EUROPEISKA KOMMISSIONENS SVAR

PÅ EUROPEISKA REVISIONSRÄTTENS SÄRSKILDA RAPPORT

Cybersäkerheten vid EU:s institutioner, organ och byråer: beredskapsnivån står inte i proportion till hoten

SV

SV

Innehållsförteckning

I. KOMMISSIONENS SVAR I KORTHET 2

a) Allmän inledning 2

b) Kommissionens ställningstagande till revisionsrättens viktigaste iakttagelser och rekommendationer 2

c) Den senaste utvecklingen och nästa steg 3

II. KOMMISSIONENS SVAR PÅ REVISIONSRÄTTENS HUVUDSAKLIGA IAKTTAGELSER 3

1. Nivåer av cybersäkerhetmognad vid EU:s institutioner, organ och byråer 3

2. Samarbetsmekanismer för EU:s institutioner, organ och byråer 4

3. Utbyte av information om betydande incidenter eller sårbarheter 5

III. KOMMISSIONENS SVAR PÅ REVISIONSRÄTTENS SLUTSATSER OCH REKOMMENDATIONER 5

Rekommendation 1 – Förbättra cybersäkerhetsberedskapen hos alla EU:s institutioner, organ och byråer genom gemensamma bindande regler och ökade resurser för CERT-EU 5

Rekommendation 2 – Verka för ytterligare synergieffekter bland EU:s institutioner, organ och byråer på utvalda områden 6

Rekommendation 3 – Öka CERT-EU:s och Enisas fokus på de av EU:s institutioner, organ och byråer som är mindre mogna 6

I detta dokument presenteras Europeiska kommissionens svar på iakttagelserna i en särskild rapport från Europeiska revisionsrätten i enlighet med artikel 259 i budgetförordningen. Dokumentet ska offentliggöras tillsammans med den särskilda rapporten.

I. KOMMISSIONENS SVAR I KORTHET

a) Allmän inledning

Cybersäkerhet har blivit en högt prioriterad politisk och operativ fråga för Europeiska kommissionen. Covid-krisen har ökat vårt beroende av digitala tjänster (molntjänster, mobila enheter och artificiell intelligens). Under de två senaste åren har vi sett en mycket omfattande övergång till att arbeta hemifrån. Detta betyder att både cyberkriminalitet och cyberspionage, som utgör de två största hoten mot EU:s institutioner, organ och byråer, också har ökat i stor skala. Kommissionen uppmärksammar denna tendens. Den har visat konsekvent och handlingskraftigt ledarskap i fråga om cybersäkerhet. Genom cybersäkerhetsakten som trädde i kraft 2019 utvidgades Enisas mandat och byrån inrättades permanent. Genom akten upprättades även ett formellt samarbete mellan Enisa och CERT-EU (incidenthanteringsorganisationen som bistår alla EU:s institutioner, organ och byråer). Kommissionen föreslog 2020 en förstärkning av direktivet om säkerhet i nätverks- och informationssystemen, vilken nu närmar sig en överenskommelse i den lagstiftande församlingen.

Strategin för cybersäkerhet från 2020 innehöll också tre åtgärder av betydelse för cybersäkerheten vid EU:s institutioner, organ och byråer. Dessa bestod i en förordning om informationssäkerhet hos EU:s institutioner, organ och byråer, en förordning om gemensamma cybersäkerhetsregler för EU:s institutioner, organ och byråer och avsikten att ta fram en ny rättslig grund för CERT-EU för att stärka dess mandat och finansiering så att organisationen har lämpliga resurser för att hantera ökade hot, risker och incidenter.

Arbetet med att bereda dessa förslag går framåt. Även om de ännu inte har antagits av kollegiet, bör så ske under första kvartalet 2022. Viktiga frågor som diskuteras institutionerna emellan i detta förberedande skede är bland annat förslagets rättsliga grund samt de budgetresurser som institutionerna, organen och byråerna har för att uppfylla kraven, både vad gäller att tillgodose deras egna behov av cybersäkerhet och att få fram nödvändiga resurser till stöd för CERT-EU:s budget och för särskilda tjänster.

Cybersäkerhetsberedskapen vid EU:s institutioner, organ och byråer har olika nivåer av mognad. Flera av dem har mycket god beredskap och bör fortsätta att tjäna som föredömen som uppmuntrar och inspirerar till framsteg och fortsatta förbättringar i hela cybersäkerhetslandskapet. I syfte att göra mätbara framsteg är det viktigt att ta hänsyn till deras olika nivåer av cybersäkerhetsmognad samt att göra prioriteringar genom att först rikta åtgärderna mot dem vars identifierade brister gör dem mest utsatta för risker.

b) Kommissionens ställningstagande till revisionsrättens viktigaste iakttagelser och rekommendationer

Kommissionen välkomnar revisionsrättens rapport om cybersäkerheten vid EU:s institutioner, organ och byråer. Den noterar att man i rapporten framhåller vikten av att alla EU:s institutioner, organ och byråer omfattas av gemensamma rättsliga ramar för informationssäkerhet och cybersäkerhet så att den allmänna cybersäkerhetsnivån höjs för alla. Kommissionen noterar även att revisionsrättens huvudsakliga iakttagelser och rekommendationer inte riktar sig till kommissionens egna operativa cybersäkerhet som sådan, utan till dess politiska roll som den institution som föreslår lagstiftning som leder till att cybermognaden vid EU:s institutioner, organ och byråer ökar.

De kommande förordningarna om informationssäkerhet hos EU:s institutioner, organ och byråer och om gemensamma cybersäkerhetsregler för EU:s institutioner, organ och byråer kommer att innehålla gemensamma regler för hur höga nivåer av informationssäkerhet och cybersäkerhet ska uppnås. Det är dock institutionerna, organen och byråerna som självständigt ska genomföra dem inom de egna organisatoriska och operativa ramarna (särskilt i fråga om hot och riskprofil). Den föreslagna förordningen om cybersäkerhet kommer att innehålla mekanismer för efterlevnad som är lämpliga och står i proportion till de nya reglernas syfte och omfattning utan att detta påverkar institutionernas, organens och byråernas självständighet.

Kommissionen är för närvarande ordförande för undergruppen för cybersäkerhet vid den interinstitutionella kommittén för digital omställning (ICDT), vilket är ett roterande ordförandeskap (i upp till två år). Noteras ska att inga särskilda resurser har avsatts för undergruppen, utan all verksamhet baseras på att deltagarna frivilligt gör sitt bästa.

Kommissionen samtycker till den allmänna uppfattningen om att förstärka CERT-EU:s resurser och mandat.

Med denna tolkning stöder kommissionen de viktigaste iakttagelserna och rekommendationerna i rapporten. Vårt ställningstagande förklaras närmare i de ytterligare kommentarerna i avsnitt III. Vad gäller rekommendationerna godtar kommissionen 1a, b, c, d, e, f och g samt 2a, b och c.

c) Den senaste utvecklingen och nästa steg

Generaldirektörerna för EU:s institutioner, organ och byråer har avslutat sitt formella samråd om de konsoliderade förslagen till de två förordningarna (om informationssäkerhet och cybersäkerhet), och en bedömning av återkopplingen genomförs för närvarande innan paketet slutförs och antas av kollegiet under första kvartalet 2022.

II. KOMMISSIONENS SVAR PÅ REVISIONSRÄTTENS HUVUDSAKLIGA IAKTTAGELSER

1. Nivåer av cybersäkerhetmognad vid EU:s institutioner, organ och byråer

Kommissionen delar uppfattningen att det är viktigt att ta hot och risker med i beräkningen när institutionernas, organens och byråernas utgifter för cybersäkerhet iakttas.

Vad avser personalaspekten påverkas dess stabilitet vid EU:s institutioner, organ och byråer på samma sätt av ett antal faktorer. Marknaden för rekrytering av cybersäkerhetsexperter blir alltmer komplex. I många fall är personalreglerna inte anpassade till specialiserade yrkesprofiler (rekrytering, karriärutveckling och utbildning). Dessutom innebär budgetmyndighetens allmänna tryck på personalnivåer vid institutionerna, organen och byråerna att nya högt prioriterade områden, t.ex. cybersäkerhet, inte har tillräckligt med tjänster, särskilt vad gäller det interna operativa arbetet.

I hänvisningen till förbättrad förvaltning och riskhantering bör hänsyn tas till att övervakningen av efterlevnad nu övergår från pilotförsök till fullständig utbyggnad. Därför är det normalt att

täckningen än så länge är ganska begränsad. Detta projekt för efterlevnad är nästa etapp i en långsiktig process för ökning av cybermognaden. Denna inleddes med en definiering av gemensamma metoder för riskhantering, framtagning av gemensamma verktyg samt utbyggnad av system för övervakning, provning och validering av hur sårbarheter hanteras och tillgångar inventeras. Framsteg har gjorts under denna långa process trots komplexiteten i kommissionens tillgångar i form av mer än 1 000 informationssystem som drivs av över 50 generaldirektorat och genomförandeorgan.

2. Samarbetsmekanismer för EU:s institutioner, organ och byråer

CERT-EU har varit mycket framgångsrik i att främja samarbete både mellan EU:s institutioner, organ och byråer och på europeisk nivå genom sin roll som fullvärdig medlem i CSIRT-nätverket som inrättats enligt nätverks- och informationssäkerhetsdirektivet. På detta sätt är CERT-EU ett exempel på hur samarbete och cybersäkerhetstjänster kan förbättras. Revisionsrättens iakttagelser av CERT-EU illustrerar väldigt tydligt det utmärkta arbete som organisationen gör inför ett alltmer fientligt landskap av cyberhot och med permanent bristande resurser.

Inom ramen för det nuvarande interinstitutionella avtalet är EU:s decentraliserade byråer och gemensamma företag officiellt representerade i CERT-EU:s styrelse genom Enisa. Utöver detta framförs deras åsikter i styrelsemöten av en företrädare för den rådgivande kommittén för IKT (ICTAC). Denne får delta i möten för att bistå Enisa i dess roll som ombud för byråerna men har ingen formell plats eller röst. Frågan om byråernas adekvata representation i CERT-EU:s styrelse kommer att behandlas i förslaget till förordning. Det består i att komplettera styrelsens sammansättning med upp till tre representanter som ska utses av EU-byråernas nätverk på förslag av dess rådgivande kommitté för IKT.

Deltagande i ICDT:s undergrupp för cybersäkerhet sker efter bästa förmåga, och omfattningen av detta engagemang bestäms av var och en av EU:s institutioner, organ och byråer. Förbättrat informationsutbyte vid upphandlingar är en viktig fråga för arbetsgrupp 2 i undergruppen för cybersäkerhet. Den behandlas nu vid utarbetandet av det nya ramavtalet för cybersäkerhet.

Vad gäller gemensamma verktyg för tjänster såsom e-post och videokonferenser finns redan möjligheten att använda Secem-2-systemet. Detta har kommissionen infört i alla EU:s institutioner, organ och byråer och kan användas för krypterad e-post om man använder krypteringsnycklar och krypteringscertifikat på rätt sätt. Utöver detta håller verktyget SECABC på att utvecklas. Det ska göra det möjligt att kryptera e-post mellan institutionerna, och avsikten är att de av EU:s institutioner, organ och byråer som är intresserade ska kunna använda det från och med 2022. Videokonferenser kan redan genomföras säkert för utbyte av känslig icke-säkerhetsskyddsklassificerad information. Detta system kan utvidgas till andra institutioner, organ och byråer vid enskilda tillfällen genom kontroll av konferensdeltagarnas identitet. Utbyte av känslig information kommer även att behandlas i den förslagna förordningen om informationssäkerhet (dvs. genom gemensamma etiketter och markeringar).

3. Utbyte av information om betydande incidenter eller sårbarheter

Det faktum att inte alla av EU:s institutioner, organ och byråer anmäler betydande incidenter eller sårbarheter till CERT-EU behandlas i den föreslagna förordningen om cybersäkerhet i linje med kommissionens förslag i NIS2-direktivet[1]. Nivån på genomförandet kommer att bero på de extraresurser som de självständiga institutionerna, organen och byråerna tilldelar till detta. Möjligheten att införa krav på anmälning är begränsad, även enligt det förslag till förordning som nu planeras, på grund av institutionernas, organens och byråernas institutionella självständighet. Den föreslagna förordningen om cybersäkerhet kommer att innehålla mekanismer för efterlevnad som är lämpliga och står i proportion till de nya reglernas syfte och omfattning utan att detta påverkar institutionernas, organens och byråernas självständighet.

III. KOMMISSIONENS SVAR PÅ REVISIONSRÄTTENS SLUTSATSER OCH REKOMMENDATIONER

Rekommendation 1 – Förbättra cybersäkerhetsberedskapen hos alla EU:s institutioner, organ och byråer genom gemensamma bindande regler och ökade resurser för CERT-EU

Den föreslagna förordningen kommer att inbegripa särskilda åtgärder som ytterligare ska höja den gemensamma cybersäkerhetsnivån. Dessa ska bestå i planer för cybersäkerhet som ska tas fram och genomföras på institutionernas, organens och byråernas nivå inom deras egen ram för cybersäkerhetsförvaltning.

Kommissionen godtar rekommendationen. Vad avser dess särskilda underkategorier meddelar kommissionen följande:

a) Kommissionen godtar rekommendation 1 a. Den föreslagna förordningen kommer att innehålla bestämmelser om ramar för förvaltning och kontroll som inrättas på högsta ledningsnivå vid varje institution, organ och byrå för att se till att hanteringen av alla cybersäkerhetsrisker är effektiv och ansvarsfull.
b) Kommissionen godtar rekommendation 1 b. I den föreslagna förordningen kommer den riskbaserade metoden för hantering av cybersäkerhet att lyftas fram ytterligare genom att tydliggöra att åtgärder, planer för it-säkerhet och faktiskt genomförande av nödvändiga kontroller bör följa bedömningarna.
c) Kommissionen godtar rekommendation 1 c. Kurser i cybersäkerhet, medvetenhetshöjande insatser och utbildningsprogram kommer att anges som en del av cybersäkerhetens grunder i den föreslagna förordningen.
d) Kommissionen godtar rekommendation 1 d. Vår erfarenhet visar att även om regelbundna revisioner och tester är nödvändiga, räcker de inte för att säkerställa att framsteg görs.

[1] Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148, COM(2020) 823 final.

Därför behövs regelbunden rapportering och insyn som en del av förvaltningen av cybersäkerheten enligt led a.

e) Kommissionen godtar rekommendation 1 e. Den föreslagna förordningen kommer att innehålla bestämmelser om institutionernas, organens och byråernas anmälningar av cyberhot, sårbarheter och incidenter till CERT-EU.

f) Kommissionen godtar rekommendation 1 f. Kommissionen stöder behovet att förbättra CERT-EU:s resurser. Bestämmelser om personal och ekonomiska bidrag från EU:s institutioner, organ och byråer kommer att ingå i den föreslagna förordningen.

g) Kommissionen godtar rekommendation 1 g. Den föreslagna förordningen kommer att innehålla mekanismer för efterlevnad som står i proportion till bestämmelsernas syfte och tillämpningsområde och tar hänsyn till institutionernas, organens och byråernas institutionella självständighet. Innehållet i den kommande förordningen beror på resultatet av lagstiftningsförfarandet och grundar sig på ett beslut av unionslagstiftaren i fråga om kommissionens förslag.

Rekommendation 2 – Verka för ytterligare synergieffekter bland EU:s institutioner, organ och byråer på utvalda områden

Kommissionen, som för närvarande är ordförande för undergruppen för cybersäkerhet vid den interinstitutionella kommittén för digital omställning (ICDT), samtycker till rekommendationerna att främja lösningar för konsekvent och säker delning av känslig information, systematisk delning av information om cybersäkerhetsprojekt samt gemensamma upphandlingsramar och avtal för cybersäkerhetstjänster.

Kommissionen godtar rekommendationen. Vad avser dess särskilda underkategorier meddelar kommissionen följande:

a) Kommissionen godtar rekommendation 2 a. Kommissionen bidrar med tekniska initiativ och tjänster till ICDT:s undergrupp för cybersäkerhet för att främja och stödja gemensamma verktyg för delning av känslig information genom tjänster såsom e-post och videokonferenser. Vi noterar även att gemensamma markeringar och regler för hantering av känslig icke-säkerhetsskyddsklassificerad information kommer att behandlas i den förslagna förordningen om informationssäkerhet.

b) Kommissionen godtar rekommendation 2 b. Arbetsgrupperna i ICDT:s undergrupp för cybersäkerhet behandlar denna punkt och kommer att vidareutveckla den. Förbättrat informationsutbyte vid upphandlingar behandlas nu vid utarbetandet av det nya ramavtalet för cybersäkerhet.

c) Kommissionen godtar rekommendation 2 c. EU:s institutioner, organ och byråer har redan tillgång till interinstitutionella ramavtal på området för IKT som förvaltas av kommissionen. Utarbetandet av det nya ramavtalet för cybersäkerhet kommer att samordnas med ICDT:s undergrupp för cybersäkerhet.

Rekommendation 3 – Öka CERT-EU:s och Enisas fokus på de av EU:s institutioner, organ och byråer som är mindre mogna

Denna rekommendation är riktad till CERT-EU och Enisa.