Cyber attack on Lazio Region IT systems Rapetto: "An emblematic incident, testifying to widespread vulnerability”

Dramatic, indeed apocalyptic to say the least, and the risk is that the lesson will soon be forgotten. The cyber attack that hit the Lazio Region's portal is no trivial matter. **Umberto Rapetto**, former Italian Financial Police General, the man behind a number of successful investigations into hacking and cyber attacks, an expert in computer security, university lecturer and author of several books on the subject, told SIR that “this incident is emblematic, testifying to widespread vulnerability." Italy needs to train its IT system users and raise awareness because IT is not 'Toyland', Rapetto points out.

The cyber attack that shut down all services offered by the Lazio Region exposed the flaws in its IT systems. How could security have been neglected to this extent? We preferred not to devote time and resources to a deep-rooted problem. I wrote a book in 1990 titled "*Il tuo computer è nel mirino*" (Your computer is in the firing line). 31 years have passed, but some still consider information technology as some sort of Toyland. The automation process, both in the private and public sectors, has shown that the necessary precautions to prevent disastrous repercussions are never taken. A car without brakes is not an option, nor are automation processes without adequate security measures to safeguard data and secure the functioning of essential services such as health, transport or energy. An attack of this kind makes you wonder if they had ever given it a thought. It suggests a somewhat superficial attitude. Although we are used to brash displays, we cannot expect to give hackers the finishing blow like Cassius Clay may have done in the boxing ring. The Lazio Region's knockout is emblematic, it evidences widespread vulnerability. The failure to find a solution for the past 48 hours, the fact that hackers shut down the Lazio Region's website and its IT systems shows that we have become accustomed to dealing with difficulties just as children do when they lose at football. In the meantime, everything has come to a standstill, not just health care. Calls for tenders and other services have disappeared from the portal. The same thing could happen to any other public administration. The extent of such unpreparedness is not only technical but also cultural. In fact, this form of vulnerability was not expected to impact on daily life in connection with the vaccination campaign. An incident of this kind is a matter of alarm to all people endowed with common sense. **That such an important region was hacked is a telling event.** A year ago, Anonymous stole information from the servers of San Raffaele Hospital in Milan, but it was soon forgotten. Few will remember this cyber attack in a week's time. Except for citizens currently unable to access their electronic health records. Health files are currently inaccessible. It entails also considerable repercussions under civil law, as citizens may file a complaint with the Privacy Law Authority on the grounds that their personal information processed by the Region has not been saved. **Moreover, institutional leaders such as President Sergio Mattarella and Prime Minister Mario Draghi were vaccinated in the Lazio Region. Are their data at risk now?** If hackers were only able to seize information on Covid vaccinations, they would at best have knowledge of the date of their shots. The question is whether they managed to access all medical records. Many personalities in the capital are defenceless when it comes to cyber attacks. It must be determined whether that information had been duplicated in the previous days, before being rendered indecipherable through encryption. **Could they be sold?** That is exactly the

case. Potential buyers of data relevant to pharmaceutical companies, private healthcare facilities, insurance companies and banks, which are unlikely to take out policies or grant loans to people with vulnerable health conditions, are not hard to find. **Where does Italy stand in terms of IT security compared to other European countries?** Other countries have also been hit and exposed the vulnerabilities of their IT systems. The Irish health service was hit by a cyber attack, but they were able to respond with immediate planning: they informed their citizens via Twitter, they suspended a number of activities, giving priority to ambulances and first aid. An accident can happen, but it must be foreseeable and countered with timely planning. This is a disaster, it's no trivial matter. A Region with its IT system shut down is hardly reassuring. **The National Cybersecurity Agency is due to become operational very soon** There has been a lot of hype, but only because 300 people will be hired. Except that I don't know where they are going to find 300 qualified workers. Nobody seems to worry about how to proceed. The situation is apocalyptic. The cyber attack was just a foretaste of the Banquet that could be coming. **The National Recovery and Resilience Plan encourages the implementation of telemedicine, based on a network of massive electronic data. But if security is threatened, how can this sector be expanded?** Priority should be given to the creation of an infrastructure that ensures impermeability, this entails reverting to dedicated IT networks. But first of all its users must be properly trained, and it’s important to raise awareness on this issue, which is currently lacking. There’s no time to rest on laurels. However, nobody seems to be concerned about this. Seats of power are being sought instead. **Which of those seats should be removed?** It is necessary to do an inventory of those willing to engage in the challenge and identify those lagging behind - they will be the first to be hit by hackers. **It now seems that the cyber attack on the Lazio Region portal originated in Germany.** Not quite. The geographical aspect is bizarre. The entire world is interconnected and its roots can no longer be traced geographically. So those who are being traced include anyone who pretends to be somewhere else in the world using simple techniques. The hacker could have been standing on the opposite side of via Cristoforo Colombo (the street where the Region's building is located in Rome, *Ed.'s note*). **Apparently the hacker succeeded in penetrating the account of a smart-worker.** This is to be expected. So far we have been referring to smart-working, although it would be more appropriate to call it remote-working. In fact, there is nothing smart about it. People work with the same computers that their children use to play video games or access social networks, i.e. devices lacking basic security requirements. All these things were known but nothing was done, and the tragedy is that in a week we will have forgotten all about it.

Elisabetta Gramolini