CYBERSECURITY AND DATA PROTECTION

The Group put the Information Security Department in place, which employs a comprehensive approach to ensuring the stability of business operations by protecting the confidentiality, integrity and availability of information and information systems.

Rusagro takes cybersecurity risks into account, particularly those pertaining to the safety of data belonging to partners, customers, employees, and shareholders. The Group employs cutting-edge security technologies, continuously enhances cyber threat management mechanisms and takes measures against leaks of personal and other confidential data.

Business-oriented information security system

After more than six years of collaboration between Rusagro Tech and Infosystems Jet JSC, a Russian information security (IS) solutions provider, the Group's shift to a business-oriented IS system was completed in 2024.

Focus area of the IS system

- Applied information security systems and cryptographic protection
- Monitoring of and response to incidents
- Network infrastructure protection
- Development of IS architecture and methodologies

History of development

2017

Stage 1

Comprehensive IS audit and development of a long-term IS development strategy

The primary IS survey covered the head office and production sites of all Rusagro Group's business segments: Meat, Oil and Fats, Sugar and Agriculture. To measure the IS level, Rusagro adapted the capability maturity model integration (CMMI), which allows for a unified assessment of the maturity level of IS processes in different divisions of the agroholding.

The strategy included various control mechanisms such as annual GAP-analysis of changes in the maturity level of IS processes and an assessment of the required resources, which takes into account the specifics of the Company's various business segments.

Result

The five-year IS strategy was fully implemented.

The approved assessment method indicates that the IS has attained a degree of maturity that is nearly at the maximum.

Audit of IT infrastructure

16
KEY INFORMATION SYSTEMS

500+
SERVERS

4,700
AWS

80
IS CONTROLS

2018–2022

Stage 2

Assessment of processes and upgrade

Infosystems Jet conducted the annual assessment of the IS process maturity across Rusagro Group, which also provided a comparison of the results from the previous and current years.

The work covered not only the corporate segment of the IT infrastructure, but also the process segment, including industrial automated systems that support the operation of production chains.

15
SITES

16
INFORMATION SYSTEMS

4
AUTOMATED PROCESS CONTROL SYSTEMS

Result

The Company deployed its own security operation centre (SOC) to identify and respond to IS-related incidents. The security information and event management (SIEM) was also rolled out in all business segments of Rusagro Group with 800 sources connected. The existing ITSM system was used as a foundation for the security incident lifecycle management system and the incident management process, which necessitated the development of related documents and regulations, the introduction of a reporting system and streamlining of the security incident-related interaction with top management. The rolled-out analytics platform allowed for the analysis of large volumes of data for IS incident investigations, resulting in about 400–450 confirmed incidents per year.

Privileged user control and web application security systems were put in practice.

A process of handling IS-related requests to the IS Department from the Company's employees was set up.

In addition to assessing the maturity of IS processes, the technical security of the Company's external IT perimeter and its internal infrastructure, including various information systems, is subject to the annual analysis. Based on the findings, we eliminate the vulnerabilities that have been found, thus greatly raising our Company's overall security level.

The penetration test automation platform was put in place to simulate the hacker's logic and behaviour using machine algorithms, which allow for cutting-edge testing of the security of the organisation's infrastructure, detection of vulnerability points in the IT infrastructure and user behaviour (at the end of 2022, the vendor left Russia, rendering the system unusable).

At the end of 2022, the Company involved a contractor to roll out the process of monitoring and blocking fraudulent resources on the Internet that abuse Rusagro brands (Brand protection service), as well as monitoring and responding to leaks of user accounts, and analysing media, shadow forums, and communities for leaks of confidential information.

2023

Stage 3

Transition of the Group to the IS Health Model assessment system and annual audit of information security

Moving to a system of qualitative and quantitative indicators was the next step in the Company's development.

The IS Department followed the overall business principle in implementing the transition to the IS Health Model assessment system.

The model is based on IS process management, linking IS and IT metrics to business objectives. It is used to identify operational and strategic level indicators to make the right management decisions and to capture the threshold and target states of the indicators.

Result

The introduction of the system allowed for better interaction with related functions through the introduction of joint performance indicators.

The imported security orchestration, automation and response (SOAR) system was substituted with the button incident response functionality, which enables timely and safe (with second-hand confirmation) response to Internet attacks, phishing mailings, etc. The SOAR system is used to organise the collection and enrichment of data on the Company's assets (for IS purposes), including the register of published web applications. The SOAR system is integrated with 18 different third-party systems to realise the said functions. The use of the system has significantly reduced the response time to IS incidents.

Since the transition to the new IS maturity assessment model, the Health Model, the development of IS processes and systems has continued. The key highlights of this stage are listed below:

Works were carried out to expand the incident monitoring area of the SIEM system (the total number of sources increased to about 1,500) and to develop internal logic (about 400 detection rules were developed over the years of operation).

IS requirements are integrated into the process of information systems implementation projects. Before putting the system into operation, it is mandatory to check the system components for critical vulnerabilities, set up monitoring of IS events in the SIEM system, work out the issues of data backup, recovery plans in case of failure, etc.

1. Audit of SIEM correlation rules and recommendations for their improvement
2. Web penetration testing and internal penetration testing, Testing of Wi-Fi networks
3. Analysis of the possibility of unacceptable events for the business and development of recommendations
4. Analysis of the system of personal data processing and protection

Continuous cybersecurity initiatives

Training and education of employees

Implementing regular information, training and awareness-raising activities for employees on cyber hygiene compliance to ensure sustained immunity to external disruptive influences from malicious actors.

IS architecture

This provides a structured approach to managing the protection of systems and services to meet regulatory and IS requirements to ensure business resilience in the face of today's cyber threats.

Legal compliance

Audits were initiated and are being completed to assess the Group's compliance with regulatory and legislative requirements for the replacement of foreign-made solutions with domestic ones as part of the implementation of Decree of the President of the Russian Federation No. 250 dated 1 May 2022 'On Additional Measures on Ensuring Information Security of the Russian Federation', meeting the requirements of Federal Law No. 152-FZ 'On Personal Data' dated 27 July 2006, Federal Law No. FZ-187 dated 26 July 2017 'On the Security of Critical Information Infrastructure' and Federal Law No. FZ-98 dated 29 July 2004 'On Commercial Secrets'.

IS risk management

A methodology for assessing IS risks based on the cost of downtime of business systems and processes was introduced, thus ensuring reasonable sufficiency in decision-making.

Vulnerability management

Work is underway to build a vulnerability management process: related regulations have been approved, and the process of annual full scanning of the Company's external perimeter and internal infrastructure for vulnerabilities has been implemented. The results of the scanning are used to eliminate identified short-comings in co-operation with other directorates.

IS methodology

Ensuring a highly dynamic and flexible system of internal regulations.

Proactive protection

Integration with a publicly accessible database of compromise indicators that compiles information on malicious IP addresses, URLs, domains, etc., is used for proactive threat protection. Coupled with SOAR system, a list of threat indicators is used to automatically generate blocking policies on Fortigate firewalls. This approach prevents a large number of potentially dangerous external calls and increases the security of the Company's perimeter.