International Journal of Information Systems for Crisis Response and Management
Volume 10 • Issue 2 • April-June 2018

Cyber Security Vulnerability Management in CBRN Industrial Control Systems (ICS)

Roberto Mugavero, Department of Electronic Engineering – University of Rome "Tor Vergata", Rome, Italy
Stanislav Abaimov, National Inter-Universitary Consortium for Telecommunications, Italy
Federico Benolli, OSDIFE - Observatory on Security and CBRNe Defence, Rome, Italy
Valentina Sabato, OSDIFE - Observatory on Security and CBRNe Deefence, Rome, Italy

ABSTRACT

As cyberattacks are becoming the prevalent types of attacks on critical infrastructures, due protection and effective response are crucial in CBRN facilities. This article explores comprehensive cyber security vulnerability management related to CBRN Control Systems and Industrial Control Systems (ICS) and provides recommendations that will increase CBRN operational cyber security and ensure further platform for the research in the field of operational vulnerability detection and remediation. The article reviews several key issues related to ICS vulnerability management cycle, vulnerability sharing with security developers, patch and network management, cyber offensive threats and threat actors and related cyber security challenges. It covers such specific issues as ICS connectivity to private/public networks, critical ICS accessibility via Web Access, Wi-Fi and/or unauthorised software inside corporate networks. The proposed solutions refer to some areas of vulnerability management for the awareness and development of countermeasures.

KEYWORDS

CBRN Infrastructures, Cyber Security, Dynamic Updating Architecture, End-to-End Encryption, Input Device Control, Limited Vulnerability Reporting, Network Segmentation, Vulnerability Management

1. EXECUTIVE SUMMARY

With cyberattacks becoming the prevalent types of attacks on critical infrastructures, due protection and effective response are especially crucial in chemical, biological, radioactive and nuclear (CBRN) facilities, whose damage not only entails country level process disruptions, but also endangers human existence globally.

Based on the current approaches to physical and operational security and safety, this article explores comprehensive cyber security vulnerability management related to CBRN Control Systems and Industrial Control Systems (ICS). The aim of this article is to review the cyber risk landscape and provide recommendations that will increase CBRN operational cyber security and facilitate further research in vulnerability detection and remediation.

The article reviews selected key issues related to the ICS vulnerability management cycle, vulnerability sharing with security developers, patch management, network management, cyber offensive threats and threat actors, as well as related cyber security challenges in CBRN defence. It also covers such specific issues as ICS connectivity to private and public networks, critical ICS accessibility via Web Access, Wi-Fi and unauthorised software inside corporate networks.

DOI: 10.4018/IJISCRAM.2018040103

The proposed solutions refer to the following areas of vulnerability management: Dynamic Updating Architecture, Network Segmentation, Input Device Control, End-to-end Encryption, Limited Vulnerability Reporting for the awareness and development of countermeasures. Selected cost-effective and affordable security measures have been considered to increase the efficiency and to decrease the complexity of vulnerability management in CBRN defence.

2. INTRODUCTION

Rapidly advancing cyber technologies have been assisting threat actors in offensive cyber operations since the creation of computers, computer networks and computerized control systems. The exponentially evolving infiltration techniques and publicly available hacking tools facilitate the attacks implementation and increase their variability. Though even AI-empowered, modern cyber defence software does not provide ultimate protection. Innovative multi-disciplinary solutions are required to ensure the enhanced cyber safety and security of the strategic CBRNe infrastructure.

2.1. Background

According to the European Directive 114/08[1], the term Critical Infrastructure refers to those assets, systems or part thereof, located in the EU Member States, which are fundamental for essential social functions, health, safety, security, and economics. Directive 114/08 defines the European Critical Infrastructure as every critical infrastructure located in the EU Member States, the disruption or destruction of which would consist of significant consequences on at least two Member States. In this regard, the eventual impact on CBRN critical infrastructure shall be generally assessed in terms of crosscutting criteria that refers to[2]:

1. Casualties (potential number of fatalities or injuries);
2. Economic effects (economic loss, degradation of products or services, environmental effects);
3. Public effects (public confidence, physical suffering and disruption of daily life, loss of essential services).

The following critical infrastructures gain particular relevance:

- Nuclear fuel-cycle industry (Generation plants);
- Health (Public and private medical services, Emergency health services, Veterinary services);
- Transport (Public transport network (underground, train, bus, etc.), Ports, airports, train stations);
- Chemical Industry.

Each of the above sectors can be exposed to a malicious use of hazardous materials that could threaten both health and security of citizens and society. In such environment, it becomes fundamental to monitor and survey every critical asset with the aim at mitigating the CBRNe threat.

2.1.1. CBRNe Risks

When an event affects a critical infrastructure facility, it could cause several direct and indirect damages, forcing Member States to enhance and ensure both safety and security procedures to protect both citizens and critical infrastructure. In this regard, Directive 114/08 defines who is responsible for safeguarding of public health and security into all phases of emergency cycle.

In a path to steady national CBRNe security enforcement, and within a framework of strategy for defense against terrorism, it is necessary to briefly consider the entire spread of various physical threats that could affect new terrorist targets: