Os impactos da Diretiva NIS2 em Portugal

Uma iniciativa

APDSI

Com a participação dos Associados Colectivos

Accenture Portugal

Art Resilia

AXIANS Portugal

CyberX

Devoteam Cyber Trust

DXC Portugal

Ethiack

Sincronideia

Introdução

Rumo à Conformidade com a Diretiva NIS2 em Portugal

É com grande satisfação que a Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) apresenta este *whitepaper*, fruto da colaboração e conhecimento especializado dos nossos associados coletivos. Através deste documento, buscamos fornecer uma visão abrangente sobre a Diretiva NIS2 e seus potenciais impactos no contexto empresarial português.

O Enquadramento da NIS2 em Portugal: No início deste ano, a Diretiva NIS2 entrou em vigor, apresentando-se como um marco regulatório essencial para a cibersegurança no espaço europeu. No entanto, em território nacional, a transposição desta diretiva para o ordenamento jurídico português ainda está em curso, com o prazo limite estabelecido para 17 de outubro de 2024. Reconhecemos a urgência e importância de analisar as implicações da NIS2 para o tecido empresarial português.

A Contribuição Única dos Nossos Associados Coletivos: Este documento é resultado do esforço conjunto de diversas empresas associadas à AP2SI, cada uma com sua experiência única em segurança da informação. A diversidade das áreas de atuação dos nossos associados coletivos enriqueceu esta compilação, permitindo-nos oferecer diversas visões sobre como a NIS2 pode influenciar as operações empresariais em Portugal.

Estrutura do Documento: Nas próximas páginas, cada um dos nosso associados apresenta análises comparativas da NIS2 em relação à sua antecessora, destacando as principais mudanças percecionadas. São também exploradas áreas específicas da NIS2 que podem ter um impacto significativo nas operações empresariais em Portugal, considerando a singularidade do nosso tecido empresarial.

São também abordadas as adaptações necessárias e os desafios antecipados que as empresas portuguesas podem enfrentar durante os processos de implementação para alcançar a conformidade. Por fim, são resumidas as principais conclusões e recomendações de cada organização participante.

Agradecemos aos nossos associados coletivos que colaboraram nesta iniciativa pelo compromisso em partilhar conhecimento para o benefício coletivo. Este *whitepaper* reflete o espírito de cooperação da AP2SI e espera ser uma ferramenta útil para as empresas portuguesas no caminho rumo à conformidade com a Diretiva NIS2.

Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
https://ap2si.org

Entidades Participantes

Introdução

A Accenture é uma equipa global com mais de 700 mil colaboradores em todo o mundo, que presta serviços por 49 países e que fornecem serviços de consultoria em diversas áreas incluindo gestão, tecnologia e estratégia. No âmbito do presente *whitepaper* damos especial relevo aos serviços de cibersegurança de última geração para proteção end-to-end, sustentados por mais de 16 mil profissionais dedicados e com um amplo conhecimento sobre cada indústria, e que levaram a que a Accenture fosse nomeada como líder entre os provedores globais de cibersegurança.

Com base neste conhecimento profundo sobre a cibersegurança, analisamos no presente *whitepaper* os impactos específicos da Diretiva NIS2 (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho) no tecido empresarial português.

Resumo

A Diretiva NIS2 visa substituir a Diretiva NIS que tinha por objetivo desenvolver as capacidades de cibersegurança em toda a União Europeia. Esta nova diretiva introduz diferenças relevantes em quatro aspetos chave:

(1) estratégia nacional e europeia de cibersegurança;
(2) âmbito de aplicação da norma;
(3) lista de medidas de gestão do risco de cibersegurança;
(4) supervisão e execução.

Face a estas alterações, e sendo o novo conjunto de requisitos de segurança muito mais concreto, a diretiva encontra-se agora mais próxima das melhores práticas de segurança, exigindo a que as organizações que atuam em setores críticos implementem uma estratégia de cibersegurança que permita garantir e demonstrar conformidade com a mesma.

Compreensão da NIS2

A Diretiva NIS2 (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho) visa substituir a Diretiva NIS (Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho) que tinha por objetivo desenvolver as capacidades de cibersegurança em toda a União, atenuar as ameaças aos sistemas de rede e informação utilizados para prestar serviços essenciais em setores-chave e garantir a continuidade de tais serviços em face de incidentes, contribuindo assim para a segurança da União e para o eficaz funcionamento da sua economia e sociedade. Contudo e embora desde a entrada em vigor da Diretiva NIS tenham sido alcançados progressos significativos no sentido de aumentar a ciber-resiliência, a sua implementação provou-se difícil, resultando em elevadas divergências na sua aplicação pelos Estados-Membros. Estes fatores aliados ao surgimento de novas ameaças levaram à nova Diretiva NIS2.

Analisando esta nova diretiva, é possível destacar diferenças relevantes em quatro grandes aspetos: (1) estratégia nacional e europeia de cibersegurança; (2) âmbito de aplicação da norma; (3) lista de medidas de gestão do risco de cibersegurança; (4) supervisão e execução. Posto isto, no presente *whitepaper* refletiremos apenas sobre os últimos três, dado somente estes terem impacto (direto) sobre o tecido empresarial português.

Posto isto, é possível desde logo notar que, enquanto a anterior diretiva tinha como âmbito de aplicação operadores de serviços essenciais e prestadores de serviços digitais, a nova apenas diz respeito a entidades que atuem em setores críticos (sendo que estas se segregam entre entidades essenciais e importantes). Esta diferença deve-se à integração deste setor, entre outros como crítico (a lista completa de setores agora considerados como críticos inclui: serviços postais e de estafeta, gestão de resíduos, produção, fabrico e distribuição de produtos químicos, produção, transformação e distribuição de produtos alimentares, alguns subsetores da indústria transformadora, prestadores de serviços digitais e investigação). São agora consideradas como entidades importantes qualquer organização que atue num setor crítico e, para além disto, a identificação dos operadores de serviços essenciais apresenta agora um conjunto de critérios muito mais objetivos e alargados de forma a potenciar um maior nível de conformidade entre os distintos estados-membros, contrastando com a anterior diretiva que deixava a cabo de cada estado-membro a identificação de entidades em âmbito. Entre estes critérios destacam-se a aplicabilidade a qualquer média empresa (ou maior) que preste

serviços críticos ou exerça atividade nestas áreas na União Europeia e a entidades de administração pública.

Por sua vez, a lista de medidas mínimas de gestão do risco de cibersegurança foi também alterada, encontrando-se estas agora definidas de forma muito mais concreta. Na constituição da nova lista encontram-se identificados como requisitos os seguintes aspetos:

- Políticas de análise dos riscos e de segurança dos sistemas de informação;
- Tratamento de incidentes;
- Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises;
- Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos;
- Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades;
- Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;
- Práticas básicas de ciber-higiene e formação em cibersegurança;
- Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem;
- Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos;
- Utilização de soluções de autenticação multifator ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, se for caso disso.

Mais ainda, a diretiva explicita ainda que a conformidade com estes fatores deverá ter em consideração todos os riscos inerentes à sua atividade, incluindo os que são derivados da sua cadeia logística (fornecedores e prestadores de serviço) e tendo em conta o input de avaliações coordenadas a realizar pelas entidades europeias relevantes.

Por último, a no que refere à componente de supervisão e execução, as grandes diferenças encontram-se no âmbito da extensão dos atuais poderes das autoridades de supervisão. Estas entidades passarão a possuir competências para realizar inspeções presenciais, auditorias de segurança (regulares ou ad-hoc), requisitar informação adicional e evidências. Aliada a esta lista de novas competências, encontra-se ainda um agravamento extremamente significativo do valor das coimas passíveis de ser aplicadas em caso de incumprimento. Estes valores poderão ir até 10 milhões de euros ou 2% do volume de negócios anual a nível mundial no caso das entidades essenciais e até 7 milhões de euros ou 1,4% do volume de negócios anual a nível mundial no caso de entidades importantes.

Adaptações Necessárias e Desafios Antecipados

Como resultado das alterações introduzidas, a diretiva ganha um novo nível de relevância no tecido empresarial português, obrigando todas as organizações que atuem em setores críticos a responder a um conjunto de novas necessidades e desafios.

Neste sentido, uma das implicações mais significativas é a necessidade de novas organizações prestarem atenção à sua conformidade com a diretiva, exigindo que seja feito um caminho significativo num mercado que possui ainda um baixo grau de maturidade relativamente ao tema da cibersegurança.

Porém, os desafios não se limitam apenas às novas organizações em âmbito. Também as empresas anteriormente abrangidas necessitam de garantir a conformidade com os novos requisitos de forma exímia, dadas as alterações à competência das autoridades de supervisão e ao aumento significante do valor das coimas em caso de inconformidade. Neste sentido, poderão tornar-se especialmente relevantes sistemas e entidades que certifiquem e demonstrem a conformidade para com os requisitos.

Face a estas alterações, e sendo o novo conjunto de requisitos de segurança muito mais concreto, a diretiva encontra-se agora mais próxima das

melhores práticas de segurança. Em virtude desta aproximação, torna-se agora crucial às organizações adaptarem um standard internacional de referência, que guie a estratégia de cibersegurança da organização, facilitando a demonstração de conformidade com a presente diretiva. De facto, a melhor resposta para a conformidade com os requisitos introduzidos na Diretiva NIS2 será uma forte aposta numa estratégia de cibersegurança holística, sustentada na gestão de risco e que tenha como objetivo a resiliência do negócio.

Conclusões e Recomendações

Em suma, as alterações introduzidas na Diretiva NIS2 conferem-lhe um novo patamar de relevância no panorama empresarial português, impondo às organizações que atuam em setores críticos o desafio de enfrentar uma série de novas necessidades e exigências. Face a estas mudanças, torna-se cada vez mais relevante a implementação de um standard internacional de referência, que guie a estratégia de cibersegurança da organização e que permita garantir e demonstrar conformidade com a diretiva, de forma a tornar o negócio resiliente e a evitar pesadas coimas.

Saiba mais sobre a Accenture Portugal em https://www.accenture.pt/.

Introdução

A Art Resilia é uma empresa focada e especializada na prestação de serviços de cibersegurança, segurança de informação e tecnologia. O portfólio de serviços tem como objetivo ajudar e impulsionar as empresas a endereçar riscos de cibersegurança de uma forma estrutural e holística. A abordagem técnica e teórica é tornar os processos, tecnologia e pessoas resilientes às ameaças digitais que são potenciais criadoras de disrupção de negócio nas organizações. Os serviços prestados são caracterizados em duas vertentes:

Ofensiva: Atividades que visam a realização de processos de auditoria especializada e monitorização digital por forma a identificar riscos, vulnerabilidades e vetores de ataque nas vertentes tecnológicas, pessoas e processos.

Defensiva: Tarefas de monitorização pró-ativa assentes em processos de deteção, mitigação, resposta e recuperação a eventos e incidentes de segurança. Serviços de consultoria que visam implementar ou avaliar a ciber resiliência nas organizações do ponto de vista processual.

Contexto

A NIS (Diretiva (UE) 2016/1148) foi lançada em 6 de Julho de 2016 e foi a primeira diretiva da União Europeia abrangente sobre cibersegurança. A diretiva visa garantir que os Estados Membros da união adotem medidas de segurança e resiliência comuns com foco na prevenção e resposta a incidentes / ameaças. Em Portugal, a NIS 1 foi transposta pela Lei n.º 46/2018.

A sucessora - NIS2 (Diretiva (UE) 2022/2555) - introduz uma série de alterações, melhorias e simplificação na ótica da gestão de riscos e tratamento de incidentes, alargando também a sua aplicabilidade a mais organizações.

NIS vs. NIS2: O que mudou?

A alteração mais relevante é o facto de que enquanto a NIS 1 apresenta recomendações e boas práticas, as principais disposições da NIS 2 são regulatórias, de implementação obrigatória, cujo incumprimento prevê severas sanções.

Os seguintes tópicos afiguram-se como as principais mudanças.

Alargamento do âmbito

A NIS2 adiciona ao âmbito da sua precedente, Serviços Digitais (p.e. Serviços de Data Center), Fabricantes de determinados produtos críticos, serviços postais e correios e Administração pública. Estes setores são classificados como "Setores altamente críticos" ou "Outros setores". Já as entidades podem ser "Essenciais" ou "Importantes" - estas classificações vão impactar o nível de supervisão e aplicação da Diretiva. Os critérios que definem quais as empresas que devem cumprir são mais detalhados e contemplam, p.e., o nº de funcionários e volume de negócio.

Requisitos de Segurança

Introdução de medidas fundamentais de cibersegurança que incluem análise de riscos, políticas de segurança, resposta a incidentes, gestão de crise e continuidade de negócio.

Colaboração

Criação da EU CyCLONe para coordenar a gestão de incidentes em grande escala na União Europeia.

Comunicação de Incidentes

Diretrizes mais claras para o processo e prazos de notificação de incidentes, definindo como obrigatória a notificação, às autoridades, num período de 24 horas após um incidente, bem como, fornecer uma atualização mensal.

Sanções mais severas

Prevê sanções mais severas ao não cumprimento que podem chegar, no caso de organizações essenciais, até 2% da faturação anual ou pelo menos 10 milhões de euros, prevalecendo o montante mais elevado.

Responsabilidade dos Órgãos de Gestão

A NIS2 visa responsabilizar a gestão das organizações pela implementação e cumprimento das medidas de segurança.

Quais os desafios das empresas em conseguir a conformidade com a NIS2?

De entre os diversos desafios que as organizações enfrentam, neste artigo considera-se relevante evidenciar a importância da segurança na cadeia de

fornecimento (supply chain), sendo este requisito um dos controlos adicionais que as organizações abrangidas têm de implementar e gerir. Significa isto que, na prática, existe uma aplicação indireta em todas as empresas que são fornecedoras de serviços e produtos aplicados nas organizações críticas e essenciais. Refere-se como aplicação indireta pois será natural a exigência acrescida das organizações a toda a sua cadeia de fornecimento.

Existe uma tendência crescente, por parte dos atores maliciosos, em focar os seus ataques na cadeia de fornecimento. Isto deve-se ao facto de esta, diversas vezes, abranger todas as atividades e processos das organizações, desde a criação, produção e entrega de produto ou serviço, e é, normalmente, composta por vários elos interconectados. Esta complexidade oferece diversas oportunidades de exploração por parte de atores maliciosos. É assim crucial, e ao mesmo tempo um tremendo desafio, implementar medidas de mitigação dos riscos inerentes à cadeia de fornecimento, sejam elas tecnológicas, processuais ou contratuais.

Um ataque por meio da cadeia de fornecimento, normalmente acontece quando o ator malicioso utilizando um vetor de ataque, como a exploração de uma vulnerabilidade de um software, produto ou sistema, ou comprometendo a infraestrutura do fornecedor, ou mesmo tirar partido de um utilizador comprometido, consegue privilégios que lhe permitem propagar o ataque entre as organizações, avançando pelos elos de ligação da cadeia de fornecimento. Essa abordagem possibilita que o atacante atravesse diferentes partes da cadeia, ampliando o seu alcance.

De notar que existe, por parte dos operadores de infraestrutura crítica e essencial, uma grande dependência de serviços terceirizados e daí advém a dificuldade de controlar a cadeia de fornecimento em profundidade.

Em suma, as dificuldades que as organizações enfrentam a gerir segurança na cadeia de fornecimento são:

- Falta de compreensão do risco real que representa a cadeia de fornecimento de serviços e produtos;
- Visibilidade limitada e em profundidade de toda a cadeia de fornecimento;
- Não saber ou ter falta de capacidade para endereçar a segurança dos fornecedores de forma eficaz;

Naturalmente que caberá a cada organização governar a gestão da segurança e risco na cadeia de fornecimento, no entanto há aspetos transversais e abordagens eficientes que podem ser tidas em conta aquando da implementação de políticas.

O primeiro aspeto trata-se de endereçar sobre quem, ou que equipas, recaem as responsabilidade de gerir a segurança na cadeia de fornecimento. Será recomendável que quanto maior for a organização mais premente é a necessidade de apontar um responsável direto. Com ou sem equipa dedicada, prevê-se como essencial esta figura para construir políticas adequadas aos processos de negócio, compreendendo as necessidades do mesmo, sobretudo compreendendo e gerindo o risco para cada processo.

O segundo aspeto é a compreensão em profundidade da cadeia de fornecimento. Embora a NIS 2 só refira fornecedores diretos nos seus requisitos, conhecer toda, ou grande parte, da cadeia, irá permitir endereçar mais riscos e, por consequência, implementar mais medidas e controlos para gerir esse risco.

Por último, como endereçar e o que exigir dos fornecedores que fazem parte da cadeia de fornecimento dos processos críticos de negócio? Este ponto deve estar corretamente definido nas políticas de segurança e pode ser partido em diversas categorias, dependendo do fornecedor e o risco que acarreta para os processos de negócio. Um método cada vez mais usado é a exigência de certificações de segurança, suportadas por implementações de sistemas de gestão de risco como a série ISO 27000. Outro método, é usar os próprios meios para conduzir diligências profundas aos processos e procedimentos com que o fornecedor aborda segurança de informação no seu serviço, produto e organização. Políticas mais exigentes podem requerer a execução de auditorias contratadas pelas próprias empresas com vista a avaliações de segurança especializadas e independentes.

Em suma, os operadores críticos e essenciais terão de compreender os riscos que os seus fornecedores lhes aportam, classificá-los de acordo com esses riscos, implementar medidas para controlar e monitorizar os mesmos e realizar as diligências necessárias para exigir os padrões de segurança adequados.

Quais as estratégias que podem ser utilizadas para atingir a conformidade?

Como estratégia à conformidade com a diretiva, identificamos uma que parece ser mais assertiva, optar pela implementação da ISO 27001:2022. Esta norma define uma framework que estabelece os requisitos para um Sistema de Gestão e Segurança da informação (SGSI) focado em gestão de risco. Considera-se que a correta implementação de um SGSI permite às empresas aproximarem-se da diretiva NIS2 na totalidade.

É possível estabelecer uma conexão direta de um dos artigos mais relevantes da diretiva, o Artigo 21º Medidas de gestão dos riscos de cibersegurança com o Anexo A da ISO 27001:2022, neste contexto, a norma pode ser utilizada como uma ferramenta eficaz para alcançar a conformidade. Além disso, existe também o Quadro Nacional de Referência de Cibersegurança que juntamente com o respetivo guia de implementação, proporciona outra alternativa para atingir a conformidade. Neste âmbito, as organizações poderão optar por qualquer uma destas frameworks, sendo que ao escolher a ISO 27001 inclui uma possibilidade de certificação, que pode ser benéfica não só no campo da conformidade, mas também, ao nível do negócio. Já no caso da adoção do Quadro Nacional, a finalidade não se concentra tanto na certificação, mas sim em enriquecer a implementação de medidas que fortalecem a postura de segurança e resiliência da empresa.

Conclusões e Recomendações

Neste artigo evidencia-se a grande expansão de requisitos e âmbito de aplicabilidade que a NIS2 tem, aumentando, portanto, o impacto nas organizações a operar em território nacional. Se, porventura, organizações de sectores críticos (ex.: infraestruturas críticas), já ao abrigo da anterior versão da NIS, deverão estar mais preparadas e próximas da conformidade - o que se traduz numa maior resiliência face às ameaças que enfrentam - existe agora um conjunto muito alargado de organizações que certamente terão um longo caminho a percorrer.

Uma das formas que nesta exposição se propõe é implementar um SGSI, por intermédio do referencial ISO 27001, que permite implementar na totalidade os controlos e requisitos que a NIS2 exige. Naturalmente, implementar o SGSI só por si não é suficiente, é necessário incluir as diretrizes específicas da NIS2 aquando da implementação dos controlos do referencial. Por exemplo, a inclusão no procedimento e políticas de resposta a incidentes dos canais de comunicação e protocolos com a rede europeia.

Evidenciou-se também a importância da segurança na cadeia de fornecimento, como requisito adicional da NIS2 face à NIS, só por si um tópico complexo de abordar pela grande interdependência que existe em operadores críticos e essenciais com serviços e produtos de fornecedores.

Saiba mais sobre a Art Resilia em https://www.artresilia.com/.

Introdução

A Axians é um parceiro de cibersegurança que tem por base as relações de confiança com os seus parceiros, fornecendo soluções de valor acrescentado que tratem os riscos de cibersegurança das organizações, possibilitando contribuir para uma estratégia de negócio concertada, diferenciada e de confiança numa economia digital em crescimento.

A nossa unidade de negócio Digital Trust, está focada única e exclusivamente nas matérias que circundam a cibersegurança, seja por intermédio de serviços estratégicos para estabelecer a estrutura de governança e os processos para a gestão das atividades das diversas iniciativas de uma organização, que incluam risco de cibersegurança, integrando-as no ciclo de vida do negócio, ou por intermédio de soluções tecnológicas que nos permitem integrar as melhores soluções de mercado, adotando as melhores práticas no desenho e implementação de arquiteturas tecnológicas.

Por fim, pretendemos que os nossos parceiros estejam efetivamente seguros no seu dia a dia, com o apoio da Axians e para isso, temos uma equipa de operações, focada na monitorização de eventos e no apoio à identificação de vulnerabilidades, por intermédio do nosso SOC de última geração.

Compreensão da NIS2

Se com a NIS1 o objetivo passava por garantir uma harmonização em todos os Estados-Membros da UE relativamente às capacidades dos membros no que toca à cibersegurança, já a NIS2 traz com ela medidas de controlo adicionais.

É agora estabelecida uma lista de sanções administrativas, incluindo coimas por incumprimento das obrigações em matéria de gestão dos riscos de cibersegurança e de comunicação de informações. Verifica-se igualmente a clara existência de uma mensagem por parte da EU relativamente ao reforço dos requisitos de segurança com uma lista de medidas específicas, incluindo o tratamento de incidentes, a gestão de crises, o tratamento e divulgação de vulnerabilidades, políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança, assim bem como a necessidade da existência de uma cultura base de higiene e formação em cibersegurança.

Conclui-se que a NIS2 traz com ela um claro reforço em matéria de medidas de implementação e controlo.

Adaptações Necessárias e Desafios Antecipados

Um dos maiores desafios nas organizações passa pela alteração cultural.

Verifica-se que ainda hoje muitas empresas do tecido empresarial português apresentam um nível de maturidade muito baixo, relativamente a matérias relacionadas com a segurança da informação. Erradamente muitas organizações entendem que em matéria de cibersegurança a tecnologia é dona e senhora da solução e nesse sentido enumeras organizações continuam a apostar e a delegar este tema como sendo exclusivamente tecnológico, o que é hoje claramente visto como um dos grandes erros estratégicos.

O desafio passa efetivamente pela mudança cultural e organizacional, e isso poderá ser feito através do desenvolvimento de um Programa de Segurança da Informação, que possa endereçar os 3 grandes pilares de um sistema de informação, Pessoas (por intermédio da formação e capacitação), Processos (pela adoção de práticas sistematizadas) e por fim utilizando a Tecnologia (como forma de suportar, os processos que serão operacionalizados por pessoas)

Conclusões e Recomendações

De acordo com a nossa visão a NIS2 deverá ser entendida como uma peça agregadora, um concentrador de conceitos e boas práticas em forma de diretriz, na medida em que são abordados na mesma alguns aspetos, que em conjunto e em harmonia, capacitam as organizações para os desafios e riscos da cibersegurança.

Desenvolver um plano de continuidade de negócio, com base na real identificação dos processos de negócio é claramente um dos pontos chave.

Quantas organizações efetivamente não têm a sua cadeia de valor devidamente identificada e detalhada, verificando se que muitas das vezes todos os processos estão efetivamente mapeados ?

Temas como a avaliação de risco, o modelo de governo de IT, funções e responsabilidades, passando pelos planos de resposta a incidentes, estão entre

alguns dos temas que devem ser devidamente endereçados.

A implementação da NIS2 deverá ser encarada como uma oportunidade para as organizações em geral, e aquelas cuja diretriz se aplica, na medida em que muitas das obrigações, remetem para a adoção de práticas essenciais, como forma de garantir a segurança da informação.

Saiba mais sobre a AXIANS Portugal em https://www.axians.pt/.

Introdução

A CyberX - The Ethical Hacking Services é uma empresa portuguesa especializada em auditorias de segurança em várias frentes, incluindo Testes de Intrusão (pentest), Análise de Código (SAST), Análise de Vulnerabilidades, Red Teaming, Campanhas de Phishing e Workshops. A nossa equipa, integrada por Ethical Hackers especializados e certificados a nível internacional, em sinergia com a gestão, dedica-se a assegurar a entrega de resultados com um grau de precisão e qualidade excecionais.

Com a sua expertise, a CyberX é um parceiro estratégico para organizações que buscam cumprir com as rigorosas exigências de segurança digital da NIS2. Suas soluções avançadas e workshops educativos não só protegem os ativos digitais, mas também promovem um ambiente digital mais seguro, alinhando-se perfeitamente com os objetivos da diretiva de fortalecer a segurança cibernética em toda a Europa.

Análise de NIS2 e Principais Mudanças

A Diretiva NIS2 é uma legislação da União Europeia que atualiza e substitui a Diretiva NIS original, com o objetivo de fortalecer a segurança cibernética em toda a UE. Esta nova diretiva amplia o âmbito de aplicação para incluir mais setores e tipos de entidades, estabelecendo requisitos mais rigorosos de segurança e de comunicação de incidentes.

As entidades são classificadas como "essenciais" ou "importantes", cada uma sujeita a diferentes níveis de supervisão e obrigações. A NIS2 também enfatiza a gestão do risco, a coordenação na gestão de crises de cibersegurança, e introduz coimas mais severas para garantir a conformidade. Ela traz consigo uma série de mudanças e desafios que podem ter um impacto substancial nas operações das empresas em Portugal, principalmente considerando as especificidades do tecido empresarial português. Alguns dos pontos chave são as seguintes.

<u>Ampliação do Âmbito de Aplicação</u>

A NIS2 expande o seu alcance para além dos operadores de infraestruturas críticas e prestadores de serviços essenciais, abrangendo agora novos setores. Essa expansão visa garantir uma maior proteção dos sistemas de informação e redes em setores cruciais para a sociedade, o que pode significar que mais empresas portuguesas estarão sujeitas a estas diretrizes.

A expansão do âmbito representa uma resposta adaptativa às mudanças rápidas e complexas no ambiente digital e de segurança cibernética. A decisão de alargar o escopo foi motivada por vários fatores:

- Digitalização Acelerada e Interconexão de Setores: Com o avanço tecnológico e a crescente digitalização, muitos setores tornaram-se altamente dependentes de infraestruturas de TIC. Isso aumentou o risco de ataques cibernéticos que podem ter um impacto significativo não apenas em uma única entidade, mas em toda a cadeia de valor ou mesmo no bem-estar social e econômico.
- Riscos Cibernéticos Ampliados: Os ataques cibernéticos estão se tornando mais sofisticados, frequentes e têm um alcance mais amplo. A necessidade de uma resposta mais abrangente e robusta a esses riscos tornou-se evidente. Incluir mais entidades e setores sob o guarda-chuva da NIS2 visa fortalecer a resiliência geral ao risco cibernético na UE.
- Inconsistências na Aplicação da NIS1: A implementação da NIS1 revelou limitações, como a falta de harmonização e a aplicação inconsistente entre os Estados-membros. Expandir o escopo e padronizar as exigências através da NIS2 visa abordar essas inconsistências e garantir um nível mais uniforme de segurança cibernética em toda a UE.
- Inclusão de Novos Setores e Entidades: Setores como redes sociais, administração pública e manufatura de certos produtos, como dispositivos médicos, foram incluídos para refletir sua importância crescente e seu papel na infraestrutura crítica. Esses setores, anteriormente excluídos ou marginalizados na NIS1, são agora reconhecidos como vitais para a segurança e economia nacionais e europeias.

Classificação de Entidades e Obrigações de Comunicação de Incidentes

A Diretiva NIS2 introduz mudanças significativas na classificação de entidades e nas obrigações de comunicação de incidentes, refletindo uma abordagem mais robusta e detalhada à segurança cibernética na União Europeia.

A NIS2 distingue entre "entidades essenciais" (EE) e "entidades importantes" (IE). As entidades essenciais incluem setores como energia, transporte, bancário, infraestrutura de mercado financeiro, saúde, água potável, águas residuais, infraestrutura digital (por exemplo, provedores de serviços de nuvem, data centers, DNS) e gestão de serviços de TIC. Já as entidades importantes abrangem setores como serviços postais e de courier, gestão de resíduos, produção de alimentos, e fabricação de uma gama de produtos, incluindo dispositivos médicos e equipamentos eletrônicos. A distinção entre essas categorias baseia-se na expectativa do impacto de um incidente, com as entidades essenciais sujeitas a uma supervisão proativa do governo, enquanto as entidades importantes só são verificadas após um incidente de cibersegurança.

A NIS2 introduz requisitos rigorosos para a notificação de incidentes cibernéticos. As entidades afetadas são obrigadas a informar as autoridades nacionais dentro de 24 horas após tomar conhecimento do incidente, seguido de um relatório formal em 72 horas com detalhes sobre a gravidade, impacto e indicadores de comprometimento conhecidos. Um relatório final deve ser submetido dentro de um mês após a notificação do incidente.

Gestão do Risco e Ampliação das Coimas

A NIS2 introduz uma abordagem de gestão do risco, incentivando as empresas a implementarem medidas concretas para gerir os riscos de cibersegurança. Este ponto é particularmente crítico para as empresas portuguesas, que precisarão adaptar suas práticas para atender a estes requisitos.

Além disso, a diretiva traz alterações nas coimas, que agora são mais elevadas e visam incentivar a conformidade e a adoção de medidas adequadas de segurança cibernética. Para "entidades essenciais", as multas máximas podem chegar a 10 milhões de euros ou 2% da faturação anual global, o que for maior. Para "entidades importantes", o máximo é de 7 milhões de euros ou 1,4% da faturação anual global, o que for maior.

Gestão de Crises de Cibersegurança

A NIS2 melhora a coordenação na gestão de crises de cibersegurança em larga escala a nível da União Europeia, o que implica uma necessidade de maior cooperação e comunicação entre as entidades. Para as empresas portuguesas, isso pode significar a necessidade de integrar sistemas de comunicação mais robustos e eficazes para lidar com tais crises, além de um CSIRT bem estruturado. Este cenário reflete a crescente importância da cibersegurança no contexto europeu e global, e a necessidade de as empresas estarem preparadas para enfrentar estas novas realidades.

Adaptações Necessárias e Desafios Antecipados

A adaptação das empresas aos requisitos da Diretiva NIS2 envolve uma série de passos estratégicos, tanto na atualização de sistemas e processos existentes quanto na introdução de novas práticas de segurança cibernética. Estas adaptações são essenciais para garantir a conformidade e melhorar a resiliência cibernética, como por exemplo:

- Revisão de Políticas de Segurança e Gestão de Riscos: As empresas precisam revisar e fortalecer suas políticas de segurança e procedimentos de gestão de riscos para atender aos requisitos mais rigorosos da NIS2.
- Melhoria da Infraestrutura de TI e Segurança de Rede: Implementação de tecnologias avançadas e soluções de segurança para proteger contra ameaças cibernéticas modernas. Em especial, a adoção de testes de intrusão, que, de acordo com a Norma 86, desempenham um papel importante para evitar os incidentes.
- Treinamento e Sensibilização em Segurança Cibernética: Realizar programas de treinamento regular para sensibilizar funcionários sobre práticas seguras e protocolos de resposta a incidentes.
- Atualização de Sistemas de Resposta a Incidentes: Estabelecer ou aprimorar sistemas de resposta a incidentes para

garantir relatórios rápidos e eficazes, conforme exigido pela NIS2.
- Auditorias e Avaliações de Conformidade: Realizar auditorias regulares e avaliações de conformidade para garantir que as medidas de segurança estejam alinhadas com os padrões da NIS2.
- Fortalecimento da Segurança na Cadeia de Suprimentos de TIC: Avaliar e mitigar riscos de segurança nas relações com fornecedores e na cadeia de suprimentos.

A longo prazo, a conformidade com a NIS2 não só aumentará a segurança cibernética, mas também pode oferecer vantagens competitivas e melhorias operacionais, entretanto ela também traz desafios significativos:

- Carga para Pequenas e Médias Empresas: Embora a diretiva exclua explicitamente pequenas e microempresas, a ampliação do escopo pode impor uma carga regulatória e financeira significativa para as PMEs que se enquadram na definição de entidades "essenciais" ou "importantes". Isso pode ser particularmente desafiador para o tecido empresarial português, onde as PMEs desempenham um papel crucial.
- Necessidade de Recursos e Especialização: A conformidade com a NIS2 exige investimentos significativos em tecnologia, pessoal e formação. Especialmente para novos setores incluídos, pode haver uma falta de conhecimento e experiência em lidar com os requisitos específicos de segurança cibernética. Dada a escassez atual de talentos na área no mundo e em Portugal mais ainda, acreditamos que este é um dos maiores desafios.
- Conformidade Contínua: Manter a conformidade contínua com a legislação em evolução requer esforços constantes e atualizações regulares das políticas e práticas de segurança.

Conclusões e Recomendações

A Diretiva NIS2 da União Europeia representa um avanço significativo na abordagem à segurança cibernética, refletindo as alterações no panorama de ameaças e o aumento da digitalização dos serviços. Com a expansão do seu âmbito, a NIS2 agora inclui uma gama mais vasta de setores, incluindo aqueles anteriormente menos considerados em termos de supervisão cibernética. Esta expansão, embora necessária para enfrentar ameaças cibernéticas contemporâneas, implica desafios adicionais devido a limitações de recursos e de conhecimento especializado.

A necessidade de auditorias regulares, testes de intrusão, e avaliações de conformidade enfatiza a importância de uma abordagem proativa à segurança cibernética. No entanto, elas podem ser onerosas e tecnicamente desafiantes, especialmente para organizações menores, realçando a necessidade de apoio e orientação contínuos por parte dos governos e autoridades reguladoras. Em resumo, enquanto a NIS2 impulsiona a segurança cibernética em toda a UE, a sua implementação bem-sucedida requer um equilíbrio cuidadoso entre a rigorosa conformidade e o suporte prático às empresas afetadas, assegurando assim que todos os setores possam atender aos novos padrões sem comprometer a sua operacionalidade ou competitividade.

Saiba mais sobre a CyberX em https://cyberx.pt/.

Introdução

A Integrity agora com o nome e a marca Devoteam Cyber Trust é uma empresa com mais de 15 anos de experiência em fornecer serviços de segurança ofensiva, consultoria e engenharia de cibersegurança para organizações de várias dimensões, no setor público e privado, com uma carteira diversificada de clientes nacionais e internacionais. A Devoteam Cyber Trust tem ampla gama de certificações e os nossos consultores especializados são altamente qualificados e certificados em padrões da indústria. O nosso enfoque é proporcionar uma ajuda especializada e experiente face às necessidades específicas de cada organização tendo como um dos objetivos no auxílio aos nossos clientes para atingir conformidade com a Diretiva NIS2.

Análise de NIS2 e Principais Mudanças

O surgimento da Diretiva(UE)2022/2555 (NIS2) trouxe um manifesto alargamento do seu âmbito de aplicação pelo que se entende que tanto o tecido empresarial português como a nível internacional, considerando também o âmbito da cadeia de abastecimento, terá um significativo impacto devido às suas exigências. O setor público já era abrangido não pela Diretiva NIS, mas pela sua transposição no ordenamento jurídico português. O lançamento da mais recente consulta pública "Projeto de Regulamento relativo à implementação do Regime Jurídico da Segurança no Ciberespaço nas entidades da Administração Pública", através do Aviso n.º 1517/2024 é manifestamente revelador da preocupação do legislador português nesta matéria. Prevemos que o impacto na Administração Pública seja elevado, ainda que a maior abrangência a novos setores adense as exigências a muitas empresas em Portugal, mesmo no setor privado.

A Diretiva NIS (EU 2016/1148), pioneira na regulamentação europeia de cibersegurança, desde a sua criação em 2016, promoveu e auxiliou a implementação de uma cultura de ciber-higiene nas organizações. Ao determinar a adoção de práticas de cibersegurança, a Diretiva impulsionou a adoção de processos, políticas e procedimentos que previnem e gerem riscos cibernéticos. As entidades reguladoras de cada Estado-Membro adaptaram-se às novas exigências trazidas para os respetivos ordenamentos jurídicos e as entidades abrangidas, tanto operadores de serviços essenciais como prestadores de serviços digitais, não só começaram a responder às suas obrigações, como ficaram mais conscientes da importância que a cibersegurança pode ter. Apesar da sua limitação em termos de abrangência, da sua aplicabilidade ter sido focada em prestadores de serviços essenciais e prestadores de serviços digitais, estes beneficiaram de diretrizes que estão em consonância com as melhores práticas de cibersegurança. Por outro lado, as restantes organizações ao tomarem conhecimento da Diretiva ficaram mais alertas para a importância da adoção de boas práticas de cibersegurança, assim como para a possibilidade de elas próprias poderem, eventualmente, vir a estar abrangidas, em legislação futura. A NIS é, sem dúvida, um marco importante e foi um ponto de partida no que à cibersegurança dos Estados-Membros diz respeito. Contudo, apresentou, do ponto de vista prático, algumas lacunas que tentam ser supridas com o surgimento da nova Diretiva. Os protagonistas e principais destinatários da NIS, os operadores de serviços essenciais e prestadores de serviços digitais, cedem o palco na NIS2 às entidades essenciais e entidades importantes. A NIS2 trouxe um claro alargamento dos setores abrangidos, críticos para a economia e sociedade, e um aumento dos poderes das autoridades nacionais de supervisão e promoção de grupos de intercâmbio de informação entre Estados-Membros. Na nova Diretiva, além dos setores bem conhecidos incluídos na NIS, tais como energia, mercados financeiros, transportes, prestadores de serviços digitais, setor bancário ou fornecimento e distribuição de água potável, outros setores foram acrescentados: telecomunicações, gestão de resíduos, alimentação, espaço, serviços postais e de estafeta, entre outros. Importa ainda referir que a Diretiva permite a possibilidade de cada Estado-Membro, aquando da transposição, poder alargar o seu âmbito de aplicabilidade.

No que toca à notificação de incidentes, há uma maior exigência de urgência na sua comunicação face à anterior Diretiva. É definido um prazo de 24 horas para o aviso de um incidente significativo e 72 horas para a comunicação de incidentes. Há uma clara preocupação com a divulgação coordenada de informação de vulnerabilidades e partilha de responsabilidade e de conhecimento. Criam-se meios

de divulgação coordenada de vulnerabilidades e é criada uma base de dados de vulnerabilidades europeia. O UE-CyCLONe (Rede de organizações de Coordenação de Cibercrises) surge com o objetivo de apoiar a gestão coordenada de incidentes e crises de cibersegurança em grande escala e garantir o intercâmbio de informações entre Estados-Membros e instituições da UE. Existe um reforço da responsabilização por parte da gestão no cumprimento das medidas de gestão de risco. Em caso de incumprimento, as autoridades devem aplicar coimas com o valor mínimo estipulado pela NIS2, o que não acontecia ao regime sancionatório anterior, onde a definição de valores mínimos era deixada ao livre-arbítrio de cada Estado - Membro. A disparidade de valores aplicados em cada Estado-Membro, aquando da transposição da NIS, veio justificar este balizamento de valores, que permite uma maior harmonização do regime sancionatório aplicável na União Europeia. A experiência da transposição da Diretiva NIS trouxe-nos o conhecimento que nos permite antecipar, em pé de igualdade ou até num espectro mais amplo, os desafios que irão surgir. As exigências legais mais aprimoradas e de fronteira mais alargadas, uma vez que abrange mais setores, irão ditar uma necessidade de maior investimento na proteção de redes e sistemas. Devido à sua natureza e por vezes por falta de recursos especializados estamos em crer que será a Administração Pública a mais permeável a enfrentar dificuldades na conformidade com a Diretiva NIS2.

Adaptações Necessárias e Desafios Antecipados

O impacto da NIS2 será variável não só de acordo com o espírito do legislador no momento da sua transposição, uma vez que tem discricionariedade para estender a mais sectores a obrigatoriedade de resposta à Diretiva, mas também de acordo com o setor. Prevê-se que na área da banca o impacto da NIS2 não seja tão expressivo, não só devido às exigências legais e regulamentares já existentes, mas também pelo surgimento do DORA (Regulamento (UE) 2022/2554), relativo à resiliência operacional digital do setor financeiro. Manifestamente, existem trâmites que apenas serão conhecidos no momento da sua transposição. Existe, porém, informação suficiente para poder antecipar aquilo que são as linhas orientadoras pelas quais a NIS2 dá continuidade com o seu surgimento. As empresas, independentemente do setor onde se enquadram e da sua dimensão, devem consciencializar-se que serão afetadas, ainda que na qualidade de elementos de cadeia de abastecimento, ou na qualidade de parte de um todo, pelas diretrizes que a Diretiva impõe. Posto isto, para além da discricionariedade legislativa, existem setores, ainda que não diretamente indicados na letra da lei, serão visados por esta.

Para adotar a NIS2 em organizações com algum tipo de sistema de gestão implementado é necessária uma abordagem holística, abrangendo tecnologia, pessoas e processos. Possíveis certificações existentes têm um âmbito de aplicabilidade definido, fronteiras que delimitam a sua aplicação. A NIS2 aplica-se, porém a toda a organização, de forma transversal, em todas as áreas de negócio que sejam consideradas críticas, e não apenas a um determinado âmbito de aplicabilidade definido em sede de implementações de sistemas de gestão já existentes. Posto isto, deve existir um esforço no sentido de cumprimento com todas as exigências normativas da Diretiva na organização alinhado com o todas as políticas, processos e procedimentos já implementados, sendo que existirão adaptações que são necessárias realizar. A forma e os prazos estabelecidos pela Diretiva no que toca a notificação de incidentes às autoridades competentes, por exemplo, deverão ser alinhados com o procedimento de gestão de incidentes, caso já se encontre estabelecido na organização. Deverá ser realizada uma atualização da avaliação de risco, considerando as ameaças cibernéticas e os cenários que sejam pertinentes à luz da NIS2. O plano de tratamento de risco deverá contemplar todas as medidas preventivas de deteção, resposta e recuperação exigidos. Inevitavelmente existirão pontos que deverão ser adaptados, e poderão existir outros que carecem de serem criados. Tanto Políticas como Procedimentos deverão ser revistos com especial atenção no que toca à área de proteção de dados, resposta a incidentes e continuidade de negócio. São inúmeras as ações a realizar, contudo, ressalvamos um ponto crucial: a cadeia de abastecimento. É, pois, relevante apelar a uma sensibilização para este tema sendo uma das mais significativas novidades. A NIS2 é uma oportunidade de melhoria, não só para empresas que ainda não estão sensibilizadas para as práticas gerais de

cibersegurança, mas também para aquelas que já iniciaram a sua jornada.

Conclusões e Recomendações

Responder a um novo normativo implica uma avaliação sobre o estado atual da arte, sobre aquilo que temos e aquilo que pretendemos alcançar. Com a adotação da NIS2 não será diferente. A resposta às suas exigências pode tornar-se desafiadora na medida em que exige a alocação de recursos tanto a nível de tempo, investimento financeiro e de profissionais especializadas. Outro dos desafios expectáveis é a própria resistência à mudança, que a NIS2 combate através de medidas como promoção da consciencialização e formação e a adoção de medidas sancionatórias cada vez mais pesadas. Perante estes desafios, não é demais reforçar a necessidade de uma abordagem proactiva por parte das organizações para que não só atinjam a sua conformidade regulatória, mas aumentar também a sua resiliência contra ameaças cibernéticas.

O surgimento da NIS2 é uma clara evolução e tudo indica que não ficamos por aqui. As exigências legais podem correr atrás da permanente atualização tecnológica, mas não se desvirtuam da sua relevância, em particular pela preocupação demonstrada pela harmonia da cadeia de abastecimento, mas acima de tudo pelo carácter preventivo que assume. Devemos antecipar, em uníssono, eventuais disrupções e a promoção de comunicação entre entidades permite prever com maior rapidez e eficácia potenciais ameaças. Ditam as melhores práticas e a dita a sabedoria popular que “a porta deve ser trancada” e que para isso não é frutífero aguardar pela consubstanciação de um determinado incidente. Prevenir é tão importante quanto a capacidade de garantir a reação e recuperação.

Uma mudança, ainda que para melhor, implica custos operacionais que poderão ser otimizados recorrendo a profissionais especializados, através de um olhar experiente e atento, atingindo não só a conformidade regulamentar, como também a competitividade no mercado e resiliência empresarial.

Saiba mais sobre a Devoteam Cyber Trust em https://www.integrity.pt/.

Introdução

Os serviços de cibersegurança da DXC ajudam as organizações a avaliar o risco e a abordar proactivamente todas as perspetivas da segurança: desde a ciber inteligência à conformidade com as mais recentes normas. Utilizamos metodologias comprovadas, automação inteligente e parceiros líderes do setor para adaptar as soluções de segurança às necessidades dos nossos clientes.

Com uma vasta oferta distribuída por quatro pilares: *Cyber Risk & Compliance*; *Infrastructure*, *App & Data Protection*; *Cyber Transformation & Operations* e *Digital Identity*, somos capazes de identificar, proteger, detetar, responder e recuperar as infraestruturas de TI dos nossos clientes.

A segurança é um pilar fundamental para a DXC. Incorporamos a resiliência cibernética nas operações e cultura de TI das organizações. Seja em migrações para a cloud, na proteção de dados adotando uma estratégia zero trust, ou na gestão de centros de operações de segurança, tratamos da segurança para que se possa concentrar no seu negócio.

A NIS2 (*Network and Information Security* 2, ou na versão portuguesa: SRI2 - Segurança das Redes e da Informação 2) representa uma oportunidade para que as organizações europeias se tornem mais resilientes às potenciais ameaças a que estão sujeitas ao operarem num mundo cada vez mais digital. Na DXC compreendemos os desafios que se colocam às empresas e sector público para que consigam cumprir com os objetivos que esta nova legislação irá trazer, bem como a forma mais abrangente de ultrapassar esses desafios e rapidamente atingir o nível de maturidade requerido por esta legislação.

Análise de NIS2 e Principais Mudanças

Objectivos

Após a publicação da diretiva NIS1 em julho de 2016, que viria a ser transposta para a Lei n.º 46/2018, verificaram-se algumas lacunas que necessitavam de ser endereçadas, em particular os sectores que foram deixados de fora nesta primeira versão e que se revelam como fundamentais para o normal funcionamento da sociedade, como seja por exemplo, o sector do retalho.

Tendo em conta as lacunas existentes na NIS1, foi então elaborada e publicada em janeiro do ano passado a NIS2 cujos objetivos passam por:

- Alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na UE;
- Melhoria das capacidades de cibersegurança a nível dos estados-membros;
- Maior cooperação e gestão dos riscos a nível da EU;
- Obrigações para as entidades essenciais e importantes de comunicarem incidentes com impacto significativo.

Para que se alcancem estes objetivos, foi necessário introduzir diversas alterações para suprir as lacunas existentes na anterior diretiva, como veremos de seguida.

Coimas

À semelhança do que aconteceu com o RGPD quando entrou em vigor em 2018, também a NIS2 traz uma significativa alteração face à anterior diretiva: as coimas. "*Num montante máximo não inferior a 10 000 000EUR, ou num montante máximo não inferior a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade essencial pertence, consoante o montante que for mais elevado*." [1] para aquelas entidades consideradas essenciais. Já as entidades importantes estão sujeitas a "*coimas num montante máximo não inferior a 7 000 000EUR ou num montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade importante pertence, consoante o montante que for mais elevado*." [1]

Apesar ser redutor olhar para a Diretiva apenas do ponto de vista das coimas, sendo que traz várias mudanças relativamente à anterior diretiva, é desde já importante realçar este ponto pois poderá ser o fator decisivo para a rápida adoção de medidas que

[1] Art. 34º 4. E 5. - Diretiva (UE) 2022/2555 Do Parlamento Europeu E Do Conselho De 14 De Dezembro De 2022

venham a tornar mais seguros ambos os sectores público e privado.

Entidades essenciais e importantes

Como referido anteriormente, a NIS2 passa a abranger mais sectores do que a primeira versão e também a distinguir entre os que são essenciais versus os que são importantes [2].

Desta forma, a NIS2 identifica entidades *essenciais* como pertencentes aos sectores de Energia, transportes, sector bancário, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, gestão de serviços TIC (entre empresas), administração pública e espaço.

E entidades *importantes* aquelas que pertencem aos sectores de Serviços postais e de estafeta, gestão de resíduos, produção, fabrico e distribuição de produtos químicos, produção, transformação e distribuição de produtos alimentares, indústria transformadora, prestadores de serviços digitais e investigação.

A principal diferença é que a disrupção de serviços nas entidades essenciais teria consequências graves para a economia e/ou sociedade do país como um todo. Ambas as categorias têm de adotar as medidas de segurança. No entanto, existe uma supervisão pró-ativa para as entidades essenciais, enquanto as importantes apenas são monitorizadas após um incidente, ou após a identificação de uma não-conformidade.

Incidentes significativos e obrigações

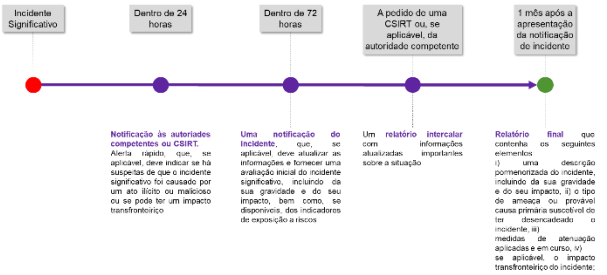
De uma forma geral as obrigações das entidades abrangidas pela NIS2 incorporam medidas de governação, medidas de gestão dos riscos de cibersegurança e obrigações de notificação.

Embora sejam várias as obrigações a que as entidades estão sujeitas, as que dizem respeito à notificação são de particular importância, pois estas irão forçar a que as entidades se preparem para o momento em que venham a ter um incidente significativo, pois como é sabido, mais cedo ou mais tarde, esse momento irá chegar.

A NIS2 considera que um incidente é significativo se [3]:

a) *"Tiver causado ou for suscetível de causar graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa;*
b) *Tiver afetado ou for suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis."*

E para estes incidentes passa a existir a obrigação de notificação de acordo com a figura seguinte.



Embora esta diretiva traga também outros pontos relevantes para a criação de uma Europa mais segura, como por exemplo o reforço da cooperação europeia na resposta a incidentes, os que indicámos resumem aqueles que serão os que mais impacto terão nas organizações nacionais, as quais irão ser obrigadas a cumprir com esta diretiva, após a sua transposição para a legislação nacional até outubro deste ano.

O impacto da NIS2 no panorama nacional

Evolução ou revolução?

Poderá a NIS2 ser um verdadeiro game-changer no que respeita à proteção das empresas e organizações nacionais? Se recuarmos cinco anos, aquando da introdução do RGPD, poderíamos fazer a mesma pergunta relativamente à proteção de dados: seria na altura o RGPD também um game-changer?

Se analisarmos os últimos cinco anos de RGPD verificamos que apesar de poder não ter sido uma verdadeira disrupção, foi sem dúvida um marco na Europa, e no mundo, no que diz respeito à proteção de dados. Atualmente vemos que o tratamento de dados, ainda que continue a ter bastantes falhas em

[2] Art. 3º - Diretiva (UE) 2022/2555 Do Parlamento Europeu E Do Conselho De 14 De Dezembro De 2022

[3] Art. 23º 3. - Diretiva (UE) 2022/2555 Do Parlamento Europeu E Do Conselho De 14 De Dezembro De 2022

algumas entidades, passou a ser realizado com mais cuidado, seja por via das potenciais coimas ou por qualquer outra, foi sem dúvida benéfico para os cidadãos europeus. Se fizermos uma analogia com a segurança das redes e informação na UE, é de esperar que também a NIS2 venha a ter um impacto significativo na segurança dos estados-membros. Se o RGPD se focava no indivíduo, já a NIS2 está focada na segurança das organizações, dos estados-membros e da Europa como um todo. Mais do que uma revolução, espera-se que a NIS2 venha a ser uma natural evolução das boas práticas que já hoje existem em algumas entidades.

Preparação para a conformidade

Neste momento assistimos já à preparação de algumas entidades que estão a alterar, ou já alteraram, parte dos seus processos e equipas de segurança para corresponder às exigências feitas pela NIS2. Em particular as obrigações de notificação irão forçar a uma mudança de processos e procedimentos, mas também, na grande maioria dos casos, da estrutura de recursos humanos. A começar pelo facto de "*que qualquer pessoa singular responsável por uma entidade essencial …, dispõe de poder para assegurar o seu cumprimento da presente diretiva.*"[4], algo que raramente vemos, com exceção das grandes organizações ou daquelas com elevada maturidade em cibersegurança. O mesmo artigo refere ainda que "*os Estados-Membros devem assegurar que seja possível considerar essas pessoas singulares responsáveis pela violação dos seus deveres de assegurar o cumprimento da presente diretiva*"[4]**Error! Bookmark not defined.**. Este último ponto em particular, poderá ser um grande desafio para as organizações pois implica também dar o poder aos responsáveis pelo cumprimento desta legislação, algo que nem todas as organizações estão ainda preparadas para o fazer.

Ainda no campo dos recursos humanos, "*as entidades em causa apresentam à CSIRT ou, se aplicável, à autoridade competente sem demora injustificada e, em qualquer caso, no prazo de 24 horas depois de terem tomado conhecimento do incidente significativo, um alerta rápido, que, se aplicável, deve indicar se há suspeitas de que o incidente significativo foi causado por um ato ilícito ou malicioso ou se pode ter um impacto transfronteiriço*"[5]. Coloca-se então a questão se estarão as entidades preparadas para fazer esta análise e notificação em 24 horas. Olhando para o panorama nacional, é seguro afirmar que a grande maioria não está preparada para o fazer. Dada a escassez de recursos humanos que existem na área de cibersegurança, a solução poderá passar pela utilização de recursos/empresas externas para auxiliar nesta análise e notificação.

Conclusões e Recomendações

À parte das adaptações que as diferentes entidades terão de fazer para estarem em conformidade com esta diretiva, a NIS2 impõe também uma mudança de atitude face a incidentes de cibersegurança. Passa a ser mais difícil esconder os incidentes com medo dos danos que poderão causar na reputação, pois os danos são muito maiores quando estas atitudes vêm a público. Acima de tudo passa por uma evolução, ou revolução em alguns casos, na forma de encarar e liderar com incidentes de cibersegurança.

Estamos culturalmente habituados a deixar tudo para o último momento. No entanto, neste caso, esta prática irá produzir maus resultados pois o próprio processo de adoção interna das medidas previstas na diretiva será na sua maioria longo, pois algumas das entidades abrangidas são organizações de grande dimensão, que pela sua natureza, levam tempo a adaptar-se a mudanças. Ao contrário do que parcialmente aconteceu com outras diretivas, é também importante que o sector público não se exclua de todo este processo, e que seja um modelo exemplar a seguir pelas entidades privadas. Seja no sector público ou no privado, quanto mais cedo se começarem a adotar as medidas propostas, melhor preparadas estarão as entidades para aquando da entrada em vigor da legislação em outubro deste ano.

Saiba mais sobre a DXC Portugal em https://dxc.com/pt/pt.

[4] Art. 32º 6. - Diretiva (UE) 2022/2555 Do Parlamento Europeu E Do Conselho De 14 De Dezembro De 2022

[5] Art. 23º 4. - Diretiva (UE) 2022/2555 Do Parlamento Europeu E Do Conselho De 14 De Dezembro De 2022

Introdução

A Ethiack é uma empresa portuguesa especialista em cibersegurança proativa, ofensiva e preventiva. A plataforma da Ethiack oferece Hacking Ético Autónomo, suportado por Inteligência Artificial e Machine Learning, o que permite gerir o risco de exposição digital das organizações e identificar, continuamente, vulnerabilidades com elevado impacto e precisão (+99%). A solução emite alertas em tempo real e providencia relatórios detalhados sobre a sua mitigação, o que permite otimizar recursos humanos e financeiros, ajudando as equipas a serem mais eficientes e proativas. A missão da Ethiack é proteger o progresso tecnológico e a transformação digital, fazendo da cibersegurança um bem acessível a todos.

A nossa análise às implicações da NIS 2 centra-se em alguns aspetos que requerem a implementação de processos robustos, nomeadamente o da gestão de risco, sobretudo naquilo que se relaciona com a gestão de ativos e vulnerabilidades.

Compreensão da NIS2

Análise Comparativa

Tal como preconizado na Diretiva (UE) 2016/1148 (NIS 1)[6], foi efetuada uma avaliação da sua implementação, por força do seu Artigo 23.º, tendo a Comissão Europeia chegado a algumas conclusões. Dessa forma, ficaram evidentes alguns pontos que fragilizaram a sua implementação e que importava serem melhorados[7].

Neste contexto, ficou patente que houve uma discrepância significativa ao nível da interpretação e implementação de várias matérias por parte dos Estados Membros, nomeadamente quanto à definição do conceito de "serviços essenciais", quanto à definição dos requisitos para reporte de incidentes de segurança ou, ainda, quanto ao nível de articulação transfronteiriça. Adicionalmente, conclui-se que a definição de setores potencialmente vulneráveis a ciber-incidentes era também incompleta, tendo levado a números bastante díspares ao nível do reporte de cada Estado Membro à ENISA no que concerne às entidades abrangidas pela NIS 1.

Surge, assim, a Diretiva (UE) 2022/2555 (NIS 2)[8], que pretende alcançar um objetivo mais ambicioso de assegurar um "elevado nível comum de cibersegurança na União".

Comparativamente com o diploma anterior, a nova regulamentação é, desde logo, mais extensa (27 vs. 46 artigos), sendo substancialmente mais detalhada. Por outro lado, altera um dos seus focos de "operadores de serviços essenciais e prestadores de serviços digitais" para "entidades essenciais e importantes" e introduz o critério da sua dimensão, entre outros, de forma a reduzir a ambiguidade constatada na NIS 1, ao nível da definição das entidades abrangidas pela sua aplicação. Expande, também, o número de setores críticos (7 vs. 11), adicionando, ainda, um conjunto de 7 outros setores considerados também potencialmente críticos (Anexo II).

Outra área que mereceu um incremento de exigência é a que regula a resposta a incidentes e gestão de crises. Globalmente, quer a definição funcional das CSIRT, quer a especificação dos seus requisitos, é, agora, mais alargada, às quais passa a caber a divulgação coordenada de vulnerabilidades.

Impactos previstos nas organizações

Globalmente, a tónica dominante é mais exigente para os diversos atores. O paradigma passa de uma definição mais ou menos vaga de procedimentos para uma abordagem mais proativa, que apela a ações concretas.

Ao nível das empresas, desde que sejam consideradas entidades essenciais ou importantes, a NIS 2 passa a exigir a existência de medidas de gestão de risco de cibersegurança (Art.º 21.º), obrigando os membros do órgão de direção a frequentar ações de formação incentivando-os a providenciarem ações similares aos restantes trabalhadores (Art.º 20, n.º 2).

[6] http://data.europa.eu/eli/dir/2016/1148/oj

[7] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019DC0546

[8] http://data.europa.eu/eli/dir/2022/2555/oj

Adicionalmente, os elementos de gestão destas entidades poderão ser responsabilizados pela violação dos seus deveres de assegurar o cumprimento da atual diretiva (Art.º 32.º, n.º 6; Art.º 33.º, n.º 5).

De forma a evidenciar a implementação das medidas de gestão de risco referidas, poderá ainda recair sobre estas entidades a exigência de utilização de produtos, serviços ou processos certificados no âmbito dos sistemas europeus de certificação de cibersegurança (Art.º 24.º).

Desafios

Atendendo ao aumento dos setores considerados críticos, bem como ao estabelecimento de critérios quantitativos para a definição de entidades essenciais ou importantes, é de prever que mais empresas venham a estar abrangidas pela NIS 2. Há alguns desafios que podem ser antecipados, não só para as entidades diretamente abrangidas pela NIS 2, mas também por outras que com elas se relacionam.

Medidas de gestão do risco de cibersegurança

Dessa forma, sobretudo em organizações menos maduras do ponto de vista da gestão de risco, será necessário cuidar da aplicação das medidas estabelecidas no Artigo 21.º. Neste domínio, há a considerar as medidas que estão sob controlo exclusivo de cada organização e as que dependem de terceiros.

Ao nível das primeiras, destacam-se a segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos (Art.º 21.º, n.º 2, alínea i). Em primeiro lugar, este tipo de medidas necessita de lidar com o fator humano, muitas vezes considerado como um potencial vetor de ataque mais fácil de explorar. Por outro lado, as entidades passarão a ter de identificar todos os seus ativos, não só físicos como digitais. Se ao nível dos físicos a inventariação é de concretização mais imediata, ao nível dos ativos digitais, as organizações poderão sentir um desafio maior, não só por não compreenderem o que é um ativo digital, mas também, por não terem implementado meios para os identificar.

Ao nível das medidas dependentes de terceiros estão, sobretudo, aquelas que se relacionam com alguns dos seus fornecedores e prestadores de serviços diretos. A sua implementação irá implicar, consequentemente, alterações noutras entidades fora do âmbito desta diretiva, uma vez que uma das áreas onde é necessário cuidar da gestão do risco é na que respeita à cadeia de abastecimento (Art.º 21.º, n.º 2, alíneas d) e e).

Na nossa análise, este deverá ser um dos efeitos menos antecipados pela generalidade do tecido empresarial, sobretudo ao nível das micro e pequenas empresas que pertençam à cadeia de abastecimento das entidades essenciais ou importantes. Adicionalmente, a imposição de práticas de segurança mais exigentes a estes agentes económicos, poderá gerar alguma entropia na implementação rigorosa dos processos para gestão de riscos, não só pelo desconhecimento, numa primeira fase, mas também pelos custos acrescidos que tal acarretará, mais tarde.

Contexto de supervisão e avaliação

Outro aspeto relevante diz respeito à utilização de determinados produtos, serviços ou processos de TIC, dado que, a fim de demonstrar o cumprimento de alguns dos requisitos estabelecidos no Artigo 21.º, as entidades essenciais e importantes poderão ser compelidas a adotar produtos com certificação ao nível da cibersegurança (Art.º 24.º, n.º 1). Neste domínio, o efeito sobre a cadeia de abastecimento também poderá impactar organizações que, à partida, estão fora do âmbito da diretiva, se as entidades essenciais e importantes tiverem necessidade de fornecimentos externos dessa natureza.

Relativamente à NIS 1, esta nova versão vem alargar as capacidades de supervisão das autoridades competentes. Assim, é de esperar uma verificação mais ativa do cumprimento da implementação da NIS 2, nomeadamente via inspeções remotas, auditorias (regulares e ad-hoc) ou apresentação de evidências da implementação de políticas de cibersegurança (Art.º 32.º e 33.º). Na nossa leitura, isto aponta para a possibilidade de as autoridades competentes desenvolverem formas de análise remota que permitam avaliar as entidades essenciais e

importantes, mesmo sem o conhecimento destas. A título de exemplo, será trivial uma análise dos ativos digitais expostos por uma dada organização,

possibilitando, dessa forma, a verificação acerca da correta gestão de ativos, da sua postura de segurança e, eventualmente, a identificação de práticas menos cuidadas ao nível da cibersegurança como a da gestão de vulnerabilidades dos serviços expostos. Efetivamente, esta é uma das funções atribuídas às CSIRT (Art.º 11.º, n.º 3, §2).

No contexto das medidas de gestão dos riscos de cibersegurança, existe um outro aspeto que merece destaque, aspeto esse centrado nas políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança (Art.º 21.º, n.º 2, alínea f). Na nossa leitura, este aspeto aponta para a recolha de indicadores, não só por via da gestão dos ativos, mas também pelas ações a empreender face ao estado desses mesmos ativos. Tal aspeto deverá incluir a análise de vulnerabilidades, de forma que as organizações possam incorporar a sua mitigação no contexto das medidas de gestão, tanto de forma automatizada, como por via de auditorias realizadas por técnicos especializados, genericamente referidos como testes de penetração (*Pentests*).

Conclusões e Recomendações

Atendendo à proximidade da entrada em vigor da Diretiva (UE) 2022/2555 (NIS 2), parece ser necessária uma atenção da generalidade do tecido empresarial, não só das potenciais entidades essenciais ou importantes, mas também dos seus fornecedores. Dessa forma, será possível começar a endereçar uma lista de ações conducentes à adequação de cada um a esta realidade mais exigente.

A um certo nível, existem pontos convergentes com a implementação de alguns tipos de certificação, como por exemplo a ISO 27001, ou SOC 2. Nesse sentido, o desafio de adequação a esta realidade será superior para aquelas organizações que ainda não tenham passado por processos semelhantes.

Todavia, o bem percecionado que o incremento da cibersegurança ao nível da União Europeia pode trazer, nomeadamente para melhorar o funcionamento do mercado interno e aumentar o nível global de segurança dos cidadãos e dos serviços que suportam o funcionamento atual da sociedade, merece uma atenção cuidada e uma implementação célere e robusta.

Globalmente, uma vez que a tónica passa a estar assente em processos proativos, atendendo ainda à necessidade que as organizações passarão a ter de gerirem o risco, bem como a uma postura mais vigilante das autoridades competentes, somos da opinião de que as empresas deverão cuidar de forma mais eficaz da sua gestão de ativos, nomeadamente os digitais. Neste domínio, uma vez que, em muitos casos, o conjunto desses ativos expostos é bastante dinâmico, entendemos que a sua monitorização deve ser permanente, de forma a detetar, atempadamente, alterações na sua composição, possibilitando uma atuação em tempo útil sobre os mesmos.

Adicionalmente, essa monitorização deverá ser acompanhada de um processo de identificação de vulnerabilidades permanente, não só pela circunstância da mudança de ativos anteriormente referida, mas, sobretudo, porque todos os dias são identificadas mais de 70 novas vulnerabilidades que impactam diretamente aplicações e sistemas em produção utilizados por muitas organizações a nível global.

Atendendo à escassez de recursos humanos existente no domínio da cibersegurança, fará sentido considerar a gestão das vulnerabilidades associada à gestão de ativos de forma integrada, dentro de um conceito de gestão da superfície de ataque. Dessa forma, as organizações poderão ter uma abordagem holística dos ativos digitais e do seu estado, permitindo estabelecer as medidas adequadas de mitigação no contexto dos processos de gestão de risco a implementar, obtendo, simultaneamente, uma otimização de recursos, num cenário de superfícies de ataque tendencialmente crescentes.

Saiba mais sobre a Ethiack em https://ethiack.com.

Introdução

A Sincronideia está integrada num grupo que conta com trinta e sete anos de desenvolvimento de serviços no âmbito das tecnologias de informação, a partir do Vale do Ave. Dentro do grupo, recorrendo a uma equipa multidisciplinar, a Sincronideia presta um conjunto de serviços de consultoria com especial foco no âmbito específico da proteção de dados pessoais e, de forma mais abrangente, no âmbito da gestão da Segurança da Informação. Dedica-se ao desenvolvimento de projetos, em vários setores de atividade, incluindo indústria, serviços de várias áreas, setor social, saúde e Administração Pública, sendo de realçar o trabalho realizado no contexto específico de autarquia local.

É precisamente da experiência resultante da prestação de serviços no contexto da administração pública local que se têm vindo a apresentar desafios mais envolventes para a equipa, coincidentemente, ou não, no que respeita a algumas das alterações percecionadas como mais relevantes no texto da NIS II. Acresce que, segundo os relatórios anuais "Threat Landscape" da ENISA, tem sido precisamente este setor a liderar o ranking do número de incidentes de segurança reportados. Concretamente, no período de julho 2022 a junho 2023, o setor da administração pública foi responsável por cerca de um quinto do total de incidentes reportados.

Com este artigo propomo-nos refletir sobre parte da argumentação que o legislador europeu elencou para justificar a necessidade de novo processo legislativo, através da comparação das duas Diretivas. Pretende-se, neste âmbito, prever se as alterações prescritas pela nova Diretiva poderão responder aos desafios reais no âmbito da implementação de sistemas de gestão da segurança da informação, que têm vindo a ser identificados.

Compreensão da NIS2

A nova Diretiva apresenta um conjunto de novas, ou reforçadas exigências, que o legislador europeu entendeu como não tendo sido devidamente respondidas pelo quadro legislativo anterior e pela forma como o mesmo foi transposto para as ordens jurídicas dos Estados-Membros. Embora não se constitua como o principal foco deste artigo, importa referir as principais alterações, com impacto direto nas entidades abrangidas: a maior especificação no que respeita aos deveres de notificação de incidentes; o reforço das prescrições quanto à abordagem da gestão da segurança com base na avaliação de risco e a ampliação das entidades abrangidas por este quadro legal, englobando aqui um conjunto mais alargado de setores e obrigando os Estados Membros e identificar entidades que sejam consideradas essenciais ou importantes para o cumprimento dos objetivos do quadro legal.

Analisando as duas Diretivas num contexto muito específico, identifica-se na primeira apenas uma referência ao termo "governação" e a ausência de referências à expressão "cadeia de abastecimento", enquanto na segunda já se distinguem dez referências a cada um dos dois tópicos referidos.

No que concerne à Governação, entender-se-á a sua importância no âmbito da gestão de qualquer sistema, sendo que a segurança da informação não é, naturalmente, exceção.

Na nova diretiva, o legislador europeu prescreve, de forma clara, que os Estados-Membros legislem de forma que os órgãos de direção das entidades abrangidas não só aprovem as medidas de gestão do risco de cibersegurança, como também sejam efetivamente responsabilizados, de acordo com a ordenação jurídica de cada Estado-Membro, pelas infrações que eventualmente venham a ser cometidas. Destaca-se ainda a referência direta à responsabilização dos funcionários públicos e dos eleitos locais a desempenhar funções de direção.

Ainda no mesmo âmbito, o legislador reforça a importância e necessidade da formação nestas matérias, obrigando à implementação de planos de formação transversais, desde logo preceituando a obrigação de frequência de ações formativas por parte da gestão de topo, e atribuindo a estes responsáveis a responsabilidade direta na promoção de formação perante toda a restante hierarquia institucional.

Debrucemo-nos agora sobre o contexto de obrigações respeitantes à cadeia de abastecimento constantes da nova Diretiva.

Antes de mais, considera-se pertinente sublinhar a crescente dificuldade, cada vez mais evidente, em

captar e manter recursos nas entidades públicas, sobretudo nesta área das Tecnologias de Informação, instituído que está um ambiente de crescente promoção da transição digital. Esta é uma dificuldade reconhecida pela tutela que motivou, inclusive, esforços legislativos que procuram promover a atratividade da área.

Naturalmente, a resposta às crescentes necessidades deverá ser suportada por uma variedade de serviços externos de vários âmbitos, desde a resposta a necessidades mais especializadas, até ao suporte de serviços de simples manutenção de infraestruturas e apoio a utilizadores.

É um facto assumido que aos recursos internos das instituições cabem cada vez mais responsabilidades de gestão de serviços externos. Esta crescente e exigente tarefa exige que os recursos internos desenvolvam mais capacidades de gestão.

Também aqui, a abordagem agora assumida na NIS II, concretamente de reforço das obrigações impostas à cadeia de abastecimento, vem responder às dificuldades notadas pelas entidades públicas, em estender, para a sua cadeia de abastecimento, as medidas de gestão de risco que têm vindo, progressivamente, a ser integradas na sua gestão interna.

Adaptações Necessárias e Desafios Antecipados

A habitual organização de competências que determina a operacionalização efetiva das instituições deve incluir, obrigatoriamente, os recursos responsáveis pela segurança e pontos de contato permanentes, atribuindo aos mesmos competências de atuação adequadas no âmbito da legislação vigente, adaptada ao real contexto da instituição.

As principais tarefas, que decorrem da gestão da informação, devem sair do silo das unidades organizacionais de tecnologias de informação e integrar as competências e atribuições de outros perfis, desde logo da gestão de topo. Estas alterações terão, naturalmente, impacto na cultura organizacional vigente, estando o sucesso das mesmas, no que respeita ao atingir dos objetivos de segurança, dependentes da forma como se definirá um modelo de governação que considere as especificidades únicas de cada entidade.

As exigências agora a impor à cadeia de abastecimento poderão apresentar um grau adicional de complexidade, considerando a necessidade de cumprimento do conjunto de obrigações impostas pelo Código dos contratos públicos ora vigente.

Caberá a cada entidade, através dos responsáveis internos adequados, transpor para as peças de contratação pública, o conjunto de requisitos que garanta a qualidade, resiliência global de produtos e serviços, mas que também imponha a prática de medidas de gestão de riscos e de gestão da segurança e da cibersegurança.

Considerando em avaliação, meramente percecionada da experiência, que a larga maioria dos procedimentos tem o custo como fator único de decisão de adjudicação, torna-se imperativo que a definição de requisitos seja suficientemente específica para incluir os almejados objetivos no âmbito da estratégia de segurança como complemento ao fornecimento do bem ou serviço em si. Esta definição deverá ser ponderada, por forma a não ferir os princípios de não limitação da concorrência.

O recurso ao critério de adjudicação em modalidade multifator, ou o recurso à prévia qualificação, pode melhor servir as novas obrigações da instituição, transpondo as prescrições da NIS II para a cadeia de abastecimento, sem descurar os habituais objetivos da contratação pública, nomeadamente financeiros e de qualidade técnica e organizativa. Caberá ao conjunto de fornecedores definir e implementar as suas próprias iniciativas no âmbito da segurança da informação, por forma a poderem responder às novas exigências promovendo a livre concorrência. Com o término dos procedimentos de contratação não termina o novo trabalho das instituições, cabendo-lhes, de futuro, a avaliação contínua dos serviços a prestar.

Conclusões e Recomendações

A responsabilização adicional agora atribuída aos órgãos de direção deve servir de móbil para definitivamente envolver estes recursos em cada etapa de definição e aprovação procedimental, dotando-os de conhecimento efetivo sobre as tarefas respeitantes à Gestão da Segurança da Informação, por forma a que os mesmos patrocinem devidamente

cada projeto transmitindo e atestando um compromisso efetivo para com os objetivos de gestão da Segurança da Informação. Este envolvimento crescente, e agora devido, fomentará junto das lideranças a noção contextual e abrangente da importância estratégica que a Segurança da Informação representa para a instituição e, por inerência, para o conjunto alargado de partes interessadas que exigem a manutenção de serviços dos quais são utilizadores, e da consequente preservação da Informação detida pela Instituição.

No que respeita à cadeia de abastecimento, exige-se que os procedimentos de contratação pública devam incluir, por defeito, um conjunto de requisitos que a responsabilizem pela definição e implementação efetiva de medidas que salvaguardem toda a cadeia, em benefício último da entidade adjudicante.

Para que se atinjam estes objetivos será necessário o reforço do trabalho colaborativo entre responsáveis das áreas dos Sistemas de Informação, da área Administrativa e Jurídica e da própria gestão de topo.

Face ao exposto considera-se que a nova Diretiva se apresenta como oportunidade para que, especialmente, o setor abordado neste artigo possa reforçar a sua estratégia no âmbito da segurança da informação, através da otimização do modelo de governação e transpondo de forma adequada essa mesma estratégia para a sua cadeia de abastecimento.

Saiba mais sobre a Sincronideia em https://sincronideia.pt/.

Sobre a AP2SI

A Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) foi fundada em Janeiro de 2012, é uma associação sem fins lucrativos e de natureza privada e tem como objetivo contribuir para o desenvolvimento da Segurança da Informação em Portugal, de forma ativa, através da sensibilização para o valor e necessidade de proteção da Informação, e do desenvolvimento e promoção de orientações que visem reforçar o conhecimento e a qualificação dos indivíduos e organizações.

Visite-nos em https://ap2si.org ou contacte-nos em geral@ap2si.org.

Os impactos da Diretiva NIS2 em Portugal

1ª edição – Fevereiro de 2023