Cybersecurity

ATM S.A. makes all necessary efforts to ensure the continuity of the Thinx IX service in accordance with the requirements of the Act on the National Cybersecurity System of 5 July 2018 (Journal of Laws of 2018, item 1560), as well as to provide our clients with access to knowledge enabling understanding of cybersecurity threats and use of effective ways to protect against these threats in the scope related to the Thinx IX service provided.

ATM S.A. focuses on process approach and information security, and thus commitment to daily support and promotion of activities that contribute to the effectiveness of processes and adequate security of processed information, including the determination of opportunities and risks, and analysis of improvement and security activities followed by their implementation.

The company operates based on an information security management system compliant with the ISO/IEC 27001 standard. The main assumption of the system is risk assessment, including the risk of threats that have an adverse impact on the key service provision process, and ultimately the implementation of measures to minimize the likelihood of their occurrence.

The company has implemented procedures and operating principles based on international ISO/IEC 27001 and ISO 22301 standards in the areas such as:

- Operational continuity monitoring of Thinx IX service components

  The NOC (Network Operations Center) team provides non-stop monitoring (24/7/365) of operational continuity of all Thinx IX service components. The monitoring allows to manage technical problems and identify potential security breaches. The Incident Management Team ensures an appropriate response to a security incident.

- Unavailability or failure of the key service

  Action plans in case of a failure or unavailability of individual Thinx IX components have been developed and they are tested. Exchange of knowledge and experience is provided as part of the crisis management improvement.

- Division of the responsibility for individual areas of the system

  The individual roles and responsibilities assigned as part of the implementation and maintenance of the Thinx IX service are clearly defined.

- Network configuration, addressing and solution architecture

  The documentation describing the solution architecture is maintained and constantly updated.

  The carrier-class equipment used to provide the Thinx IX service has service care provided. The solution architecture minimizes the impact of any potential failure on the quality of the service provided to the client. Audits and verifications carried out by qualified engineers ensure proper configuration and minimize the risk of security errors or vulnerabilities.

- Criteria and terms of service, traffic allowed within Thinx IX

On the interface/VLAN connected to Thinx IX, the client must only have the addressing assigned by ATM S.A. (belonging to Thinx IX) configured.

The client is obliged to address the traffic directed to Thinx IX only to Thinx IX clients.

- Management of permissions and access to systems and devices

Administrative access to network devices is limited to the designated employees. Permissions are periodically verified, and their level depends on the level of knowledge and experience of the administrator.

- Anti-DDoS protection

The anti-DDoS protection is provided using Blackholing. Blackholing works in passive stand-by mode and in the event of an attack does not require configuration changes on the side of ATM S.A. The client that observes an attack on its infrastructure can broadcast the attacked prefix marked with the special BGP community attribute to the route servers of the node, and any unwanted traffic will be redirected to a device that will automatically neutralize this traffic.

- Additional security measures

The node prefix 212.91.0.0/22 is not broadcast to the Internet, therefore the possibility of a DDoS attack on devices connected to the node has been limited.

The layered security model also includes the configuration of the client solution.

ATM S.A. – as the service provider – provides a number of protection systems (both organizational and ICT). However, in our experience, the security of each network service is directly proportional to the protection of the weakest link. That is why it is so important to properly configure client devices that use the Thinx IX service.

- Redundancy

Clients should use services of two independent operators. In the event of complete unavailability of the service provided by one of the operators, the other ensures business continuity.

- Connection encryption

An important aspect is also a secure data transmission connection in the second layer of the ISO/OSI model (L2) between two locations, encrypted e.g. using the MACsec protocol.

- Link monitoring – how to detect irregularities and potential DoS/DDoS attacks?

Clients in the Atman Customer Zone application, located at https://strefaklienta.atman.pl/, have access to traffic statistics in a given time interval: annual, monthly, weekly, daily, hourly or within the range specified by the user (with one-minute accuracy). With this function, clients can track the link saturation and, if necessary, modify the configuration of their own network components or request a service upgrade. In addition, it is recommended to enable NetFlow analysis on the client side, which provides accurate information about the location, type and strength of the

attack. Security measures such as IDS/IPS, as well as monitoring the usage of individual network infrastructure components cannot be overestimated.

According to the guidelines of the Act, if you notice something worrying that is related to cybercrime, please contact us via e-mail or telephone:

- servicedesk@atman.pl
- +48 22 51 56 800

Moreover, it is possible to inform the relevant services about this fact:

1. Reporting network security incidents
2. Accepting reports of illegal content on the Internet