N°4508
Entrée le 20.08.2026
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Finances

Gemeinsam Äntwert vum Premierminister, vum Finanzminister a vun der Ministesch fir Digitaliséierung op d'parlamentaresch Fro n°4508 vum 21. Juli 2026 iwwer « Cybersécurité et protection des données du cadastre et du registre foncier »

Fir d'Beäntwerung vun der parlamentarescher Fro ass et sënnvoll, de Begréff „Kadasterdonnéeën" an zwou Kategorien opzedeelen.

Engersäits ëmfaasst dëse Begréff de Kadasterplang, also de grafeschen Deel mat der Duerstellung vun de Parzellen, hiren Nummeren an, wann zoutreffend, de Gebaier déi dorop sinn.

Anerersäits ëmfaasst de Begréff d'Eegentums- an eventuell Sachrechter, déi op de jeeweilege Parzelle bestinn, besonnesch d'Donnéeë betreffend d'Eegentemer souwéi aner bestoend Rechter. Dës Informatioune ginn an de „Registres fonciers" am Kader vun der „Publicité foncière" verwalt.

Déi grafesch Kadasterdaten gi vun der Administration du cadastre et de la topographie (ACT) digital erstallt, aktualiséiert a verwalt.

D'Aktualiséierung vun den Eegentums- a Sachrechter gëtt och vun der ACT op Basis vun notariellen Akten digital virgeholl. Déi betreffend Donnéeë si gréisstendeels mat der nationaler Identifikatiounsnummer vun den Eegentemer verknäppt.

Déi zoustänneg Datebank souwéi de Module vun de « Registres fonciers » gi vum Centre des technologies de l'information de l'État (CTIE) bedriwwen a geréiert. D'ACT benotzt dëse System ausschliisslech fir d'Fortféierung, d'Historiséierung an d'Bereetstellung vun den Informatiounen.

Aus Grënn vun der Informatiounssécherheet gëtt an den Äntwerten op d'Froen op detailléiert Beschreiwunge vun techneschen Ofleef verzicht.

1. Wéi ass d'Backup-Strategie vun der ACT organiséiert, a gëtt et, wéi an anere Länner recommandéiert, eng reegelméisseg, physesch getrennte (offline oder "air-gapped") Sécherung vun de Kadaster- a Grondbuchdaten, déi net iwwer d'Netz erreechbar ass ?

Bei der ACT gi reegelméisseg Backups op een Online-System gemaach, an dee gëtt reegelméisseg och op Tape kopéiert. Dat betrëfft all d'Daten, déi vun der Verwaltung geréiert ginn, also och de Kadasterplang.

D'Datebank vun de *Registres fonciers* gëtt vum CTIE bedriwwen. De CTIE ass sech senger Expositioun bewosst, déi domadder zesummenhänkt, dass d'Administratioun als IT Provider vum Staat d'Majoritéit vun de nationale Regësteren hebergéiert. Dofir benotzt de CTIE, niewent klassesche Back-up-Léisungen,

och eng spezialiséiert Léisung déi Erpressungsversich soll verhënneren, bei deene sensibel Datebanke géife verschlësselt oder geläscht ginn.

2. Wéini gouf déi lescht Kéier gepréift respektiv getest, dass esou eng Offline-Sécherung och tatsächlech an enger raisonabeler Zäit restauréiert ka ginn ?

Et gi reegelméisseg Daten aus deene Backups zeréckgeholl. D'Date vum Kadasterplang gi reegelméisseg aus dem Backup an en Test-System gelueden, sou dass ee Restore och am Noutfall funktionéiert.

3. Ass d'ACT (respektiv d'IT-Systemer, déi si benotzt, iwwer den CTIE oder soss) als "wesentlech" oder "wichteg" Entitéit am Sënn vun der NIS2-Direktiv respektiv dem entspriechende Lëtzebuerger Gesetz agestuuft, a wat sinn d'konkret doraus resultéierend Obligatiounen a Kontrollen?

D'ACT an de CTIE ginn als « entité essentielle » (wesentlech Entitéit) am Sënn vum nationale Gesetz vum 5. Mee 2026 consideréiert.

Grondsätzlech mussen déi "wesentlech" an déi "wichteg" Entitéiten déi selwecht Sécherheetsufuerderungen ëmsetzen, wéi se an der NIS-2-Direktiv virgesi sinn.

De groussen Ënnerscheed tëscht dësen zwou Kategorie vun Entitéite läit am Beräich vun der Opsiicht duerch déi zoustänneg Autoritéit, wat zu Lëtzebuerg den ILR ass.

Déi "wichteg" Entitéite sinn enger Opsiicht ex post ënnerworf. Déi "wesentlech" Entitéiten, an domadder och d'ACT an de CTIE, ënnerleien doriwwer eraus och enger Opsiicht ex ante, wat enger ëmfaassender Opsiicht entsprécht. Dofir musse béid Entitéiten als "wesentlech" Entitéite reegelméisseg verschidden Dokumentatioune virleeën, wéi beispillsweis Risikobewäertungen oder Beschreiwunge vun de bestoende Sécherheetsmoossnamen.

4. Wéi ass den Zougang zu de sensibele Systemer vun der ACT geséchert (Multi-Faktor Authentifikatioun, Priviligenmanagement, Monitoring vun ongewéinlechen Zougréffer), fir dass en Ugréff mat geklauten, awer gültege Login-Donnéeën – wéi et bei der ANCPI de Fall war – erkannt oder verhënnert ka ginn?

Wat den Accès vun enger physescher Persoun op d'Date vun de *Registres fonciers* (beim CTIE) ugeet, ass dësen duerch eng staark Authentifizéierung mat LuxTrust Produiten oder enger 2-Faktor Léisung gereegelt. Den Accès vun aneren informatesche Systemer op dëse Register gëtt vun der ACT autoriséiert an ass duerch d'Plattform fir den automateschen Austausch vun Donnéeë vum CTIE ofgeséchert. Den Accès op all aner Applikatioun vum Kadaster funktionéiert nëmmen innerhalb vum Staatsréseau (physesch just bei der ACT oder via VPN) mat engem valide Login iwwert de Windows Domain. Fir de VPN-Accès ass och ee LuxTrust Produit oder eng 2-Faktor Léisung néideg.

5. Gouf am Kader vun der Kris bei der ANCPI oder de virdru genannte Fäll an anere Länner eng spezifesch Risikobewäertung oder e “Lessons Learned”-Prozess fir d’ACT respektiv fir aner kritesch Verwaltungsdatebanken zu Lëtzebuerg gemaach oder ugestouss?

Scho bei der Attack an der Slowakei (am Januar 2025) huet d’ACT séchergestallt, dass am Noutfall déi néideg Backups parat sinn, an déi och kënnen zeréckgesat ginn.

6. Sinn an der Vergaangenheet scho Versich vun Ugréffer oder Erpressungsversich géint d’ACT oder aner Systemer mat sensibelen Eegentums- respektiv Registerdaten (z.B. RCS, Zivilstandsregister) festgestallt ginn?

Déi automatesch Protektiounsmechanisme vum CTIE, mat deem déi staatlech IT-Infrastruktur geschützt gëtt, interceptéieren all Dag schiedlechen Internettrafic. Inwifern dës Attacke bestëmmte Systemer viséiere kann net ëmmer determinéiert ginn. Weder der ACT nach dem CTIE sinn Erpressungsversich bekannt.

7. Wéi séier géif d’ACT am Fall vun engem änlechen Ausfall (Läschung vun de produktive Systemer) hir Servicer fir Notären a Bierger nees kënne garantéieren, a gëtt et fir dëse Krisefall e formellen, reegelméisseg geteste Continuity-Plang?

D'Bierger, d’Verwaltungen an Notairë brauchen haaptsächlech Zougréff op d'*Registres fonciers* an dee gëtt vum CTIE geréiert. De CTIE baséiert sech zanter ville Joren op en SMSI (Système de Management de la Sécurité de l’Information) deen eng ganz systematiséiert Approche erlaabt fir d’Informatiounssécherheet tranversal an den Administratiounen z’assuréieren. E Schlësseloutil ass hei d’*Gestion des risques* fir Menacë proaktiv kënnen ze antizipéieren. De CTIE huet spezifesch Prozedure fir verschidden Zenarien virgesinn. Esou soll d’Verwaltung am Noutfall séier reagéiere kënnen, notamment och am Fall vum geziilte Läschen. Dës Prozedure sinn dorops ausgeluecht d’Servicer bannent engem Dag ze restauréieren a ginn och reegelméisseg getest.

Och fir de Kadasterplang ass ee Restore an engem Dag méiglech. Ee Continuity Plang gëtt donieft am Kader vun der NIS2 Direktiv formaliséiert.

8. Iwwerhëlt d’Rôle vun der CERC (Cellule d’évaluation du risque cyber) resp. vum GOVCERT och de proaktiive Monitoring vun esou spezifeschen Datebank-Infrastrukture wéi der ACT, oder läit d’Verantwortung dofir eleng bei der Verwaltung selwer?

De GOVCERT.LU assuréiert e proaktive Monitoring an eng Detektioun fir de Reseau vum Staat an enger Perimeter Approche. Dat deckt d'Servicer of déi vum Internet aus accessibel sinn an awer och intern Netz Iwwergäng. Am Fall wou eppes opfält gëtt mat der betraffener Verwaltung eng Analyse gemaach a jee no Fall reagéiert. Entspriechend der Envergure vum Incident kënnen d’Mechanisme vun der Krisegestioun

aktivéiert ginn, esou wéi se am *Plan gouvernemental de gestion de crise cybernétique et numérique* definéiert sinn. Den nationalen Impakt vum Incident gëtt an der *Cellule d'Évaluation du Risque Cyber (CERC)* entspriechend engem nationale Klassifikatiounssystem bewäert. Géigemoossname fir den Incident anzegrenzen an den Impakt ze reduzéiere kënnen och an der CERC diskutéiert a beschloss ginn. Wa politesch Decisiounen néideg sinn, kann d'Krisegestioun eskaléiert gi mat der Convocatioun vun enger Cellule de Crise (CC).

Lëtzebuerg, den 20. August 2026
De Finanzminister
(s.) Gilles Roth