Nations Unies ECE/TRANS/WP.30/GE.2/2017/2

Conseil économique et social

Distr. générale
7 mars 2017
Français
Original : russe

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des problèmes douaniers intéressant les transports

Groupe d'experts des aspects juridiques de l'informatisation du régime TIR

Quatrième session
Genève, 16 et 17 mai 2017
Point 4 de l'ordre du jour provisoire
Identification du titulaire et vérification de l'intégrité des messages électroniques d'échange de données

Identification du titulaire et vérification de l'intégrité des messages électroniques d'échange de données

Communication du Gouvernement de la Fédération de Russie*

* Le présent document reproduit tel quel le texte qui a été transmis au secrétariat.

GE.17-03650 (F) 030517 040517
1703650

I. Menaces actuelles pour la sécurité informatique (dans le contexte du traitement automatique des données)

Menace	*Attaque*	*Contexte de l'attaque*	*Cible de l'attaque*	*Source de l'attaque*	*Code menace*
Altération de documents électroniques	Modification du logiciel	En dehors de l'activité du système	Tout poste du réseau local	Même poste du réseau local	I1
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Serveur	Tout poste du réseau local	
	Saisies incorrectes dans des documents électroniques	Durant l'activité du système	Tout poste du réseau local	Même poste du réseau local	I2
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
	Introduction d'un logiciel malveillant	Durant l'activité du système	Tout poste du réseau local	Même poste du réseau local	I3
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Serveur	Tout poste du réseau local	
	Interception de documents électroniques	Durant l'activité du système	Serveur	Tout poste du réseau local	I4
		Au cours d'une transmission de données	Réseau de transmission de données	Nœuds intermédiaires	I5
			Modem	Nœuds intermédiaires	

Menace	*Attaque*	*Contexte de l'attaque*	*Cible de l'attaque*	*Source de l'attaque*	*Code menace*
Introduction d'un document électronique inexistant	Modification du logiciel	En dehors de l'activité du système	Tout poste du réseau local	Même poste du réseau local	I1
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Serveur	Tout poste du réseau local	
	Introduction d'un logiciel malveillant	Durant l'activité du système	Tout poste du réseau local	Même poste du réseau local	I3
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Serveur	Tout poste du réseau local	
	Introduction manuelle	Durant l'activité du système	Serveur	Tout poste du réseau local	I6
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Réseau local	Tout poste du réseau local	
		Au cours d'une transmission de données	Réseau de transmission de données	Nœuds intermédiaires	I7
			Modem	Nœuds intermédiaires	

Menace	*Attaque*	*Contexte de l'attaque*	*Cible de l'attaque*	*Source de l'attaque*	*Code menace*
Violation de la confidentialité de documents électroniques	Modification du logiciel	Comme dans le cas précédent			
	Introduction d'un logiciel malveillant				
	Affichage d'un écran	Durant l'activité du système	Tout poste du réseau local	Tout poste du réseau local	I8
			Serveur de messagerie	Serveur de messagerie	
	Interception de documents électroniques	Durant l'activité du système	Réseau local	Tout poste du réseau local	I4
		Au cours d'une transmission de données	Réseau de transmission de données	Nœuds intermédiaires	I5
			Modem		
	Copie non autorisée	En dehors de l'activité du système	Serveur	Tout poste du réseau local	I9
Refus de réception d'un document électronique	Modification du logiciel	Durant l'activité du système	Tout poste du réseau local	Tout poste du réseau local	I3
			Serveur de messagerie	Serveur de messagerie	
		Au cours d'une transmission de données	Entité douanière extérieure	Entité douanière extérieure	
Répudiation d'un document électronique	Comme dans le cas précédent				I10
Duplication d'un document électronique	Modification du logiciel	Comme dans le cas précédent			I16
	Introduction d'un logiciel malveillant				
	Attaque itérative dans un réseau	Durant l'activité du système ou en dehors de celle-ci	Serveur	Tout poste du réseau local	I12
			Réseau local	Tout poste du réseau local	
			Réseau de transmission de données	Nœuds intermédiaires	
			Modem		

Menace	*Attaque*	*Contexte de l'attaque*	*Cible de l'attaque*	*Source de l'attaque*	*Code menace*
Perte ou suppression d'un document électronique	Interception de documents électroniques	Durant l'activité du système	Serveur	Tout poste du réseau local	I4
			Réseau local	Tout poste du réseau local	
			Réseau de transmission de données	Nœuds intermédiaires	
			Modem		
	Copie non autorisée	En dehors de l'activité du système	Serveur	Tout poste du réseau local	I9
	Modification du logiciel	Comme dans le cas précédent			I11
	Introduction d'un logiciel malveillant				
Accès non autorisé au système de gestion des documents électroniques	Accès non autorisé	Durant l'activité du système ou en dehors de celle-ci	Tout poste du réseau local	Même poste du réseau local	I13
				Tout poste du réseau local Serveur (par script d'authentification (LOGIN SCRIPT))	
			Serveur de messagerie	Serveur de messagerie	
				Tout poste du réseau local	
			Serveur	Tout poste du réseau local	
			Tout poste du réseau local	À partir d'Internet	
Accès non autorisé au canal de transmission de données	Accès non autorisé au canal	Durant l'activité du système	Réseau local	Tout poste du réseau local	I14
		Au cours d'une transmission de données	Réseau de transmission de données	Nœud intermédiaire	I15
			Modem		
Attaque depuis un réseau extérieur	Attaque depuis un réseau extérieur	Durant l'activité du système ou en dehors de celle-ci	Serveur		I18
			Poste du réseau		
			Modem		

Menace	*Attaque*	*Contexte de l'attaque*	*Cible de l'attaque*	*Source de l'attaque*	*Code menace*
			Routeur		
Dysfonctionnement du logiciel	Modification du logiciel, modification de la configuration des machines ou introduction d'un logiciel malveillant	Durant l'activité du système ou en dehors de celle-ci	Toute cible	Toute source	I17
Configuration de routeur non autorisée	Configuration de routeur non autorisée	Durant l'activité du système ou en dehors de celle-ci	Routeurs	Tout élément du réseau de transmission de données	I18

II. Protection contre les menaces

	Mesures de protection		
Code menace	*Organisationnelles*	*Physiques*	*Techniques*
I1	1. Instructions relatives à la modification de la configuration du logiciel 2. Instructions à l'intention des utilisateurs 3. Attribution de responsabilité en cas d'infraction aux règles établies 4. Instructions relatives au changement des droits accordés aux utilisateurs	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Interdiction du téléchargement sur des postes de travail automatisés à partir de disques externes 2. Protection des fichiers exécutables contre toute modification 3. Environnement d'exécution de programmes fermé pour chaque utilisateur du système 4. Contrôle périodique de l'intégrité des fichiers exécutables et des paramètres des programmes 5. Utilisation de la signature électronique 6. Journalisation
I2	1. Validation des saisies 2. Contrôle du flux des documents 3. Instructions à l'intention des utilisateurs 4. Attribution de responsabilité en cas d'infraction aux règles établies	Non	1. Validation des saisies (au moyen d'un programme) 2. Contrôle du flux des documents (au moyen d'un programme) 3. Journalisation

	Mesures de protection		
Code menace	*Organisationnelles*	*Physiques*	*Techniques*
I3	1. Instructions relatives à la modification de la configuration du logiciel 2. Instructions à l'intention des utilisateurs 3. Attribution de responsabilité en cas d'infraction aux règles établies	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Interdiction du téléchargement sur des postes de travail automatisés à partir de disques externes 2. Protection des fichiers exécutables et des fichiers système contre toute modification 3. Environnement d'exécution de programmes fermé pour chaque utilisateur du système 4. Contrôle périodique de l'intégrité du système 5. Journalisation 6. Utilisation de moyens de prévention des attaques
I4	1. Instructions relatives à la modification de la configuration du logiciel 2. Instructions à l'intention des utilisateurs 3. Attribution de responsabilité en cas d'infraction aux règles établies 4. Instructions relatives au changement des droits accordés aux utilisateurs	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Restriction de l'accès au serveur en fonction de l'adresse MAC 2. Autorisation de l'accès au serveur limitée aux postes de travail protégés 3. Interdiction des accès simultanés au serveur par des utilisateurs portant le même nom 4. Réorganisation de l'information 5. Protection de la console du serveur 6. Journalisation 7. Utilisation de moyens de prévention des attaques
I5	1. Recours à une société extérieure	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Réorganisation de l'information 2. Utilisation de la signature électronique 3. Contrôle du temps passé

	Mesures de protection		
Code menace	*Organisationnelles*	*Physiques*	*Techniques*
I6	1. Instructions relatives au changement des droits accordés aux utilisateurs 2. Instructions à l'intention des utilisateurs 3. Attribution de responsabilité en cas d'infraction aux règles établies	1. Isolation du système protégé des autres systèmes	1. Restriction de l'accès aux ordinateurs individuels, au serveur, etc. 2. Autorisation de l'accès au serveur limitée aux postes de travail protégés 3. Restriction de l'accès au serveur en fonction de l'adresse MAC 4. Interdiction des accès simultanés au serveur par des utilisateurs portant le même nom 5. Journalisation 6. Utilisation de moyens de prévention des attaques
I7	1. Recours à une société extérieure	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Utilisation de la signature électronique 2. Réorganisation de l'information 3. Établissement d'une liaison 4. Contrôle du temps passé
I8	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Verrouillage de l'écran 2. Restriction de l'accès aux ordinateurs individuels 3. Contrôle de l'accès aux ordinateurs individuels
I9	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Restriction de l'accès au serveur en fonction de l'adresse MAC 2. Autorisation de l'accès au serveur limitée aux postes de travail protégés 3. Interdiction des accès simultanés au serveur par des utilisateurs portant le même nom 4. Réorganisation de l'information 5. Protection de la console du serveur 6. Journalisation 7. Utilisation de moyens de prévention des attaques

	Mesures de protection		
Code menace	*Organisationnelles*	*Physiques*	*Techniques*
I10	1. Recours à une société extérieure 2. Archivage des documents électroniques	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Journalisation 2. Utilisation de la signature électronique
I11	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Isolation du système protégé des autres systèmes	1. Restriction de l'accès aux ordinateurs individuels 2. Contrôle de l'accès aux ordinateurs individuels 3. Journalisation 4. Utilisation de moyens de prévention des attaques
I12	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies 3. Archivage des documents électroniques	1. Isolation du système protégé des autres systèmes	1. Établissement d'une liaison 2. Signature électronique 3. Contrôle du temps passé 4. Journalisation
I13	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies 3. Instructions relatives à l'utilisation d'outils de sécurité informatique pour la prévention des accès non autorisés 4. Restriction du nombre d'utilisateurs autorisés à configurer les routeurs	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux 3. Isolation du système protégé des autres systèmes	1. Restriction de l'accès aux ordinateurs individuels et au serveur 2. Contrôle de l'accès aux ordinateurs individuels et au serveur 3. Journalisation 4. Verrouillage de l'écran 5. Changement du nom générique de l'administrateur du système de sécurité 6. Restriction de l'autorisation d'intervention sur le réseau au seul administrateur du système de sécurité ou administrateur du réseau 7. L'administrateur du système de sécurité doit être le propriétaire de l'ensemble des fichiers exécutables et des principaux paramètres du système 8. Utilisation de moyens de prévention des attaques 9. Utilisation de pare-feux et d'antivirus 10. Utilisation de toutes les fonctions de sécurité des routeurs

	Mesures de protection		
Code menace	*Organisationnelles*	*Physiques*	*Techniques*
I14	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Protection du réseau câblé	1. Chiffrement
I15	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Protection du réseau câblé	1. Chiffrement
I16	1. Instructions à l'intention des utilisateurs 2. Attribution de responsabilité en cas d'infraction aux règles établies	1. Contrôle de l'accès aux locaux 2. Protection physique des locaux	1. Restriction de l'accès aux archives électroniques 2. Copies de sauvegarde 3. Utilisation d'antivirus
I17	Toutes les mesures	Toutes les mesures	Toutes les mesures
I18	1. Instructions relatives à l'utilisation des canaux de transmission de données 2. Recours à une société extérieure 3. Instructions à l'intention des utilisateurs 4. Attribution de responsabilité en cas d'infraction aux règles établies		1. Limitation du nombre des canaux de transmission de données utilisés 2. Isolation physique d'Internet des ordinateurs ayant accès au système de gestion des documents électroniques 3. Restriction de l'accès aux ordinateurs individuels équipés d'un modem 4. Journalisation 5. Utilisation de moyens de prévention des attaques 6. Utilisation de pare-feux 7. Utilisation de toutes les fonctions de sécurité des routeurs

III. Profil informel du transgresseur

Transgresseur − Personne qui tente d'effectuer des opérations ou des actions interdites par erreur, par ignorance, ou encore délibérément, avec de mauvaises intentions (de façon intéressée) ou sans (par jeu ou par plaisir, pour s'affirmer, etc.) et qui pour cela emploie divers moyens, méthodes et possibilités.

Le système de sécurité doit être conçu sur la base des hypothèses suivantes concernant les types de transgresseurs possibles :

a) « ***Utilisateur non averti*** » − Membre du personnel d'une organisation pouvant tenter d'effectuer des opérations interdites, d'accéder à des ressources informatiques auxquelles il n'a pas de droit d'accès, d'introduire des données incorrectes dans le système, etc., en agissant par erreur, par incompétence ou par négligence, sans mauvaise intention, et en utilisant uniquement des moyens matériels et logiciels internes (qui lui sont accessibles).

b) « ***Dilettante*** » − Membre du personnel d'une organisation tentant de contourner le système de sécurité de façon désintéressée, dans le seul but de s'affirmer (pour « s'amuser »). Afin de contourner le système et d'effectuer des opérations interdites, il peut avoir recours à diverses méthodes d'obtention de droits supplémentaires d'accès à des ressources (noms et mots de passe d'autres utilisateurs, notamment), exploiter des failles du système de sécurité et utiliser des programmes internes (programmes installés sur son poste de travail) qui lui sont accessibles (il effectue des opérations non autorisées en outrepassant ses droits). Il peut également tenter d'utiliser à cette fin des outils et des moyens externes (débogueurs, utilitaires, etc.), des programmes mis au point de façon indépendante ou des moyens techniques standard.

c) « ***Transgresseur externe (cybercriminel)*** » − Personne étrangère à l'organisation ou collaborateur externe agissant intentionnellement, ou par curiosité ou pour « s'amuser », éventuellement avec la complicité d'autres personnes. Il peut avoir recours à divers moyens et méthodes d'effraction connus sur les réseaux couramment utilisés (réseaux X.25 ou réseaux IP), notamment l'introduction à distance de logiciels malveillants et l'utilisation d'utilitaires et de programmes spécifiques permettant d'exploiter les failles du système de sécurisation des nœuds du réseau.

d) « ***Cybercriminel interne*** » − Membre du personnel d'une organisation agissant à des fins particulières ou par esprit de vengeance à la suite d'une offense, éventuellement avec la complicité d'autres personnes ne faisant pas partie de l'organisation. Il peut avoir recours à divers moyens et méthodes d'effraction, notamment des méthodes secrètes pour obtenir des accès, des méthodes passives (moyens techniques d'interception sans modification des composants du système), des méthodes et moyens d'intervention (modification du matériel, connexion aux canaux de transmission de données, introduction de logiciels malveillants et utilisation d'utilitaires et de programmes spécifiques), ainsi que des combinaisons de ces moyens et méthodes, de l'intérieur de l'entreprise comme de l'extérieur, c'est-à-dire à partir du réseau public.