BANCO DE PORTUGAL
EUROSISTEMA

Cibersegurança no sistema financeiro: riscos, cooperação e governação

30 de junho de 2017

Intervenção na sessão de abertura do Administrador Hélder Rosalino [1]

Bem-vindos ao Banco de Portugal e à conferência que organizamos sobre "Cibersegurança no sistema financeiro: riscos, cooperação e governação".

Agradeço, em nome do Conselho de Administração do Banco de Portugal e dos departamentos organizadores, o elevado interesse demonstrado na participação nesta Conferência, tanto de entidades do sistema bancário aqui amplamente representadas, como de muitas outras entidades que se associaram a esta iniciativa.

Não obstante o tema da cibersegurança ser transversal a todo o tipo de organizações e setores de atividade, esta conferência foca-se essencialmente no sistema financeiro e aborda algumas das dimensões da cibersegurança que se colocam a este setor.

- Temos um primeiro painel sobre o impacto do ciber-risco no Sistema Financeiro e na continuidade de negócio:

  Painel sobre Impacto do Ciberrisco no Sistema Financeiro
  e a Continuidade de Negócio
  Moderador:
  Gabriel Andrade, Diretor Adjunto do Departamento de Risco, Banco de Portugal

  Duncan Brown, Associate Vice President, European Security Practice, IDC EMEA
  Keith Gross, Head of Financial Crime & Security, Banking & Payments Federation Ireland
  Alain Raes, Chief Executive EMEA & ASAP, SWIFT

- Temos um segundo painel que se foca na Cooperação e Governação de Cibersegurança no contexto do Sistema Financeiro:

[1] Preparado para apresentação.

Painel sobre Cooperação e Governação de Cibersegurança no contexto do Sistema Financeiro

Moderator:
Manuel Vilares, Coordenador da Comissão de Risco, Banco de Portugal

Pedro Veiga, Coordenador do Centro Nacional de Cibersegurança
Katherine Gagnon, World Bank
Iniciativas do Banco de Portugal, Orlando Gonçalves (Departamento de Supervisão Prudencial) e Luis Gonçalves (Departamento de Sistemas e Tecnologias de Informação)

O tema da Cibersegurança

É um tema de grande atualidade, a todos os títulos, como o comprova o ataque informático registado na passada terça-feira (conhecido como *NotPetya*) e que teve impactos à escala global.

Como, aliás, já tinha acontecido com o ciberataque registado em maio, conhecido como *WannaCry*, que colocou a cibersegurança no centro do debate público e das preocupações de todas as organizações públicas e privadas.

No entanto, esses ataques também vieram demonstrar que ainda não estamos suficientemente preparados para enfrentar esta nova ameaça e que, tão pouco, temos uma consciência coletiva apurada sobre o que a mesma representa.

O que sabemos é que o contexto atual, neste âmbito, se carateriza:

- Pela crescente complexidade e volumetria dos ciberataques;
- Pela existência de redes de cibercrime cada vez mais sofisticadas, eventualmente suportadas por Estados cuja economia se pode basear, em parte, nesta atividade, dado o retorno financeiro que pode gerar;
- Pela falta de enquadramento legal adequado, ou em desenvolvimento ainda embrionário, criando um sentimento de impunidade na concretização de atos maliciosos no ciberespaço;
- Pelo caráter permanente e imprevisível dos ataques: sem hora específica para acontecer e podendo vir geograficamente de qualquer lado, o que obriga a uma vigilância contínua e cada vez mais complexa de implementar;

- Pelo aumento do risco para o funcionamento das organizações, com ciberataques progressivamente mais destrutivos e com capacidade efetiva de interrupção de setores e negócio vitais para o funcionamento da economia.

  Foi, aliás, o que aconteceu com os mais recentes ataques (WannaCry e o NotPetya), que causaram danos a nível mundial e de forma transversal, afetando setores como a banca, a saúde, os operadores de serviços de comunicações, entre outros.

Vivemos, sem dúvida, num ambiente de elevada complexidade em termos de cibersegurança, potenciado por um conjunto de riscos e ameaças que a todos convoca para a reflexão e sobretudo para a ação.

O contexto

A utilização de tecnologias e de sistemas de informação permitiu, nas últimas décadas, uma completa transformação da forma de funcionamento das sociedades.

Num curto espaço de tempo, passámos a comunicar globalmente a custos muito baixos, construímos novas formas de relações entre as pessoas e entre as empresas, aprendemos a tirar partido do grande volume de dados e de informação que produzimos, automatizámos processos, passámos a controlar à distância, entre muitas outras evoluções de base tecnológica.

Em suma, reorganizamos completamente a nossa vida em torno das tecnologias.

E quando olhamos para a frente percebemos que o potencial de evolução e de aplicação destas tecnologias é enorme e tenderá inevitavelmente a acelerar.

No sistema financeiro a evolução foi paralela e Portugal tem estado na linha da frente em algumas áreas de inovação. Podemos recordar, como exemplo pioneiro e sempre citado, o "sistema multibanco" que permite a realização de um grande número de operações bancárias em rede e fora dos balcões, a par da recente massificação da banca digital e da extraordinária evolução dos sistemas de pagamentos eletrónicos a que temos assistido.

Todas estas evoluções permitiram significativos ganhos de eficiência e de eficácia.

A dependência

Porém, as vantagens foram tão grandes e a evolução foi tão rápida que, sem nos apercebermos disso, toda a sociedade ficou dependente das tecnologias de informação. De tal forma que já não conseguimos imaginar como poderemos funcionar sem elas.

Não pondo, naturalmente, em causa os enormes benefícios das tecnologias de informação, a verdade é que a dependência criada é motivo de enorme preocupação.

As vulnerabilidades geradas por esta dependência assumem várias facetas, que produziram alguns exemplos recentemente conhecidos:

- Um respeita à relativa facilidade e impunidade com que indivíduos ou grupos conseguem realizar roubos e causar danos a terceiros, como aconteceu no caso do roubo ao Banco Central do Bangladeche, que se traduziu em perdas na ordem dos 84 milhões de euros, mas cujos danos podiam ter ultrapassado os mil milhões de euros;
- Outro exemplo, são as próprias falhas nos sistemas, ou automáticas ou provocadas manualmente, cujos impactos podem ser extremamente elevados, como aconteceu recentemente quando uma falha de energia no *Data Center* da *British Airways* levou ao cancelamento de inúmeros voos e a impactos financeiros extremamente elevados;
- Temos ainda a crescente interligação dos mundos Ciber e físico, que levaram, por exemplo, a que um ciberataque desligasse centrais elétricas na Ucrânia, no final do ano passado. Ou que *hackers* conseguissem desligar as câmaras de videovigilância na tomada de posse do Presidente dos Estados Unidos.
- E temos naturalmente a disseminação massiva de *software* malicioso que pode levar à disrupção total ou parcial dos sistemas de informação, como são exemplo os ataques que ocorreram recentemente.

É neste contexto de ameaça quase permanente, sob diferentes facetas, que a cibersegurança assume uma crescente e fundamental importância.

Essa importância remete-nos para os temas da Governação e da Cooperação no domínio da cibersegurança.

O bom governo da cibersegurança é um desafio incontornável no momento atual e sê-lo-á ainda mais no futuro. Essa é uma consciência que estamos agora a assumir, talvez um pouco tarde.

Esse bom governo deve estar consubstanciado numa Estratégia Global de cibersegurança, baseada numa visão organizacional a 360º e associada a uma cultura de segurança corporativa, recuperando o conceito de *Corporate Security*.

Este conceito assenta numa abordagem integrada da segurança da informação, dos sistemas e tecnologias e da segurança física.

Esta Estratégia Global deverá assentar sobre os três pilares essenciais da cibersegurança [**pessoas, processos e tecnologia**], mas também sobre uma cultura de cooperação institucional que promova a partilha de informação e, sobretudo, que desenvolva a criação de redes de confiança e de trabalho conjunto entre entidades congéneres e pares.

É necessário, mais do que nunca, promover uma forte colaboração e organização no domínio ciber-crime para enfrentar as crescentes ameaças.

Os indivíduos e as organizações têm de criar condições suficientes para, por um lado, promoverem a sua autoproteção, e por outro, participar como parte integrante de um sistema de defesa que tem que envolver todos.

Esta questão será aprofundadamente debatida no painel sobre a **Cooperação e Governação de Cibersegurança,** na segunda parte desta conferência.

Do mesmo modo, é de extrema importância apostar na formação e na consciencialização das pessoas (e com isso de toda a organização), como pilar fulcral e de primeira linha na defesa a ciber-ataques. Neste domínio há ainda um longo trabalho a fazer.

O papel do Banco de Portugal

O Banco de Portugal está naturalmente atento e preocupado com esta realidade.

Importa referir que o Banco de Portugal desenvolve, desde 2011, uma estratégia consistente no domínio da cibersegurança, com resultados importantes e reconhecidos ao nível nacional e internacional.

Internamente, o Banco de Portugal dispõe de recursos altamente especializados em cibersegurança e tem vindo, nos últimos tempos, a desenvolver e reforçar as suas competências e a alargar as suas redes de cooperação no domínio da prevenção do cibercrime.

Enquanto regulador e supervisor do sistema financeiro, o Banco de Portugal tem igualmente desenvolvido, mais recentemente, um conjunto de iniciativas e ações orientadas para a integração e o bom funcionamento de todo o sistema no domínio da cibersegurança.

Isso tem acontecido:

- Através da criação de uma equipa especializada na vertente de SOC (Security Operations Center) e de CSIRT – Computer Security Incident Response Team, com recursos humanos dedicados à gestão da Cibersegurança na perspetiva interna e sectorial;
- Através da promoção de parcerias estratégias nesta área, nomeadamente com o Centro Nacional de Cibersegurança e com a Polícia Judiciária, na figura da sua Unidade Nacional de Combate ao Cibercrime;

  e em termos gerais

- Através da promoção de uma cultura de partilha de conhecimento, experiências e metodologias de defesa e mitigação, tanto ao nível do SEBC, como ao nível nacional na relação com várias entidades ligadas ao sistema financeiro.

Recentemente, tendo em consideração as suas obrigações enquanto banco central, o Banco de Portugal iniciou um processo de reforço das suas competências e organização

no sentido da criação de um CSIRT para o setor bancário, com enfoque nas seguintes vertentes:

- Estabelecimento de canais de comunicação para troca de informações relevantes com todas as entidades do setor financeiro;
- Desenvolvimento de processos de *intelligence*, que visem a previsão atempada de ataques planeados;
- Reforço da capacidade de deteção automática de ciberataques, mediante a criação de controlos tecnológicos de vária ordem.

Esta evolução deverá posicionar o Banco de Portugal, naturalmente, como a entidade centralizadora e agregadora do setor bancário para a vertente da cibersegurança, funcionando como entidade responsável ao nível sectorial.

Nesse papel, o Banco incentivará a cooperação e a colaboração dentro do sector bancário, de forma próxima e integrada com a autoridade nacional, o Centro Nacional de Cibersegurança.

Nessa linha, foi criado um grupo de trabalho interno para apoio ao Centro Nacional de Cibersegurança na transposição da Diretiva relativa à Segurança das Redes e dos Sistema de Informação (SRI/NIS). Trabalho que já está em curso.

Estas ações são representativas da importância que a cibersegurança assume para o Banco de Portugal, na perspetiva própria e do sector financeiro.

A organização desta conferência é o reflexo dessa importância. É também uma forma de fomentar a partilha de conhecimento e de apresentar o papel do Banco de Portugal na promoção da cibersegurança, sobretudo na perspetiva do seu papel sectorial.

Concluindo

Temos que começar por reconhecer que a cibersegurança tem atualmente um papel fundamental na defesa de alguns dos nossos princípios básicos de cidadania e mesmo na defesa de alguns dos alicerces fundamentais em que está construído o nosso modelo de vida atual.

Pelo papel que desempenha na nossa organização económica e social, o setor bancário é especialmente visado pelas atividades do cibercrime, quer pela relevância das suas funções, quer pela abertura e vulnerabilidades naturais dos sistemas tecnológicos que suportam a sua atividade.

A gestão destes riscos é cada vez mais importante, sobretudo devido aos desafios que as instituições financeiras enfrentam atualmente nos domínios da transformação digital e da evolução dos quadros regulamentares conexos, que tendem a criar ambientes cada vez mais abertos e competitivos no sector bancário. Neste contexto, é assumido que o sistema financeiro se deve apetrechar de modo particular para a promoção da cibersegurança.

Pela sua parte, o Banco de Portugal assumirá de forma clara e empenhada as suas responsabilidades nesta área. Quer como agente ativo na criação e promoção de um sistema integrado de ciber-defesa para o setor bancário, quer como supervisor exigindo naturalmente que os Bancos implementem estratégias e mecanismos de proteção, partilha e reporte de informação necessários.

Espero que esta conferência se transforme num valioso contributo para ajudar à construção de uma visão partilhada sobre os desafios que enfrentamos no domínio da cibersegurança e sobre as melhores formas de cooperação para combater a nova e crescente ameaça do cibercrime.

Muito obrigado

Hélder Rosalino

Glossário de termos:

Ciberataque [Definição] – Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente.

[Fonte] - Austrian Cyber Security Strategy (2013), citado em NATO CCDCOE.

CiberCrime [Definição] – Atos criminosos cometidos cometidos on-line utilizando redes de comunicação eletrónicas e sistemas de informação.

[Fonte] – Comissão Europeia.

Ciberdefesa [Definição] – O termo "ciber defesa" refere-se a todas as medidas utilizadas para defender o espaço cibernético com os meios militares e apropriados para alcançar objetivos estratégico militares. A ciber defesa é um sistema integrado, que compreende a implementação de todas as medidas relacionadas com as TIC e a segurança da informação, os recursos milCERT e CNO (operações de rede do computador), bem como o apoio dos recursos físicos do exército.

[Fonte] - Austrian Cyber Security Strategy (2013), citado em NATO CCDCOE.

Ciberespaço [Definição] – Metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras, por exemplo, através de mensagens eletrónicas, em salas de conversa ou em fóruns de discussão.

[Fonte] - Associação para a Promoção e Desenvolvimento da Sociedade de Informação.

Rede Nacional de CSIRT [Definição] – A Rede Nacional de CSIRTs é um forum de para a partilha de informação de carácter operacional. Tem como principais objetivos:

- Estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;

- Criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contra-medidas pró-ativas e reativas;
- Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;
- Promover uma cultura de segurança em Portugal.

[Fonte] - Centro Nacional de Cibersegurança Portugal

Segurança das Redes e dos Sistemas de Informação [Definição] – a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles.

[Fonte] – Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.