Security is an area of considerable concern to the state. Ensuring freedom from threats, or rendering such threats harmless to the normal functioning of public in stitutions, private entities, or society (ensuring security), is the primary objective of each state. There are multiple levels at which this objective should be met. Effective protection against threats allows the state to fulfil its public mission of meeting the needs of society (including its security needs) and supporting its development. One of the actors in the national cybersecurity system is local government.1 Local governments are separate decentralised authorities which perform public tasks, have their own governing bodies and the attribute of independence, and act on local or regional scales to exercise their competences in their own name and at their own responsibility. It should be noted, however, that the legislators have not provided local governments with the instruments they need to properly perform their cybersecurity tasks, as these are largely managed by State institutions. Cybersecurity is one of the domains of any country's security. It is all the more important today, and the repercussions of cybersecurity breaches affect not only public spaces but also the social sphere. Therefore, the State must respond quickly and decisively to cyberattacks, while seeking more and more advanced protection mechanisms. In their efforts to react to the increasingly frequent threats to cyberspace, the Polish legislators decided to introduce an appropriate regulation which would allow an accurate diagnosis and a sufficient response in the event of a cyberattack. The aim of the national cybersecurity system is to ensure cybersecurity at the national level, entailing the uninterrupted provision of both essential and digital services, which is to be achieved by guaranteeing a proper level of security within information systems used to provide such services, as well as by providing smooth incident-management procedures.2 The lawmakers have not provided any exact definition of the system, and have specified it only through certain statutory deter minants (including the purpose), which makes it difficult to define its overall status. The system of cybersecurity should indeed work as a system, i.e. as a group of synchronised institutional and functional components which deploy their relevant skills and know-how to perform specific tasks. This system should be composed of various cybersecurity-related entities, organised into one interconnected whole, and equipped with the appropriate tools. The current solution undoubtedly lacks coh