



Äntwert vum Premierminister, vum Minister fir Wirtschaft, PME, Energie an Tourismus, vum Inneminister a vun der delegéierter Ministesch beim Premierminister fir Medien a Connectivitéit op d'parlamentaresch Fro n° 2652 vum 23. Juli 2025 vun den honorabelen Deputéierten Taina Bofferding a Ben Polidori."

- 1. Ass de Haut-Commissariat à la Protection nationale (HCPN) an dësem Kontext zesummegegruff ginn? Wann net, firwat net? Ass ee „Plan d'intervention d'urgence“ (PIU) ausgeléist ginn? Wa jo, wéi gouf en ëmgesat a mat wat fir engem Resultat?**

Op Decisoun vum Premierminister huet den HCPN eng Krisen-Cellule am nationale Krisenzentrum zu Senneng aberuff, wou all déi concernéiert Acteuren zesumme komm sinn. Dës Cellule gouf vum Wirtschaftsminister, Minister fir kleng a mëttelstänneg Betriber, Energie- an Tourismusminister, Lex Delles präsidéiert, dëst a Präsenz vum Inneminister, Léon Gloden. Et war dee Moment wichteg en Iwwerbléck iwwert d'Situatioun bei der Post ze kréien an och e provisoiresche Bilan iwwert déi direkt Auswierkunge bei den Noutruffnummern 112 an 113 ze zéien. Ab 20 Auer huet sech d'Situatioun stabiliséiert an d'Post konnt iwwert den Owend rëm successiv déi verschidde Servicer eropfueren.

- 2. Ëm wat fir eng technesch Stéierung oder eventueller Cyberattack huet et sech am aktuelle Fall gehandelt? Goufen Elementer identifizéiert, déi op eng gezielten Attack hiweisen?**

Déi technesch Stéierung, déi den 23. Juli 2025 opgetrueden ass, war d'Resultat vun enger Cyberattack, laut de forenseschen Analysen. Dë forensesch Analysen, déi vun den Experten aus dem Beräich Telekommunikatioun a Cybersécherheet bei POST duerchgefouert goufen, hu gewisen, datt eng Schwachstell an engem standardiséierte Software-Komponent ausgenutzt gouf, fir eng groussflächeg Stéierung an d'Onverfügbarkeet vun de Servicer ze verursaachen.

D'Elementer, déi am Kader vun den Analysen identifizéiert goufen, weisen drop hin, datt et sech ëm eng Attack gehandelt huet. Et gouf keng Intrusioun an déi intern Systemer vu POST, an et sinn och keng Date kompromettéiert oder geklaut ginn. D'Attack sollt eng Stéierung vum normale Fonctionnement vun de Servicer ausléisen, déi trotz der héich redundanter Architektur eng generaliséiert Perturbatioun vum gesamte POST-Reseau verursaacht huet.

- 3. Wéi laang waren déi betrafte Systemer ausgefall, a wéi eng Zerwisser waren insgesamt betraff?**

Déi betrafte Systemer waren vum Mëttwoch, 23. Juli 2025, vun 16:15 Auer un fir ongeféier 3 an eng hallef Stonnen ausgefall. De progressive Retablissement huet géint 19:50 Auer ugefaangen, mat enger Prioritéit op d'Noutruffnummern 112 an 113, déi géint 20:00 Auer erëm iwwer alleguer d'Netzer vun der POST erreechbar waren. Déi meescht aner Servicer ware kuerz drop och nees gréisstendeels restauréiert.

Zerwisser vun der POST déi vum Incident vum 23. Juli 2025 betraff waren:

- De 4G an 5G Reseau an d'Telephonie fixe (réseau fixe) vun der POST waren weder fir Data nach fir Telefongesprécher disponibel. D'Indisponibilitéit vum 4G an 5G huet dozou gefouert, dass d'Appellen iwert 2G ausgefouert goufen. D'Kapazität vum 2G ass awer net duergangen fir all d'Appellen z'assuréieren, wouduerch et ënnert anerem zu Problemer komm ass, fir den 112 an 113 aus dem Post-Reseau eraus unzeruffen.
- D'POST-Internetsäiten, déi mobil Applikatiounen vun der POST an den e-banking eboo

- Intern Applikationen vu POST
- D'Verkaafsnetz an de Contact Center

4. Wat sinn d'Prozeduren an esou Fäll, besonnesch fir systemrelevant Verwaltungen a Zerwisser fir de Kontakt mat de Bierger trotz engem Ausfall vum Internet- an Telefonsreseau oprecht ze erhalen?

De CGDIS huet fir seng eege Systemer verschidde Backup-Niveauen a Prozeduren, déi jee no Situatioun kënne genotzt an aktivéiert ginn.

Wann, wéi an dësem Fall, d'Uriff op d'Noutruffnummer 112 selwer duerch extern Problemer deelweis ënnerbrach oder gestéiert sinn, da beméit sech de CGDIS, fir der Bevëlkerung alternativ Weeër unzibidden, fir den 112 ze erreechen. An dësem konkrete Fall goufen alternativ Méiglechkeeten wéi Festnetz oder en aneren Handy-Reseau-Provider recommandéiert. Doriwwer eraus waren déi lokal Asazentere vum CGDIS besat. Dës haten iwwer d'Funknetz jidderzäit direkte Kontakt mam 112, fir de Fall, datt e Bierger hei no Hëllef gefrot hätt, wat och an dräi Fäll esou gemaach gouf. Weiderhi stoung de CGDIS an direktem Kontakt iwwer Funk mat der Police, fir deene Leit entgéintzekommen, déi sech bei der Police fir en Noutfall gemellt hätten.

Ab deem Moment wou eng Krisen-Cellule aberuff gëtt, koordinéiert eng national Kommunikatiounscellule d'Kommunikatioun mat de Medien an dem Bierger. Dës Cellule stinn déi verschidde Systemer zur Verfügung fir via d'Medie mat de Bierger ze kommunizéieren oder per LU-Alert d'Bevëlkerung direkt ze alertéieren. An den Noutfallpläng ass och virgesi fir bei Problemer vun de Kommunikatiounssystemer eng technesch Cellule d'appui anzeberuffen.

5. Ginn et alternativ Kommunikationsstrukturen, wéi zum Beispill Satellitennetz, Noutruffnummern iwwer aner Kanäl oder lokal Radiosystemer, déi an esou engem Fall agesat kënne ginn?

D'Rettungsdéngschter wéi de CGDIS an d'Police kommunizéieren iwwer de RENITA, en alternative Funkreseau, dee komplett autonom an onofhängeg vun de mobilen Netzer funktionéiert. Dëse Funkreseau steet dem Bierger awer net direkt zur Verfügung.

Den HCPN koordinéiert de Moment d'Aarbechte fir déi néideg Léieren aus dem Incident ze zéien.

6. Wéi wëll d'Regierung d'Resilienz an d'Redundanz vun de staatlechen Infrastrukture verstärken, fir am Fall vun Attacken oder änlechen technesche Stéierungen e kontinuierleche Fonctionnement vun den essentiellen Zerwisser sécherzestellen?

De Secteur vun der ëffentlecher Verwaltung fält an de Beräich vun der d'Directive iwwer d'Resilienz vun de kriteschen Entitéiten. Dës Directive gëtt duerch de Projet de loi 8307 transposéiert an huet als Zil d'Resilienz vun de kriteschen Entitéiten ze stäerken. Am Sënn vun dëser Directive ergräift och de Staat um Niveau vu senge kriteschen Infrastrukturen Kontinuitéitsmoossnamen a stäerkt hir Resilienz.

Doriwwer eraus koordinéiert den HCPN zenter Enn 2024 d'Aarbechten un enger nationaler Resilienz-Strategie. Am Kader vun dëser Strategie geet et ganz allgemeng drëm fir déi Strukturen déi essentiel fir de Fonctionnement vum Land sinn, sou opzestellen a fir Redundanz um Niveau vu kritesche Ressourcë ze suergen, datt se méiglechst widderstandsfäeg sinn.

7. Dei betrafte Bierger kënnen am Fall vun engem flächendeckende Handyreseauausfall net temporär op alternativ Netzoperatoren zeréckzegräifen. Ass d'Regierung der Meenung,

dass esou een Netzwierk- oder Provider-Redundanz via Reglementéierung kéint virgeschriwwen ginn, fir eng minimal Déngschtkontinuitéit ze garantéieren? Sinn an deem Sënn legal oder technesch Dispositiounen geplangt, déi een "roaming national d'urgence" oder eng interoperabel Backup-Struktur forcéieren?

Déi haiteg mobil Telekommunikatiounsreseau sinn technesch komplex Systemer déi aus villen, aneneegräifenden Eenzelelementer bestinn. Incidende kënnen deemno op ville Niveaue passéieren déi fir d'Clientë jeeweils ënnerschiddlech Repercussiounen hunn. Deemno gëtt et och méi wéi eng technesch Variant vun Handyreseausausfäll op déi mat enger passender technescher Léisung kéint reagéiert ginn. Fir esou Léisungen auszeschaffen si pousséiert technesch Analysen noutwenneg. No dëser technescher Analys, wäerten déi néideg Verbesserungen gemaach ginn.

Lëtzebuerg, de 31. Juli 2025

Den Premierminister,

(s.) Luc FRIEDEN