DIRECTIVE 3/2021

Cybersecurity in Data Communications and Relations with OMIE

19 - October - 2021

DIRECTIVE 3/2021

Cybersecurity in data communications and relations with OMIE

1. PREAMBLE

Security in data communications and relationships, even before COVID-19, has always been a key issue for companies, especially those like OMIE with a high level of using information technology and communications (ITC), due to the characteristics and weaknesses of working in an environment subjected to the application of emerging technologies. This environment opens the door to attacks that can undermine the operation and continuity of business.

The number of main computer attacks that have occurred during the COVID-19 pandemic has increased andthey have appeared in various forms, such as e-mails that are supposedly from known contacts and sources that seem duly accredited, messages with specific and particularly sensitive information (a request for or attempted execution of financial transactions), viruses, malware, cybercrime, spyware, and a number of existing threats, all with the aim of carrying out fraudulent financial effects, obtaining information, or hijacking or corrupting computer systems.

The new remote work model has also been a great challenge for companies, and it has significantly increased risks, including the vulnerability of falling victim to cyberattacks and fraud.

In light of the aforementioned circumstances, OMIE, in its capacity as market operator, must continually attend to this significant issue in order to set forth a strategy that protects assets, agents and information that support peaceful business continuity.

In accordance with the foregoing, this Directive aims to respond to the existing cybersecurity risks in the agents' and market's infrastructures, providing a guide for managing and resolving future risk scenarios in order to ensure the integrity and proper functioning of the agents' computer equipment and the market's platforms, as well as for communications with agents in the event of potential issues related to fraudulent actions, losses or intercepted data.

2. PROCEDURE

As one of its essential characteristics, the electricity market's proper functioning requires the market operator's and the agents' compliance with cybersecurity measures and instructions on communications and information systems used in communications with OMIE.

The increase in the number of cyberattacks against companies and individuals, as well as the types of attacks, require establishing measures at all levels (technical, organizational, awareness-raising) to prevent cybersecurity incidents that may alter the performance of processes.

In recent times, different types of attacks on company infrastructures (viruses, malware, spyware...) have been seen. Those that employ e-mail mechanisms are particularly notable in which information or identities obtained fraudulently (through social engineering or by intercepting e-mails from accounts that are compromised by third parties), are used by unauthorized senders to send messages and request improper operations or actions to be carried out.

It is therefore necessary to stay vigilant at all times and to follow basic cybersecurity rules. This is an essential requirement that must be applied for the infrastructures used by the agents for negotiation and in the data communications and relationships between OMIE and market agents.

OMIE's platforms and data communications with OMIE

OMIE has established technical, procedural, and organizational cybersecurity measures that ensure the proper and secure functioning of its information systems and market platforms.

The market platforms used by the agents (www.mercado.omie.es) are accessed through a secure connection which requires personal digital certificates that ensure the user's identity, preventing access without an authorized certificate. Digital certificates are also used for signing off on operations carried out by the agent on the market website, that enable operations' traceability. The actions carried out by agents in their relationship with the market must be performed exclusively through that platforms and by properly using personal certificates.

All confidential information that is supplied by the agents or required for their actions on the market is accessible exclusively through the market website (www.mercado.omie.es) using the digital certificates issued by OMIE.

In the event the information's content is modified, OMIE will replace the information that is accessible through the market website andmay notify the agents of its modification, indicating revisiting the website to find the new information; however, OMIE will never send the modified parts by e-mail.

OMIE does not provide sensitive information (data on bids, market results, energy delivery invoices or credit or debit notices) by e-mail.

In the event that an agent receives e-mails that may appear to have been sent by OMIE and which demand the performance of atypical, unusual, exceptional or emergency actions, the agent must review the message properly and if they have any suspicions about its authenticity, they should contact OMIE immediately via established methods to confirm its authenticity.

Agent obligations

Agents must take all reasonable precautions that are fitting for professional diligence to protect their IT infrastructure and prevent fraudulent or unauthorized use of or access to data and the market's trading platforms. Likewise, they should immediately contact OMIE if they have reason to suspect that their IT infrastructure has been unduly accessed, potentially compromising the information exchanged with the market, the agent's IT equipment that communicates with the market, the digital certificates for accessing the market, or if confidential or security-related data on accessing the market platforms have been unduly disclosed.

In case of doubt about information that appears to have been sent from OMIE, the agent must always refer to the information published on the market website, or if necessary, confirm the authenticity of that information by calling OMIE's contact numbers.

Regarding the digital certificates issued by OMIE for agents to access the market website, the agent is required to uphold their safe-keeping and maintenance; they must have them revoked and request the issuance of new digital certificates if they lose a certificate (given the question around any unauthorized external access being carried out with an agent's certificate) or if they suspect that they may have been improperly accessed.

As regards access infrastructure and digital communications with OMIE, the agent must have established cybersecurity and surveillance mechanisms and procedures on using and exchanging sensitive information. They must also consider best practices in cybersecurity, which guarantee that the aforementioned processes are carried out safely.

At all times, agents must ensure that their IT infrastructures are not impacting the proper functioning of the market platforms, and they must work with OMIE to manage and solve these situations.

Acting in the event of an internal cybersecurity incident at an agent's facilities

In the event that a market agent detects an internal cybersecurity incident that could put the information exchanged with OMIE, the agent's computer equipment that communicates with the market, or the digital certificates for accessing trading platforms at risk, besides the internal processes that it has established for handling

cybersecurity incidents, the agent must cooperate with OMIE throughout the incident management process.

As soon as an incident is detected, the agent must immediately notify OMIE through the official means of communication that have been established, as indicated in the “Contact information” found on the market website and described in ANNEX I.

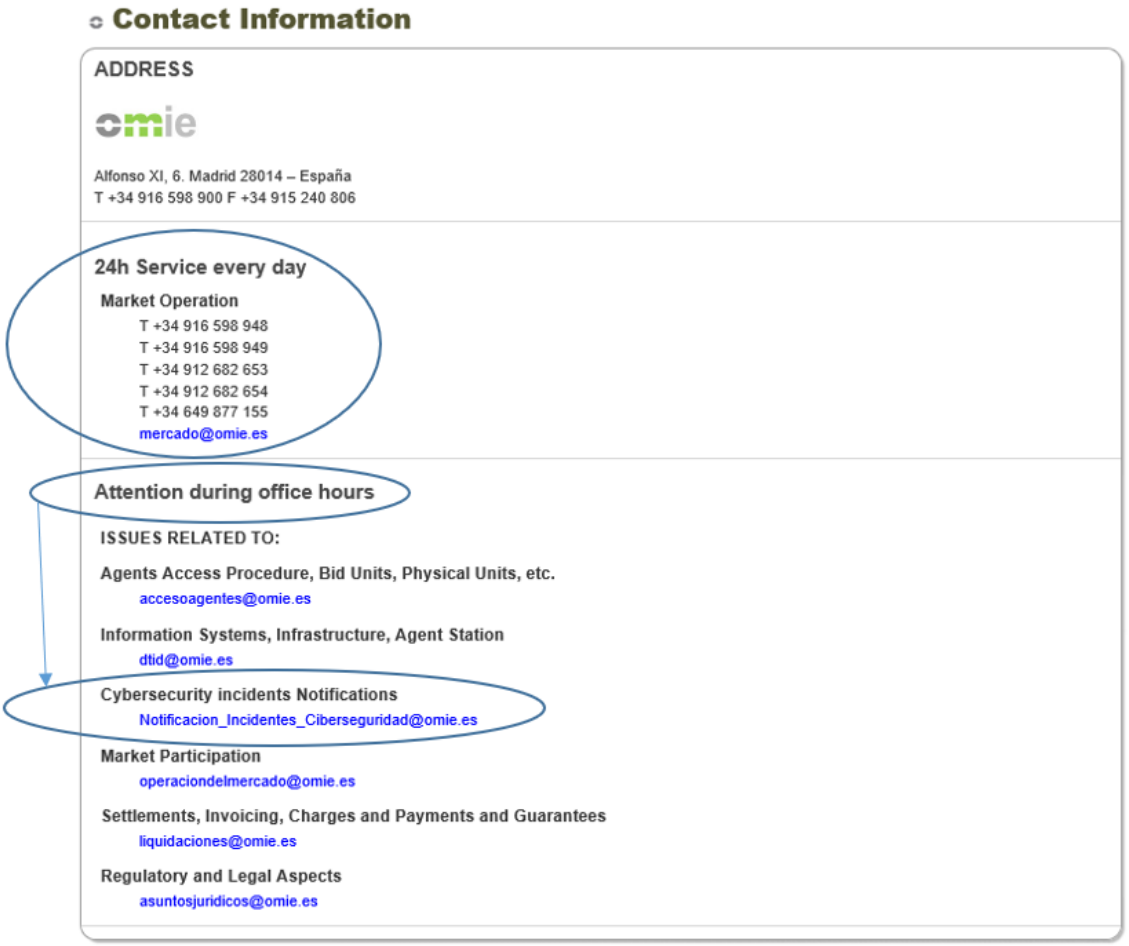
The notification must contain details on the agent’s handling of the incident in significant aspects of the incident that may affect the market, especially in everything related to the agent’s equipment that communicates with the market or where the market’s information is stored, particularly with regard to digital access certificates.

The agent is obliged to provide any other relevant information that may be required by OMIE regarding the incident and the possible actions in the agent’s infrastructure that may be related to the market. This helps ensure that progress is made in establishing the necessary measures in a coordinated way until the incident is fully resolved, or at least until it can be fully ensured there is no risk to the market. At that time, OMIE must be informed again, along with the information on full or partial closure of the incident. The agent must communicate any relevant information associated with the detection, containment, and mitigation sections, and, finally, recovery from the incident.

In case of risk to the market, OMIE may, at any time during this process, interrupt agent access or demand actions such as the revocation of certificates, the renewal or modification of encryption keys or similar elements used by agents to protect the market’s proper functioning.

In order for the entire incident management process to be carried out properly and for communication between OMIE and the agent to be agile and effective, the agent is required to keep information on their designated contacts updated on the market website for dialogue with OMIE; they are accessible according to the routes indicated in ANNEX II

ANNEX I



ANNEX II

www.mercado.omie.es

Agent Data - Current Data - Agents and **Contacts Persons**