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

Coordinatore
Chiar. mo Prof.
Andrea DE LUCIA

Tutor
Chiar. mo Prof.
Roberto PARENTE

Candidato

Valter RASSEGA

Matr. 8887600012

A.A. 2016-2017

Abstract

La rete digitale globale, con la sua capacità di stabilire contatti diretti e in tempo reale tra persone in ogni parte del pianeta, rappresenta uno strumento formidabile per sviluppare relazioni e realizzare scambio di informazioni e di conoscenza.

Nel cyberspazio convivono persone di ogni tipo, caratterizzate da interessi diversi, culture differenti e diversi modi di relazionarsi con il prossimo. Dal punto di vista economico, la rete globale è oggi un formidabile strumento transazionale per lo scambio di beni e di servizi e non vi è settore commerciale e industriale che non sia approdato in qualche modo nel cyberspazio.

La rivoluzione cibernetica, indotta dalle nuove e sempre più potenti tecnologie elettroniche e informatiche, non si è limitata a connettere in rete la quasi totalità della superficie del pianeta ma si sta rapidamente espandendo verso il controllo diretto di una miriade di dispositivi fisici tra i più vari, dagli Smartphone ai dispositivi indossabili, dai sistemi di controllo del traffico cittadino alle infrastrutture di produzione e distribuzione di energia elettrica. E' la c.d. "Internet of Things" o Internet delle cose, che interconnette in rete tutti i dispositivi elettronici in grado di comunicare con il mondo esterno.

Una pervasività che non ha risparmiato il settore pubblico che, in primo luogo, è chiamato a fornire risposte su numerosi fronti, non ultimo quello normativo, e, per quanto possibile, garantire il rispetto delle regole presenti nel mondo reale anche nello spazio cibernetico.

In particolare, il settore pubblico deve farsi carico di garantire la sicurezza fisica e informatica delle c.d. infrastrutture critiche nazionali, che includono tutti quei servizi essenziali per la sicurezza nazionale, il buon funzionamento del Paese e la sua crescita economica e, non ultimo, il benessere della popolazione. Sono Infrastrutture Critiche il sistema elettrico ed energetico, le reti di comunicazione in genere, le reti e le infrastrutture di trasporto di persone e merci (navale, ferroviario, aereo e stradale), il sistema sanitario pubblico, i circuiti economici e finanziari, le reti del Governo nazionale, delle Regioni, quelle per la gestione delle emergenze e della Protezione Civile.

La sfida è complessa e la Pubblica Amministrazione da sola non sembra in grado di poter rispondere in modo efficace agli attacchi informatici sempre più sofisticati che, quotidianamente, colpiscono il mondo civile, industriale ed economico. Le infrastrutture critiche nazionali non ne sono immuni e, di conseguenza, i Servizi Pubblici Strategici sono esposti a significativi rischi. Su questo tema, i Governi occidentali hanno da tempo avviato una stretta collaborazione con il settore privato, ed è emersa la necessità di definire una strategia e un modus operandi condiviso e di qualità tra i vari attori coinvolti.

Questo lavoro si propone di affrontare in maniera sistematica il tema "caldo" della Cyber Security, un ambito che coinvolge governi nazionali, settori militari, servizi di informazione, il sistema economico e il mondo delle imprese nel suo complesso e, via via e a vario titolo e grado di interesse, ogni singolo cittadino del mondo.

In questo scenario inedito, fortemente connotato da incertezza e variabilità delle minacce, l'applicazione sic et simpliciter delle tecniche "tradizionali" di valutazione del rischio di derivazione aziendale risulta inadeguata allo scopo, nonostante un certo grado di adattamento al nuovo scenario sia già in corso.

L'analisi si concentra sulla parte relativa all''evoluzione adattativa' che sta interessando il risk management nel campo della cyber security e dello stato dell'arte nel panorama accademico e scientifico mondiale nell'introduzione di nuovi e più evoluti strumenti per l'analisi del Cyber Risk.

Il lavoro si conclude con un caso di studio effettuato su di una grande azienda italiana che fornisce un servizio pubblico strategico quale l'energia elettrica.