Radosław Zawierucha
Mgr
PKP Informatyka Sp. z o.o.
radoz72@gmail.com

DOI: 10.35117/A_ENG_23_06_07_08_04

Building assumptions of a research and development center for the monitoring of railway automation.

Abstract: The paper describes the initial analysis of the construction of the Research and Development Team (R&D) in the area of cyber security with particular emphasis on data analytics from railway automation systems. The study addresses organizational, technical and business issues. Due to the own experience of the last years of work, this paper is constructed from the operational and organizational perspective of PKP Informatyka. Hence the assumed substantive context, formal, organizational and legislative environment of the expected domain of operation of the research and development team under development. The work describes the tasks, research methods, competences and products of the research team. The project itself is of a project nature - it provides for certain assumptions, adopts selected methodologies and assumes the achievement of specific results.

Keywords: Research and Development Team; Cybersecurity; Railway Automation Systems

Introduction

The subject of this paper is a preliminary analysis of the establishment of a Research and Development Team (R&D Team) in the field of cybersecurity. The study addresses organizational, technical, and business issues. Due to the author's professional position and personal experience in recent years, this work is constructed from the operational and organizational perspective of PKP Informatyka. This determines the assumed substantive context, formal, organizational, and legislative environment of the anticipated domain of the developed research and development team. The undertaking itself is project-based—it anticipates certain assumptions, adopts selected methodologies of action, and aims to achieve specific results.

Definitions

- **Research and Development Team (R&D Team):** A research and development team in the field of cybersecurity.
- **Basic Research:** Original experimental or theoretical research work undertaken primarily to acquire new knowledge about the foundations of phenomena and observable facts, without aiming at direct commercial application.
- **Applied/Industrial Research:** Research aimed at acquiring new knowledge and skills to develop new products, processes, and services or to introduce significant improvements to existing products, processes, and services; this research includes the creation of components of complex systems, the construction of prototypes in a laboratory environment or in an environment simulating existing systems, especially for evaluating the suitability of specific types of technology, as well as the construction of necessary pilot lines in these studies, including obtaining proof in the case of generic technologies.
- **CSIRT GOV:** Computer Security Incident Response Team CSIRT GOV led by the Head of the Internal Security Agency.

- **CSIRT MON:** Computer Security Incident Response Team operating at the national level, led by the Minister of National Defense, functioning within the Cyber Defense Forces Component Command.
- **CSIRT NASK:** Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network – National Research Institute based in Warsaw.
- **Research and Development Activity, R&D:** Research and development activity encompasses creative work undertaken systematically to increase the body of knowledge. The term includes three types of activities: basic research, applied/industrial research, and development work. For a software development project to be classified as R&D, its completion must result in scientific or technical advancement, and the project's goal must be to eliminate an element of scientific or technical uncertainty in a systematic way.
- **Innovation:** The implementation of a new or significantly improved product (good or service) or process, or a new organizational method; new processes or organizational methods are implemented when their actual use in the company's operations begins.
- **ISAC-Kolej:** Information Sharing and Analysis Center.
- **Laboratory:** Infrastructure enabling the launch of a test environment tailored to conduct the most demanding tests, research, and development work in the field of IT/OT security.
- **PoC:** Proof of Concept, a prototype version of the target solution, demonstrating its applicability in a limited scope or with narrowed functionalities.
- **Technology Readiness Level (TRL):** A method of assessing the advancement of research and development projects. It delineates nine levels of advancement, assigned respectively to basic research (level I), industrial research (levels II-VI), and development work (levels VII-IX). Level IX of a research and development project signifies the creation of a ready, production-ready innovative solution.
- **Development Work:** Acquiring, combining, shaping, and utilizing currently available knowledge and skills from science, technology, and business activities, as well as other knowledge and skills for production planning and creating and designing new, altered, or improved products, processes, and services, excluding work involving routine and periodic changes introduced to products, production lines, manufacturing processes, existing services, and other ongoing operations, even if such changes are improvements. Development work does not include routine and periodic changes introduced to products, production lines, manufacturing processes, existing services, and other ongoing operations, even if such changes are improvements.
- **State of the Art:** The highest commonly and publicly known level of advancement in technical work, device type, or field.
- **Competence Teams:** Teams of experienced employees with appropriate competencies and qualifications specialized in a specific field.

Characteristics of Recipients and Stakeholders

- **Project Stakeholders**
  - Entities operating in the railway market in Poland – carriers, infrastructure operators, manufacturers.
  - Business owners;
  - System custodians;
  - End customers of the provided services – business entities.
- **Project Recipients/Users**
  - Networks and scientific institutes;

- Research and development teams;
- CSIRT teams;
- CERT PKP Informatyka;
- SOC PKP Informatyka;
- Security teams of the PKP Group;
- Competence teams;
- Companies of the PKP and PKP PLK groups;
- System administrators and users;
- CERT and SOC teams of other entities.

Purpose of Establishing the Research and Development Team (R&D Team)

The purpose of building the Research and Development Team is to create research potential for developing and implementing innovative solutions in the field of cybersecurity. Initially, the task of the R&D Team will be to gather knowledge about the latest trends and the state of science, as well as to respond to emerging new challenges and customer needs. Based on this, the R&D Team will identify and propose applications of innovative cybersecurity solutions in the infrastructure of the parent organization and in the infrastructure of service recipients.

To increase knowledge resources and utilize them to create new innovative applications, the tasks of the R&D Team will include, among others:

- Review and analysis of previously used solutions;
- Testing and researching innovative solutions;
- Establishing cybersecurity laboratories;
- Evaluating innovative solutions.

One of the identified initiatives for the R&D Team is the creation of cybersecurity laboratories. They will be used for research, training, and as a tool for promoting research and development in the field of cybersecurity.

Based on the research work of the Research and Development Team, the following will be carried out:

- Planning the implementation of new solutions;
- Implementing new solutions.

The Research and Development Team will also conduct work that meets the formal requirements of R&D activities, ultimately aiming to build solutions with a technology readiness level of IX. Activities of this nature include:

- Innovative research;
- Building innovative tools and solutions;
- Developing innovative frameworks and research methodologies.

Additionally, the Research and Development Team will be involved in promotional activities, the process of building competencies, and establishing networks of cooperation with institutions and research centers.

Benefits and Risks of Establishing the R&D Team

Identified benefits of building the Research and Development Team include:

- Centralization of knowledge about cybersecurity solutions;
- Improvement in the quality of cybersecurity services provided;
- Enhancement of cybersecurity levels;
- Assessment of the effectiveness of existing solutions;
- Development of an agile system to respond to customer needs;
- Creation of innovative solutions;
- Introduction of new cybersecurity products;

- Establishment of collaborations with research and development units, academic institutions, and R&D teams within the railway subsector and IT security area;
- Capability to provide research and analytical services in cybersecurity within the railway subsector;
- Co-financing of the R&D team's work through grants by conducting formal R&D processes.

Identified risks associated with building the Research and Development Team include:

- Inability to ensure and acquire appropriate competencies within the team;
- Improper assignment of roles within the R&D team;
- Failure to develop innovative solutions;
- Lack of development of reportable and transparent KPIs;
- Suboptimally designed internal collaboration and with external entities;
- Excessive maintenance costs of the team not offset by operational revenues.

Tasks, Services, and Products Produced by the R&D Team

Within the defined objectives of establishing the Research and Development Team, four primary areas of tasks and services have been identified:

- **Analytical Activities**
  - These may involve system analysis and vulnerability assessments. The goal of vulnerability analysis is to generate knowledge about vulnerabilities, associated threats, and to develop countermeasures.
  - Reviews and tests of previously implemented solutions will also be conducted.
  - The R&D team will analyze new IT solutions in the cybersecurity domain to assess their quality and applicability in the railway subsector.
  - Examples of products and activities:
    - Incident analysis reports;
    - Penetration test reports;
    - Opinions and recommendations on the application of new solutions within the Company.
- **Prototyping and Implementation Activities**
  - Upon positive evaluation of solutions, the R&D team will develop implementation plans and create Proof of Concepts (PoCs).
  - Security systems approved by clients will be implemented and configured.
  - Implementation activities will also include security tests and consultations.
  - *Examples of products and activities:*
    - Implementation plans;
    - Deployment of cybersecurity systems;
    - Client consultations;
    - Project documentation.
- **R&D Activities**
  - Establishment of a cybersecurity laboratory.
  - The R&D team will utilize knowledge, data, and experience gathered from other activities to conduct comprehensive research and development work.
  - Conducted analyses will form the basis for fundamental research, allowing the identification of innovative solutions to detected research problems.
  - Technological research will aim to bring solutions to Technology Readiness Level IV, i.e., readiness for laboratory testing.
  - Ultimately, innovative solutions developed by the R&D team will be advanced to production level and subsequently implemented for clients.
  - *Examples of products and activities:*

        - Cybersecurity laboratory;
        - Innovative frameworks for security incident management;
        - Innovative tools, e.g., automation tools or log analyzers;
        - Innovative applications.
- **Promotional and Educational Activities**
    - The Research and Development Team should support CERT and SOC teams in tasks related to promoting cybersecurity knowledge within railway entities.
    - Workshops and training sessions will be conducted based on the knowledge produced.
    - Additional products of R&D work will include articles, publications, and bulletins promoting the Company's services and advancing the state of knowledge.
    - The R&D team will also be responsible for collaboration with scientific institutions, other R&D organizations, and research networks.
    - *Examples of products and activities:*
        - Research publications;
        - Informational bulletins;
        - Workshops and training sessions promoting security within the Company;
        - Training on the use of positively evaluated technologies for clients.

Roles and Competencies of the Research and Development Team

The tasks undertaken by the Research and Development Team require building a team with interdisciplinary competencies. Due to the nature of R&D work, it is essential to combine extensive professional experience, theoretical knowledge, as well as analytical skills and experience in R&D projects.

Based on these requirements, the following positions have been defined within the R&D team:

- Research and Development Team Coordinator;
- Security Analyst;
- IT Architect;
- Implementation Engineer;
- Security Tester.

For each role within the Research and Development Team, the following competencies have been identified:

- **Research and Development Team Coordinator:**
    - Experience in planning R&D processes;
    - Ability to write project and technical documentation, as well as reports;
    - Experience in data aggregation, analysis, and visualization;
    - Knowledge of PRINCE2 or PMI PMP methodologies (project and portfolio-level reporting);
    - Ability to write scientific articles, reports, reviews, and summaries;
    - Ability to conduct pre-implementation analyses and design business processes;
    - Ability to prepare research proposals and funding applications/offers;
    - Knowledge of SQL;
    - Proficiency in using project tools;
    - Familiarity with JIRA and Confluence tools.
- **Security Analyst:**

- Advanced knowledge in areas such as network technologies, operating systems, security technologies and solutions, IT standards, norms, and methodologies, and conducting penetration tests;
- Knowledge and experience in configuring and administering Windows and Linux/Unix operating systems;
- Practical knowledge of network threats and security systems and technologies: IDS, IPS, Firewall, WAF, SIEM, EDR, DLP, antivirus software, sandbox, vulnerability scanners, anti-spam systems;
- Proficiency in protocols: HTTP, HTTPS, SSH, FTP, SMTP, IMAP, POP, SNMP, WMI, syslog, NTP, DHCP, DNS, CIFS, NFS, etc.;
- Knowledge of cryptographic issues;
- Ability to analyze malware;
- Experience in conducting post-intrusion analysis;
- Advanced knowledge in conducting penetration tests;
- At least 2 years of experience in IT security roles;
- Practical knowledge of security measures used in IT systems and methods of conducting attacks on IT systems, defense strategies, and tools for event analysis and incident detection.

- **IT Architect:**
  - Knowledge of UML notation;
  - Analytical thinking and problem-solving skills;
  - Ability to model solution architectures;
  - Knowledge of IT/OT architecture and security (e.g., database modeling, component division, framework application);
  - Experience in programming interfaces in languages such as C#, Python;
  - Proficiency in using project tools;
  - Familiarity with JIRA and Confluence tools;
  - Knowledge of architectural patterns for building solution architectures;
  - Practical knowledge of LAN/WAN networks.
- **Implementation Engineer:**
  - Knowledge of containerization and CI/CD concepts;
  - Experience working with virtualized environments;
  - Good understanding of IT solutions (operating systems, server systems, telecommunication services);
  - Experience in managing MS SQL Server, SharePoint, Exchange;
  - Knowledge of SQL;
  - Proficiency in scripting languages (e.g., Python, bash, Perl);
  - At least one year of experience in implementing IT systems.
- **Security Tester:**
  - Proficiency in TCP/IP protocols and protocols such as HTTP, HTTPS, SSH, FTP, SMTP, IMAP, POP, SNMP, WMI, syslog, NTP, DHCP, DNS, CIFS, NFS,
  - Minimum of 2 years working in positions related to IT security testing;
  - Familiarity with penetration testing methodologies (OWASP, WASC-TC, PTES, OSSTMM);
  - Ability to write technical reports;
  - Knowledge of cryptographic issues;
  - Understanding of hardware testing using reverse engineering techniques;
  - Ability to conduct security testing of mobile applications and APIs;
  - Experience with physical security testing;
  - Proficiency in scripting languages (e.g., Python, Bash, Perl);

- Knowledge and experience in using Windows and Linux/Unix operating systems..

Methodology of the Research and Development Team

Research Tools. Within the tasks and objectives identified for the R&D Team, the use of appropriate tools will be essential. According to the current state of technology in the field of cybersecurity research, the following are utilized:

- **Sandboxes**: Mechanisms for running computer programs in environments isolated from the rest of the system. These tools are used to execute potentially dangerous programs or those from untrusted sources.
- **Virtual Hardware Platforms**: Virtualization is a method of creating a separated layer of computer hardware using software. It allows the components of a single computer—such as processors, RAM, storage, and more—to be divided into multiple virtual devices, commonly known as virtual machines (VMs). They are used, among other things, to run sandboxes.
- **Physical Hardware Platforms**: PCs, servers, network devices.
- **Network Traffic Analyzers**: Software for analyzing network traffic.
- **Development and Design Tools**: Computer programs used for creating, designing, modifying, and testing software (e.g., compilers, debuggers).
- **Domain-Specific IT and Industrial Automation Systems**: Specialized IT/OT systems used in the railway sector.
- **Access to Knowledge Bases**: Utilizing available information sources and know-how.

Simultaneously, the verification, updating, and expansion of the tool list will be among the key tasks of the R&D Team.

Research Process

In the core tasks of the R&D Team, methodologies developed by SOC and CERT will be employed. The foundation for the R&D Team's activities will be frameworks and metrics for CSIRT teams, such as the FIRST CSIRT Services Framework and NIST information protection metrics.

The basis for conducting research and development work in the R&D Team is adherence to criteria defining R&D activities, namely:

- **Novelty Criterion**: In the business sector, R&D projects should lead to results new to the company and solutions not previously used in the industry. This includes generating knowledge for new products or processes.
- **Creativity Criterion**: An R&D project is based on original, non-obvious concepts and hypotheses.
- **Unpredictability Criterion**: In the early stages of research, it's impossible to precisely determine the outcomes and costs. This means that prototypes developed during R&D aim to verify hypotheses rather than obtain technical or legal certifications.
- **Methodical Criterion**: Research and development activities are conducted in a planned manner, with precise documentation of the process and its results.
- **Reproducibility Criterion**: The results of an R&D project should potentially allow other research teams to utilize the generated knowledge or solutions.

In the R&D process, it's also crucial to select appropriate metrics that enable precise evaluation of the effectiveness of developed solutions.

For example, in the area of automatic malware detection, metrics typical for classification problems in machine learning are used (such as precision, recall, and F1 score). In assessing the effectiveness of firewall rule sets, metrics from software development are

applied, such as cyclomatic complexity or Halstead complexity, as well as unique metrics measuring, for instance, the level of rule interdependence.

Collaboration Models with the Research and Development Team

Collaboration Model with SOC and CERT Teams. Collaboration with SOC and CERT will be based on the exchange of information and experiences in the IT and network domains. This model also includes conducting research commissioned by these teams. Tasks related to cybersecurity will be carried out, and their results will be presented in meetings summarizing the R&D work.

Collaboration Model with KPRM, MON, ABW, NASK PIB. Collaboration with authorities responsible for cybersecurity (CSIRT GOV, CSIRT MON, CSIRT NASK) and public authorities in the Republic of Poland will proceed according to the principles outlined in the Act of July 5, 2018, on the National Cybersecurity System, as well as in line with Resolution No. 125 of the Council of Ministers dated October 22, 2019, on the Cybersecurity Strategy of Poland for 2019-2024.

Collaboration Model with the Railway Institute, NASK, ISAC-Kolej, Networks, and Other Research Entities. Collaboration with ISAC-Kolej will be based on the principles established in the agreement to create ISAC-Kolej concluded by the Company. The Research and Development Team will report identified issues that increase the risk of cybersecurity incidents and support the process of developing policies, procedures, and standards tailored to the needs of the railway subsector.

In R&D work, the Research and Development Team may utilize the cybersecurity and railway subsector research expertise of the Scientific and Academic Computer Network National Research Institute (NASK), the Railway Institute, and research networks under currently valid or newly concluded agreements. Simultaneously, the R&D Team may provide services to the aforementioned institutions, for example, through joint participation in grant programs.

Conclusion

Critical infrastructure is essential for maintaining vital social functions and ensuring the safety and protection of citizens. Damage, destruction, or disruption of such infrastructure due to natural disasters, terrorism, failures, criminal activities, or malicious behaviors can have a significant and negative impact on the security and well-being of citizens. Critical infrastructures (CI) are indispensable for guaranteeing basic economic and social functions to the citizens of the European Union (EU). The services they provide, combined with their cross-border nature and interdependencies, make critical infrastructures increasingly vulnerable to various threats, not only natural and accidental but also deliberate. With technological advancement and deep interconnections, the landscape of potential threats within the EU territory is changing and evolving, paving the way for greater susceptibility to them. One type of threat is cyberattacks, which, in the event of a "cascading failure," sequentially damage the network. Failure of a single component of a given critical infrastructure can lead to the collapse of its other parts and ultimately to severe damage to the entire network. Additionally, the growing dependence of CI on foreign technological advancements (using and implementing IT solutions from outside the EU, mainly from China) constitutes another factor of complexity and vulnerability to external attacks and damages.

The current protection of critical infrastructures is regulated by Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (the so-called ECI Directive), transposed into the legal systems of individual member states. In Poland, this was achieved through the adoption of the Act of October 29, 2010, amending the Act on Crisis Management. The area of cybersecurity

is addressed by the EU NIS and NIS2 directives. The NIS Directive was adopted on July 6, 2016, and is the first European law on cybersecurity. The directive imposes a range of obligations on member states, requiring them to establish specific institutions and introduce cooperation mechanisms. In Poland, its provisions are implemented by the Act on the National Cybersecurity System (NCS) of August 28, 2018. Currently, the implementation of the provisions of the NIS2 directive into Polish legislation is awaited through an amendment to the NCS Act, increasing the obligations and tasks of entities in terms of protection against cyber threats.

The implementation of the discussed tasks requires actions by the relevant institutions in accordance with the presented cooperation model.