AMCHAM

AMERICAN CHAMBER OF COMMERCE IN SWEDEN

The Home of American Business

Brev från American Chamber of Commerce inför telekom-rådet 5 december

Inför mötet bland telekom- och digitalministrar från EU:s medlemsstater den 5 december står europeiskt teknologiskt ledarskap och konkurrenskraft på agendan. I detta sammanhang vill vi uttrycka oro angående European Cybersecurity Certification Scheme for Cloud Services (EUCS) och dess potentiella negativa effekter på cybersäkerhet och teknisk utveckling i Europa, särskilt vad gäller generativ AI-utveckling i kritiska sektorer. Vi föreslår att denna fråga diskuteras vid rådsmötet med tanke på de breda ekonomiska, tekniska och handelsmässiga konsekvenserna.

EUCS är ett EU-övergripande system som kan göras obligatoriskt genom EU-förordningar, lokala lagar och upphandlingsriktlinjer. Vi stöder målet för EUCS att förena och harmonisera praxis för säkerhet i molnet och vi tror att de fortsatta förseningarna i antagandeprocessen kan vara skadliga för EU:s cybersäkerhet. **Vi är dock oroade över kraven i det aktuella utkastet (som läckte till media den 22 november), då de skulle förbjuda molntjänsteleverantörer (CSP) som inte har sitt huvudkontor i Europa och helt ägs av en EU-enhet att kvalificera sig för högsta nivå av EUCS-certifiering.** I den nuvarande texten är den högsta certifieringsnivån avsedd att gälla allmänt för data relaterade till allmän ordning, allmän säkerhet, folkhälsa eller utförande av väsentliga statliga funktioner.

Detta riskerar att begränsa tillgång av europeiska företag och regeringar från de säkraste molntjänsterna och cyberskydden i en tid då dessa institutioner fortsätter att påverkas negativt av skadlig programvara, ransomware och DDOS-attacker. Att diskriminera mot molnleverantörer baserat på ursprungsland skulle också medföra komplexitet och kostnader för europeiska företag som verkar över flera jurisdiktioner, eftersom de inte längre skulle kunna skala effektivt. Nystartade EU-företag som verkar globalt skulle möta ökade komplexiteter och kostnader. De vidsträckta effekterna av denna policy skulle komma att märkas över hela ekosystemet för cybersäkerhet, inklusive på europeiska företag som underleverantörer som är involverade i molntjänstleveranser.

Dessutom skulle kunder som använder AI och Generativ AI möta begränsningar när det gäller att utnyttja fördelarna med global molninfrastruktur och tillgång till olika dataset, vilket skulle hindra kvaliteten och mångfalden av modeller. För hälso- och sjukvård och biovetenskap är tillgång till internationella dataset och skalande tillgång till den senaste medicinska tekniken avgörande för att accelerera innovationstakten och förbättra liv.

Även om det har diskuterats flitigt under två år, har systemet sett minimala förändringar trots industrins inspel. Branschens oro återspeglas i över 40 positionspapper och brev sedan 2022, hittills obesvarade av kommissionen och ENISA.

I avsaknden av en konsekvensanalys från kommissionen har tankesmedjor gjort försök att modellera scenarier för konsekvenser av förslaget. **En studie varnar för att Europa kan förlora 29–610 miljarder euro årligen, vilket påverkar mindre stater oproportionerligt mycket. För Sverige kan de beräknade förlusterna uppgå till runt 20 miljarder euro i årliga förluster.**

Att förbjuda leverantörer utanför EU är ett politiskt beslut med breda ekonomiska och handelsmässiga konsekvenser, ett som bör involvera diskussioner mellan medlemsstaterna. Vi vet att åsikterna mellan medlemsstaterna skiljer sig markant och oroar oss för att det nuvarande förslaget skulle möjliggöra protektionistisk politik utan politisk debatt. Dessutom riskerar det nuvarande

diskriminerande tillvägagångssättet att gynna medlemsstater med en mer utvecklad molnindustri samtidigt som den begränsar tillgången för andra medlemsstater till kritisk teknik och påverkar framtida investeringar i Europa från molnleverantörer med huvudkontor utanför EU.

Cybersäkerhetslagen har gett ENISA ett tydligt mandat om EUCS och tillräcklig flexibilitet för medlemsstaterna att anta strängare nationella åtgärder under vissa förhållanden. EUCS kommer inte att åsidosätta eller på något sätt hindra medlemsstaterna från att anta särskilda certifieringssystem för nationell säkerhet. Medlemsstaterna kan också införa ytterligare eller strängare cybersäkerhetskrav för användningen av ICT-produkter av kritiska enheter, förutsatt att de inte omfattas av EUCS. Detta inkluderar restriktioner för tjänster eller leverantörer som tar hänsyn till icke-tekniska faktorer.

Vidare har EU antagit förordningar för skydd av både personliga och icke-personliga uppgifter, inklusive skydd från tredjelandslagar, enligt GDPR och datalagen. Dessa förordningar har diskuterats enligt EU:s normala lagstiftningsförfarande med bidrag från medlemsstaterna och samråd med berörda parter.

Nästa diskussionsomgång mellan kommissionen och medlemsstaterna, som potentiellt blir den sista, kommer att äga rum den andra veckan i december, innan förslaget når ett omröstningsförfarande som en implementing act. Vi ber er att begära en politisk diskussion om EUCS-processen och dess oadresserade breda konsekvenser vid nästa telekommunikationsråd. Det är vår övertygelse att denna viktiga fråga förtjänar en debatt utanför den tekniska nivån och att medlemsstaterna bör ha möjlighet att diskutera rättsliga krav på politisk nivå och under EU:s normala lagstiftningsprocess.

Slutligen vill vi slå ett slag för att cybersäkerheten och den teknologiska utvecklingen gynnas av att teknikleverantörer tillåts innovera och konkurrera med varandra. Därför tar cybersäkerhetskrav bäst fram enligt tekniska krav snarare än politiska motiv.