INSTRUÇÃO 3/2021

Cibersegurança nas relações e comunicações informáticas com o OMIE

19 – outubro - 2021

INSTRUÇÃO 3/2021

Cibersegurança nas relações e comunicações informáticas com o OMIE

1. PREÂMBULO

A segurança nas relações e comunicações informáticas, inclusive antes da Covid-19, foi sempre um tema-chave para as empresas, especialmente aquelas que têm uma alta componente de utilização de meios eletrónicos, como é o caso do OMIE, dadas as características e fragilidades pressupostas em trabalhar num meio sujeito à aplicação de tecnologias emergentes. Este meio abre a porta a ataques que podem minar a operação e a continuidade dos negócios.

Com o aparecimento da Covid-19, os principais ataques informáticos que ocorreram durante a pandemia aumentaram apresentando-se de diversas formas, tais como *e-mails* supostamente provenientes de fontes conhecidas e aparentando estar devidamente acreditadas, mensagens com informação específica e especialmente sensível (e.g. pedidos ou tentativas de execução de transações económicas), vírus, *malware*, cibercriminalidade, *spyware* e incontáveis ameaças existentes, tudo com o objetivo de obter efeitos económicos fraudulentos, apoderar-se de informação ou sequestrar ou corromper sistemas informáticos.

Adicionalmente, o novo modelo de trabalho remoto foi um grande desafio para as companhias, e aumentou significativamente os riscos, entre eles a vulnerabilidade a ataques e fraudes cibernéticos.

Perante as circunstâncias mencionadas, o OMIE, na sua qualidade de operador do mercado, deve proceder a qualquer momento a ocupar-se desta relevante questão com o objetivo de configurar uma estratégia que proteja ativos, agentes e informação, permitindo assim a continuidade pacífica dos negócios.

Em conformidade com aquilo que foi exposto anteriormente, esta Instrução pretende responder aos riscos de cibersegurança existentes nas infraestruturas dos agentes e do mercado, proporcionando orientações para a gestão e solução de futuros cenários de risco com o objetivo de assegurar a integridade e o bom funcionamento dos equipamentos informáticos dos agentes e das plataformas do mercado, tal como das comunicações com os agentes face a possíveis problemas de atos fraudulentos ou perdas ou interceção de dados.

2. DESENVOLVIMENTO

O adequado funcionamento do mercado de eletricidade requer, como uma das suas características essenciais, o cumprimento, por parte do operador do mercado e por parte dos agentes, de medidas e instruções de cibersegurança nos sistemas de informação e comunicação utilizados nas comunicações com o OMIE.

O aumento do número de ciberataques a empresas e particulares, bem como os tipos de ataque, requerem o estabelecimento de medidas a todos os níveis (técnicos, organizativos, de consciencialização) para evitar incidentes de cibersegurança que alterem o funcionamento dos processos.

Nos últimos tempos têm-se observado diferentes tipos de ataques às infraestruturas das empresas (vírus, *malware*, *spyware*, etc.). Destacam-se entre estes os que utilizam os mecanismos de correio eletrónico, que a partir de informação obtida de maneira fraudulenta, mediante engenharia social ou intercetando correios eletrónicos de contas comprometidas por terceiros não autorizados, usurpam a identidade dos remetentes das mensagens e solicitam a realização de ações ou operações inadequadas.

Por isso mesmo é necessário manter uma atenção constante e seguir as normas básicas de cibersegurança, sendo esse um requerimento essencial que deve ser aplicado nas infraestruturas utilizadas pelos agentes para a negociação, e nas relações e comunicações informáticas entre o OMIE e os agentes do mercado.

Plataformas do OMIE e comunicações informáticas com o OMIE

O OMIE tem já estabelecidas medidas de cibersegurança de caráter técnico, procedimental e organizativo que garantem o funcionamento correto e seguro dos seus sistemas de informação e das plataformas de mercado.

O acesso às plataformas de mercado utilizadas pelos agentes (www.mercado.omie.es) realiza-se através de uma ligação segura na qual se requer o uso de certificados digitais pessoais que garantem a identidade do utilizador, sendo impedido o acesso caso não se disponha de um certificado autorizado. O certificado digital utiliza-se também para assinar as operações realizadas pelo agente na plataforma *web* de agentes, e permite o rastreio das ditas operações. As ações realizadas pelos agentes na sua relação com o mercado devem ser levadas a cabo exclusivamente através das referidas plataformas e mediante o uso adequado de certificados pessoais.

Toda a informação confidencial submetida pelos agentes ou requerida para as suas ações no mercado pode apenas aceder-se através da plataforma *web* de agentes (www.mercado.omie.es) utilizando os certificados digitais emitidos pelo OMIE.

Em caso de modificação do conteúdo da informação, o OMIE substituirá a informação acessível através da plataforma, podendo notificar os agentes da sua modificação indicando que se volte a aceder à plataforma para obter os novos valores, mas nunca enviando os valores modificados por correio eletrónico.

O OMIE não fornece informação sensível (dados de ofertas, resultados do mercado, faturas de entrega de energia ou notas de crédito ou débito) por correio eletrónico.

Caso o agente receba correios eletrónicos que possam em aparência ter sido enviados pelo OMIE, nos quais seja requerida a realização de ações atípicas, não habituais, com caráter excecional ou de emergência, o agente deverá rever adequadamente a mensagem e, se tiver alguma suspeita sobre a sua autenticidade, deve contactar imediatamente o OMIE através dos meios estabelecidos para confirmar a autenticidade da mesma.

Obrigações dos agentes

Os agentes devem tomar todas as precauções razoáveis e próprias de uma diligência profissional adequada para proteger a sua infraestrutura informática e evitar o uso ou acesso fraudulento ou não autorizado aos dados e às plataformas de negociação do mercado. Além disso, deverão pôr-se em contacto de imediato com o OMIE se tiverem motivos para suspeitar que ocorreu um acesso indevido à sua infraestrutura informática que tenha podido comprometer a informação trocada com o mercado, os equipamentos informáticos do agente através dos quais se acede ao mercado, os certificados digitais de acesso ao mesmo, ou se foram indevidamente divulgados dados confidenciais ou de segurança dos acessos às plataformas de mercado.

Em caso de dúvida perante uma informação aparentemente recebida do OMIE, o agente deve remeter-se sempre para a informação publicada na plataforma *web* de agentes, ou, em caso de necessidade, proceder a confirmar a autenticidade da dita informação mediante uma chamada para os números de contacto do OMIE.

No que respeita aos certificados digitais emitidos pelo OMIE para o acesso dos agentes à plataforma *web* do mercado, o agente está obrigado à respetiva custódia e manutenção, devendo revogar e solicitar a emissão de novos certificados digitais em caso de perda do certificado, perante a dúvida de que se estejam a realizar acessos externos não autorizados com algum certificado do agente ou face à suspeita de que possam ter sido acedidos de maneira indevida.

Relativamente à infraestrutura de acesso e às comunicações digitais com o OMIE, o agente deve ter estabelecidos mecanismos e procedimentos de cibersegurança e de vigilância para o uso e troca de informação sensível, tendo também em conta as melhorias práticas em cibersegurança que garantam que os mencionados processos se realizem de maneira segura.

Os agentes devem sempre garantir que as suas infraestruturas informáticas não causam nenhum impacto no correto funcionamento das plataformas do mercado,

devendo também colaborar com o OMIE no sentido de gerir e solucionar essas situações.

Procedimento face a um incidente de cibersegurança nas instalações de um agente

Caso um agente do mercado detete algum incidente de cibersegurança interna que possa pôr em risco a informação trocada com o OMIE, os equipamentos informáticos do agente através dos quais se acede ao mercado, ou os certificados digitais de acesso às plataformas de negociação, além dos processos internos que estejam estabelecidos para lidar com incidentes de cibersegurança, o agente deverá também cooperar com o OMIE durante todo o processo de gestão do incidente.

Assim que for detetado o incidente, o agente deverá imediatamente notificar o OMIE dessa ocorrência através dos meios oficiais de comunicação estabelecidos, tal como está indicado na “Informação de contacto”, acessível na plataforma *web* de agentes e descrita no ANEXO I.

A notificação deve detalhar a gestão do incidente por parte do agente nos aspetos relevantes que possam afetar o mercado, particularmente naquilo que se refere aos equipamentos eletrónicos do agente mediante os quais se acede ao mercado ou nos quais se armazena informação do mesmo, com especial menção aos certificados digitais de acesso.

O agente está obrigado a proporcionar informação adicional relevante que lhe possa ser requerida pelo OMIE no que respeita ao incidente e aos possíveis procedimentos na infraestrutura do agente que tenha relação com o mercado, para que, de maneira coordenada, se avance no estabelecimento das medidas necessárias até à completa resolução do incidente ou, pelo menos, até que se assegure completamente a ausência de qualquer risco para o mercado, momento em que se deverá informar novamente o OMIE, fornecendo a informação associada à conclusão total ou parcial do incidente. O agente deve comunicar a informação relevante discriminada pelas diferentes fases de deteção, contenção e mitigação e, finalmente, recuperação do incidente.

Durante este processo, em caso de risco para o mercado, o OMIE poderá interromper a qualquer momento o acesso do agente ou exigir ações tais como a revogação de certificados, a renovação ou modificação de chaves criptográficas ou elementos similares que o agente utilize, a fim de proteger o correto funcionamento do mercado.

Com o objetivo de que todo o processo de gestão do incidente se realize de maneira adequada e a comunicação entre o OMIE e o agente seja ágil e eficaz, o agente está obrigado a manter atualizados, na plataforma *web* de agentes, os dados das pessoas de contacto designadas pelo agente para a interlocução com o OMIE, acessíveis mediante o trajeto indicado no ANEXO II

ANEXO I

ANEXO II

www.mercado.omie.es

Dados de Agentes - Dados operativos - Agentes e **Pessoas de contacto**