

## Comissão reforça as defesas da Europa contra os ataques informáticos

***A Comissão Europeia anunciou hoje duas novas medidas para garantir que a Europa se consegue defender de ataques contra os seus sistemas de informação (TI) essenciais. Uma proposta de directiva sobre as novas formas de cibercrime é complementada por uma proposta de regulamento destinado a reforçar e modernizar a Agência Europeia para a Segurança das Redes e da Informação (ENISA). As duas iniciativas estão previstas na [Agenda Digital para a Europa](#) e no Programa de Estocolmo, no intuito de aumentar a confiança e a segurança na rede (cf. [IP/10/581](#), [MEMO/10/199](#) e [MEMO/10/200](#)). Nos termos da proposta de directiva, os autores de ataques informáticos e os fabricantes de software conexo ou maligno podem ser julgados e condenados a penas mais pesadas. Os Estados-Membros serão também obrigados a responder com rapidez aos pedidos de ajuda em caso de ataque informático, tornando a cooperação judicial e policial europeia mais eficaz neste domínio. O reforço e modernização da ENISA contribuirá também para que a UE, os Estados-Membros e o sector privado desenvolvam as respectivas capacidades e preparação para prevenir, detectar e responder aos desafios à cibersegurança. Ambas as propostas serão enviadas ao Parlamento Europeu e ao Conselho de Ministros da UE para aprovação.***

A Comissária Malmström, responsável pelos Assuntos Internos, referiu: «O crime está a explorar novos caminhos. Com a ajuda de software maligno, é possível assumir o controlo de grande número de computadores e obter números de cartões de crédito ou informações sensíveis e lançar ataques de grande escala. É tempo de reforçarmos os nossos esforços contra o cibercrime, muitas vezes utilizado pela criminalidade organizada. As propostas que hoje apresentamos são um passo importante, visto que são previstos os crimes de criação e venda de software maligno e é reforçada a cooperação policial europeia.»

A Vice-Presidente da Comissão responsável pela Agenda Digital, Neelie Kroes, disse que «para que todos os europeus se convertam ao digital é necessário que se sintam confiantes e seguros em linha. As ameaças informáticas não conhecem fronteiras. Uma Agência Europeia para a Segurança das Redes e da Informação modernizada trará mais conhecimentos especializados e reforçará os intercâmbios de boas práticas na Europa. As instituições e os Governos da UE devem trabalhar mais do que nunca em conjunto, para nos ajudar a compreender a natureza e a escala das novas ameaças informáticas. Precisamos dos conselhos e do apoio da ENISA para conceber mecanismos de resposta eficazes para proteger os nossos cidadãos e empresas em linha».

O facto de a Europa estar empenhada em aproveitar plenamente o potencial das redes e sistemas de informação não deve implicar que se torne mais vulnerável às perturbações por causas acidentais ou naturais (como a ruptura de cabos submarinos) ou decorrentes de actos maliciosos (como a pirataria informática ou outros ataques informáticos). Esses actos podem recorrer, por exemplo, a ferramentas cada vez mais sofisticadas que permitem piratear um grande número de computadores e manipulá-los como um exército de robôs na internet (*botnets*), sem o conhecimento dos proprietários. Estes computadores infectados podem ser usados mais tarde para a prática de ataques devastadores contra sistemas de TI públicos e privados, como ocorreu na Estónia em 2007, quando a maior parte dos serviços públicos em linha, bem como os servidores do Governo, do Parlamento e da Polícia ficaram temporariamente sem funcionar. O número de ataques contra sistemas de informação tem vindo a aumentar a um ritmo regular desde que, em Fevereiro de 2005, a UE adoptou as primeiras normas aplicáveis aos [ataques contra sistemas de informação](#). Em Março de 2009, os sistemas informáticos de organismos governamentais e do sector privado de 100 países foram atacados por uma rede de computadores «sequestrados», que extraíram documentos sensíveis e confidenciais. Neste caso, mais uma vez, o *software* maligno criou *botnets*, que são redes de computadores infectados que podem ser controlados à distância para a prática de ataques coordenados.

O pacote hoje proposto pela Comissão virá reforçar a resposta da Europa às perturbações informáticas. A proposta da Comissão sobre o cibercrime baseia-se nas normas em vigor desde 2005 e introduz novas circunstâncias agravantes e penas mais elevadas, consideradas necessárias para combater de forma mais eficaz as ameaças crescentes e a ocorrência de ataques de grande escala contra sistemas de informação.

Além disso, a proposta abre caminho ao reforço da cooperação judicial e policial entre Estados-Membros, introduzindo a obrigação de utilizar melhor a rede já existente de pontos de contacto (que funcionam 24 horas por dia, 7 dias por semana) e dar resposta aos pedidos urgentes no prazo fixado.

Por último, a proposta de directiva prevê a criação de um sistema de registo e rastreio dos ataques informáticos.

### **Cooperação reforçada entre os países e o sector industrial**

Para ajudar a coordenar a resposta da Europa, a Comissão propõe um novo regulamento para reforçar e modernizar a Agência Europeia para a Segurança das Redes e da Informação ([ENISA](#)), criada em 2004. Esta modernização virá reforçar a cooperação entre os Estados-Membros, as autoridades policiais e o sector industrial. A ENISA terá um papel importante para fazer aumentar a confiança, que é essencial ao desenvolvimento da sociedade da informação, reforçando a segurança e a privacidade dos utilizadores.

No âmbito das suas novas atribuições, a ENISA mobilizará os Estados-Membros da UE e as partes interessadas do sector industrial em actividades conjuntas na Europa, tais como exercícios de segurança informática, parcerias público-privado para a resiliência das redes, análises económicas, avaliação de riscos e campanhas de sensibilização.

Uma ENISA modernizada terá maior flexibilidade e adaptabilidade e poderá prestar assistência e aconselhamento aos países e instituições da UE em matéria normativa.

Por último, para responder à crescente intensidade dos desafios à cibersegurança, a proposta de regulamento prorroga o mandato da agência por cinco anos e prevê o aumento gradual dos respectivos recursos financeiros e humanos. A Comissão propõe que a estrutura de gestão da ENISA seja reforçada através de maiores poderes de controlo do conselho de administração, no qual estão representados os Estados-Membros da UE e a Comissão Europeia.

### **Antecedentes**

A proposta de directiva sobre os ataques contra sistemas de informação revoga a Decisão-Quadro 2005/222/JAI do Conselho. Os Estados-Membros devem cumprir a nova directiva sobre o cibercrime e transpô-la para a legislação nacional no prazo de dois anos a contar da sua adopção.

A ENISA foi criada em 2004 e o seu mandato actual termina em Março de 2012. Propõe-se agora a sua prorrogação por 5 anos. Esta proposta de regulamento é o resultado de um vasto processo, que incluiu uma avaliação da referida agência, recomendações do seu conselho de administração, duas consultas públicas e uma avaliação de impacto com uma análise de custo/benefício.

### **Para mais informações**

Página inicial de Cecilia Malmström, Comissária dos Assuntos Internos da UE:

[http://ec.europa.eu/commission\\_2010-2014/malmstrom/index\\_en.htm](http://ec.europa.eu/commission_2010-2014/malmstrom/index_en.htm)

Página inicial de Neelie Kroes, Vice-Presidente da Comissão para a Agenda Digital

[http://ec.europa.eu/commission\\_2010-2014/kroes/index\\_en.htm](http://ec.europa.eu/commission_2010-2014/kroes/index_en.htm)

Sala de imprensa da sociedade da informação

[http://ec.europa.eu/information\\_society/newsroom/cf/menu.cfm](http://ec.europa.eu/information_society/newsroom/cf/menu.cfm)

[MEMO/10/459](#)

[MEMO/10/463](#)