet, ainsi que les experts et les chercheurs en informatique spécialisés dans ce domaine.

8. Intégrité

29. L'intégrité des informations échangées et stockées dans le système international eTIR doit être préservée. Il est donc nécessaire de mettre en place des contrôles pour empêcher toute modification des données, quelle que soit l'origine de cette modification (erreur lors du transfert des données, erreur humaine, mauvaise configuration ou cyberattaque). On trouvera dans le tableau ci-dessous la liste des exigences relatives à la confidentialité dans le système international eTIR.

Tableau 7
Exigences relatives à l'intégrité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
IN.1	L'intégrité des informations transférées entre les systèmes informatiques du système international eTIR est assurée.	Tous les messages envoyés vers ou reçus par le système international eTIR sont signés numériquement par l'expéditeur. Le destinataire valide la signature électronique du message à sa réception et la rejette si elle n'est pas valide.
IN.2	L'intégrité des informations stockées dans le système eTIR est assurée.	La totalité des messages envoyés vers ou reçus par le système eTIR est intégralement enregistrée, y compris la signature numérique. Ces journaux sont ensuite conservés et gérés en toute sécurité dans l'espace de stockage des journaux eTIR, dont l'accès est restreint.

9. Sécurité des nœuds

30. Le terme nœud désigne, selon la définition figurant dans la section consacrée à l'architecture, tout dispositif, physique ou virtuel, qui héberge les programmes ou les informations composant le système international eTIR ou interagit avec eux. Il peut s'agir de serveurs virtuels hébergeant les différents composants logiciels du système international eTIR ou de dispositifs faisant partie de l'infrastructure du réseau, comme les pare-feu, les routeurs, les proxies, les proxies inverses, ou de dispositifs affectés à la sécurité informatique tels que les systèmes de détection ou de prévention des intrusions. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la sécurité des nœuds dans le système international eTIR.

Tableau 8
Exigences relatives à la sécurité des nœuds

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NS.1	Configurer les serveurs virtuels, les conteneurs ou les pods de manière sécurisée pour empêcher tout accès non autorisé.	On s'assurera que toutes les recommandations relatives à la sécurité de l'information formulées par les fournisseurs du système d'exploitation sont appliquées. Les moyens d'identification électronique des comptes de service de ces serveurs sont conservés en toute sécurité dans un système de gestion des mots de passe et ne sont accessibles qu'au personnel autorisé. S'il y a lieu, on activera le pare-feu logiciel et on mettra en œuvre les principes du blocage par défaut et du moindre privilège.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NS.2	Configurer les périphériques de l'infrastructure réseau de manière sécurisée pour empêcher tout accès non autorisé.	Appliquer les principes du blocage par défaut et du moindre privilège sur les périphériques réseau tels que les pare-feu. S'assurer que toutes les recommandations des fournisseurs sont appliquées. Disposer d'une documentation fiable sur les interconnexions de réseaux et la configuration des dispositifs. Ces actions sont effectuées par l'entité hôte.
NS.3	Isoler les réseaux dignes de confiance contenant des données sensibles des réseaux non dignes de confiance pour empêcher tout accès non autorisé.	Appliquer les meilleures pratiques en matière de conception de l'infrastructure de réseau en répartissant les serveurs dans différentes zones de sécurité, en fonction de leur rôle et de la sensibilité des informations qui y sont stockées. Mettre en place une liste blanche d'adresses IP, de telle façon que l'accès au système international eTIR soit interdit par défaut, sauf aux serveurs externes figurant sur une liste précise (parties prenantes eTIR). Ces actions sont effectuées par l'entité hôte.
NS.4	Observer ce qui se passe sur les nœuds pour détecter d'éventuels problèmes de sécurité.	Activer la journalisation pour les nœuds qui la prennent en charge et diriger les données vers le système de surveillance. Restreindre l'accès aux journaux aux seuls employés autorisés. Protéger les données des journaux contre les modifications non autorisées et les problèmes de fonctionnement. Configurer des alertes automatiques fondées sur des règles, y compris pour les échecs de journalisation.

10. Non-répudiation

31. On trouvera dans le tableau ci-dessous la liste des exigences relatives à la non-répudiation dans le système international eTIR.

Tableau 9
Exigences relatives à la non-répudiation

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NR.1	Les Parties prenantes au système eTIR sont responsables des messages qu'elles envoient au système international eTIR.	Lorsqu'elles envoient des messages au système international eTIR, les Parties prenantes au système eTIR doivent les signer électroniquement de façon à être identifiées et authentifiées avec certitude. En outre, la condition AU.1 doit être remplie.
NR.2	L'intégrité du message envoyé par les parties prenantes eTIR au système international eTIR est assurée.	Il doit être satisfait aux exigences IN.1 et IN.2.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
NR.3	Le système international eTIR peut continuer à valider les messages stockés dans les journaux eTIR jusqu'à la fin de la période de conservation des données.	Les certificats numériques devant être renouvelés périodiquement, un système de gestion des clés doit être mis en place pour conserver les anciens certificats numériques de toutes les Parties prenantes au système eTIR, de façon à pouvoir continuer à authentifier et à vérifier l'intégrité des messages échangés dans le passé et conservés dans les journaux eTIR.

11. Sécurité physique

32. Cette section regroupe les principales exigences relatives à la sécurité physique des locaux, des bâtiments et des infrastructures de l'Organisation des Nations Unies (ONU) hébergeant le système international eTIR, et les mesures connexes mises en place. Le tableau ci-après énumère les exigences relatives à la sécurité physique des bâtiments et des infrastructures accueillant le système international eTIR.

Tableau 10
Exigences relatives à la sécurité physique

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
PS.1	Le centre informatique hébergeant le système international eTIR doit être à l'abri de toute perquisition, réquisition ou confiscation, le but étant de protéger les informations qui y sont stockées.	Le système international eTIR est hébergé dans un centre informatique situé dans les locaux de l'ONU et il n'est géré que par des employés de l'Organisation. Il est donc protégé par les dispositions de la Convention sur les privilèges et immunités des Nations Unies.
PS.2	Le centre informatique hébergeant le système international eTIR doit être suffisamment protégé contre les intrusions et les catastrophes.	Les locaux de l'ONU sont entièrement cernés par une clôture, gardés 24 heures sur 24 et 7 jours sur 7 par des agents de sécurité et protégés par un système de vidéosurveillance. Seules les personnes agréées porteuses d'un badge électronique y sont admises. Le centre informatique n'est accessible qu'aux membres d'une petite équipe d'informaticiens accrédités. Il est équipé de systèmes de détection et d'extinction des incendies performants.

12. Codage sécurisé et sécurité logicielle

33. Le codage sécurisé est l'art de développer des logiciels de façon à éviter qu'ils ne soient accidentellement porteurs de failles de sécurité. Les erreurs et les failles logiques sont à l'origine de la plupart des vulnérabilités logicielles couramment exploitées. On trouvera dans le tableau ci-dessous la liste des exigences relatives au codage sécurisé et à la sécurité des applications dans le système international eTIR.

Tableau 11
Exigences relatives au codage sécurisé et à la sécurité des applications

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
SC.1	Définir les exigences en matière de sécurité dès les premières étapes du cycle de développement des logiciels[14] afin de diminuer leur coût et le nombre de problèmes de sécurité.	Prendre en compte tous les aspects liés à la sécurité pour chaque fonctionnalité lors de sa conception et de son ajout à la liste des tâches à effectuer pour le développement du système eTIR. Valider systématiquement les données en entrée avant de les traiter. Concevoir et intégrer des tests de validation axés sur la sécurité (« scénarios criminels »). Effectuer un traitement correct des erreurs afin de toujours laisser le système dans un état stable. Veiller à ce que tous les problèmes de sécurité soient dûment consignés et se voient attribuer le degré de gravité adéquat. Examiner régulièrement le code source pour en éliminer les classes et fonctions inutiles et remanier certaines parties du code.
SC.2	Distinguer les différentes étapes du cycle de développement des logiciels pour éviter de mélanger différentes versions.	Utiliser différents environnements avec des contrôles et des procédures de sécurité appropriés pour les étapes « Développement », « Intégration et test des systèmes », « Tests d'acceptation » et « Production ».

13. Gestion de la vulnérabilité

34. La gestion de la vulnérabilité consiste à repérer, classer, hiérarchiser, corriger et atténuer les vulnérabilités des logiciels. La gestion de la vulnérabilité fait partie intégrante de la sécurité informatique et de la sécurité des réseaux. Elle comprend l'évaluation des vulnérabilités. On trouvera dans le tableau ci-après la liste des exigences relatives à la gestion de la vulnérabilité dans le système international eTIR.

Tableau 12
Exigences relatives à la gestion de la vulnérabilité

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
VU.1	Veiller à ce que les vulnérabilités connues soient corrigées afin d'empêcher d'éventuels problèmes de sécurité.	Mettre à jour et corriger les nœuds, y compris les systèmes d'exploitation et les logiciels médiateurs, de façon régulière. Faire des mises à jour régulières en installant les dernières versions stables des sections des logiciels dépendant de tierces parties. Migrer régulièrement vers les dernières versions des composants des systèmes externes (ITDB, système de courrier et système de non-répudiation).
VU.2	Effectuer des évaluations et des tests de vulnérabilité pour éviter les éventuels problèmes de sécurité.	Analyser régulièrement les nœuds, les systèmes et leurs composants pour y détecter des vulnérabilités connues. Effectuer des examens de sécurité du code (par exemple des tests d'intrusion) pour valider les nouvelles versions du système international eTIR.

[14] Voir en.wikipedia.org/wiki/Systems_development_life_cycle.

Identifiant	*Description et objectif*	*Comment satisfaire à l'exigence*
VU.3	Veiller à ce que les incidents soient correctement gérés afin d'éviter les problèmes de sécurité éventuels.	Les alertes émises par le système de surveillance doivent être analysées en fonction de leur gravité et selon les procédures appropriées. La gestion de chaque incident est étudiée, ce qui permet d'apprendre, d'améliorer et d'effectuer des actions de suivi permettant d'éviter d'autres problèmes similaires.

C. Sécurité du système international eTIR

1. Introduction

35. Le présent chapitre vient compléter les parties précédentes des spécifications techniques. Il a pour objectif d'expliquer aux Parties contractantes à la Convention TIR et aux Parties prenantes au système eTIR divers aspects de la sécurité du système international eTIR. On y montre comment la CEE s'emploie à satisfaire à plusieurs des exigences relatives à la sécurité dont il a été question précédemment. Cette volonté de transparence présente également l'intérêt de permettre à toutes les Parties prenantes au système eTIR de faire des propositions d'amélioration, l'objectif étant de disposer à long terme d'un système eTIR plus sûr.

2. Sensibilisation à la sécurité informatique

36. Il est important de considérer la sécurité informatique comme une chaîne dont le niveau de solidité serait celui de son maillon le plus faible. Étant donné que des êtres humains font partie de cette chaîne, quel que soit le nombre de dispositifs de sécurité ou de barrières logicielles présentes, la sécurité de l'ensemble du système sera menacée si l'élément humain ne dispose pas des connaissances et de l'expérience nécessaires pour comprendre les menaces courantes et savoir comment y faire face.

37. La sensibilisation à la sécurité informatique repose essentiellement sur la prise de conscience des risques que fait planer l'évolution rapide des méthodes de cyberattaque qui ciblent le comportement humain. À l'heure où la menace progresse et où la valeur des informations augmente, les cybercriminels étendent leurs capacités et leurs domaines d'action, développent de nouvelles méthodes et techniques d'attaque et agissent pour des motifs plus variés. Ils ciblent de plus en plus (et exploitent avec succès) le comportement humain individuel pour s'introduire dans les réseaux d'entreprise et les systèmes d'infrastructures critiques. Les personnes visées peuvent ne pas être conscientes de la sensibilité des informations et des menaces et faire l'économie des contrôles et processus de sécurité traditionnels, rendant ainsi leur organisation vulnérable.

38. Pour que les mesures prises dans ce domaine soient efficaces, il importe que tous les employés de la CEE soient sensibilisés à la sécurité informatique, et pas seulement les informaticiens du système international eTIR. En effet, à titre d'exemple, tout employé ouvrant un document infecté par un logiciel malveillant (qui serait par exemple joint à un courriel) est susceptible d'ouvrir une porte dérobée permettant à un cybercriminel de compromettre la sécurité informatique de son organisation. C'est pourquoi le Bureau de l'informatique et des communications a mis sur pied en 2015 un ensemble de trois formations de sensibilisation à la sécurité informatique (niveaux « élémentaire », « avancé » et « complémentaire »). La formation élémentaire est obligatoire pour tous les employés de l'ONU. Elle vise à les sensibiliser et à les familiariser aux mesures à prendre en cas de menace potentielle.

3. Les aspects juridiques

39. La Convention sur les privilèges et immunités des Nations Unies[15], adoptée par l'Assemblée générale des Nations Unies le 13 février 1946 à New York, comporte de nombreuses dispositions relatives au statut de l'Organisation, de ses biens et de ses fonctionnaires, en ce qui concerne les privilèges et immunités qui doivent leur être accordés par les États Membres. L'article 2 de cette convention dispose en particulier que les locaux de l'ONU sont inviolables : Ses biens et avoirs, où qu'ils se trouvent et quel que soit leur détenteur, sont exempts de perquisition, réquisition, confiscation, expropriation ou de toute autre forme de contrainte.

40. Cela signifie en pratique que seuls les agents de sécurité du Département de la sûreté et de la sécurité de l'ONU s'occupent de la sûreté et de la sécurité des biens et des avoirs situés dans les locaux de l'ONU. La police et les autres forces de sécurité du pays hôte ne peuvent pas entrer dans les locaux de l'ONU sans y avoir été autorisées par ces agents de sécurité. Par conséquent, tant que le système international eTIR est hébergé dans un centre informatique situé dans les locaux de l'ONU, il est protégé par les privilèges et immunités décrits ci-dessus.

4. La sécurité physique

41. On entend par mesures de sécurité physique les dispositions prises pour interdire tout accès non autorisé aux installations, aux équipements et aux ressources et pour protéger le personnel et les biens contre tous dommages ou préjudices (tels que les actes d'espionnage, le vol ou les attaques terroristes). La sécurité physique implique le recours à plusieurs strates de systèmes interdépendantes qui peuvent inclure la vidéosurveillance, les agents de sécurité, les barrières de protection, les serrures, le contrôle d'accès, la détection des intrusions dans le périmètre, les dispositifs de dissuasion, la protection contre l'incendie ou tout autre système conçu pour protéger les personnes et les biens. Dans les organismes du système des Nations Unies, cet aspect de la sécurité est assuré par le Département de la sûreté et de la sécurité, qui fournit des services professionnels permettant à l'ONU de mener à bien son action dans le monde entier. Pour des raisons évidentes de sécurité, il ne sera question, dans ce chapitre, que des aspects généraux de la sécurité physique.

42. Les locaux de l'ONU sont entourés d'un périmètre de protection fermé (murs, clôtures, bornes de sécurité, etc.) qui empêche toute personne ou tout véhicule non autorisé d'y pénétrer. Les locaux sont surveillés par des agents de sécurité 24 heures sur 24, d'un bout à l'autre de l'année. Ils sont équipés d'un système de vidéosurveillance contrôlé en permanence par les agents de sécurité, dont les images sont enregistrées en prévision d'éventuelles enquêtes. Seules les personnes autorisées porteuses d'un badge électronique délivré par le Département de la sûreté et de la sécurité y sont admises. Le centre informatique n'est accessible qu'aux membres d'une petite équipe d'informaticiens accrédités et l'emplacement du centre informatique dans les locaux n'est pas connu du public.

43. En outre, des systèmes de détection et d'extinction des incendies équipent l'ensemble des locaux, et en particulier le centre informatique, et des exercices de sécurité sont effectués plusieurs fois par an.

5. L'entité hôte

44. En ce qui concerne l'entité hôte, c'est à dire l'ONU, plusieurs aspects liés à la sécurité ont déjà été décrits dans les parties précédentes des spécifications techniques eTIR :

- La présentation détaillée de l'architecture du système international eTIR[16] montre comment le recours à une infrastructure fondée sur une batterie de serveurs virtuels et à un équilibreur de charge peut jouer un rôle dans la conception d'un système exempt de tout point de défaillance isolé ;

[15] Voir https://treaties.un.org/doc/treaties/1946/12/19461214%2010-17%20pm/ch_iii_1p.pdf.
[16] Voir le document ECE/TRANS/WP.30/GE.1/2021/30.

- Dans les prescriptions techniques[17], le rôle important de l'entité hôte est décrit de façon détaillée au chapitre des exigences relatives à la disponibilité, à la sauvegarde et, surtout, à la tolérance aux pannes, où sont présentées plusieurs caractéristiques du centre informatique ;
- En ce qui concerne la maintenance[18], l'entité hôte joue également un rôle important dans des domaines tels que la gestion des incidents, la sauvegarde et la restauration, la surveillance et la gestion des correctifs et des mises à niveau.

45. L'entité hôte est également responsable de la sécurité générale de son centre informatique, de ses réseaux et de son infrastructure (ainsi qu'il est mentionné plus haut au chapitre des exigences relatives à la sécurité des nœuds). L'idéal serait en outre que l'entité d'hôte, pour démontrer sa maturité et son implication en matière de sécurité informatique, soit détentrice d'un certification reconnue, par exemple selon la norme ISO/IEC 27001:2013.

46. Enfin, étant donné que l'entité hôte est obligée de procéder régulièrement à des modifications sur ses réseaux, son infrastructure et ses nœuds (matériel des réseaux, du système de sécurité ou des serveurs), un processus de gestion des modifications bien défini doit être mis en place pour tester, hiérarchiser, autoriser et mettre en œuvre ces modifications de façon contrôlée et efficace. L'entité hôte doit communiquer avec ses clients de façon appropriée et opportune à propos de ces modifications, et lorsqu'une période d'indisponibilité paraît inévitable il doit en être question à l'avance pour que la recherche de solutions de substitution soit possible ou pour que les parties prenantes eTIR concernées en soient au moins informées. L'idéal serait que la CEE puisse exprimer son point de vue lors de l'autorisation et de la planification des modifications ayant une incidence sur le système international eTIR ou sur l'ITDB, éventuellement en siégeant au Conseil consultatif sur le changement de l'entité hôte.

6. La sécurité logicielle

47. L'un des objectifs de l'approche DevOps (ou DevSecOps) est de penser à la sécurité informatique dès les premières étapes du processus de développement, au lieu de n'en tenir compte qu'à la fin, c'est à dire lorsque il est plus coûteux d'apporter des modifications aux logiciels. Pour atteindre cet objectif, la CEE a adopté les règles suivantes :

- **Prise en compte des exigences relatives à la sécurité en tant que fonctions** : la sécurité et le respect des obligations en la matière ne sont pas des aspects distincts traités à la fin du développement du logiciel ; ils sont au contraire pris en compte pendant le développement et intégrés à la liste des tâches au même titre que les autres fonctions ;
- **Système de validation** : toutes les données en entrée contenues dans les messages eTIR sont validées à plusieurs niveaux, l'objectif étant de vérifier leur exactitude, leur conformité aux spécifications et leur pertinence. Ce système prévoit entre autres une couche de validation pour chaque message de demande, une couche de validation utilisant le fichier XSD correspondant et des contraintes d'intégrité dans la base de données eTIR. En outre, on effectue des tests de validation automatisés avec des données en entrée non conformes, des valeurs nulles ou vides, des valeurs trop longues et certains scénarios criminels[19] ;
- **Traitement des erreurs** : les erreurs survenant pendant le fonctionnement du système international eTIR doivent être traitées comme il se doit pour que le système soit toujours en bon état de fonctionnement. Toutes les erreurs doivent être enregistrées en vue d'une étude plus approfondie. Elles doivent faire l'objet de tests, si possible automatisés, dont le but sera de vérifier que le mécanisme de traitement des erreurs se comporte comme prévu ;

[17] Voir le document ECE/TRANS/WP.30/GE.1/2021/31.

[18] Voir le document ECE/TRANS/WP.30/GE.1/2021/33.

[19] On entend par « scénario criminel » une stratégie qui pourrait être utilisée par des cybercriminels pour violer la sécurité du système international eTIR.

- **Analyse de la vulnérabilité** : on utilise un outil d'analyse statique de code pour vérifier régulièrement le code source afin de détecter les mauvaises pratiques susceptibles de créer des failles de sécurité. En outre, comme de nombreuses bibliothèques sont utilisées de nos jours dans les logiciels, on utilise un outil de vérification pour vérifier la vulnérabilité des versions desdites bibliothèques en consultant une base de données des vulnérabilités connues, afin de repérer les mises à niveau importantes à effectuer pour corriger ces problèmes ;
- **Protéger les outils de développement** : il est important d'assurer la sécurité des outils et des connaissances internes qu'utilisent ou produisent les informaticiens. Tout d'abord, le système de contrôle de version, qui conserve le code source du système international eTIR et de tous les utilitaires connexes. Ensuite, la documentation interne conservée dans le système de gestion des connaissances et dans le système de suivi des problèmes. Enfin, le pipeline d'intégration continue et tous les outils connexes nécessaires aux différents processus de développement, y compris la documentation destinée aux Parties prenantes au système eTIR (comme les guides techniques) ;
- **Télémétrie** : enregistrement du comportement du système international eTIR. Les informaticiens doivent concevoir et mettre en œuvre ce système de telle façon qu'il génère et enregistre des données qui pourront ensuite être analysées dans l'optique, entre autres, d'éviter les incidents (de sécurité). Ces données doivent fournir des informations sur les éléments suivants : succès ou échec de la validation des messages eTIR, utilisation de signatures numériques non valides, erreurs détectées par le système, efficacité du traitement des messages, etc. Toutes les données générées et enregistrées dans les journaux eTIR sont ensuite exploitées et peuvent être visualisées sous forme de graphiques, pour étudier les variations et, si besoin est, déclencher des alertes, sur la base de modèles spécifiques pouvant signaler une cyberattaque éventuelle ;
- **Veille technologique permanente** : les informaticiens doivent suivre régulièrement des formations pour se tenir au courant de l'évolution des technologies et des techniques de sécurisation des logiciels, notamment en étudiant les derniers produits d'entités telles que l'OWASP[20].

7. Évaluations de la sécurité

48. Une évaluation de la sécurité informatique est une étude visant à localiser les vulnérabilités et les risques en matière de sécurité informatique. Elle peut être réalisée en interne par la CEE, par des experts en sécurité informatique de l'ONU, ou encore par des sociétés spécialisées externes mandatées par la CEE. L'objectif d'une évaluation de la sécurité est de faire en sorte que les contrôles de sécurité nécessaires soient intégrés à la conception et à la mise en œuvre du système international eTIR. Une évaluation de la sécurité correctement réalisée doit déboucher sur le signalement des éventuelles failles en matière de sécurité et sur des propositions relatives à la manière d'y remédier. Les résultats des évaluations de la sécurité sont confidentiels.

49. Les informaticiens doivent s'efforcer d'évaluer régulièrement la sécurité, et dans l'idéal d'automatiser certaines de ces évaluations pour qu'elles aient lieu fréquemment. Par exemple, le type d'évaluation de la sécurité baptisé « évaluation de la vulnérabilité », dont le but est d'analyser le code source et les composants logiciels utilisés pour élaborer et faire fonctionner le système international eTIR, doit être automatisé à l'aide d'outils spécifiques et exécuté régulièrement. Les vulnérabilités potentielles pourront ainsi être immédiatement détectées, et corrigées par l'application de correctifs et la mise à niveau des composants logiciels.

[20] L'Open Web Application Security Project® (OWASP) est une fondation à but non lucratif qui s'efforce d'améliorer la sécurité des logiciels. Voir owasp.org.

50. Chaque fois qu'une nouvelle version majeure du système international eTIR est développée, une évaluation plus approfondie de la sécurité doit être menée à bien, soit par des experts en sécurité informatique de l'ONU, soit par une société spécialisée externe mandatée par la CEE. Cette évaluation de la sécurité s'effectue le plus souvent sous la forme de « tests d'intrusion » dans lesquels les personnes chargées des essais jouent le rôle d'agresseurs et tentent de trouver et d'exploiter les failles de sécurité du système international eTIR. En fonction de différents facteurs, on déterminera si ce test essai doit être du type « boîte noire » (Black Box), « boîte grise » (Grey Box), ou « boîte blanche » (White Box). Ces types de test se distinguent par la quantité d'informations dont disposent les personnes chargées des essais. Dans la méthode « boîte noire », elles n'ont aucune connaissance préalable du système qui sera ciblé. Dans le cas d'une évaluation de type « boîte grise », le niveau d'accès au système et sa connaissance ne sont que partiels. Enfin, on parle d'évaluation de type « boîte blanche » lorsque les personnes chargées des essais ont un accès complet au code source, aux diagrammes de réseau et à d'autres informations pertinentes.