FEV. 23

NOTA INFORMATIVA

TECNOLOGIA, MEDIA E TELECOMUNICAÇÕES

CNPD aprova diretriz sobre medidas de segurança

No dia 10 de janeiro de 2023, a Comissão Nacional de Proteção de Dados ("**CNPD**") aprovou a Diretriz/2023/1[1] ("**Diretriz**") sobre medidas organizativas e de segurança, tendo em vista promover a consciencialização das organizações para a relevância da implementação de políticas de segurança adequadas, clarificando que o número significativo de ataques ocorridos em 2022, radica, na sua maioria, na falta de investimento nesta área – resultando em vulnerabilidades nas infraestruturas e falta de formação dos utilizadores.

De acordo com a CNPD, os ataques mais frequentemente perpetrados afetam, na sua grande maioria, dados pessoais, resultando em *data breaches*, o que convoca o regime previsto no Regulamento Geral sobre a Proteção de Dados – melhor dizendo, deve ter lugar uma *(i)* análise de risco e documentação do incidente, e, dependendo dessa análise, *(ii)* deve ser a CNPD notificada no prazo de 72 horas (enfatizando a CNPD que se trata de um prazo contínuo, não se suspendendo aos sábados, domingos e feriados), e, *(iii)* novamente dependendo do risco identificado em primeiro lugar, poderão ter de ser notificados os titulares dos dados pessoais.

Considerando o curto prazo de notificação à CNPD, o responsável pelo tratamento deverá, desejavelmente, implementar políticas internas que lhe permitam detetar e gerir incidentes de segurança com impacto na proteção de dados pessoais, bem como, assegurar mecanismos de controlo eficazes quanto à atuação dos subcontratantes, de modo a garantir que estes não prejudicam o cumprimento das suas obrigações legais.

A CNPD visa combater, através de uma ótica preventiva, os crescentes ataques a sistemas de informação – enfatizando que foram registados em número crescente em 2022.

Pedro Lomba
Marta Salgado Areias
Carolina Ventura
Equipa de Tecnologia, Media e Telecomunicações

1 Disponível aqui.

A CNPD teve por objetivo, com a publicação da Diretriz, sensibilizar as entidades que tratam dados pessoais – quer na qualidade de subcontratantes, quer na qualidade de responsáveis pelo tratamento – para a necessidade de investirem nesta área, elencando algumas medidas, a título de exemplo, e enfatizando que estas são forçosamente dinâmicas devendo ser atualizadas sempre que necessário. Esta atualização deve ser motivada pelo acompanhamento do estado da arte e do risco crescente, bem como, pela regular avaliação substantiva e profunda das operações de tratamento e do impacto que as tecnologias implicam no funcionamento das suas organizações e, no caso dos dados pessoais, dos riscos para os direitos e liberdades das pessoas singulares.

As medidas elencadas pela Diretriz devem ser consideradas pelas organizações nos seus planos de prevenção e de minimização dos riscos e devem ser tomadas como um incentivo para impulsionar esta área, na medida em que se tem vindo a tornar claro que as medidas de segurança tipicamente utilizadas, deixaram de ser suficientes, ante a sofisticação que os ciberataques têm vindo a atingir.

A CNPD recomenda - entre outras – a realização de auditorias de segurança e avaliações de vulnerabilidades, para que a organização possa conhecer as suas fragilidades, sugerindo a monitorização dos utilizadores mais frágeis e consequente investimento em formação. Também a nível organizacional, a CNPD sugere a adoção de alarmística que identifique situações de acesso ou tentativas de utilização indevida, o que por sua, vez permite, uma mais célere identificação de incidentes de segurança.

No âmbito técnico, as medidas deverão ser adaptadas ao contexto. Por exemplo, a CNPD recomenda a utilização de sistemas e infraestruturas que permitam segmentar ou isolar as redes de dados, de modo a prevenir a propagação interna e externa de *malware*. Na utilização de equipamento em ambiente externo, a CNPD sublinha, designadamente, que os acessos apenas devem ser feitos por VPN.

A chave para a implementação de medidas adequadas está na sua adaptação ao caso concreto e no dinamismo com que são adaptadas e revistas, sendo essencial investir na proteção das organizações contra ataques informáticos, com um grau crescente de sofisticação, de modo a acompanhar o grau crescente de risco.

Em suma, a nova Diretriz preconiza uma aliança entre a prevenção e o dinamismo, encorajando as organizações a definirem antecipadamente e a colocarem em prática planos de prevenção adequados às características e sensibilidade do tratamento de dados pessoais que levam a cabo, bem como, das particularidades da organização.

Importa, por fim, dar nota de que Cabe às entidades que atuam na qualidade de responsáveis pelo tratamento à luz do Regulamento Geral sobre a Proteção de Dados, assegurar o respeito pelos direitos e interesses dos titulares dos dados, estando aptas demonstrar que adotaram medidas de segurança adequadas.

Esta Diretriz deve ser o ponto de partida para as organizações implementarem políticas de segurança adequadas, e refletirem sobre a crescente importância da cibersegurança, bem como, do potencial danoso que um ataque informático pode representar. ■