COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 31.5.2006
COM(2006) 251 final

COMUNICAÇÃO DA COMISSÃO AO CONSELHO, AO PARLAMENTO EUROPEU, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Estratégia para uma sociedade da informação segura – "Diálogo, parcerias e maior poder de intervenção"

{SEC(2006) 656}

ÍNDICE

COMUNICAÇÃO DA COMISSÃO AO CONSELHO, AO PARLAMENTO EUROPEU, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Estratégia para uma sociedade da informação segura – "Diálogo, parcerias e maior poder de intervenção"

1. INTRODUÇÃO

A Comunicação "i2010 - Uma sociedade da informação europeia para o crescimento e o emprego"[1] sublinhou a importância da segurança das redes e da informação para a criação de um espaço único europeu da informação. A disponibilidade, a fiabilidade e a segurança das redes e sistemas de informação são cada vez mais fundamentais para as nossas economias e para todo o tecido social.

O objectivo da presente comunicação é revitalizar a estratégia da Comissão Europeia delineada em 2001, na Comunicação "Segurança das redes e da informação: Proposta de abordagem de uma política europeia"[2]. Nesta se analisa a situação actual no que respeita a ameaças à segurança da sociedade da informação e se definem medidas suplementares a adoptar para melhorar a segurança das redes e da informação (SRI).

Aproveitando a experiência adquirida pelos Estados-Membros e a nível da Comunidade Europeia, pretende-se aprofundar uma estratégia dinâmica e global na Europa, baseada numa cultura de segurança e alicerçada no **diálogo, em parcerias e num maior poder de intervenção**.

Para responder aos desafios de segurança na sociedade da informação, a Comunidade Europeia elaborou uma abordagem em três vertentes que abrange: medidas de segurança específicas para as redes e a informação, o quadro regulamentar das comunicações electrónicas (que inclui as questões associadas à privacidade e à protecção dos dados) e a luta contra a cibercriminalidade. Embora estas três vertentes possam, em certa medida, ser desenvolvidos separadamente, as numerosas interdependências exigem uma estratégia coordenada. A presente comunicação expõe a estratégia e estabelece o quadro para fazer avançar e aperfeiçoar uma abordagem coerente da SRI.

A Comunicação de 2001 define a SRI como "*a capacidade de uma rede ou sistema da informação para resistir, com um dado nível de confiança, a eventos acidentais ou acções maliciosas. Estes eventos ou acções podem comprometer a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos através dessa rede ou sistema*". Nos últimos anos, a Comunidade Europeia tem recorrido a diversas acções para melhorar a SRI.

O quadro regulamentar das comunicações electrónicas, cuja revisão está em curso, inclui disposições relativas à segurança. Concretamente, a directiva relativa à privacidade nas comunicações electrónicas[3] prevê a obrigação de os fornecedores de serviços de

---

1 COM(2005) 229 final de 1.6.2005
2 COM(2001) 298 final de 6.6.2001
3 Directiva 2002/58/CE

comunicações electrónicas publicamente disponíveis garantirem a segurança dos seus serviços. Foram estabelecidas disposições contra o *spam*[4] e o software-espião[5].

A confiança e a segurança desempenham igualmente um papel importante nos programas comunitários de investigação e desenvolvimento. O 6.º Programa-Quadro de Investigação incide nestas questões através de uma vasta gama de projectos. A investigação relativa à segurança será reforçada no 7º Programa-Quadro, com o estabelecimento de um programa de investigação europeu sobre segurança (ESRP)[6]. Além disso, o programa "Safer Internet Plus" apoia projectos de ligação em rede e o intercâmbio das melhores práticas para combater os conteúdos nocivos que circulam nas redes de informação.

Como resposta às ameaças à segurança, a Comunidade Europeia decidiu, em 2004, entre outras coisas, criar a Agência Europeia para a Segurança das Redes e da Informação (ENISA). A ENISA contribui para o desenvolvimento de uma cultura de segurança das redes e da informação em benefício dos cidadãos, consumidores, empresas e organizações do sector público em toda a União Europeia (UE).

A UE desempenha igualmente um papel activo nas instâncias internacionais que abordam estes assuntos, como a OCDE, o Conselho da Europa ou a ONU. Na Cimeira Mundial sobre a Sociedade da Informação, em Túnis, a UE deu um apoio decidido aos debates sobre a disponibilidade, a fiabilidade e a segurança das redes e da informação. A Agenda de Túnis[7], que, juntamente com o Compromisso de Túnis, define novas etapas para o debate político sobre a sociedade da informação mundial, tal como aprovado pelos líderes mundiais, sublinha a necessidade de continuar a luta contra a cibercriminalidade e o *spam*, assegurando simultaneamente a protecção da privacidade e da liberdade de expressão. Esta agenda identifica a necessidade de um entendimento comum das questões de segurança da Internet e de uma maior cooperação para facilitar a recolha e difusão de informação relativa à segurança e o intercâmbio de boas práticas entre todas as partes interessadas no que toca a medidas de combate às ameaças à segurança.

2. MELHORAR A SEGURANÇA DA SOCIEDADE DA INFORMAÇÃO: OS DESAFIOS ESSENCIAIS

Apesar dos esforços a nível internacional, europeu e nacional, a segurança continua a levantar problemas difíceis.

Primeiramente, os ataques a sistemas de informação são motivados cada vez mais pelo lucro e não pelo simples desejo de criar perturbações ou rupturas. Faz-se prospecção ilegal de dados, cada vez mais sem conhecimento do utilizador, enquanto o número de variantes (e o ritmo de evolução) do *malware*[8] está a aumentar rapidamente. O *spam* é um bom exemplo desta evolução: está a tornar-se um veículo para vírus e actividades fraudulentas e criminosas, como

---

4 Comunicações comerciais não solicitadas

5 Software de monitorização instalado sem aviso adequado e sem o consentimento ou o controlo do utilizador

6 O ESPR está a ser preparado no âmbito de uma acção preparatória para a investigação sobre segurança que decorre no período 2004-2006.

7 Para uma parceria mundial na sociedade da informação: Seguimento da fase de Túnis da Cimeira Mundial sobre a Sociedade da Informação (WSIS), COM(2006) 181 final de 27.4.2006.

8 Software malévolo

o software-espião, o *phishing*[9] e outras formas de *malware*. A sua distribuição generalizada assenta cada vez mais em *botnets*[10], ou seja, servidores e PC comprometidos que são utilizados como retransmissores sem o conhecimento dos seus proprietários.

A implantação crescente de dispositivos móveis (incluindo telemóveis 3G, consolas portáteis de videojogos, etc.) e serviços de rede para dispositivos móveis levantará novos desafios, uma vez que os serviços IP se desenvolvem rapidamente. Estes poderão vir a ser uma via mais comum para ataques do que os computadores pessoais, dado que estes últimos dispõem já de um nível de segurança significativo. Na verdade, todos os novos tipos de plataformas de comunicação e sistemas de informação abrem inevitavelmente novas janelas de oportunidade para ataques malévolos.

Outro acontecimento significativo é o advento da "inteligência ambiente", que tornará omnipresentes dispositivos inteligentes apoiados nas tecnologias informáticas e de ligação em rede (através, p. ex., de redes RFID[11], IPv6 e de sensores). Uma vida diária plena de interligações e ligações em rede promete oportunidades significativas, mas cria igualmente riscos suplementares para a segurança e a privacidade. As plataformas e aplicações mais comuns contribuem positivamente para a interoperabilidade e a implantação das tecnologias da informação e das comunicações (TIC), mas podem igualmente fazer aumentar os riscos. Por exemplo, quanto maior é a utilização dos programas informático disponíveis no mercado, maior é o impacto da ocorrência de falhas ou da exploração de vulnerabilidades. A emergência de certas "monoculturas" em plataformas e aplicações de software pode facilitar consideravelmente o crescimento e a propagação de ameaças à segurança, como o *malware* e os vírus. **A diversidade, a abertura e a interoperabilidade são elementos integrantes da segurança, pelo que devem ser promovidas**.

A importância do sector das TIC para a economia europeia e para a sociedade europeia no seu todo é incontestável. As TIC são um factor de inovação essencial e estão na origem de quase 40% do aumento da produtividade. Além disso, este sector altamente inovador é responsável por mais de um quarto de toda a actividade de I&D europeia e desempenha um papel fundamental no crescimento económico e na criação de emprego em toda a economia. Um número crescente de cidadãos europeus vive numa sociedade verdadeiramente baseada na informação, na qual a utilização das TIC acelerou rapidamente enquanto função essencial de interacção humana, tanto social como económica. De acordo com o Eurostat, 89% das empresas da UE utilizaram activamente a Internet em 2004 e cerca de 50% dos consumidores tinham utilizado recentemente a Internet[12].

Uma ruptura na SRI pode produzir um impacto que transcende a dimensão económica. Existe, sem dúvida, uma preocupação generalizada quanto à possibilidade de os problemas de segurança desincentivarem os utilizadores e retardarem a implantação das TIC, tendo em conta que a disponibilidade, a fiabilidade e a segurança constituem um pré-requisito para garantir os direitos fundamentais em linha.

---

9 Forma de fraude na Internet que visa roubar informação valiosa associada, nomeadamente, a cartões de crédito, números de contas bancárias ou ainda identificadores e senhas de utilizador.

10 Redes de *bots*, sendo estes aplicações que executam acções por conta de um controlador remoto e são instaladas dissimuladamente numa máquina-vítima.

11 Identificação via radiofrequências

12 Eurostat, "Internet activities in the European Union", 40/2005.

Por outro lado, dada a crescente conectividade entre redes, também outras infra-estruturas críticas (transportes, energia, etc.) estão a ficar cada vez mais dependentes da integridade dos seus sistemas de informação.

As empresas e os cidadãos na Europa ainda subestimam os riscos por várias razões, pensando-se que a mais importante é, no caso das empresas, a escassa visibilidade do rendimento do investimento em segurança e, no caso dos cidadãos, o facto de não estarem conscientes da sua responsabilidade na cadeia de segurança global.

Na verdade, dada a omnipresença dos sistemas informáticos e de comunicações, a segurança das redes e da informação é um desafio para todos:

- As **administrações públicas** têm agir no que respeita à segurança dos seus sistemas, não só para protegerem informação do sector público, mas igualmente para servirem de exemplo das melhores práticas para outros intervenientes;

- As **empresas** têm de encarar a SRI como um trunfo e um factor de vantagem competitiva e não como "um custo negativo";

- Os **utilizadores** têm de compreender que os seus sistemas domésticos são críticos para a "cadeia de segurança" global.

Para enfrentarem com êxito os problemas acima descritos, todas as partes interessadas necessitam de dados fiáveis sobre os incidentes e as tendências no domínio da segurança da informação. Contudo, é difícil obter dados fiáveis e completos sobre tais incidentes, por múltiplas razões, que vão da rapidez com que estes ocorrem à relutância de algumas organizações em divulgarem e publicarem casos de ruptura na segurança. No entanto, uma das pedras angulares do desenvolvimento de uma cultura de segurança consiste em **melhorar o nosso conhecimento do problema**.

É importante que os programas de sensibilização, concebidos para evidenciarem as ameaças à segurança, não minem a confiança dos consumidores e utilizadores, incidindo apenas nos aspectos negativos da segurança. Assim, **a SRI deve, sempre que possível, ser apresentada como uma virtude e uma oportunidade** e não como uma responsabilidade e um custo. Deve ser vista como um trunfo na criação de confiança, nomeadamente a confiança dos consumidores, uma vantagem competitiva para as empresas que utilizam sistemas de informação e uma vertente da qualidade do serviço para fornecedores, públicos ou privados, de serviços.

O desafio fundamental para os decisores políticos consiste em adoptar uma abordagem holística. Esta abordagem deve reconhecer o papel de cada uma das partes interessadas e assegurar uma correcta coordenação de todas as disposições políticas e regulamentares que têm influência directa ou indirecta na SRI. Os processos de liberalização, desregulamentação e convergência deram origem a uma multiplicidade de intervenientes nos vários grupos de interessados, o que não facilita esta tarefa. O contributo da ENISA para este objectivo pode ser importante. A ENISA pode funcionar como um centro de partilha de informação, de cooperação entre todos os interessados e de intercâmbio de práticas recomendáveis, na Europa e com o resto do mundo, de modo a contribuir para a competitividade das nossas empresas de TIC e para o bom funcionamento do mercado interno.

3. PARA UMA ABORDAGEM DINÂMICA DE UMA SOCIEDADE DA INFORMAÇÃO SEGURA

Uma sociedade da informação segura deve assentar numa **SRI reforçada** e numa **cultura de segurança** generalizada. Para tal, a Comissão Europeia propõe uma **abordagem dinâmica e integrada** que envolve todas as partes interessadas e se baseia **no diálogo, em parcerias e num maior poder de intervenção**. Dada a complementaridade dos papéis dos sectores público e privado na criação de uma cultura de segurança, as iniciativas políticas neste domínio devem basear-se num **diálogo aberto e inclusivo entre os vários interessados**.

Esta abordagem, bem como as acções conexas, complementará e enriquecerá o plano da Comissão para avançar no desenvolvimento de um quadro político global e dinâmico através de um conjunto de iniciativas previstas para 2006:

(1) Abordar a evolução do *spam* e das ameaças, como o software-espião e outras formas de *malware*, numa comunicação sobre estas questões específicas.

(2) Elaborar propostas para melhorar a cooperação entre as autoridades responsáveis pela aplicação da lei e fazer face a novas formas de actividade criminosa que exploram a Internet e minam o funcionamento de infra-estruturas críticas. Esta questão será objecto de uma comunicação específica sobre a cibercriminalidade.

Estas iniciativas políticas complementam igualmente as actividades actualmente em fase de planeamento que visam os objectivos do Livro Verde da Comissão relativo a um programa europeu de protecção das infra-estruturas críticas (PEPIC)[13], criado como resposta a um pedido do Conselho de Dezembro de 2004. Em princípio, o processo do Livro Verde conduzirá a um plano de acção que combinará uma abordagem global da protecção das infra-estruturas críticas com as necessárias políticas sectoriais, incluindo uma para o sector das TIC. A política sectorial para as TIC examinará, **através de um diálogo entre os vários interessados**, os elementos catalisadores económicos, empresariais e sociais com vista a reforçar a segurança e a resistência de redes e sistemas de informação.

Por outro lado, a revisão de 2006 do quadro regulamentar das comunicações electrónicas ponderará igualmente a introdução de elementos que melhorem a SRI, como medidas técnicas e organizativas a adoptar pelos fornecedores de serviços, disposições respeitantes à notificação de casos de ruptura da segurança ou ainda medidas correctivas e sanções específicas para a violação de obrigações.

Compete essencialmente ao sector privado oferecer soluções, serviços e produtos de segurança aos utilizadores finais. Por conseguinte, é estrategicamente importante que **a indústria europeia seja simultaneamente um utilizador exigente** de produtos e serviços de segurança **e um fornecedor competitivo** de produtos e serviços SRI.

É necessário que os governos nacionais estejam em condições de identificar e aplicar as melhores práticas na definição de políticas e de demonstrar empenho nesses objectivos políticos, gerindo os seus próprios sistemas de informação de modo seguro. As autoridades públicas, nos Estados-Membros e a nível comunitário, têm um papel essencial a desempenhar na acção de informar correctamente os utilizadores para que estes possam contribuir para a sua própria segurança. A sensibilização para as questões da SRI e o fornecimento de informação adequada e oportuna, através de portais Web dedicados à segurança electrónica,

---

[13] COM(2005) 576 final de 17.11.2005

sobre ameaças, riscos e alertas e sobre as melhores práticas devem ser prioritários. Para tal, a análise da viabilidade da **criação de um sistema europeu multilingue de alerta e partilha de informação**, que assente em iniciativas públicas e privadas nacionais, existentes ou previstas, e as ligue entre si, poderá ser um objectivo importante para a ENISA.

A dimensão mundial da segurança das redes e da informação exige que a Comissão, a nível internacional e em coordenação com os Estados-Membros, intensifique os seus esforços para **promover a cooperação mundial neste domínio**, nomeadamente através da aplicação da agenda adoptada na Cimeira Mundial sobre a Sociedade da Informação (WSIS) que teve lugar em Novembro de 2005.

Por último, as actividades de investigação e desenvolvimento, nomeadamente a nível comunitário, contribuirão para criar parcerias novas e inovadoras que impulsionem o crescimento da indústria europeia das TIC em geral e da indústria europeia da segurança das TIC em especial. Assim, a Comissão procurará que sejam atribuídos recursos financeiros adequados à investigação em tecnologias para a SRI e a fiabilidade no âmbito do 7.º Programa-Quadro comunitário.

3.1. Diálogo

3.1.1. *Como primeiro passo para melhorar o diálogo entre as autoridades públicas, a Comissão propõe-se lançar um exercício de* ***aferição de desempenhos das políticas nacionais relacionadas com a SRI****, incluindo políticas de segurança específicas para o sector público. Este exercício contribuirá para identificar as práticas mais eficazes, de modo que estas possam, em seguida, ser implantadas, sempre que possível, mais generalizadamente na UE e para tornar as administrações públicas um vector das melhores práticas no domínio da segurança. Os trabalhos relativos à identificação electrónica, nomeadamente no âmbito do recente plano de acção eGovernment, poderão desempenhar um papel importante neste contexto.*

Se adequadamente estruturados, os resultados desta aferição de desempenhos **identificarão as melhores práticas de sensibilização das PME e dos cidadãos para a necessidade** de agirem no que respeita aos seus próprios desafios e requisitos específicos na área da SRI e à sua capacidade para tal. Deve pedir-se à ENISA que desempenhe um papel activo neste diálogo e na consolidação e intercâmbio das melhores práticas.

3.1.2. *É necessário um* ***debate estruturado entre os vários interessados*** *sobre o melhor modo de explorar as ferramentas e os instrumentos regulamentares existentes para alcançar um equilíbrio social adequado entre segurança e protecção dos direitos fundamentais, incluindo a privacidade. A conferência "i2010 - Para uma sociedade da informação europeia omnipresente", que está a ser organizada pela próxima Presidência finlandesa, e a consulta sobre as implicações da RFID para a segurança e a privacidade, que se integra na consulta mais ampla lançada recentemente pela Comissão, contribuirão para este debate. Por outro lado, a Comissão organizará:*

- Um evento para empresas com vista a incentivar o seu empenho na adopção de abordagens eficazes de implantação de uma cultura de segurança **na indústria**.

- Um seminário que estudará formas de sensibilização para as questões da segurança e de reforço da confiança dos **utilizadores finais** na utilização das redes e sistemas de informação electrónicos.

3.2. Parcerias

3.2.1. Para que a definição de políticas seja eficaz, é necessária uma compreensão clara da natureza e dimensão dos desafios. Tal exige não só dados estatísticos e económicos fiáveis e actualizados sobre os incidentes de segurança da informação e os níveis de confiança dos consumidores e utilizadores, mas também dados actualizados sobre a dimensão e as tendências da indústria da segurança das TIC na Europa. A Comissão tenciona pedir à ENISA que desenvolva ***uma parceria de confiança com os Estados-Membros e as partes interessadas*** *com vista à criação de um* ***quadro adequado para a recolha de dados****, incluindo os procedimentos e mecanismos de recolha e análise de dados, em toda a UE, sobre os incidentes de segurança e a confiança dos consumidores.*

Paralelamente, dada a elevada fragmentação do mercado na UE e a sua natureza muito específica, a Comissão convidará os Estados-Membros, o sector privado e a comunidade dos investigadores a **estabelecer uma parceria estratégica** para assegurar a disponibilidade de dados sobre a indústria da segurança das TIC e sobre as tendências de evolução dos mercados de produtos e serviços na UE.

3.2.2. Para aumentar a capacidade de resposta da Europa a ameaças contra a segurança das redes, a Comissão pedirá à ENISA que examine a ***viabilidade de um sistema europeu de alerta e partilha de informação*** *que facilite uma resposta eficaz às ameaças existentes e emergentes às redes electrónicas. Um dos requisitos desse sistema é a criação de* ***um portal comunitário multilingue*** *que apresente informação, adaptada às necessidades dos destinatários, sobre ameaças, riscos e alertas.*

3.3. Maior poder de intervenção

Um maior poder de intervenção de cada grupo de interessados constitui um pré-requisito para fomentar um maior conhecimento das necessidades e dos riscos em termos de segurança, a fim de promover a SRI.

3.3.1. Neste contexto, a Comissão convida os ***Estados-Membros*** *a:*

- Participarem activamente no acima proposto exercício de aferição de desempenhos das políticas nacionais de SRI;

- Promoverem, em estreita cooperação com a ENISA, campanhas de sensibilização para as virtudes, os benefícios e as vantagens da adopção de tecnologias, práticas e comportamentos de segurança eficazes;

- Impulsionarem a implantação de serviços da Administração Pública em linha para comunicar e promover boas práticas de segurança, que poderão, em seguida, alargar-se a outros sectores;

- Estimularem o desenvolvimento de programas sobre a segurança das redes e da informação, a integrar nos currículos do ensino superior.

3.3.2. *A Comissão convida igualmente as partes interessadas do* ***sector privado*** *a tomarem iniciativas para:*

- Definir adequadamente as responsabilidades dos produtores de software e dos fornecedores de serviços Internet no que respeita à oferta de níveis de segurança adequados e fiscalizáveis. Aqui, é necessário apoio à utilização de processos normalizados conformes com as normas de segurança comummente aceites e as regras das melhores práticas.

- Promover a diversidade, a abertura, a interoperabilidade, a utilizabilidade e a concorrência como vectores essenciais da segurança e estimular a implantação de produtos, processos e serviços de reforço da segurança, para impedir e combater o roubo de dados de identificação e outros ataques violadores da privacidade.

- Difundir boas práticas de segurança para operadores de redes, fornecedores de serviços e PME, que proporcionem níveis básicos de segurança e continuidade da actividade empresarial.

- Promover programas de formação no sector empresarial, nomeadamente nas PME, para dotar os trabalhadores dos conhecimentos e competências necessários para adoptarem, com eficácia, as práticas de segurança.

- Trabalhar com vista à implantação de regimes de certificação da segurança pouco onerosos para produtos, processos e serviços adaptados às necessidades específicas da UE (nomeadamente no que respeita à privacidade).

- Envolver o sector dos seguros no desenvolvimento de ferramentas e métodos adequados de gestão dos riscos para fazer face aos riscos associados às TIC e promover uma cultura de gestão dos riscos em organizações e empresas (nomeadamente PME).

4. CONCLUSÕES

É necessário o empenho total de todas as partes interessadas para identificar e vencer os desafios da segurança relacionados com os sistemas e redes de informação na UE. A abordagem política delineada na presente comunicação procura alcançar este objectivo mediante o reforço duma **abordagem reunindo os vários interessados**. Este processo assentará nos interesses mútuos, identificará o papel de cada um e criará um quadro dinâmico para a promoção de uma definição eficaz de políticas públicas e de iniciativas do sector privado.

Em meados de 2007, a Comissão apresentará um relatório ao Conselho e ao Parlamento sobre as actividades já iniciadas, as primeiras conclusões e o ponto da situação das diversas iniciativas, incluindo as da ENISA e as lançadas pelos Estados-Membros e pelo sector privado. Se necessário, a Comissão proporá uma recomendação sobre a segurança das redes e da informação (SRI).