ACCIÓ

Catalonia Trade & Investment

INFORME JUSTIFICATIU DE LA COMPRA D'EMERGÈNCIA CABINA EMMAGATZEMATGE

La nit del passat 19 de juny, ACCIÓ va patir un incident greu de seguretat informàtica que va comprometre la seguretat, disponibilitat i integritat dels sistemes d'informació essencials per al funcionament de l'entitat (es va produir un ciberatac per ransomware).

Aquests fets s'han posat en coneixent de les autoritats pertinents: Agència de Ciberseguretat de Catalunya, APdCAT i denúncia davant els Mossos d'Esquadra.

Aquest atac va deixar encriptada tota la informació (servidors, serveis, dades) d'emmagatzematge al Centre de Processament de Dades, a la cabina HP MSA2025 que ACCIÓ tenia en producció i va provocar la interrupció de serveis digitals essencials, el risc de pèrdua de dades sensibles i confidencials i la necessitat immediata de contenir i mitigar l'impacte del ciberatac.

Davant d'aquesta situació, i seguint les recomanacions dels equips tècnics i de l'Agència de Ciberseguretat de Catalunya, s'ha determinat la necessitat urgent de reubicar i protegir físicament els servidors afectats mitjançant la instal·lació de cabines específiques amb sistemes de seguretat reforçada, refrigeració adequada i aïllament electromagnètic.

En el decurs de la investigació per part de l'Agència de Ciberseguretat de Catalunya se'ns informa que la cabina d'ACCIÓ no es pot recuperar ja que conté dades que poden permetre esbrinar el vector inicial de l'atac i que, a més, pot ser requerida per altres autoritats a nivell europeu.

Des de l'àrea IT d'ACCIÓ es comença a treballar en la recuperació de servidors, serveis i dades utilitzant una cabina d'emmagatzematge que estava aturada, que ja no té garantia ni suport de fabricant i, a més, és sensiblement menys eficient que l'anterior.

En el moment de posar en producció els serveis que s'estan recuperant ens trobem amb:

- Poca fiabilitat del sistema d'emmagatzematge, que pot causar caigudes dels sistemes i pèrdua de dades.
- Sense suport tècnic del fabricant.
- Sense un sistema vàlid de còpies de seguretat un cop recuperat el servei després de l'incident.

Davant aquesta situació, entenem que existeix un perill greu i imminent de perdre tota la informació de què disposa ACCIÓ, en cas de fallides del sistema o de nous atacs. Addicionalment, estarien compromesos els drets i llibertats de les persones, ja que es podria produir un accés il·legítim a les seves dades personals, de què la ACCIÓ n'és responsable.

Per tot l'exposat, entenem que la situació en la que es troba ACCIÓ és compatible amb els supòsits de l'article 120 de la Llei de Contractes del Sector Públic, i per tant, sol·licitem la contractació d'una cabina d'emmagatzematge, amb les prestacions similars o superiors a l'esmentada anteriorment, i segons la disponibilitat del mercat, considerant la contractació per la via d'emergència, que permeti:

- Dotar als usuaris d'un servei eficient amb accés a discs SSD .
- Fiabilitat de tenir el suport i la garantia del fabricant.

Meritxell Rosich
Directora de la Unitat de Talent i Recursos

Generalitat de Catalunya