N°3505
Entrée le 13.02.2026
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Digitalisation

Äntwert vun der Ministesch fir Digitaliséierung op d'parlamentaresch Fro n° 3505 vum 22. Januar 2026 vun der Madamm Diane Adehm.

1. **Wéi eng staatlech Internetsäite waren den 20. Januar 2026 konkret betraff a wéi laang waren déi jeeweileg Sitten net accessibel?**
2. **Kann Madamm Minister preziséieren ob et sech ëm eng vereenzelt an isoléiert Attack gehandelt huet oder ass se a méi engem grousse Kontext ze gesinn a steet am Zesummenhang mat deenen anere rezenten Attacken ?**
3. **Leeft d'IT-Infrastruktur vum CTIE iwwer d'Post? Wa jo, ass d'Attack bei der Post geschitt oder direkt beim CTIE ?**
4. **Wéi séier konnt déi Attack detektéiert ginn?**
5. **Wéi eng Sécherheets- a Schutzmoossname waren zu deem Zäitpunkt aktiv a hunn dës Moossname wéi virgesi gegraff?**
6. **Gëtt et Hiweiser iwwert d'Hierkonft vun der Attack ?**
7. **Waren nieft staatleche Säiten och privat Entreprise viséiert?**
8. **Kann d'Madamm Ministesch ausschléissen, datt Donnéeë geklaut gi sinn oder et zu soss engem Schued komm ass?**
9. **Wéi eng konkret Verbesserungen si virgesinn, fir d'Resilienz géint änlech Attacken zousätzlech ze stäerken?**

Duerch eng DDoS-Attack waren d'Internetsitten déi vum Zenter fir Informatiounstechnologië vum Staat (CTIE) am ".public.lu-Domaine" hebergéiert ginn, zum groussen Deel den 20. Januar Moies tëschent 07:58 an 08:39 Auer net méi erreechbar.

Eng DDoS-Attack (Distributed Denial of Service) ass en Ugréff, bei deem e Webservice duerch eng extrem héich Unzuel un Internetrequête aus villen ënnerschiddleche Quellen iwwerlaascht gëtt. De But ass net Donnéeën ze klauen, mee dofir ze suergen dass e Webservice net méi disponibel oder zumindest gestéiert ass. An dësem Fall war d'Internetpräsenz vum Staat gestéiert. D'Sitte vun de Ministèren an Administratiounen op ".gouvernement.lu" sou wéi d'App vu MyGuichet.lu an déi staatlech Back-Officen waren weider accessibel.

Cyberattacken sinn en dynamesche Prozess bei deenen d'Ugräifer reegelméisseg nei Methoden an Techniken entwéckelen fir d'Sécherheetsmesuren, déi en Place sinn, ze ëmgoen. Et ass eng Zort Kaz-a-Maus-Spill bei deem jidder Säit probéiert där anerer e Schrëtt viraus ze sinn. Soubal am Domaine vun der

IT-Sécherheet nei Protektiounsmechanismen entwéckelt ginn, probéieren d'Ugräifer nei Methode ze fannen fir dës ze ëmgoen.

Bei der DDoS-Attack vum 20. Januar waren d'Internetrequêten, déi d'Webserveren vum CTIE cibléiert hunn, esou configuréiert, dass se vun de Sécherheetsmechanismen als solch net ze erkennen waren, wat zu enger temporärer Surcharge vun de Webserveren an engem zäitwäilegen Ausfall vun der Internetpräsenz gefouert huet. D'Monitoringsystemer vum CTIE mellen eng Surcharge quasi à l'instantanée, wouropshin déi zoustänneg Ekippen analyséiere wat zu dëser Surcharge féiert a wéi se ka vun de Systemer opgefaangen ginn. Et ass net ubruecht, d'Hierkonft vum Ugréff ze veréffentlechen, fir all ongewollt Publicitéit, déi d'Ugräifer siche kéinten, ze limitéieren.

Den CTIE registréiert zanter e puer Joëren all Daag Tentativen vun Attacken op seng Systemer. Bei deenen allermeeschten dovunner verhënneren d'Mesure, dass d'Attacken en Impakt hunn.

Mat dem Zil d'Resilienz vu senge Servicer ze verstäerken, adaptéiert an optimiséiert de CTIE lafend déi verschidden, komplementar Protektiounsmechanismen déi en Place sinn fir déi staatlech IT-Infrastruktur ze schützen. 2025 huet de CTIE, zum Beispill, Disponibilitéit vun der interner staatlecher Kommunikatiounsinfrastruktur verstäerkt a seng Ubannung un d'Internetprovider weider diversifizéiert. D'Sécherheetssystemer ginn doriwwer eraus och reegelméisseg aktualiséiert fir vun neien, méi performanten Technologien ze profitéieren a mam Fortschrëtt – och deem vun den Ugräifer – kënne matzegoen.

Lëtzebuerg, den 13/02/2026.

D'Ministesch fir Digitalisierung

(s.) Stéphanie Obertin