MeetOn "Cibersegurança"

CONCLUSÕES

27 de outubro de 2022

*A APDSI organizou a 27 de outubro de 2022 um **debate sobre o futuro das regulações de cibersegurança na Europa e em Portugal**, numa altura em que se impõe a necessidade de uma maior regulação nos setores, produtos e serviços, procurando mitigar as lacunas que ainda sentimos todos os dias em matéria de cibersegurança.*

*Este encontro online contou com a participação de **António Gameiro Marques**, Diretor-Geral do Gabinete Nacional de Segurança, de **Nuno Teodoro**, Cyber Security and Privacy Officer (CSPO) da Huawei, de **Pedro Machado**, Data Protection Officer (DPO) da AGEAS, de **Augusto Fragoso**, Diretor-Geral de Informação e Inovação da ANACOM, e de **António Bacalhau**, Head of Cybersecurity & Portugal Security Lead na Accenture.*

O debate foi moderado e coordenado por Miguel Brito Campos, Vogal da Direção da APDSI, que trouxe para início da sessão temas como a NIS 2.0 - Diretiva de Network and Information Security, Cyber Resilience Act (CRA) e Digital Operational Resilience Act (DORA) estão na ordem do dia para a maioria das Organizações.

Nuno Teodoro, ***Cyber Security and Privacy Officer*** **(CSPO) da Huawei, introduz o debate observando que a digitalização na nossa vida quotidiana é cada vez mais uma realidade**, o que obriga a uma relevância e a cuidados também cada vez maiores em matéria de cibersegurança.

A Europa está a munir-se de um conjunto de estratégias que vão passar a fazer parte do nosso dia-a-dia porque são transversais a vários setores. Por um lado, **Portugal sabe que vai haver crescentes requisitos em matéria de cibersegurança e ameaças muito fortes** na área dos fornecedores de serviços e de equipamentos, mas também na banca. Por outro, e de uma perspetiva europeia, é **importante que consigamos elevar o nosso nível de maturidade e fazer frente às principais ameaças.**

De recordar que a soberania tecnológica assenta em três pilares fundamentais: poder de computação; controlo sobre os nossos dados; e conetividade segura.

A NIS 2.0 procura um grupo para gerir incidentes de larga escala na União Europeia com um papel mais ativo e relevante na comunicação e na cooperação, aspetos cada vez mais transversais para dar resposta às problemáticas que a maior parte das organizações vive e que todos os dias são notícia.

“O que eu acho é que as organizações nacionais talvez não estejam preparadas para esta regulação e para as diretivas que aí vêm. Acho que temos de reunir várias visões e perceber se estamos a caminhar no sentido certo enquanto Estado Membro e a competir com a realidade das ciberameaças e aumento dos dispositivos IOT”, resume Nuno Teodoro.

Pedro Machado, ***Data Protection Officer*** **(DPO) da AGEAS destaca dois instrumentos, o DORA e o CRA como dois paradigmas a que faz sentido prestar atenção**. O DORA decorre da estratégia para o digital da Europa e tem um âmbito específico para entidades – não tem um target transversal no mercado. Tanto é focado no setor financeiro, como na banca, agências de rating, mercados, seguros, prestadores de IT ou

em qualquer outro setor de investimento, Já “entidade financeira” abarca um contexto mais completo.

O DORA apresenta-se em cinco pilares:

- Está focado na gestão de risco para TIC (*governance* e registo de atividades);
- Obriga à comunicação de incidentes TIC, pelo que vamos assistir a uma normalização de incidentes e às suas respetivas obrigações de notificação com a produção de relatórios anónimos dentro da União Europeia;
- Obrigações de testes exaustivos e técnicos de resiliência a cada três anos por entidades independentes que têm de ser disponibilizados aos setores de banca, seguros e fundos de pensões;
- Gestão de risco focada em terceiros (prestadores de serviços), nomeadamente através da definição de estratégias e uma nova revisão contratual;
- Partilha de informação ao nível da *intelligence* numa lógica de prevenção de ameaças e gestão de vulnerabilidades.

Já o CRA tem o seu foco nos produtos e visa evitar que se propaguem os ciberataques em hardware, software e tudo o que faz parte dos dispositivos em rede. A antevisão deste tipo de ciberataques prevê um esquema de classificação que os classifica como mais ou menos críticos.

Esta obrigatoriedade de haver testes regulares aos fabricantes de automóveis, por exemplo, vai constituir um enorme desafio, sobretudo para peças e outros dispositivos que vêm de fora do espaço da União Europeia: “estamos a caminhar no sentido certo, no entanto, não podemos ignorar a importância de uma correta fiscalização destas matérias. No meu entender existe aqui um desafio grande ao nível da consciencialização do cumprimento**. O mercado parece só corresponder com um grande regime sancionatório. Estamos a esquecer-nos dos valores de uma Europa que deveríamos estar a construir”, lamenta Pedro Machado.**

Augusto Fragoso, Diretor-Geral de Informação e Inovação da ANACOM, entende que neste contexto regulatório é cada vez mais difícil termos uma atuação eficiente dada a escala dos cenários onde se desenvolve o risco, a transversalidade sectorial desses cenários e a abrangência dos impactos, muitas vezes transfronteiriços. A natureza da própria formação europeia leva a que as respostas, ao nível dos remédios e ao nível da produção de melhor regulamentação demorem muito tempo desde que se observa um evento no mercado e a altura em que aparece um mecanismo habilitante para responder a essa situação. Os eventos de risco verificam-se, concretizam-se e modificam-se em poucos meses e a UE pode demorar anos a elaborar uma resposta. “Se não mudarmos a eficiência destes mecanismos de resposta ao nível europeu e ao nível nacional, para atacarmos (a probabilidade de ocorrência do risco) o quanto antes, temos de repensar toda a forma como nos desenvolvemos neste campo”.

Nos países menos burocráticos, as respostas podem surgir mais depressa, o que é visto como positivo dada a crescente interdependência e transversalidade de qualquer ameaça no domínio da cibersegurança. Hoje em dia é difícil que existam eventos que não afetem vários mercados e setores em simultâneo, exigindo uma resposta “cada vez mais capaz do ponto de vista da colaboração”.

Em Portugal as entidades envolvidas numa estrutura de resposta neste contexto (cybersegurança e defesa do cyberespaço), quer no domínio da governança nacional quer no domínio técnico, são sempre diversificadas e em número significativo, mas nem sempre a relação entre elas se baseia nos mecanismos de cooperação e articulação mais eficientes, objetivando uma oportunidade de melhoria que, espacialmente no contexto desses mecanismos, deve ser continua

Outro desafio que Portugal tem pela frente tem a ver com a capacitação de profissionais com as competências adequadas em matéria de cibersegurança: “há uma grande dificuldade em contratar competências, e, convenhamos, essa dificuldade não creio que seja eliminada no futuro, antes pelo contrário. Daí que, para podermos enfrentar esse facto, teremos que fazer um uso muitíssimo mais eficiente de mecanismos de

colaboração, de troca de experiências e de partilha de competências e, naturalmente, da tecnologia, nomeadamente com o aumento da utilização das capacidade de automação e de inteligência artificial.

A segurança *by design* deveria fazer parte, cada vez mais, da estratégia de desenvolvimento de produtos e serviços , trazendo-a para os níveis mais baixos de desenvolvimento (IRL – Innovation Rediness Level), assegurando nomeadamente a certificação a fim de constituir uma plataforma de confiança e conformidade com os níveis adequados à natureza do risco em cada momento.

Além do universo ciber digital, a curto prazo teremos de prestar muita atenção às infraestruturas físicas e à sua segurança efetiva, como no caso dos cabos submarinos, por exemplo. “Estamos a passar por uma fase em que, com uma guerra em progresso, se levantam questões sobre estas importantes infraestruturas”, alerta Augusto Fragoso.

António Gameiro Marques, Diretor-Geral do Gabinete Nacional de Segurança, afirma que todos têm razões para estar preocupados, mas acredita ser necessária alguma empatia para com quem tem de assegurar a segurança do ciberespaço – que inclui a cibersegurança, a ciberdefesa, cooperação e capacitação, investigação, desenvolvimento e formação neste domínio.

De salientar que na semana passada foi aprovada a estratégia nacional de **ciberdefesa que tem por objetivo defender o país “no e” através do ciberespaço**. Neste momento está a decorrer o processo de revisão da nova estratégia Nacional de Segurança do Ciberespaço, que tem de estar publicada até ao final de junho de 2023. Esta estratégia vai estar condicionada e alinhada pela Diretiva NIS 2.0 – Network and Information Systems Security 2.0) (praticamente fechado nas instituições europeias) e tinha como prazo de incorporação nos estados-membros até 21 meses. Todavia, este período poderá ser encurtado para metade (11 meses) “com implicações bastante significativas” no volume das sanções a aplicar. Neste tema **a Europa vai passar a ter execução coerciva: “quem não cumprir com um conjunto mínimo de requisitos é sancionado e este quadro de sanções destina-se mesmo ao top management das organizações”.**

A cibersegurança está no momento presente na base da gestão de risco. Por isso, exige supervisão antes dos eventos acontecerem, o que requer recursos humanos que não abundam no Estado, e que obrigam a um alargamento de uma forma muito significativa dos negócios das empresas.

A NIS 2.0 contempla áreas que até aqui ainda não eram vistas como potenciais alvos de ciberataques, como as águas residuais, por exemplo, e não apenas a água potável como acontecia até aqui. “Um ataque pode ter um impacto brutal num afluente e numa cidade ou vila”, diz António Gameiro Marques.

Neste contexto, os prestadores de serviços de redes de dados têm de ser ainda mais confiáveis. Os fornecedores de serviços públicos de redes eletrónicas - a ANACOM e o CNCS - estão “condenados a entenderem-se” mas a NIS 2.0, com a DORA e a CRA acima referidas, trazem tantas novidades que podem tornar o panorama regulatório complexo (entidades como a Administração Pública e o retalho normalmente são avessas à regulação) e há o receio da comunidade científica que o mesmo possa vir a condicionar a investigação em áreas estratégicas para a União Europeia, se tal não for acautelado. Portugal criou o conceito de Zonas Livres Tecnológicas (ZLTs) que visam precisamente fomentar a I&D&I com níveis de regulação mínimos.

António Bacalhau, ***Head of Cybersecurity | Portugal Security Lead*** **na Accenture, já tem o mapa regulatório para todas as entidades porque existe uma pressão regulatória muito grande sobre a segurança, tanto que o contexto regulamentar europeu e americano está a tornar-se cada vez mais complexo** (só no último ano houve mais de cinco mil alterações regulamentares”.

No entanto, como implementar o DORA para podermos ver o risco de forma integrada? “Considerando os riscos operacionais e tecnológicos de uma organização de forma integrada porque os pontos a implementar são tantos e têm uma exigência no setor financeiro tão grande, que temos de ter uma entrega interativa convergindo o risco do negócio com o tecnológico”, explica António Bacalhau, que não esquece que para tudo isto ser realidade é preciso talento e um ecossistema que ajude a cumprir os termos

regulatórios, mas também a sua operacionalização. “O que temos feito é trabalhar estas *frameworks* para melhor se adaptarem aos nossos clientes, independentemente da regulação necessária”, descreve.

Perguntas e respostas

Estão as Organizações públicas e privadas em Portugal preparadas para estas novas realidades? Os dispositivos IOT médicos, ou de sinalização que, normalmente, estão conectados, sem grande capacidade de processamento, podem ser alvo de ataques que impactam o seu desempenho. Como vamos lidar com estes potenciais alvos de caos?

António Gameiro Marques diz que será o 5G que vai ter essa capacidade de endereçamento direto, seja num automóvel ou num gigantesco navio, e, portanto, a tendência vai ser para que esses dispositivos sejam uma porta de entrada para ciberataques. Todavia, por via da regulação, está em curso um processo de desenvolvimento de esquemas de certificação que vai fazer com que nós, clientes (cidadãos da EU), quando adquirimos dispositivos dessa natureza, possamos ver uma etiqueta indicadora da resiliência desse dispositivo a potenciais ciberataques. Assim, surgem regras de produção e comercialização desses produtos. Mais uma vez, quem vier de fora da União Europeia sem essa certificação, vai ter coimas bastante significativas. Outra preocupação é a segurança com os nossos dados que pode comprometer o que é essencial em democracia: a nossa liberdade enquanto cidadãos.

Augusto Fragoso é da opinião que a certificação (*security by design*) vai ajudar, mas o *IoT ware* ou *malware* estará muito presente nas nossas vidas. “Os nossos dados estão nas mãos dos fabricantes, mais do que na posse de alguns decisores de políticas públicas que talvez até necessitassem mais deles”, considera, enquanto antecipa que as muitas camadas de dados que o IoT gera, podem vir a ser um problema de ciberdefesa nacional.

Nuno Teodoro também partilha da opinião que o “5G vai potenciar o IoT”. A título de exemplo, é estimado que em 2025 existam mais de 150 mil ligações de dispositivos de

IoT por minuto. É uma área que vai ter muitos milhões de investimento associado, mas “tudo o que é possível de ser conectado, é possível de ser atacado”. Todas estas reflexões vão embater numa questão de segurança nacional porque a população vai estar totalmente ligada, por isso, este é um tema que vai crescer em termos de relevância porque **“terão de ser tomadas medidas mais estruturantes na proteção do ecossistema”.**

No caso das grandes organizações, existe sempre a dependência de uma entidade parceira. Os ecossistemas são apoiados por entidades externas que também vão ter um caminho a percorrer para fazer face às tentativas de ataques com o objetivo de afetar esse ecossistema e que vão ser cada vez mais relevantes. Será necessária uma “capacidade de implementação e verificação” que, à data de hoje, “não temos”, observa Nuno Teodoro.

Pedro Machado, refere que ao falarmos de ciberataques, na maior parte das vezes associamo-los a ataques de *phishing*, mas esquecemo-nos que os mais complexos ataques têm origem em vulnerabilidades antigas. “Grande parte dos incidentes ao nível mundial tem origem em serviços mal configurados e que são, posteriormente, explorados. Há uma falta de consciência de risco entre perceber as oportunidades e estar consciente dos perigos que elas acarretam”, alerta.

Por outro lado, **Pedro Machado salienta que há uma “falta de harmonização de competências logo desde tenra idade”, e sugere que a formação para a programação e cibersegurança tem de passar a fazer parte dos níveis mais básicos de educação**, mas também num estender de ensinamentos a toda a população.

António Bacalhau acrescenta que no ensino, tem de começar a dar-se formação em como usar a tecnologia em benefício da sociedade de uma forma segura. O 5G pode inundar o mundo de equipamentos que vão ser usados por toda a sociedade e esta transformação digital não será travada pela regulamentação.

A questão que, entretanto, as organizações terão de colocar internamente é: estando eu a ser atacado se vou conseguir prestar serviço aos clientes? A resposta tem de ser “sim”, mas para isso tem que se atingir um estado de maturidade muito elevado.

“Tecnologias emergentes são uma oportunidade, mas tem de haver literacia digital para todas as camadas da população”, acrescenta, também, António Bacalhau.

Como é gerida a cadeia de comando até ao CEO e o que deve ser transmitido às entidades em caso de ataque?

Pedro Machado alerta que este é um dos principais problemas da sociedade: uma má *governance*. Em caso de alerta tem de se garantir a independências das funções do DPO, que dá pareceres não vinculativos e não deve acumular funções dentro da organização que possam conflituar: não pode fiscalizar, processar e avaliar.

O procedimento de resposta em caso de ciberameaça tem de envolver uma equipa de crise e um procedimento de reação: quem faz o quê, que circuitos vamos ter de percorrer, onde nos voltamos a encontrar, quem fala à comunicação social e que mensagem é passada. **“O *rules and responsabilities* tem de estar claro”,** sublinha.

Augusto Fragoso é da opinião que temos problemas sérios ao nível da governança. É reconhecido o peso inquestionável da informação na constituição de valor económico e de desenvolvimento dos diversos mercados, e das soberanias, “mas não a valorizamos de facto, nem lhe atribuímos tangibilidade suficiente para que ela possa ser entendida na sua total expressão por economistas, gestores e governantes”.

Na realidade, quando falamos de criação de conhecimento e sensibilização para este facto fundamental no suporte dos mercados presentes e futuros, não podemos pensar apenas em formar e sensibilizar as gerações futuras, endereçando agora, apenas, as crianças e os jovens (porque eles apenas exercerão posições de decisão e influência num futuro ainda longínquo e incompatível com a necessidade de ação imediata), temos de levar esse conhecimento, essa formação, essa sensibilização, às posições de topo que hoje decidem e influenciam, quer no âmbito governamental, quer no político, quer ainda no operacional – público e privado.Os órgãos de Governança têm que elevar o entendimento da criticidade do factor segurança em geral, cyber segurança em particular e sustentabilidade dos modelos de gestão, operando-o no dia a dia com a importância estratégica que de facto têm. Note-se que ainda não há uma verdadeira cultura e uma incorporação no nosso pensamento diário desta questão da

cibersegurança. “Enquanto assim for, os resultados não são os que desejamos e os nossos governantes continuarão a a não investir no sítio certo ou de acordo com o valor real que a dimensão informação tem na sociedade atual.”, resume Augusto Fragoso.

Nuno Teodoro, finaliza enfatizando que temos uma baixa maturidade ao nível da cibersegurança: “as organizações não estão a fazer o básico. Os ataques que temos tido são com base em vulnerabilidades que existem há anos”.

Cooperação e resiliência são, no fim do dia, as palavras e ações fundamentais para fazerem face às ameaças cada vez mais complexas e com maior impacto nas sociedades.

SOBRE A APDSI

Criada em 2001, a Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI) tem por objetivo a promoção e desenvolvimento da transformação e inclusão digital em Portugal, reunindo com este interesse comum profissionais, académicos, empresas, organismos públicos e cidadãos em geral.

Na linha destes propósitos a APDSI tem vindo a desenvolver diversas atividades em torno de causas tecnológicas e societais, que se traduzem num conjunto de eventos, recomendações e estudos realizados por grupos de trabalho multidisciplinares em diversas áreas de intervenção, como a Segurança e Privacidade, a Ética no Digital, os Serviços Públicos Digitais, a Saúde, a Cidadania e Inovação Social, o Território Inteligente, as Tecnologias de Inteligência Digital, a Política Digital e Governança, os Futuros da Sociedade da Informação, as Competências digitais e o Ambiente e Energia.

Em todos estes trabalhos a APDSI procura identificar as tendências de evolução e também as interações entre as tecnologias e outras dimensões sociais e económicas, contribuindo com uma visão mais aberta para a discussão e tendo como meta a eficaz perceção e implementação destes conceitos na Sociedade Portuguesa. A APDSI tem o Estatuto de Utilidade Pública e foi em 2008 reconhecida como ONGD.

ASSOCIE-SE

URL | www.apdsi.pt

email | secretariado@apdsi.pt

APDSI

ASSOCIAÇÃO
PARA A PROMOÇÃO E DESENVOLVIMENTO
DA SOCIEDADE DA INFORMAÇÃO

Associação de Utilidade Pública

ONG – Organização Não Governamental

Rua Alexandre Cabral, 2C – Loja A
1600-803 Lisboa – Portugal
URL: www.apdsi.pt

Tel.: (+351) 217 510 762
Fax: (+351) 217 570 516
E-mail: secretariado@apdsi.pt

Apoio

FCT Fundação para a Ciência e a Tecnologia

Patrocinadores Globais da APDSI

Platina

accenture aws Google

Ouro

devoteam INCM Meta