EIROPAS KOMISIJA

Briselē, 30.9.2010
SEC(2010) 1123 galīgā redakcija

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS

pavaddokuments

priekšlikumam

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par uzbrukumiem informācijas sistēmām, ar ko atceļ Pamatlēmumu 2005/222/TI

{COM(2010) 517 final}
{SEC(2010) 1122 final}

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMS

1. PROBLĒMAS IZKLĀSTS

Kopš Pamatlēmuma par uzbrukumiem informācijas sistēmām pieņemšanas (turpmāk - pamatlēmums par uzbrukumiem) ir ievērojami palielinājies uzbrukumu informācijas sistēmām skaits. Viens no vadošajiem uzņēmumiem interneta drošības jomā ziņoja, ka draudi konfidenciālai informācijai (pretstatā publiski pieejamai informācijai) 2008. gadā ir ievērojami palielinājušies, 2008. gadā fiksēto apdraudējumu skaits ir palielinājies no 624 267 gadījumiem līdz 1 656 227 gadījumiem[1]. Turklāt ir novēroti vairāki iepriekš nepieredzēti plaši un bīstami uzbrukumi, piemēram Igaunijā un Lietuvā attiecīgi 2007. un 2008. gadā. 2009. gada martā inficētu datoru tīkls uzbruka valsts un privāto organizāciju datorsistēmām 103 valstīs, iegūstot sensitīvus un klasificētus dokumentus[2]. Tas tika paveikts, izmantojot "robottīklus"[3] - attāli vadāmu inficētu datoru kopumu. Visbeidzot, pasaule pašlaik pieredz tā sauktā "*Conficker*" (pazīstams arī kā *Downup*, *Downadup* un *Kido*) robottīkla izplatīšanos, kopš 2008. gada novembra tas ir sasniedzis vēl nepieredzētu izplatības līmeni un darbības plašumu, skarot miljoniem datoru visā pasaulē[4].

Otrkārt, nepietiekama sadarbība dalībvalstu un jo īpaši ES tiesībaizsardzības un tiesu iestāžu starpā apgrūtina saskaņotu un efektīvu šo uzbrukumu atvairīšanu. Kaut arī pamatlēmuma īstenošanas ziņojumi rāda, ka lielākā daļa dalībvalstu saskaņā ar pamatlēmuma 11. pantu ir izveidojušas pastāvīgus kontaktpunktus uzbrukumu jautājumos, turpina pastāvēt problēmas attiecībā uz šo kontaktpunktu atsaucību un spēju rīkoties steidzamu sadarbības lūgumu gadījumos[5].

Kontaktpunkta pastāvēšana negarantē tā pienācīgu darbību. Ziņojumos Komisijai vairākas dalībvalstis norādīja, ka to attiecīgie kontaktpunkti bija izveidoti, tomēr tie nedarbojās 24 stundas diennaktī, kā tas bija prasīts pamatlēmumā par uzbrukumiem. Tas nozīmē, ka tie nevarēja atbildēt uz steidzamiem lūgumiem ārpus sava darba laika. Publiskā un privātā sektora sadarbību bieži kavē kontaktpunktu zemā efektivitāte vai to nespēja apstrādāt privātā sektora sadarbības lūgumus.

Treškārt, joprojām ir maz pieejamu datu par kiberuzbrukumiem, kā arī par policijas un tiesu iestāžu rīcību, kas seko šādiem uzbrukumiem. Ne visas dalībvalstis vāc datus par kiberuzbrukumiem. Tās, kas šādus datus vāc, nedara to tādā veidā, kas ļautu šos datus salīdzināt, jo dalībvalstīs ir atšķirīgas statistikas metodoloģijas.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, 10. lpp.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 Termins "robottīkls" nozīmē ar destruktīvu programmatūru (datorvīrusu) inficētu datoru kopumu. Šādam inficētu datoru (spoku) kopumam var likt veikt īpašas darbības, piemēram uzbrukt informācijas sistēmām (kiberuzbrukumi). Šos "spokus" var kontrolēt kāds cits dators, bieži vien bez inficēto datoru lietotāju ziņas. Šo "kontrolējošo" datoru sauc arī par "vadības un kontroles centru". Personas, kas kontrolē šo centru, ir vieni no nodarījuma izdarītājiem, jo viņi izmanto inficētos datorus, lai sāktu uzbrukumus informācijas sistēmām. Ir ļoti grūti izsekot nodarījuma izdarītājus, jo datori, kas veido robottīklu un veic uzbrukumu, un nodarījuma izdarītājs var atrasties dažādās vietās.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Komisijas ziņojums Padomei, pamatojoties uz 12. pantu Padomes 2005. gada 24. februāra pamatlēmumā par uzbrukumiem informācijas sistēmām, COM (2008) 0448 galīgā redakcija.

Plaša mēroga uzbrukumi informācijas sistēmām apdraud sabiedrību plašākā nozīmē, ietverot informācijas sistēmu lietotājus, valdības un pašvaldības, starptautiskās organizācijas un privātas vienības.

Uzbrukumus mērķiem, kas atrodas ES, var veikt no trešām valstīm, un otrādi.

2. SUBSIDIARITĀTE

Kibernoziedzība ir starptautiska problēma, ar ko ļoti reti var cīnīties tikai valsts līmenī. Ir vispāratzīts, ka tās novēršanai un problēmas risināšanai ir nepieciešama rīcība ES un starptautiskā līmenī. Vairums uzbrukumu notiek pāri ES robežām. Tie skar visas dalībvalstis, un ir pierādījumi, ka ievērojama daļa no tiem ir saistīti ar darbībām, kas tiek veiktas no vienas dalībvalsts otrā. Informācijas sistēmas bieži ir tehniski savstarpēji savienotas un savstarpēji atkarīgas arī pāri valstu robežām. Ekspertu vidū valda vienprātība, ka nepieciešams rīkoties starptautiskā un ES līmenī un mērķis efektīvi cīnīties pret šāda veida noziedzību nav atbilstoši sasniedzams, ja dalībvalstis rīkojas vienas pašas.

Ja katrā valstī tiek īstenota sava pieeja kibernoziedzībai, pastāv sadrumstalotības un neefektivitātes risks Eiropas mērogā. Valstu pieeju dažādība un sistemātiskas pārrobežu sadarbības trūkums ievērojami samazina vietējo apkarošanas pasākumu efektivitāti. Daļēji tas notiek arī tādēļ, ka informācijas sistēmu savstarpējās savienotības dēļ zems drošības līmenis vienā valstī var palielināt sistēmu neaizsargātību citas valstīs.

3. KĀDI IR MĒRĶI?

3.1 Vispārīgie, īpašie un operatīvie mērķi

ES rīcības vispārīgais mērķis ir apkarot noziedzību – gan organizēto, gan cita veida – un saskaņā ar Līguma par Eiropas Savienības darbību 67. pantu saukt pie krimināltiesībām par to, cīnoties pret plaša mēroga kiberuzbrukumiem informācijas sistēmām.

A Īpašais mērķis – saukt pie krimināltiesībām un notiesāt noziedzniekus, kas atbildīgi par plaša mēroga uzbrukumiem, tuvinot krimināltiesību normas saistībā ar uzbrukumiem informācijas sistēmām

B Īpašais mērķis – uzlabot tiesībaizsardzības iestāžu (TAI) pārrobežu sadarbību

C Īpašais mērķis – izveidot efektīvas uzraudzības sistēmas un nodrošināt datu vākšanu

4. KĀDI IR POLITIKAS RISINĀJUMI?

4.1 1. risinājums. Iepriekšējā stāvokļa saglabāšana / ES līmenī netiek veikti jauni pasākumi

Šis risinājums nozīmē, ka ES neveiks nekādus turpmākus pasākumus, lai apkarotu šo īpašo kibernoziedzības veidu. Pašreizējie pasākumi turpinātos, jo īpaši programmas īpaši svarīgas informācijas infrastruktūras aizsardzībai un publiskā un privātā sektora sadarbības cīņai pret kibernoziedzību veicināšanai.

4.2 2. risinājums. Programmas izstrāde, lai stiprinātu centienus atvairīt uzbrukumus informācijas sistēmām ar neleģislatīvu pasākumu palīdzību

Neleģislatīvo pasākumu ietvaros papildus īpaši svarīgas informācijas infrastruktūras aizsardzības programmai galvenā uzmanība būtu pievērsta pārrobežu tiesībaizsardzības pasākumiem un publiskā un privātā sektora sadarbībai, šiem pasākumiem būtu jāatvieglo rīcības koordināciju ES līmenī. Neleģislatīvo pasākumu priekšlikumā varētu iekļaut tādas darbības kā tiesībaizsardzības iestāžu kontaktpunktu 24/7 tīkla stiprināšanu, kibernoziedzības ekspertu un tiesībaizsardzības iestāžu publiskā un privātā sektora kontaktpunktu ES tīkla izveidi un standarta ES nolīguma par pakalpojumu kvalitāti izstrādi tiesībaizsardzības iestāžu sadarbībai ar privātā sektora pārstāvjiem.

4.3 3. risinājums. Pamatlēmuma par uzbrukumiem noteikumu mērķtiecīga atjaunināšana, lai vērstos pret īpašajiem draudiem, ko rada plaša mēroga uzbrukumi informācijas sistēmām

Šis risinājums nozīmē īpašu, mērķtiecīgu (tas ir, ļoti konkrētu) tiesību aktu ieviešanu, kas vērsti pret īpaši bīstamiem plaša mēroga uzbrukumiem informācijas sistēmām. Šādi mērķtiecīgi tiesību akti būtu saistīti ar pasākumiem operatīvās pārrobežu sadarbības stiprināšanai cīņai pret uzbrukumiem informācijas sistēmām un pašreizējo minimālo sankciju palielināšanu. Šis risinājums izpaustos kā pašreizējā pamatlēmuma par uzbrukumiem atjaunināta versija, kas papildināta ar vairākiem neleģislatīviem pasākumiem, kā sagatavotības uzlabošana, drošības un pretoties spēju veicināšana īpaši svarīgas informācijas infrastruktūras aizsardzības jomā, līdzekļu un procedūru uzlabošana tiesībaizsardzības iestāžu pārrobežu sadarbībai un apmaiņa ar paraugprakses piemēriem.

4.4 4. risinājums. Vispusīga kibernoziedzības apkarošanas ES tiesiskā regulējuma ieviešana

Ja ir konstatēts, ka nepieciešama tūlītēja rīcība, lai vērstos pret kompleksu uzbrukumu informācijas sistēmām izplatību, rodas jautājums, vai būtu atbilstoši ieviest arī plašāku ES tiesisko regulējumu par kibernoziedzību kā tādu. Šāds tiesiskais regulējums attiektos ne tikai uz uzbrukumiem informācijas sistēmām, bet arī uz tādiem jautājumiem kā finanšu kibernoziedzība, nelikumīgs tīmekļa saturs, elektronisko pierādījumu vākšana/glabāšana/pārsūtīšana un sīki izstrādāti noteikumi par jurisdikciju. Šis ES tiesiskais regulējums būtu piemērojams līdztekus Eiropas Padomes Konvencijai par kibernoziedzību, kas tādējādi būtu papildināta ar jauniem noteikumiem, kas nepieciešami tieši ES ietvaros.

4.5 5. risinājums. Eiropas Padomes Konvencijas par kibernoziedzību atjaunināšana

Šā risinājuma ietvaros būtu nepieciešams no jauna risināt sarunas par konvencijas saturu, kas ir ilgstošs process un neatbilst rīcībai atvēlētajam laikposmam, kas ierosināts ietekmes novērtējumā. Starptautiskā līmenī, šķiet, trūkst vēlmes no jauna risināt sarunas par konvenciju. Tādējādi konvencijas atjaunināšana nav uzskatāma par reālu risinājumu, jo tas nav panākams rīcībai atvēlētajā laikposmā.

5. IETEKMES NOVĒRTĒJUMS

Risinājumu varianti	Saimniecis kā ietekme	Sociālā ietekme	Ietekme uz pamattiesībām	Ietekme uz trešām valstīm	Piemērotība A,B,C mērķu sasniegšanai	Saskaņotība ar starptautiskajām tiesībām
1. risinājums. Iepriekšējā stāvokļa saglabāšana /ES līmenī netiek veikti jauni pasākumi	0	0	0	-	0	0
2. risinājums. Programmas izstrāde, lai stiprinātu centienus atvairīt uzbrukumus informācijas sistēmām ar neleģislatīvu pasākumu palīdzību	-/+	++	-/+	++	A + B ++ C +	-/+
3. risinājums. Pamatlēmuma par uzbrukumiem noteikumu mērķtiecīga atjaunināšana, lai vērstos pret draudiem, ko rada plaša mēroga uzbrukumi informācijas sistēmām	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
4. risinājums. Vispusīga kibernoziedzības apkarošanas ES tiesiskā regulējuma ieviešana	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Vēlamais risinājums (2. risinājums un 3. risinājums). Neleģislatīvi pasākumi apvienojumā ar mērķtiecīgu pamatlēmuma par uzbrukumiem atjaunināšanu	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. KĀ SALĪDZINĀMI POLITIKAS RISINĀJUMI?

6.1 1. risinājums. Iepriekšējā stāvokļa saglabāšana

Šis risinājums nenovēršami vājinās privātā sektora, dalībvalstu un Savienības pozīcijas cīņā pret kibernoziedzību, ņemot vērā tās raksturu un izplatību. Pat ilgstoši saglabājot pašreizējo pasākumu līmeni, būtu nepieciešama Eiropas līmeņa koordinācija.

6.2 2. risinājums. Programmas izstrāde, lai stiprinātu centienus atvairīt uzbrukumus informācijas sistēmām ar neleģislatīvu pasākumu palīdzību

Šim risinājumam piemīt visas ieteikuma tiesību līdzeklim raksturīgās priekšrocības un trūkumi. Pozitīvs aspekts ir iespēja apskatīt katru politikas risinājumu tāda veidā, kas ir saskaņots ar valstu paraugpraksi, tādējādi atvieglojot visefektīvāko pasākumu noteikšanu.

Tomēr šīs risinājums ir neefektīvāks attiecībā uz mērķu sasniegšanu.

6.3 3. risinājums. Pamatlēmuma par uzbrukumiem noteikumu mērķtiecīga atjaunināšana, lai vērstos pret draudiem, ko rada plaša mēroga uzbrukumi informācijas sistēmām

Šis risinājuma variants piedāvā savlaicīgu un mērķtiecīgu apzināto problēmu risinājumu. Tas pievēršas tiem krimināltiesību jautājumiem, kas nepieciešami efektīvai šo noziegumu izdarītāju saukšanai pie krimināltatbildības. Ar to tiek uzlabota starptautiskā sadarbība, ieviešot tūlītējas starptautiskās palīdzības mehānismus steidzamu sadarbības lūgumu gadījumos un ar papildinošo pasākumu, piemēram, ekspertu tikšanos, palīdzību tiek veicināta sadarbība ar privāto sektoru. Ar šo risinājumu tiek ieviesti vairāki atbildību pastiprinoši apstākļi, piemēram, plaša mēroga uzbrukumi, kā arī uzbrukumi, slēpjot izdarītāju patieso identitāti un kaitējot identitātes likumīgajam īpašniekam.

Visbeidzot, problēmas mēroga apzināšanai tiek ieviesti uzraudzības pienākumi.

6.4 4. risinājums. Vispusīga kibernoziedzības apkarošanas ES tiesiskā regulējuma ieviešana

Šā risinājuma, tāpat kā 3. risinājuma, papildu vērtība ir tā, ka tiek ieviesti saistoši noteikumi, tādējādi ir sagaidāma lielāka efektivitāte, ja vien tos pilnībā īsteno. Turklāt ir sagaidāms, ka palielināsies gan leģislatīvo, gan neleģislatīvo pasākumu pozitīvā ietekme plašākā kibernoziedzības jautājumu lokā, nevis tikai plaša mēroga uzbrukumu jomā. Turklāt, šis risinājums pievērstos krimināltiesību tiesiskajam regulējumam un tajā pašā laikā uzlabotu pārrobežu sadarbību tiesībaizsardzības jomā. Taču, šāda holistiska pieeja šajā posmā vēl negūst ieinteresēto personu vispārēju atbalstu, kaut arī to īstenojot būtu iespējams spert ievērojamu soli uz priekšu kibernoziedzības apkarošanā, vairāk nekā to spēj visi pārējie risinājumi.

7. VĒLAMAIS POLITIKAS RISINĀJUMS

Pēc ekonomiskās ietekmes, sociālās ietekmes un ietekmes uz pamattiesībām analīzes jāsecina, ka labākā pieeja problēmām nolūkā sasniegt noteiktos mērķus ir 2. un 3. risinājums.

Tātad vēlamais risinājums būtu 2. un 3. risinājuma apkopojums, jo tie papildina viens otru un tādējādi vislabāk ļauj sasniegt nospraustos mērķus pēc būtības un piemērotā termiņā.

8. UZRAUDZĪBA UN NOVĒRTĒŠANA

Īstenošanas ziņojums būtu jāpublicē 2 gadu laikā pēc direktīvas spēkā stāšanās. Šajā ziņojumā būtu jāpievērš uzmanība precīzai direktīvas īstenošanai dalībvalstīs.

Turklāt būtu jāveic regulārs novērtējums, lai noteiktu, kā un cik lielā mērā direktīva ir palīdzējusi sasniegt nospraustos mērķus. Pirmais novērtējums būtu jāveic 5 gadu laikā pēc direktīvas spēkā stāšanās, turpmāk Komisija publicēs novērtēšanas ziņojumus ik pēc 5 gadiem, iekļaujot tajos informāciju par īstenošanas gaitu. Ņemot vērā novērtējumu secinājumus un ieteikumus, Komisijai būtu jāapsver turpmāki grozījumi direktīvā vai cita iespējamā rīcība.