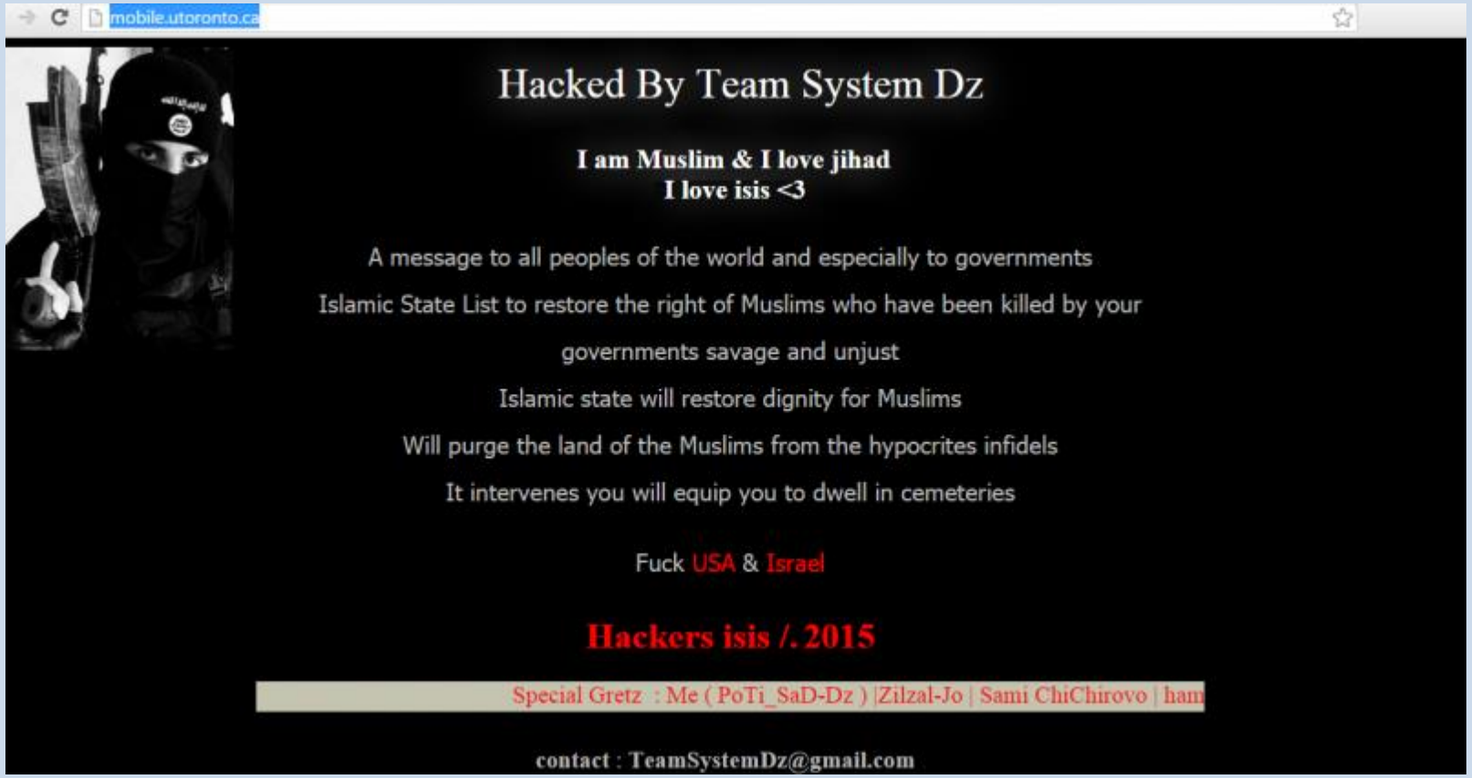
Cybersecurity Summit

Gensèric Cantournet – CSO RAI

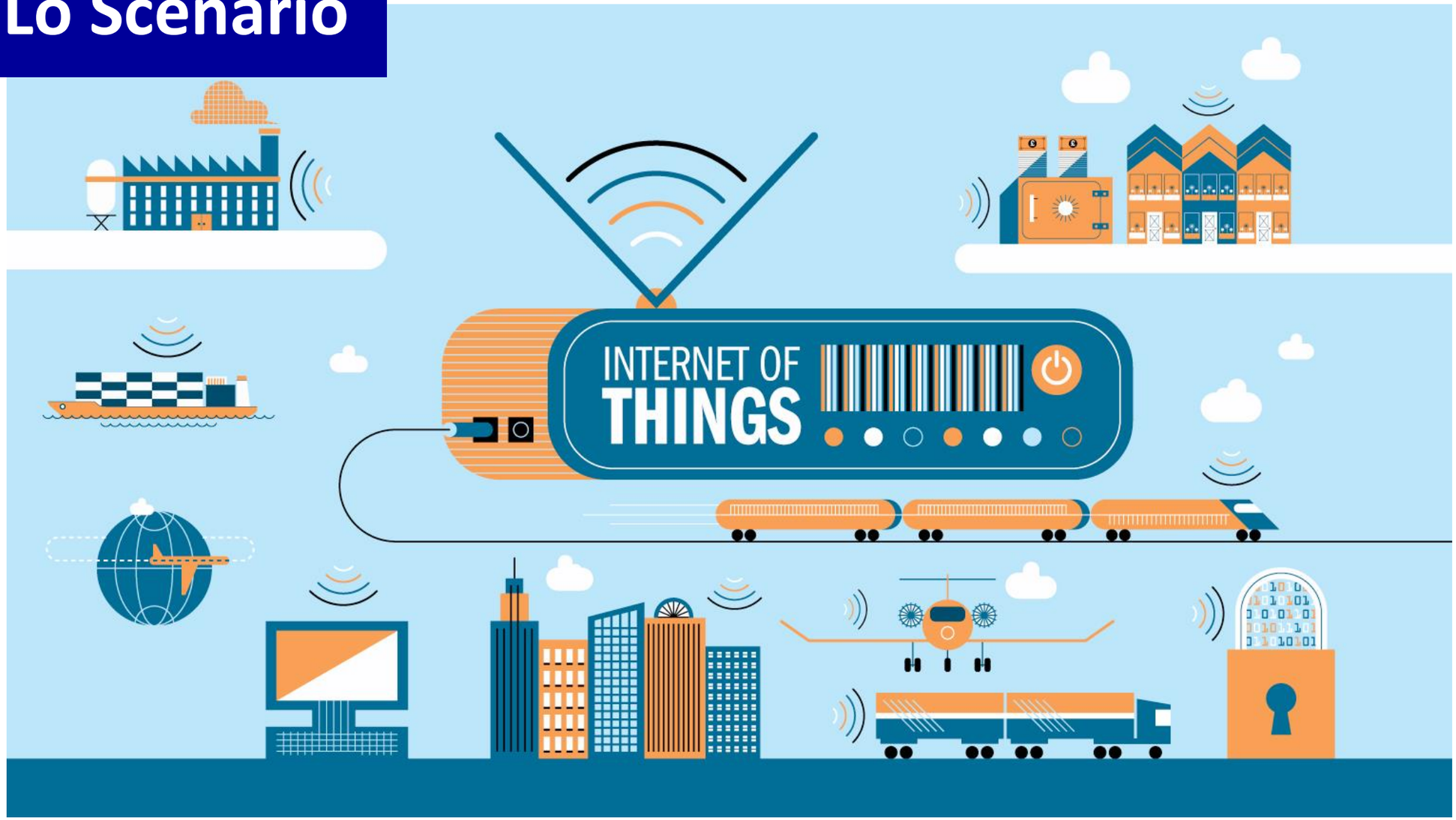
Milano - 7 giugno 2017

Non ha più senso parlare di sicurezza informatica,
così come non ha senso parlare della sicurezza di un singolo componente di un servizio,
ma solo della fornitura sicura dello stesso nel suo complesso.



VALE PIÙ L'INTEGRITÀ DEL SERVIZIO CHE L'EROGAZIONE STESSA DEL MEDESIMO

Lo Scenario



SECURITY BY DESIGN:

DA OPPORTUNITÀ A NECESSITÀ

Tutti gli aspetti della nostra vita quotidiana

PERSONALE,

PROFESSIONALE,

AZIENDALE

stanno **convergendo** rapidamente verso il *Cyberspazio*.

Il processo

è inevitabile mosso da esigenze di

INNOVAZIONE,

AGILITÀ ,

FLESSIBILITÀ ORGANIZZATIVA.

SECURITY BY DESIGN:

DA OPPORTUNITÀ A NECESSITÀ

Le AZIENDE, ma anche i singoli cittadini, si trovano quindi a misurarsi con un

UNIVERSO FLUIDO,

fatto di **MINACCE INFORMATICHE SEMPRE PIÙ ELABORATE**,

dalle quali scaturiscono **ATTACCHI SEMPRE PIÙ FREQUENTI ED EFFICACI**;

un panorama normativo in continua evoluzione;

una ***UBIQUITOUS CONNECTIVITY*** sempre più pervasiva, che espande secondo dopo secondo i confini del perimetro da difendere.

L’USABILITA’

NON PUO’ ESSERE UN NEMICO DELLA

SICUREZZA

Questo richiede ai soggetti interessati una

CAPACITÀ ORGANIZZATIVA SEMPRE MAGGIORE,

in grado di razionalizzare e

GESTIRE LA COMPLESSITÀ ALL’INSEGNA DELLA FLESSIBILITÀ.

IOT

SMART WORKING,

SMART MANIFACTURING,

AI DRIVEN USER EXPERIENCE

sono solo alcuni degli **avamposti** ai quali è necessario garantire adeguato presidio.

DIGITAL TRANSFORMATION E’

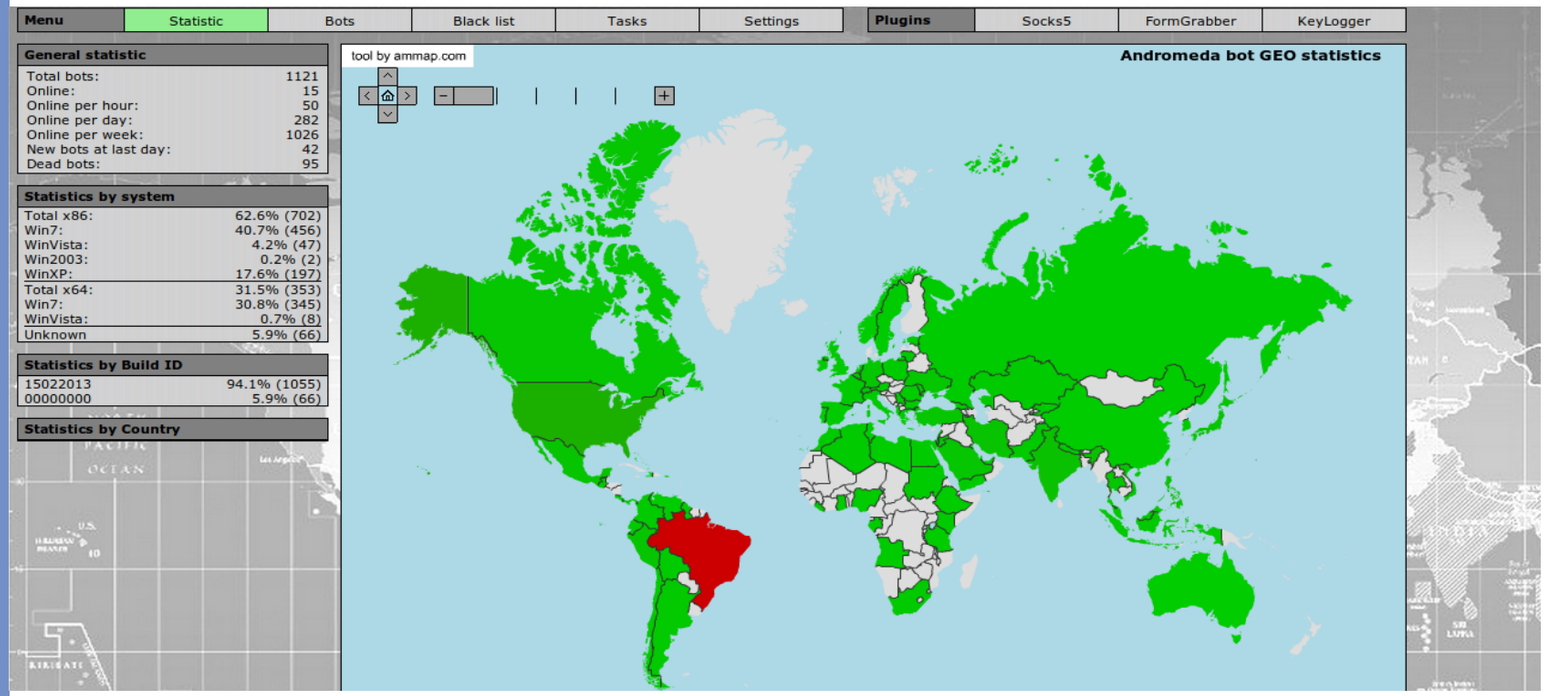
CONTAMINAZIONE ED INNOVAZIONE

La capacità delle aziende, ma anche di interi impalcati sociali, di soddisfare la crescente necessità d’innovazione, di dinamismo, di flessibilità, stimolate da *driver* potenti si giocherà sul campo del rapporto con gli individui.

Le basi di questo rapporto insistono sui pilastri della **SICUREZZA** e della **PRIVACY**,
ai quali sono legate numerose derivate come la corretta gestione dei **BIG DATA** ed il **MANAGEMENT DELLE IDENTITÀ DIGITALI.**

I TRE DRIVER DELLA TRASFORMAZIONE

CYBER THREAT INTELLIGENCE: un semplice dosaggio non può essere risolto come un banale *incident*, ma è necessario capire se nasconde altri *layer* di attacco, se è un semplice diversivo, se è un *cluster* di una strategia più ampia e se questa strategia coinvolge solo la nostra Azienda o anche altro.



INFO SHARING: lo scambio di informazioni deve necessariamente essere elevato al picco più alto, oltre la singola azienda ma anche oltre le aziende stesse, coinvolgendo in maniera sempre più attiva, proattiva e diretta soggetti coordinatori che non possono che essere di matrice pubblica.

ENTREPRISE RISK MANAGEMENT: integrata alla *Cyber Security* è la conseguenza inevitabile proprio della *Digital Trasformation* e del rapidissimo incremento della superficie di esposizione al rischio che essa sta generando.

L’APPROCCIO ERM

E’ impossibile pensare di preservare la conformità delle operazioni a leggi e regolamenti, l’*affidabilità e l’integrità delle informazioni, la salvaguardia del patrimonio aziendale, l’efficacia e l’efficienza delle operazioni* – i 4 pilastri di fondazione dell’approccio ERM - prescindendo da un robusto presidio di *Cyber Security*

La *Cyber Security* è sempre più ***precondizione*** per l’operatività aziendale, le nuove fondamenta su cui sono incardinate tutte le attività d’impresa.

E proprio in ragione di questo andrebbe elevata a **MATRICE DI SICUREZZA**, su cui innestare le verticali settoriali.

Milano 7 giugno 2017