N°5850
Reçue le 07.03.2022

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

Äntwert vum Här Premierminister, Staatsminister a vum Här Verdeegegungsminister op déi dringend parlamentaresch Fro n° 5850 vum 2. Mäerz 2022 vum honorabelen Deputéierten Laurent MOSAR iwwert „cyberattaques sur des infrastructures critiques“

Ad 1)

Der Regierung ass bekannt, dass den europäesche Réseau vum Satellittebedreiwer VIASAT EUROPE LIMITED zanter dem 24. Februar deelweis gestéiert ass. Dës Stéierung vum Satellittenetzwierk huet, ënnert anerem, och zum Ausfall um Niveau vun der Iwwerwaachung, respektiv Fernsteierung vun de Wandrieder vun der Firma Enercon GmbH an Europa gefouert. Och Wandrieder vun der Lëtzebuerger Firma Soler si betraff. No den Informatioune vum Bedreiwer vun de Wandrieder ass dës Situatioun awer net direkt kritesch fir de Fonctionnement, well d'Wandrierder och ouni Satelitteverbindung bedriwwe kënne ginn.

Ad 2)

D'Regierung huet besonnesch am Kader vun der Ëmsetzung vun der nationaler Cybersécherheetsstrategie eng Rei vun Initiative geholl, vir eis national kritesch Infrastrukturen op nationalem Niveau géint Cyberattacken ze schützen, respektiv fir d'Bedreiwer vu kriteschen Infrastrukturen am Beräich Cybersécherheet ze ënnerstëtzen. Speziell am jëtzege Kontext kéint den nationalen DDoS Scrubbing Center, deen am Fall vun enger gréisserer DDoS Attack géif aktivéiert ginn, vu gréisster Wichtegkeet ginn. Iwwer 30 kritesch Infrastrukturen an wichteg Betrieber kënnen haut schonn am Noutfall vun deem Schutz profitéieren.

D'modifizéiert Gesetz vum 23. Juli 2016 iwwer den Haut-Commissariat à la protection nationale (HCPN) gesäit vir, dass de Bedreiwer vun enger kritescher Infrastruktur e "Plan de sécurité et de continuité (PSCA)" opstelle muss. Dëse Plang, deen ënnert der Responsabilitéit vum Opérateur opgestallt geet, soll op Basis vun enger Risikoanalyse d'Moossnamen fir de Schutz, d'Kontinuitéit, d'Resilienz an de Krisemanagement vun der kritescher Infrastruktur definéieren. Den HCPN kann de Bedreiwer an deem Kontext Recommandatiounen zoukomme loossen. Et ass awer de Bedreiwer hier Verantwortung fir ze décidéieren wéi eng Moossnamen ëmgesat ginn fir d'Sécherheet vun der kritescher Infrastruktur ze assuréieren.

Allgemeng ass d'Appreciatioun déi, dass d'Bedreiwer vu kriteschen Infrastrukture gutt opgestallt sinn am Beräich vun der Cybersécherheet vir a Friddenszäiten hir Servicer adequat kënnen ze assuréieren.

Mat dem Ausbrieche vum Krich an der Ukraine huet sech d'Sécherheetslaag an Europa awer fundamental geännert, esou dass och zu Lëtzebuerg d'Cybersécherheetsdispositiver un déi nei Situatioun ugepasst ginn (cf. läscht Fro).

Ad 3)

D'SES als eegestänneg kommerziell Firma hëlt hir Responsabilitéit iwwert Sécherheetsfroen op operationellem Niveau. Fir relevant Informatiounen an Décisioune gëtt de Verwaltungrot – an deem de Staat och vertrueden ass – informéiert an involvéiert, esou wéi dat bäi private Firme virgesinn ass. D'SES ass sech de Risike grad an dësem Moment absolut bewosst an hëlt esou wäit wéi méiglech Précautiounen.

Ad 4)

Wéi all aner gréisser Entreprise ginn et ëmmer erëm Cyberattacken – och an net-Krisenzäiten. A ganz eenzelne Fäll kann een net ausschléissen, dass déi net komplett vun Ufank un ofgewiert kënne ginn. Duerch d'Moossnamen déi en place sinn, gouf et awer bis elo keen Impakt vun esou Attacken – wa Problemer optriede géifen ginn déi generell ganz séier erkannt, isoléiert an ouni Schued geléist.

Ad 5)

D'SES ka wéi all aner Firma zu Lëtzebuerg vun den séllege Servicer am Beräich Cybersécherheet profitéieren, déi notamment vu Securitymadein.lu proposéiert ginn. Och am Beräich vun der Ofwier vu gréisseren DDoS Attacke géint d'Infrastrukture vun der SES zu Lëtzebuerg schafft d'Regierung mat der SES zesummen.

Ad 6)

Déi national Cybersécherheetsautoritéite sinn agebonnen an den internationale Netzwierker fir Cybersécherheet vun der Europäescher Unioun, der NATO an anere weltwäit agéierenden Organisatiounen. Si stinn am Moment an engem permanenten Austausch mat dëse Netzwierker an halen d'Evolutioun vun der Situatioun genee am A.

Aktuell musse mer vun engem erhéichtem Niveau vun der Menace ausgoen. Et ass allerdéngs zu dësem Moment keng akut Bedroung vun der Cybersécherheet a Lëtzebuerg ze erkennen.

Op nationalem Niveau ass "Cellule d'évaluation du risque cybernétique – CERC" aberuff gi fir déi aktuell Situatioun vun der Menace zu Lëtzebuerg ze suivéieren a gegebenefalls zousätzlech Moossnamen ze ergräifen.

De GOVCERT huet d'Bedreiwer vu kriteschen Infrastrukture kontaktéiert fir se op den erhéichten Niveau vun der Menace opmierksam ze maachen. Si kruten zousätzlech Recommandatioune matgedeelt an un d'Häerz geluecht, hir Systemer besonnesch aktiv ze iwwerwaachen an all Anomalie direkt ze mellen.

Et sief nach drop higewisen dass Lëtzebuerg am Fall vun enger massiver Cyberattack géint eist Land kéint, am Kader vum Kooperatiounsaccord mat der NATO, Appell un d'Ënnerstëtzung vun der NATO maachen.

Den ILR huet d'Opérateure vun essentielle Servicer genau wei vun Telekomsbetrieber ëm ee regelméissege Reporting vun Opfällegkeeten am Cyberdomaine gebieden, dat fir een enke Suivi vun der Situatioun ze maachen a fir de Fall vun Anomalien sou séier wei méiglech kënnen ze reagéieren.

Do dernieft ginn d'Opérateuren iwwert déi rezent Entwécklunge vu Cyberincidenten mat Hëllef vun engem wöchentleche Rapport vun der ENISA informéiert, a se kréien d'bonnes pratiques an der Cybersécherheet ausgedeelt.

Am Kader vun dem Gesetz iwwert d'Sécherheet vun de Réseauen an informatesche Systemer ass ee Suivi vun den nationalen Autoritéite virgesinn, fir déi strukturell an technesch Moossnamen, déi di betraffen Operateuren ergräifen, nozekucken an eventuell Lacune festzestellen.

Och am Kader vun der Cyberdéfensestrategie, déi am Aklang mat der nationaler Cybersécherheetsstrategie geschriwwe gouf, hu kritesch Infrastrukture Méiglechkeeten, fir sech beschtméiglech op Cyberattacken ze preparéieren an ze schützen (z.B. mat Weiderbildungen, Exercicen, Kooperatiounen an Austausch tëschent Experten, asw.).

Op transatlanteschem/NATO Niveau goufen och eng Rei Moossname getraff, déi déi kritesch Infrastrukturen vun den Alliéierten mat ofdecken. Sou zum Beispill den "NATO Cyber Defence Pledge", wou d'NATO-Memberlänner versprach hunn, eng Rei Moossnamen ëmzesetzen, déi d'Cybersécherheet vum Land a senge kriteschen Infrastrukturen verbessert. D'NATO évaluéiert all Joer, wat d'NATO-Memberlänner an engem Joer ëmgesat hunn. Des weideren gëtt et och um Niveau vun der NATO d'Méiglechkeet, sech mat anere Länner zu verschiddenen Themen auszetauschen, sou zum Beispill iwwert den NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), an deem och Lëtzebuerg Member ass.

Lëtzebuerg, de 7. Mäerz 2022

De Premierminister, Staatsminister

(s.) Xavier BETTEL