

Dit document dient te worden beschouwd als een **niet-exhaustief model**.
De verstrekte data vormen niet-representatieve voorbeelden.

Begeleidingsdocument voor het uitwerken van een beveiligingsplan

Naam van de operator

Adres

Contactpersoon

Overwegingen

Dit document is bedoeld als leidraad bij de opstelling van een beveiligingsplan door de operatoren.

Voor meer informatie kunt u deze twee publicaties van ENISA¹ raadplegen:

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

¹ <https://www.enisa.europa.eu/publications>

Inhoud

1.	Algemene beschrijving van de kritieke infrastructuur	4
1.1.	Overzicht van de verstrekte diensten	4
1.2.	Overzicht van de kritieke infrastructuren	4
2.	Risicoanalyse.....	6
2.1.	Overzicht impactanalyse	6
2.2.	Scenario's.....	6
3.	Permanente maatregelen.....	8
3.1.	Inventaris	8
3.2.	Autonomie op afstand	9
3.3.	Fysieke beveiliging	10
4.	Stapsgewijze maatregelen.....	11
4.1.	Algemene stapsgewijze maatregelen	11
4.2.	Specifieke stapsgewijze maatregelen.....	11
5.	Operationele test.....	12
6.	Bijlagen	13
6.1.	Verkopersafhankelijkheid per voorziening	13
6.2.	Andere	13

1. Algemene beschrijving van de kritieke infrastructuur

1.1. Overzicht van de verstrekte diensten

1.1.1. Spraak

1. Mobiel
2. Vast

1.1.2.Data

1. Mobiel
2. Vast

1.1.3.Internet

1.1.4.Andere mobiele diensten

1.1.5.Andere vaste diensten

1.2. Overzicht van de kritieke infrastructuren

1.1.6.Fysiek (per site)

1. Locaties

Locatie	Adres	Type
BRUSSELS-DC	Gps-coördinaten Straatnaam ...	Datacenter
BRUSSELS-NO	Gps-coördinaten Straatnaam ...	Netwerkkantoor

1.1.7.Logisch (HLD)

Per dienst gedefinieerd in deel 1, uitleg en een plan van de dragende infrastructuur.

1.1.8.Dienstgericht (dienst: op welke site, overbodigheid, ...)

Per voorziening in een kritieke infrastructuur, een lijst om aan te duiden waar de activa zich bevinden, welke diensten ze ondersteunen en hoe overtollig ze zijn.

Site	Locatie								
Diensten	Vast			Mobiel			Internet	Overbodigheid	Soort van overbodigheid
	Spraak	Data	Overige	Spraak	Data	Overige			
BSC				x	x	x		Tussen sites	Dubbele dekking
RNC				x	x	x		Tussen sites	Dubbele dekking
Rand-RTR	x	x	x	x	x	x		Lokaal	op kaartniveau

Activa om rekening mee te houden (als relevant):

Voedingskabel	LEX (lokale centrale)	PoP (IP transit)
Routers	TAX	Twisted (koper)paar
Randrouters	Tandemcentrale	Coaxkabels
SBC	MSC	Glasvezels
HLR/AUC	VLR	SMS-C
HSS	SGSN	MMS-C
BTS	GGSN	Dieselgenerator
BSC	SGW	UPS
Node B en eNode B	ePDG	STP
RNC	SDH, ADM, ROADM, ODXC	SCP
MME	WDM en DWDM	Firewall
ANDSF	DHCP	Hypervisor
PCRF	DNS	IXP's

2. Risicoanalyse

2.1. Overzicht impactanalyse

Een lijst van waar de beduidende/mogelijke impact (in % van het totaal aantal klanten) van elke geïdentificeerde locatie in 1.1.6.1 wordt onderzocht met betrekking tot elke verstrekt dienst (1).

Locatie	Mobiele spraak 2G	Mobiel internet 2G	Mobiel internet 3G	Mobiel internet 4G	Vaste spraak	...	Belang (Heel weinig ... heel veel)
BRUSSELS-DC	30%	40%	10%	50%	Nihil		Hoog

2.2. Scenario's

2.2.1. Gevaren

Inventaris en beschrijving van de gevaren waarmee de studie rekening houdt:

Gevaren	Beschrijving	Waarschijnlijkheid (schaal hieronder)
Softwarematige storing		Geloofwaardig
Vandalisme	Berokkenen van schade aan infrastructuur zonder profijt.	Geloofwaardig

Niet-volledige lijst van gevaren:

- Elektromagnetische interferentie
- Diefstal van hardware
- Hardwarematige storing
- Softwarematige storing
- Niet-succesvolle wijziging/update van hardware
- Niet-succesvolle wijziging/update van software
- Overbelasting
- Kaping van netwerkverkeer
- Malware en virussen
- Geavanceerde aanhoudende bedreiging
- Fout in het beleid/de procedure
- Spionage
- Kidnapping/Kaping
- Menselijke fouten
- Kwaadwillige opzet van interne werknemers
- 'Denial of service'-aanval
- Probleem met stroom/kabels/koeling
- Ontwerpfout
- Veiligheidsstop
- Natuurramp
- Brand
- Brandstichting
- Brandstof/water uitgeput
- Terreuraanval
- Vandalisme
- Andere

2.2.2. Risicomatrix

Risico's kunnen beoordeeld worden op basis van de mogelijke impact en de waarschijnlijkheid:

Risico's		Waarschijnlijkheid				
		Minimaal	Onwaarschijnlijk	Mogelijk	Geloofwaardig	Frequent
Impact	Klein	Heel laag	Heel laag	Laag	Laag	Matig
	Merkbaar	Heel laag	Laag	Laag	Matig	Hoog
	Matig	Laag	Laag	Matig	Hoog	Hoog
	Ernstig	Laag	Matig	Hoog	Hoog	Heel hoog
	Rampzalig	Matig	Hoog	Hoog	Heel hoog	Heel hoog

3. Permanente maatregelen

3.1. Inventaris

Inventaris en beschrijving van de bestaande maatregelen ter voorkoming van de gevaren geïdentificeerd in deel 2 per site.

Restimpact van de gevaren geïdentificeerd in deel 2 nadat rekening werd gehouden met maatregelen.

Site	BRUSSELS-DC				
Gevaren	Kwetsbaarheden	Permanente maatregelen	Restimpact per dienst	Restwaarschijnlijkheid	Restrisico
Stroomonderbreking	Slechts één generator	Overtollige transformator Generator met 3 dagen brandstof	Mobiele spraak: Matig Vaste spraak: Laag	Minimaal	Mobiele spraak: laag Vast: erg laag
Brand	Elektrisch onderdeel. Hoge temperatuur van het toestel	Argonsysteem. Brandblusapparaten in elke ruimte. Rechtstreekse lijn naar 101.	Merkbaar	Mogelijk	Laag

3.2. Autonomie op afstand

Site	Aanwezigheid	Dienst op afstand	Toegang op afstand	Eventualiteit
BRUSSELS-DC	24/7	Toezicht: NOC	Vaste spraak (2 fysieke kabels) Vaste data (1 glasvezel)	Mobiele telefoon van een andere provider. Glasvezel/kabel vervangen.
LEUVEN-RTR	Werkdag 0700-1700	Toezicht: NOC Badgedienst: BRUSSELS-DC.	Vaste spraak (1 fysieke kabel) Vaste data (4 softwarelinks + 2 verschillende glasvezeltoegangen)	Permanentie ter plaatse binnen 2 uur. Wachtwoordmanager beschikbaar in het NOC.

3.3. Fysieke beveiliging

Locatie	Veiligheidselementen							
	Bewakingsagenten	Poort	Deuren	Zones	Badgesysteem	Sleutel	CCTV	Alarm
BRUSSELS-DC	JA Private bewakingsfirma 24/7	JA	JA	Verschillende zones.	JA	Permanentie + personeel ter plaatse	JA 1 week opnames	BRAND + Inbraak + Overstroming
LEUVEN-RTR	Nee	Nee	JA	Slechts 1 bewakingszone	JA	NOC + Permanentie	JA 1 week opnames	BRAND + Inbraak + Overstroming

4. Stapsgewijze maatregelen

4.1. Algemene stapsgewijze maatregelen

Inventaris en beschrijving van de bestaande maatregelen ter voorkoming van de gevaren geïdentificeerd in &2.

Drempel die de stapsgewijze maatregelen activeert.

Gevaren	Stapsgewijze maatregelen	Trigger
Terreuraanval	Veiligheidsbarrières zijn gesloten.	CUTA 4

4.2. Specifieke stapsgewijze maatregelen

4.2.1. Prioritisering tussen diensten.

In geval van een ernstige storing, zal de dienst worden heropgestart in deze volgorde:

- ...

4.2.2. Communicatieplan.

Trigger/Impact	Communicatiemiddelen	Beschrijving
Vaste spraak >100.000	Sms/Media	Verwachte reparatietijd
...		

4.2.3. Maatregelen om de impact te minimaliseren.

Per gevaar en, indien nodig, per site of voorziening, lijst van de acties ondernomen in geval het gevaar zich voordoet.

Gevaren	Sites	Activa	Acties
Brand	Alle sites	Alle activa	<ul style="list-style-type: none"> • Argonsysteemactivering. • Fysieke controle. • Brandweer bellen. <p>Of zie Handleiding sectie XXX (te verstrekken)</p>
Stroomonderbreking	Alle sites	Alle activa	<ul style="list-style-type: none"> • Generatorinstallatie buitenshuis. •
Hardwarematige storing	BRUSSELS_DC	Router	<ul style="list-style-type: none"> • Handmatig omleiden van verkeer. • Reserve ter plaatse brengen. •

4.2.4. Herstelprocessen.

Maatregelen in voege om een site te herstellen na een crash, per voorziening.

Sites	Activa	Reserve	Herstelproces
BRUSSELS_DC	Router	JA	<ul style="list-style-type: none"> • De reserve afhalen in de centrale winkel. • Router upgraden. • Meest recente back-upconfiguratie installeren op de router (max. 24 uur oud) • Router met faling inspecteren om te achterhalen wat de storing heeft veroorzaakt.
BRUSSEL-DC	MME-rekken	JA in calamiteitencontainer	<ul style="list-style-type: none"> • Breng de calamiteitencontainer ter plaatse. • Aansluiting van de container. • Opstarten van de container. •

5. Operationele test

Planning van de hoofdtests:

Kritieke infra	Type tests	Doel van de tests	Frequentie	Testbeperkingen
Alle kritieke sites	Stroomtoevoer	Test van de generator	1/maand	Niet aangesloten op het stroomnet.
BRUSSELS-DC	Luchtkoeling	Test van het back-upsysteem	1/jaar.	Geen.

6. Bijlagen

6.1. Verkopersafhankelijkheid per voorziening.

Voorziening	Verkopers	Type	Diensten	Afhankelijkheid	Escalatie	Veiligheidsbeoordeling van verkopers en ondersteunende bedrijven
Edge routers	Router maker	RouterXX	ALLEMAAL	Support nodig om te werken	Niveau 1: BE Telecom - België Niveau 2: Telco Company - India	RouterXXX: Interne BE Telecom: Overheid Teclco company: Interne

Het veld 'diensten' verwijst naar de diensten gedefinieerd in deel 1.1.

'Afhankelijkheid' moet als volgt worden beoordeeld:

- Geen nood aan support om te werken.
- Nood aan support om te werken.
- Nood aan support om (delen van) toestellen te installeren/vervangen.
- Andere.

Het escalatieveld moet de verschillende escalatieniveaus bevatten alsook het land van activiteit en de ondersteunende bedrijfsnaam.

Het veld van Veiligheidsbeoordeling bevatten, voor elke verkoper/ondersteunende bedrijf, de type van veiligheidsbeoordeling die gedurende de contractuele fase plaatsvond:

- Interne: interne veiligheidsbeoordeling uitgevoerd door de operator.
- Externe: externe veiligheidsbeoordeling uitgevoerd door een particuliere instelling.
- Overheid: externe veiligheidsbeoordeling uitgevoerd door een overheidsinstantie.
- Niets.

6.2. Andere