KOMISIJA EVROPSKH SKUPNOSTI

Bruselj, 31.5.2006
COM(2006) 251 konč.

SPOROČILO KOMISIJE SVETU, EVROPSKEMU PARLAMENTU, EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Strategija za varno informacijsko družbo – „Dialog, partnerstvo ter povečanje vpliva in moči“

{SEC(2006) 656}

KAZALO

SPOROČILO KOMISIJE SVETU, EVROPSKEMU PARLAMENTU, EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Strategija za varno informacijsko družbo – „Dialog, partnerstvo ter povečanje vpliva in moči“

1. UVOD

Sporočilo „i2010 – Evropska informacijska družba za rast in zaposlovanje“[1] je poudarilo pomembnost omrežne in informacijske varnosti pri vzpostavitvi enotnega evropskega informacijskega prostora. Razpoložljivost, zanesljivost in varnost omrežij in informacijskih sistemov postajajo vedno bolj pomembni za naše gospodarstvo in družbeni sistem.

Namen tega sporočila je ponovno oživiti strategijo Evropske Komisije, določeno leta 2001 v sporočilu „Varnost omrežij in informacij: predlog pristopa evropske politike.“[2] Preverja trenutno stanje ogroženosti varnosti informacijske družbe in določa, katere dodatne ukrepe je treba sprejeti za izboljšanje varnosti omrežij in informacij (VOI).

Na podlagi izkušenj držav članic in izkušenj, pridobljenih na ravni Evropske skupnosti, je cilj nadalje razvijati dinamično, globalno strategijo v Evropi, osnovano na kulturi varnosti ter utemeljeno na **dialogu, partnerstvu ter povečanju vpliva in moči.**

Pri reševanju varnostnih izzivov informacijske družbe je Evropska skupnost razvila tridelni pristop, ki obsega: posebne ukrepe za varnost omrežij in informacij, regulativni okvir za elektronske komunikacije (ki zajema vprašanja zasebnosti in zaščite podatkov) in boj proti kibernetskemu kriminalu. Čeprav bi bilo te tri vidike do določene mere mogoče razvijati ločeno, številne medsebojne odvisnosti zahtevajo usklajeno strategijo. To sporočilo določa strategijo in omogoča okvir za izvedbo in izboljšanje skladnega pristopa k VOI.

Sporočilo iz leta 2001 opredeljuje VOI kot *„zmožnost omrežja ali informacijskega sistema, da na določeni stopnji zaupanja prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo razpoložljivost, verodostojnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ter s tem povezanih storitev, ki jih ponujajo ta omrežja in sistemi ali so prek njih dostopne.“* V zadnjih letih je Evropska skupnost izvedla številne ukrepe za izboljšanje VOI.

Regulativni okvir za elektronske komunikacije, katerega pregled je v teku, vključuje določbe, povezane z varnostjo. Zlasti Direktiva o zasebnosti in elektronskih komunikacijah[3] vsebuje obveznost za dobavitelje javno dostopnih komunikacijskih storitev, da ščitijo varnost svojih

---

1 COM(2005) 229 konč., 1.6.2005.
2 COM(2001) 298 konč., 6.6.2001.
3 Direktiva 2002/58/ES.

storitev. Določeni so ukrepi zoper nezaželeno elektronsko pošto[4] in vohunsko programsko opremo[5].

V programih Evropske skupnosti, ki so posvečeni raziskovanju in razvoju, imata pomembno vlogo tudi zaupanje in varnost. 6. okvirni raziskovalni program obravnava ta vprašanja prek številnih projektov. Raziskovanje, povezano z varnostjo, se bo okrepilo v 7. okvirnem programu z vzpostavitvijo Evropskega programa za raziskave na področju varnosti (EPVR). [6] Poleg tega program „Varnejši internet plus“ podpira projekte vzpostavljanja omrežij in izmenjavo najboljših praks za boj proti škodljivi vsebini, ki kroži po informacijskih omrežjih.

Evropska Skupnost se je leta 2004 odločila ustanoviti Evropsko agencijo za varnost omrežij in informacij (ENISA), kar je bil del njenega odziva na ogrožanje varnosti. ENISA prispeva k razvoju kulture varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja na področju celotne Evropske unije (EU).

EU je dejavna tudi v mednarodnih forumih, ki obravnavajo ta področja, kot so OECD, Svet Evrope ali ZN. Na Svetovnem vrhu o informacijski družbi v Tunisu je EU močno podprla razprave o razpoložljivosti, zanesljivosti ter varnosti omrežij in informacij. Tuniška strategija[7], ki skupaj s tuniško obvezo določa nadaljnje ukrepe za politično razpravo o globalni informacijski družbi, kot so potrdili svetovni voditelji, poudarja potrebo nadaljnjega boja proti kibernetskemu kriminalu in nezaželeni elektronski pošti ob hkratnem zagotavljanju varovanja zasebnosti in svobode izražanja. Opredeljuje potrebo po skupnem razumevanju vprašanj internetne varnosti in po nadaljnjem sodelovanju, s čimer bi pospešili zbiranje in razširjanje informacij, povezanih z varnostjo, in izmenjavo dobre prakse med vsemi zainteresiranimi stranmi o ukrepih za boj proti ogrožanju varnosti.

2. IZBOLJŠANJE VARNOSTI INFORMACIJSKE DRUŽBE: KLJUČNI IZZIVI

Kljub naporom na mednarodni, evropski in nacionalni ravni, varnost še vedno predstavlja velik problem.

Prvič, razlogi za napad na informacijske sisteme so vedno bolj povezani z dobičkom in ne z željo povzročiti motnjo zaradi motnje same. Podatki se pridobivajo nezakonito, vedno pogosteje brez vednosti uporabnika, medtem ko se število različic (in stopnja razvoja) škodljive programske opreme[8] naglo povečuje. Nezaželena elektronska pošta je dober primer tega razvoja: postaja sredstvo prenosa virusov ter goljufivih in kriminalnih dejavnosti, kot so vohunska programska oprema, „phishing“[9] in druge oblike škodljive programske opreme. Njena široka razširjenost je vedno pogosteje povezana z „botneti“[10], tj. kompromitiranimi strežniki in osebnimi računalniki, ki služijo kot posredniki brez vednosti njihovih lastnikov.

---

4 Ali nenaročena komercialna sporočila.

5 Vohunska programska oprema (spyware) je sledilna programska oprema, uporabljena brez ustreznega opozorila, pristanka ali nadzora uporabnika.

6 EPVR se pripravlja v okviru pripravljalnih ukrepov za raziskave varnosti v obdobju 2004–2006.

7 *Na poti h globalnemu partnerstvu v informacijski družbi: Spremljanje izvajanja tuniške faze Svetovnega vrha o informacijski družbi (WSIS)*, COM(2006) 181 konč., 27.4.2006.

8 „Malware“ pomeni škodljivo programsko opremo.

9 „Phishing“ je oblika internetnih goljufij, katerih namen je kraja dragocenih informacij, kot so kreditne kartice, bančni računi, uporabniški ID in gesla.

10 „Botneti“ so omrežja botov, ki so aplikacije, ki opravljajo naloge za oddaljenega kontrolorja in se tajno namestijo na računalnik žrtve.

Naraščajoč razvoj mobilnih naprav (vključno z mobilnimi telefoni tretje generacije, prenosnimi video igricami, itd.) in mobilne mrežne storitve bodo sprožili nove izzive, saj se storitve, ki temeljijo na IP, hitro razvijajo. Te lahko sčasoma postanejo običajnejša pot za napade kot osebni računalniki, saj so slednji že razvili visoko stopnjo varnosti. Res je, da vse nove oblike komunikacijskih okolij in informacijskih sistemov omogočajo nove niše za zlonamerne napade.

Drug pomemben dogodek je pojav „inteligentnega okolja“, v katerem bodo inteligentne naprave, ki jih podpira računalniška in omrežna tehnologija, postale vseobsegajoče (npr. prek RFID[11], IPv6 in senzorskih omrežij). Popolnoma medsebojno povezano in z omrežji prepleteno vsakdanje življenje obljublja velike priložnosti. Vendar pa se bodo s tem pojavila dodatna tveganja, povezana z varnostjo in zasebnostjo. Čeprav skupna okolja in aplikacije pozitivno vplivajo na inteoperabilnost in na vzpostavitev informacijskih in komunikacijskih tehnologij (IKT), lahko hkrati povečajo tveganja. Na primer, večja kot je uporaba standardne programske opreme, večji je vpliv izkoriščanja slabosti sistema ali pojava napak. Pojav določenih „monokultur“ v računalniških okoljih in aplikacijah lahko močno pospeši rast in razširjanje varnostnih groženj, kot so škodljiva programska oprema in virusi. **Raznolikost, odprtost in interoperabilnost so bistveni deli varnosti in jih je treba spodbujati.**

Pomembnost sektorja IKT za evropsko gospodarstvo in za evropsko družbo v celoti je neizpodbitna. IKT predstavlja pomemben del inovacij in je zaslužen za skoraj 40 % rasti proizvodnje. Poleg tega je ta izjemno inovativen sektor zaslužen za več kot četrtino celotnih evropskih prizadevanj v zvezi z raziskavami in razvojem in igra ključno vlogo pri ustvarjanju gospodarske rasti in delovnih mest v celotnem gospodarstvu. Vedno več Evropejcev živi v resnično informatizirani družbi, kjer se je uporaba IKT naglo povečala kot bistvena funkcija človeškega družbenega in gospodarskega vzajemnega delovanja. Po podatkih Eurostata je leta 2004 89 % podjetij v EU aktivno uporabljalo internet in približno 50 % potrošnikov je pred kratkim uporabilo internet[12].

Kršitev VOI ima lahko vpliv, ki presega gospodarske dimenzije. Obstaja splošna zaskrbljenost, da bodo varnostni problemi vodili k odvrnitvi uporabnikov in manjši uporabi IKT, saj so razpoložljivost, zanesljivost in varnost predpogoj za zagotavljanje temeljnih pravic „on line“.

Poleg tega zaradi večje povezljivosti med omrežji tudi druge ključne infrastrukture (kot so promet, energija itd.) postajajo vedno bolj odvisne od neoporečnosti njihovih zadevnih informacijskih sistemov.

Tako podjetja kot državljani v Evropi še vedno podcenjujejo nevarnost. Za to obstaja več razlogov, vendar se v primeru podjetij zdi najpomembnejši razlog slaba razvidnost donosa pri investicijah v varnost, v primeru državljanov pa, da se ne zavedajo svoje odgovornosti v globalni verigi varnosti .

Zaradi vsesplošne razširjenosti IKT in informacijskih sistemov predstavlja varnost omrežij in informacij izziv za vsakogar:

---

[11] Identifikacija radijske frekvence.

[12] Eurostat, *Internetne dejavnosti v Evropski uniji*, 40/2005.

- **Javna uprava** mora obravnavati varnost svojih sistemov, ne samo zaradi zaščite informacij javnega sektorja, ampak tudi zato, da bi služila kot zgled dobre prakse za druge udeležence;

- **Podjetja** morajo obravnavati VOI bolj kot pridobitev in element konkurenčne prednosti in ne kot „negativni strošek“;

- **Posamezni uporabniki** morajo razumeti, da so njihovi domači sistemi odločilni za celotno „verigo varnosti“.

Za uspešno rešitev zgoraj navedenih problemov potrebujejo vse interesne skupine zanesljive podatke o incidentih in trendih informacijske varnosti. Vendar pa je težko pridobiti zanesljive in izčrpne podatke o tovrstnih incidentih iz več razlogov, ki segajo od hitrosti nastopa dogodka, povezanega z varnostjo, do nepripravljenosti nekaterih organizacij, da razkrijejo in objavijo kršitve varnosti. Kljub temu pa je eden izmed temeljev razvoja kulture varnosti **izboljšanje našega poznavanja problema.**

Pomembno je, da programi ozaveščanja, namenjeni osvetlitvi primerov ogrožanja varnosti, ne spodkopavajo zaupanja potrošnikov in uporabnikov z osredotočanjem na samo negativne vidike varnosti. Zato bi moral biti VOI, kadar je to mogoče, **predstavljen kot prednost in priložnost** in ne kot obveznost in strošek. Treba ga je obravnavati kot pridobitev pri gradnji splošnega zaupanja in zaupanja potrošnikov, kot konkurenčno prednost za podjetja, ki delajo z informacijskimi sistemi, in kot vprašanje kvalitete storitve ponudnikov storitev v javnem in zasebnem sektorju.

Ključni izziv za oblikovalce politike je doseči celovit pristop. Ta pristop mora prepoznati ustrezne vloge različnih interesnih skupin. Zagotoviti mora ustrezno uskladitev javne politike in predpisov, ki posredno ali neposredno vplivajo na VOI. Proces liberalizacije, deregulacije in zbliževanja je ustvaril številne udeležence med različnimi skupinami interesnih skupin, kar ne olajša naloge. Prispevek ENISE k temu cilju je lahko pomemben. ENISA lahko služi kot center za delitev informacij, sodelovanje med vsemi zainteresiranimi stranmi in izmenjavo priporočljivih praks, tako znotraj Evrope kot z ostalim svetom, da bi prispevala h konkurenčnosti naših industrij IKT in dobremu delovanju notranjega trga.

3. NA POTI K DINAMIČNEMU PRISTOPU K VARNI INFORMACIJSKI DRUŽBI

Varna informacijska družba mora temeljiti na **poudarjeni VOI** in široko razširjeni **kulturi varnosti.** V ta namen Evropska komisija predlaga **dinamičen in celosten pristop**, ki vključuje vse interesne skupine in temelji na **dialogu, partnerstvu ter povečanju vpliva in moči.** Glede na komplementarni vlogi javnega in zasebnega sektorja pri vzpostavitvi kulture varnosti morajo politične pobude na tem področju temeljiti na **odprtem in vključujočem dialogu več interesnih skupin.**

Ta pristop in z njim povezani ukrepi bodo dopolnili in obogatili načrt Komisije, da nadaljuje z razvojem obsežnega in dinamičnega političnega okvira s pomočjo številnih pobud v letu 2006:

(1) Obravnavanje razvoja nezaželene elektronske pošte in groženj, kot so vohunska programska oprema in druge oblike škodljive programske opreme, v sporočilu o teh posebnih vprašanjih.

(2) Oblikovanje predlogov za izboljšanje sodelovanja med organi pregona in obravnavanje novih oblik kriminalne dejavnosti, ki izkoriščajo internet in spodkopavajo delovanje ključnih infrastruktur. To bo predmet posebnega sporočila o kibernetskem kriminalu.

Te politične pobude tudi dopolnjujejo dejavnost, ki se načrtuje za dosego ciljev zelene knjige Komisije o Evropskem programu za varovanje ključne infrastrukture (EPCIP), ki je nastal kot odgovor na zahtevo Sveta iz Decembra 2004. Proces iz zelene knjige bi lahko vodil do akcijskega načrta, ki bi združeval celotni krovni pristop k varovanju ključnih infrastruktur in potrebne politike, značilne za posamezne sektorje, vključno s politiko za sektor IKT. Sektorsko značilna politika za IKT bi s pomočjo **dialoga več interesnih skupin** preučila zadevne gospodarske, poslovne in družbene gonilne sile z namenom okrepitve varnosti in odpornosti omrežij in informacijskih sistemov.

Poleg tega bo pregled regulativnega okvira za elektronske komunikacije 2006 obravnaval tudi elemente za izboljšanje VOI, kot so tehnični in organizacijski ukrepi, ki jih sprejmejo ponudniki storitev, določbe, ki urejajo priglasitev kršitev varnosti, ter posebna pravna sredstva in sankcije v zvezi s kršitvami obveznosti.

Za zagotovitev rešitev, storitev in varnostnih izdelkov končnim uporabnikom je zadolžen predvsem zasebni sektor. Zato je strateškega pomena, da je **evropska industrija hkrati zahteven uporabnik** varnostnih izdelkov in storitev ter **konkurenčni dobavitelj** izdelkov in storitev VOI.

Nacionalne vlade morajo biti sposobne opredeliti in izvajati najboljše prakse pri oblikovanju politike in izkazati zavezanost tem političnim ciljem, tako da svoj informacijski sitem upravljajo na varen način. Javni organi v državah članicah in na ravni EU imajo ključno vlogo pri ustreznem obveščanju uporabnikov, s čimer jim omogočijo, da prispevajo k lastni varnosti in zaščiti. Ozaveščanje o vprašanjih VOI in zagotavljanje ustreznih in pravočasnih informacij, prek za to namenjenih spletnih portalov e-varnosti o grožnjah, tveganjih in opozorilih ter najboljših praksah bi morali biti prednostni nalogi. Preučitev izvedljivosti **vzpostavitve evropskega večjezičnega sistema za delitev informacij in opozarjanje**, ki bi gradil na podlagi obstoječih ali načrtovanih nacionalnih in zasebnih pobud in jih povezoval med seboj, bi zato lahko bila eden od glavnih ciljev ENISE.

Globalna razsežnost varnosti omrežij in informacij od Komisije zahteva, da na mednarodni ravni in v sodelovanju z državami članicami poveča svoja prizadevanja za **spodbujanje globalnega sodelovanja za VOI**, zlasti z izvajanjem strategije, sprejete na Svetovnem vrhu informacijske družbe (WSIS) novembra 2005.

Raziskave in razvoj, zlasti na ravni EU, bodo pomagale tudi k razvoju novega in inovativnega partnerstva za pospeševanje rasti evropske industrije IKT na splošno in zlasti evropske industrije IKT v zvezi z varnostjo. Komisija bo zato skušala zagotoviti, da se ustrezna finančna sredstva dodelijo za raziskave o VOI in zanesljivosti tehnologij v skladu s 7. okvirnim programom EU.

---

[13] COM(2005) 576 konč., 17.11.2005.

3.1. Dialog

*3.1.1. Komisija kot prvi korak k stopnjevanju dialoga med javnimi organi predlaga izvedbo **primerjalne analize nacionalnih politik, povezanih z VOI**, vključno s posebnimi varnostnimi politikami za javni sektor. Ta analiza bo pripomogla k opredelitvi najbolj učinkovitih praks, ki se bodo lahko prenesle, če bo to mogoče, na širši osnovi na celotno EU in pripomogle k temu, da bo javna uprava postala gonilo najboljše prakse in varnosti. Prizadevanja v zvezi z elektronsko identifikacijo na primer bi kot del nedavnega akcijskega načrta za e-upravo lahko v tem smislu igralo pomembno vlogo.*

Ob primerni strukturiranosti bodo rezultati te primerjalne analize **opredelili najboljše prakse za izboljšanje ozaveščenosti malih in srednje velikih podjetij ter državljanov glede potrebe**, da obravnavajo svoje specifične izzive in zahteve glede VOI in s tem povezane zmožnosti. ENISA bi morala imeti aktivno vlogo v tem dialogu ter pri združevanju in izmenjavi najboljših praks.

*3.1.2. Potrebna je **strukturirana debata več interesnih skupin** o tem, kako najbolje izkoristiti obstoječa orodja in regulativne instrumente za dosego ustreznega družbenega ravnovesja med varnostjo in zaščito temeljnih pravic, vključno z zasebnostjo. K tej debati bosta prispevala načrtovana konferenca „i2010 – Na poti k vseobsegajoči evropski informacijski družbi“, ki jo organizira prihodnje finsko predsedstvo, in posvetovanje o posledicah RFID za varnost in zasebnost, ki je del širših posvetovanj, ki jih je Komisija nedavno začela. Poleg tega bo Komisija organizirala:*

- Poslovni dogodek za spodbujanje zaveze industrije k sprejetju učinkovitih pristopov za izvajanje kulture varnosti **v industriji**.

- Seminar, ki bo odražal načine za povečanje ozaveščenosti o varnosti in okrepitev zaupanja **končnih uporabnikov** v uporabo elektronskih omrežij in informacijskih sistemov.

3.2. Partnerstvo

*3.2.1. Učinkovito oblikovanje politike zahteva jasno razumevanje narave in obsega izzivov. To zahteva ne samo zanesljive in najnovejše statistične in gospodarske podatke o incidentih informacijske varnosti ter stopnji zaupanja potrošnikov in uporabnikov, temveč tudi najnovejše podatke o obsegu in trendih industrije IKT v zvezi z varnostjo v Evropi. Komisija namerava ENISO zaprositi, da vzpostavi **zaupno partnerstvo z državami članicami in zainteresiranimi stranmi** za razvoj **ustreznega okvira zbiranja podatkov**, vključno s postopki in mehanizmi zbiranja in analiziranja podatkov o varnostnih incidentih in zaupanju potrošnikov iz celotne EU.*

Vzporedno bo Komisija, zaradi zelo razdrobljenega trga EU in njegove precej specifične narave, povabila države članice, zasebni sektor in raziskovalno skupnost k **vzpostavitvi strateškega partnerstva** za zagotovitev razpoložljivosti podatkov o industriji IKT v zvezi z varnostjo in o nastajajočih tržnih trendih za izdelke in storitve v EU.

*3.2.2. Za izboljšanje evropske sposobnosti odzivanja na ogrožanje varnosti omrežij bo Komisija zaprosila ENISO, da preuči **izvedljivost evropskega sistema za delitev informacij in opozarjanje,** s čimer bi omogočila učinkovito odzivanje na obstoječe in porajajoče se primere ogrožanja elektronskih omrežij. Zahteva takšnega sistema bo **večjezični portal EU** za zagotovitev ustreznih informacij o grožnjah, tveganjih in opozorilih.*

3.3. Povečanje vpliva in moči

Povečanje vpliva in moči posameznih skupin interesnih skupin je predpogoj za spodbujanje ozaveščenosti glede potreb v zvezi z varnostjo in tveganj za spodbujanje VOI.

*3.3.1. V ta namen Komisija **države članice** poziva, da:*

- Proaktivno sodelujejo v predlagani primerjalni analizi nacionalnih politik VOI;
- V tesnem sodelovanju z ENISO spodbujajo kampanj ozaveščanja o prednostih, ugodnostih in koristih sprejema učinkovitih varnostnih tehnologij, praks in ravnanja;
- Spodbujajo storitve e-uprave za sporočanje in pospeševanje dobrih varnostnih praks, ki bi jih potem lahko razširili na druge sektorje;
- Spodbujajo razvoj programov varnosti omrežij in informacij kot del učnega načrta visokega izobraževanja.

***3.3.2.** Komisija prav tako poziva interesne skupine **zasebnega sektorja**, da oblikujejo pobude za:*

- Razvoj in ustrezno opredelitev odgovornosti za proizvajalce programske opreme in ponudnike internetnih storitev v povezavi z zagotavljanjem ustrezne in preverljive stopnje varnosti. Pri tem je potrebna podpora za standardizirane procese, ki bi zadostili pravilom skupno določenih varnostnih standardov in najboljših praks.
- Pospeševanje raznolikosti, odprtosti, interoperabilnosti, uporabnosti in konkurenčnosti, ki so ključna gonila varnosti, ter spodbujanje uporabe izdelkov, procesov in storitev, ki krepijo varnost, za preprečevanje in boj proti kraji identitete ter drugim vdorom v zasebnost.
- Razširjanje dobrih varnostnih praks za operaterje omrežij, ponudnike storitev ter mala in srednje velika podjetja kot osnovne ravni za varnost in poslovno kontinuiteto.
- Spodbujanje programov usposabljanja v poslovnem sektorju, zlasti za mala in srednje velika podjetja, da bi zaposleni pridobili znanje in sposobnosti, potrebne za učinkovito izvajanje varnostnih praks.
- Delovanje v smeri dostopnih varnostnih shem potrjevanja za izdelke, procese in storitve, ki bodo obravnavale potrebe, značilne za EU (zlasti glede zasebnosti).

- Vključitev zavarovalniškega sektorja pri razvoju ustreznih orodij in metod za obvladovanje tveganja za reševanje tveganj, povezanih z IKT, in spodbujanje kulture obvladovanja tveganja v organizacijah in podjetjih (zlasti v malih in srednje velikih podjetjih).

4. SKLEPI

Opredelitev in reševanje izzivov varnosti v zvezi z informacijskimi sistemi in omrežji v EU zahteva popolno zavezanost vseh interesnih skupin. Politični pristop, začrtan v tem sporočilu, poskuša to doseči z okrepitvijo **pristopa sodelovanja več interesnih skupin**. Ta bi gradil na skupnih interesih, opredelitvi ustreznih vlog in razvil dinamični okvir za spodbujanje učinkovitega oblikovanja javne politike in pobud zasebnega sektorja.

Komisija bo sredi leta 2007 Svetu in Parlamentu poročala o začetih dejavnostih, začetnih ugotovitvah in stanju izvajanja posameznih pobud, vključno s pobudami ENISE, ter pobudami, sprejetimi na ravni držav članic in zasebnega sektorja. Če bo potrebno, bo Komisija predlagala priporočilo o varnosti omrežij in informacij (VOI).