N°4102
Entrée le 28.05.2026
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes, de la Défense, de la
Coopération et du Commerce extérieur

Direction de la défense

Äntwert vun der Verdeedegungsministesch op d'parlamentaresch Fro n°4102 vum 18. Mee 2026 vum honorabelen Deputéierten Sven Clement

1) Ass d'Ministesch iwwer dësen Dateleak bei Thales informéiert ginn, a gouf eng Evaluatioun vun de potenzielle Risiken fir d'Lëtzebuerger Verdeedegung an national Sécherheet duerchgefouert?

Ech gouf net direkt iwwert dëse Virfall informéiert, well et aktuell keng Informatioune ginn, déi drop hindeiten, dass Donnéeë vun der Lëtzebuerger Defense betraff sinn. De Virfall gëtt vun eisem „Security Operations Center"[1] (SOC) suivéiert. Kontakt mat Thales gouf och opgeholl, fir iwwert de Virfall um neiste Stand gehalen ze ginn.

2) Benotzt d'Lëtzebuerger Arméi oder d'Directioun vun der Verdeedegung Produkter oder Servicer vu Thales? Wa jo, wéi eng, a gëtt et Indicatiounen, datt Daten aus dëse Systemer vun dësem Leak betraff kéinte sinn?

Jo, souwuel d'Lëtzebuerger Arméi wéi och d'Direktioun fir Defense benotze Produkter a Servicer vun Thales. Aus sécherheetstechnesche Grënn kënne mir keng weider Detailer dozou ginn. Et ginn aktuell keng Indizien, dass Date vun der Lëtzebuerger Defense betraff sinn. Thales ass nach amgaang hir Investigatiounen ze féieren a steet souwuel mat de franséischen Autoritéite wéi och mat der Lëtzebuerger Defense a Kontakt.

3) Gëtt et Prozedure fir ze evaluéieren, ob Lëtzebuerger Militär- oder Sécherheetspersonal an de kompromittéierten Donnéeë figuréiere kéinten, zum Beispill iwwer hir Benotzung vu LuxTrust-Servicer am beruffliche Kontext?

De SOC vun der Lëtzebuerger Defense, souwéi den MILCERT[2] a CERT Gouvernemental (GOVCERT.LU)[3], maachen de Suivi vun esou Virfäll. Hinne stinn eng Rei Méiglechkeeten zur Verfügung fir esou Virfäll ze analyséieren an ze evaluéieren. Ënner anerem si si am Kontakt mam betraffene Fournisseur souwéi mat anere CERTe fir schnellstméiglech erauszefannen ob Donnéeë vun der Lëtzebuerger Defense betraff sinn. Falls perséinlech Donnéeën involvéiert sinn, ass de Fournisseur verflicht d'EU-Dateschutz Gesetzgebung anzehalen a soumat och all betraffe Persounen driwwer z'informéiere falls seng Donnéeë geleakt goufen.

[1] Den "Luxembourg Defence Security Operations Center" (Defence SOC), ass zoustänneg fir d'Iwwerwaachung, Detektioun, Analys an d'Äntweren op Cybersécherheetsbedrohungen a Virfäll géint d'Lëtzebuerger Defense.
[2] De MILCERT.LU ass zoustänneg fir d'Äntweren op IT-Sécherheetstëschefäll bei der Lëtzebuerger Arméi. Des Funktioun gëtt vum Héije Kommissariat fir national Sécherheet assuréiert.
[3] De GOVCERT.LU ass zentrale Kontaktpunkt fir all Aarte vun IT-Tëschefäll, déi d'Informatiounssystemer vun der Regierung an aneren als kritesch agestuuften ëffentlechen oder privaten Infrastrukturbedreiwer gefäerde kéinten. Des Funktioun gëtt vum Héije Kommissariat fir national Sécherheet assuréiert.

4) Wéi eng Mesurë sinn a Plaz, fir d'Supply-Chain-Sécherheet bei Fournisseure wéi Thales z'iwwerwaachen, déi strategesch wichteg fir d'NATO a fir Lëtzebuerg sinn, besonnesch no widderhuelten Incidenter (LockBit 2022, Leak 2024, a lo erëm 2026)?

Et sinn ënnerschiddlech Mesurën *en place*. Dat geet vu spezifeschen Artikelen a Kontrakter mat de Fournisseuren, bis zur Iwwerwaachung vun der Cybersécherheetslag duerch zoustänneg Servicer wei déi vum SOC oder GOVCERT. Dës weidere spillen EU-Direktiven a Gesetzgebunge wéi d'"Directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union" (Directive NIS 2) oder de "Règlement général sur la protection des données". Dës Direktiven a Gesetzgebunge verflichten d'Fournisseuren hir Clientë souwéi zoustänneg Autoritéiten iwwer esou Virfäll ze informéieren.

Dës Weidere orientéiert d'Direktioun fir Defense sech och u bewäerte Praktike wéi déi vun der internationaler Norm ISO/IEC 27002 wou spezifesch Sécherheetsmesuren dra sti puncto Sécherheet vun der Supply-Chain.

5) Gëtt et eng Zesummenaarbecht mat der NATO respektiv mat alliéierte Partnernatiounen, fir d'Auswierkunge vun dësem Leak op gemeinsam Infrastrukturen, Kommunikatiounssystemer oder gedeelt Projeten ze evaluéieren?

Allgemeng gëtt et eng Zesummenaarbecht mat der NATO an alliéierte Partnernatiounen, mee fir dëse spezifesche Fall ass dëst aktuell net néideg well et keng Indizie ginn, dass Donnéeë vun der Defense betraff sinn.

6) Ass d'Ministesch der Meenung, datt déi opgetauchte Sécherheetsproblemer bei Thales Konsequenze fir zukünfteg Ausschreiwungen oder Kooperatioune mat dësem Fournisseur mussen hunn?

An all eisen Ausschreiwunge spille Sécherheetsaspekter eng Roll a sinn Deel vun der Evaluatioun vun den Offeren an och spéiderhin Deel vum Kontrakt mam Fournisseur. Dëst gëllt och weiderhi fir zukünfteg Ausschreiwungen a méiglech Kooperatioune mat Thales.

Lëtzebuerg, den 28. Mee 2026.

D' Verdeedegungsministesch

(s.) Yuriko Backes