N°2746
Entrée le 03.09.2025
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Äntwert vum Premierminister a vun der Verdeedegungsministesch op d'parlamentaresch Fro n° 2746 vum 6. August 2025 vum honorabelen Deputéierten Sven Clement.

1. Wéi bewäert d'Regierung de Fakt, datt an engem kuerzen Zäitraum souwuel Operateuren zu Lëtzebuerg, a Groussbritannien, a Frankräich an an der Belsch vu Cyberattacke getraff goufen?

D'Cyberattacke géint Operateuren déi an engem kuerzen Zäitraum a verschiddenen europäesche Länner stattfonnt hunn, illustréieren datt Operateuren eng privilegiéiert Cible fir Ugräifer bleiwen. D'Origine an d'Motivatioune vun den Ugräifer kënne ganz ënnerschiddlech sinn a mussen au cas par cas analyséiert ginn. Der Regierung leien aktuell keng Informatioune vir iwwert e Lien tëschent deenen ernimmten Attacken.

2. Ginn et Indicatiounen, datt dës Attacke koordinéiert oder vun der selwechter Acteursgrupp duerchgefouert goufen?

Et leien der Regierung aktuell keng Indicatioune vir, datt dës Attacke koordinéiert oder vum selwechten Acteur duerchgefouert goufen.

3. Wéi eng Informatiounen deelt Lëtzebuerg mat eisen NATO- a EU-Partneren iwwer dës Attacken?

Den Haut-Commissariat à la protection nationale (HCPN) steet a reegelméissegem Kontakt mat sengen EU Partneren. Entspriechend de Prozeduren huet den HCPN iwwert verschidde Kanäl (z.B. "EU CSIRTs Network" an "EU Cyber Crisis Liaison Organisation Network") souwuel multilateral ewéi bilateral Informatioune gedeelt.

Duerch déi lafend Ermëttlunge vun der Police ass et net méiglech méi Detailer ze ginn.

Well d'Analysen nach net ofgeschloss sinn, goufen op Säite vun der Defense bis elo keng Informatioune mat NATO- an EU-Partner gedeelt.

4. Huet d'Regierung e spezifeschen Threat Assessment iwwer déi aktuell Cyberbedrohungen fir eisen Telekommunikatiounssecteur gemaach?

Als Follow-up vum „Nevers Call" huet Lëtzebuerg am EU-Kader an als Member vum "Groupe de coopération NIS" un enger Evaluatioun vun de Menacen (Threats), Vulnerabilitéiten a Risike fir

europäesch Kommunikatiounsinfrastruktur a Reseauen deelgeholl. D'Resultater vun dëser Evaluatioun huet d'EU Kommissioun am Februar 2024 publizéiert[1].

Den Institut Luxembourgeois de Régulation (ILR) deelt reegelméisseg Informatiounen iwwer aktuell Menacen a Risike mat den Telekommunikatiounsoperateuren déi vun hinne superviséiert ginn.

Operateuren, déi eng Kontroll iwwer d'Signaliwwerdroung an hire Reseauen ausüben, musse reegelméisseg eng Risikoanalys un den ILR schécken an dem verschidde Menacen, Vulnerabilitéiten a Risike consideréiert an evaluéiert ginn.

Technesch Informatiounen zu den aktuelle Menacë kënnen awer och direkt tëscht den Operateuren a CSIRTen iwwer d'Plattform "MISP" (Malware Information Sharing Platform) ausgetosch ginn.

5. Wéi coordonéiert sech de Service de Renseignement mat internationale Partner fir dës systematesch Bedrohungen ze analyséieren?

Am Kader vu senge Missioune kooperéiert de Service de Renseignement ob enger permanenter Basis mat sengen internationalen Partner fir dës systematesch Bedrohungen ze analyséieren. Dës Echangen ënnert Experte fannen esouwuel ob bilateraler wéi multilateraler Ebene statt.

6. Ginn et Pläng fir d'national Cybersécherheetskapazitéiten ze verstäerken, wéi zum Beispill d'Schafung vun enger spezialiséierter Cyber-Eenheet?

De "Plan gouvernemental de gestion de crise cybernétique et numérique", deen sech op Cyberincidenten a -menacen awer och generell op all Typ vu Sécherheetsincidenten am digitale Beräich bezitt, definéiert de Kader fir d'Krisegestioun an dësem Beräich. Dëse Plang ass 2025 vun de staatlechen Experten iwwerschafft an erweidert ginn a gëtt zäitno dem Regierungsrot ënnerbreet.

Donieft huet d'Regierung 2024 e Konzept ausgeschafft fir eng national Cyberreserve opzestellen. D'Ëmsetzungsméiglechkeete vun esou enger nationaler Cyberreserve wäert d'Regierung am Kader vum Aktiounsplang zur nationaler Resilienzstrategie evaluéieren.

Aktuell huet Lëtzebuerg d'Méiglechkeet op d'EU-Cyberreserve zeréckzegräifen, am Fall wou eis national Kapazitéiten net géifen duergoen oder héich spezialiséiert Fachkenntnesser néideg wäre fir d'Situatioun ze geréieren. Dëst ass e spezialiséierte Service dee vun der ENISA, der Europäiescher Agence fir Cybersécherheet, geréiert gëtt, dëst am Kader vun EU Cyber Solidarity Act. De Recours op dës Reservekapazitéit gëtt iwwert den HCPN am Kader vum Plan gouvernemental de gestion de crise cybernétique et numérique organiséiert.

[1] https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

Op Säite vun der Defense ginn duerch d'Ëmsetzung vun hirer Cyberdefense Strategie Cybersécherheetskapazitéiten entwéckelt déi och national agesat ginn:

- d'Cyber Range, eng virtuell Trainingsplattform, déi ënner anerem benotzt gëtt fir d'Weiderbildung vun CybersécherheetsexpertInnen. Dës Plattform steet och de kriteschen Infrastrukturen zur Verfügung fir d'Trainéiere vun hiren ExpertInnen.
- den Opbau vun engem *Defence Security Operation Centre* (DSOC), deen spezifesch d'IT Sécherheet vun den Netzwierker a Kapazitéite vun der Defense iwwerwaacht a reagéiert am Fall vun engem Virfall. Een Informatiounsaustausch mat de relevanten nationalen Acteuren ass och eng vun den Aufgaben vum DSOC.

7. Wéi gesäit eise Bäitrag zu europäeschen oder NATO Cyber-Defense-Initiativen aus?

Lëtzebuerg ass souwuel op europäeschem wei och op NATO-Niveau u verschiddene Cyberdefense Initiative bedeelegt.

Op NATO-Niveau ass Lëtzebuerg Deel vum *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE), deen eng interdisziplinär Expertis an den Beräicher vun der Recherche, Training an Exercicen huet. An deem Kontext mécht Lëtzebuerg säit 2021 beim Cyberexercice *Locked Shields* mat. *Locked Shields* ass dee weltwäit gréissten an komplexste multinationale Cyberexercice. D'Lëtzebuerger Defense invitéiert och ëmmer CyberexpertInnen déi fir krittesch Infrastrukturen zoustänneg sinn, an ExpertInne vun anere Lëtzebuerger Entreprisen fir bei dësem Exercice matzemaachen. Lëtzebuerg ass a sëllegen Aarbechtsgruppe vertrueden an bedeelegt sech zum Beispill un der Weiderentwécklung a Support fir d'*NATO Malware Information Sharing Platform*, déi een séiert Deelen vun techneschen Informatiounen zu Malware tëschent den Alliéierten erméiglecht.

Op EU-Niveau ass Lëtzebuerg Deel vu Projeten, déi op Säite vun der *European Defence Agency* ausgeschafft ginn. Beispiller vun esou Projete sinn:

- *EU milCERT Operational Network* (MICNET), ee Projet fir d'Kommunikatioun an den Informatiounsaustausch tëschent de milCERTen[2] auszebauen.
- *Cyber Defence Exercises* (CyDef-X), eng Initiativ fir d'Koordinatioun vu Cyberexercicen op EU-Niveau besser ze koordinéieren a spezifesch Exercicen auszeschaffen.
- PESCO[3] Projeten am Beräich Cyber: Lëtzebuerg ass u verschiddene PESCO Projete bedeelegt oder mécht de Suivi dovun, sou zum Beispill bei de Projete *Cyber Ranges Federations*, *Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)* an *Cyber and Information Domain Coordination Center (CIDCC)*.

[2] MILCERT – Computer Emergency Response Team, déi zoustänneg si fir d'Behandele vun Cybersécherheetsvirfäll op militäreschen IT Kapazitéiten
[3]Permanent.Structured.Cooperation.(PESCO) huet als Ziel d'Kooperatioun am Defense Beräich tëschent den EU Memberstaaten ze verdéiwen.

8. Huet d'Attack op POST eisen nationale Contingency-Plang fir Cyberattacke beaflosst, a ginn et Updates?

De “Plan gouvernemental de gestion de crise cybernétique et numérique” gëtt generell lafend entspriechend de Lektiounen aus de rezenten Aktivatioune vum Plang aktualiséiert.

Entspriechend dem Erfarungsréckbléck zum Incident bei der POST ass den HCPN chargéiert, dem Regierungsrot zäitno Propositiounen z’ënnerbreede fir d’Resilienz vun den nationalen zivillen Kommunikatiounsinfrastrukturen ze verbesseren.

9. Wéi bereet ass Lëtzebuerg fir eng eventuell eskaléiert Cyberbedrohung, déi méi grouss Deeler vun eiser kritescher Infrastruktur betrëfft?

Am Fall vun enger eskaléierter Cyberbedrohung op Deeler vun eiser kritescher Infrastruktur, ka Lëtzebuerg op zousätzlech spezialiséiert Kapazitéite vun der EU Cyber Reserve zeréckgräifen (c.f. Äntwert op d’Fro 6). Donieft ass den HCPN an den Europäiesche Reseauen “EU CSIRTs Network” an “European Cyber Crisis Liaison Organisation Network” permanent engagéiert, fir den Echange vun techneschen an takteschen Elementer iwwer Cybermenacen a Cyberattacken, a fir d’operationell Koordinatioun um europäeschen Niveau vun der Analys an der Gestioun vun enger Cyberattack mat transnationalem Charakter.

Lëtzebuerg, den 3.September 2025.

De Premierminister,

(s.) Luc FRIEDEN