EUROPEISKA KOMMISSIONEN

Bryssel den 17.9.2013
C(2013) 5878 final

Herr talman,

Kommissionen vill tacka riksdagen för det motiverade yttrandet om förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (COM (2013) 48 final).

Kommissionen delar inte riksdagens åsikt att förslaget inte är förenligt med subsidiaritetsprincipen. Såsom förklaras närmare i den konsekvensanalys som åtföljer förslaget motiveras EU:s insatser på detta område av att effekterna av många incidenter överskrider de nationella gränserna och hindrar att den inre marknaden fungerar väl. Kommissionen har hittills tillämpat ett tillvägagångssätt baserat på frivillighet genom att uppmana medlemsstaterna att upprätta lämplig nät- och informationssäkerhetskapacitet och samarbeta för att motverka gränsöverskridande incidenter och genom att uppmana industrin att bättre hantera risker och investera i säkerhetslösningar. Denna metod har emellertid inte lyckats undanröja den ojämna nivån på beredskapen och det begränsade samarbetet i hela EU. Exempelvis ingår endast tio medlemsstater i den europeiska gruppen av incidenthanteringsorganisationer (ECG-gruppen). Underlåtenhet att ingripa på EU-nivå skulle leda till en situation där vissa medlemsstater ständigt skulle släpa efter när det gäller beredskap och insatser, vilket skulle försvaga den samlade nivån av nät- och informationssäkerhet inom EU med tanke på den nära kopplingen mellan de olika nätet och systemen. Medlemsstaterna håller också på att börja införa sina egna lagstadgade krav på riskhantering och incidentrapportering på ett samordnat sätt, vilket skapar hinder för den inre marknaden i form om ytterligare administrativa bördor och kostnader för att följa reglerna för de företag som verkar i fler än en medlemsstat. I många svar på kommissionens offentliga samråd betonades den börda som uppstår till följd av frånvaron av en verkligt integrerad marknad och ett verkligt harmoniserat regelverk. Detta har också störande verkningar på tillhandahållandet av gränsöverskridande tjänster som kan bli oåtkomliga, upphävas eller avbrytas på grund av säkerhetsöverträdelser. Såsom anges i konsekvensanalysen blev kommissionen tvungen att avbryta systemet för handel med utsläppsrätter i januari 2010 på grund av säkerhetsöverträdelser vid de nationella registren, som hindrade företag från att sälja och köpa utsläppsrätter inom EU. eBay och PayPal har upplevt webbaserade attacker som gjorde alla eller delar av deras webbplatser otillgängliga

Per WESTERBERG
Riksdagens talman
100 12 Stockholm

under olika tidsperioder 2010, vilket i sin tur påverkade den elektroniska handeln på den inre marknaden.

Kommissionen tog särskild hänsyn till proportionalitetsprincipen vid utarbetandet av sitt förslag. De krav som fastställs för medlemsstaterna ligger på den miniminivå som krävs för att uppnå adekvat beredskap och möjliggöra ett förtroendefullt samarbete. Medlemsstaterna kan ta hänsyn till nationella särdrag samtidigt som det säkerställs att gemensamma EU-principer tillämpas på ett proportionerligt sätt.

Till exempel ges medlemsstaterna i kapitel II i förslaget frihet att definiera vilka uppgifter som ska åligga den behöriga myndigheten och organisationerna för incidenthantering. Förslaget ger även medlemsstaterna tillräcklig flexibilitet att besluta om strukturen hos dessa enheter: I artikel 6 i förslaget krävs inte att myndigheterna för nät- och informationssäkerhet är oberoende, och enligt artikel 7 får medlemsstaterna fritt inrätta en incidenthanteringsorganisation inom eller utanför den behöriga myndigheten.

På EU-nivå är det nät som inrättats enligt kapitel III en samarbetsmekanism som inte har status som juridisk person. Möjligheten att samarbeta på EU-nivå kring incidenter som har en gränsöverskridande dimension bör inte på något sätt hindra en snabb reaktion på lokal nivå.

När det gäller reglerna för marknadens aktörer i kapitel IV är både räckvidden och de materiella skyldigheterna för marknadsaktörerna begränsade. Vad gäller räckvidden omfattas endast de som tillhandahåller kritisk infrastruktur, medan mikroföretag är undantagna. Eftersom förteckningen i bilaga 2 inte är uttömmande står det medlemsstaterna fritt att fastställa den exakta räckvidden för och arten av marknadsaktörerna på nationell nivå. När det gäller de materiella skyldigheterna införs inga exakta säkerhetsåtgärder genom förslaget, men det innehåller bestämmelser om allmän riskhantering och krav på tillhandahållande av information. För att undvika att lägga en oproportionerlig börda på små aktörer står kraven i proportion till den risk som nätverket eller informationssystemet i fråga står inför.

Kostnaderna för förslaget för såväl medlemsstaterna som marknadsaktörerna beskrivs i konsekvensanalysen. Kommissionen anser att de inte är alltför stora med beaktande av vad som står på spel och troligen kommer att uppvägas av de övergripande ekonomiska och sociala vinsterna. Baserat på de beräkningar som gjorts i konsekvensanalysen anser kommissionen exempelvis att den genomsnittliga kostnaden för efterlevnaden för små och medelstora företag skulle uppgå till mellan 2500 och 5 000 euro, medan nu tillgängliga uppgifter från privata sektorn om den genomsnittliga kostnaden för den mest allvarliga säkerhetsöverträdelse som ett litet företag eller medelstort företag utsätts för varierar mellan 41 000 och 77 000 euro[1]. Kostnaderna för att inte göra något är därför betydande. Vidare kommer en samordnad strategi på EU-nivå att begränsa kostnaderna för användarna, som annars kanske måste uppfylla olika eller motstridiga nationella krav.

[1] http://www.pwc.co.uk/audit-assurance/publications/2013-information-security-breaches-survey.jhtml

Kommissionen hoppas att dessa klargöranden svarar på de frågor som Sveriges riksdag tagit upp och ser fram emot att fortsätta denna dialog i framtiden.

Högaktningsfullt

Maroš Šefčovič
Vice ordförande