Le présent document doit être considéré comme un **modèle non exhaustif**.
Les données sont indiquées à titre d'échantillon non représentatif.

Document d'aide pour l'élaboration d'un plan de sécurité

Nom de l'exploitant

Adresse

Personne de contact

Considérations

Le but du présent document est d'assister les exploitants dans la préparation de leur plan de sécurité.

Vous trouverez de plus amples informations dans les deux documents ci-dessous publiés par l'ENISA[1]:

- "Technical Guideline on Security Measures".
- "Technical Guideline on Threats and Assets".

[1] https://www.enisa.europa.eu/publications

Contenu d'un PSE

1. Description générale de l'infrastructure critique

1.1. Aperçu des services fournis

1.1.1. Voix

1. Mobile
2. Fixe

1.1.2.Données

1. Mobiles
2. Fixes

1.1.3.Internet

1.1.4.Autres services mobiles

1.1.5.Autres services fixes

1.2. Aperçu des infrastructures critiques

1.1.6.Physique (par site)

1. Localisations

Localisation	Adresse	Type
BRUXELLES-CD	Coordonnées GPS Nom de rue...	Centre de données
BRUXELLES-CR	Coordonnées GPS Nom de rue...	Centre de réseau

1.1.7.Logique (HLD)

Par service défini au point 1, une explication et un plan de l'infrastructure de support.

1.1.8.Orientation service (service : sur quel site, redondance...)

Par élément situé dans une infrastructure critique, une liste pour indiquer où se trouvent les éléments, quels services ils soutiennent ainsi que leur redondance.

Site	Localisation								
Services	Fixe			Mobile			Internet	Redondance	Type de redondance
	Voix	Données	Autres	Voix	Données	Autres		Intersites, locale, néant	N+1, fibres, générateur...
BSC				x	x	x		Intersites	Double couverture
RNC				x	x	x		Intersites	Double couverture
Edge RTR	x	x	x	x	x	x		Locale	Au niveau de la carte

Éléments à prendre en compte (le cas échéant) :

Alimentation	LE (Local Exchange)	PoP (IP transit)
Routeurs	TAX	Paire torsadée (de cuivre)
Edge routers	Tandem exchange	Câbles coaxiaux
SBC	MSC	Fibre optique
HLR/AUC	VLR	SMS-C
HSS	SGSN	MMS-C
BTS	GGSN	Générateur diesel
BSC	SGW	UPS
Node B et eNode B	ePDG	STP
RNC	SDH, ADM, ROADM, ODXC	SCP
MME	WDM et DWDM	Pare-feu
ANDSF	DHCP	Hyperviseur
PCRF	DNS	IXP

2. Analyse des risques

2.1. Aperçu de l'analyse d'impact

Liste où l'importance/l'impact potentiel (comme un % du nombre total de clients) de chaque localisation identifiée au point 1.1.6.1 est analysé par rapport à chaque service fourni (1).

Localisation	Voix mobile 2G	Internet mobile 2G	Internet mobile 3G	Internet mobile 4G	Voix fixe	….	Importance (très faible … très élevée)
BRUXELLES-CD	30 %	40 %	10 %	50 %	Néant		Élevée

2.2. Scénarios

2.2.1. Menaces

Inventaire et description des menaces qui sont prises en compte dans l'étude :

Menaces	Description	Probabilité (échelle ci-dessous)
Bug du logiciel		Crédible
Vandalisme	Acte de détérioration gratuite de l'infrastructure	Crédible

Liste non exhaustive des menaces :

- Perturbation électromagnétique
- Vol de matériel
- Défaillance du matériel
- Bug du logiciel
- Changement/mise à jour du matériel défectueux
- Changement/mise à jour du logiciel défectueux
- Surcharge
- Piratage du trafic réseau
- Malwares et virus
- Menace avancée persistante
- Politique/procédure défaillante
- Espionnage
- Kidnapping/piratage
- Erreurs humaines
- Intentions malveillantes de collaborateurs internes
- Attaque de type « refus de service » (Denial of Service)
- Panne de courant/câbles/refroidissement
- Erreur de conception
- Arrêt de sécurité
- Catastrophe naturelle
- Incendie
- Incendie criminel
- Panne de carburant/eau
- Attaque terroriste
- Vandalisme
- Autres

2.2.2. Matrice des risques

Les risques peuvent être évalués en fonction de leur impact potentiel et de leur probabilité :

Risque		Probabilité				
		Minimale	Peu probable	Possible	Crédible	Fréquente
Impact	Mineur	Très faible	Très faible	Faible	Faible	Modéré
	Notable	Très faible	Faible	Faible	Modéré	Élevée
	Modéré	Faible	Faible	Modéré	Élevé	Élevé
	Grave	Faible	Modéré	Élevé	Élevé	Très élevé
	Catastrophique	Modéré	Élevé	Élevé	Très élevé	Très élevé

3. Mesures permanentes

3.1. Inventaire

Inventaire et description des mesures empêchant les menaces identifiées au point 2 par site.

Impact résiduel des menaces identifiées au point 2 après la prise en compte des mesures.

Site	BRUXELLES-CD				
Menaces	Points vulnérables	Mesures permanentes	Impact résiduel par service	Probabilité résiduelle	Risque résiduel
Panne de courant	Un seul générateur	Transformateur redondant. Générateur avec 3 jours de carburant.	Voix mobile : modéré Voix fixe : faible	Minimale	Voix mobile : faible Fixe : très faible
Incendie	Composant électrique. Température élevée de l'appareil.	Système à l'argonite. Extincteurs dans toutes les pièces. Ligne directe avec le 101.	Notable	Possible	Faible

3.2. Autonomie à distance

Site	Présence	Service à distance	Accès à distance	Intervention
BRUXELLES-CD	24/7	Supervision : NOC	Voix fixe (2 câbles physiques) Données fixes (1 fibre)	Téléphone mobile d'un autre fournisseur Remplacer fibre/câble
LOUVAIN-RTR	Jour ouvrable 0700-1700	Supervision : NOC Service de badge : BRUXELLES-CD	Voix fixe (1 câble physique) Données fixes (4 liens logiques + 2 entrées de fibre différentes)	Permanence sur place dans les 2 heures Carte d'accès disponible au NOC ….

3.3. Sécurité physique

Localisation	Éléments de sécurité							
	Gardes	Portail	Portes	Zones	Système de badges	Clé	CCTV	Alarme
BRUXELLES-CD	OUI Société de sécurité privée 24/7	OUI	OUI	Zones différentes	OUI	Permanence + personnel sur site	OUI Enregistrement d'1 semaine	INCENDIE + Intrusion + Inondations
LOUVAIN-RTR	Non	Non	OUI	Seulement 1 zone de sécurité	OUI	NOC + Permanence	OUI Enregistrement d'1 semaine	INCENDIE + Intrusion + inondations

4. Mesures graduelles

4.1. Mesures graduelles générales

Inventaire et description des mesures empêchant les menaces identifiées au point 2.

Seuil d'activation des mesures graduelles

Menaces	Mesures graduelles	Déclencheur
Attaque terroriste	Les barrières de sécurité sont fermées ….	CUTA 4

4.2. Mesures graduelles spécifiques

4.2.1. Priorisation entre les services

En cas de défaillance majeure, le service sera relancé dans l'ordre suivant :

- …

4.2.2. Plan de communication

Déclencheur/impact	Moyens de communication	Description
Voix fixe > 100 000	SMS/Médias	Temps de réparation estimé
…		

4.2.3. Mesures pour minimaliser l'impact

Par menace et, le cas échéant, par site ou élément, liste des actions entreprises en cas d'occurrence de menace

Menaces	Sites	Éléments	Actions
Incendie	Tous les sites	Tous les éléments	• Activation du système à l'argonite • Vérification physique • Appel des pompiers Ou voir manuel, section XXX (à fournir)
Panne de courant	Tous les sites	Tous les éléments	• Installation de générateur à l'extérieur • ….
Défaillance du matériel	BRUXELLES-CD	Routeur	• Reroutage manuel du trafic • Apporter pièce de rechange sur place • ….

4.2.4. Processus de redressement

Mesures en place pour redresser un site après un crash par élément

Sites	Éléments	Pièce de rechange	Processus de redressement
BRUXELLES-CD	Routeur	OUI	• Récupérer la pièce de rechange dans le stock central • Mise à niveau du routeur • Charger le routeur avec la dernière configuration de back-up (max. 24h) • Inspection du routeur défaillant pour trouver la cause première de la défaillance
BRUXELLES-CD	Racks MME	OUI dans le conteneur d'intervention	• Amener le conteneur d'intervention sur le site • Connexion au conteneur • Démarrage du conteneur • ….

5. Test opérationnel

Planification des tests principaux :

Infra. critique	Type de tests	But des tests	Fréquence	Limites des tests
Tous les sites critiques	Alimentation électrique	Test du générateur	1x/mois	Pas de charge
BRUXELLES-CD	Refroidissement à air	Test du système de back-up	1x/an	Aucune

6. Annexes

6.1. Dépendances à l'égard des fournisseurs par élément.

Éléments	Fournisseurs	Type	Services	Dépendance	Escalade	Evaluation de sécurité des fournisseurs de services ou d'assistance
Edge routers	Router maker	RouterXX	TOUS	Besoin de soutien pour faire fonctionner	Niveau 1 : BE Telecom - Belgique Niveau 2 : Telco Company - Inde	Router maker: Interne BE Telecom: Autorité Telco Company: Interne

Le champ « services » se rapporte aux services définis au point 1.1.

La dépendance doit être évaluée comme suit :

- Pas besoin de soutien pour faire fonctionner.
- Besoin de soutien pour faire fonctionner.
- Besoin de soutien pour installer/remplacer (des pièces) des appareils.
- Autre

Le champ « escalade » doit contenir les différents niveaux d'escalade, le pays d'exploitation et le nom de la société.

Le champ « Évaluation de sécurité » doit contenir pour chaque fournisseur/entreprise fournissant le support le type d'évaluation de sécurité qui a eu lieu lors de la phase contractuelle :

- Interne : évaluation interne effectuée par l'exploitant.
- Externe : évaluation externe réalisée par un organisme privé
- Autorité : évaluation externe réalisée par un organisme public.
- Aucune.

6.2. Autres