Università degli Studi di Salerno

DIPARTIMENTO DI SCIENZE AZIENDALI - MANAGEMENT & INNOVATION SYSTEMS
DISA-MIS

DOTTORATO DI RICERCA IN
MANAGEMENT & INFORMATION TECHNOLOGY
XV° ciclo (XXIX° nazionale)

ABSTRACT

CYBER SECURITY RISK MANAGEMENT NEI SERVIZI PUBBLICI STRATEGICI

Coordinator
Prof.
Andrea DE LUCIA

Tutor
Prof.
Roberto PARENTE

Candidate

Valter RASSEGA

Matr. 8887600012

A.A. 2016-2017

Abstract

The global digital network, with its ability to communicate directly and in real time between people in every part of the planet, is a formidable tool to develop relationships and realize exchange of information and knowledge.
In cyberspace they coexist people of all kinds, characterized by different interests, different cultures and different ways of relating to others. From an economic point of view, the global network has become a formidable transactional tool for the exchange of goods and services and there is the commercial and industrial sector that has not arrived in some way in cyberspace.
The cybernetic revolution, induced by new and increasingly powerful electronic and computer technologies, it is not limited to connect the network, almost all of the planet's surface but is rapidly expanding to the direct control of myriad physical devices of the most varied , from Smartphone to wearable devices, from city traffic control to the electricity production and distribution infrastructure systems. And 'the SO-CALLED "Internet of Things" and the Internet of things, the network that interconnects all electronic devices capable of communicating with the outside world.
A pervasive who did not spare the public sector which, first, is called on to provide answers on many fronts, not least regulatory, and as far as possible, ensure compliance with the rules in the real world even in cyberspace.
In particular, the public sector must take responsibility to ensure the physical and cyber security of SO-CALLED National Critical Infrastructure, including all the essential services for national security, the proper functioning of the country and its economic growth and, not least, the well-being of the population. Are Critical Infrastructures electric and energy system, communication networks in general, networks and transport infrastructure of people and goods (ship, rail, air and road), the public health system, economics and financial channels, the national networks of government , regions, those for emergency management and civil protection.
The challenge is complex and Public Administration alone seems unable to respond effectively to increasingly sophisticated cyber-attacks that day, affecting the civilian world, industrial and economic. NCI are not immune and, as a result, the Public Strategic Services are exposed to significant risks. On this issue, Western governments have long established close cooperation with the private sector, and highlighted the need to define a strategy and a shared modus operandi and quality between the various actors involved.
This work aims to address systematically the "hot" topic of cyber security, an area that involves national governments, military, intelligence services, the economy and the business world as a whole and, gradually and in various capacities and degree of interest, every single citizen of the world.
In this unprecedented scenario, strongly characterized by uncertainty and variability of the virus, the application sic et simpliciter of "traditional" evaluation techniques of the corporate risk derivation is inadequate for this purpose, despite a certain degree of adaptation to the new scenario is already underway.
The analysis focuses on the relative adaptive-evolution that is affecting the risk management in the field of cyber security and state of the art in the academic and scientific world views in the introduction of new and more advanced tools for analysis the Cyber Risk.
The work ends with a case study of a large Italian company which provides a strategic public service such as electricity.