TWEĠIBIET TAL-KUMMISSJONI EWROPEA

GĦAR-RAPPORT SPEĊJALI TAL-QORTI EWROPEA TAL-AWDITURI

Iċ-ċibersigurtà tal-istituzzjonijiet, il-korpi u l-aġenziji tal-UE: Il-livell ta' tħejjija b'mod ġenerali mhux proporzjonat mat-theddid

Kontenut

Dan id-dokument jippreżenta t-tweġibiet tal-Kummissjoni Ewropea għall-osservazzjonijiet ta' rapport speċjali tal-Qorti Ewropea tal-Awdituri, f'konformità mal-Artikolu 259 tar-Regolament Finanzjarju u li għandu jiġi ppubblikat flimkien mar-Rapport Speċjali.

I. IL-KUMMISSJONI TWIEĠEB FIL-QOSOR

a) Introduzzjoni ġenerali

Iċ-ċibersigurtà saret prijorità politika u operazzjonali ewlenija tal-Kummissjoni Ewropea. Il-kriżi tal-COVID aċċellerat id-dipendenza tagħna fuq is-servizzi diġitali (cloud computing, apparat mobbli, intelliġenza artifiċjali). F'dawn l-aħħar sentejn, rajna bidla kbira lejn ix-xogħol mid-dar. Dan ifisser li kemm iċ-ċiberkriminalità kif ukoll l-ispjunaġġ ċibernetiku, iż-żewġ theddidiet ewlenin li qed jiffaċċjaw l-EUIBAs (Istituzzjonijiet, Korpi u Aġenziji tal-Unjoni Ewropea), effettivament saru wkoll online b'mod estensiv. Il-Kummissjoni tirrikonoxxi din it-tendenza. Hija wriet tmexxija konsistenti u deċiżiva fiċ-ċibersigurtà. L-Att dwar iċ-Ċibersigurtà daħal fis-seħħ fl-2019, u fost l-oħrajn espanda l-mandat tal-ENISA u poġġieh fuq bażi permanenti. Dan l-Att stabbilixxa wkoll kooperazzjoni formali bejn l-ENISA u s-CERT-UE (it-tim ta' rispons f'emerġenza relatata mal-kompjuters li jappoġġa l-EUIBAs kollha). Fl-2020, il-Kummissjoni pproponiet tisħiħ tad-Direttiva dwar is-Sigurtà tan-Networks u tal-Informazzjoni, li daqt jintlaħaq qrib fuqu fil-leġiżlatura.

L-Istrateġija taċ-Ċibersigurtà tal-2020 kien fiha wkoll tliet azzjonijiet li jaffettwaw iċ-ċibersigurtà tal-EUIBAs. Hija ħabbret Regolament dwar is-Sigurtà tal-Informazzjoni fil-korpi u l-aġenziji tal-istituzzjonijiet tal-UE, Regolament dwar ir-Regoli Komuni dwar iċ-Ċibersigurtà għall-istituzzjonijiet, il-korpi u l-aġenziji tal-UE u l-intenzjoni tagħha li tipprovdi bażi legali ġdida għas-CERT-UE biex issaħħaħ il-mandat u l-finanzjament tagħha biex tiżgura r-riżorsi adegwati tagħha fid-dawl ta' theddid, riskji u inċidenti li qed jiżdiedu.

Il-ħidma tat-tħejjija ta' dawn il-proposti mxiet 'il quddiem. Għalkemm għadhom ma ġewx adottati mill-Kulleġġ, huwa mistenni li dawn jiġu adottati fl-ewwel kwart tal-2022. Kwistjonijiet importanti diskussi bejn l-istituzzjonijiet f'dan l-istadju preparatorju jikkonċernaw il-bażi legali tal-proposta kif ukoll il-kapaċità baġitarja tal-EUIBAs kollha biex jissodisfaw ir-rekwiżiti kemm f'termini ta' finanzjament tal-ħtiġijiet taċ-ċibersigurtà tagħhom stess kif ukoll biex isibu r-riżorsi meħtieġa biex jappoġġaw is-CERT-UE, il-baġit u b'mod partikolari l-karigi.

Il-livell ta' tħejjija għaċ-ċibersigurtà tal-istituzzjonijiet, il-korpi u l-aġenziji tal-UE għandu livelli differenti ta' maturità. Diversi EUBIAs għandhom prestazzjoni b'saħħitha f'termini ta' tħejjija ċibernetika u jenħtieġ li jkomplu jservu bħala mexxejja, filwaqt li jistimulaw u jispiraw il-progress u aktar titjib fix-xenarju kollu taċ-ċibersigurtà. Sabiex jinkiseb progress li jista' jitkejjel, huwa importanti li jiġu rikonoxxuti l-livelli differenti ta' maturità fost l-EUIBAs u li jiġu stabbiliti prijoritajiet billi l-azzjonijiet ta' titjib jiġu diretti l-ewwel nett lejn dawk l-EUIBAs fejn il-lakuni identifikati jwasslu għall-ogħla skopertura għar-riskju.

b) Il-pożizzjoni tal-Kummissjoni dwar l-osservazzjonijiet u r-rakkomandazzjonijiet ewlenin tal-QEA

Il-Kummissjoni tilqa' r-rapport tal-QEA dwar iċ-Ċibersigurtà tal-istituzzjonijiet, il-korpi u l-aġenziji tal-UE. Tieħu nota li r-rapport jissottolinja l-importanza ta' oqfsa legali komuni għall-EUIBAs kollha dwar is-sigurtà tal-informazzjoni u ċ-ċibersigurtà biex jiżdied il-livell ġenerali taċ-ċibersigurtà b'mod ġenerali. Il-Kummissjoni tinnota li l-osservazzjonijiet u r-rakkomandazzjonijiet ewlenin tal-QEA mhumiex immirati lejn iċ-ċibersigurtà operazzjonali proprja tal-Kummissjoni nnifisha, iżda lejn ir-rwol ta' politika tal-Kummissjoni li tipproponi leġiżlazzjoni biex iżżid il-maturità ċibernetika tal-EUIBAs.

Ir-regolamenti futuri dwar is-"Sigurtà tal-Informazzjoni fil-korpi u l-aġenziji tal-istituzzjonijiet tal-UE" u r-"Regoli Komuni dwar iċ-Ċibersigurtà għall-istituzzjonijiet, il-korpi u l-aġenziji tal-UE" se jistabbilixxu r-regoli komuni biex jinkisbu livelli għoljin ta' sigurtà tal-informazzjoni u ċibersigurtà iżda l-implimentazzjoni tagħhom, fil-kuntest organizzazzjonali u operazzjonali ta' kull EUIBA (b'mod partikolari, il-profili tat-theddid u tar-riskju tagħhom), tibqa' taħt ir-responsabbiltà awtonoma tal-EUIBAs. Ir-Regolament propost dwar iċ-ċibersigurtà se jkollu mekkaniżmi ta' konformità li jkunu xierqa u proporzjonati għall-objettiv u l-kamp ta' applikazzjoni tar-regoli l-ġodda, mingħajr preġudizzju għall-awtonomija tal-istituzzjonijiet, il-korpi u l-aġenziji.

Il-Kummissjoni bħalissa tippresjedi s-sottogrupp taċ-ċibersigurtà tal-kumitat interistituzzjonali dwar it-trasformazzjoni diġitali (ICDT) li huwa ħatra b'rotazzjoni (għal perjodu ta' mhux aktar minn sentejn (2)). Ta' min jinnota li ma ngħatawx riżorsi ddedikati għall-ħidma tas-sottogrupp: l-azzjonijiet kollha huma bbażati fuq l-aħjar sforzi mill-parteċipanti fuq bażi volontarja.

Il-Kummissjoni taqbel mal-idea ġenerali li jissaħħu r-riżorsi u l-mandat tas-CERT-UE.

B'dan il-fehim, il-Kummissjoni tappoġġa l-osservazzjonijiet u r-rakkomandazzjonijiet ewlenin tar-rapport. Il-pożizzjoni dettaljata tagħna hija spjegata fil-kummenti addizzjonali fit-Taqsima III. Rigward ir-rakkomandazzjonijiet, il-Kummissjoni taċċetta r-rakkomandazzjonijiet 1a, b, c, d, e, f, g u 2a, b, c.

c) L-aħħar żviluppi rilevanti u l-passi li jmiss

Tlestiet konsultazzjoni formali fil-livell tad-Diretturi Ġenerali tal-EUIBAs dwar l-abbozzi konsolidati taż-żewġ Regolamenti (sigurtà tal-informazzjoni, ċibersigurtà) u l-valutazzjoni tal-feedback riċevut għadha għaddejja, qabel it-tlestija tal-pakkett u l-adozzjoni mill-Kulleġġ fl-ewwel kwart tal-2022.

II. TWEĠIBIET TAL-KUMMISSJONI GĦALL-OSSERVAZZJONIJIET EWLENIN TAL-QEA

1. Livelli ta' maturità taċ-ċibersigurtà tal-EUIBAs

Il-Kummissjoni taqbel li meta jiġi osservat il-livell ta' nfiq mill-EUIBAs fuq iċ-ċibersigurtà huwa importanti li jitqiesu t-theddid u r-riskji.

Bl-istess mod, fir-rigward tal-aspett tar-riżorsi umani, l-istabbiltà tal-persunal tal-EUIBA hija influwenzata minn għadd ta' fatturi. Is-suq għar-reklutaġġ ta' esperti speċjalizzati fiċ-ċibersigurtà qed isir dejjem aktar kumpless. F'ħafna każijiet, ir-regoli dwar ir-riżorsi umani mhumiex adattati għal profili speċjalizzati (reklutaġġ, żvilupp tal-karriera, taħriġ). Barra minn hekk, il-pressjoni ġeneralizzata fuq il-livelli tal-persunal fl-EUIBAs mill-awtorità baġitarja tfisser li oqsma emerġenti ta' prijorità għolja bħaċ-ċibersigurtà jibqgħu sottofornuti mill-karigi, b'mod partikolari fis-servizzi operazzjonali interni.

Ir-referenza għall-progress fil-governanza u l-ġestjoni tar-riskju jenħtieġ li tqis il-fatt li l-monitoraġġ tal-konformità issa miexi minn proġett pilota għal introduzzjoni sħiħa. Għalhekk, huwa normali li l-kopertura s'issa hija pjuttost baxxa. Dan il-proġett ta' konformità huwa l-istadju li jmiss ta' proċess ta' titjib fil-maturità ċibernetika fit-tul li beda bid-definizzjoni ta' metodoloġija komuni tar-riskju, il-kostruzzjoni ta' għodod komuni, l-introduzzjoni tal-ġestjoni tal-vulnerabbiltà u l-

monitoraġġ, l-ittestjar u l-validazzjoni tal-inventarju tal-assi. Sar progress f'din it-triq twila minkejja l-kumplessità tal-bażi tal-assi tal-Kummissjoni b'aktar minn 1 000 sistema ta' informazzjoni mħaddma minn aktar minn 50 Direttorat Ġenerali u Aġenziji Eżekuttivi.

2. Mekkaniżmi ta' kooperazzjoni tal-EUIBAs

Is-CERT-UE hija storja fenomenali ta' suċċess fil-promozzjoni tal-kooperazzjoni mhux biss bejn l-EUIBAs, iżda wkoll fil-livell Ewropew, permezz tal-parteċipazzjoni tagħha bħala membru sħiħ tan-network tas-CSIRT stabbilit skont id-Direttiva NIS. B'dan il-mod, is-CERT-UE hija każ eżemplari ta' kif jistgħu jissaħħu l-kooperazzjoni u s-servizzi taċ-ċibersigurtà. L-osservazzjonijiet tal-QEA dwar is-CERT-UE juru b'mod ċar ħafna x-xogħol eċċezzjonali li qed tagħmel is-CERT-UE fid-dawl ta' xenarju ta' theddid ċibernetiku dejjem aktar ostili u b'nuqqas ta' riżorsi kroniċi.

Skont l-Arranġament Interistituzzjonali (IIA) attwali, l-aġenziji deċentralizzati u l-impriżi konġunti tal-UE huma rrappreżentati uffiċjalment fil-bord ta' tmexxija tas-CERT-UE mill-ENISA. Barra minn hekk, il-fehmiet tagħhom huma espressi fil-laqgħat tal-bord ta' tmexxija minn rappreżentant tal-Kumitat Konsultattiv tal-ICT (ICTAC), li jista' jattendi biex jassisti lill-ENISA fir-rwol tagħha li tirrappreżenta l-aġenziji iżda ma għandha l-ebda sede jew vot formali. Il-punt ta' rappreżentanza adegwata tal-aġenziji fil-bord ta' tmexxija tas-CERT-UE se jiġi indirizzat fir-Regolament propost billi titlesta l-kompożizzjoni tal-bord ta' tmexxija b'sa tliet rappreżentanti maħtura min-Network tal-Aġenziji tal-Unjoni (EUAN), fuq proposta mill-Kumitat Konsultattiv tal-ICT tiegħu.

Il-parteċipazzjoni fis-sottogrupp taċ-ċibersigurtà tal-ICDT issir fuq bażi tal-aħjar sforz, fil-livell ta' involviment deċiż minn kull EUIBA. It-titjib fil-kondiviżjoni tal-informazzjoni dwar l-akkwist, bħala suġġett importanti fil-kamp ta' applikazzjoni tat-Task Force 2 tas-Sottogrupp dwar iċ-Ċibersigurtà, qed jiġi indirizzat fit-tħejjija tal-kuntratt qafas il-ġdid taċ-ċibersigurtà.

Fir-rigward tal-għodod komuni għal servizzi bħall-email u l-vidjokonferenza, diġà hemm il-faċilità li tintuża s-sistema SECEM-2 implimentata mill-Kummissjoni għall-EUIBAs kollha, għal posta elettronika kriptata skont il-ġestjoni effettiva tal-kjavi u ċ-ċertifikati tal-kriptaġġ. Barra minn hekk, is-SECABC, għodda li tippermetti l-kriptaġġ tal-posta elettronika bejn l-istituzzjonijiet qed tiġi żviluppata, bl-intenzjoni li toffri aċċess għaliha lil kull EUIBA interessat mill-2022. Il-vidjokonferenzi siguri għas-servizzi ta' SNC diġà nkisbu u jistgħu jiġu estiżi għal EUIBAs oħra fuq bażi *ad hoc* billi jiġu ġestiti l-identitajiet tal-parteċipanti fil-laqgħa. Il-kondiviżjoni ta' informazzjoni sensittiva se tiġi indirizzata wkoll fir-Regolament propost dwar is-sigurtà tal-informazzjoni (jiġifieri permezz ta' tikkettar u mmarkar komuni).

3. Kondiviżjoni ta' informazzjoni dwar inċidenti jew vulnerabbiltajiet sinifikanti

Il-fatt li mhux l-EUIBAs kollha qed jinnotifikaw lis-CERT-UE dwar inċidenti jew vulnerabbiltajiet sinifikanti huwa indirizzat fl-abbozz tar-Regolament dwar iċ-ċibersigurtà f'konformità mal-proposta tal-Kummissjoni fid-Direttiva NIS-2[1]. Il-livell ta' implimentazzjoni se jiddependi fuq riżorsi addizzjonali ddedikati għal dan mill-EUIBAs awtonomi. L-ambitu għall-infurzar ta' tali notifiki għadu limitat, inkluż skont ir-Regolament propost kif ippjanat bħalissa, minħabba l-awtonomija

[1] Il-Proposta għal Direttiva tal-Parlament Ewropew u tal-Kunsill dwar miżuri għal livell għoli komuni ta' ċibersigurtà madwar l-Unjoni kollha, li tħassar id-Direttiva (UE) 2016/1148, COM/2020/823

istituzzjonali tal-EUIBAs. Ir-Regolament propost dwar iċ-ċibersigurtà se jkollu mekkaniżmi ta' konformità li jkunu xierqa u proporzjonati għall-objettiv u l-kamp ta' applikazzjoni tar-regoli l-ġodda, mingħajr preġudizzju għall-awtonomija tal-istituzzjonijiet, il-korpi u l-aġenziji.

III. IL-KUMMISSJONI TWIEĠEB GĦALL-KONKLUŻJONIJIET U R-RAKKOMANDAZZJONIJIET TAL-QEA

Rakkomandazzjoni 1 – Titjib tat-tħejjija għaċ-ċibersigurtà tal-EUIBAs kollha permezz ta' regoli vinkolanti komuni u żieda fir-riżorsi għas-CERT-UE

It-test propost tar-Regolament se jinkludi miżuri speċifiċi mfassla biex ikomplu jżidu l-livell komuni taċ-ċibersigurtà. Dawn il-miżuri se jissarrfu fi pjanijiet taċ-ċibersigurtà, definiti u implimentati fil-livell tal-EUIBAs skont il-qafas ta' governanza taċ-ċibersigurtà tagħhom stess.

Il-Kummissjoni taċċetta din ir-rakkomandazzjoni. B'referenza għas-subrakkomandazzjonijiet speċifiċi, il-Kummissjoni tinnota dan li ġej:

a) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1a. L-abbozz ta' Regolament se jinkludi dispożizzjonijiet dwar l-oqfsa ta' governanza u kontroll, stabbiliti fl-ogħla livell ta' ġestjoni eżekuttiva ta' kull EUIBA, biex tiġi żgurata ġestjoni effettiva u prudenti tar-riskji kollha taċ-ċibersigurtà.
b) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1b. L-abbozz ta' Regolament se jsaħħaħ ir-referenza għall-approċċ ibbażat fuq ir-riskju għall-ġestjoni taċ-ċibersigurtà billi jagħmilha ċara li l-azzjonijiet, il-pjanijiet għas-sigurtà tal-IT u l-implimentazzjoni reali tal-kontrolli essenzjali jenħtieġ li jsegwu l-valutazzjonijiet.
c) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1c. L-edukazzjoni dwar iċ-ċibersigurtà, il-programmi ta' sensibilizzazzjoni u ta' taħriġ se jiġu kkwotati bħala parti mil-linja bażi taċ-ċibersigurtà fl-abbozz ta' Regolament.
d) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1d. Fl-esperjenza tagħna, għalkemm l-awditi u t-testijiet regolari huma essenzjali, dawn mhumiex biżżejjed biex jiżguraw li qed isir progress. Għalhekk, huma meħtieġa rapportar u trasparenza regolari, bħala parti mill-qafas ta' governanza taċ-ċibersigurtà taħt il-punt a).
e) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1e. L-abbozz ta' Regolament se jinkludi dispożizzjonijiet relatati man-notifika, mill-EUIBAs, ta' theddid, vulnerabbiltajiet u inċidenti ċibernetiċi sinifikanti lis-CERT-UE.
f) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1f. Il-Kummissjoni tappoġġa l-ħtieġa li jissaħħu r-riżorsi tas-CERT-UE. Dispożizzjonijiet relatati mal-persunal u l-kontribuzzjonijiet finanzjarji mill-EUIBAs se jiġu inklużi fit-test tal-abbozz ta' Regolament.
g) Il-Kummissjoni taċċetta r-rakkomandazzjoni 1g. Ir-Regolament propost se jkollu mekkaniżmi ta' konformità li huma proporzjonati u proporzjonati għall-objettiv u l-kamp ta' applikazzjoni tad-dispożizzjonijiet, fir-rigward tal-awtonomija istituzzjonali tal-EUIBAs. Il-kontenut tar-Regolament futur jiddependi fuq l-eżitu tal-proċedura leġiżlattiva u huwa r-riżultat ta' deċiżjoni meħuda mil-Leġiżlatur tal-UE fir-rigward tal-proposta magħmula mill-Kummissjoni.

Rakkomandazzjoni 2 – Jiġu rakkomandati aktar sinerġiji fost l-EUIBAs f'oqsma magħżula

Il-Kummissjoni, li bħalissa qed tippresjedi s-Sottogrupp taċ-Ċibersigurtà tal-Kumitat Interistituzzjonali għat-Trasformazzjoni Diġitali (ICDT), taqbel mar-rakkomandazzjonijiet biex jiġu promossi s-soluzzjonijiet għal kondiviżjoni konsistenti u sigura ta' informazzjoni sensittiva, il-kondiviżjoni sistematika ta' informazzjoni dwar proġetti taċ-ċibersigurtà u oqfsa komuni tal-akkwist u kuntratti għas-servizzi taċ-ċibersigurtà.

Il-Kummissjoni taċċetta din ir-rakkomandazzjoni. B'referenza għas-subrakkomandazzjonijiet speċifiċi, il-Kummissjoni tinnota dan li ġej:

a) Il-Kummissjoni taċċetta r-rakkomandazzjoni 2a. Il-Kummissjoni qed tressaq inizjattivi u servizzi tekniċi lis-Sottogrupp taċ-Ċibersigurtà tal-ICDT biex tippromwovi u tappoġġa għodod komuni għall-kondiviżjoni ta' informazzjoni sensittiva, li jippermetti s-servizzi bħall-email u l-vidjokonferenza. Aħna nosservaw ukoll li l-marki komuni u r-regoli komuni ta' trattament għal informazzjoni sensittiva mhux klassifikata se jiġu indirizzati fir-Regolament propost dwar is-sigurtà tal-informazzjoni.
b) Il-Kummissjoni taċċetta r-rakkomandazzjoni 2b. It-task forces eżistenti taħt is-Sottogrupp taċ-Ċibersigurtà tal-ICDT qed jindirizzaw dan il-punt u se jiġu żviluppati aktar. It-titjib fil-kondiviżjoni tal-informazzjoni dwar l-akkwist qed jiġi indirizzat fit-tħejjija tal-kuntratt qafas il-ġdid taċ-ċibersigurtà.
c) Il-Kummissjoni taċċetta r-rakkomandazzjoni 2c. L-EUIBAs diġà għandhom aċċess għal kuntratti qafas interistituzzjonali fil-qasam tal-ICT ġestiti mill-Kummissjoni. It-tħejjija tal-kuntratt qafas il-ġdid taċ-ċibersigurtà se tiġi kkoordinata mas-Sottogrupp taċ-Ċibersigurtà tal-ICDT.

Rakkomandazzjoni 3 – Żieda fl-enfasi tas-CERT-UE u tal-ENISA fuq EUIBAs inqas maturi

Din ir-rakkomandazzjoni hija indirizzata lis-CERT-UE u lill-ENISA.