



HACKER ATTACK ON THE LAZIO REGION: WHAT DOES IT TEACH US?



On August 4, 2021, the Lazio Region suffered a hacker attack on the regional data server. The attack started from the computer of an employee in smart working, infected by malware. Data on VM-Ware virtual machines and regional documents were encrypted. Also aggravating the Lazio Region's position was the absence of an offline backup and the hackers' deletion of the online one. The attack, from an analysis of the latest "Clusit report" on IT security in Italy, was among the most predictable, as the public sector is among the most affected targets by Cybercrime since 2020. The majority of attacks occur with malware and the trend is clearly growing.

But what are the legal/regulatory considerations in reference to this attack?

First of all, it is necessary to analyze the minimum security measures of the AGID (Agency for Digital Italy) applicable to the Public Administration, which require that the supports containing at least one of the backup copies be not permanently accessible from the system, in order to avoid that attacks to the latter may also involve all the backup copies.

It is also necessary to take into consideration the prescriptions of the European Directive NIS (Network and Information Security), which imposes on the Member States of the European Union the adoption of a series of

common measures for IT security, with the aim of defining a single strategic line between the various States of the Union against the risk of incidents damaging networks and information systems.

The critical infrastructure of the Lazio Region is fully covered by the European NIS Directive, which expressly provides for the obligation to implement an incident response plan that describes the detailed procedures to ensure an effective response to incidents involving personal data breach, as well as a recovery plan to be executed after a security incident.

Secondly, the Lazio Region is subject to the application of privacy regulations, which provide specific obligations to notify data subjects when the breach poses a high risk to their rights and freedoms. The Italian Guarantor Authority for the protection of personal data has immediately followed with particular attention the developments of the IT attack suffered by the Region and has already analyzed the first preliminary notification of data breaches sent by the Region itself, in order to assess the severity of the attack.

This attack could lead the Lazio Region to suffer not only damage to its image, but also a privacy penalty which, in the most serious cases, can reach € 20,000,000.00.