UPDATE #33 2018

Digital Business Community

Workshop

"REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO"

Centro Nacional de Cibersegurança

18 Abril 2018

Preparar a segurança no ciberespaço nacional

A transposição da Diretiva SRI para o ordenamento jurídico nacional está em marcha, aguardando luz-verde do Parlamento. Em paralelo, a versão 2.0 da Estratégia Nacional de Segurança do Ciberespaço será entregue ao Executivo em maio. Há governance, estratégia e medidas para que Portugal possa ter, até novembro, todas as ferramentas necessárias para garantir a segurança no mundo digital. Mas é preciso mais: parcerias, reforço da cooperação entre público e privado e consciencialização de cidadãos e empresas para os perigos do online deverão ser prioridades.

NO WORKSHOP RESERVADO sobre o "Regime Jurídico da Segurança do Ciberespaço", que resultou de uma parceria entre a APDC e o Centro Nacional de Cibersegurança (CNCS), estiveram em debate dois temas verdadeiramente críticos: a proposta de lei sobre o Regime Jurídico da Segurança do Ciberespaço, aprovada pelo Conselho de Ministros a 15 de março, que transpõe para o ordenamento nacional a Diretiva SRI, que contém as medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em todo o espaço europeu; e a nova versão da Estratégia Nacional de Segurança no Ciberespaço.

"A tecnologia traz consigo um conjunto de oportunidades, mas também muitas ameaças. Não é por isso que a vamos deixar de usar. Mas temos muita coisa nos nossos negócios dependentes do ciberespaço e estamos expostos a um novo conjunto de ameaças que é preciso antecipar e evitar. Um sistema legislativo adequado e a prevenção têm que ser apostas, pelo que é fundamental saber qual o enquadramento jurídico que vai vigorar e as ações que serão encetadas", destacou na abertura deste encontro, que decorreu a 18 de abril, o Presidente da APDC, Rogério Carapuça. Daí a importância deste evento para as empresas do setor das TIC e Media que tiverem a oportunidade de estar presentes.

REAJUSTAR ÀS METAS DE BRUXELAS

São já vários os processos em desenvolvimento, com deixou claro Alexandre Leite, do CNCS e um dos dois responsáveis pelo projeto de lei de transposição, que explicou as metas e os objetivos da Diretiva SRI (2016/1148)

Para o Presidente da APDC, a cibersegurança é uma matéria que existe ter um sistema legislativo adequado e mecanismos de prevenção eficientes

e as opções feitas no âmbito da definição do Regime Jurídico da Segurança do Ciberespaço, que transpõe para Portugal uma Diretiva que é obrigatória em todo o espaço europeu. Assim como as implicações da nova legislação de cibersegurança, que deverão entrar em vigor ainda este ano.

Tal como os demais países europeus, Portugal tem até 9 de maio - a data limite dada por Bruxelas para todos os países - para a transposição das regras europeias sobre cibersegurança, através da Diretiva SRI. Coube à Presidência do Conselho de Ministros e ao Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança (GNS/CNCS), que iniciou atividades em outubro de 2014, liderar o processo de transposição para o ordenamento jurídico nacional.

Para combater a crescente ameaça dos ciberataques e tirar partido das oportunidades da nova era digital, Bruxelas adotou uma abordagem comum de cibersegurança, cujo pilar assenta nesta Diretiva, que define as regras de segurança das redes e de informação. Nela, estabelece-se a obrigação de todos os estados-membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação, criando-se ainda um Grupo de Cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações, e uma Rede Europeia de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT), para reforçar a confiança entre estados-membros e promover uma cooperação operacional célere e eficaz.

Alexandre Leite explica que na avaliação realizada por Bruxelas, uma das limitações detetadas foi a da inexistência de uma cooperação formal entre os vários países ao nível do reporte de incidentes e de partilha de informação em matéria de cibersegurança. Pelo que "o legislador entendeu ser necessário construir uma rede que permitisse essa partilha".

Não sendo fácil "saber quem são as entidades com responsabilidade nacional de coordenação", a Diretiva obrigou os legisladores nacionais a designarem uma ou várias autoridades, deixando essa decisão aos estados-membros, tendo em conta as respetivas caraterísticas e modelos. Obriga ainda à designação de uma equipa de resposta a incidentes de segurança informática nacional para partilha de informação.

A capacitação nacional e a adoção de uma estra-

Prevenção, educação e sensibilização, I&D e inovação e estrutura de governance nacional foram as apostas estratégicas nacionais, como explicou Alexandre Leite, do CNCS

tégia com requisitos fixados foram outros objetivos. "Portugal fez a avaliação da estratégia que o país adotou, tendo sido definidos eixos para endereçar questões como a prevenção, educação e sensibilização, I&D e inovação e ter uma estrutura de governance nacional que possa atribuir às entidades responsabilidades", explica este responsável.

Em Portugal, a estrutura nacional implementada após 2014 passou pela criação de um Centro Nacional de Cibersegurança (CNCS), a autoridade nacional competente em matéria de cibersegurança do Estado e dos operadores de infraestruturas críticas nacionais. Entretanto, o CERT.PT, que coordena a resposta a incidentes, transitou para a esfera do CNCS, passando a CSIRT nacional.

A Diretiva traz ainda dois conceitos novos: o de prestadores de serviços essenciais e os prestadores de serviços digitais, englobando aqui os que prestam serviços digitais de computação na nuvem, mercados online e motores de busca. Alexandre Leite destaca que nesta matéria dos prestadores de serviços digitais, "não há prerrogativa nacional sobre as entidades identificadas", já que se incluem todas as que entrarem no conceito.

Já quanto aos operadores de serviços essenciais, o legislador europeu consagrou que são entidades públicas ou privadas que prestem um serviço considerado essencial à sociedade, cujas falhas podem pôr em causa o regulador funcionamento do país. Aqui, foram definidos sete setores – transportes, energia, água, saúde,

Para Gameiro Marques, líder do Gabinete Nacional de Segurança, num mundo cada vez mais globa, nada se faz sem a cooperação entre entidades do setor público e privado. Só isso garante medidas efetivas em matéria de cibersegurança

banca, serviços financeiros e estruturas digitais – ficando cada país livre de incluir mais setores. A proposta nacional manteve os termos da Diretiva e, tal como os demais países, Portugal terá que até dezembro de 2018 identificar os operadores de serviços essenciais. No que se refere ao regime sancionatório adotado para o mercado nacional, mas o valor das coimas "é relativamente baixo", uma vez que a preocupação foi de "não aumentar os custos de contexto das empresas", refere Alexandre Leite.

Há ainda algumas soluções legislativas nacionais extra-diretiva, como incluir também a Administração Pública como entidade sujeita à jurisdição do CNCS, sendo obrigada a cumprir requisitos de segurança e notificação de incidentes, e na estrutura e modelo de governance, onde o modelo nacional passou a incluir também o Conselho Superior de Segurança no Ciberespaço.

MÚLTIPLAS INICIATIVAS EM MARCHA

A proposta de lei que transpõe para o enquadramento legal nacional a Diretiva foi aprovada em Conselho de Ministros em meados de março, estando ainda em abril a aguardar votação final na Assembleia da República. Mas tal como na Europa a Diretiva é "apenas uma iniciativa entre muitas que a estratégia europeia de cibersegurança preconiza", também a lei que a transpõe "é apenas uma iniciativa entre muitas que constarão da futura estratégia nacional da segurança no ciberespaço", como explica este responsável.

Assim, estão em preparação dois diplomas

Alexandre Leite

CNCS

"Tal como a Diretiva é uma iniciativa entre muitas que a estratégia europeia de cibersegurança preconiza, também a lei que a transpõe é apenas parte das muitas que constarão da futura Estratégia Nacional da Segurança no Ciberespaço. Não é a lei que vai resolver todos os problemas"

"As coimas definidas na transposição da Diretiva têm um valor relativamente baixo. Estamos a criar um regime novo e a ênfase que é dada não é na parte sancionatória, mas sim na cooperação e da partilha de informação"

"Vamos ter uma visão clara de todo o regime legislativo para a cibersegurança, com requisitos objetivos e com prazos claros, quando a legislação complementar for aprovada. Terá que ser no prazo de 150 dias após a publicação a lei que transpõe a Diretiva SRI"

Gameiro Marques

Diretor-Geral do Gabinete Nacional de Segurança

"A estratégia é tão relevante quanto a sua capacidade de execução. O Conselho Superior de Segurança do Ciberespaço destina-se a controlar, monitorizar a acompanhar a execução dessa estratégia, que envolve vários atores, desde o público ao privado, passando pelas áreas de soberania, da economia e das universidades"

"O que estamos agora a fazer de mais relevante é a desenvolver a versão 2.0 da Estratégia Nacional de Segurança do Ciberespaço. Esta é uma área muito IT driven e que tem um impacto brutal na nossa sociedade e na forma como fazemos as coisas no dia a dia"

"Temos que fazer tudo sempre pensado no futuro e ligando à economia real. E nada se faz neste mundo global sem cooperar. Há que ter medidas efetivas"

O evento contou com um período de debate, onde foram detalhados vários aspectos da nova versão da Estratégia Nacional de Cibersegurança. Pedro Veiga, coordenador do CNCS até maio, foi um dos participantes

complementares. O primeiro, sobre requisitos de segurança, está a ser elaborado por uma equipa multidisciplinar. O segundo, de requisitos de notificação de incidentes, definindo em concreto os prazos para notificação, como é que esta se processará, quais os requisitos e obrigações inerentes e qual o conteúdo da notificação. "Teremos uma visão clara de todo o regime, com requisitos objetivos e com prazos, quando a legislação complementar for aprovada. Terá que ser feito no prazo de 150 dias após a publicação a lei que transpõe a Diretiva", acrescenta Alexandre Leite.

Já Gameiro Marques, Diretor Geral do Gabinete Nacional de Segurança, detalhou a estrutura de governance nacional que, em matéria de Cibersegurança, está na dependência direta do Primeiro-Ministro, através da ministra da Presidência e da Modernização Administrativa.

Trata-se de um verdadeiro "ecossistema" que envolve muitas áreas e organismos, como o Centro de Ciberdefesa, na dependência do EMGFA, a Unidade de Combate ao Cibercrime, da PJ, ou os Serviços de Informações da República. Salienta ainda a importância da Rede CSIRT nacional, composto por elementos dos setores público e privado. Todo este "conjunto é gerido pelo Conselho Superior de Segurança do Ciberespaço", entidade responsável pela "formulação da a estratégia e o controlo da sua execução".

Um dos dossiers considerado fundamental, que está em desenvolvimento, é a versão 2.0 da Estratégia Nacional de Segurança do Ciberespaço (ENSC), que surgiu pela primeira vez no espaço nacional em 2015. Esta revisão resulta não só de esta ser uma área muito IT driven mas ainda do próprio documento, que estabelece um timeline para se proceder a atualizações. O documento deverá ser entregue ao Executivo ainda em maio.

Para Gameiro Marques, a nova proposta é mais abrangente, tendo em conta toda a experiência e aprendizagem conseguida com o que foi feito até agora. Pretende-se fazer diferente, num trabalho de revisão que envolveu contributos do setor privado e de entidades ligadas à investigação e desenvolvimento e à inovação. A visão? "Garantir que Portugal seja um pais seguro e próspero, através de uma ação inovadora e inclusiva", permitindo que o país seja resiliente a ataques e garanta o regular funcionamento da sociedade face à evolução digital.

Ter recursos humanos em número suficiente para os desafios que se colocam com a economia digital, fomentar a ligação entre I&D e inovação e a economia real e tornar Portugal capaz de suster, identificar e combater ameaças no ciberespaço são as metas no novo documento. As medidas que preconiza serão depois densificadas num plano de ação, que terá que ser publicado até 120 dias após a publicação da ENSC.

"O plano de ação será a ferramenta fundamental do Conselho Superior de Segurança do Ciberespaço para monitorizar a execução da estratégia, que terá uma longevidade de 5 anos. Ainda que todos os anos possa ser adequada às evoluções que a própria sociedade verificar", explica Gameiro Marques. Em termos de timeline, serão recebidos até 7 de maio todos os contributos para a ENSC, sendo então elaborado o documento final que será aprovado a 16 de maio pelo Conselho Superior de Segurança do Ciberespaço. Será depois enviado à tutela, iniciando-se assim o respetivo processo legislativo.

COOPERAÇÃO E PARTILHA SÃO CRÍTICAS

No debate que se seguiu, que contou com a intervenção de Pedro Veiga, coordenador do CNCS (que apresentou a sua demissão do cargo a 5 de maio), detalharam-se algumas as alterações que foram introduzidas na ENSC 2.0, a partir das debilidades detetadas com a aplicação da primeira versão. Como passar a abranger as autarquias e as regiões autónomas, que operam infraestruturas essenciais. "Agora, temos vindo a assinar protocolos com autarquias, o que nem sempre é fácil", destaca. Lisboa foi a primeira a assinar um protocolo.

Acresce que a ENSC, publicada antes da Diretiva de Bruxelas ser aprovada, tinha determinações a seguir. "Percebemos logo que precisávamos de caminhar na direção da Diretiva e começámos a dar especial interesse em protocolar a colaboração com entidades que considerávamos críticas", refere Pedro Veiga. Nomeadamente com os portos, entidades reguladoras dos setores dos serviços essenciais definidos na Diretiva e com grandes empresas, como a ANA, REN, EDP e Galp.

"Tentámos capitalizar as lições aprendidas da versão anterior. Não havia foco nas estruturas de informação críticas para Portugal", acrescenta Gameiro Marques. Assim, a nova versão teve um processo de desenvolvimento diferente

Rogério Carapuça e Gameiro Marques têm como objetivo reforçar a cooperação e as parcerias do CNCS e as empresas das TIC e Media

e mais inclusivo. A nova estratégia tem que ser "security by design e by default", com responsabilização e comunicação.

É ainda dado muito enfâse à cooperação com outras entidades, nomeadamente na rede CSIRT. "Vamos incentivar as entidades a cooperar porque a partilha de informação é fundamental nesta área", acrescenta Pedro Veiga, que destaca ainda a capacitação de pessoas e empresas para o digital e o tema da cibersegurança como outros desafios, onde se espera contar com o apoio da sociedade e de associações como a APDC. "Estamos disponíveis para parcerias", garantiu.

É que, como mostra o mais recente relatório da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) – que se vai transformar brevemente numa agência de cibersegurança, com o papel de ajudar os estados-membros, as instituições e as empresas a lidarem com ciberataques – as grandes tendências são de uma cada vez maior complexidade dos ataques cibernéticos e a existência de uma verdadeira indústria de ataques informáticos. E não é só dos criminosos que vêm as ameaças. Muitas vezes, resultam dos próprios funcionários das organizações, que se esquecem de adotar as necessárias medidas de prevenção.•

Patrocinadores Silver

Patrocinadores Bronze

AXIANS CGI CISCO DELOITTE DXC TECHNOLOGY FUJITSU GFI GOOGLE
HP HPE IBM MICROSOFT NOVABASE PAYPAL RANDSTAD SAS

Parceiros

JLM & ASSOCIADOS NOSSA
VdA VIATECLA