SMART GRID CYBER SECURITY ROADMAP

Miguel AREIAS
EDP – Portugal
miguel.areias@edp.pt

Bruno GARRANCHO
Logica – Portugal
bruno.garrancho@logica.com

Paulo MONIZ
EDP – Portugal
paulo.moniz@edp.pt

Pedro RODRIGUES
EDP - Portugal
pedrodias.rodrigues@edp.pt

ABSTRACT

This paper addresses the roadmap to strengthen security at EDP critical information infrastructures, from organizing the security operational services, architectural strengthen and staff awareness at EDP Distribuição, to the advances of the Portuguese Smart Grids project and the achievements of the InovGrid cyber security working group with focus on the new critical infrastructure, technological vulnerabilities and threats, on the grid reliability and resilience in the context of increased number of sensors, decentralized processing and holistic enterprise data management. Considering the operational efficiency and business competitiveness challenges which result in new architecture evolutions, in particular the integration of cloud computing, it also covers the involvement in international R&D projects, and on the contribution to and adoption of security standards and interoperability guidelines.

INTRODUCTION

EDP-Energias de Portugal, as a leading group in renewable generation and electrical distribution with operations in Europe and in the Americas, that recently became world leader of the Dow Jones Sustainability Index, is deeply committed to its InovGrid Programme in the emerging environment of smart grids.

With a coordinated multiple dimension focus on advanced metering, customer involvement, intelligent grid management, distribution automation, micro-generation integration and new generation telecommunications, cyber security is at the core of the company´s business sustainability plan and of the InovGrid Programme.

With Security being a priority for top management, EDP has performed a security assessment to its critical infrastructure in order to understand security vulnerabilities and also to define a solid roadmap to protect its critical systems against threats from a variety of external and internal sources. As a result of that assessment, EDP has promoted an on-going cyber security program that addresses several areas like security policies, security monitoring, network control access and security awareness initiatives. The main objective for this program is not only to improve protection of the current infrastructure but also to provide the security basis for new architectural and operational evolutions as a result of new paradigms for the electric power distribution sector.

Adopting a strategy based on the premise that security will be more effective when planned and designed at earlier phases, EDP has decided to create a Cyber Security Group whose mission is to address the new challenges brought by the new generations of power grids, where remote terminal units, with complex computational, communication and sensing capabilities, will spread over the entire infrastructure and, somewhat, enabling malicious individuals or groups to conjure cyber attacks. The purpose of this group is also to integrate the results from past and on-going security projects, as well as recent research results and technologies, in order to understand the potential threats from the new architectural paradigms and define, at design phase, requirements that will strengthen the security of the infrastructure.

Defining and ensuring Security for such complex and innovative architectures like Smart Grids is a significant endeavor, and demands a structured approach, based on Public Security Standards and best practices that will enable a better understanding of the risk and security maturity of the EDP organization, as well as guiding future action and investments.

BEYOND PERIMETER DEFENSE

Understanding that Cyber Security has become an emergent concern for our societies, especially due to several problems experimented in recent situations where some services have been disrupted due to successful cyber attacks or misuse of information systems [1], EDP has decided, in 2008, to perform an assessment of its critical infrastructure. The main idea was to challenge the implemented security architectural paradigms, based in a perimeter defense strategy, and find vulnerabilities that could expose its systems and jeopardize the service being provided. The decision was not simple due to the fact that the security architecture in place has successfully resisted several external attacks and the fact that corporations don’t usually like to admit that their infrastructure could have vulnerabilities. Nevertheless, the initial step was taken and the assessment has proven that the perimeter security was, in fact, well implemented, despite some weakness identified, namely regarding security monitoring and resilience against inside threats.

As a result of the assessment, EDP has decided to promote a cyber security program whose main objective was to mitigate the identified vulnerabilities and also to prepare the Critical Infrastructure to the new Security challenges brought by Smart Grids. The program is divided in four major projects: security policies definition; network access control; security operations center and security awareness.

The first project, related with Security Policies, is the cornerstone of the new security strategy for EDP. The goal of this project is to define security policies, metrics and requirements, which will be the base for future architectural evolutions, keeping in mind that the main objective is to evolve from a perimeter defense to a depth defense strategy. In the scope of this project lays also the identification of security metrics to define security events that should be monitored. Others aspects like network access policies and security architecture references are also included in the results of the project, which should serve as the first step in the evolution of all Smart Grids projects.

The network access project fully embodies the defense-in-depth strategy in opposition to the perimeter approach. In the perimeter strategy perspective all the threats come from external networks, with all internal infrastructures being considered secure and used only by trusted people. However, in such large infrastructures, considering not only IT architecture but also distinct physical buildings, it is hard, if not impossible, to effectively control all accesses those secure areas, especially in remote locations. To face this problem, network access control is vital, ensuring that only trusted equipments with the appropriate configurations are allowed to connect to the network. This project aims to control these logical accesses to Critical EDP Infrastructures.

The major project, that will dramatically change the way security is handled in the organization, is the Security Operation Center (SOC) implementation. The security operation center combines people, technology, processes and procedures in order to provide a global IT infrastructure inventory and surveillance, correlating security events and centralizing the security monitoring, analysis and response in a 7x24 basis, as depicted in Figure 1.

The core of a Security Operation Center is the Security Information and Event Management (SIEM) platform. The SIEM collects data from a myriad of sources, like servers, firewalls or routers, correlating and analyzing the events according to the security policies defined, in order to generate alerts for a console operator. Adopting a SOC dramatically improves the organization's ability to rapidly recognize and respond to malicious information security events. It can also assist in ensuring that organizations leverage the full value of the often expensive investment in security technology and meet most of regulatory compliance requirements [2,3].

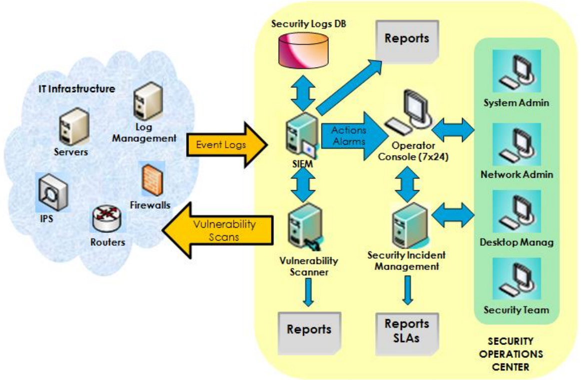

Figure 1 – Security Operation Center

The last project is about security awareness. Since security cannot be dissociated from cultural behavior, it is crucial to create and promote a security culture, from the application end-users to system administrators, through top management or procurement people. Information security should be regarded across all organization and different roles should have different concerns regarding security, so it is important to build specific awareness actions to different audiences in order to promote a security culture through the organization.

CYBER SECURITY GROUP

In parallel with the previously described ongoing security projects, a Cyber Security Group was created with the mission of providing standards, solutions, tools and security metrics to protect EDP's critical information infrastructure from attacks and erroneous actions from a variety of external and internal sources, defending customers and the society in general from malicious actions that could affect our lives.

This Group is comprised by information security and business experts from EDP, systems experts from the major partner – Logica Portugal, and representatives from component manufacturers – EFACEC and CONTAR. The idea to include all these elements is again the result of understanding that security is transversal to all areas and that is not worthy to implement strong security mechanisms at the component level, if these mechanisms were not designed and developed with a vision of the overall solution. Following an isolated approach can result in expensive solutions, can jeopardize the functionality of the systems and, most importantly, reducing overall security.

Without diminishing the overall mission statement, currently the group is mainly focused in the Smart Grid project, addressing security challenges brought by the new generations of power grids. One relevant aspect is that the group is performing what EDP believes to be the best approach to implement security, which is to plan and think security at a design phase. This approach leads to better and less expensive technical solutions.

SMARTGRIDS SECURITY APPROACH

Design security requirements and solutions is not an easy task, especially when it comes to such complex, innovate and dynamic architectures like the one depicted in Figure 2. Smart Grids encompass energy boxes that are installed at customer houses, equipments at the power transformers and substations, different layers to provide communications services, databases, commercial and technical applications, real time requirements and a myriad of functionalities [4]. The dynamic comes from the fact that this project is at prototype phase and the technologies that best fit the project's goals are always changing, as we can observe by the evolution in communication mechanisms.

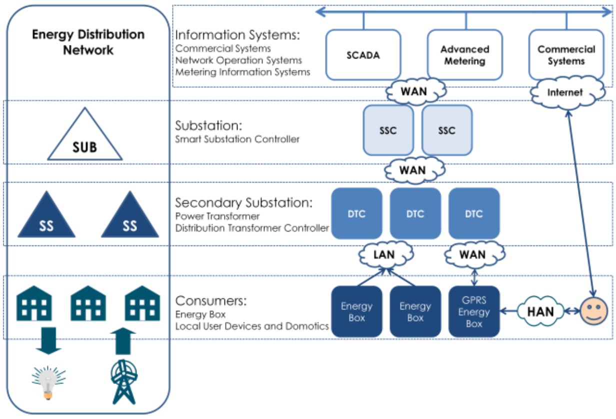

Figure 2 – InovGrid Architecture

To accomplish the group mission the first step was to create security requirements to be included in the Smart Grid project documentation. The security requirements, structured by architectural modules and security themes, were included in the functional specifications of the project since its second phase, in 2009. During 2010, the group did also participate in the design and proposal of technical solutions for security controls mechanisms at different architectural levels, collaborating in the definition of technical requirements.

To face the overwhelming task of writing security requirements for the Smart Grids, the group decided to follow a structured approach, assigning the pertinent requirements to each architectural module to identify dependencies and correlations. This initial step allowed the Group to guarantee that, when discussing the specification with each technical team, the holistic vision is always present, so that the security aspects of the entire solution are not neglected when defining the requirements specific to each module. The architecture division has the advantage to allow a specific focus and thorough discussion of each component, with the participation of everyone responsible for that development.

Regarding the security areas division, the group adopted the approach proposed by the ISO 27002. In this framework we can find security divided in areas like access control, physical security or human resources. Some of the controls specified in each area could be applied to specific architecture components because most have a technological solution, however the group also wrote requirements related with organization operations. As an example we have requirements to create and update the inventory of assets.

SMARTGRIDS AND THE CLOUD

Through Smart Grids it is also possible to incorporate new sustainable energies such wind and solar generation, and interact locally with distributed power sources, or plug-in electrical vehicles. To support this new paradigm, Smart Grids will boost a widespread use of intelligent data sensors on the grid improving both energy efficiency and demand response. All those equipments will require substantial computing power for control and management and cloud computing will provide substantial cost benefits.

Using real time information through cloud computing gives clients the possibility to understand how energy is consumed and what they can do to reduce that consumption. On the other hand, on the utility side, providing information about benefits can foster incentives for consumption adjustments and, as a result, reduce demand during peak usage periods.

Regarding energy efficiency, using clouds allow us to reduce the computational power of Data Centers through efficient application management, increasing the efficiency of servers, power supplies and cooling systems. However, the risks incurred by the migration of such critical activities to an unprotected cloud environment would be unacceptable [5, 6].

To address this problem EDP joined a European Consortium, supported by the European Commission Framework 7 Programme and lead by IBM, constituted of 14 partners from 7 different countries to produce a more secure and resilient cloud infrastructure called

TCLOUDS (Trustworthy Clouds). TCLOUDS intends to build a resilient Internet platform by designing architecture and prototypes for a federation of trustworthy infrastructure clouds using an advanced Cloud-of-clouds middleware to address security and resilience of this platform.

In this project EDP will prototype how these control, planning and transaction systems can be migrated to a cloud infrastructure while increasing their resilience and intrusion tolerance. This will be a combination of smart metering and a web-based real-time status and energy consumption control system that enables public utility providers to monitor and efficiently control a public lighting network.

FUTURE CHALLENGES FOR THE GROUP

The Cyber Security Group is currently developing studies on authentication methods, as well as non-repudiation and integrity solutions for the information flowing through the network. Since the functional capabilities of all architecture components are yet to be decided, and the technologies are constantly evolving, the definite solution has not been settled.

As participants in the TCLOUDS Consortium, the Group has to guarantee that the experience acquired during the InovGrid project is incorporated in the project’s initiatives. Furthermore, security concerns and technical requirements defined for the current InovGrid components have to be transposed to the new architecture element – the cloud. This means incorporating, in future versions of the InovGrid concept, the work results from TCLOUDS and other research conducted by the group members in collaboration with academic entities.

REFERENCES

[1] U.S.-Canada Power System Outage Task Force, Final report on the August 14, 2003 blackout in the United States and Canada, available at https://reports.energy.gov/B-F-Web-Part1.pdf, April 2004.

[2] Dwen-Ren Tsai; Wen-Chi Chen; Yin-Chia Lu; Chi-Wen Wu, "A Trusted Security Information Sharing Mechanism" *on the 2009 IEEE International Carnahan Conference, 43rd Annual Conference,* Zurich, Switzerland

[3] Renaud Bidou, “Security Operation Center Concepts & Implementation”, available at http://www.iv2-technologies.com/ SOCConceptAndImplementation.pdf

[4] Moslehi, K; Kumar, R, 2010, "A Reliability Perspective of the Smart Grid", *Smart Grid, IEEE Transactions* vol. 1, issue 1, 57.

[5] Kaufman, L.M. 2010, "Can Public Cloud Security Meet Its Unique Challenges?", *Security & Privacy, IEEE,* vol. 8, issue 4, 55-57.

[6] J.W. Rittinghouse and J.F. Ransome, “Cloud Security Challenges”, *Cloud Computing: Implementation, Management, and Security*, CRC Press, 2009, pp. 158–161