l'Ingegnere Italiano

376

Cyber

ACCA SOFTWARE

l'esperto N°1

IFC-Open BIM

La scelta BIM di chi vuole libertà di collaborazione e vera disponibilità dei dati

IFC-Open BIM vuol dire libertà di comunicare, condividere, collaborare.
Solo lo standard IFC-Open BIM consente il dialogo tra tutti gli operatori che lavorano sul modello digitale della costruzione durante tutto il suo ciclo di vita, dalla progettazione all'esecuzione, dalla manutenzione alla dismissione dell'opera.
Con IFC-Open BIM, inoltre, **puoi accedere per sempre liberamente ai tuoi dati**, indipendentemente dal software e dalla versione del software che li ha prodotti.

Noi ci crediamo. Per questo vogliamo essere sempre di più i migliori specialisti dell'IFC-Open BIM in Italia e nel mondo.

Il primo **freeware per la visualizzazione e la modifica di un modello BIM in formato IFC**

Il maggior numero di **software certificati IFC da buildingSMART International** al mondo

La prima ed unica **piattaforma di BIM Management certificata IFC da buildingSMART International** al mondo

SCARICA GRATIS usBIM.viewer+
su www.acca.it

buildingSMART Standard Member

L'Ingegnere Italiano è la rivista
dedicata alla ricerca, alla tecnologia
e ai progetti di ingegneria.
Un magazine che si propone di raccontare l'eccellenza
dell'ingegneria italiana
nel contesto internazionale,
coniugando il rigore scientifico
con i nuovi linguaggi e l'innovazione.

Direttore responsabile
Armando Zambrano

Direttore editoriale
Gianni Massa

Curatore del numero
Michele Pierri

Coordinamento editoriale e giornalistico
Antonio Felici

Consulente editoriale
PPAN | *ppan.it*

Progetto grafico
Stefano Asili | *asi.li*

Stampa
artigrafiche Boccia | *artigrafiche boccia.it*

Pubblicità
Agicom srl – Castelnuovo P. (Roma) | *agicom.it*

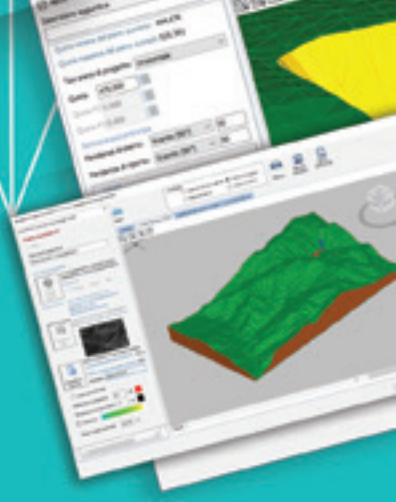
Segreteria direzione
Filomena Petroni

Editore
Consiglio Nazionale degli Ingegneri:
Stefano Calzolari, Giovanni Cardinale, Gaetano Fede,
Michele Lapenna, Ania Lopez, Massimo Mariani,
Gianni Massa, Antonio Felice Monaco, Roberto Orvieto,
Angelo Domenico Perrini, Luca Scappini, Raffaele Solustri,
Angelo Valsecchi, Remo Giulio Vaudano, Armando Zambrano
www.tuttoingegnere.it

Un ringraziamento particolare per il contributo alla realizzazione di questo numero:
Vincenzo Coppola, Michele Pierri.

Hanno collaborato a questo numero:
Agostino G. Bruzzone, Michele Colajanni, Emilio Coppa, Simone Crolla,
Gianluca Di Fusco, Francesco Fantera (PPAN), Luciano Floridi,
Luisa Franchina, Giovanni Lagorio, Davide Lamanna, Fabio Lazzini,
Alessandro Mollo, Elena Pasquini (PPAN), Marina Ribaudo, Paola Rocco,
Biagio Tagliaferro, Angelo Tofalo.

l'Ingegnere Italiano



Blumatica Geomatrix

Topografia e Catasto

Blumatica Geomatrix FREE

Gestione basilare del rilievo catastale in ambito CAD

Blumatica Geomatrix-C

Gestione avanzata del rilievo topografico catastale in ambiente CAD completo

Blumatica Geomatrix-Q

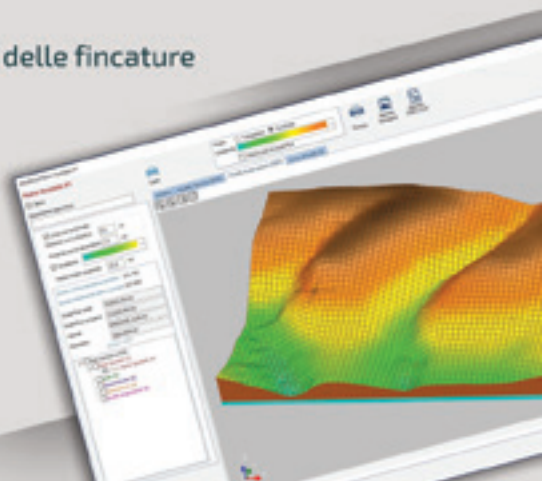
Gestione di piano quotato, curve di livello, spianamenti, riproduzione del modello digitale di elevazione DEM e del modello digitale del terreno DTM con esportazione in formato IFC

Dettagli che fanno la differenza!

- Acquisisci e rappresenti i dati in ambiente CAD dal libretto di PRE.GEO o dal formato .dat
- Storicizzi nel file tutte le modifiche e puoi ripristinare libretto e schema del rilievo ad un certo momento storico
- Visualizzi altri rilievi in modalità dati temporanei e procedi con la fusione di più libretti
- Verifichi il rispetto delle tolleranze in tempo reale ed ottieni i dettagli dei dati fuori tolleranza
- Acquisisci in modo automatizzato le mappe dal servizio di consultazione della cartografia catastale Web Map Service (WMS) dell'Agenzia delle Entrate
- Esporti e visualizzi il rilievo e le mappe su Google Earth
- Progetti spianamenti con piani orizzontali, inclinati, di compensazione sterro/riporto con calcolo automatico delle quote rosse
- Esporti tutti i dati del piano quotato 2D o 3D in formati vettoriali standard (DXF, DWG, ecc.) e i modelli digitali (DEM e DTM) in formato IFC
- Definisci i profili longitudinali con dettaglio e personalizzazione delle fincature

Prova GRATIS anche tu!

www.blumatica.it/geomatrix



blumatica
Software Edilizia e Sicurezza

Via Imo snc - 84098 Pontecagnano Faiano (SA) - Fax: 089.848741
Tel.: 089.848601 - E-mail: info@blumatica.it

I

GLI INGEGNERI GIOCANO UN RUOLO CHIAVE

Ormai da tempo tra le linee di indirizzo del Consiglio Nazionale Ingegneri c'è quella di aprire l'Ordine a quei settori diversi da quelli tradizionali, nei quali però l'ingegneria gioca un ruolo progressivamente sempre più rilevante. Non a caso, lo scorso numero di questa rivista è stato dedicato al rapporto tra food e ingegneria, due mondi apparentemente lontani ma in realtà fortemente connessi. Ancora più stretto è il legame che lega l'ingegneria al composito mondo delle reti.

La nostra vita professionale e privata dipende in misura sempre più crescente dalla sicurezza associata alle reti, ai dispositivi mobili, ai sistemi di cloud computing, ai software, ai sistemi e ai big data, alle informazioni personali. In altre parole, la Cyber Security. Un legame talmente forte da trasformare il relativo settore dell'Ict in uno di quelli trainanti a livello europeo. Il mercato della sicurezza informatica procede a gonfie vele e nel 2020 si prevede che raggiungerà il valore di 170 miliardi di euro, contro i 75 miliardi del 2015. La conseguenza è che in Europa le professioni legate all'Ict viaggiano verso una crescita del 30%. Secondo alcune stime entro la fine di quest'anno la domanda mondiale di sicurezza informatica toccherà 6 milioni di posti di lavoro, un quarto dei quali rischiano di rimanere vacanti. Insomma, un panorama di grandi opportunità professionali per gli ingegneri.

L'ingegnere, in particolare quello dell'informazione, può giocare, in questa nuova ed ampia prospettiva di gestione della sicurezza dentro aziende, amministrazioni pubbliche ed organizzazioni che progettano, realizzano o gestiscono infrastrutture Ict, un ruolo centrale. Egli può inserirsi, infatti, sia nelle attività di pianificazione, progettazione, sviluppo dei sistemi software e sistemi di rete, sia nelle attività di identificazione dei requisiti di sicurezza dei sistemi e in quelle di definizione delle soluzioni, favorendo l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura Ict. Il nuovo orientamento alla sicurezza dei sistemi apre spazi per gli ingegneri dell'informazione in nuove attività libero professionali comprendenti le verifiche di sicurezza dell'intero sistema, da affidare necessariamente a terze parti rispetto ai produttori e fornitori, allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità dei sistemi informatici e di rete, evidenziando le eventuali "falle" e suggerendo, al bisogno, gli eventuali rimedi. Ulteriori e ampie occasioni professionali per gli ingegneri dell'informazione scaturiscono, inoltre, dalla emergente necessità di attività di collaudo di grandi e piccole infrastrutture informatiche, a tutela degli interessi collettivi di sicurezza.

Questo numero della rivista dedicato alla Cyber Security, come sempre ricco di contributi di alto profilo scientifico, rappresenta una piccola dimostrazione di come gli ingegneri, in particolare quelli dell'informazione, abbiano tutte le carte in regola per candidarsi a favorire, consolidare e orientare i processi in atto, promuovendo la cultura della sicurezza Ict e, al tempo stesso, lavorando concretamente affinché il benessere sociale e la qualità della vita dei cittadini vengano preservati.

Buona lettura!

Armando Zambrano

Presidente CNI

IL MOTORE DEL DUEMILA

"Il motore del duemila sarà bello e lucente".

1976. 42 anni fa. Per intenderci l'anno in cui Fidel Castro diventa Presidente di Cuba e, in California, Steve Jobs e Steve Wozniak fondano la Apple Computer.

In Italia la sovrapposizione artistica dei linguaggi e dei talenti di Lucio Dalla e Roberto Roversi indaga e interpreta l'evoluzione umana rispetto all'evoluzione della tecnologia. L'automobile, il motore; simboli della modernità del ventesimo secolo che toccano e influenzano molteplici aspetti della vita dell'uomo.

La loro poesia in musica, immaginando il "motore del 2000", si interroga sul futuro della società in relazione alla ricerca del perfezionamento delle componenti meccaniche. Al confine tra la tecnica e lo sviluppo delle giovani generazioni simbolicamente interpretate dal "ragazzo del 2000". Da un lato una visione abbastanza nitida, la lucentezza e la bellezza del "motore". Dall'altro la consapevolezza che la strada verso il futuro dipende dal "cuore del giovane uomo fermo sull'uscio ad aspettare dentro quel vento".

Oggi siamo nel terzo millennio.

E quel motore, prima immaginato, ha prodotto cambiamenti sociali ed economici. Ha generato grandi movimenti nel passaggio di noi umani su questo pianeta.

Oggi siamo il presente di quel futuro e domani saremo il passato del prossimo futuro.

Automazione, industria 4.0, intelligenza artificiale, ict. Oggi, ancora più di ieri, il motore potrà essere "bello e lucente" solo se sapremo costruire la connessione tra uomo e tecnologia. Tra pensiero meditante e pensiero calcolante. Tra cultura tecnica e cultura umanistica. Perché ancora quel motore "non ha lo scarico calibrato e un odore che non inquina".

In ogni scoperta, in ogni sua applicazione, il ruolo dell'ingegneria, quale filo che lega l'idea alla sua realizzazione per la vita degli umani, è fondamentale.

Dalla ruota all'hyperloop. Passando per la bussola, la stampa, il motore a scoppio, la lampadina, la penicillina, il computer, internet. Dall'era analogica a quella dell'informazione, passando per quella del digitale.

E proprio l'ingegneria e il suo linguaggio vive un'epoca contraddittoria. Da un lato società e istituzioni stentano a riconoscerne il ruolo fondante per guardare al futuro trasformando questo Paese, dall'altro un quarto dei top manager mondiali sono ingegneri (Intel, Pimco, General eletric, Amazon, Google … hanno affidato proprio all'ingegneria lo sviluppo creativo delle loro aziende).

Hic sunt leones. Qui ci sono i leoni.

Così le antiche mappe indicavano le zone inesplorate del pianeta. Territori di cui non si sapeva nulla. Poi abbiamo iniziato a conoscere il mondo. E a rappresentarlo.

Mappe, carte geografiche.

Uno dei miei maestri, Silvano Tagliagambe, riprendendo il parallelismo di Rudolf Carnap tra mappe e teorie scientifiche, ci insegna, che l'elemento caratterizzante di una teoria scientifica non è il suo linguaggio, ma la sua struttura, cioè l'insieme delle relazioni tra le sue componenti.

Ed è proprio il ruolo fondante delle relazioni tra gli elementi, delle competenze, ciò di cui abbiamo necessità.

Questo nuovo scenario da un lato mette l'ingegneria al centro della scena offrendo un'opportunità irripetibile, dall'altro la mette di fronte alla necessità di dotarsi di nuove competenze, nuovi linguaggi, nuova capacità di selezionare e sovrapporre conoscenze, consentendo di divenire forza creativa, economica, sociale. Nel mondo contemporaneo, oggi e domani, l'ingegnere dovrà ancora di più unire la cultura tecnica all'immaginazione, alla capacità di guardare altrimenti, di andare oltre.

Quella che tutti chiamano "nuova rivoluzione", però, non è solo un pranzo di gala.

Mai come nella nostra epoca siamo chiamati a fronteggiare un enorme problema di sicurezza informatica. Al quale va necessariamente associata la questione della privacy e, aggiungo, della semplificazione (quando riusciremo a partecipare ad una gara pubblica con semplicità, magari utilizzando lo smartphone?).

Sono temi di assoluta delicatezza che se non affrontati adeguatamente possono determinare gravi conseguenze, di tipo economico e non. Per questo motivo gli ingegneri, oltre a recitare un ruolo da protagonisti nell'immaginario collettivo digitale, rappresentano un vero e proprio punto di tenuta della sicurezza del sistema Paese, dunque della sua competitività. Per ottenere questo, però, è necessario immaginare e realizzare percorsi formativi e di inserimento incentivanti che consentano di realizzare una catena tra formazione e mondo del lavoro nel sistema paese, sulla scia, anche, del modello sperimentato nel nord Europa. Un obiettivo possibile, raggiungibile. A patto che si riesca a dare vita ad un ambiente di lavoro e di confronto, all'interno del quale istituzioni, università e ricerca, cittadini e soprattutto ingegneri possano marciare tutti nella stessa direzione.

Insomma, automazione e robotica, catalizzatori esponenziali, rendono lo sviluppo industriale ancora più interconnesso all'ambiente, alla società, al nostro essere nel mondo. E come sempre, nella storia dell'uomo, tutto ciò ha potenziali effetti positivi e potenziali effetti negativi. L'ingegneria saprà essere pilastro fondante di questo processo di catalisi se saprà gestire la complessità multidisciplinare, se non sarà relegata ad adempimento formale, se il suo linguaggio e la sua forza creativa saranno riconosciute da istituzioni e società.

Gianni Massa

Vice Presidente Vicario CNI

TROVARE IL GIUSTO EQUILIBRIO TRA DEMOCRAZIA E SICUREZZA

La Cyber Security rappresenta la più importante sfida di questo millennio. Quotidianamente ci troviamo a dover affrontare questioni legate alla sicurezza che inevitabilmente interessano ogni settore della Pubblica Amministrazione e del privato e, non secondariamente, il singolo cittadino sempre più esposto, in molti casi in modo inconsapevole, ai rischi dell'internet of every things.

Siamo di fronte a un fenomeno che evolve rapidamente, al passo con lo sviluppo tecnologico, e si riflette sulla società e sulla quasi totalità della popolazione. Il numero degli utenti connessi ad Internet nel mondo ha infatti superato la soglia dei 4 miliardi di persone e questo significa che oggi più della metà della popolazione mondiale naviga online. Sono numeri destinati a crescere e, se consideriamo l'avvento del 5G, è chiara l'accelerazione verso un ecosistema di trasformazione abilitante per tante tecnologie. In un futuro molto prossimo tutto sarà connesso, la velocità e la molteplicità delle interconnessioni incideranno prepotentemente nella realtà grazie gli innumerevoli vantaggi offerti dai nuovi servizi in una pluralità di settori ma, con la tecnologia di quinta generazione, anche le minacce cibernetiche sono destinate a crescere in maniera esponenziale. Già nel corso dello scorso anno si è registrato un considerevole aumento degli attacchi classificati come "gravi".

Il punto focale è che se fino a qualche anno fa ignorare il tema non produceva problemi devastanti, oggi, in un mondo sempre più interconnesso, sottovalutare il rischio della minaccia cyber può causare scenari irreversibili. Un'insufficiente prevenzione e una debole capacità di difesa possono essere causa di enormi danni alle Amministrazioni pubbliche e alle aziende che, senza nemmeno rendersene conto, subirebbero esfiltrazioni di dati sensibili e quindi conseguenze sfavorevoli non solo in termini economici.

Fortunatamente oggi iniziamo a percepire maggiormente quanto la minaccia cibernetica sia più sofisticata e pervasiva. Una minaccia non più percepita come virtuale in quanto frutto di azioni fisiche e concrete. La digitalizzazione nella vita quotidiana, dove il rapporto digitalizzato con le amministrazioni dello Stato, la domotica e la mobilità intelligente sono ormai realtà, nasce una necessità di rafforzamento del livello di sicurezza che può essere soddisfatto creando maggiore sinergia tra il singolo, le aziende e le Istituzioni. Poiché non possiamo sottrarci da quelli che sono i rischi della digitalizzazione possiamo solo creare azioni di sistema per ridurli. Ciascuno, al proprio livello, deve fare la propria parte.

Da ingegnere dico che abbiamo grandi responsabilità anche e soprattutto in fase progettuale, dobbiamo infatti strutturare nuovi approcci per ridisegnare il Paese tenendo conto di norme specifiche sulle diverse branche della sicurezza. Da rappresentante del Governo, invece, sono fermamente convinto che è compito delle Istituzioni rafforzare il patrimonio di competenze nazionali in materia di cyber sicurezza. Per raggiungere questo ambizioso traguardo bisogna puntare ad accompagnare l'evoluzione dell'aspetto tecnologico con un fattore umano caratterizzato dall'organizzazione di percorsi di alta specializzazione, essenziali per creare un network nazionale solido ed esteso capace di dialogare a livello globale. Dobbiamo rafforzare una strategia nazionale per valorizzare chi deve fare "sistema" con i principali player internazionali dell'innovazione.

Il Governo incoraggia in varie forme la partnership tra pubblico e privato per fronteggiare gli attacchi informatici e proteggere le infrastrutture critiche. La priorità rimane stabilire sinergie all'interno di un ecosistema Governo-Industria-Università così come avviene, ad esempio, in Israele, Paese oggi all'avanguardia negli investimenti in Cyber Security e dove il distretto tecnologico di Silicon Wadi ospita Università, Centri di ricerca, grandi aziende, organizzazioni istituzionali e Start up.

Infine, per spingere la nostra visione più avanti nel tempo, dobbiamo sin da oggi creare dei tavoli interdisciplinari per anticipare un futuro in cui le macchine potrebbero, grazie alla velocità di calcolo, l'A.I. ed il machine learning, prendere decisioni autonomamente. Le domande a cui dovremo rispondere sono tante. Come reagiremo rispetto a qualcosa che finora ha potuto solo l'uomo? Come potremo fornire gli anticorpi necessari alla nostra società futura? Secondo quali criteri etici verranno creati gli algoritmi di funzionamento di macchine complesse?

Da un lato è forte l'esigenza di restare al passo con i tempi, in termini di progresso, dall'altro si prospetta il bisogno di protezione dei valori costituenti della nostra Democrazia. Scienza e Ingegneria saranno sempre più invasivi nella trasformazione dei modelli di società e la politica dovrà essere capace di rispondere a queste importanti variazioni per difendere i cittadini dalla compressione dei propri diritti.

Lavorando in linea con i nostri valori riusciremo a trovare il giusto equilibrio fra democrazia e sicurezza e a prevenire i rischi del quinto dominio senza privarci delle opportunità che esso ci offre.

On Angelo Tofalo

Sottosegretario di Stato alla Difesa

376

/sommario

Luciano Floridi

What the Near Future of Artificial Intelligence Could Be

Introduction

Artificial Intelligence (AI) has dominated recent headlines, with its promises, challenges, risks, successes, and failures. What is its foreseeable future? Of course, the most accurate forecasts are made with hindsight. But if some cheating is not acceptable, then smart people bet on the uncontroversial or the untestable. On the uncontroversial side, one may mention the increased pressure that will come from law-makers to ensure that AI applications align with socially acceptable expectations. For example, everybody expects some regulatory move from the EU, sooner or later. On the untestable side, some people will keep selling catastrophic forecasts, with dystopian scenarios taking place in some future that is sufficiently distant to ensure that the Jeremiahs will not be around to be proven wrong. Fear always sells well, like vampire or zombie movies. Expect more. What is difficult, and may be quite embarrassing later on, is to try to "look into the seeds of time, and say which grain will grow and which will not" (*Macbeth*, Act I, Scene III), that is, to try to understand where AI is more likely to go and hence where it may not be going. This is what I will attempt to do in the following pages, where I shall be cautious in identifying the paths of least resistance, but not so cautious as to avoid any risk of being proven wrong.

Part of the difficulty is to get the level of abstraction right (Floridi 2008a, b), i.e. to identify the set of relevant observables ("the seeds of time") on which to focus because those are the ones that will make the real, significant difference. In our case, I shall argue that the best observables are provided by an analysis of the *nature of the data* used by AI to achieve its performance, and of the *nature of the problems* that AI may be expected to solve[1]. So, my forecast will be divided into two, complementary parts. In section two, I will discuss the nature of the data needed by AI; and in section three, I will discuss the scope of the problems AI is more likely to tackle successfully. I will conclude with some more general remarks about tackling the related ethical challenges. But first, let me be clear about what I mean by AI.

[1] For a reassuringly converging review based not on the nature of data or the nature of problems, but rather on the nature of technological solutions, based on a large scale review of the fortcoming literture on AI, see "We analyzed 16,625 papers to figure out where AI is headed next" https://www.technologyreview.com/s/612768/we-analyzed-16625-papers-to-figure-out-where-ai-is-headed-next/

AI: A Working Definition

AI has been defined in many ways. Today, it comprises several techno-scientific branches, well summarised in (Corea Aug 29 2018) by *Figura 1*

Altogether, AI paradigms still satisfy the classic definition provided by John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon in their seminal "Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", the founding document and later event that established the new field of AI in 1955:

For the present purpose the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent if a human were so behaving. (Quotation from the 2006 re-issue in (McCarthy et al. 2006))

As I have argued before (Floridi 2017), this is obviously a counterfactual: were a human to behave in that way, that behaviour would be called intelligent. It does not mean that the machine is intelligent or even thinking. The latter scenario is a fallacy, and smacks of superstition. Just because a dishwasher cleans the dishes as well as, or even better than, I do does not mean that it cleans them like I do, or needs any intelligence in achieving its task. The same counterfactual understanding of AI underpins the Turing test (Floridi, Taddeo, and Turilli 2009), which, in this case, checks the ability of a machine to perform a task in such a way that the outcome would be indistinguishable from the outcome of a human agent working to achieve the same task (Turing 1950).

The classic definition enables one to conceptualise AI as a growing resource of interactive, autonomous, and often self-learning (in the machine learning sense, see *Figura 1*) agency, that can deal with tasks that would otherwise require human intelligence and intervention to be performed successfully. This is part of the ethical challenge posed by AI, because artificial agents are:

sufficiently informed, 'smart', autonomous and able to perform morally relevant actions independently of the humans who created them […]. (Floridi and Sanders 2004)

Although this aspect is important, it is not a topic for this article, and I shall return to it briefly only in the conclusion.

In short, AI is defined on the basis of outcomes and actions and so, in what follows, I shall treat AI as a reservoir of smart agency on tap. The question I wish to address is: what are the foreseeable ways in which such a technology will evolve and be used successfully? Let us start from the data it needs.

AI's Future: From Historical Data to Hybrid and Synthetic Data, and the Need for Ludification

They say that data are the new oil. Maybe. But data are durable, reusable, quickly transportable, easily duplicable, and simultaneously shareable without end, while oil has none of these properties. We have gigantic quantities of data that keep growing, but oil is a finite resource. Oil comes with a clear price, whereas the monetisation of the same data depends on who is using them and for what. And all this even before introducing the legal and ethical issues that emerge when personal data are in play, or the whole debate about ownership ("my data" is much more like "my hands" and much less like "my oil"). So, the analogy is a stretch, to say the least. This does not mean that is entirely worthless though. Because it is true that data, like oil, are a valuable resource, and must be refined in order to extract their value. In particular, without data, algorithms — AI included — go nowhere, like an engine with an empty tank. AI needs data to train, and then data to apply its training. Of course, AI can be hugely flexible, it is the data that determine its scope of application and degree of success. For example, in 2016 Google used DeepMind's machine learning system to reduce its energy consumption:

Because the algorithm is a general-purpose framework to understand complex dynamics, we plan to apply this to other challenges in the data centre environment and beyond in the coming months. Possible applications of this technology include improving power plant conversion efficiency (getting more energy from the same unit of input), reducing semiconductor manufacturing energy and water usage, or helping manufacturing facilities increase throughput.[2]

[2] https://deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-40/

It is well known that AI learns from the data it is fed, and progressively improve its results. If you show an immense number of photos of dogs to a neural network, in the end it will learn to recognize dogs increasingly well, including dogs it never saw before. To do this, usually one needs huge quantities of data, and it is often the case that the more the better. For example, in recent tests a team of researchers from the University of California in San Diego trained an AI system on 101.6 million electronic health record (EHR) data points (including text written by doctors and laboratory test results) from 1.362.559 paediatric patient visits at a major medical centre in Guangzhou, China. Once trained, the AI system was able to demonstrate:

[…] high diagnostic accuracy across multiple organ systems and is comparable to experienced pediatricians in diagnosing common childhood diseases. Our study provides a proof of concept for implementing an AI-based system as a means to aid physicians in tackling large amounts of data, augmenting diagnostic evaluations, and to provide clinical decision support in cases of diagnostic uncertainty or complexity. Although this impact may be most evident in areas where healthcare providers are in relative shortage, the benefits of such an AI system are likely to be universal. (Liang et al. 2019)

However, in recent times AI has improved so much that, in some cases, we are moving from an emphasis on the quantity of large masses of data, sometimes improperly called Big Data (Floridi 2012), to an emphasis on the quality of data sets that are well curated. For example, in 2018, DeepMind, in partnership with Moorfields Eye Hospital in London, UK, trained an AI system to identify evidence of sight-threatening eye diseases using optical coherence tomography (OCT) data, an imaging technique that generates 3D images of the back of the eye. In the end, the team managed to:

demonstrate performance in making a referral recommendation that reaches or exceeds that of experts on a range of sight-threatening retinal diseases after training on only *14.884 scans [my italics]*. (De Fauw et al. 2018), p. 1342.

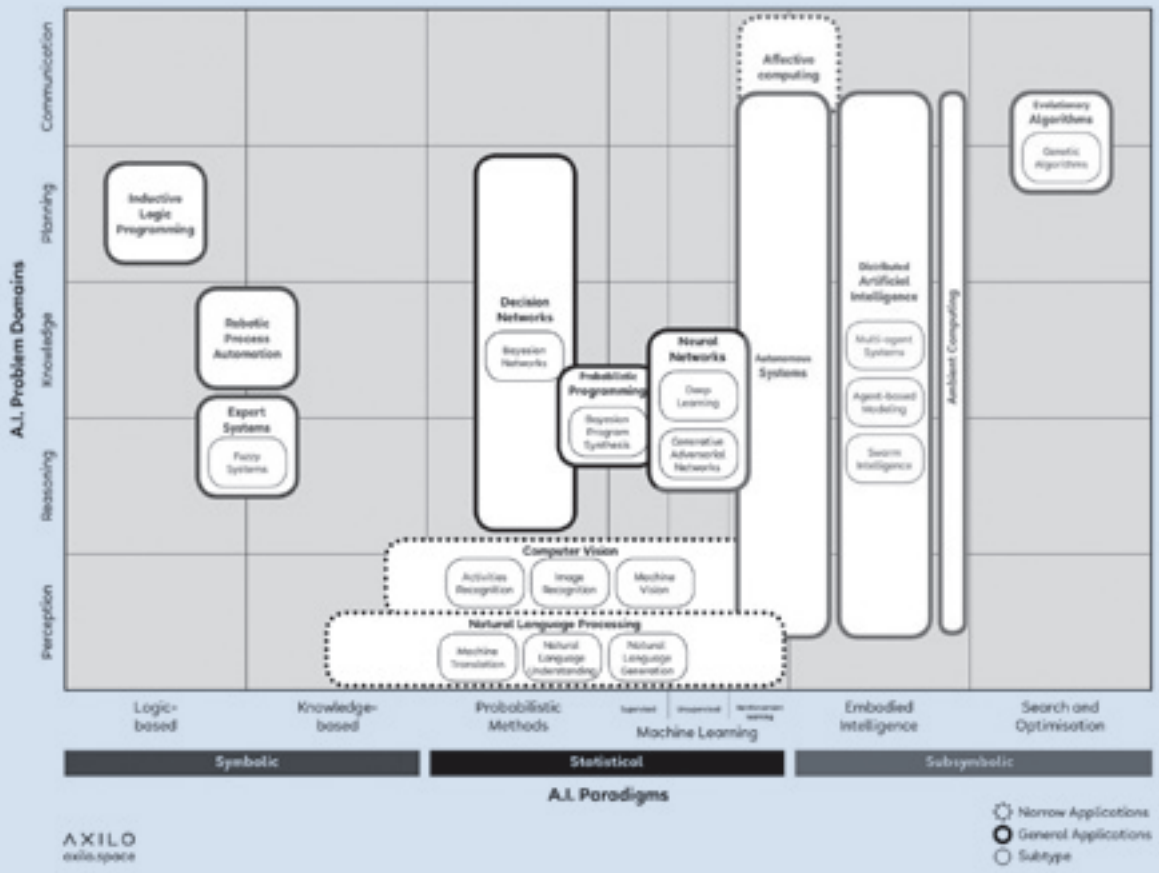
I emphasise "only 14.884 scans" because "small data" of high quality is one of the futures of AI. AI will have a higher chance of success whenever well-curated, updated, and fully reliable data sets become available and accessible to train a system in a specific area of application. This is quite obvious and hardly a new forecast. But it is a solid step forward, which helps us look further ahead, beyond the "Big Data" narrative. If quality matters, then provenance is crucial. Where do the data come from? In the previous example, they were provided by the hospital. Such data are sometimes known as *historical*, *authentic*, or *real-life* (henceforth I shall call them simply historical). But we know that AI can generate its own data. I am not talking about metadata, or secondary data about its uses (Floridi 2010). I am talking about its primary input. I shall call such entirely AI-generated data synthetic. Unfortunately, the term has an ambiguous etymology. It began to be used in the 1990s to refer to historical data that had been anonymised before being used, often to protect privacy and confidentiality. These data are synthetic only in the sense that they have been synthesised from historical data, e.g. through "masking".[3] They have a lower resolution, but their genesis is not an artificial source. The distinction between the historical data and those synthesised from them is useful, but this is not what I mean here, where I wish to stress the completely and exclusively artificial provenance of the data in question. It is an ontological distinction, which may have significant implications in terms of epistemology, especially when it comes to our ability to explain the synthetic data produced, and the training achieved by the AI using them (Watson et al. forthcoming).
A famous example can help explain the difference.

In the past, playing chess against a computer meant playing against the best human players who had ever played the game. One of the features of Deep Blue, the IBM's chess program that defeated the world champion Garry Kasparov, was

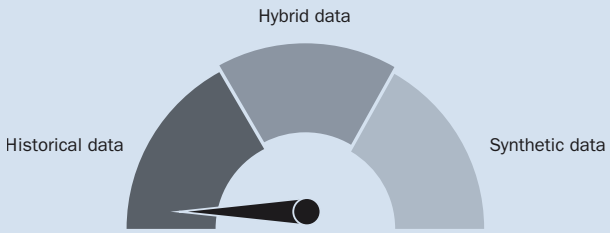
"an effective use of a Grandmaster game database" (Campbell, Hoane Jr, and Hsu 2002), p. 57.

[3] https://www.tcs.com/blogs/the-masking-vs-synthetic-data-debate

1



2



1 – AI Knowledge Map (AIKM), source: (Corea Aug 29 2018).
2 – Shifting from entirely historical to truly synthetic data

But AlphaZero, the last version of the AI system developed by DeepMind, learnt to play better than anyone else, and indeed any other software, by relying only on the *rule*s of the game, with no data input at all from any external source. It had no historical memory whatsoever:

The game of chess represented the pinnacle of artificial intelligence research over several decades. State-of-the-art programs are based on powerful engines that search many millions of positions, *leveraging handcrafted domain expertise and sophisticated domain adaptations*. [my italics, these are the non-synthetic data]. AlphaZero is a generic reinforcement learning and search algorithm—originally devised for the game of Go—that achieved superior results within a few hours [...] *given no domain knowledge except the rules of chess* [my italics]. (Silver et al. 2018), p. 1144.

AlphaZero learnt by playing against itself, thus generating its own chess-related, synthetic data. Unsurprisingly, Chess Grandmaster Matthew Sadler and Women's International Master Natasha Regan, who have analysed thousands of AlphaZero's chess games for their forthcoming book Game Changer (New in Chess, January 2019), say its style is unlike any traditional chess engine. "It's like discovering the secret notebooks of some great player from the past," says Matthew.[4]

Truly synthetic data, as I am defining them here, have some wonderful properties. Not only do they share those listed at the beginning of this section (durable, reusable, quickly transportable, easily duplicable, simultaneously shareable without end, etc.). They are also clean and reliable (in terms of curation), they infringe no privacy or confidentiality at the development stage (though problems persist at the deployment stage, because of the predictive privacy harms (Crawford and Schultz 2014)), they are not immediately sensitive (sensitivity during the deployment stage still matters), if they are lost it is not a disaster because they can be recreated, and they are perfectly formatted to be used by the system that generates them. With synthetic data, AI never has to leave its digital space, where it can exercise complete control on any input and output of its processes. Put more epistemologically, with synthetic data AI enjoys the privileged position of a maker's knowledge, who knows the intrinsic nature and working of something because it made that something (Floridi 2018). This explains why they are so popular in security contexts, for example, where AI is deployed to stress-test digital systems. And sometimes synthetic data can also be produced more quickly and cheaply that historical data. AlphaZero became the best chess player on earth in nine hours (it took 12 hours for shogi, and 13 days for Go).

Between historical data that are more or less masked (impoverished through lower resolution, e.g. through anonymisation) and purely synthetic data, there is a variety of more or less *hybrid* data, which you can imagine as the offspring of historical and synthetic data. The basic idea is to use historical data to obtain some new synthetic data that are not merely impoverished historical data. A good example is provided by Generative Adversarial Networks (GANs), introduced by (Goodfellow et al. 2014):

Two neural networks — a Generator and a Discriminator [my capitals in the whole text] — compete against each other to succeed in a game. The object of the game is for the Generator to fool the Discriminator with examples that look similar to the training set. [...] When the Discriminator rejects an example produced by the Generator, the Generator learns a little more about what the good example looks like. [...] In other words, the Discriminator leaks information about just how close the Generator was and how it should proceed to get closer. [...] As time goes by, the Discriminator learns from the training

[4] https://deepmind.com/blog/alphazero-shedding-new-light-grand-games-chess-shogi-and-go/

[5] https://securityintelligence.com/generative-adversarial-networks-and-cybersecurity-part-1/

[6] https://motherboard.vice.com/en_us/article/7xn4wy/this-website-uses-ai-to-generate-the-faces-of-people-who-dont-exist

set and sends more and more meaningful signals back to the Generator. As this occurs, the Generator gets closer and closer to learning what the examples from the training set look like. *Once again, the only inputs the Generator has are an initial probability distribution (often the normal distribution) and the indicator it gets back from the Discriminator. It never sees any real examples* **[my italics].**[5]

The Generator learns to create synthetic data that are like some known input data. So, there is a bit of a hybrid nature here, because the Discriminator needs to have access to the historical data to "train" the Generator. But the data generated by the Generator are new, not merely an abstraction form the training data. So, not a case of parthenogenesis, like AlphaZero giving birth to its own data, but close enough to deliver some of the very appealing features of synthetic data nevertheless. For example, synthetic human faces created by a Generator pose no problems in terms of privacy, consent or confidentiality at the development stage.[6]

Many methods to generate hybrid or synthetic data are already available or being developed, often sector specific. There are also altruistic trends to make such data sets publicly available (Howe et al. 2017). Clearly, the future of AI lies not just in "small data" but also, or perhaps mainly, in its increasing ability to generate its own data. That would be a remarkable development, and one may expect significant efforts to be made in that direction. The next question is: what factor can make the dial in *Figura 2* move from left to right?

The difference is made by the genetic process, i.e. by the rules used to create the data. *Historical data* are obtained by *recording rules*, as they are the outcome of some observation of a system behaviour. Synthesised data are obtained by *abstracting rules* that eliminate, mask or obfuscate some degrees of resolution from the historical data, e.g. through anonymisation. *Hybrid* and truly *synthetic data* can be generated by *constraining rules* or *constitutive rules*. There is no one-to-one mapping, but it is useful to consider hybrid data as the data on which we have to rely, using constraining rules, when we do not have constitutive rules that can generate synthetic data from scratch. Let me explain.

The dial moves easily towards synthetic data whenever AI deals with "games"—understood as any formal interactions in which players compete according to rules and in view of achieving a goal—the rules of which are constitutive and not merely constraining. The difference is obvious if one compares chess and football. Both are games, but in chess the rules establish the legal and illegal moves before any chess-like activity is possible, so they are generative of all and only the acceptable moves. Whereas in football, a previous activity—let's call it kicking a ball—is "regimented" or structured by rules that arrive after the activity. The rules do not and cannot determine the moves of the players, they simply put boundaries to what moves are "legal". In chess, as in all board games whose rules are constitutive (draughts, Go, Monopoly, shogi…), AI can use the rules to play any possible legal move that it wants to explore. In nine hours, AlphaZero played 44 million training games. To have a sense of the magnitude of the achievement consider that the *Opening Encyclopedia 2018* contains approximately 6.3 million games, selected from the whole history of chess. But in football, this would be meaningless because the rules do not make the game, they only shape it. This does not mean that AI cannot play virtual football; or cannot help identifying the best strategy to win against a team whose data about previous games and strategies are recorded; or cannot help with identifying potential players, or training them better. Of course, all these applications are now trivially feasible and already occur. What I mean is that when (1) a process or interaction can be transformed into a game, and (2) the game can be transformed into a *constitutive-rule* game, then (3) AI will be able to generate its own, fully synthetic data and be the best "player" on this planet, doing what AlphaZero did for chess (in the next section I shall describe this process as *enveloping* (Floridi 2014a)). To quote Wiener:

The best material model of a cat is another, or preferably the same, cat. (Rosenblueth and Wiener 1945), p. 316.

Ideally, the best data on which to train an AI are either the fully historical data or the fully synthetic data generated by the same rules that generated the historical data. In any board game, this happens by default. But insofar as any of these two steps (1)-(2) is difficult to achieve, the absence of rules or the presence of merely constraining rules is likely to be a limit. We do not have the actual cat, but only a more or less reliable model of it. Things can get more complicated once we realise that, in actual games, the constraining rules are simply conventionally imposed on a previously occurring activity, whereas in real life, when we observe some phenomena, e.g. the behaviour of a kind of tumour in a specific cohort of patients in some given circumstances, the genetic rules must be extracted from the actual "game" through scientific (and these days possibly AI-based) research. For example, we do not know and perhaps we may never know what the exact "rules" for the development of brain tumours are.

We have some general principles and theories according to which we understand their development. So, at this stage (and it may well be a permanent stage), there is no way to "ludify" (transformation into a game in the sense specified above, I avoid gamifying which has a different and well-established meaning) brain tumours into a "constitutive-rule game" (think of chess) such that an AI system, by playing according to the identified rules, can generate its own synthetic data about brain tumours that would be equivalent to the historical data we could collect, doing for brain tumours what AlphaZero has done for chess games. This is not necessarily a problem.

On the contrary, AI, by relying on historical or hybrid data (e.g. brain scans) and learning from them, can still outperform experts, and expand its capabilities beyond the finite historical data sets provided (e.g., by discovering new patterns of correlations), or deliver accessible services where there is no expertise. It is already a great success if one can extract enough *constraining* rules to produce reliable data *in silico*. But without a reliable system of *constitutive rules*, some of the aforementioned advantages of synthetic data would not be available in full (the vagueness of this statement is due to the fact that we can still use hybrid data).

Ludification and the presence or absence of constraining/constitutive rules are not either-or hard limits. Recall that hybrid data can help to develop synthetic data. What is likely to happen is that, in the future, it will become increasingly clear when high-quality databases of historical data may be absolutely necessary and unavoidable—when you need the actual cat, to paraphrase Wiener—and hence when we will have to deal with issues about availability, accessibility, legal compliance with legislation, and, in the case of personal data, privacy, consent, sensitivity and other ethical questions. However, the trend towards the generation of as-synthetic-as-possible (synthesised, more or less hybrid, all the way to fully synthetic) data is likely to be one of AI's holy grails, so I expect the AI community to push very hard in that direction. Generating increasingly non-historical data, making the dial move as far as possible to the right, will require a "ludification" of processes, and for this reason I also expect the AI community to be increasingly interested in the gaming industry, because it is there that the best expertise in "ludification" is probably to be found. And in terms of negative results, mathematical proofs about the impossibility of ludifying whole kinds or areas of processes or interactions should be most welcome in order to clarify where or how far an AlphaZero-like approach may never be achievable by AI.

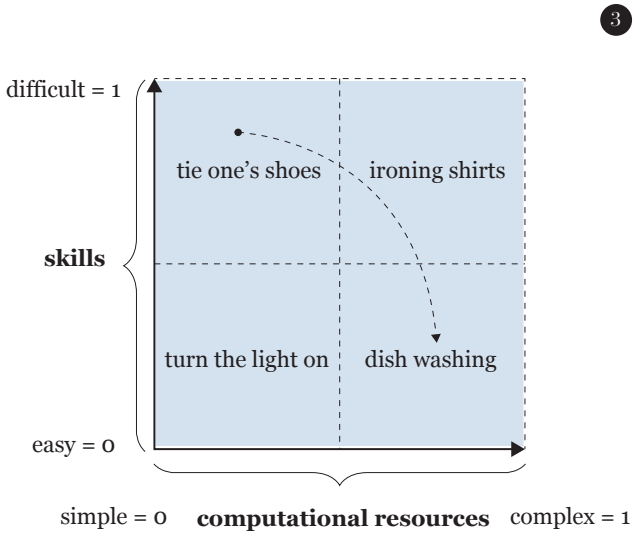
AI's Future: From Difficult Problems to Complex Problems, and the Need for Enveloping

I have already mentioned that AI is best understood as a reservoir of agency that can be used to solve problems. AI achieves its problem-solving goals by detaching the ability to perform a task successfully from any need to be intelligent in doing so. The App in my mobile phone does not need to be intelligent to play chess better than I do. Whenever this detachment is feasible, some AI solution becomes possible in principle. This is why understanding the future of AI also means understanding the nature of problems where such a detachment may be technically feasible in theory and economically viable in practice.
Now, many of the problems we try to solve through AI occur in the physical world, from driving to scanning labels in a supermarket, from cleaning flows or windows to cutting the grass in the garden. The reader may keep in mind AI as robotics in the rest of this section, but I am not discussing only robotics: smart applications and interfaces in the Internet of Things are also part of the analysis, for example.
What I would like to suggest is that, for the purpose of understanding AI's development when dealing with physical environments, it is useful to map problems on the basis of what resources are needed to solve them, and hence how far AI can have such resources. I am referring to *computational resources*, and hence to degrees of *complexity*; and to *skill-related resources*, and hence to degrees of *difficulty*.

The degrees of complexity of a problem are well known and extensively studied in computational theory (Arora and Barak 2009, Sipser 2012). I shall not say much about this dimension but only remark that it is highly quantitative and that the mathematical tractability it provides is due to the availability of standard criteria of comparison, perhaps even idealised but clearly defined, such as the computational resources of a Turing Machine. If you have a "metre", then you can measure lengths. Similarly, if you adopt a Turing Machine as your starting point, then you can calculate how much time, in terms of steps, and how much space, in terms of memory or tape, a computational problem consumes to be solved. For the sake of simplicity—and keeping in mind that finely-grained and sophisticated degrees of precision can be achieved, if needed, by using tools from complexity theory—let's agree to map the complexity of a problem (dealt with by AI in terms of space–time = memory steps required) from 0 (simple) to 1 (complex).

The degrees of difficulty of a problem, understood in terms of the skills required to solve it, from turning on and off a light to ironing shirts, need a bit more of a stipulation to be mapped here because usually the relevant literature, e.g., in human motor development, does not focus on a taxonomy of problems based on resources needed, but on a taxonomy of the performance of the human agents assessed and their abilities or skills demonstrated in solving a problem or performing a task. It is also a more qualitative literature.
In particular, there are many ways of assessing a performance and hence many ways of cataloguing skill-related problems, but one standard distinction is between gross and fine motor skills. Gross motor skills require the use of large muscle groups to perform tasks like walking or jumping, catching or kicking a ball. Fine motor skills require the use of smaller muscle groups, in the wrists, hands, fingers, and the feet and toes, to perform tasks like washing the dishes, writing, typing, using a tool, or playing an instrument.
Despite the previous difficulties, you can see immediately that we are dealing with different degrees of difficulty. Again, for the sake of simplicity—and recalling that finely-grained and sophisticated degrees of precision can be achieved, if needed, by using tools from developmental psychology—let's agree to map the difficulty of a problem (dealt with by AI in terms of skills required) from 0 (easy) to 1 (difficult).

We are now ready to map the two dimensions in *Figura 3*, where I have added four examples.



3 - Translating difficult tasks into complex tasks

Turning the light on is a problem whose solution has a very low degree of complexity (very few steps and states) and of difficulty (even a child can do it). However, tying one's own shoes requires advanced motor skills, and so does lacing them, thus it is low in complexity (easy), but it is very high in difficulty. As Adidas CEO Kasper Rorsted remarked in 2017:

The biggest challenge the shoe industry has is how do you create a robot that puts the lace into the shoe. I'm not kidding. That's a complete manual process today. There is no technology for that.[7]

Dishwashing is the opposite: it may require a lot of steps and space, indeed increasingly more the more dishes need to be cleaned, but it is not difficult, even a philosopher like me can do it. And of course, top-right we find ironing shirts, which is both resource-consuming, like dishwashing, and demanding in terms of skills, so it is both complex and difficult, which is my excuse to try to avoid it. Using the previous examples of playing football and playing chess, football is simple but difficult, chess is easy (you can learn the rules in a few minutes) but very complex, this is why AI can win against anyone at chess, but a team of androids that wins the world cup is science fiction.

The reader will notice that I placed a dotted arrow moving from low-complexity high-difficulty to high-complexity low-difficulty.[8] This seems to me the arrow that successful developments of AI will follow. Our artefacts, no matter how smart, are not really good at performing tasks and hence solving problems that require high degrees of skilfulness. However, they are fantastic at dealing with problems that require very challenging degrees of complexity. So, the future of successful AI probably lies not only in increasingly hybrid or synthetic data, as we saw, but also in translating difficult tasks into complex tasks.

How is this translation achieved? By transforming the environment within which AI operates into an AI-friendly environment. Such translation may increase the complexity of what the AI system needs to do enormously but, as long as it decreases the difficulty, it is something that can be progressively achieved more and more successfully. Some examples should suffice to illustrate the point, but first, let me introduce the concept of enveloping.

In industrial robotics, the three-dimensional space that defines the boundaries within which a robot can work successfully is defined as the robot's envelope. We do not build droids like Star Wars' C3PO to wash dishes in the sink exactly in the same way as we would. We envelop environments around simple robots to fit and exploit their limited capacities and still deliver the desired output. A dishwasher accomplishes its task because its environment—an openable, waterproof box—is structured ("enveloped") around its simple capacities. The more sophisticated these capacities are, the less enveloping is needed, but we are looking at trade-off, some kind of equilibrium. The same applies to Amazon's robotic shelves, for example. It is the whole warehouse that is designed to be robot-friendly. Ditto for robots that can cook[9] or flip hamburgers,[10] which already exist. Driverless cars will become a commodity the day we can successfully envelop the environment around them. This is why it is plausible that in an airport, which is a highly controlled and hence more easily "envelopable" environment, a shuttle could be an autonomous vehicle, but not the school bus that serves my village, given that the bus driver needs to be able to operate in extreme and difficult circumstances (countryside, snow, no signals, no satellite coverage etc.) that are most unlikely (mind, not impossible) to be enveloped. In 2016, Nike launched HyperAdapt 1.0, its automatic electronic self-lacing shoes, not by developing an AI that would tie them for you, but by re-inventing the concept of what it means to adapt shoes to feet: each shoe has a sensor, a battery, a motor,

and a cable system that, together, can adjust fit following an algorithmic pressure equation.[11] Enveloping used to be either a stand-alone phenomenon (you buy the robot with the required envelop, like a dishwasher or a washing machine) or implemented within the walls of industrial buildings, carefully tailored around their artificial inhabitants. Nowadays, enveloping the environment into an AI-friendly infosphere has started to pervade all aspects of reality and is happening daily everywhere, in the house, in the office, and in the street. We have been enveloping the world around digital technologies for decades, invisibly and without fully realising it. The future of AI also lies in more enveloping, for example, in terms of 5G and the Internet of Things, but also insofar as we are all more and more connected and spend more and more time "onlife", and all our information is increasingly born digital. In this case too, some observations may be obvious. There may be problems, and hence relative tasks that solve them, that are not easily subject to enveloping. Yet here it is not a matter of mathematical proofs, but more of ingenuity, economic costs, and user or customer preferences. For example, a robot that iron shirts can be engineered. In 2012, a team at Carlos III University of Madrid, Spain, built TEO, a robot that weighs about 80 kilograms and is 1.8 metres tall. TEO can climb stairs, open doors and, more recently, has been shown to be able to iron shirts (Estevez et al. 2017), although you have to put the item on the ironing board. The view, quite widespread, is that:

'TEO is built to do what humans do as humans do it,' says team member Juan Victores at Carlos III University of Madrid. He and his colleagues want TEO to be able to tackle other domestic tasks, like helping out in the kitchen. Their ultimate goal is for TEO to be able to learn how to do a task just by watching people with no technical expertise carry it out. 'We will have robots like TEO in our homes. It's just a matter of who does it first,' says Victores.

And yet, I strongly doubt this is the future. It is a view that fails to appreciate the distinction between difficult and complex tasks and the enormous advantage of enveloping tasks to make them easy (very low difficulty), no matter how complex. Recall that we are not building autonomous vehicles by putting robots in the driving seat, but by rethinking the whole ecosystem of vehicles plus environments, that is, removing the driving seat altogether. So, if my analysis is correct, the future of AI is not full of TEO-like androids that mimic human behaviour, but is more likely represented by Effie,[12] Foldimate[13] and other similar domestic automated machines that dry and iron clothes. They are not androids, like TEO, but box-like systems that may be quite sophisticated computationally. They look more like dishwasher and washing machines, with the difference that, in their enveloped environments, their input is wrinkled clothes and their output is ironed ones. Perhaps similar machines will be expensive, perhaps they may not always work as well as one may wish, perhaps they may be embodied in ways we cannot imagine now, but you can see how the logic is the correct one: do not try to mimic humans through AI: exploit what machines, AI included, do best. Difficulty is the enemy of machines, complexity is their friend, so envelop the world around them, design new forms of embodiment to embed them successfully in their envelop, and at that point progressive refinements, market scale, and improvements will become perfectly possible.

[7] https://qz.com/966882/robots-cant-lace-shoes-so-sneaker-production-cant-be-fully-automated-just-yet/

[8] I am not the first to make this point, see for example: https://www.campaignlive.co.uk/article/hard-things-easy-easy-things-hard/1498154

[9] http://www.moley.com/

[10] https://misorobotics.com/

[11] Strange thins happen when the software does not work properly: https://www.bbc.co.uk/news/business-47336684

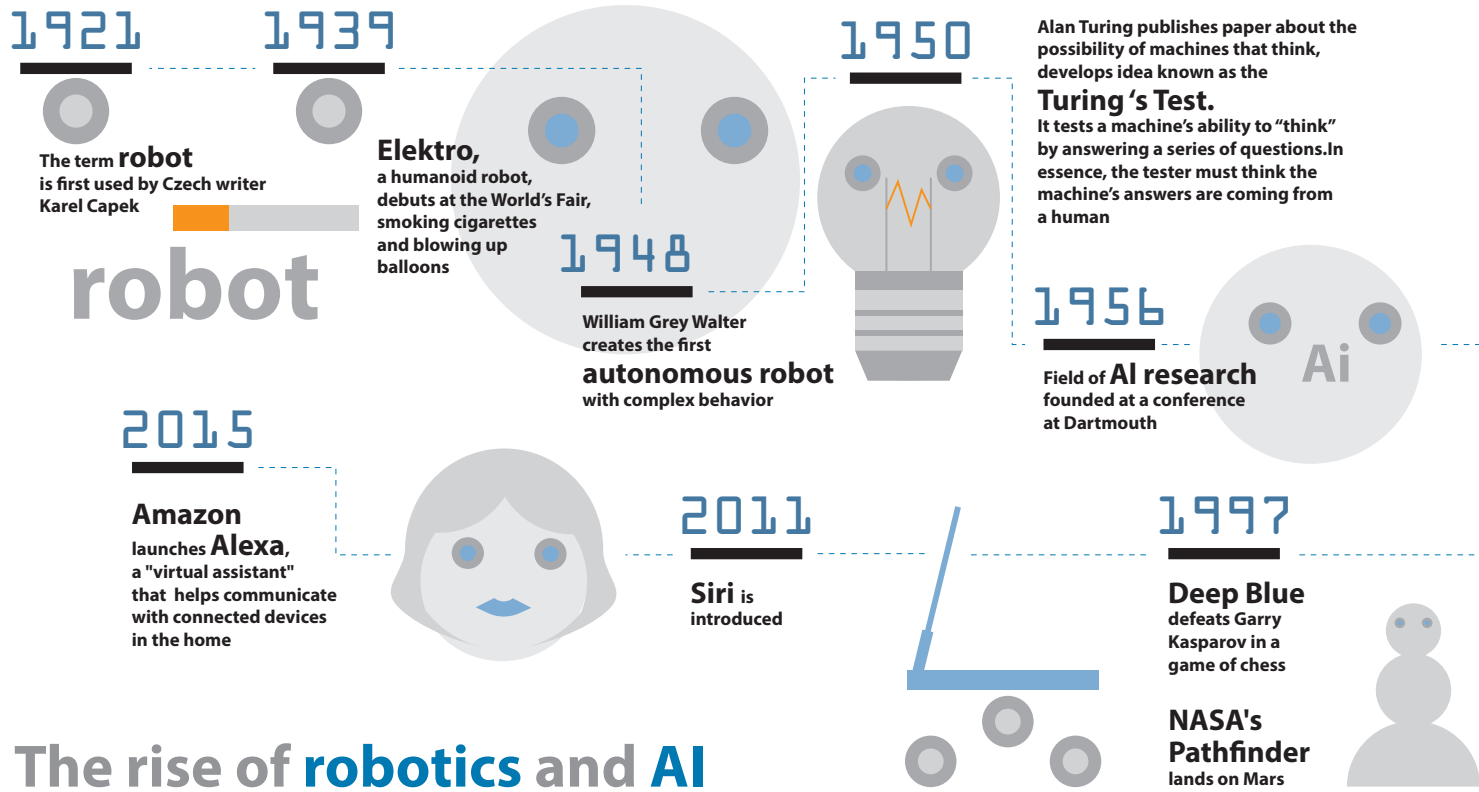
[12] https://helloeffie.com/

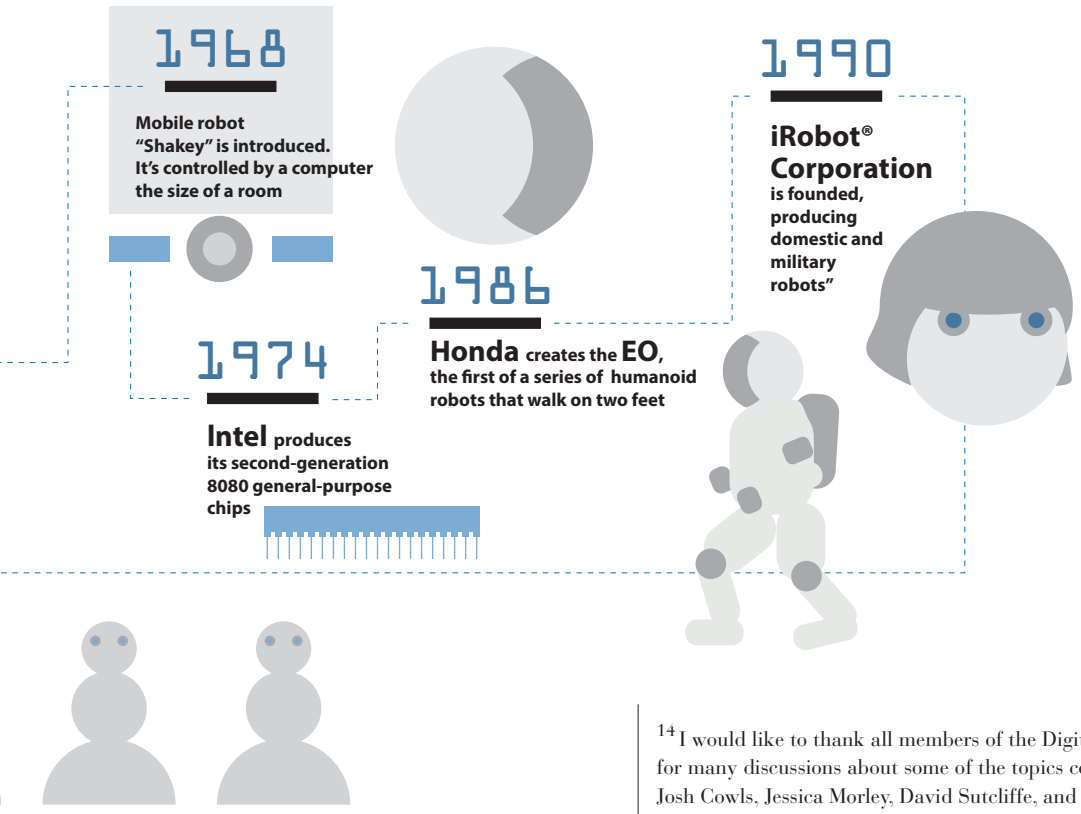
[13] https://foldimate.com/

Conclusion: A Future of Design

The two futures I have outlined here are complementary and based on our current and foreseeable understanding of AI. There are unknown unknowns, of course, but all one can say about them is precisely this: they exist, and we have no idea about them. It is a bit like saying that we know there are questions we are not asking but cannot say what these questions are. The future of AI is full of unknown unknowns. What I have tried to do in this article is to look at the "seeds of time" that we have already sowed. I have concentrated on the nature of data and of problems because the former are what enable AI to work, and the latter provide the boundaries within which AI can work successfully. At this level of abstraction, two conclusions seem to be very plausible. We will seek to develop AI by using data that are as much as possible hybrid and preferably synthetic, through a process of ludification of interactions and tasks. In other words, the tendency will be to try to move away from purely historical data. And we will do so by translating as much as possible difficult problems into complex problems, through the enveloping of realities around the skills of our artefacts. In short, we will seek to create hybrid or synthetic data to deal with complex problems, by ludifying tasks and interactions in enveloped environments. The more this is possible the more successful AI will be. Which leads me to two final comments.

Ludifying and enveloping are a matter of designing, or sometimes re-designing, the realities with which we deal (Floridi 2019). So, the foreseeable future of AI will depend on our design abilities and ingenuity. It will also depend on our ability to negotiate the resulting (and serious) ethical, legal and social issues (ELSI), from new forms of privacy (predictive or group-based) to nudging and self-determination. The very idea that we are increasingly shaping our environments (analog or digital) to make them AI-friendly should make anyone reflect (Floridi 2013). Anticipating such issues, to facilitate positive ELSI and avoid or mitigate any negative ones, is the real value of any foresight analysis. It is interesting to try to understand what the paths of least resistance may be in the evolution of AI. But It would be quite sterile to try to predict "which grain will grow and which will not" and then to do nothing to ensure that the good grains grow, and the bad ones do not (Floridi 2014b). The future is not entirely open (because the past shapes it), but neither is it entirely determined, because the past can be steered in a different direction. This is why the challenge ahead will not be so much digital innovation *per se*, but the governance of the digital, AI included.[14]





[14] I would like to thank all members of the Digital Ethics Lab, OII, Univeristy of Oxford, for many discussions about some of the topics covered in this article, and Nikita Aggarwal, Josh Cowls, Jessica Morley, David Sutcliffe, and Mariarosaria Taddeo for their hugely helpful coments on a last draft.

References

Arora, Sanjeev, and Boaz Barak. 2009. **Computational complexity: a modern approach.** Cambridge: Cambridge University Press.

Campbell, Murray, A Joseph Hoane Jr, and Feng-hsiung J Hsu. 2002. **"Deep blue."** Artificial intelligence 134 (1-2):57-83.

Corea, Francesco. Aug 29 2018. **"AI Knowledge Map: how to classify AI technologies, a sketch of a new AI technology landscape."** Medium - Artificial Intelligence https://medium.com/@Francesco_AI/ai-knowledge-map-how-to-classify-ai-technologies-6c073b969020.

Crawford, Kate, and Jason Schultz. 2014. **"Big data and due process: Toward a framework to redress predictive privacy harms."** BCL Rev. 55:93.

De Fauw, Jeffrey, Joseph R. Ledsam, Bernardino Romera-Paredes, Stanislav Nikolov, Nenad Tomasev, Sam Blackwell, Harry Askham, Xavier Glorot, Brendan O'Donoghue, Daniel Visentin, George van den Driessche, Balaji Lakshminarayanan, Clemens Meyer, Faith Mackinder, Simon Bouton, Kareem Ayoub, Reena Chopra, Dominic King, Alan Karthikesalingam, Cían O. Hughes, Rosalind Raine, Julian Hughes, Dawn A. Sim, Catherine Egan, Adnan Tufail, Hugh Montgomery, Demis Hassabis, Geraint Rees, Trevor Back, Peng T. Khaw, Mustafa Suleyman, Julien Cornebise, Pearse A. Keane, and Olaf Ronneberger. 2018. **"Clinically applicable deep learning for diagnosis and referral in retinal disease."** Nature Medicine 24 (9):1342-1350.

Estevez, David, Juan G Victores, Raul Fernandez-Fernandez, and Carlos Balaguer. 2017. **"Robotic ironing with 3D perception and force/torque feedback in household environments."** 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).

Floridi, Luciano. 2008a. **"The Method of Levels of Abstraction."** Minds and Machines 18 (3):303-329.

Floridi, Luciano. 2008b. **"Understanding epistemic relevance."** Erkenntnis 69 (1):69-92.

Floridi, Luciano. 2010. **Information: a very short introduction.** Oxford: Oxford University Press.

Floridi, Luciano. 2012. **"Big Data and Their Epistemological Challenge."** Philosophy & Technology 25 (4):435-437.

Floridi, Luciano. 2013. **The Ethics of Information.** Oxford: Oxford University Press.

Floridi, Luciano. 2014a. **The Fourth Revolution - How the Infosphere is Reshaping Human Reality.** Oxford: Oxford University Press.

Floridi, Luciano. 2017. **"Digital's cleaving power and its consequences."** Philosophy & Technology 30 (2):123-129.

Floridi, Luciano. 2018. **"What the Maker's Knowledge could be."** Synthese 195 (1):465-481.

Floridi, Luciano. 2019. **The Logic of Information.** Oxford: Oxford University Press.

Floridi, Luciano 2014b. **"Technoscience and Ethics Foresight."** Philosophy & Technology 27 (4):499-501.

Floridi, Luciano, and Jeff W Sanders. 2004. **"On the morality of artificial agents."** Minds and Machines 14 (3):349-379.

Floridi, Luciano, Mariarosaria Taddeo, and Matteo Turilli. 2009. **"Turing's imitation game: still an impossible challenge for all machines and some judges—an evaluation of the 2008 Loebner contest."** Minds and Machines 19 (1):145-150.

Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. **"Generative adversarial nets."** Advances in neural information processing systems.

Howe, Bill, Julia Stoyanovich, Haoyue Ping, Bernease Herman, and Matt Gee. 2017. **"Synthetic Data for Social Good."** arXiv preprint arXiv:1710.08874.

Liang, Huiying, Brian Y. Tsui, Hao Ni, Carolina C. S. Valentim, Sally L. Baxter, Guangjian Liu, Wenjia Cai, Daniel S. Kermany, Xin Sun, Jiancong Chen, Liya He, Jie Zhu, Pin Tian, Hua Shao, Lianghong Zheng, Rui Hou, Sierra Hewett, Gen Li, Ping Liang, Xuan Zang, Zhiqi Zhang, Liyan Pan, Huimin Cai, Rujuan Ling, Shuhua Li, Yongwang Cui, Shusheng Tang, Hong Ye, Xiaoyan Huang, Waner He, Wenqing Liang, Qing Zhang, Jianmin Jiang, Wei Yu, Jianqun Gao, Wanxing Ou, Yingmin Deng, Qiaozhen Hou, Bei Wang, Cuichan Yao, Yan Liang, Shu Zhang, Yaou Duan, Runze Zhang, Sarah Gibson, Charlotte L. Zhang, Oulan Li, Edward D. Zhang, Gabriel Karin, Nathan Nguyen, Xiaokang Wu, Cindy Wen, Jie Xu, Wenqin Xu, Bochu Wang, Winston Wang, Jing Li, Bianca Pizzato, Caroline Bao, Daoman Xiang, Wanting He, Suiqin He, Yugui Zhou, Weldon Haw, Michael Goldbaum, Adriana Tremoulet, Chun-Nan Hsu, Hannah Carter, Long Zhu, Kang Zhang, and Huimin Xia. 2019. **"Evaluation and accurate diagnoses of pediatric diseases using artificial intelligence."** Nature Medicine.

McCarthy, John, Marvin L Minsky, Nathaniel Rochester, and Claude E Shannon. 2006. **"A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955."** AI magazine 27 (4):12.

Rosenblueth, Arturo, and Norbert Wiener. 1945. **"The role of models in science."** Philosophy of Science 12 (4):316-321.

Silver, David, Thomas Hubert, Julian Schrittwieser, Ioannis Antonoglou, Matthew Lai, Arthur Guez, Marc Lanctot, Laurent Sifre, Dharshan Kumaran, Thore Graepel, Timothy Lillicrap, Karen Simonyan, and Demis Hassabis. 2018. **"A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play."** Science 362 (6419):1140-1144.

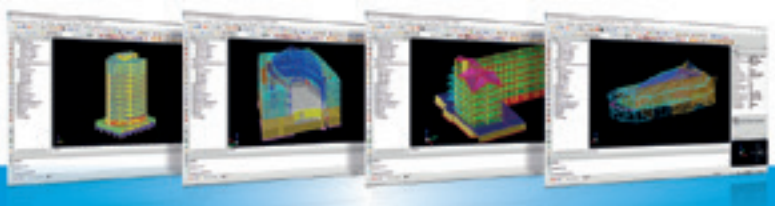
Sipser, Michael. 2012. **Introduction to the theory of computation**. 3rd ed. Boston, MA: Cengage Learning.

Watson, David S., Jenny Krutzinna, Ian N. Bruce, Christopher E.M. Griffiths, Iain B. McInnes, Michael R. Barnes, and Luciano Floridi. forthcoming. **"Clinical Applications of Machine Learning Algorithms: Beyond the Black Box."** British Medical Journal.

concrete
structural engineering software

Sismicad 12. Fluido, adattabile, piu' versatile di quanto pensi.

Confrontati con le sue caratteristiche, guarda i filmati esplicativi, leggi il manuale, provalo e testalo nei casi che ritieni più interessanti. Potrai verificare come Sismicad, con il suo solutore FEM integrato, il facile input 3D (anche in Autocad), le funzionalità BIM, le verifiche per edifici esistenti, i rinforzi, la geotecnica, le murature, l'acciaio, le pareti in legno con giunzioni e molto altro, sia da tempo un software di riferimento seguito da molti professionisti per la sua adattabilità a tutte le esigenze di calcolo strutturale. **Provalo, è più versatile di quanto pensi!**



www.concrete.it

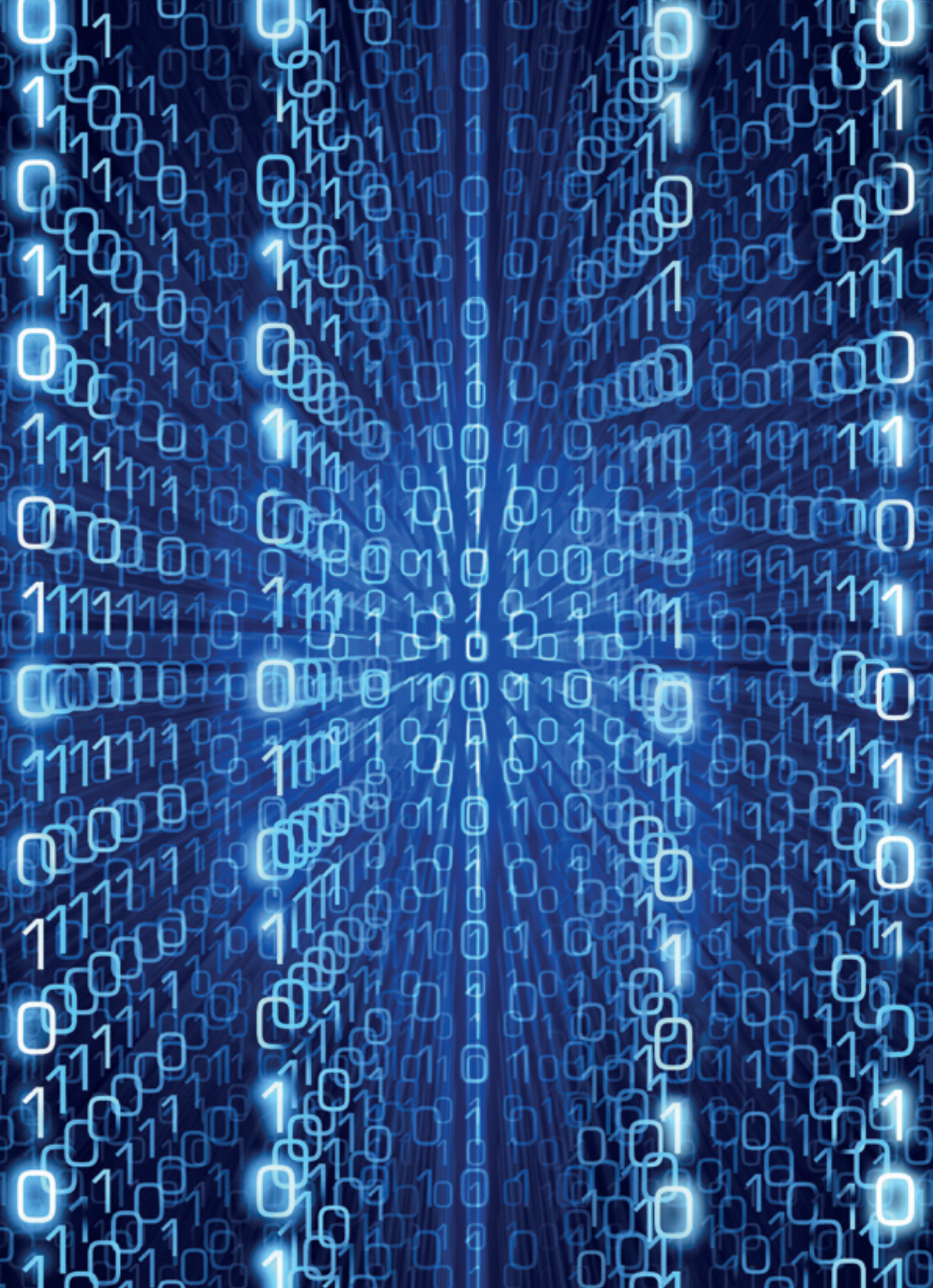
Michele Colajanni

Le opportunità e le sfide ancora aperte del 5G

Una generazione per ogni decennio. A partire dall'1G degli anni '80, ogni decade ci porta una nuova generazione di tecnologie per interconnessioni mobili. Non sorprende, quindi, che gli anni 2020 saranno caratterizzati dal 5G così come è lecito attendersi che il decennio 2030 ci condurrà alla maturità della sesta generazione. Ad ogni generazione, banda più ampia, tipicamente di un ordine di grandezza, minore latenza, e maggiore capacità nel numero di dispositivi interconnessi. Eppure, nessun'altra generazione come la quinta è divenuta oggetto di acceso dibattito geopolitico-industriale. Al confronto, il 4G è passato inosservato. L'interesse strategico del 5G deriva dall'obiettivo di connettere tutto il mondo a banda larga, così come il 6G ha l'ambizione di abilitare le connessioni anche dagli oceani grazie a un'integrazione con la rete satellitare. Connettere tutti gli oggetti e le persone significa aver la possibilità di controllare non tanto i contenuti che saranno cifrati, ma i metadati e, ove necessario, favorire, rallentare o impedire tali interconnessioni. Tuttavia, simili scenari non costituiscono il focus di questa nota.

C'è molto entusiasmo intorno al 5G, ai limiti dell'esagerazione, come se scoprissimo per la prima volta le connessioni a banda larga e le possibili applicazioni. Tuttavia, c'è una novità dirompente: il 5G realizza il sogno di un Internet mobile a banda (veramente) larga. Il suo avvento non sarà la soluzione di tutti i problemi di *digital divide* né ci condurrà in un futuro da fantascienza. Almeno, non da subito. Rimane una potente tecnologia abilitante che, tuttavia, per esprimere le sue potenzialità, avrà bisogno di essere abilitata mediante nuove applicazioni innovative, la maggior parte da inventare e soprattutto da realizzare.

Una volta resi disponibili e affidabili tutti gli strumenti del 5G, ci sono tre livelli da considerare, a complessità crescente: infrastruttura, gestione e applicazioni. L'installazione di antenne per le microcelle 5G è un'opera costosa ma praticabile, la loro gestione efficiente presenta problemi ancora da risolvere, la realizzazione di nuovi servizi mobili, magari integrati con nuovi materiali interconnessi e con applicazioni di realtà aumentata, presenta ampi spazi di ricerca e sviluppo. Il 5G sarà di impatto solo se si realizzeranno applicazioni innovative scalabili, sicure e affidabili in grado di sfruttare le innumerevoli potenzialità della banda larga in mobilità. La partita dell'innovazione a valore aggiunto del 5G si gioca a livello gestionale e applicativo, mentre la ricerca nel settore delle telecomunicazioni è già proiettata verso il 6G: interconnettere tutto il pianeta che è costituito al 70% da oceani; una meravigliosa opportunità per la nascente *blue economy.* Tornando con i piedi sul terreno, rimangono da risolvere problemi gestionali e la realizzazione di nuove applicazioni.



6 cose da sapere riguardo il 5G

1 Una tecnologia G-Whiz

5G è sinonimo di tecnologia wireless di quinta generazione; segue il 4G ma ha una svolta. L'1G e 2G erano basati sulla fornitura di servizi vocali; Il 3G ci ha portato dati mobili; e il 4G l'internet mobile; tuttavia il 5G trasformerà radicalmente il ruolo che la tecnologia mobile gioca nella società.

2 5G spaventosamente veloce

Il 5G potenzierà la velocità di download fino a 20Gb al secondo rispetto alla velocità di 1Gb al secondo del 4G.

3 Più che velocità, affidabilità

Le reti 5G promettono tempi di ritardo nella risposta ridotti che impediscono il fastidioso jitter e altri problemi di esperienza noti come latenza. Con il 5G, gli utenti dovrebbero vedere una latenza massima di appena 4 ms, in calo da circa 20 ms sulle celle LTE. La specifica 5G richiede anche una latenza di appena 1 ms per le ultra-reliable low latency communications.

4

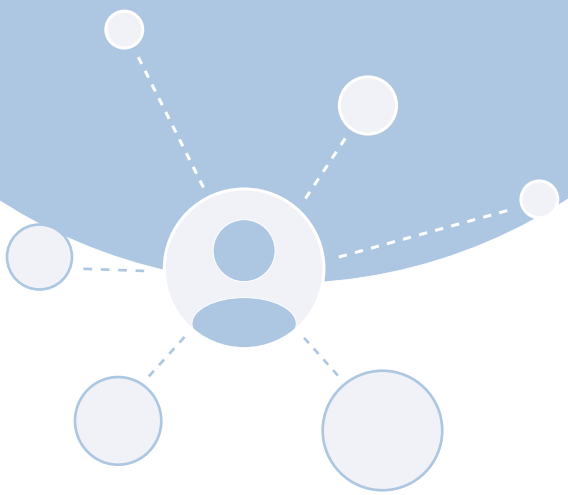
Il grande botto economico

Il 5G scatenerà una crescita economica senza precedenti. La sola catena del valore del 5G potrebbe generare quasi 3,5 trilioni di dollari di entrate e supportare 22 milioni di posti di lavoro entro il 2035. Nel corso del tempo, il 5G stimolerà la crescita del PIL globale reale di 3 trilioni complessivi dal 2020 al 2035.

5

Tecnologia di trasformazione

Il 5G, alla fine, renderà il mobile un insieme di tecnologie che collegano le persone alle persone e le informazioni a un sistema unificato che collega le persone e le “macchine” ad ogni cosa.



6

Maggiore efficienza

Il 5G non solo risulta essere più veloce e quasi senza lag, ma è anche più efficiente. Il 5G consuma infatti meno energia sui dispositivi, il che significa una maggiore durata della batteria. La maggiore capacità della rete 5G comporta anche che sarà in grado di gestire la rapida crescita dei dispositivi connessi, guidata dalla domanda dell’IoT.

leonardocompany.com

Helicopters | Aeronautics | Electronics, Defence & Security Systems | Space

LEONARDO
CYBER SECURITY

Gestione del 5G

5G, a livello di standard, deve garantire sulla stessa infrastruttura fisica diverse tipologie di utilizzo: il potenziamento della banda larga mobile (*enhanced Mobile Broadband* o eMBB), comunicazioni estremamente affidabili e a bassa latenza (*Ultra Reliable Low Latency Communications* o uRLLC) e l'interconnessione robusta ed economica di miliardi di dispositivi (*massive Machine Type Communications* o mMTC). Le risorse assegnate a ciascun servizio devono soddisfare i requisiti dell'applicazione e al contempo massimizzare l'utilizzo delle risorse dell'infrastruttura fisica che sta supportando servizi con diverse esigenze.
La gestione efficiente e scalabile in tempo reale delle risorse per offrire funzioni differenti è una sfida emergente che deve essere affrontata dai provider con la collaborazione della comunità di ricerca accademica e industriale. La sfida è aperta soprattutto quando vi sono da supportare servizi con requisiti di prestazioni e affidabilità stringenti e con la presenza di elevato traffico eterogeneo. In tali scenari è necessario individuare soluzioni innovative che siano in grado di sfruttare le enormi quantità di dati fornite dalla rete sottoponendole a un apprendimento continuo che produca conoscenza cognitiva ai fini di una gestione efficace di tutte le risorse end-to-end coinvolte nelle comunicazioni 5G.
Le prestazioni con garanzia di *Quality of Service* (QoS), infatti, non coinvolgono solo l'infrastruttura radio, ma anche la rete core costituita da connessioni tipicamente in fibra ottica e da datacenter specializzati.
Le interdipendenze esistenti tra rete radio, rete wired e datacenter non possono essere ignorate, ma gli effetti e le soluzioni sono ancora oggetto di studio.Inoltre, i requisiti di QoS end-to-end di alcune applicazioni aprono nuovi scenari a livello di progettazione e dislocazione dei data center. Dopo una decade di orientamento generalizzato verso il cloud, rientrano in gioco i *data center metropolitani* e l'*edge computing* per le smart city, per l'Industria 4.0 e per alcune applicazioni sanitarie. Non sono cambiamenti indotti dalla moda informatica del momento o dal marketing come si sente dire con superficialità. È irriverente ritenere che miliardi di investimenti tecnologici possano seguire i gusti degli architetti informatici come se fossero trend degli stilisti. La verità è che il traino dei cambiamenti è determinato dalla continua evoluzione delle caratteristiche della rete e delle applicazioni in rete: le connessioni limitate e prestazionalmente scadenti degli anni '80 e '90 portano verso l'informatica distribuita; viceversa, connessioni di ottime qualità e diffuse sul territorio consentono il cloud computing; servizi che necessitano di bassissima latenza e massima affidabilità preferiscono l'edge computing anche in presenza di reti wired e wireless buone, ma non ancora tali da soddisfare i requisiti delle applicazioni in tempo reale.

Applicazioni

La rivoluzione del 5G non riguarda realmente la tecnologia, ma gli utenti di tale tecnologia e avrà un impatto significativo solo se riuscirà a modificare radicalmente i processi che gli utenti utilizzano per massimizzare il valore percepito dai servizi forniti. È stato così per il 2G che ha aperto la strada alla telefonia mobile diffusa; analoga rivoluzione c'è stata con il 3G che ha consentito la navigazione Internet in movimento modificando le modalità di comunicazione, la fruizione dei servizi informatici e le possibilità di lavoro anywhere-anytime; non si è sperimentato nulla di altrettanto dirompente con il 4G; c'è molta attesa mediatica per il 5G che, tuttavia, deve ancora concretizzarsi. Le connessioni in fibra ottica sono operative da tempo. Chi vive nelle città e nelle aree industriali ben fornite non percepirà grandi cambiamenti. Gli impianti industriali, al loro interno, possono già usufruire di reti a larga banda, elevata affidabilità e nessun rumore; non è scontato che necessiteranno del 5G. Potrebbero beneficiarne le persone e aziende che non sono ben connesse, ma questo rappresenta un passo verso la civiltà, non una rivoluzione dirompente. La vera novità del 5G è costituita dalla mobilità. Poter collegare persone, dispositivi e dati in modo innovativo e in mobilità a banda larga significa che le applicazioni non saranno più utilizzabili o meno a seconda della posizione. L'utente potrà usufruire di qualsiasi servizio informatico in qualsiasi luogo portando a pieno compimento l'obiettivo dell'anywhere-anytime previsto già nella seconda metà degli anni '90. Tuttavia, non è più o non è solo la crescita degli uomini connessi che spingerà al miglioramento; saranno le "cose", anche se oggi non vi sono molte applicazioni che necessitano di larga banda in mobilità. Il 3G e il 4G funzionano benissimo per tutte le realtà che non richiedono trasmissioni da 1 a 10 Giga al secondo proprie del 5G.
Le principali sfide ICT del prossimo futuro sono delineate: tecnologie di interconnessione a banda larga rese disponibili su ampia scala, diffusione degli oggetti interconnessi (IoT) in tutti i settori, quali industria, difesa, sanità, mobilità, agricoltura, domotica, avvento della realtà aumentata anche in campo formativo, maggiore autonomia delle macchine e delle applicazioni dotate di strumenti di apprendimento automatico che saranno gli unici a poter gestire in tempo utile le enormi quantità di dati generati.

Serve il 5G per tutto questo? In parte sì, ma le novità più dirompenti sono da attendersi dagli sviluppi del mondo fisico che combinerà nuovi materiali *touch,* nanotecnologie e biomateriali con capacità adattative e di interconnessione. E la maggior parte di questi nuovi oggetti e applicazioni saranno in mobilità, trasferiranno e acquisiranno grandi quantità di dati, avranno bisogno di basse latenze, da cui la necessità di avere una rete Internet mobile a banda larga. Senza una vera innovazione dal punto di vista dell'IoT, il 5G rischia di migliorare il download e l'upload degli attuali servizi informatici in mobilità: un miglioramento incrementale apprezzabile, ma lungi dalla rivoluzione attesa dall'avvento del 5G. Per sfruttare appieno le sue potenzialità serve sia visione sia capacità di realizzazione applicativa. Cercansi sviluppatori di nuove applicazioni e soprattutto idee che vadano oltre la possibilità di vedere un film ad alta definizione o di giocare su un tablet in movimento. Gaming, sanità, logistica, trasporti, realtà aumentata appaiono in pole position, ma solo perché ragioniamo in senso evolutivo e non disruptive. La disponibilità tecnologica crea nuove esigenze, ed è per questo che la vera sfida è l'individuazione della *killer application* del 5G. Saranno le decine di miliardi di veicoli, oggetti e materiali intelligenti interconnessi, le nuove applicazioni di realtà aumentata e virtuale, le video conferenze e i giochi immersivi in mobilità, le innumerevoli applicazioni che nasceranno dalla medicina, dalle realtà industriali più innovative e dagli ambiti militari che hanno sempre costituito un fondamentale driver tecnologico? È un problema ricorrente della società digitale e il 5G non fa eccezione: nel momento in cui avremo a disposizione tutte le tecnologie che ci abiliteranno all'interconnessione mobile a banda larga, il limite all'innovazione, quella vera, dirompente, sarà costituito dalla fantasia. Per potenziarla bisognerebbe orientare gli investimenti verso le idee parallelamente ai fondi destinati alle infrastrutture. Ed è bene precisarlo, no, l'intelligenza artificiale non ci aiuterà in questa sfida delle idee.

MapeWrap® EQ System

LA RISPOSTA **SICURA** IN CASO DI **TERREMOTO**

MapeWrap EQ Adhesive:
Adesivo monocomponente all'acqua pronto all'uso in dispersione poliuretanica

MapeWrap EQ Net:
Tessuto bidirezionale in fibra di vetro pre-apprettato

Il sistema di **presidio brevettato** e **certificato** nei confronti delle **azioni sismiche**, indicato per l'**ANTIRIBALTAMENTO** delle tramezze e dei tamponamenti.

SISMABONUS

Rinforza con Mapei e ottieni le detrazioni fiscali sugli interventi di riduzione del rischio sismico.

È TUTTO **OK**, CON **MAPEI**

Scopri di più su **rinforzo-strutturale.it**

MAPEI
ADESIVI · SIGILLANTI · PRODOTTI CHIMICI PER L'EDILIZIA

Gianluca Di Fusco, Luisa Franchina,
Davide Lamanna

Security by design: automazione e conformità adattiva per infrastrutture IT resilienti

"Fact does not come from the grand leaps of discovery but rather from the small, careful steps of verification."

Pete Herzog

Nell'ambito della *software engineering,* con il termine *security by design* si intende un software progettato, fin dalla prima fase di sviluppo, per essere sicuro.
Nello scenario attuale le pratiche malevole di attacco e modifica delle componenti software, inerenti alle varie architetture informatiche sia in ambito pubblico che privato, sono in continua crescita. Il concetto alla base dell'applicazione della *security by design* consiste nel cercare di minimizzare gli impatti su infrastrutture, applicazioni e servizi scaturenti da queste attività, nonché di salvaguardare i dati contenuti al loro interno.

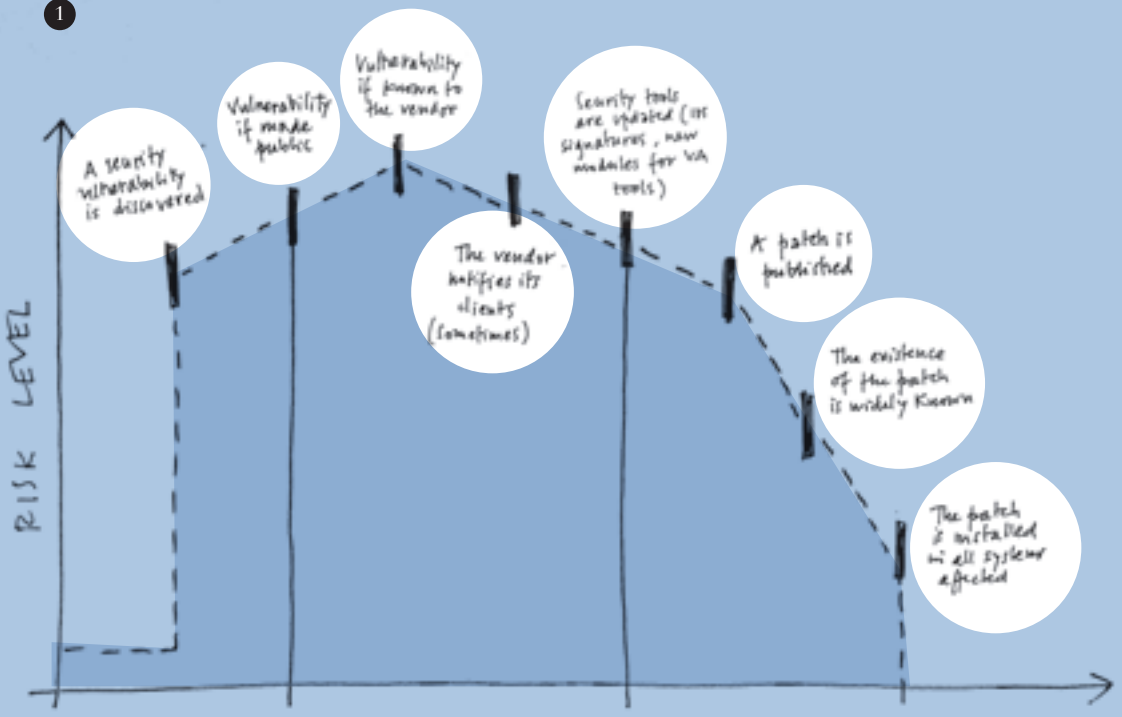
Gli strumenti a disposizione degli sviluppatori sono molteplici e possono essere applicati lungo le diverse fasi dello sviluppo, dalla progettazione sino al testing. Tuttavia, nonostante ciò, la maggior parte dei sistemi vengono colpiti da attacchi che sfruttano vulnerabilità dei software. Principalmente tali vulnerabilità possono essere ricondotte ad errori presenti nel codice, errori che possono mettere a rischio la sicurezza dei dati che vengono trattati. Si fa riferimento a vulnerabilità di sicurezza quando ci si trova di fronte ad un problema del software di cui è stato scoperto un metodo (*exploit*) sfruttabile a vantaggio dell'attaccante; in assenza di tali veicoli di attacco siamo in presenza di un semplice bug.

Le vulnerabilità nell'ICT hanno un loro ciclo di vita; dal momento in cui vengono scoperte sino al momento in cui viene applicata la dovuta correzione (la *patch*) cambia il livello di rischio a cui si è esposti.

In particolare, le fasi più pericolose possono essere ricondotte sostanzialmente all'istante in cui la vulnerabilità viene comunicata al pubblico sino al momento in cui viene effettuato un primo intervento di aggiornamento dei tool necessari all'attuazione della correzione (*Figura 1*).[1]

[1] https://www.cybersecurity360.it/nuove-minacce/sicurezza-software-e-vulnerabilita-informatiche-che-ce-da-sapere/

1



2

1 – Ciclo di vita delle vulnerabilità di sicurezza – Fonte OWASP
2 – Ciclo della IT Automation

Il problema delle vulnerabilità ed il relativo discorso inerente la sicurezza dei sistemi assume oggi una connotazione particolare se si prendono in considerazione le moderne tecniche di *IT Automation* e la loro estensione alle principali tecnologie/metodologie presenti nell'infrastruttura IT aziendale.

La scalabilità senza precedenti richiesta oggi ai moderni e dinamici ambienti IT si può ottenere solo attraverso l'automazione. In particolare, la continua ricerca della riduzione della complessità tramite il ricorso all'automazione all'interno delle strutture software/hardware aziendali richiede un costante e rapido scambio di informazioni tra gli attori impegnati nelle business unit relative ai reparti Development e Operations dell'IT. Questi hanno la necessità di operare uno sviluppo costante degli ambienti software verso una semplificazione della gestione IT, da un lato, e verso la ricerca continua della conformità, dall'altro. La conformità, e in particolare una conformità adattiva, è quanto riteniamo occorra per far fronte in modo nuovo ed efficace alla crescente minaccia delle azioni malevole intraprese dagli attaccanti nello sfruttare le vulnerabilità dei sistemi.

Il ruolo della IT Automation

Con automazione dell'IT, anche detta automazione dell'infrastruttura, si intende l'uso di software per creare istruzioni e processi ripetibili con i quali sostituire o ridurre l'interazione del personale con i sistemi IT (*Infrastructure as a Code*). I software di automazione operano entro i vincoli delle istruzioni, degli strumenti e delle strutture date, per eseguire le attività con un intervento manuale minimo o nullo. Grazie all'impiego dell'automazione i tool software, i framework e gli applicativi in generale riescono a condurre i propri task con il minimo intervento da parte degli addetti ai lavori.

Generalmente essa si basa su strumenti software per riuscire a definire e gestire una serie prescritta di azioni dettagliate immesse manualmente o tramite "trigger" esterno. Con l'automazione sostanzialmente vengono sostituite una serie di azioni che in precedenza venivano svolte manualmente con tempi più lunghi e tassi di errore più alti. L'automazione è una scelta strategica che consente l'ottimizzazione dell'IT e la trasformazione digitale dei processi. Infatti l'inserimento in azienda di processi automatizzati risulta particolarmente utile quando si vanno a industrializzare quelle attività che un amministratore IT o il suo personale devono eseguire di frequente; la possibilità di poter affidare ad un processo automatizzato determinate mansioni fa guadagnare tempo alle risorse umane e permette una considerevole riduzione degli errori e dei costi per l'impresa (*Figura 2*).[2]

[2] https://searchitoperations.techtarget.com/definition/IT-automation

[3] Processo mediante il quale un amministratore di sistema assegna risorse e privilegi, non solo agli utenti di una rete ma anche a chi le utilizza da remoto (ad esempio i fornitori).

Ma cosa prevede l'automazione dell'IT e quando risulta essere una pratica indicata?

In linea teorica, è possibile automatizzare qualsiasi processo IT, almeno in parte. L'automazione può essere applicata e integrarsi all'automazione della rete, al *provisioning*[3] di risorse e servizi cloud e infrastrutturali nonché al *deployment* delle applicazioni e alla gestione delle configurazioni. Inoltre, proprio in virtù del fatto che è possibile automatizzare la maggior parte dei processi, l'automazione può configurarsi come una pratica indicata in qualsiasi scenario; un approccio globale all'automazione dell'IT può evitare al personale di dedicarsi a processi ripetitivi e manuali, consentendo una maggiore produttività, riducendo gli errori, migliorando la collaborazione e offrendo più tempo da destinare ad attività che richiedono maggiori capacità decisionali e di valutazione.

In particolare, in merito all'attività di provisioning, essa è nel complesso un'attività onerosa sia che venga svolta su ambienti fisici che in cloud. Per un più efficiente funzionamento dei sistemi aziendali è indispensabile un'infrastruttura che possa essere operata ed orchestrata come se fosse software. I Data Center che ospitano rack, apparati e cavi, oggi rappresentano il luogo fisico di creazione e gestione di risorse virtualizzate come reti, sistemi di storage, container e macchine virtuali. La maggior parte di questi elementi è oggi definita da software (*Software Defined Data Center*), aspetto questo che ha contribuito ad aumentare la scalabilità e ad aprire la strada a molteplici possibilità di integrazione e gestione. Inoltre, il passaggio al software garantisce (e richiede) la codifica dei processi. Ciò consente di soddisfare in modo preciso e granulare le richieste dell'azienda, che opera quindi con maggiore consapevolezza dei costi e dei vincoli in termini di tempo.

Proprio in questo ambito si colloca l'automazione. Configurare diversi ambienti applicando manualmente i modelli di configurazione è un'attività che porta via molto tempo; problema questo che può essere risolto proprio grazie alla codifica, che permette di eseguire queste operazioni grazie all'applicazione di un modello unico e standard.
Una volta sviluppato ed integrato il modello, si può impostare l'esecuzione automatica e autonoma delle regole e dei passaggi previsti. Un'automazione che si integra nell'infrastruttura e nei sistemi di gestione esistenti per la gestione dei deployment nel Data Center, consente di usufruire appieno delle risorse che sono già a disposizione per raggiungere obiettivi prefissati.

Tuttavia, non tutte le applicazioni vengono dispiegate nello stesso modo; le stesse possono infatti presentare diverse impostazioni, richiedere diversi file system, abilitare utenti particolari, determinate porte, ecc.. Una volta automatizzato il *provisioning*, sarà necessario dare istruzioni a tutte queste risorse. Memorizzare le caratteristiche di un ambiente applicativo in un documento, foglio di calcolo, file di testo non aiuta a ottenere un ambiente ripetibile e solido nel quale ospitare le applicazioni. Man mano che i sistemi e le complessità aumentano, diventa indispensabile registrare il profilo dei sistemi per poterli gestire in modo efficace e ripetibile. Per ottenere tale risultato è necessario adottare una solida soluzione che sia in grado di gestire le configurazioni e che consenta agli sviluppatori di definire semplicemente l'infrastruttura (fisica, virtualizzata, in cloud ecc.) in modo che possa essere facilmente compresa da tutto il personale IT.[4]

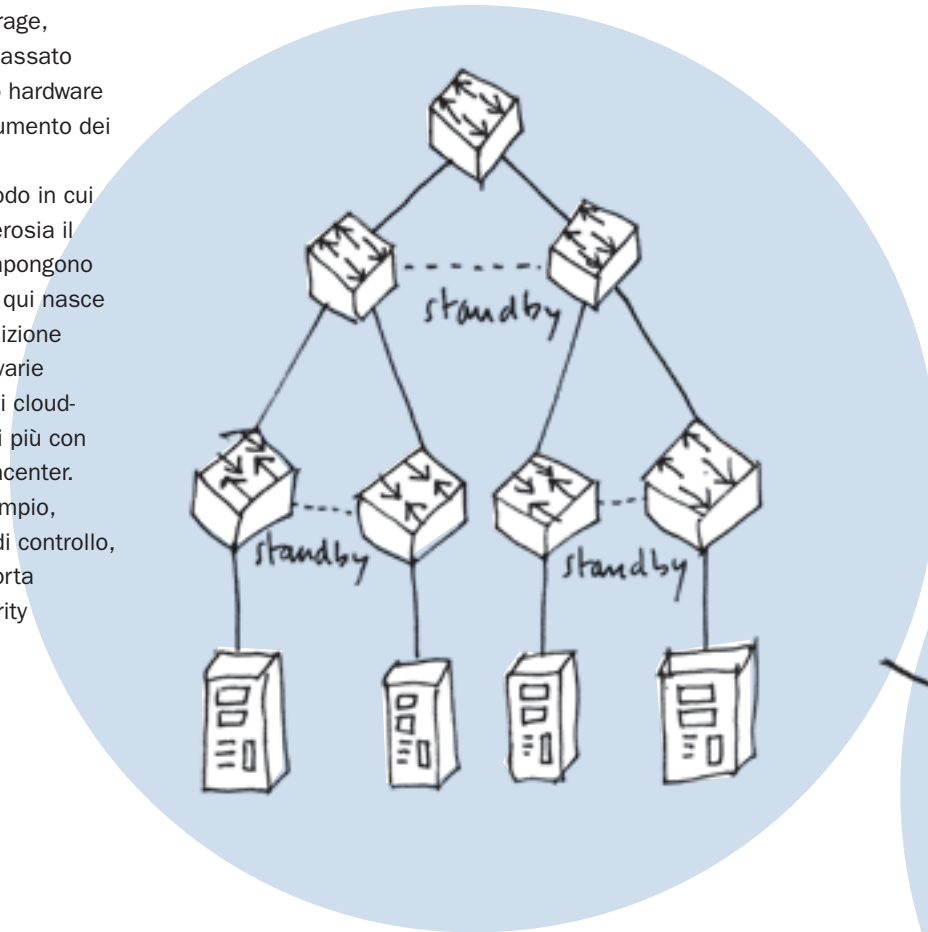
Più semplice è l'automazione di script e di pratiche specifiche per la gestione del sistema, più facile risulterà portare a termine le attività. Occorre dunque gestire le configurazioni in modo snello e riproducibile, usando tool e pratiche di automazione di ambienti di sviluppo e produzione. Questi ultimi, al pari di altri elementi software dello stack, vengono gestiti e versionati usando linguaggi che sono contemporaneamente *machine-readable* e *human-readable*. Ciò consente una loro istantanea riproduzione in caso di necessità di espansione o di rimedio a disastri di qualsiasi tipo: si è subito pronti con gli ambienti e quindi immediatamente operativi con lo sviluppo. Anche il deployment delle applicazioni diventa un'operazione automatica, infinitamente riproducibile e priva di errori umani.
Si parla di auto-documentazione, in quanto la descrizione degli ambienti di sviluppo, test e produzione avviene in modo formale e comprensibile sia dall'essere umano che dalla macchina, potendo essa stessa subire il ciclo di revisione e miglioramento progressivo del software.

Qual è dunque il ruolo della Cyber Security in tale contesto e come muta l'approccio al mantenimento di alti livelli di sicurezza?

Con l'introduzione del Cloud e delle Infrastrutture IT automatizzate, si industrializza e velocizza il rollout di nuovo software e si introduce una Quality of Experience nettamente superiore per gli operatori ed i responsabili della sicurezza. Ogni aspetto della configurazione dei sistemi e delle applicazioni viene messo facilmente sotto controllo. La sfida diventa la ricerca continua di conformità della configurazione delle componenti IT nei diversi livelli di astrazione, di aderenza agli standard industriali, una continua tensione verso le buone prassi in incessante evoluzione. Diversamente dal passato questa ricerca di conformità può essere condotta in modo sistematico e non artigianale, senza rinunciare ad usufruire dinamicamente dell'infrastruttura, adattandosi *on-demand* a richieste di banda/computing e storage comunque mutevoli nel tempo: giovandosi essa stessa di tale dinamicità diviene una ricerca di *conformità adattiva.*

Il Software Defined Datacenter ha introdotto un cambio di paradigma nell'implementazione di sistemi di storage, networking, capacità computazionale e security. In passato il networking e la security erano relegate in un unico hardware dedicato. Questo necessariamente portava ad un aumento dei costi operativi e della complessità di gestione.
Oggi nelle architetture software-defined cambia il modo in cui i vari elementi interagiscono e l'orchestrazione, ovverosia il dispiegamento su scala temporale dei task che compongono le operazioni, acquisisce un'importanza centrale. Di qui nasce l'attenzione per i framework che supportano la definizione delle modalità in cui la security deve evolvere nelle varie componenti architetturali del datacenter e dei servizi cloud-based. Tali framework dovranno integrarsi sempre di più con le principali piattaforme per il Software Defined Datacenter.
I sistemi per il Software Defined Networking, ad esempio, esaltano il concetto di disaccoppiamento tra piano di controllo, che indirizza e dirige i flussi, e piano dati, che trasporta il traffico; concetto che è centrale in ambito di Security Governance.

L'approccio tradizionale alla sicurezza delle infrastrutture, è basato sulla sicurezza perimetrale e sulla protezione dei punti di ingresso. Ma i pattern di traffico all'interno dei Data Center hanno subito una metamorfosi notevole, estendendo la superficie di attacco e aumentando il numero di punti da monitorare. Del resto i Firewall non possono essere collocati ovunque. Né esistono soluzioni tradizionali per progettare le infrastrutture effimere. Di qui nasce il concetto di microsegmentazione in domini virtuali, che coprono tutta la superficie di attacco. Proteggendo ogni dominio microsegmentato, si protegge l'intera infrastruttura sia in direzione Nord-Sud, ossia relativamente al traffico tra il Datacenter e tutto ciò che sta fuori dal Datacenter (come da approccio tradizionale), che in direzione Est-Ovest (traffico inter host all'interno del Datacenter), considerando non *trustful* anche il traffico intra-host (all'interno del singolo host tra diverse risorse virtualizzate al suo interno). Access Control List e policy di sicurezza vengono così applicate a tutte le risorse fisiche e virtuali del Datacenter, in modo da contenere gli attacchi e minimizzare l'impatto delle intrusioni.



[4] https://www.redhat.com/it/topics/automation/whats-it-automation

[5] SOFTWARE-DEFINED IT, IPERCONVERGENZA E CLOUD, Roma - 06 Aprile 2016, Kelen Zakelj - Soiel.it

Soluzioni innovative per la Cyber Security in contesti di Software Defined IT devono quindi:

- essere integrate nativamente nei flussi di orchestrazione e automazione;
- essere integrate nativamente nei flussi di orchestrazione e automazione (SDN);
- semplificare l'applicazione delle politiche di sicurezza anche nei flussi di traffico Est-Ovest;
- mantenere il controllo dei canali di comunicazione tra i diversi host virtuali;
- evitare movimenti laterali di agenti malevoli (compromissione o danneggiamento di servizi o sottrazione di dati sensibili).[5]

La microsegmentazione in domini virtuali protetti realizza la cosiddetta *Zero Trust security*. Zero trust è un modello di sicurezza basato sul principio di mantenere severi controlli di accesso e di non fidarsi di nessuno per impostazione predefinita, anche quelli già all'interno del perimetro della rete, in base al concetto "never trust, always verify".

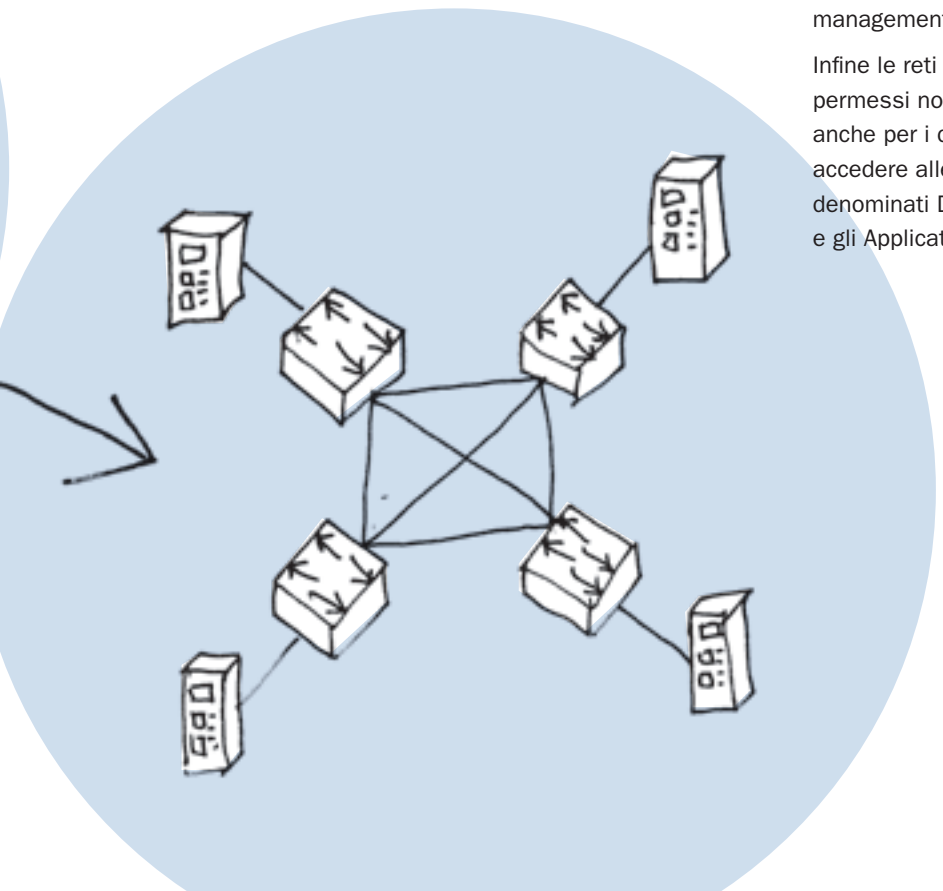
Una *Zero Trust* network deve soddisfare i seguenti requisiti:

- essere indipendente dalla piattaforma e pronta per l'integrazione di risorse virtuali, e.g. Virtual Machine;
- avere un'architettura orientata al soddisfacimento di obiettivi di conformità adattiva;
- essere scalabile e flessibile;
- avere un'architettura segmentata;
- essere estensibile.

Una rete gerarchica tradizionale deve evolvere versa una topologia maggiormente piatta e magliata *(meshed).*

Deve inoltre essere *fabric-friendly* ovvero orientata ad un approccio industriale alla sicurezza, il che conduce ad un approccio alla conformità adattiva. Oltre a garantire un accesso sicuro, è necessario poter ispezionare e loggare ogni tipo di traffico, funzione che viene svolta da specifici elementi denominati *segmentation gateway* che svolgono molteplici funzioni di controllo in diversi livelli di astrazione (firewall, intrusion prevention system, access control, account management, protocolli crittofrafici).

Infine le reti Zero Trust abilitano meccanismi di ruoli e permessi non solo per gli utenti e per le applicazioni, ma anche per i dati, che vengono trattati come entità viventi per accedere alle quali è necessario utilizzare speciali identificativi denominati Data ID (in analogia con gli User ID e gli Application ID).



Tecnologia dei Container e metodologia DevOps

Il processo di automazione dell'IT, viene applicato anche attraverso tecnologie specifiche quali i container e anche ad alcune metodologie come il DevOps.

I container consentono il frazionamento del software in *Microservices,* ovvero servizi elementari in cui viene decomposto un servizio complesso. I microservizi vengono incapsulati in strutture autoconsistenti, i container appunto. La Service Oriented Architecture (SOA) ha mandato in pensione lo sviluppo di applicazioni monolitiche, ma ha lasciato in piedi dipendenze funzionali pesanti tra i vari strati architetturali (front-end, back-end, DB…) che di fatto non hanno semplificato di molto la gestione di progetti software via via più complessi. Oggi si tende invece a disaccoppiare drasticamente le componenti funzionali elementari, conferendo piena autonomia ad ognuna (es., un DB per ogni microservizio) e coordinandole liberamente in grafi orientati in continua evoluzione. Si sposta quindi la complessità sul networking, gestibile in modo trasversale e generale.

Ognuno di questi microservizi viene containerizzato in modo da renderlo auto-consistente e portabile in altri ambienti. Nelle immagini dei container viene inserito quanto necessario al deployment dei container in un ambiente diverso, portandosi dietro tutte le dipendenze necessarie, le quali non devono quindi essere soddisfatte nel nuovo ambiente. I container sono oggetti leggeri, che favoriscono la scaling orizzontale, ovverosia la creazione di nuovi container identici e messa in batteria per scopi di bilanciamento e affidabilità. Versionando le immagini dei container si ottiene software costantemente aggiornato e, ciononostante, immediatamente disponibile per deployment istantanei su infrastrutture che sono, a loro volta, immutabili e riproducibili in virtù degli strati precedenti.

I container consentono dunque l'esecuzione delle applicazioni e delle relative dipendenze, in processi isolati dalle risorse hardware e software sottostanti e offrono notevoli vantaggi rispetto alle macchine virtuali. La differenza fondamentale tra la tecnologia container e la classica virtualizzazione si trova a livello del sistema operativo. Di fatti nei container, il sistema operativo viene condiviso tra tutte le istanze in esecuzione su di esso, formula questa che garantisce una forte riduzione in termini di risorse computazionali e di memoria utilizzate.
I molteplici benefici apportati dall'adozione di soluzioni basate su container stanno spingendo le aziende a pianificare progetti di migrazione verso questa soluzione, specie in contesti *cloud-native.* In particolare, sono molteplici gli scenari che hanno tipicamente come target le soluzioni a container come ad esempio:

Creazione di un ambiente multi-cloud: la forte standardizzazione e la portabilità dei container facilitano la creazione di ambienti ibridi e multi-cloud.

Adozione di metodologie DevOps: i container facilitano l'adozione di metodologie DevOps supportando l'intera pipeline di sviluppo ed abilitando rilasci automatici ed incrementali direttamente nell'ambiente di produzione.

Il vero punto di forza della tecnologia container risiede nel fatto che essa è supportata dalla complementarietà alla classica virtualizzazione e da una serie di benefici garantiti dalla sua adozione quali:

Implementazione rapida: in quanto ogni applicazione viene compressa all'interno di un singolo componente che può essere in questo modo facilmente configurato e rilasciato tramite riga di comando. Essendo auto consistente, il container non necessita di lunghe procedure di configurazione all'interno degli ambienti di produzione.

Scalabilità: la scalabilità orizzontale può essere gestita facilmente tramite la riconfigurazione del singolo container grazie all'aumento delle risorse computazionali dedicate. In merito alla scalabilità verticale, essa può essere automatizzata attraverso l'implementazione di un orchestratore che si occuperà della duplicazione del container in esecuzione creando un pool di istanze racchiudibili in cluster definiti.

Portabilità: grazie alla forte standardizzazione della soluzione, i container facilitano la portabilità delle applicazioni semplificandone il ciclo di sviluppo, test e rilascio.

Isolamento: in quanto ogni applicazione è isolata rispetto alle altre in esecuzione sulla medesima infrastruttura fisica e tutte le componenti computazionali vengono virtualizzate a livello di sistema operativo.

Il piacere di progettare, il nuovo e l'esistente.

ORA A 64BIT ANCORA PIÙ VELOCE

MasterSap è un software semplice e veloce per calcolare e verificare strutture nuove ed esistenti.

Innovativo, intuitivo, completo. L'utilizzo di MasterSap è immediato e naturale anche grazie all'efficienza degli strumenti grafici e alle numerose modalità di generazione del modello, anche da disegno architettonico.
BIM. MasterSap sposa la filosofia di progettazione "Open BIM" che porta alla condivisione dei dati di progetto con il maggior numero di attori coinvolti nel cantiere edilizio grazie alla compatibilità con lo standard IFC.
Top performance. Il solutore, potente ed affidabile, conclude l'elaborazione in tempi rapidissimi; i postprocessori per c.a., acciaio, legno, muratura, integrati fra loro, completano, in modo immediato, dimensionamento e disegno di elementi e componenti strutturali.
L'affidabilità dell'esperienza. MasterSap conta un numero straordinario di applicazioni progettuali che testimoniano l'affidabilità del prodotto e hanno contribuito a elevare i servizi di assistenza a livelli di assoluta eccellenza.
Condizioni d'acquisto insuperabili, vantaggiose anche per neolaureati e giovani ingegneri.

AMV s.r.l. - Via San Lorenzo, 106
34077 Ronchi dei Legionari (GO)
Tel. 0481.779.903 r.a. - Fax 0481.777.125
info@amv.it - www.amv.it

AMV SOFTWARE COMPANY

Efficienza: in quanto il consumo di risorse viene limitato grazie alla condivisione di un unico sistema operativo e grazie alla virtualizzazione dei soli componenti necessari all'esecuzione dell'applicazione.

Tuttavia, i container non sono esenti da problematiche di sicurezza; vi sono cinque principali problematiche che riguardano l'utilizzo di questa tecnologia:

- Exploit del kernel: la condivisione del kernel della macchina host espone, in caso di attacco che sfrutti vulnerabilità del sistema operativo, tutti i container basati su di essa. In ambito container quindi risulta di fondamentale importanza l'attività di patching (correzione) del sistema operativo host.

Attacchi Denial of Service (DoS): nel caso in cui ad un container venisse data la possibilità di accedere a risorse illimitate sul sistema host, lo sfruttamento di una vulnerabilità o di un errore di programmazione dell'applicazione, potrebbe monopolizzare le risorse computazionali disponibili impedendo l'accesso di altri container a CPU e RAM causando un attacco DoS. Diviene opportuno quindi configurare in maniera conservativa l'allocazione delle risorse destinate ad ogni specifico container.

Container breakout: in caso di presenza di un bug interno ad una applicazione, un utente potrebbe scalare la piramide dei privilegi sino alla sua *root* (origine), riuscendo così ad ottenere un accesso illimitato alla macchina host. È necessario quindi verificare la robustezza e la sicurezza dei container tramite controlli periodici.

- Immagini infette: le immagini standard dei container (build) possono essere infettate con malware o presentare vulnerabilità note, per tale motivo è consigliabile tenere aggiornate all'ultima versione disponibile i container e operare opportuni controlli attraverso scansioni frequenti.

Segreti compromessi: durante l'esecuzione delle applicazioni il container accede periodicamente ad informazioni sensibili, chiavi API e credenziali; l'accesso indesiderato a queste informazioni comprometterebbe l'intera sicurezza dei servizi in esecuzione.

In merito al DevOps, essa è una metodologia di sviluppo del software che sfrutta le nuove logiche della condivisione e della collaboration nonché di un crowdsourcing più verticale. Come vedremo maggiormente in dettaglio nel successivo paragrafo, l'obiettivo dietro l'adozione di tale metodologia di sviluppo risiede nella volontà di accelerare i tempi di rilascio dei software ritenuti fondamentali dalle imprese. Il DevOps, infatti, è un set di pratiche e di cambiamenti culturali supportati da strumenti automatici e processi di Lean Management, che consente di automatizzare il rilascio del software rispetto alla sua catena di produzione, permettendo alle organizzazioni di poter contare su un software e applicazioni di qualità superiore e sicura in modo estremamente più rapido, per accontentare i clienti nel modo migliore e più rapidamente.

A muovere le aziende verso questo nuovo modello di lavoro il fatto che molti professionisti ICT lavorano in ambienti configurati per silos, e cercano sistemi più veloci e affidabili a supporto del loro lavoro. Ma come agevolare la messa in produzione del software? Introducendo una strategia DevOps è possibile effettuare test e implementare nuove funzionalità e applicazioni molto più rapidamente rispetto alle modalità di sviluppo tradizionali, senza contare il fatto che gli stessi sviluppatori, lavorando in prima linea sulla programmazione, sono stimolati a scrivere codici di qualità superiore.

Le caratteristiche principali della metodologia di sviluppo DevOps: Agile e CI/CD

Un ambiente DevOps ben strutturato è un ambiente basato sulla metodologia "Agile", ovvero un ambiente che ha al suo interno i principi derivati dal "Manifesto Agile" che nel 2001 ha definito un modello di sviluppo focalizzato sull'obiettivo di consegnare al cliente, in tempi brevi e frequentemente (early delivery-frequent delivery), software funzionante e di qualità. Rispetto ai metodi tradizionali a cascata o ad altri processi software, le pratiche Agile presuppongono la formazione di team di sviluppo di piccole dimensioni, cross-funzionali e auto-organizzati, lo sviluppo iterativo e incrementale, la pianificazione adattiva e il coinvolgimento diretto e continuo del cliente nel processo di sviluppo.

Altre caratteristiche fondamentali di un sistema di sviluppo DevOps sono l'integrazione continua (CI) e l'erogazione continua (CD). Per CI (Continuous Integration) si intende che nel processo di sviluppo i test su una porzione di codice sono continui e automatici, mentre per CD (Continuous Deployment) si intende che il processo di messa in produzione del codice validato dopo il dovuto collaudo diventa automatica.

Una metodologia DevOps in grado di sfruttare tutte le caratteristiche qui elencate può portare in maniera efficace un'accelerazione nei tempi di sviluppo e rilascio dei software.[6]

La CI/CD rappresenta il suggello delle potenzialità introdotte dall'IT Automation nell'articolazione con il processo di sviluppo in senso stretto. È a questo livello che si traggono i benefici più tangibili della complessa struttura fin qui descritta. Sviluppare software non si presta bene alla tradizionale separazione tra progetto e realizzazione tipica delle opere di ingegneria. Il software deve poter evolvere continuamente, in base a sopraggiunte o mutate necessità. Attrezzarsi per questo scenario significa evitare di farsi carico del deployment manuale ad ogni step iterativo. Piuttosto, occorre automatizzare il deployment in modo che il tempo che passa tra la scrittura di una nuova linea di codice e la sua esecuzione in produzione, sia prossimo allo zero. Per fare questo, il paradigma CI/CD prevede la definizione e realizzazione di pipeline di sviluppo, test e messa in produzione, in cui i singoli step e la loro sequenza siano codificati in modo formale, ancora una volta attraverso linguaggi adatti ad una descrizione che sia contemporaneamente human-readable e machine-readable. Le regole di esecuzione e gli step della pipeline possono evolvere nel tempo (es., posso aggiungere o modificare i test a cui sottoporre un determinato software), ma saranno sempre eseguiti in modo automatico ad ogni aggiornamento del codice sorgente. Fino ad arrivare al building del software che le ha passate tutte con successo. Building che avverrà in immagini di container che vengono pubblicate in registry (privati o pubblici) da dove possono essere richiamate ed eseguite in qualsiasi momento e su qualsiasi ambiente.

[6] https://www.zerounoweb.it/techtarget/searchdatacenter/programmazione-software-e-l-ora-degli-it-shop-devops/

Scegli
Decidi
Progetta

Sarà sempre al tuo fianco.

CMP Analisi Strutturale

Il più affidabile e flessibile partner per i tuoi progetti.

BIM

Analisi lineari e non lineari

Pushover

Calcolo automatico dei carichi ricorrenti

Verifica strutture

Analisi statiche e dinamiche

Namirial CMP nasce dall'esperienza decennale dello studio di progettazione CAIREPRO e dispone di procedure automatizzate, affidabili, controllabili in ciascuna fase di elaborazione del modello e indirizzabili secondo le consuetudini del progettista.

edilizianamirial.it/software-calcolo-strutturale/

Richiedi maggiori informazioni allo

071 205380

oppure a

commerciale@edilizianamirial.it

Namirial

Soluzioni Software per l'Edilizia

Antincendio Strutturale Topografia e Strade
Termoacustica Ambiente Sicurezza
Manutenzione Contabilità Progettazione Utilità

Da un punto di vista di Cyber Security, adottare metodologie e strumenti DevOps impone una integrazione dei controlli di sicurezza all'interno dei processi di sviluppo, testing e integrazione. Andare verso una DevOps security significa superare l'approccio tradizionale a compartimenti stagni e garantire contemporaneamente e in modo sinergico *Application security* e *operation security.* Il ciclo di vita dei sistemi (System Development Life Cycle, SDLC) deve evolvere verso un *Secure SDLC* e quindi includere test di sicurezza attraverso tutto il processo di sviluppo e integrazione. Quando si progetta e si implementa una *Tool Chain* per la CI/CD occorre aggiungere specifici tool che eseguono automaticamente security test ad ogni ciclo iterativo. In altre parole, occorre considerare la Cyber Security non un optional da aggiungere al DevOps, ma una sua parte integrante.

Teoricamente, la cultura DevOps lavora al miglioramento della sicurezza. Le applicazioni vengono rilasciate con un determinato livello di sicurezza che soddisfa obiettivi predefiniti (conformità adattiva). In pratica, affinché ciò sia vero, la sicurezza deve essere parte del processo DevOps e dunque organico ad esso, non una funzione separata.

Le applicazioni in produzione diventano più sicure in quanto gli ambienti di sviluppo e di produzione sono costruiti allo stesso modo, rispondendo così agli stessi standard di sicurezza. In base alla conformità adattiva, tali standard cresceranno di pari passo negli ambienti di sviluppo e di produzione, incorporando adattativamente i rimedi alle vulnerabilità che vengono incessantemente rilevate e lavorate.

Conclusioni

Le infrastrutture IT diventano sempre più complesse da gestire. Nuove soluzioni software-defined semplificano e automatizzano la loro gestione, riducendo i costi di implementazione. Di contro, per migliorare l'affidabilità e aumentare la sicurezza, la progettazione assume un ruolo centrale e preminente, sul quale occorre quindi prevedere di spendere di più e sul quale occorre investire anche per una sicurezza "consapevole".

Le tendenze espresse anche dal Cyber Security Act recentemente approvato in Europa, disegnano la postura auspicata da parte di chi usa l'ICT in termini di quella che abbiamo definito una "consapevole ricerca continua della conformità a regole e best practice in costante divenire". Ecco dunque la ragione del termine adattivo, usato per riconoscere alla disciplina della sicurezza una caratteristica innovativa, ma non nuova: la capacità di mantenere un assetto conservativo (funzionamento corretto e continuativo del business) nonostante scenari di attacco costantemente mutevoli e dinamici.

JEEP® COMPASS. BORN TO BE WILD.

Gamma Compass: Consumo di carburante ciclo misto (l/100 km): 8,3 – 5,1; emissioni CO_2 (g/km): 190 – 128 con valori omologati determinati in base al ciclo NEDC di cui al Regolamento (UE) 692/2008. I valori sono indicati a fini comparativi e potrebbero non riflettere i valori effettivi.

Jeep®

THERE'S ONLY ONE

Paola Rocco

La Cyber Security per i Cyber-physical systems (CPS) e i System of Systems (SoS)

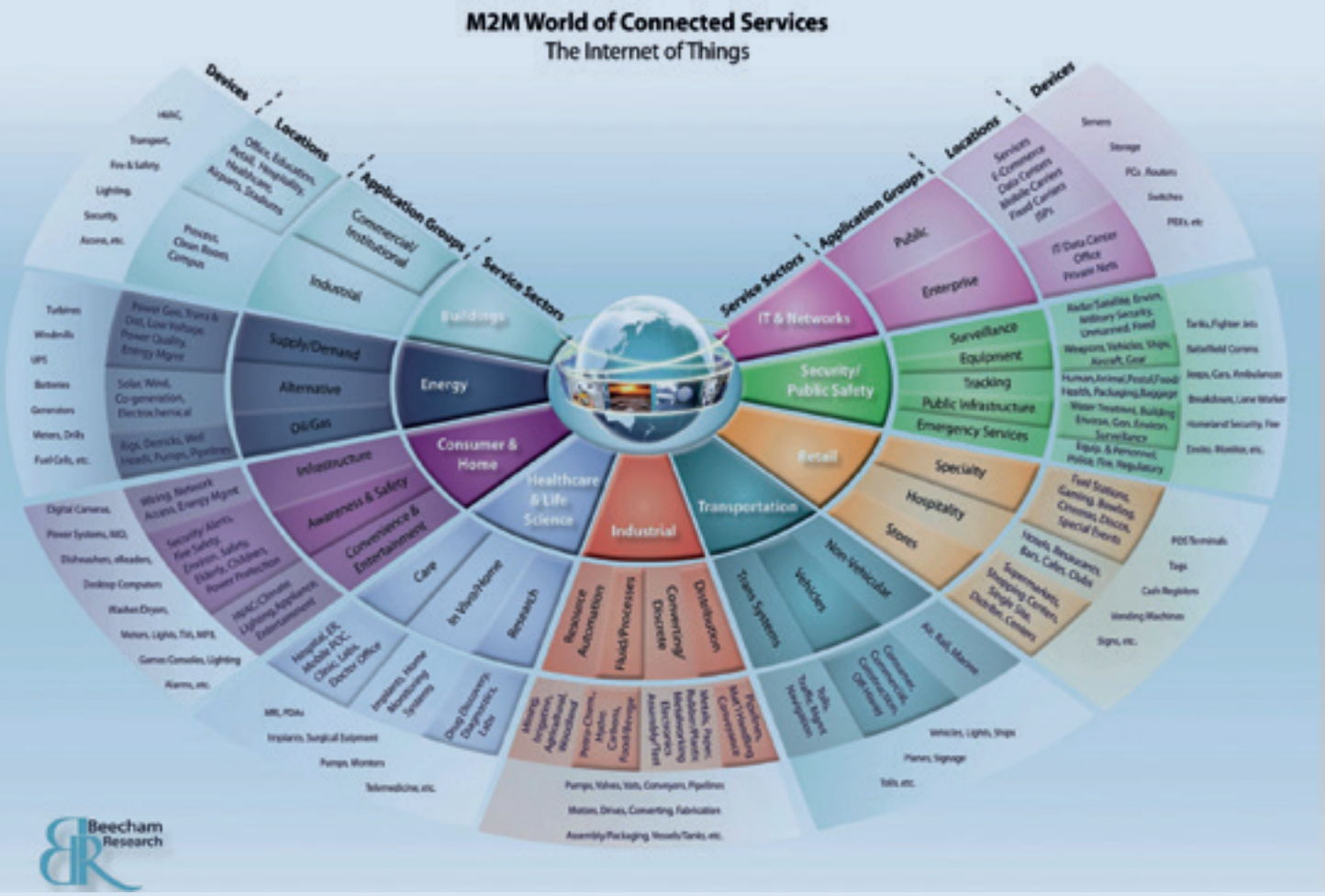
Con il termine Cyber-Physical Systems (CPS) si intendono gli smart system, cioè le architetture aggregate di sistemi fisici costituite da una componente di elaborazione e una componente di trasmissione dei dati[1].

All'interno di questa definizione generale confluiscono quindi i dispositivi IoT (Internet of Thinks), i sistemi SCADA (Supervisory Control And Data Acquisition), i sistemi ICS (Industrial Control Systems).

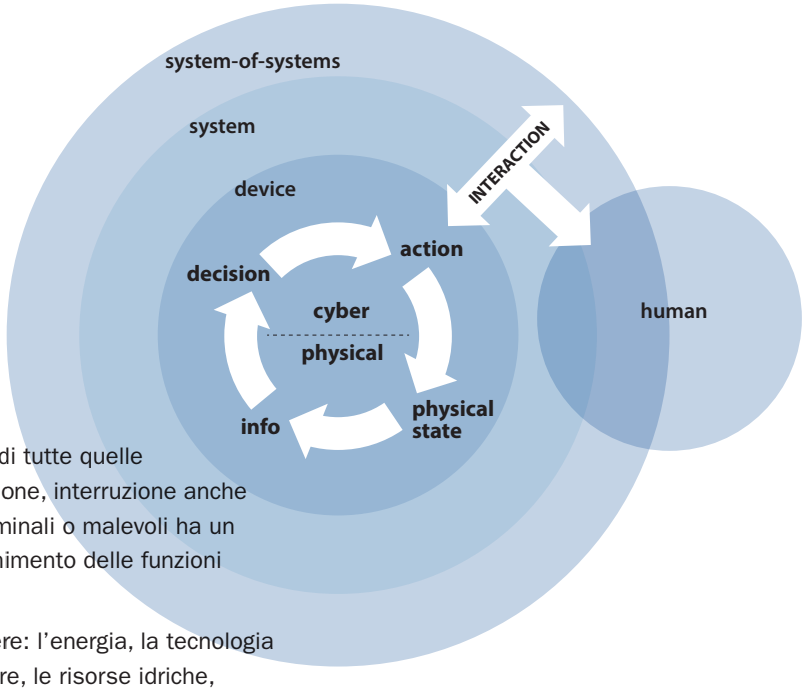
L'applicazione di tali sistemi è diffusa in ambito industriale per il controllo e il monitoraggio dei processi di produzione ed è in continua evoluzione, infatti a partire dalle prime architetture composte da elementi di interazione umana (Human Machine Interface - HMI), componenti hardware (Terminal Units - RTUs), software e sensori remoti, si è passati oggi ad un modello integrato, distribuito ed interconnesso da reti WAN che può anche utilizzare sistemi in Cloud per il suo funzionamento. Il loro utilizzo inoltre, tenderà ad aumentare notevolmente nei prossimi anni con l'introduzione del 5 G, che renderà possibile la connessione anche di dispositivi che richiedono una costante presenza di una rete a banda larga per funzionare. Le applicazioni di tali sistemi in ambito industriale sono molteplici: possono, ad esempio essere relative alla gestione e controllo di un processo di distillazione petrolchimica, ad un sistema di filtraggio dell'acqua, al controllo dei sistemi idrici, dei trasporti pubblici. A livello di astrazione maggiore si parla di System of Systems (SoS), cioè di sistemi formati da diversi Cyber-physical systems. Nel complesso quindi, i sistemi SoS hanno caratteristiche differenti rispetto ai classici sistemi di Information Technology e ne costituiscono un modello "ibrido" complesso, in cui le informazioni devono essere gestite in maniera time sensitive, in modelli di funzionamento che devono essere interoperabili e resilienti. La varietà delle componenti di cui è costituito, le caratteristiche intrinseche ed il collegamento ai servizi essenziali, accresce la complessità di un framework di Cyber Security per tali sistemi tale da garantire la riservatezza, integrità e disponibilità e la protezione dei dati alla luce delle nuove normative europee.

[1] NIST Framework for Cyber-Physical Systems: Volume 1, Overview

1



1 – Segmentation of M2M Market (Beecham Research`s Sector Map)
2 – CPS Conceptual Model NIST[1]



2

Definizioni

I sistemi CPS sono utilizzati per la gestione ed il controllo di tutte quelle infrastrutture "critiche", cioè le infrastrutture la cui distruzione, interruzione anche parziale a causa di disastri naturali, terrorismo, attività criminali o malevoli ha un grande impatto per l'economia di un Paese e per il mantenimento delle funzioni sociali vitali[2].

Gli ambiti in cui sono utilizzati i sistemi CPS possono essere: l'energia, la tecnologia dell'informazione e della comunicazione, l'industria nucleare, le risorse idriche, l'agricoltura, la produzione delle derrate alimentari e loro distribuzione; la sanità, il trasporto aereo, navale, ferroviario, stradale; le banche e servizi finanziari, l'industria chimica *(Figura 1)*.

I sistemi cyber-fisici (CPS) sono sistemi intelligenti dotati di componenti sia di tipo fisico (sensori, attuatori) che computazionale. Questi sistemi sono altamente interconnessi, integrati e forniscono nuove funzionalità per migliorare la qualità della vita e consentono progressi tecnologici in aree critiche, come l'assistenza sanitaria personalizzata, la risposta alle emergenze, la gestione dei flusso del traffico, applicazioni nell'ambito della difesa e della sicurezza delle persone, tecniche innovative per la produzione di energia rinnovabile. In *Figura 2* è schematizzato il modello di riferimento dei sistemi CPS, le macro funzionalità e le diverse interazioni. Più sistemi CPS danno origine a System of Systems (SoS) che sono definiti come "un numero finito di sistemi indipendenti tra loro che sono collegati e interconnessi per raggiungere un obiettivo unico"[3-4].

Quali sono allora le caratteristiche dei sistemi CPS?

Sicuramente l'interoperabilità tra le componenti, la flessibilità di utilizzo e la variabilità della composizione dei sistemi di cui è costituito che può cambiare dinamicamente durante il funzionamento (basti pensare all'attivazione di specifici attuatori al verificarsi di determinate condizioni).

A questo si aggiunge la complessità della gestione dell'architettura dal momento che coinvolge sia l'Information Technology (IT) nel passaggio dei dati dai sensori all'elaborazione e al calcolo, sia l'Operational Technology (OT) per tutti gli aspetti di controllo e attuazione. La combinazione di questi mondi IT e OT è una caratteristica particolarmente nuova dei CPS che introduce una maggiore complessità nella definizione dei modelli di gestione della sicurezza.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[3] Jamshidi, M., Ed. (2009). System of systems engineering - innovations for the 21st century,

[4] Maier, M.W. (1998). "Architecting principles for systems-of-systems." Systems Engineering 1(4): 284.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[6] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements

Principali minacce

La combinazione della dimensione cyber e quella fisica dei sistemi CPS definisce un nuovo modello ibrido che amplifica la risonanza delle minacce, basti pensare all'indisponibilità di un componente fisica causata da un possibile security breach delle applicazioni o dei protocolli di trasporto. Le vulnerabilità di cui sono affetti tali sistemi sono state la causa di numerosi attacchi mirati alle infrastrutture critiche, basti pensare ad esempio a Stuxnet (2010) o BlackEnergy (noto fin dal 2007). Le principali minacce ai sistemi CPS riguardano :

- modifiche non autorizzate di istruzioni, comandi o soglie di allarme che potrebbero danneggiare, disattivare o spegnere le apparecchiature, creare impatti ambientali e mettere in pericolo la vita umana;
- modifiche alle informazioni inviate agli operatori di sistema per indurli ad intraprendere azioni inappropriate, che potrebbero avere vari effetti negativi;
- diffusione di Malware, che potrebbe causare malfunzionamenti o bloccare le componenti;
- interferenze con il funzionamento dei sistemi di protezione delle apparecchiature, che potrebbero compromettere apparecchiature costose e difficili da sostituire;
- intercettazione delle comunicazioni, dal momento che si possono utilizzare protocolli non sicuri (ad esempio Modbus/TCP, IEC 40, BACnet e DNP3 nella modalità senza TLS).

Molte vulnerabilità aggiuntive sono introdotte poi dalle caratteristiche intrinseche delle singole componenti. L'utilizzo di software proprietari, ad esempio rende difficile la gestione del patching dei software, cosi come la difficoltà ad utilizzare soluzioni di sicurezza standard e l'impossibilità di applicare misure atte a rendere sicuri i dispositivi IoT, ad esempio eliminando le impostazioni di fabbrica predefinite e le configurazioni di default. In questo contesto risulta altresi difficile l'applicazione di quelli che sono i concetti base dell'application security quali la cifratura, l'autenticazione, l'autorizzazione, l'auditing e non ultima la data protection.

Modello e conclusioni

Vista la complessità dello scenario legato ai sistemi SoS, l'importanza delle infrastrutture critiche, il framework di riferimento deve garantire la protezione dei dati, delle reti e delle informazioni gestite in accordo con il livello di rischio a cui sono soggette ed in particolare garantendo:

- Un modello di governance risk- based focalizzato su tutti gli asset (cyber e fisici) di cui è composto il sistema che consenta la gestione del rischio cyber, il rispetto della privacy e della protezione dei dati[5];
- La protezione contro gli attacchi cyber, basata sulla definizione di policy e procedure, l'implementazione di sistemi di controllo accessi, la data security, la sicurezza dei sistemi e delle reti, il controllo periodico delle vulnerabilità, l'applicazione delle patch, l'auditing delle attività svolte;
- Implementazione di un Security Secure Software Development Life Cycle per tutte le componenti sia IT che OT;
- La gestione della resilienza e della continuità operativa[2];
- Un approccio preventivo e reattivo contro attacchi informatici tramite il security monitoring e l'anomaly detection che consenta di minimizzazione dell'impatto legato ad un Cyber Security incident[2];
- Il training e la security awareness per lo staff IT e OT;
- Il continual improvement[6] del modello risk based effettuato periodicamente e ad ogni variazione significativa delle sue componenti in conformità con le leggi e regolamenti applicabili.

Fabio Lazzini (Sogei)

Informatica e PA: Il ruolo dell'ingegneria nella sicurezza di una cittadinanza 2.0

Per molto tempo e fino ad un certo punto nel corso della storia, il termine "comunità" poteva essere riassunto come "un gruppo di persone che vivono nello stesso posto e che condividono le stesse regole di vita". Successivamente, la volontà dell'uomo di superare i propri limiti, di spingersi oltre alla sua stessa natura, di soddisfare la propria continua necessità di socialità e conoscenza, ha spinto l'uomo stesso a evolvere l'ecosistema attorno a sé, a modellarlo, al fine di renderlo maggiormente confacente ai propri bisogni.

Tale volontà ha portato a un aumento esponenziale delle richieste dell'uomo, ormai diventato cittadino, nei confronti della comunità in cui si trova, in termini sia di nuovi servizi a supporto della quotidianità, sia delle modalità di fruizione degli stessi, che devono essere sempre più efficienti, coinvolgenti, contestualizzati e facilmente fruibili.

La risposta a tali necessità da parte della comunità è stata negli ultimi anni una crescente spinta verso la digitalizzazione di tale ecosistema. Digitalizzazione, intesa non solo come il passaggio dal campo dei valori continui a quello dei valori discreti, ma come la possibilità di supportare le attività quotidiane di ciascuno con strumenti informatici, che semplifichino le nostre azioni e la nostra vita e consentano di ridurre il tempo di esecuzione delle attività e di abbattere le barriere della conoscenza.

Il dato di fatto è che l'ecosistema attorno all'uomo si è evoluto e si continua ad evolvere di pari passo con l'evoluzione continua di questi due concetti fondamentali, strettamente correlati tra loro: il primo è, appunto, il concetto di comunità, il secondo è il concetto di digitalizzazione.

In tal senso, il connubio tra comunità e digitalizzazione ha condotto alla trasformazione dell'intero modo di percepire il mondo e, in alcuni ambiti, la vita in generale.

È grazie a tale connubio che quindi il termine "comunità" ha finito per assumere accezioni sempre più allargate, fino a comprendere gruppi di persone connesse logicamente e non più solo geograficamente: le persone sono interconnesse, le città sono interconnesse, le nazioni e i paesi stessi lo sono, la teoria dei sei gradi di separazione ipotizzata da Frigyes Karinthy nel 1929, adesso potrebbe probabilmente considerarsi evoluta nella teoria dei cinque gradi di separazione, magari anche quattro con l'avvento e la diffusione dei social network.

Nel contesto appena descritto, considerando le dimensioni, che la comunità intesa come paese Italia ha raggiunto, è stato implicitamente ed esplicitamente assegnato alla Pubblica Amministrazione il compito di rispondere alle necessità sempre crescenti dei cittadini, cercando di offrire servizi più evoluti e fungendo, in tal modo, come un fattore abilitante per la costituzione di un ecosistema a misura delle rinnovate aspettative e attitudini del cittadino.

Nel corso degli ultimi anni, infatti, sono state avviate molteplici iniziative nell'ambito della Pubblica Amministrazione che hanno avuto come punto focale la necessità di disegnare, definire e implementare in modo innovativo alcuni servizi e di porli a disposizione dei cittadini.

In quest'ambito, la Pubblica Amministrazione è probabilmente l'unica entità, che opera per il solo bene della comunità e che possiede le risorse e la base di conoscenze che possano abilitare il raggiungimento delle aspirazioni e delle necessità del cittadino tramite la digitalizzazione dei propri servizi offerti sempre più all'avanguardia.

Dal punto di vista informatico, la PA ha il proprio punto di riferimento digitale in Sogei, hub tecnologico di informazioni e dati che partecipa attivamente alla modernizzazione del Paese e dei suoi processi innovativi, centro di competenze con un patrimonio di dati e asset che costituisce un driver strategico per affrontare le sfide ICT/digital.

In quest'azione di messa a disposizione di esperienze, competenze tecniche e tecnologiche, che le realtà afferenti la Pubblica Amministrazione richiedono e che Sogei si trova a fornire sotto forma di capability digitali sempre più evolute, il cittadino ha la possibilità di beneficiare del servizio erogato senza avere la percezione dello sforzo ingegneristico che è alla base e che risulta essere assolutamente necessario e propedeutico alla erogazione ed alla fruizione del servizio stesso. La sua "unica" preoccupazione è di avere a disposizione un servizio, che faccia risparmiare tempo, che sia efficiente ed efficace, che lo metta in condizione di poter esercitare la sua naturale richiesta di miglioramento della propria qualità della vita.

Da questo punto di vista, gli aspetti da tenere in considerazione nell'ambito del disegno e dell'erogazione di un servizio innovativo sono molteplici e tutti, per propria natura, ugualmente importanti.

Oltre agli aspetti funzionali veri e propri emergono anche quelli di privacy (il 25 maggio del 2018 è entrato in vigore il nuovo regolamento europeo per il data protection integrato dal d.lgs 101 dell'ottobre 2018) e sicurezza, sui quali il sistema Italia si è mosso già da tempo e si sta muovendo sempre con maggiore impulso. Vanno anche considerati gli aspetti di efficienza delle soluzioni, che mirano a garantire la qualità del software rispondenti ai più eminenti standard internazionali, al fine di abilitare una riusabilità ed una corretta gestione della complessità dello stesso. Fino a giungere a quelli più recenti, come gli aspetti di sviluppo sicuro del software - il secure software development life cycle è uno degli aspetti maggiormente considerati al momento - quelli di fruizione da piattaforme mobili, con l'avvento sempre più prepotente della richiesta di servizi in mobilità, e altri.

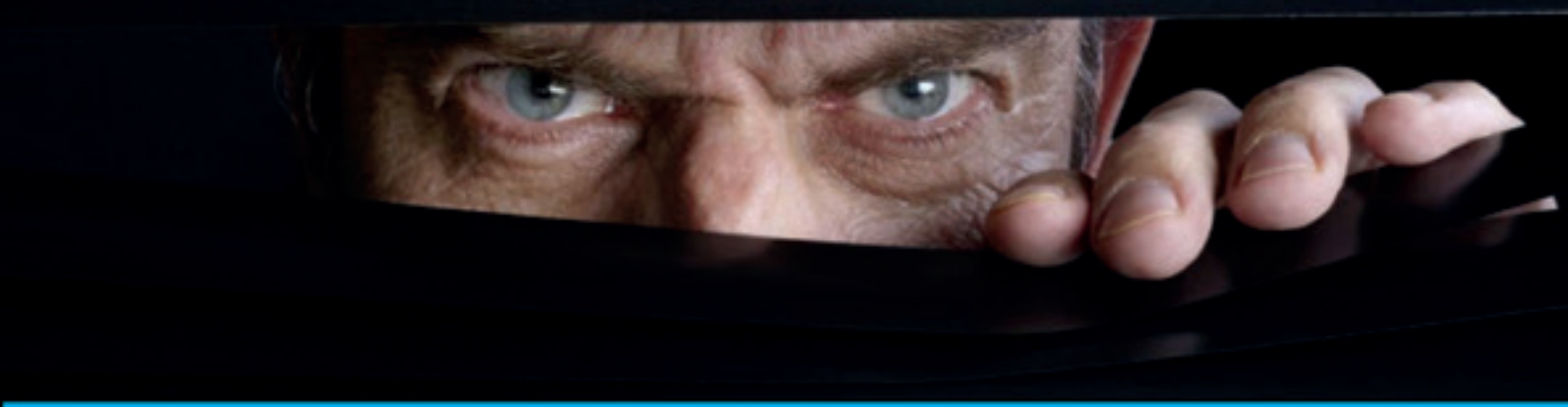
L'importanza chiave della sicurezza e della privacy dipende, in massima parte, dal fatto che i servizi digitali e digitalizzati si basano sull'utilizzo dei dati e i dati rappresentano un importante e delicato "capitale informativo", che va protetto in un contesto di minacce e di attacchi in continua evoluzione.

E in Sogei si fa quotidianamente proprio questo, attraverso un'attenta attività di ingegneria delle soluzioni. L'ingegneria in questo caso potrebbe essere considerata una scienza applicata alla risoluzione di problematiche che concorrono alla soddisfazione dei bisogni umani; più in generale l'ingegneria è Scienza delle soluzioni che ha come obiettivo l'applicazione dei risultati delle scienze matematiche, fisiche e naturali alla risoluzione di problematiche che concorrono alla soddisfazione dei bisogni umani.

Ed ecco che l'ingegneria assume subito un significato ancora più articolato se applicato a tali principi, quasi assurgendo al ruolo di sintesi tra ciò che rappresenta il bisogno di innovazione dei servizi ampiamente denunciato dai cittadini e le possibilità che lo scenario digitale attuale consente di mettere a disposizione della Pubblica Amministrazione.

Tale sintesi non può però essere eseguita secondo una logica "pull", in cui il cittadino fa richiesta di servizi, e la Pubblica Amministrazione si limita esclusivamente a dare seguito a tali richieste; al contrario, deve necessariamente essere definito attraverso un paradigma "push", che consenta di anticipare i bisogni del cittadino e le richieste dello stesso, abilitando uno stimolo che funga da scintilla per l'accensione della miccia che guida al miglioramento continuo delle condizioni e della qualità di vita dell'intera comunità, di cui si parlava all'inizio.

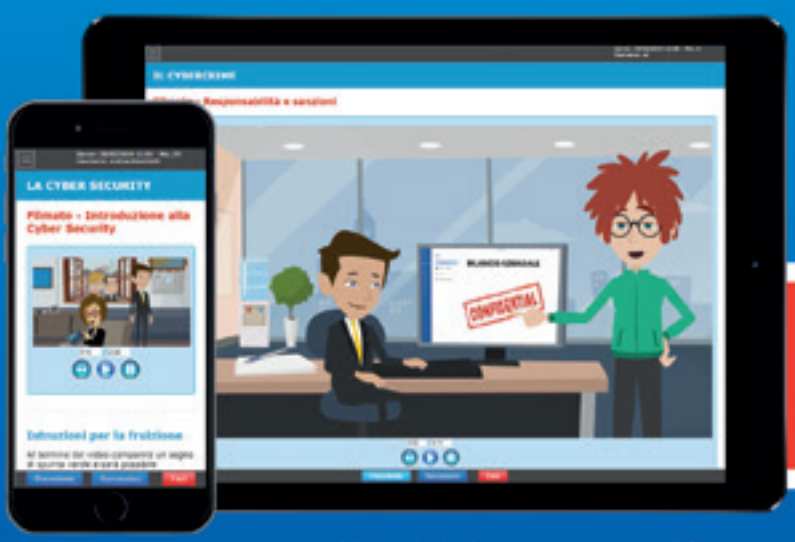
Sai come gestire e proteggere le tue informazioni aziendali?



Nuovo corso e-Learning per la formazione dei lavoratori sulla

CYBER SECURITY

Corso online di 1 ora sui rischi e le responsabilità nel trattamento di dati e informazioni tramite l'utilizzo di dispositivi informatici.



Nuovo corso per tutti i lavoratori per la gestione della sicurezza degli strumenti informatici e per la riservatezza delle informazioni aziendali. Fruibile 24h su 24, 7 giorni su 7.

Prezzo per singola erogazione.

Sconti quantità oltre 2 erogazioni.

30 €

Corso ammissibile al credito d'imposta per le spese di formazione del personale dipendente previste dal Piano Nazionale Industria 4.0

Prova il corso gratis su www.megaitaliamedia.com

Mega Italia Media Srl Via Roncadelle 70A, 25030 Castel Mella (BS) - C.F./P.Iva: 03556360174
www.megaitaliamedia.it I info@megaitaliamedia.it I Tel: 030.2650661 I Fax: 030.5531840

MEGAITALIAMEDIA
SAFETY TRAINING • WEB SOLUTIONS • E-LEARNING

Volendo fare un focus sulla parte di sicurezza, che ormai permea tutti gli aspetti della nostra vita di cittadini, emerge la necessità di generare un ecosistema paese sicuro, che faccia dell'uso delle informazioni il punto di partenza per la costituzione di modelli di business innovativi in un contesto strutturalmente sicuro e costruito attorno ai cittadini stessi e agli operatori economici.

La sicurezza per Sogei diventa, quindi un elemento centrale e abilitante dei servizi, è ideata, progettata, implementata e gestita attraverso processi strutturati, che permettano di proteggere il patrimonio informativo non solo attraverso l'implementazione delle misure di sicurezza logica (firewall, crittografia, etc.) e fisica, ma anche attraverso la definizione e l'implementazione di un "Sistema di Governo della Sicurezza e Data Protecion", che permette di governare e monitorare tutta la "filiera della sicurezza".

In quest'ottica è nato ormai da diversi anni il CERT Sogei, la struttura preposta al trattamento degli incidenti di sicurezza informatica del dominio costituito dalle strutture del MEF (Costituency), che è in grado di fornire alle amministrazioni richiedenti tutti i servizi relativi, dalla gestione dell'incidente informatico (Incident Handling) al coordinamento della task force in caso di eventi cibernetici (costituency, personale SOC, IT operation, dall'analisi forense e supporto consulenziale - metodologico e organizzativo) alla formazione e comunicazione per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o particolari tematiche di sicurezza delle informazioni.

Il CERT Sogei, costituito nell'ambito delle attività di Governo della sicurezza, ha recepito quanto previsto dalla Strategia nazionale per la sicurezza cibernetica (DPCM del 27 gennaio 2014) e collabora con le altre infrastrutture tecnologiche per la sicurezza del paese conducendo, di fatto, il cittadino, in modo sicuro verso la fruizione dei servizi pensati per lui.

Questa metodologia di implementazione di un servizio teconologico è la sintesi perfetta dei due termini chiave "comunità" e "digitalizzazione": da un lato, la rete di CERT generata dal Sistema Paese lega in una sintesi inscindibile l'intera comunità, dall'altro, tale sintesi può essere garantita attraverso l'utilizzo all'ennesima potenza della tecnologia.

Anni fa, quando è stato pensato il CERT, non era presente questo bisogno di sicurezza attualmente richiesto dal mercato e dai cittadini. Il CERT oggi opera efficacemente senza che i cittadini, pur godendone i benefici, ne abbiano conoscenza. Ma, è proprio questo il punto di forza: rendere i servizi sicuri by design e by default; fare in modo che le persone si sentano al sicuro nell'utilizzare i servizi erogati dalla Pubblica Amministrazione; forse è proprio questa la sfida più grande, ed è la stessa sfida che Sogei raccoglie ogni giorno e cerca, per quel che la riguarda, di condurre nel migliore dei modi.

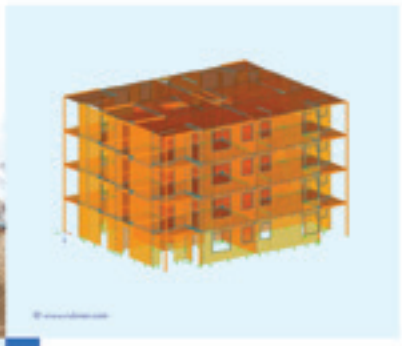
Ciò è stato possibile grazie al lavoro coordinato di centinaia di professionisti e di specialisti che, coordinati e supportati nel modo corretto, sono riusciti a mettere a disposizione della collettività un bagaglio di competenze, strumenti e soluzioni, che ha trasformato una intuizione in un ecosistema sicuro.

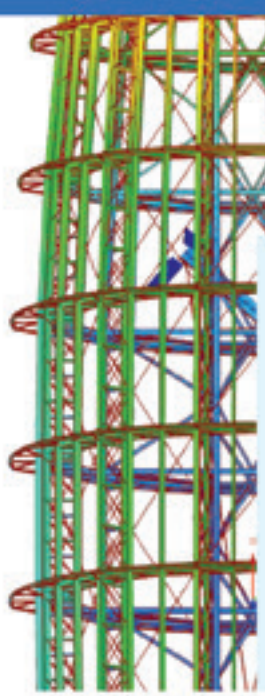
"Nihil tam arduum quod non ingenio vincas", nulla è tanto difficile che l'ingegno non riesca a vincerlo, questo uno degli adagi più cari agli ingegneri, ed è basandosi su questo adagio che Sogei contribuisce, attraverso la digitalizzazione costante ad aiutare la comunità a concentrare le energie su ciò che è utile, su ciò che serve, su ciò che consente di offrire ai cittadini la possibilità di evolversi giorno dopo giorno, andando incontro alle tendenze ed alle richieste degli stessi, ma utilizzando il proprio ingegno e la propria preparazione tecnologica per superare, giorno dopo giorno, i limiti che il cittadino crede di avere, ma di fatto si autoimpone.

Chi pensa che tutto ciò non sia frutto dello sforzo di persone, ma di un'evoluzione naturale della tecnologia, potrebbe riflettere circa la celebre frase di E. Einstein secondo il quale "Un giorno le macchine riusciranno a risolvere tutti i problemi, ma mai nessuna di esse potrà porne uno."

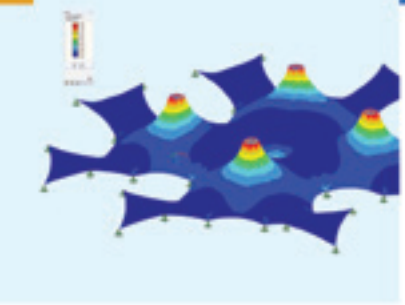
RFEM 5

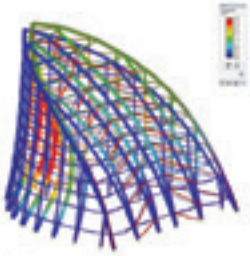
Il programma FEM definitivo





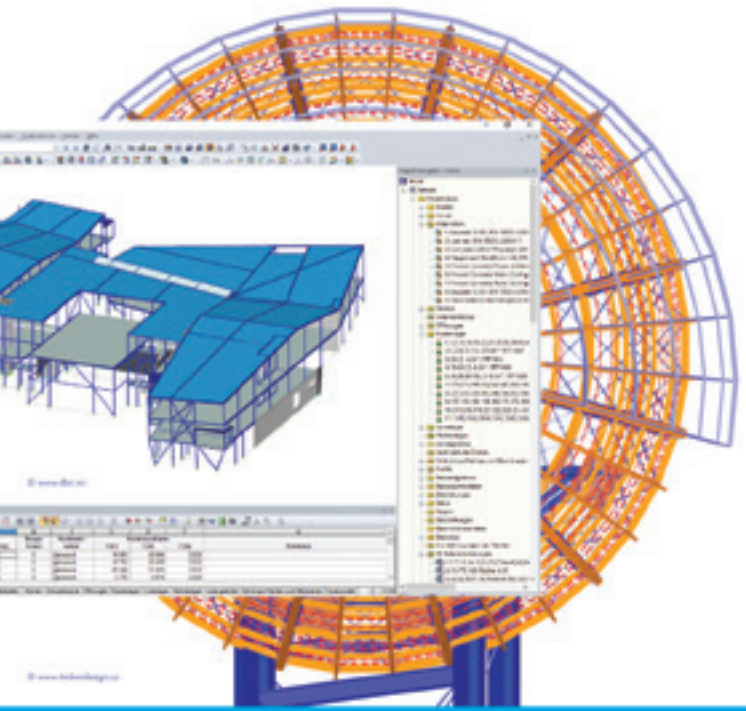
Scopri il piacere di progettare...

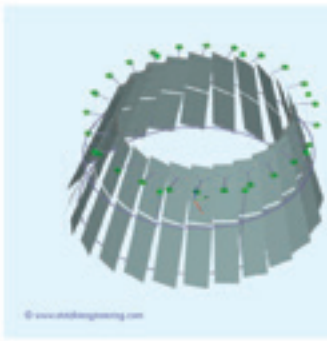




RSTAB 8

Il programma per strutture intelaiate





- **BIM e interfacce dirette**
- **Collegamenti**
- **Acciaio e alluminio**
- **Telai in legno 3D e Xlam**
- **Calcestruzzo**
- **Vetro**
- **Tensostrutture**
- **Eurocodici e norme internazionali**

GRATUITO PER STUDENTI & SCUOLE

VERSIONE TRIAL GRATUITA VALIDA 90 GIORNI

ASSISTENZA TECNICA GRATUITA

Dlubal

Software di analisi e progettazione strutturale

www.dlubal.com

Dlubal Software Srl • Via Laura Bassi Veratti 11/2D, 40137 Bologna • Tel.: +39 051 9525 443 • info@dlubal.it

Alessandro Mollo e Biagio Tagliaferro

Le piattaforme al servizio dell'information sharing

In un periodo storico in cui la parola "condividere" gioca oramai un ruolo primario nella quotidianità di un essere umano – tra post sui social network e stati temporanei sulle applicazioni di messaggistica istantanea – perché non usare la condivisione come strumento di prevenzione o mitigazione?

Info-sharing: una parola apparentemente nuova e di recente utilizzo se non fosse per il fatto che prende in prestito due parole le quali, fin dagli albori, hanno contribuito a rendere sempre più evidente l'evoluzione dell'uomo dalla scimmia.

L'essere umano di oggi è il risultato di una costante condivisione di conoscenza e, quindi, di informazioni: la scienza stessa ha fatto, e continua a fare, passi da gigante proprio grazie al continuo perpetuare di informazioni e collaborazioni; le forze dell'ordine diramano agli organi di competenza informazioni utili alla risoluzione dei singoli casi proprio perché cooperare è meglio di agire in autonomia.

Information Sharing è anche questo. E la sua trasposizione nel contesto informatico è volta a condividere informazioni circa minacce e/o attacchi informatici al fine di fornire una tempestiva risposta a quelle organizzazioni potenzialmente target dell'attività malevola: parliamo, quindi, di Threat Information Sharing.
Ma quali sono le informazioni da condividere in questo ambito?

Immaginiamo il seguente scenario: un CERT (Computer Emergency Response Team) o un CSIRT (Computer Security Incident Response Team) necessita di comunicare un'attività malevola ai danni della propria constituency. Potrebbe certamente darne tempestiva comunicazione utilizzando i canali canonici, ma in questo caso il tempo di reazione è di solito soggetto all'intervento umano. Utilizzando invece piattaforme di infosharing per condividere, anche da macchina a macchina in maniera del tutto automatica, specifici dettagli tecnici sull'evento, si ridurrebbe significativamente il tempo di attuazione. Stiamo parlando degli indicatori o, comunemente chiamati, IoC (Indicator of Compromise), i cosiddetti "artefatti" osservati all'interno di una rete o di un sistema operativo che in qualche modo sono correlabili ad una minaccia telematica come un'intrusione o un malware.

Gli IoC si suddividono sostanzialmente in tre gruppi:

- atomic, indicatori riguardanti attività avvenute sulla rete (IP, indirizzi email, nomi a domini, url);
- computed, informazioni ottenute a partire dai file ritenuti malevoli (Import hash, MD5, SHA1, SHA256, SSDEEP);
- behavioral, combinazione con altri indicatori al fine di tracciare un primo profilo (ad esempio, un IP è stato utilizzato in un determinato arco temporale e/o da una specifica nazione).

Ma avere le giuste informazioni non è sinonimo di sapere anche in che modo usarle. Fondamentalmente gli indicatori possono essere usati in due modi:

- in maniera pro-attiva per un blocco preventivo della minaccia
  - utilizzando gli IoC di tipo network (atomic) all'interno dei Firewall di rete;
  - mediante la correlazione degli IoC di tipo computed da parte degli Antivirus.
- In maniera passiva, ovvero post-mortem, al fine di diagnosticare un'infezione
  - analisi degli apparati di rete (Firewall, IDS, IPS) alla ricerca di possibili IoC di tipo atomic;
  - ricerca di evidenze di compromissione (hash dei file malevoli) all'interno del sistema operativo potenzialmente infetto.

Esistono molteplici soluzioni per la memorizzazione, consultazione e condivisione di IoC, commerciali e gratuite.

Soluzioni commerciali:

- EclecticIQ Platform[1], piattaforma di Threat intelligence basata sugli standard STIX/TAXII, argomento che verrà approfondito in seguito, che offre agli analisti la possibilità di analizzare, gestire e diffondere informazioni relative a minacce di tipo cyber;
- Soltra Edge[2], è un prodotto che automatizza i processi di condivisione, ricezione e validazione di attività malevoli. Anch'esso basato su STIX/TAXII, garantisce l'interoperabilità con altri applicativi che supportano i medesimi standard;
- Micro Focus Threat Central[3], una piattaforma che aggrega informazioni da feed pubblici, fornitori di servizi di sicurezza e dagli utenti della community. Una volta validate le informazioni vengono, poi, ricondivise coi restanti membri;
- Anomali ThreatStream[4], soluzione in cui gli IoC sono relazionati in modo da permettere agli analisti di identificare, investigare e reagire tempestivamente alle minacce permettendo, quindi, alle organizzazioni di raccogliere, ottimizzare, integrare e diffondere le informazioni sulle minacce.

Soluzioni gratuite:

- MISP[5], un prodotto opensource sviluppato da CIRCL. Iu per analisti, è una soluzione gratuita per raccogliere, memorizzare, distribuire e condividere gli indicatori di compromissione. Allo stato attuale vanta più di 6000 istanze attive utilizzate da CERT/CSIRT, SOC e forze dell'ordine. Supporta l'importazione/esportazione di eventi in formato STIX e la sincronizzazione da/verso server TAXII locali o remoti mediante una libreria ufficiale rilasciata dagli stessi autori di MISP.
  Tra i punti di forza vi è:
  - la possibilità di sincronizzare tra loro più istanze MISP in modo tale che l'organizzazione A può importare gli eventi da un'organizzazione B o condividerli verso quest'ultima;
  - l'esportazione degli indicatori in formato "digeribile" ad apparati di rete come Splunk, Snort e affini.
- MineMeld[6], sviluppato da Paloalto Network, è una soluzione opensource dall'architettura scalabile che permette di aggregare, filtrare e condividere IoC con l'accortezza di rimuoverne i doppioni o quelli che sono oltre un ciclo vita prestabilito;

[1] https://www.eclecticiq.com/platform

[2] https://www.soltra.com/en/products/soltra-edge/

[3] https://www.microfocus.com/media/flyer/threat_central_community_intelligence_sharing_enriched_with_dynamic_analysis_flyer.pdf

Linguaggio STIX e protocollo TAXII

La maggior parte delle piattaforme prese in analisi fa uso degli standard STIX/TAXII. Ma cosa sono esattamente?

STIX[7] (Structured Threat Information Expression) è un linguaggio per la raccolta di informazioni, la loro caratterizzazione e la condivisione standardizzata di eventi classificabili come “Cyber Threat & Incident”. La struttura del linguaggio è stata pensata per garantire la massima efficienza nella descrizione di eventi di sicurezza informatica, all'interno di un processo di gestione che include l'utilizzo di strumenti volti all'automatizzazione dei processi informativi.

L'implementazione e l’utilizzo del linguaggio STIX permette di raggiungere obiettivi critici quali:

- La possibilità di analizzare il rischio cyber;
- La possibilità di specificare quali indicatori possono far parte del rischio cyber oggetto di analisi;
- La possibilità di gestire le remediation specifiche;
- La possibilità di condividere le informazioni.

L’ultima versione stabile di STIX, mantenuta dal Consorzio no-profit OASIS, è la 2.0 e fa uso di Oggetti e Relazioni assimilabili rispettivamente ai nodi ed agli archi di un grafo come rappresentato in *Figura 1*.

TAXII[8] (Trusted Automated eXchange of Indicator Information)

È un protocollo per lo scambio di CTI (Cyber Threat Intelligence) mediante HTTPS e si basa principalmente su due servizi:

- Collection, contiene il repository dei vari oggetti di tipo CTI forniti dal Server TAXII e consente ai producer di caricare le informazioni che saranno messe a disposizione dei consumer. I dati vengono quindi scambiate tra Client TAXII e Server TAXII in un modello di tipo request-response;
- Channel, mantenuto dal Server TAXII, permette ai producer di effettuare il push dei dati a più consumer i quali possono a loro volta riceverli da più producer effettuando un poll dal Server TAXII

TAXII è stato progettato specificamente per supportare lo scambio di CTI in formato STIX, ma può anche essere usato per la condivisione di dati in altri formati.

[4] https://anomali.cdn.rackfoundry.net/files/ThreatStream-Datasheet.pdf

[5] http://www.misp-project.org

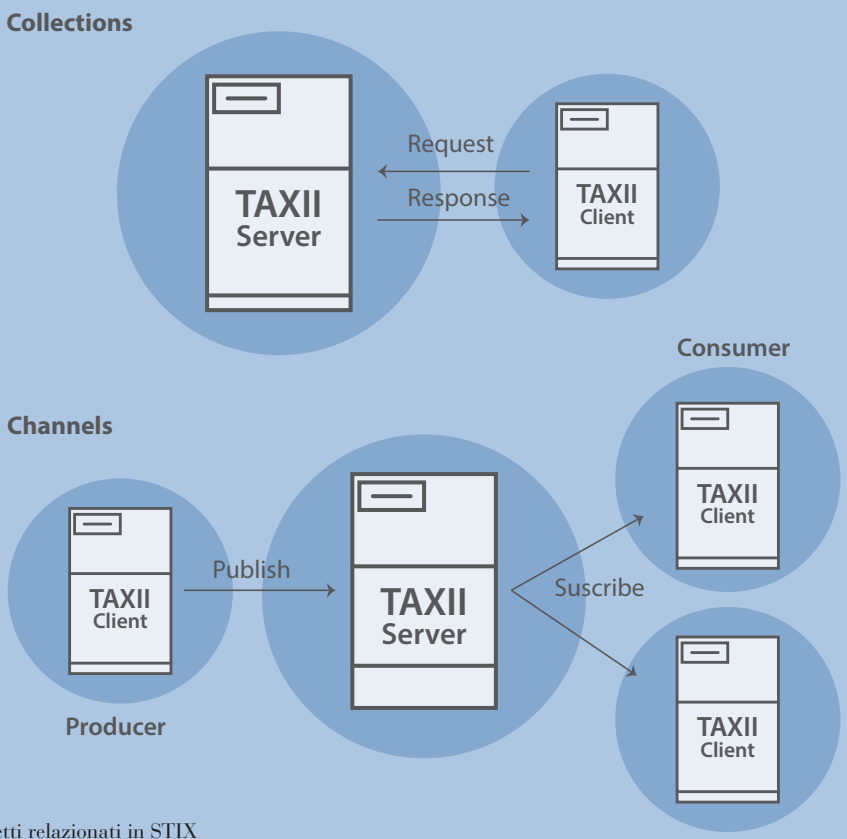
[6] https://github.com/PaloAltoNetworks/minemeld/wiki

[7] https://oasis-open.github.io/cti-documentation/stix/intro

[8] https://oasis-open.github.io/cti-documentation/taxii/intro.html

1

2



1 – Esempio di oggetti relazionati in STIX
2 – Fonte: https://oasis-open.github.io/cti-documentation/stix/intro

Progetti di info-sharing nel panorama nazionale

Lo scambio di informazioni, a partire dagli indicatori di compromissione di tipo “atomic” e “computed”, tende sempre di più a rappresentare l’elemento da utilizzare per far fronte ai crescenti rischi in campo Cyber Security. La puntuale ed immediata condivisione delle minacce aiuta le singole entità, pubbliche o private, nelle attività di prevenzione, aumenta il livello di consapevolezza sulle minacce in corso e, ove il meccanismo di scambio risulti ben definito, può permettere anche di definire azioni di contrasto specifiche ed efficaci.

Nonostante il potenziale rappresentato da questa buona pratica, in termini di attuazione, le iniziative nazionali volte a favore dell’Information Sharing risultano al momento limitate a sporadici progetti pilota o attuate con piattaforme, più o meno note, solo in specifici settori tra cui la difesa e quello finanziario.

Una decisa spinta a favore della condivisione di informazioni, sia a livello europeo che nazionale, è suggerita dalla Direttiva NIS[9] e da uno degli indirizzi operativi del Piano Nazionale per la Protezione Cibernetica[10]. Questi riferimenti suggeriscono l’attuazione di interventi mirati, in materia di accrescimento dei livelli di sicurezza, attraverso un maggiore scambio di informazioni invitando a potenziare il sistema di info-sharing anche attraverso l’adozione di linguaggi strutturati e comuni.

In risposta all’esigenza normativa l’AgID, tramite uno sviluppo interno coordinato dal CERT-PA, ha avviato un progetto atto a favorire lo scambio di informazioni, tempestive e strutturate, così da avvalorare la prevenzione e la risposta gli incidenti per far fronte alla riduzione degli impatti in caso di accadimento. Nello specifico, come indicato nel piano triennale11 (2019-2021) per l’informatica nella pubblica amministrazione, a partire dai prossimi mesi saranno attuati in tal senso due obiettivi:

- La realizzazione della piattaforma nazionale della PA per la trasmissione automatizzata degli IoC. In tal senso, in via sperimentale, AgID sta realizzando, per le pubbliche amministrazioni, una piattaforma che potrà essere utilizzata dalle PP.AA. che potranno predisporre le proprie infrastrutture all’utilizzo della piattaforma secondo gli standard e le Linee guida emanate da AgID.
- L’adeguamento delle PP.AA. agli standard di trasmissione automatizzata degli IoC. Prosieguo complementare al precedente progetto è l’emanazione degli standard e delle linee guida del modello architetturale, elementi indispensabili per fruire autonomamente del servizio.

I due progetti, dopo un primo ciclo organizzativo-sperimentale, sono in fase di consolidamento anche tramite la collaborazione di un ristretto numero di PP.AA. e aziende private, che, come “produttori” e “fruitori”, stanno conducendo positivamente dei test sull’infrastruttura tecnologica realizzata e gestita da AgID. Le tecnologie utilizzate, che si attestano sull’impiego di STIX e TAXII, subiranno nel prossimo periodo specifiche variazioni atte a garantire lo scambio di informazioni, che non saranno strettamente vincolate ai soli IoC di tipo “atomic” e “computed”, con l’intento finale di predisporre il canale di trasmissione per un utilizzo più esteso capace di processare e trasferire anche indicatori di tipo “behavioral”.

[9] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148

[10] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[11] https://pianotriennale-ict.italia.it/sicurezza/

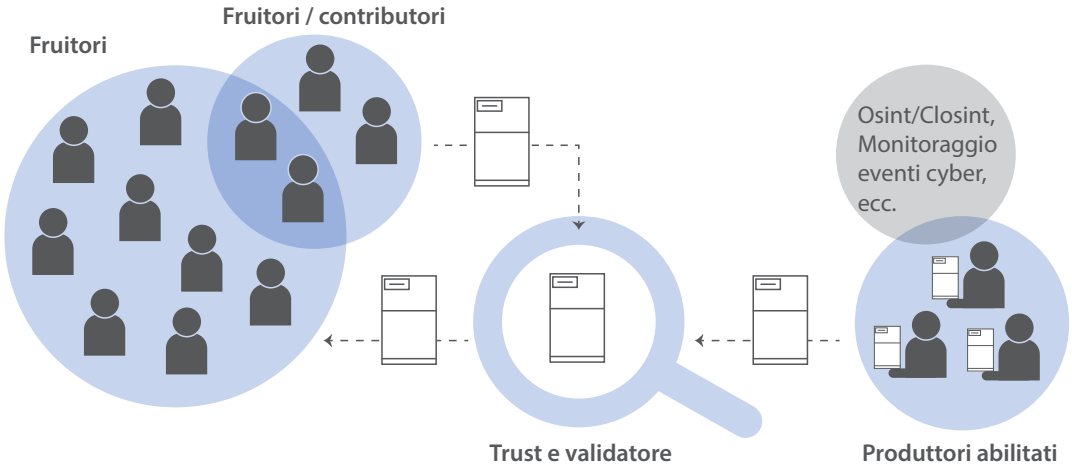
Necessità e finalità

La necessità in ambito cyber di adottare strategie e progetti a favore della condivisione delle informazioni è sempre più sentita tra gli adetti ai lavori e rappresenta una concreta opportunità di crescita anche a livello Nazionale. Nonostante le sensazioni, in attesa di progetti concreti ed indipendentemente dalle piattaforme in campo, emerge la necessità di intraprendere un percorso che favorisca e diffonda la consapevolezza rappresentata da tale opportunità.

Un processo di condivisione delle informazioni infatti non può attuarsi senza:

- dei produttori ovvero entità selezionate (CERT, CSIRT e SOC) che, più o meno regolarmente, immettano informazioni nel canale di scambio,
- un'infrastruttura "trusted" che oltre ad occuparsi di trasportare e smistare le informazioni secondo regole predefinite (a chi va cosa), adotti un processo di validazione delle informazioni,
- la volontà di una platea di fruitori favorevole sia a ricevere le informazioni che disposta a condividere dati provvedendo, anche indirettamente, ad arricchire di ulteriori IoC il canale di scambio.

Una rappresentazione tipo del modello descritto è quella di seguito riportata:



Per realizzare un progetto di information sharing non mancano quindi le piattaforme e non esiste un limite tecnologico. Per la riuscita del proposito è però necessario definire un processo che si basi sulla fiducia e la collaborazione tra entità differenti, pubbliche o private.

Come per altri aspetti della sicurezza informatica, anche in questo specifico contesto, il limite reale nell'attuazione dell'information sharing sembra essere il "fattore umano" più che quello tecnologico che dimostra, con la platea di prodotti disponibili, di essere già maturo e pronto per essere inserito nella filiera di strumenti utili in ottica di prevenzione, identificazione e mitigazione della minaccia cibernetica.

Straus7®

Nativo Non-Lineare

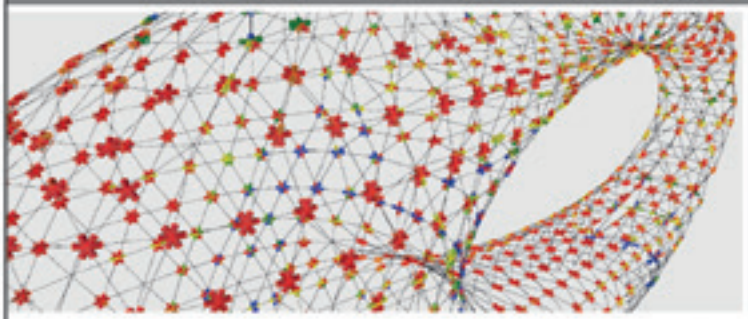
L'eccellenza FEM accessibile.

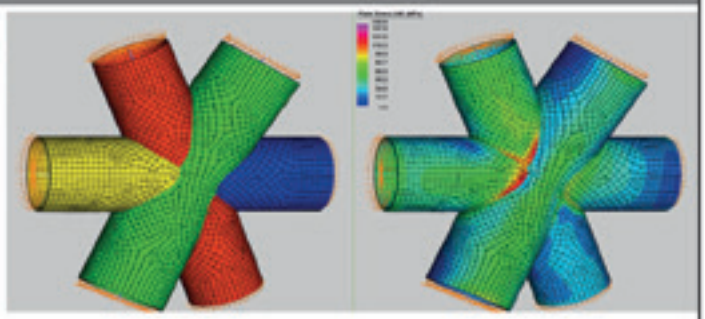
www.hsh.info

Nessun limite pratico nel calcolo strutturale agli elementi finiti

PER L'INGEGNERIA E PER L'INDUSTRIA

Il Museo del Futuro, un progetto di "Dubai Future Foundation"





Il Museo del Futuro di Dubai vuole esprimere sia nella forma, che nel sistema strutturale, lo scopo avveniristico per cui è stato realizzato. La forma circolare, con l'enorme foro centrale, è sostenuta da una struttura metallica a diagrid, i cui elementi disegnano una discretizzazione a triangoli di dimensione diversa l'uno dall'altro. La Maffeis Engineering S.p.A. è stata incaricata di sviluppare la progettazione esecutiva dei nodi di connessione e dell'analisi del metodo di montaggio dell'esoscheletro metallico. Per la progettazione dei nodi, oltre 800 nodi diversi per geometria e per numero di aste tubolari che vi convergono (da 4 a 7), è stato sviluppato un sistema parametrico in grado di generare automaticamente le geometrie dei piani medi dei tubi e, integrato tramite l'opzione API di Straus7, di generare i modelli FEM correttamente meshati e caricati con le azioni interne derivanti dall'analisi globale. L'informazione ottenuta attraverso i modelli Straus7 dei nodi è di dettaglio tale da consentire l'ottimizzazione delle saldature - aspetto di particolare importanza, tenuto conto che esse sono svolte in cantiere - e la pulizia dei nodi stessi, evitando piastre di diaframma.

Committente
MEERAS

Architetto
Killa Design

Costruttore
BAM

Maffeis Engineering S.p.A.
Engineering and Consulting

Testo, foto e immagini dei modelli di calcolo Straus7 per gentile concessione di Maffeis Engineering S.p.A.

Distributore esclusivo per l'Italia del codice di calcolo **Straus7**

HSH

HSH srl - Tel. 049 663888
Fax 049 8758747
www.hsh.info - straus7@hsh.info

Case Histories

Simone Crolla

Il mito della Silicon Valley: nascita di un fenomeno

La Silicon Valley incarna ormai da anni il paradigma vincente per l'innovazione tecnologica e di business. Per comprendere a fondo le ragioni di questa eccellenza, è necessario soffermarsi sulle origini del mito della Silicon Valley intesa come "culla dell'innovazione". Il fazzoletto di terra di cui parliamo vede nella fondazione dell'Università di Stanford nel 1891 gli albori del suo sorprendente sviluppo, che ha reso in breve tempo Stanford una delle prime università del paese. Uno dei momenti di inizio di questo mito è rappresentato dalla fondazione, in un garage di Palo Alto, da parte degli allievi di Stanford David Hewlett e William Packard dell'omonima società. Nel secondo dopoguerra l'università si impegnò nella creazione di un'area industriale prossima all'università, nasceva così lo Stanford Industrial Park come polo di alta tecnologia destinato alle aziende high-tech in grado di fornire ulteriore lustro scientifico alla Stanford University. Da quel momento le sinergie create dal binomio mondo accademico-industriale dimostrarono di essere il carburante fondamentale per il decollo della new economy. Ad oggi la Silicon Valley costituisce il principale centro d'innovazione mondiale con il più alto numero di posti di lavoro dedicati all'innovazione e una concentrazione di investimenti record, che nel 2018 si è attestata sui $130,9 miliardi.

La leadership

Il successo incontrastato della valle del silicio non può essere spiegato in maniera univoca, necessita invece di un'analisi integrata che prenda in analisi i differenti fattori che la rendono un'eccellenza a livello globale: culturali, economici, ambientali e sociali. In primis, il talento imprenditoriale unito alla spregiudicatezza e alla propensione al rischio, tipici della mentalità americana, ha contribuito nel tempo a rendere vitale e dinamica l'imprenditoria americana. La cultura del lavoro americana, improntata sul concetto del self-made man, sommata alla facilità di accesso al capitale hanno negli anni costituito il principale volano per la crescita imprenditoriale. L'altra leva strategica che più di ogni altra ha reso possibile un simile sviluppo è senz'altro legata alla fitta rete di università e centri di ricerca di altissimo livello, improntati su un rigido criterio di meritocrazia, in grado di entrare facilmente in contatto con i protagonisti del mondo imprenditoriale, cooperando in modo efficace e virtuoso per l'intero sistema economico americano.

Il rapporto con Italia

Il principale punto di forza del modello USA risiede perciò nell'attenzione e nel supporto che le startup continuano a ricevere dalla fase di lancio fino alla fase di scale-up. In Italia purtroppo il quadro non è altrettanto roseo; molte delle nascenti startup infatti muoiono prima di poter esprimere il proprio potenziale innovativo,
a causa dell'insufficiente sistema di aiuti che assiste la piccola azienda nella sola fase iniziale. Inoltre, la scarsità dei capitali di rischio, come testimonia anche il debole mercato del Venture Capital, rimane il principale gap a separare l'Italia dalle altre economie europee, lasciandoci all'11° posto e frenando bruscamente la crescita dei nostri talenti domestici. In particolare, il 2017 ha rappresentato un anno piuttosto negativo per le startup italiane, con una flessione degli investimenti del 39% rispetto ai livelli del 2016. Da queste che sono le principali debolezze del sistema italiano nasce la necessità per le piccole aziende di ricercare finanziatori esteri e internazionalizzarsi. Sono sempre di più infatti gli incubatori di startup italiane che si stanno orientando verso hub più ricettivi e moderni, molti dei quali negli USA (Silicon Valley e Boston). Tra gli early movers si segnala il gruppo IStarter - network di oltre 120 equity partner con l'obiettivo di presentare e promuovere le eccellenze italiane nel mondo – tra quelli più attivi. Il gruppo è già alla seconda edizione di "Made in Italy 2.0", iniziativa che mira a presentare una selezione di promettenti startup italiane a potenziali investitori americani. Fortunatamente le relazioni transatlantiche si muovono sempre a doppio filo e l'Italia rimane una destinazione privilegiata per molti investitori americani. Lo confermano le tre acquisizioni da parte di multinazionali americane finalizzate nel corso del 2016: quella di Amazon che ha acquisito il cloud Made in Italy dell'astigiana Nice, Intel che ha acquisito la Yogitech e Microsoft che invece ha finalizzato l'acquisizione di Solair. Laddove si sviluppano eccellenze, i radar dei principali player americani, sempre alla ricerca di innovazione e opportunità di crescita, si attivano velocemente.

Come AmCham Italy può aiutare la crescita delle relazioni transatlantiche

In un quadro così delicato, complesso, ma allo stesso tempo ricco di opportunità, AmCham riveste un ruolo importante all'interno delle dinamiche economiche e commerciali transatlantiche. La nostra attenzione è rivolta non solo ai grandi investitori USA che guardano al nostro paese, ma anche alle numerose startup italiane desiderose di compiere il salto oltreoceano. Grazie alla combinazione delle relazioni sul territorio americano e alla possibilità di sviluppare con i soci progetti di internazionalizzazione, AmCham supporta le imprese italiane nella ricerca dei partner più adatti per espandersi nel mercato americano, il più importante a livello mondiale.

Questo obiettivo viene raggiunto anche grazie alle missioni che AmCham organizza annualmente: nel giugno di quest'anno una selezione di imprenditori e professionisti sarà accompagnata nella West Coast per incontrare alcuni dei principali players americani del settore digitale e manifatturiero (Apple, Facebook, Amazon, IBM, Boeing), nonché uno tra i principali fondi di Venture Capital americani (Citi Ventures). Una missione non solo di business ma anche culturale, in grado di favorire la condivisione di valori culturali, di modelli di business e strategie, mediante il dialogo tra gli imprenditori italiani e gli esponenti americani della new wave economy.

In questo quadro, le attività di advocacy sviluppate da AmCham contribuiscono al processo di contaminazione culturale tra il sistema italiano (imprese e istituzioni) e le corporation americane in ambiti come l'Artificial Intelligence, la Ricerca e Sviluppo, la Cyber Security, settori in cui la leadership americana è ancora forte e trainante.

I differenti approcci di policy

L'approccio di policy messo in campo dagli attori istituzionali è un'altra delle variabili strategiche da considerare. Prendendo in considerazione alcuni degli interventi messi in campo dalle ultime Amministrazioni USA, quali ad esempio lo IER (International Entrepreneur Rule) e l'USCIS (United States Citizenship and Immigration Services), promossi dall'amministrazione Obama, emerge la volontà dei policymaker di stimolare l'ingresso negli USA di imprenditori esteri attraverso semplificazioni nel rilascio di permessi di residenza temporanei. Inoltre, il sistema federale denominato Small Business Administration (SBA) sostiene le piccole imprese attraverso aiuti mirati di sostegno alla ricerca nell'ambito dello Small Business Innovation Research, coordinando al contempo una rete di finanziamenti privati adibiti alle aziende più talentuose e promettenti, garantendo così la vivacità e il dinamismo del tessuto aziendale americano. Questi ed altri provvedimenti attestano la lungimiranza della governance statunitense nell'incanalare un fenomeno complesso come quello della new wave economy. Seppur con il nostro consueto ritardo, anche gli attori istituzionali italiani hanno iniziato a muoversi in questa direzione, come dimostrato dai provvedimenti presi dagli ultimi 5 governi in tema di innovazione e startup. Sebbene questi interventi, insieme rinnovata attenzione sul tema innovazione, segnalino una presa di coscienza dei policymaker su questo tipo di temi, è indubbio che il percorso da fare sia ancora lungo. Prendere esempio dal caso americano potrebbe essere un buon viatico per intraprendere le soluzioni più efficaci che rendano le nostre startup le multinazionali tascabili del futuro.

FLYGT
a xylem brand

Sistema di Pompaggio Concertor: l'intelligenza integrata con industria 4.0

Questo rivoluzionario sistema di pompaggio per acque reflue offre prestazioni ottimali riducendo il costo totale di gestione. Inoltre offre una flessibilità e semplicità senza precedenti e possiede tutti i requisiti per ottenere i benefici di legge legati all'industria 4.0.

Xylem, dove c'è acqua.

Xylem Water Solutions Italia s.r.l.
20020 Lainate (MI) Via G. Rossini, 1/A Tel. 02.90358.1
watersolutions.italia@xyleminc.com www.xylem.com/it-it

xylem
Let's Solve Water

Emilio Coppa, Giovanni Lagorio
e Marina Ribaudo

CyberChallenge.IT: Ethical Hacking per giovani talenti

Gli attacchi informatici sono in costante aumento e operano su una superficie di attacco che va ben oltre i tradizionali sistemi IT, spaziando dai server aziendali agli smart watch, dagli elettrodomestici IoT alle infrastrutture critiche, quali le centrali elettriche o gli impianti semaforici intelligenti. A questa situazione, già di per sé allarmante, si aggiunge anche una mancanza di professionisti qualificati in Cyber Security che sta diventando sempre più critica così come testimoniato, ad esempio, dal report "Cybersecurity Ventures" che stima per il 2021 una carenza di circa 3.5 milioni di professionisti a livello mondiale.

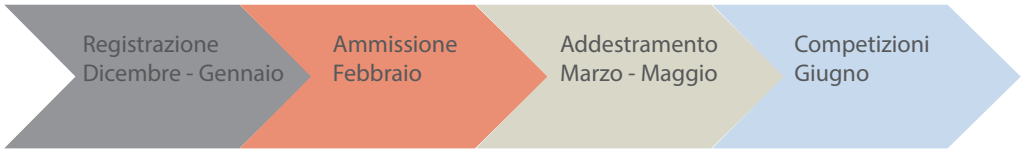
Riconoscendo quanto l'investimento in Cyber Security sia essenziale per ridurre il costo sempre crescente degli attacchi informatici, diversi paesi hanno cominciato a sviluppare appositi programmi nazionali dedicati alla formazione di una generazione di cyber-defender. Come suggerisce il nome, un cyber-defender altro non è che un esperto in sicurezza informatica, che sfrutta le sue conoscenze e abilità per la difesa dei sistemi informatici nella loro accezione più ampia.

Per far nascere e crescere questa comunità di appassionati, è necessario investire sui giovani, a partire dalle scuole superiori, stimolando il loro interesse verso i temi di Cyber Security. Per questi giovani è fondamentale fare esperienza su sistemi reali, ma è altrettanto importante rimanere nell'ambito dell'etica e della legalità. Per questo motivo si utilizzano ambienti virtuali dove i sistemi sono attaccati al solo fine di addestramento, seguendo un approccio chiamato anche ethical hacking, per sottolinearne le finalità etiche di collaborazione e accrescimento di conoscenza sui temi della sicurezza informatica.

La motivazione gioca un ruolo fondamentale nello scenario dell'ethical hacking e spesso si usano approcci orientati alla gamification, che hanno già dato ottimi risultati in altri ambiti educativi. L'attività di formazione più tradizionale viene spesso complementata da una parte di gioco, che si traduce nella partecipazione a competizioni all'interno di arene virtuali che simulano scenari reali. Fra queste competizioni quelle più popolari sono dette "Capture-The-Flag", spesso note con l'acronimo CTF. Solitamente gli organizzatori preparano delle sfide (challenge) che possono essere risolte individualmente o a squadre. Per dimostrare di aver risolto una sfida i giocatori devono "catturare una bandiera" (detta flag), ovvero trovare una sequenza segreta di caratteri che viene protetta da misure di sicurezza.

Le categorie principali di competizioni CTF sono due: jeopardy e attacco/difesa. Nel caso delle competizioni jeopardy l'obiettivo è risolvere delle sfide che coprono argomenti di tipo diverso, tra cui ricordiamo exploit di codice binario, esercizi di crittografia, attacco a servizi web. I CTF di tipo attacco/difesa prevedono interazioni via rete tra i partecipanti: ogni squadra deve infatti difendere un insieme di servizi compromessi, cercando di risolvere le vulnerabilità e, al tempo stesso, deve attaccare i servizi degli avversari per rubare le loro flag. In questo tipo di competizioni viene anche valutata la disponibilità dei servizi: spegnere la propria macchina per non essere attaccati comporta delle penalità nel punteggio.

1



2

3

1 – Le fasi del progetto CyberChallenge.IT
2 – La finale nazionale attacco/difesa a Roma nel giugno 2018, all'interno del Museo dell'Arte Classica di Sapienza.
3 – La nazionale italiana alla gara ECSC del 2017. In centro il Prof. Camil Demetrescu che, insieme al Prof. Roberto Baldoni, ha ideato il programma CyberChallenge.IT

Paesi come USA, UK e Australia organizzano da anni competizioni di questo tipo per attrarre e formare informatici appassionati di sicurezza; anche i governi di altri paesi e alcune grandi aziende hanno iniziato a finanziare attività simili. Convegni internazionali, come DEFCON, organizzano importanti gare CTF in presenza, che attraggono le migliori squadre da tutto il mondo. In Europa, ENISA propone una competizione annuale, la European Cybersecurity Challenge (ECSC), durante la quale le squadre nazionali gareggiano tra loro.

A livello italiano, l'iniziativa più significativa è il progetto CyberChallenge.IT, un progetto del Laboratorio Nazionale di Cybersecurity del CINI, che offre un percorso di addestramento gratuito e la possibilità di entrare a far parte della nazionale Italiana di cyber-defender. La *Figura 1.* schematizza le fasi del progetto che coprono un arco temporale di circa 6 mesi.

Tra dicembre e gennaio i giovani in età compresa tra i 16 e i 23 anni possono registrarsi sul portale di CyberChallenge.IT fornendo, oltre ai loro dati anagrafici, anche le motivazioni che li spingono a voler partecipare al programma di addestramento.

Il test di ammissione di febbraio serve per selezionare i candidati con buone capacità di ragionamento logico e una forte attitudine al problem-solving, senza presupporre alcuna conoscenza pregressa in Cyber Security.

L'addestramento, che dura da inizio marzo a fine maggio, mira a fornire una introduzione tecnica, scientifica ed etica ai temi che ruotano intorno alla Cyber Security. Durante le oltre 70 ore in aula, gli istruttori alternano lezioni teoriche ed esercitazioni su vari temi, tra cui crittografia, binary exploitation e web security. Nello stesso spirito delle competizioni CTF internazionali, i partecipanti sono guidati nel risolvere una serie di sfide pratiche che riproducono problemi reali proposti in ambienti isolati. Particolare enfasi viene posta nel coltivare uno spirito etico tra i partecipanti, al fine di orientarli verso un uso responsabile delle conoscenze acquisite durante l'addestramento.

A inizio giugno viene organizzata una gara CTF locale di tipo jeopardy che si svolge contemporaneamente in tutte le sedi, con un notevole sforzo organizzativo. Al termine della gara locale ogni sede forma il suo team scegliendo i quattro studenti più forti che porterà alla gara nazionale.

A fine giugno i team di tutte le sedi si sfidano in una gara CTF nazionale di tipo attacco/difesa *(Figura 2)*. La cerimonia finale premia i tre team migliori e vede la partecipazione di numerosi ospiti istituzionali; viene anche organizzato un incontro tra gli studenti e gli sponsor dell'iniziativa con l'obiettivo di avvicinare i giovani talenti al mondo del lavoro nella realtà italiana. La gara finale ha il duplice scopo di consolidare la comunità interessata all'ethical hacking e di selezionare i membri della squadra nazionale che parteciperà alla gara europea ECSC e ad altre gare internazionali.

L'edizione pilota di CyberChallenge.IT è stata organizzata nel 2017 dalla Sapienza Università di Roma e ha raccolto l'interesse di 683 giovani, provenienti da tutta Italia, tra i quali è stato selezionato il primo gruppo di talenti che hanno partecipato alla formazione. Visto l'interesse e il successo mediatico della prima edizione, a partire dall'anno successivo il progetto è stato esteso a tutto il territorio nazionale. Nel 2018 sette università si sono unite a Sapienza, riscuotendo l'interesse di 1866 giovani, tra i quali sono stati selezionati i migliori venti in ciascuna sede. Nel 2019 il numero di sedi è salito addirittura a diciotto, mostrando l'interesse sia per l'iniziativa in sé, sia per i temi che ruotano attorno alla Cyber Security, e ci sono state ben 3203 iscrizioni, di cui il 42% proveniente dalle scuole superiori.

Come già detto, tra i partecipanti al progetto CyberChallenge.IT viene formata la squadra nazionale che continua a competere rappresentando l'Italia. La squadra ha partecipato per la prima volta alla gara ECSC nel 2017 *(Figura 3)* ottenendo la medaglia di bronzo a pari merito con la nazionale UK, e nel 2018 si è posizionata in sesta posizione.

Un effetto collaterale del progetto è stata la nascita di numerosi team CTF italiani che partecipano alle competizioni internazionali organizzate settimanalmente online e pubblicate sul sito CTFTIME che costituisce un punto di riferimento per questo genere di attività.

Una iniziativa come CyberChallenge.IT è sicuramente una best practice nel panorama della formazione nazionale in ambito di Cyber Security e contribuisce ad avvicinare i giovani talenti verso un tema così cruciale per la difesa dei sistemi e delle infrastrutture del nostro paese. Naturalmente, ci sono ancora dei punti da migliorare: il successo dell'iniziativa va di pari passo con l'aumento della complessità della sua organizzazione e alcuni aspetti vanno ancora raffinati. Esiste anche un problema di genere poiché la partecipazione delle ragazze è ancora molto scarsa, riflettendo la situazione che si osserva in Italia nelle statistiche relative alle iscrizioni delle ragazze alle lauree tecnico/scientifiche. Nonostante questo, un primo seme è stato gettato, per cominciare ad affrontare in modo organico il problema della mancanza di una forza lavoro specializzata in un ambito come la Cyber Security, così cruciale non solo per il paese ma a livello globale.

EDILCAM® SISTEMI

LA TECNOLOGIA DELL'ACCIAIO PER IL CONSOLIDAMENTO STRUTTURALE.

Consolidare, adeguare, conservare in modo rapido, non invasivo, economico e duraturo.

TECNOLOGIA A PROVA DI TEST

Il **SISTEMA DI CUCITURE ATTIVE A MARCHIO CAM®** è il primo sistema ad aver ingegnerizzato il consolidamento strutturale ottenuto per via meccanica tramite la realizzazione di un reticolo tridimensionale di nastri in acciaio spessore s≤ 1 mm, posati in tensione con apparecchiature dedicate. Vanta una lunga storia sperimentale di validazione con test su edifici in scala e al vero e simulazioni di terremoti reali. (Enea, Protezione Civile, Uni-Bas, Uni-Me...) implementato dalle principali software-house nei più diffusi programmi di calcolo.

SISTEMA CAM® è una privativa EDIL CAM® Sistemi Srl

TEST ENEA

SENZA RINFORZO
Danno irreversibile PGA = **0,10 G**
Collasso totale PGA = **0,30 G**

CON UTILIZZO SISTEMA CAM
Accelerazione limite strumentale PGA = **1,20 G** fessurazioni localizzate
Riserve plastiche totalmente disponibili

MURATURA

Sede Ex Genio Civile - L' Aquila

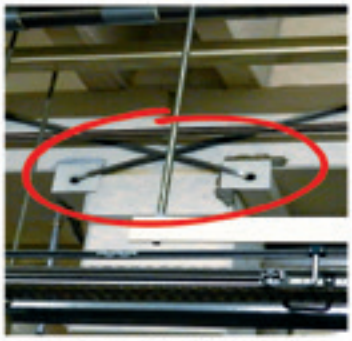
EDIFICI STORICI

Castello Rivera - L' Aquila

CEMENTO ARMATO

Scuola Silvio Pellico - Torino

EDIFICI INDUSTRIALI



Primaria Azienda Dolciaria - Brescia

Agostino G. Bruzzone

Blockchain: nuovi campi di applicazione per supportare sviluppo nel Piano Strategico Urbano

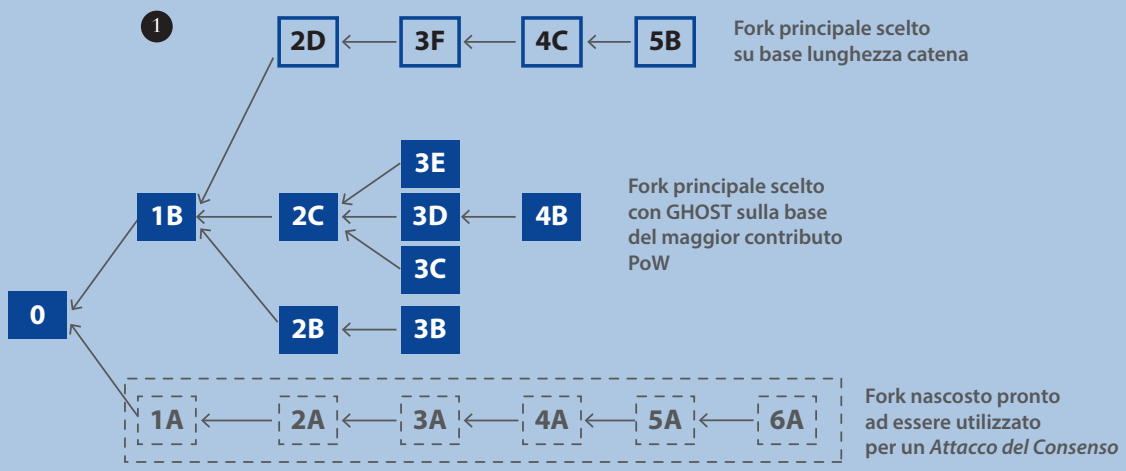
Blockchain è oggi una parola sicuramente di moda e in tutti i contesti tecnologici si tende ad includerla per nobilitare il contesto e proporsi come esploratori nelle lande misteriose dell'Innovazione.

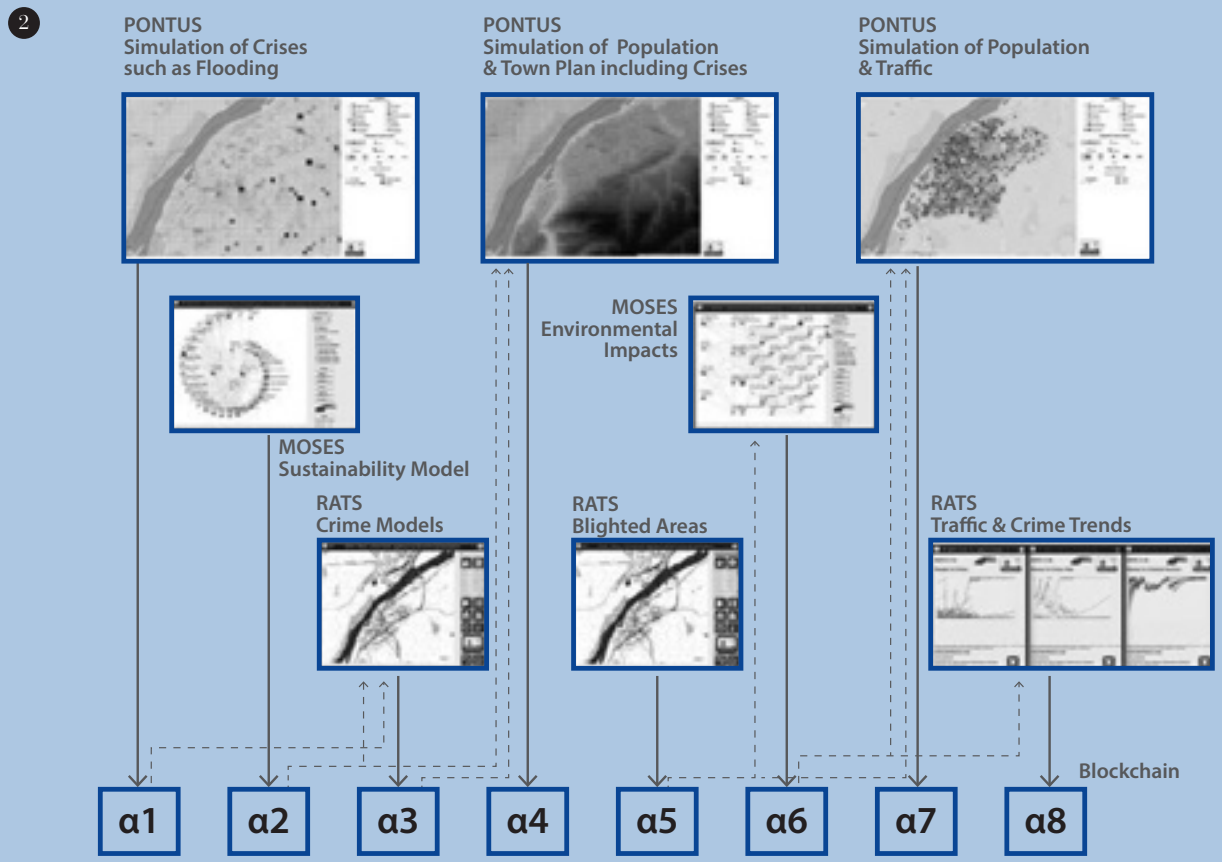
Questo fatto è comune e probabilmente non va stigmatizzato eccessivamente dato che si limita a seguire l'esempio di quegli argomenti tecnologici, in qualche modo misteriosi, criptici e promettenti, dei quali si è usi ad accennare senza voler approfondire.

Sotto questo profilo, il presente articolo non vuole ostracizzare questo atteggiamento, né fornire una trattazione dettagliata che sarebbe incompatibile con la sua brevità, ma mira piuttosto a presentare alcune peculiarità di questo contesto e in particolare evidenziare come vi siano in corso iniziative mirate a contestualizzare questa tecnologia in nuovi ambiti.

La blockchain è infatti una tecnologia moderna e promettente che, secondo una delle più diffuse definizioni, consente la creazione di un database distribuito capace di mantenere un elenco (in continua crescita) di record protetti da manomissioni e revisioni. Essa ha un qualche cosa di criptico anche nelle sue origini: non solo in quanto nata proprio come elemento di base per la creazione della criptovaluta Bitcoin, ma anche perché il creatore (o creatori) è conosciuto solo tramite lo pseudonimo di Satoshi Nakamoto e vi sono molteplici ipotesi su chi possa essere, a tutt'oggi non definitivamente confermate.

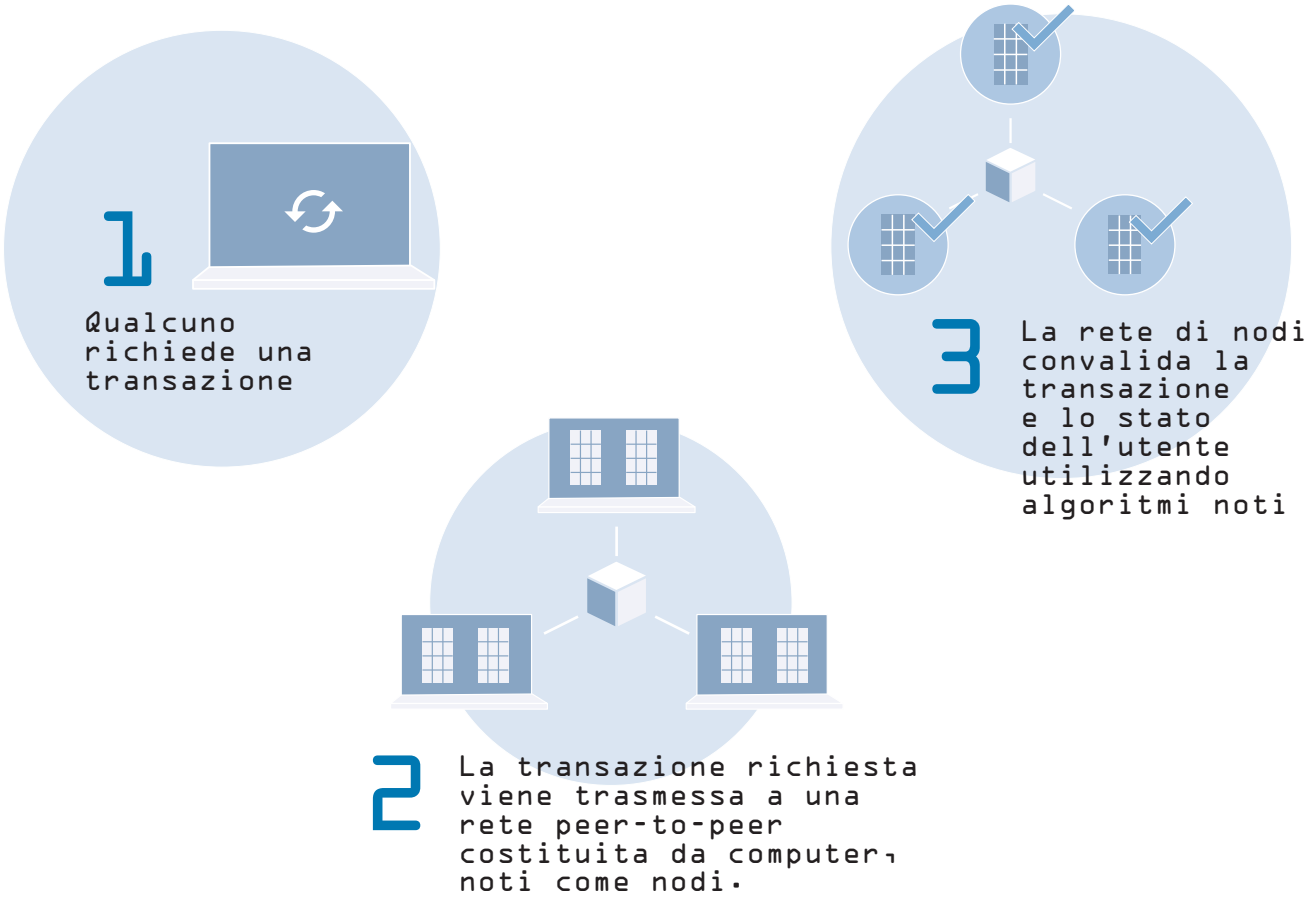
In pratica, la blockchain è un database distribuito che sfrutta la tecnologia peer-to-peer per gestire un elenco di dati, sempre crescente, mediante una procedura di codifica a blocchi (donde il nome); il metodo di codifica è mirato a garantire sicurezza e immutabilità ai dati tramite l'uso di un metodo di verifica e di algoritmi crittografici. In generale si possono classificare differenti tipologie di blockchain, per esempio rispetto al loro contesto applicativo o alla necessità (o meno) di un permesso per far parte della rete.



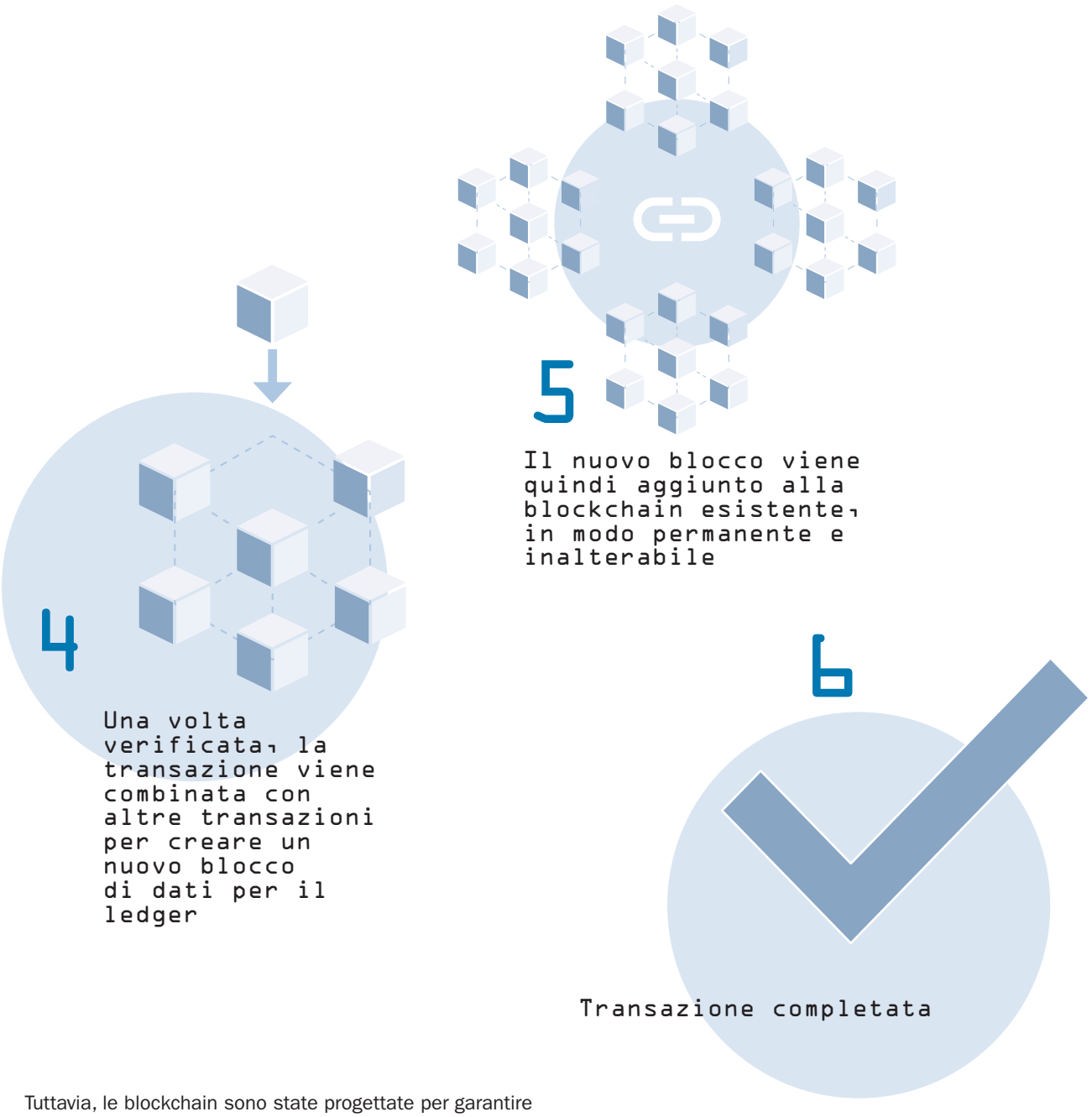


1 – Esempio di Blockchain con diversi criteri di risoluzione dei fork
2 – Applicazione della Blockchain alla Pianificazione Strategica Urbana coordinata

BLOCKCHAIN TECHNOLOGY
Come funziona?



Nella blockchain avvengono transazioni ovvero operazioni su oggetti della blockchain stessa, all'interno delle quali vi è di norma un mittente e un destinatario, ciascuno identificato da un indirizzo pubblico (generato dalla propria chiave pubblica); costoro appongono una firma digitale su ogni transazione grazie a una sign function alimentata con la propria chiave privata; non appena la transazione viene diffusa in rete, viene condotta una verifica indipendente della sua validità da parte dei nodi validatori. A questo punto, dei nodi speciali procedono ad aggregare tutte le transazioni valide, non confermate, in un blocco, che resta candidato fino a che non si raggiunge il consenso. Questi nodi speciali, spesso definiti miner, aggiungono al blocco un timestamp e un hash generato da un algoritmo crittografico; sulla base della proposta del miner, il consenso tra i nodi viene verificato per decidere se aggiungere il blocco alla catena. Fondamentale, in una blockchain, quindi è proprio il consensus algorithm che dirime il problema della sincronizzazione nel database distribuito. In effetti gli algoritmi di consenso sono molteplici e caratterizzano la blockchain suddividendosi, per esempio, nelle due macro categorie proof-based (e.g. Proof of Work PoW, Proof of Stake PoS) e vote-based (e.g. Pratical Byzantine Fault Tolerance); per inciso il primo è stato ideato vent'anni or sono ed è stato utilizzato per il Bitcoin nel processo di mining. Questo ovviamente è il block chain classico, ma ve ne sono anche altri utilizzati per esempio per tracciare un prodotto, possono essere differenti e non richiedere queste proof per finalizzare l'aggiunta di un blocco, questo avviene a volte in reti di piccole dimensioni.



Tuttavia, le blockchain sono state progettate per garantire l'integrità e la sicurezza dei dati e nelle loro soluzioni classiche sono impiegate su vaste reti e quindi con grandi capacità di calcolo; a questo corrisponde ovviamente un'esigenza di potenza computazionale e consumi energetici che sono sicuramente significativi. Ad esempio, per procedere al mining tramite la risoluzione di complessi problemi matematici di crittografia, spesso si creano mining pool capaci di divenire risorse e beneficiare del supporto fornito in questo processo.

Tuttavia, nonostante l'intrinseca robustezza rispetto ad azioni esterne ostili, nelle blockchain esistono delle vulnerabilità che, ancorché non facilmente aggirabili per vaste reti, sono pur sempre presenti e dimostrate. Sotto questo profilo, il classico esempio è rappresentato dall'attacco del consenso

(51% attack) ovvero, quando un mining pool che arriva a controllare la capacità del voto, esso può volontariamente creare una biforcazione mirata ad invalidare blocchi validi e accreditare nel database una nuova catena. Per esempio, con un attacco deliberato basato su selfish mining strategy, un miner può nascondere alcuni blocchi e attendere, per propagarli in rete, il momento opportuno per un fork (biforcazione) di cui il nuovo ramo, essendo più lungo, diventa quello valido. Come difesa, si può adottare una strategia diversa come il GHOST (Greedy Heaviest-Observed Sub-Tree) che mantiene attivi tutti i fork e sceglie la catena non più lunga, ma con maggior contributo al PoW, in questo modo un eventuale ramo nascosto proposto in un attacco al consenso non andrebbe a invalidare i rami validi *(Figura 1)*.

Di norma, gli attacchi al consenso sono mirati a compromettere solo i dati più recenti, dato che per poter creare un fork in profondità su informazioni più datate, la potenza di calcolo richiesta tenderebbe a divenire estremamente grande. Per contro, circa 5 anni fa è stato dimostrato che possedendo il 25% della potenza di hashing in una blockchain basata su PoW, si può condurre con successo un attacco del consenso.

Un modo elementare per ridurre la vulnerabilità è bloccare l'accesso alla blockchain, considerando solo i blocchi con firma digitale valida; questo è molto comune nelle applicazioni a cui corrispondono piccole reti.

Inoltre esistono algoritmi e varianti sviluppate per ovviare ai diversi aspetti e criticità, includendo oltre agli attacchi anche una particolare attenzione al miglioramento in termini di efficienza e risorse richieste.

Inoltre, vi è una continua evoluzione in questo settore, ove nuove applicazioni emergono costantemente ma che debbono essere ovviamente progettate e sviluppate con attenzione al contesto applicativo e alle specifiche configurazioni e algoritmi da adottarsi. In effetti, campi di applicazione innovativi appaiono quasi ogni giorno. Nel seguito si propone un caso dove la blockchain è impiegata per fornire un supporto nella definizione di soluzioni trasversali a problemi di pianificazione strategica nel contesto cittadino dove operano soggetti differenti che controllano specifici aspetti, ma che si influenzano reciprocamente. Nel caso proposto, in effetti, si fa riferimento all'ipotesi di valutare la costruzione di una centrale elettrica all'interno di un quadro urbano, considerando tutti gli effetti sul piano strategico di sviluppo della città e sugli aspetti di sostenibilità.

Questo caso rappresenta un esempio di uso combinato di tecnologie innovative applicando i dettami della nuova disciplina nota come Ingegneria Strategica, dedicata a guidare il processo decisionale in casi complessi. In questo contesto, il vantaggio di applicare la blockchain consiste nella possibilità di certificare i dati di input e di output

di ciascun modello utilizzato dalle diverse Authority, in modo tale da essere certi che le condizioni al contorno comuni facciano riferimento alle stesse ipotesi impiegate dagli altri Decisori.

Lo scenario adottato per la dimostrazione e la sperimentazione si riferisce a un sistema complesso che coinvolge una città con la sua popolazione e comportamenti umani, nonché traffico, sviluppi economici, impatti ambientali, pianificazione strategica, disastri naturali, incidenti industriali, emergenze, dinamiche del crimine, forze dell'ordine, etc..

In questo caso si è deciso di adottare l'approccio recente HLF (Hyperledger Fabric) che ha un'architettura estensibile e modulare capace di configurare la blockchain secondo requisiti specifici integrando per esempio diversi protocolli di consenso e servizi di ordinazione; inoltre HLF consente di eseguire applicazioni scritte in linguaggi di programmazione generici che possono essere eseguiti in un Docker, risultando isolati in modo da garantirne la sicurezza. Questo approccio è già stato applicato a casi di supply chain, logistica commerciale, tracciabilità alimentare, gestione contratti etc..

In particolare in questo caso, l'HLF separa i nodi responsabili dell'esecuzione del codice necessario a caricare i dati da quelli che gestiscono il consenso, inoltre adotta un accesso autorizzato, che limita il rischio di attacco di consenso per garantire sicurezza su una piccola rete, come già accennato.

Nel caso in esame, il problema fa riferimento ad un'area urbana di una città con circa 150.000 abitanti. L'area di interesse ha diverse caratteristiche importanti, causate dall'orografia e collocazione geografica, in particolare la città è situata nei pressi di un grande fiume, sul confine di due stati e tra montagne relativamente alte.

Considerando questi aspetti, è chiaro che la zona ed i suoi abitanti potrebbero essere soggetti a diversi rischi, come disastri naturali (ad esempio forti piogge che provocano alluvioni) o attività criminali causate dalla presenza del traffico illegale di merci, persone e/o droga. In questo quadro viene analizzata la possibilità di costruire una grande struttura industriale, da valutare insieme ad altre decisioni strategiche legate allo sviluppo della città (e.g. ridimensionamento di altre zone industriali, nuove infrastrutture, sviluppo aree verdi e commerciali). L'investitore privato interessato a costruire la centrale ha l'esigenza di concordare un piano di sviluppo coerente con i propri obiettivi, ma che deve poter garantire anche l'accordo reciproco con le autorità cittadine, l'assistenza sanitaria e le agenzie ambientali. Questo è ovviamente legato a un processo di negoziazione in cui la nuova struttura industriale porta opportunità di lavoro, reindirizza in parte il business in un'area urbana, provoca impatti ambientali con effetti diretti ed indiretti sulle altre attività cittadine. Allo stesso tempo, l'autorità pubblica in questo caso deve ridefinire il proprio piano strategico, compresi gli investimenti in

attività industriali e commerciali, le iniziative di protezione ambientale e altri aspetti cruciali come la pianificazione futura di una grande struttura da potenziare o dismettere. L'autorità cittadina deve definire inoltre come bilanciare budget e risorse tra questi elementi: nuovi impianti industriali da parte di investitori privati, attività industriali, attività commerciali, azioni sul sociale, sulla sanità e sull'ambiente. Questi aspetti influenzano direttamente la popolazione che vive nell'area, la crescita demografica e lo sviluppo dell'occupazione, nonché il recupero di aree e/o l'evoluzione di zone disagiate con potenziale sviluppo della criminalità e/o impatto dei disastri naturali.

In questo caso, sono stati costruiti diversi modelli destinati a supportare le decisioni delle diverse autorità, i quali sono alimentati con vaste basi dati raccolte dai sistemi informativi interni e da open data disponibili in rete. Sistemi intelligenti sono stati applicati per ciascun modello per finalizzare, tramite data fusion, la creazione di set di dati coerenti e completi capaci di caratterizzare ciascun contesto decisionale indipendentemente. Ovviamente, ciascun decision maker ha la possibilità di aggiungere ipotesi e piani di sviluppo differenti, mentre viene a sua volta influenzato dalle scelte fatte separatamente dagli altri attori. Nel caso specifico, i modelli impiegati consentono di sviluppare simulazioni su questo scenario che seppur operino in modo disgiunto, interagiscono su aspetti specifici del problema proprio attraverso l'accesso ai dati certificati dalla blockchain, sia legati agli input e ipotesi degli altri che ai relativi output.

Infatti, la situazione descritta chiarisce che come, per prevedere l'evoluzione dell'area nel tempo, sia strettamente necessario considerare tutti gli aspetti citati e le mutevoli interazioni. Ovviamente, questa situazione richiede l'utilizzo di modelli di diverso tipo, come il modello meteorologico e del terreno, la popolazione della città e il simulatore di infrastrutture, nonché il modello di attività criminale. In effetti, è necessario riprodurre comportamenti relativi a diversi campi: pianificazione strategica urbana, concetti di città intelligente, traffico, qualità della vita, sicurezza, soccorso in caso di calamità, criminalità, disordini, sostenibilità sociale, sviluppo economico, impatti ambientali, sviluppo industriale, applicazione della legge, assistenza sanitaria, ecc.

Considerando questo, è ovvio che lo scenario scelto fornisce ottimi casi di studio per l'interoperabilità di diversi modelli. Ovviamente, la disponibilità di modelli e di sistemi intelligenti di data analytics da impiegarsi è un elemento critico, ma va detto che già oggi sono disponibili interessanti soluzioni e applicazioni (e.g. IA-CGF, CRISOM, ALACRES2, etc.). In *Figura 2* è proposta l'architettura del sistema citato, destinato alla pianificazione strategica urbana coordinata tra più autorità sviluppato dal Simulation Team e basato su blockchain e simulazione.

Per questo genere di applicazione e considerando le specifiche condizioni al contorno, la sperimentazione ha confermato che l'approccio proposto è coerente e che le approssimazioni sono accettabili, consentendo ai modelli la possibilità di evolvere in modo parallelo verificando i dati certificati presentati dagli altri e fornendo i propri risultati proprio grazie alla condivisione della blockchain. Questa funzionalità potrebbe essere prodotta anche con altri approcci, ma nel caso specifico garantisce la tracciabilità di tutte le ipotesi e di tutte le analisi condotte dalle diverse authority, annullando praticamente i rischi di alterazione (accidentale o volontaria) delle informazioni; il tutto viene condotto senza compromettere la confidenzialità di determinati elementi dei modelli che potrebbero essere limitati all'accesso di uno specifico soggetto.

È evidente che in futuro l'impiego di soluzioni di questo genere da parte di ingegneri, potrà diventare un fondamentale ausilio nel supporto alla progettazione strategica di sistemi complessi e nel supporto alle autorità locali rispetto a tematiche di sicurezza, sviluppo e sostenibilità intesa ad ampio spettro.

References

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Weed Cocco, S., & Yellick, J. (2018).**Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.** In EuroSys: Thirteenth EuroSys Conference, April 23–26, Porto

Antonopoulos, A. M. (2017). **Mastering Bitcoin: Programming the Open Blockchain,** O' Really Media, Inc.

Beck, A. (1997). **Hashcash- A Denial of Service Counter-measure**, http://www.cypherspace.org/adam

Bruzzone, A.G., Massei, M., Sinelshchikov K. (2019). **Application of Blockchain in Interoperable Simulation for Strategic Decision Making**, Proc. of Summersim, Berlin

Bruzzone A.G. (2018). **MS2G as Pillar for Developing Strategic Engineering as a New Discipline for Complex Problem Solving**, Keynote Speech at I3M, Budapest, September

Bruzzone A.G., Massei M., Di Matteo R., Agresta M. (2018c). **Simulation of Crisis Affecting Critical Infrastructures and Industrial Plants**, Proc. of DHSS, Budapest, September

Buterin, V. (2015). **On Public and Private Blockchains**, Ethereum Blog

Dwork, C., Lynch, N., Stockmeyer, L. (1988). **Consensus in the Presence of Partial Synchrony**, Journal of the ACM, 32 (2), pp.288-323

Dziembowski, S., Faust, S. Kolmogorov V. & Pietrzak, K. (2013). **Proof of Space**, in International Association for Cryptologic Research (IACR)

Eyal, I., Sirer, E.G. (2014). **Majority is not Enough: Bit-coin Mining is Vulnerable, Proceedings of International Conference on Financial Cryptography and Data Security**, Berlin, Heidelberg, pp.436- 454

Harrison, G. (2015). **Next Generation Databases: NoSQLand Big Data**, Apress, NYC

Nakamoto, S. (2008). **Bitcoin: A peer-to-peer electronic cash system**, bitcoin.org/bitcoin.pdf

Sousa, J., Bessani, A., & Vukolic, M. (2018). **A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform**. In 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 51-58

Swan, M. (2015). **Blockchain: Blueprint for a New Economy** O' Really Media, Inc.

Vukolic, M. (2017). **Rethinking permissioned blockchains**. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 3-7

Zolar, A., Sompolinsky, Y. (2015). **Secure High-Rate Transaction Processing in Bitcoin, Financial Chryptography and Data Security**, Lecture Notes in Computer Science, vol 8975. Springer, Berlin, Heidelberg (2015).

VirIT explorer PRO

AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

l'Antivirus che ti protegge *efficacemente*

ANCHE dai Ransomware!

CONTATTACI

+39 049 8977432
www.tgsoft.it

Windows 10 ..e per tutti gli altri S.O. Windows Microsoft sia Client che Server

Windows 8 / 8.1 Windows Server 2012

..e ora anche VirIT Mobile Security PRO per ANDROID

VirIT explorer PRO è Certificato da: VB100 VIRUS | ICSA labs | OPSWAT. Anti-Malware

TG Soft
Cyber Security Specialist
www.tgsoft.it

speciale tesi di laurea

Il Consiglio Nazionale Ingegneri, in occasione della pubblicazione di questo numero dell'Ingegnere Italiano, ha lanciato una call per fare una ricognizione tra le startup e i neolaureati che abbiano discusso una tesi di laurea triennale o specialista avente come tema la Cyber Security.

In questa sezione pubblichiamo gli abstract delle tesi che il comitato scientifico della rivista ha ritenuto più interessanti.

CyberSecurity in FINDUSTRY 4.0

Monica Maria Francesca Mingoia

RELATORI Prof. Giovanni Perrone, Prof. Manfredi Bruccoleri, Prof.ssa Erica Mazzola,
Prof. Paolo Roma, Ing. Mariangela Piazza

Il progetto FINDUSTRY4.0 si occupa dello studio dell'innovazione digitale con applicazione nel settore della Fabbrica Intelligente "Smart Manufacturing". In collaborazione con Engineering Ingegneria Informatica S.p.A., l'Università degli Studi di Palermo si prefigge l'obiettivo di definire, realizzare e mettere a disposizione una piattaforma in grado di offrire tecnologie, sistemi ICT e competenze, oltre che un supporto metodologico che incentivi la diffusione e l'adozione delle tecnologie abilitanti e l'innovazione digitale nel settore manifatturiero italiano (secondo quanto previsto dal Piano Digitale Industria 4.0 del governo italiano). In questo modo viene facilitata l'introduzione dei paradigmi, dei principi, delle metodologie, delle tecnologie, dei servizi e delle soluzioni Industria 4.0.

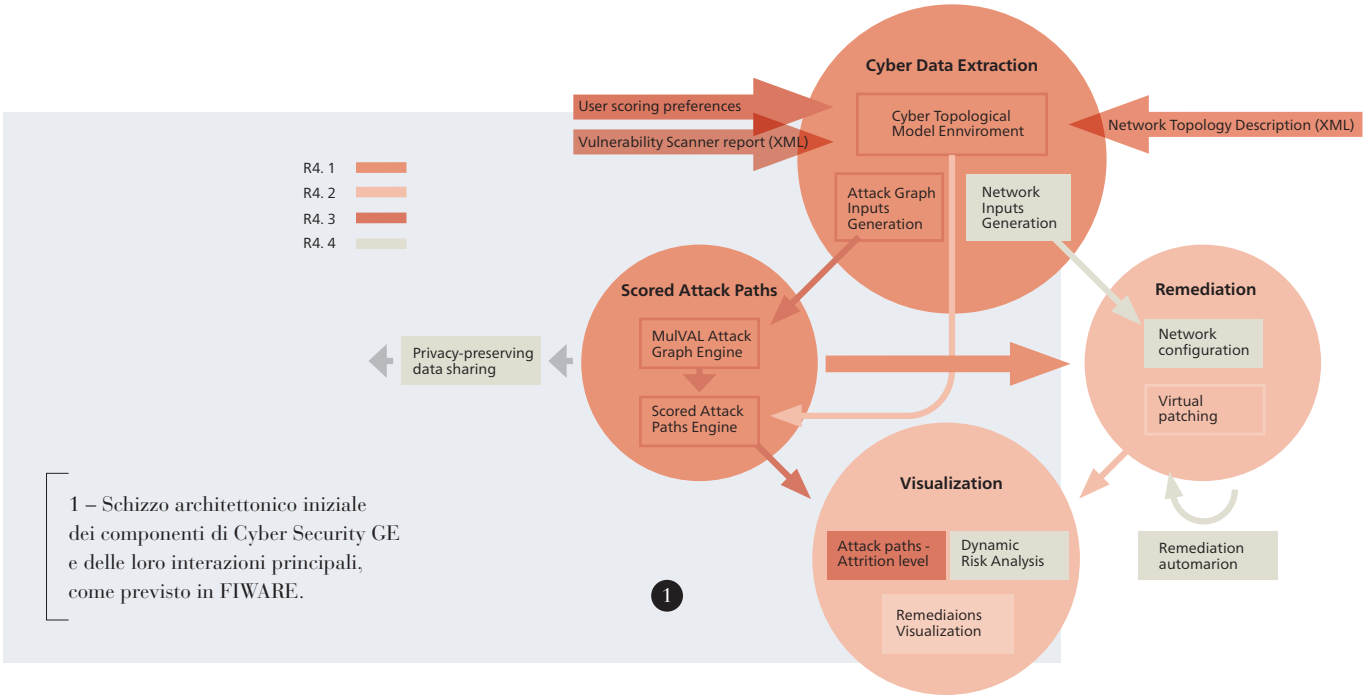
La Piattaforma FINDUSTRY4.0 risultante mira a costruire un ecosistema di servizi ICT basati su una Open Digital Platform per l'Industria 4.0, a cui vengono affiancate competenze, metodologie, ed attività di formazione che favoriscano l'adozione di tali servizi, grazie anche a nuovi modelli di business.

L'elaborato si occupa di descrivere come verrà raggiunto l'Obiettivo Realizzativo (OR) A.1.1 il quale prevede un'analisi dei requisiti per la creazione di una piattaforma a servizi che possa rispondere in maniera completa a tutte le necessità di una azienda nell'ambito manifatturiero.

In particolare si tratta di una descrizione dettagliata su come far evolvere la piattaforma già esistente FIWAREforIndustry, arricchendola di nuove funzionalità (ad es. costruzioni di nuove modalità di Interazione Uomo-Macchina o servici specifici per l'Industrial Analytics);

Inoltre essa serve a far comprendere come sulla base delle tecnologie abilitanti, si sviluppino applicazioni innovative nei domini dell'Industria 4.0 e, si ci focalizza sui pilastri del Future Internet, tra cui la Cyber Security che tra tutti, ricopre un ruolo particolarmente rilevante. Sono stati suddivisi i principali processi all'interno di un'azienda come Product Lyfe Cicle, Supply Chain e Production, a loro volta classificati in sotto processi.

Sulla base di questa suddivisione la tecnologia Cyber Security, che inoltre protegge i sistemi industriali dalle minacce di sicurezza informatica dovute all'incremento di connettività tra le aziende e al loro interno, insieme agli altri supporti tecnologici dell'Industry 4.0, è stata esaminata al fine di far emergere tutte quelle potenzialità che possano essere applicate per favorire l'ottimizzazione della produzione, la valutazione della qualità del prodotto, la manutenzione predittiva, [...].



1 – Schizzo architettonico iniziale dei componenti di Cyber Security GE e delle loro interazioni principali, come previsto in FIWARE.

Mapping spaziale automatico di sorgenti wireless tramite robot differenziale

Dott.ssa Eliana Cannella

RELATORE Prof. Giovambattista Ianni
Università della Calabria - Dipartimento di Matematica e Informatica

In questo lavoro di tesi magistrale viene presentato un robot a guida differenziale autonoma il cui compito è quello di mappare la presenza di sorgenti radio IEEE 802.11 sconosciute e la loro potenza di segnale. Attraverso un sensore LiDAR, l'area in cui il robot è dislocato viene scansionata creando una mappa 2D dell'ambiente circostante. Dopo aver ricostruito l'ambiente, il robot è in grado di muoversi liberamente identificando e mappando le sorgenti radio. Queste ultime possono essere visualizzate graficamente attraverso uno tool appositamente sviluppato, scritto in Python. È possibile visualizzare la mappa ricostruita con la posizione degli Access Point con una normalizzazione del colore in base alla potenza dei segnali registrati.

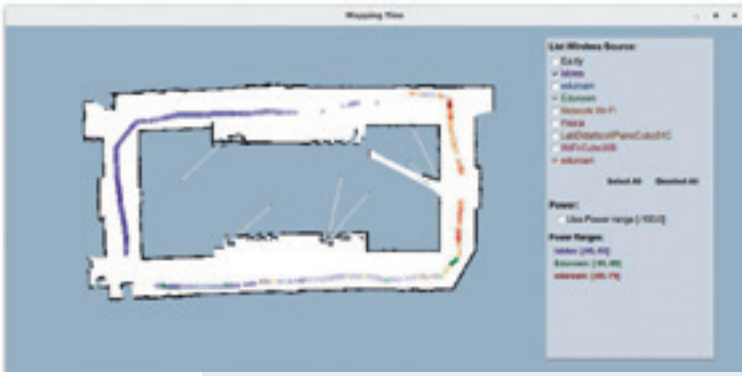
Per eseguire lo sniffing è stato usato Cinnamon, un modulo che era stato precedentemente sviluppato durante il lavoro di tesi triennale, capace di monitorare le sorgenti WiFi e registrare l'attività radio 802.11. Cinnamon utilizza la libreria Scapy per interpretare i frame catturati, raccogliendo statistiche su un livello di dettaglio più alto rispetto a strumenti analoghi. Lo strumento è stato esteso aggiungendo la possibilità di registrare la posizione spaziale in cui è avvenuta ogni singola misura.

Tra le applicazioni possibili del software sviluppato dalla tesista: mappatura e individuazione di sorgenti radio ignote; individuazione spaziale di rogue access points; troubleshooting robotizzato su reti 802.11; pattugliamento robotico non presidiato di ambienti in cui è vietato l'uso di dispositivi mobili (es. prove concorsuali, esami).

1 – Robot usato nel lavoro di tesi
2 – Mapping finale

1

2



Coprotect: gestione cooperativa di chiavi crittografiche per la sicurezza dei dati in sistemi cloud

Emanuele Raso

RELATORE Prof. Maurizio Naldi
CORRELATORI Prof. Giuseppe Bianchi, Ing. Lorenzo Bracciale
Università degli Studi di Roma Tor Vergata
Ingegneria Informatica A.A. 2017/2018

Data l'importanza della gestione sicura dei dati nei sistemi cloud, si è analizzato un sistema reale, Azure Information Protection di Microsoft, da cui sono emerse importanti criticità relative la sicurezza.

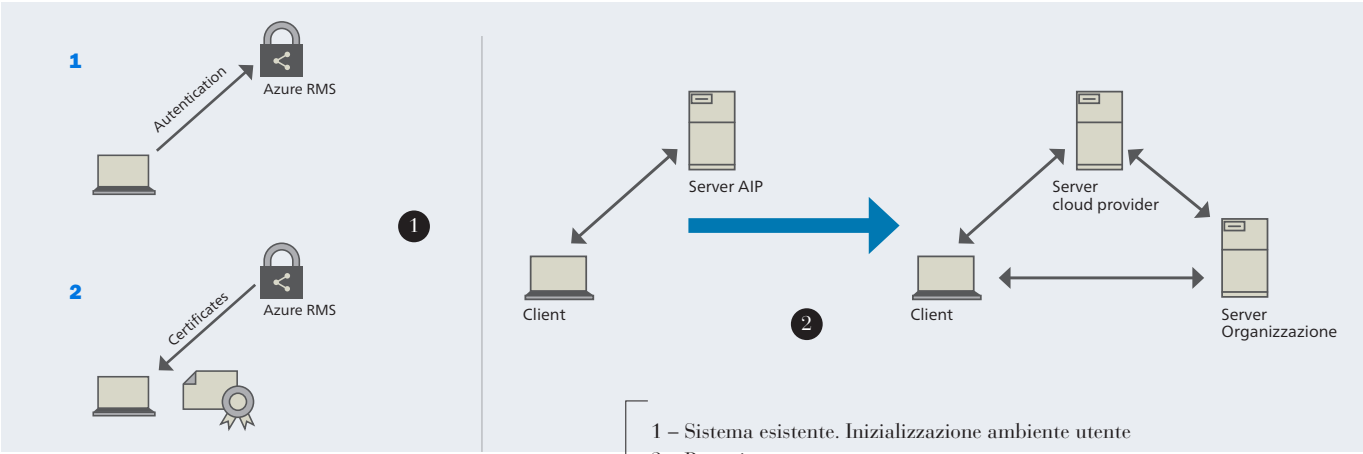
A partire dal suddetto sistema, che richiede ad un'organizzazione l'accesso a tutte le chiavi di cifratura e decifratura utilizzate, ne è stato realizzato uno nuovo che tenta di rimuovere questi vincoli. In particolare, attraverso l'applicazione del meccanismo a firma multipla e l'utilizzo di tecniche crittografiche avanzate come Pedersen Distributed Key Generation ed ElGamal, il nuovo sistema risolve il problema, rendendo l'organizzazione una componente attiva nell'architettura. *(Figura 1)*.

Il sistema realizzato prevede una gestione condivisa e cooperativa delle chiavi tra i due server del cloud provider e dell'organizzazione *(Figura 2)*, superando anche gli ostacoli imposti dalla fiducia sia nel cloud provider che nei dipendenti all'interno dell'organizzazione stessa e mantenendo la sicurezza rispetto a tutti coloro che sono al di fuori del sistema.

Obiettivi del progetto sono creare un sistema basato su un nuovo modello di fiducia (basata su più entità, creazione delle chiavi Pederson Distributed Key Generation e cifratura asimmetrica ElGamal), introdurre un meccanismo di controllo d'accesso a granularità fine, realizzare un prototipo proof-of-concept e valutare la prestazione.

Conclusioni e sviluppi futuri

- Gestione sicura dei dati senza vincoli di fiducia attraverso meccanismi cooperativi per la generazione di chiavi e la decifratura
- Controllo d'accesso a granularità fine, modificabile in base a necessità e vincoli
- Conservazione della linearità della complessità computazionale algoritmica rispetto al sistema emulato
- Policy-based Encryption per la generazione della chiave di cifratura del contenuto
- Chiave comune a file con stesse politiche
- Cache nel server del cloud provider per ridurre il carico sul server dell'organizzazione



1 – Sistema esistente. Inizializzazione ambiente utente
2 – Prototipo

Cyber Security Software Defined Radio Attacks

Le criticità remote dei sistemi su cui ci affidiamo tutti i giorni per la nostra vita

Ing. Davide Casale

Laureato in Ingegneria delle Telecomunicazioni al Politecnico di Torino.

In questo scritto viene analizzata una categoria di attacchi informatici/telematici diversa dal solito. Con l'evolversi delle così dette tecniche di Software Defined Radio (SDR) e dell'hardware relativo si è aperto un nuovo filone di Cyber Security analysis con costi di attrezzatura alla portata di tutti.

Le schede SDR, collegabili ad una cpu di qualsiasi tipo dal Raspberry PI ad un normale notebook Intel, permettono, tramite chip radio programmabili, di costruire apparati radio non più strettamente realizzati come puro hardware, ma basati, ovvero "definiti" in software, in particolare per gestire le funzioni di modulazione e demodulazione dei segnali, e, se possibile di configurazione dell'hardware. Col metodo SDR si ha un apparato riprogrammabile ogni qualvolta si voglia gestire uno standard diverso.

Questo permette di manipolare il codice "corretto" del protocollo radio specifico ed effettuare attività di "fuzzing" o attacchi specifici per provarne la robustezza.

In tale contesto sono quindi analizzati specifici modelli di minaccia (threat models) verso sistemi radio utilizzati tutti i giorni nel mondo automotive, avionica, navale e smart city ed attacchi costruiti verso i protocolli digitali radio (FM nella sua componente RDS e DAB), verso il GPS, finte base station GSM e altro.

1

2

3

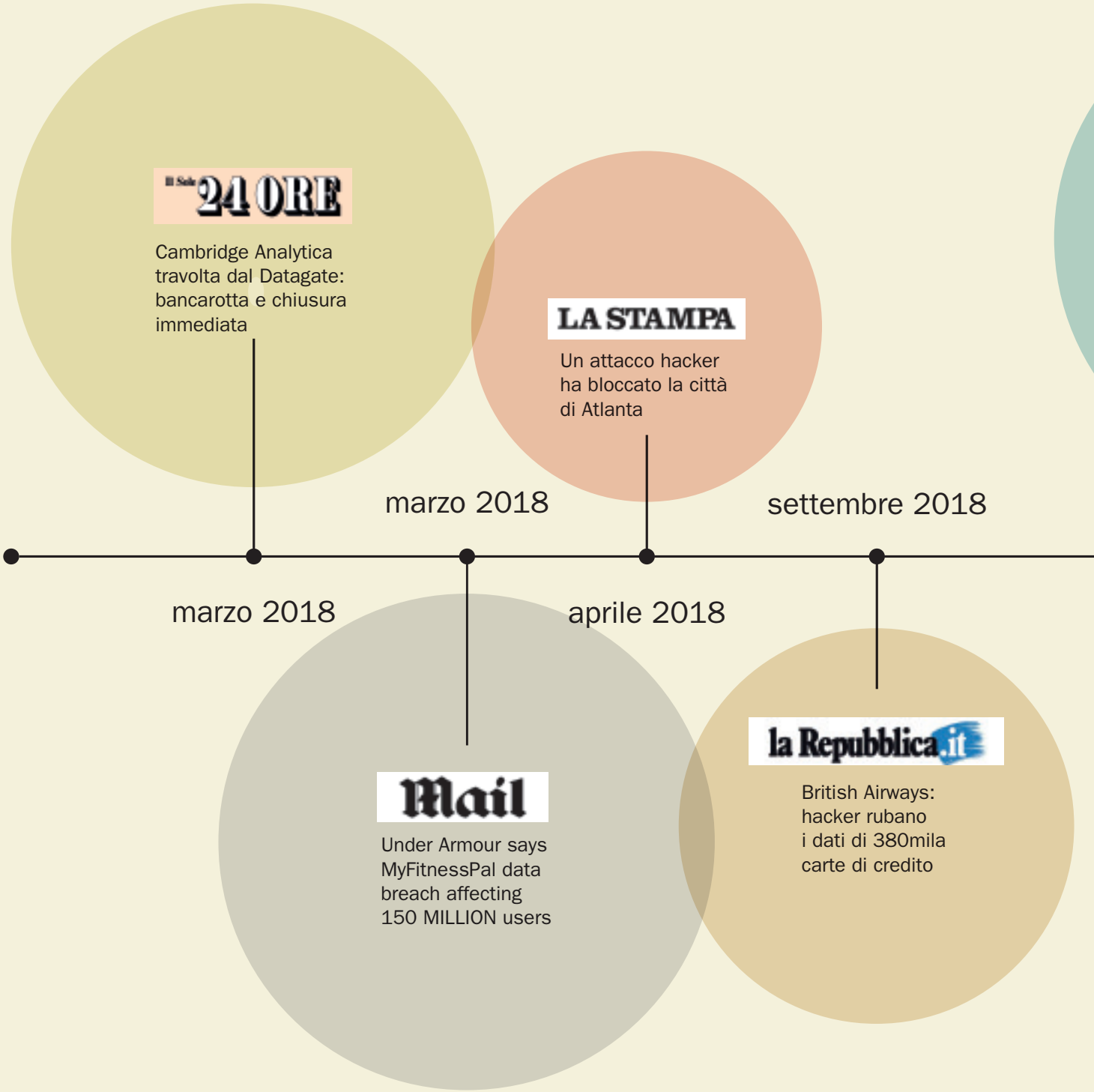
1 – RTL dongles
2 – https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
3 – https://gizmodo.com/phony-cell-towers-could-be-intercepting-yourdata-1629478616

FOCUSING

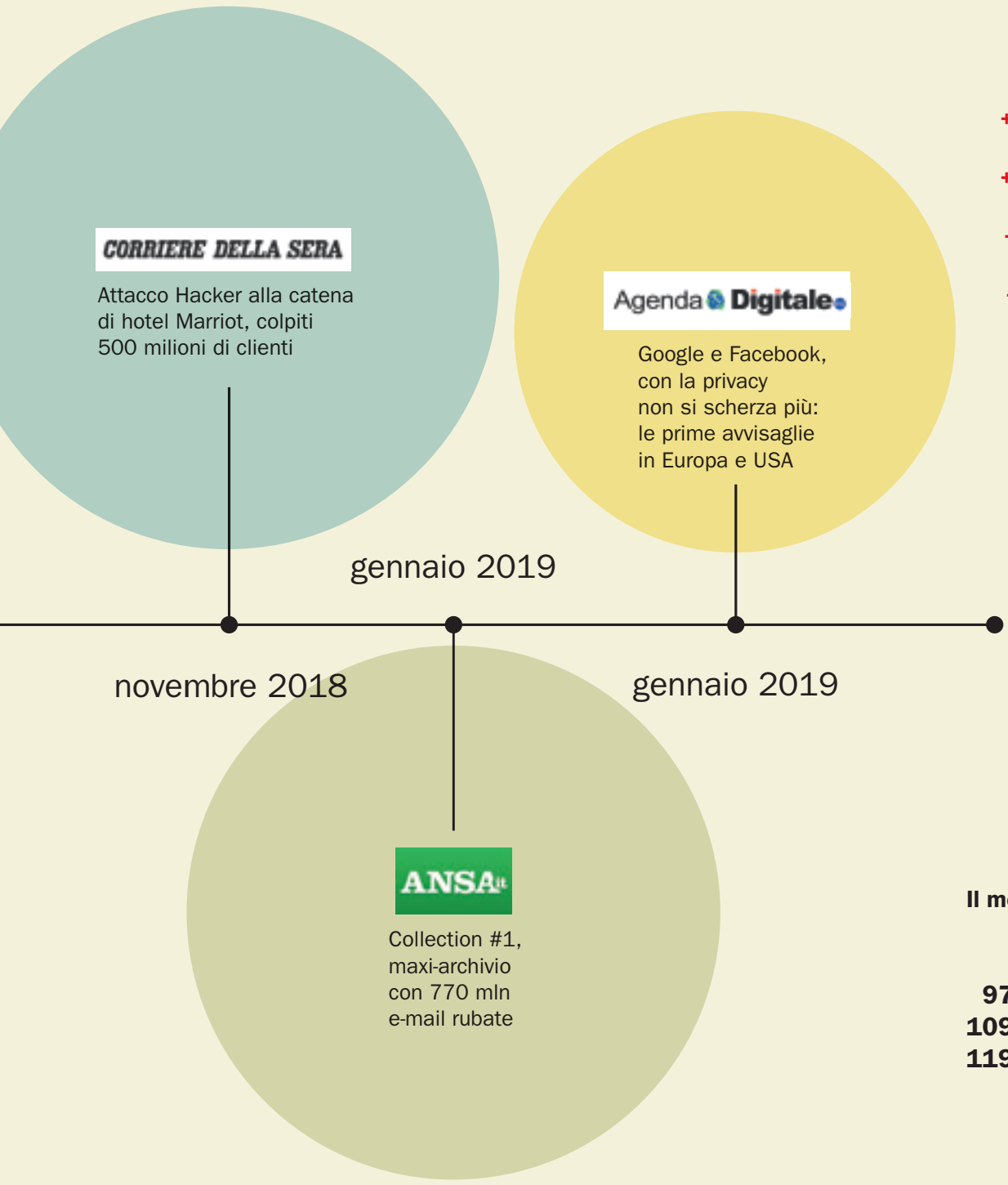
a cura di PPAN

A TUTTO SMART

Attacchi informatici nell'ultimo anno diventati notizia: la democraticità delle tipologie di società nel mirino



FONTE: OSSERVATORI.NET digital innovation 05.02.19



Il mercato italiano dell'IoT
(euro)

3,7 miliardi (2017)
5 miliardi (2018)
+35%

smart metering & smart asset management (utility)
+45% 2017 980 milioni
2018 1425 milioni

smart car
+37% 2017 810 milioni
2018 1065 milioni

smart building
+15% 22017 520 milioni
2018 600 milioni

smart logistics
+29% 2017 360 milioni
2018 465 milioni

smart city
+24% 2017 320 milioni
2018 395 milioni

smart home
+52% 2017 250 milioni
2018 380 milioni

smart asset mng
+25% 2017 210 milioni
2018 270 milioni

smart factory
+40% 2017 150 milioni
2018 250 milioni

smart agricolture
2017 100 milioni
2018 100 milioni

altro
2018 50 milioni

DATI IN EURO

Fonte:
Osservatorio Internet of Things della School of management del Politecnico di Milano
aprile 2019

Il mercato information Security
(euro)

976 milioni (2016)
1090 milioni (2017)
1190 milioni (2018)
+9%

Fonte:
OSSERVATORI.NET digital innovation
Campione:
667 organizzazioni italiane

Elena Pasquini (PPAN)

Information security, mercato in crescita per proteggere account email e portali

Minacce sempre nuove spingono verso l'alto gli investimenti sulla prevenzione dei rischi, con un mercato che ha aumentato del 9% la spesa: truffa, estorsione, spionaggio e interruzione di servizio le principali finalità dei cyber attacchi.
In parallelo cresce – ancor più velocemente – il settore dell'Internet of Things trainato dai servizi abilitati dagli oggetti connessi, ampliando lo spettro degli obiettivi sensibili.

Due ricerche di altrettanti osservatori della **School of Management del Politecnico di Milano** confermano chiaramente la tendenza verso l'introduzione nella quotidianità di oggetti "intelligenti" e di paralleli sistemi per la loro protezione.

«Il numero dei cyber attacchi cresce esponenzialmente con minacce sempre nuove», si legge nel rapporto del febbraio 2019 dell'osservatorio Information Security & Privacy. Phishing e business email compromise (83%), estorsioni (78%), intrusione a scopo di spionaggio (46&) e interruzione di servizio (36%) le finalità degli attacchi nello scenario attuale che, nel prossimo futuro, potrebbero indirizzarsi anche verso l'influenza e la manipolazione dell'opinione pubblica (per il 49% delle imprese intervistate durante la ricerca) e acquisizione del controllo di sistemi come impianti di produzione (40%).

«Necessaria una maggiore pervasività delle iniziative di sicurezza a tutti i livelli manageriali e organizzativi delle imprese e un maggiore coinvolgimento dei profili dedicati alla security nelle strategie di business», sottolineava **Gabriele Faggioli**, responsabile scientifico dell'Osservatorio in concomitanza con la presentazione della ricerca. Cui faceva eco **Alessandro Piva**, direttore dello stesso osservatorio, ricordando che «siamo di fronte a un processo dirompente per quanto riguarda la gestione della sicurezza che porrà nei prossimi mesi e anni sfide rilevanti. Le organizzazioni sono chiamate a internalizzare meccanismi di adattamento e a sviluppare regole istintive da affiancare a strumenti, processi e competenze».

Il fronte IoT

Intanto lo sviluppo del mercato italiano dell'Internet of Things non si arresta e tocca i 5 miliardi nel 2018 con un incremento del 35% rispetto al 2017, spinto sia dalle applicazioni che sfruttano la tradizionale connettività cellulare (2,8 miliardi di euro, +27%), sia da quelle che utilizzano altre tecnologie di comunicazione (2,2 miliardi, +47%). I dati arrivano dall'Osservatorio Internet of Things del Polimi, raggruppati in una ricerca presentata lo scorso aprile. Smart metering e smart asset management per le utility restano in testa nell'ideale classifica del valore per effetto soprattutto degli obblighi normativi che hanno portato all'installazione nel 2018 di 4 milioni di contatori del gas connessi e 5,2 milioni di contatori elettrici intelligenti di seconda generazione: coprono il 28% del mercato per un valore di 1,4 miliardi di euro. Ci sono poi le smart car che rappresentano il 21% del mercato (1 miliardo di euro) con 14 milioni di veicoli connessi, un terzo del parco circolante sulle strade italiane. La crescita è legata in particolare dalle auto connesse nativamente, già dotate di un sistema di connessione Sim o bluetooth fin dalla produzione.

A seguire le applicazioni per lo smart building (600 milioni, +15%) principalmente per la videosorveglianza e la gestione dei consumi energetici all'interno dell'edificio, le soluzioni IoT per la logistica utilizzate per la gestione delle flotte aziendali e per antifurti satellitari (465 milioni, +29%) e le soluzioni per la smart city (395 milioni, +24%). L'ambito con la crescita più elevata è quello della smart home, che cuba 380 milioni e fa segnare un +52% sul 2017, con smart asset management (270 milioni, 25%), smart factory (250 milioni, +40%) e agricoltura smart (100 milioni, 2% del mercato) a chiudere.

L'impatto sulla sicurezza – L'incremento di soluzioni nell'ambito di intelligenza artificiale e IoT, sebbene percepiti più come opportunità che come minaccia, è una sfida sotto il profilo della security. Le principali criticità rintracciate dal Polimi si concentrano sulla mancanza di una logica di security-by-design, scarsa consapevolezza da parte degli utenti e l'assenza di standard tecnologici e di sicurezza per quanto riguarda l'Internet of Things mentre solo il 14% del campione intervistato ritiene che l'Ai possa costituire una minaccia, soprattutto a causa dell'inaffidabilità delle macchine nel lungo periodo e della possibilità di condurre attacchi mirati. Al contrario, il 64% pensa di poterla utilizzare proprio per automatizzare il processo di raccolta e analisi dei dati in ottica preventiva contro minacce e vulnerabilità.

A colloquio con Stefano Zanero, Professore associato di "Computer security"

Come dovrebbe essere costruita la rete di protezione della smart city per essere performance? Quanto conta la collaborazione pubblico/privato?

Due sono gli aspetti importanti da sottolineare. Il primo è che la sicurezza delle smart city dipenderà in modo fondamentale dalla sicurezza dei vari elementi e sistemi che le compongono. Ognuno di questi sistemi deve essere sviluppato dall'origine con un appropriato livello di protezione. Le esperienze correnti ci dicono che ciò non è vero per gran parte dei sistemi IoT, e che per i veicoli le tecnologie migliori non saranno su strada ancora per anni (il parco veicoli è lento nella sua sostituzione). Il secondo elemento è che l'interconnessione di tali sistemi rende il complesso della smart city molto più vulnerabile dei suoi singoli componenti. L'intera esperienza della smart city è innervata dalla collaborazione pubblico/privato, e questo è vero anche per la Cyber Security.

IoT e sicurezza. Affidarsi all'intelligenza artificiale, soprattutto in sistemi complessi come una smart city, rischia di aumentare l'esposizione agli attacchi informatici disastrosi? Quali, nella pratica, potrebbero essere le ricadute di un attacco cyber? Come si struttura la prevenzione?

Sistemi complessi e interdipendenti possono dare luogo a comportamenti imprevedibili durante un attacco informatico. Ad esempio, in isolamento, il fatto che possa venire compromesso uno smart meter ha relativamente poche conseguenze: semplicemente, la misura della corrente consumata potrebbe venire alterata. Ma se un aggressore è in grado di compromettere non uno, ma centinaia di migliaia di smart meter in una città, potrebbe usarli per generare segnali errati, causando un black out o un eccesso di generazione di potenza e sbilanciando la rete elettrica. Attacchi informatici hanno già spento intere reti di distribuzione di energia, danneggiato e bloccato impianti industriali. Sappiamo che gli effetti sono potenzialmente catastrofici. Tuttavia, non dovremmo trascurare il fatto che gran parte degli aggressori non sono motivati dal creare dei danni, ma dal trarre profitto. Quindi ci immaginiamo versioni di ransomware (i virus informatici che chiedono un "riscatto" dopo aver cifrato i documenti sui nostri hard disk), che invece di tenere in ostaggio i dati blocchino una linea di produzione o un automezzo.

Sotto scacco
I principali obiettivi dei cyber attacchi

oggi

91% account email

68% account social

57% portali e-commerce

52% siti web

prossimo triennio

57% device mobili

49% infrastrutture critiche (reti elettriche, idriche e di telecomunicazioni)

49% smart home & building

48% veicoli connessi

Giulio Salvadori, Responsabile scientifico dell'Osservatorio Internet of Things

Smart home e smart factory i settori più in crescita: se le persone sono "l'anello debole" sul lato della sicurezza, quali le applicazioni più a rischio? L'interoperabilità tra i sistemi - auspicabile - nel rendere più immediata l'estensione dei network di sistemi in rete potrebbe aumentare i profili di rischio?

Certamente interconnettere i sistemi amplia la cosiddetta superficie d'attacco, aumentando i profili di rischio. Nel mondo smart home, la semplicità e l'usabilità dei sistemi renderà difficile progettare dei meccanismi di security-by-design. Nel mondo industriale la lunga vita di macchine e robot renderà critiche le operazioni di manutenzione e patching.

Il 36% dei Comuni ha avviato progetti smart city negli ultimi tre anni, con iniziative più robuste e innovative, e 395 milioni spesi nel 2018 (+24%). Ci racconta qualche esempio?

A **Firenze** nel 2017 è stato avviato un progetto con riferimento agli stalli con strisce blu che prevede l'installazione di 70mila sensori in grado di monitorarne lo stato (libero/occupato). Incrociando tali dati con lo stato dei pagamenti, il comune riceve indicazioni puntuali sul mancato pagamento della sosta.

A2A Smart City sta procedendo con l'installazione di 15mila cestini intelligenti a **Milano**, rendendo possibile il controllo a distanza del livello di riempimento e l'ottimizzazione dei percorsi dei camion per la raccolta rifiuti.

A **Segrate** nel 2017 è stata annunciata la costruzione di Milano4you, uno Smart District di circa 90mila m2 in grado di sfruttare soluzioni energetiche e architettoniche all'avanguardia, dotato di un sistema operativo per catturare, integrare ed elaborare i dati provenienti da diverse fonti (ad esempio ambientali, energetici, legati alla sicurezza o alla mobilità) e offrire nuovi servizi ai residenti.

San Benedetto del Tronto ha avviato nel 2017 un piano d'azione che include una serie di innovazioni tecnologiche. Tra queste l'installazione di lampioni non solo per la gestione dell'illuminazione pubblica, ma anche per monitorare l'inquinamento acustico o dell'aria, gli odori vicino a una discarica…. Ad esempio altri sensori previsti sono quello volumetrico per segnalare quando i cassonetti dei rifiuti sono pieni e i chip "annegati" nell'asfalto in grado, ad esempio, di riconoscere se un'auto che occupa un parcheggio per disabili è autorizzata a farlo. Infine, è prevista l'installazione di contatori idrici intelligenti, in grado di avvertire i cittadini circa eventuali consumi anomali.

La mancanza di competenze è il primo fattore che frena l'attuazione dei progetti smart city: quali sono le professionalità necessarie? In che punto del processo di progettazione/realizzazione/monitoraggio dei progetti?

Ciò che manca molto spesso è la figura di uno smart city manager, una persona con competenze sia tecniche che gestionali, in grado di coordinare le varie aree del comune (Assessori mobilità, ambiente, urbanistica, etc.) per permettere l'avvio e la gestione integrata di complessi progetti multi-applicativi all'interno di un unico programma smart city. Ciò comporta da un lato un ridisegno significativo dei processi all'interno della Pubblica Amministrazione e dall'altro il coinvolgimento di un robusto ecosistema di partner pubblici e privati che sappiano portare valore al progetto. Lo smart city manager deve essere una figura che, per esperienza e competenza, sia effettivamente in grado di seguire l'implementazione di questi progetti, coordinando le risorse necessarie e gli attori coinvolti. Una figura immersa all'interno dell'organizzazione e il cui lavoro si connoti per la forte componente multidimensionale e relazionale.

Gruppo Filippetti

PER NOI LA DIAGNOSTICA STRUTTURALE NON HA SEGRETI

RINA
NDT Examination Center
Approved by RINA

NOVATEST DA OLTRE 20 ANNI OPERA NELL'INGEGNERIA CIVILE ED INDUSTRIALE, IN PARTICOLARE NEL SETTORE DEI CONTROLLI NON DISTRUTTIVI E DELLA TOPOGRAFIA, SVILUPPANDO PRODOTTI IN-HOUSE E DISTRIBUENDO LE MIGLIORI TECNOLOGIE DISPONIBILI.

Le competenze specialistiche le hanno permesso di raggiungere risultati di eccellenza negli ambiti dei **controlli non distruttivi, della diagnostica strutturale e dei monitoraggi,** consolidandone il già ampio know how.

Novatest fornisce infine **servizi di consulenza specialistica per ispezioni radiografiche non distruttive** nel mondo delle infrastrutture, in quello dell'Oil&Gas, in quello aerospaziale, quello della cantieristica navale e in quello militare.

PRODUCT DISTRIBUTION

Novatest ricerca e seleziona le migliori tecnologie disponibili sul mercato globale e, per alcune, sigla accordi di esclusiva per la distribuzione a livello sia italiano che europeo.

PRODUCT DEVELOPMENT

Novatest sviluppa, ingegnerizza e produce alcune delle tecnologie presenti nel proprio portfolio di vendita, destinate al mondo della diagnostica e dei monitoraggi strutturali.

PROFESSIONAL CERTIFICATION

Novatest è Centro di Esame RINA perché crede nel valore della formazione continua. Organizza corsi di certificazione su metodologie di indagine nel settore dell'ingegneria civile e industriale.

PROFESSIONAL ASSISTANCE

Novatest garantisce ai propri clienti servizi di altissima qualità nella progettazione delle fasi di indagine/test, nel corretto utilizzo della strumentazione, nell'esecuzione delle indagini e nell'elaborazione dei dati acquisiti.

INDAGINI SUI MATERIALI | INDAGINI GEOLOGICHE | INDAGINI STRUTTURALI | SOFTWARE PLATFORMS | CONTROLLI NON DISTRUTTIVI | TOPOGRAFIA

NOVATEST.
TESTING - CONSULTING - TRAINING

www.novatest.it - info@novatest.it

Francesco Fantera (PPAN)

Alleanza pubblico-privato per la smart city "sicura"

Cyber Security, blockchain, IoT, analytics. Un tempo considerati appannaggio di esperti di informatica, questi termini stanno entrando giorno dopo giorno nel vocabolario collettivo insieme alla corsa all'innovazione che non risparmia le città.

Le potenzialità incredibili di hardware e software, indirettamente riconosciute già a metà degli anni Sessanta dalla cosiddetta "prima legge di Moore", a volte nascondono la graduale e inarrestabile perdita di controllo e consapevolezza rispetto al sistema in cui viviamo.

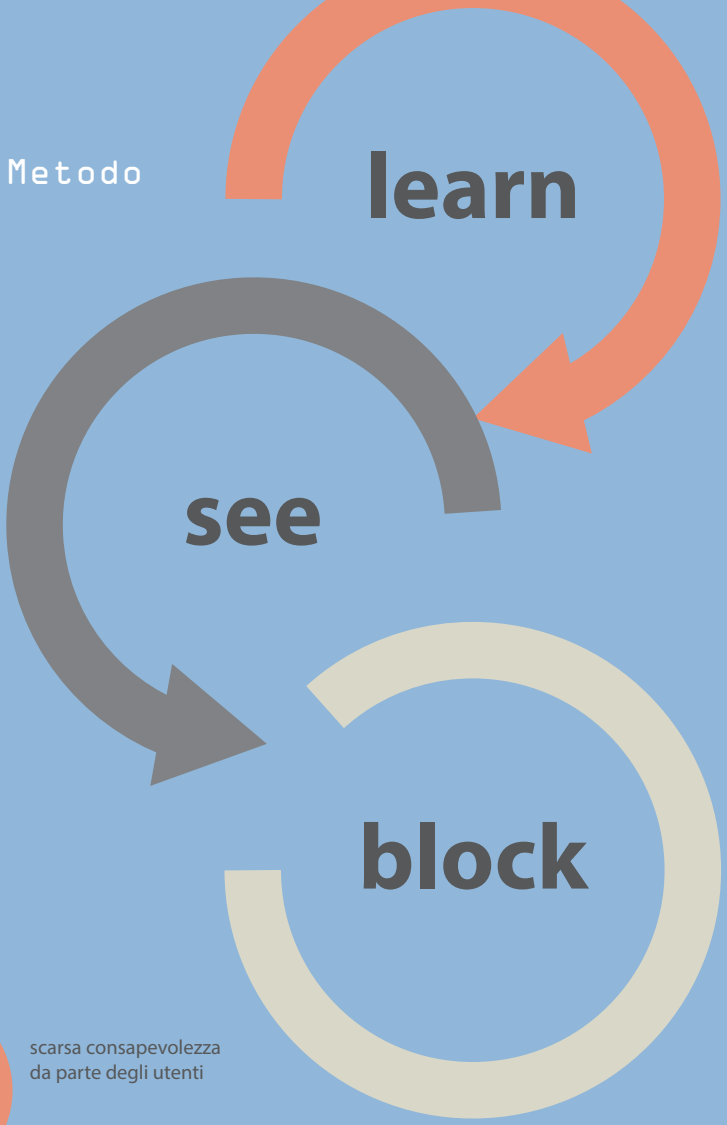
Il gap di conoscenza nei confronti degli strumenti che utilizziamo nella vita di tutti i giorni aumenta i rischi derivanti da un utilizzo poco responsabile di beni e servizi all'apparenza innocui. Un elemento da non sottovalutare se è vero che la sicurezza, è spesso indicata come uno dei bisogni primari. Ma allora perché non dovrebbe esserlo anche in quello che una volta veniva chiamato mondo virtuale?

«La connettività porta molti benefici, ma bisogna anche essere consci che le informazioni possono essere usate da malintenzionati o essere diffuse per errore da un utente poco attento». A sottolinearlo è **Fabio Florio**, responsabile del progetto *IoT Threat Defence* che **Cisco** sta portando avanti da alcuni mesi a Torino. L'iniziativa rientra all'interno della piattaforma "**Torino City Lab**", promossa dal Comune e volta a creare condizioni semplificate per imprese interessate a condurre attività di testing di soluzioni innovative in condizioni reali. E quando si parla di smart city e Cyber Security la partnership pubblico-privato ricopre un ruolo nevralgico poiché permette alle amministrazioni di accedere a tecnologie e competenze altrimenti inaccessibili, e alle aziende di collaudare i nuovi strumenti prodotti.

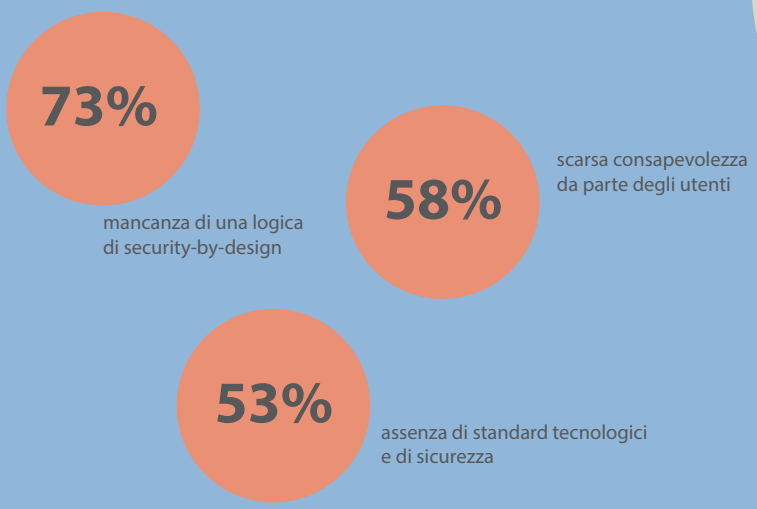
«Come Cisco abbiamo risposto ad una manifestazione d'interesse del Comune di Torino su IoT (Internet of Things) e IoD (Internet of Data). Loro obiettivo – spiega Florio – era quello di raccogliere, tramite dei sensori, una serie di dati utili alla gestione della città. Lato nostro abbiamo mostrato la volontà di partecipare concentrandoci però su un aspetto diverso, ovvero l'analisi di tutti i risultati ottenuti tramite queste sperimentazioni. Il motivo è presto detto: l'IoT è una innovazione tecnologica che consente di raccogliere una mole enorme di dati utili, ma apre tutta una serie di porte agli attacchi informatici. È quindi necessario tutelarsi andando a proteggere proprio queste reti che trasformano in cifre quanto viene restituito dai sensori. In sostanza è di questo che si occupa la Cyber Security, protegge i sistemi da tutta una serie di attacchi che continuano ad evolversi giorno dopo giorno in quanto a tipologia e complessità».

Metodo

1



2



Aree di miglioramento

1 – Approccio integrato
2 – Le criticità per gli oggetti connessi - Fonte: Osservatorio Information Security & Privacy – Polimi (febbraio 2019)

La risposta alle minacce informatiche

– «Per essere efficaci è fondamentale adottare un approccio sistemico e non riferirsi al singolo prodotto. È la collaborazione fra diversi elementi che porta ad un elevato livello di protezione – sottolinea **Florio** –. Ad esempio i sistemi ISE e Umbrella, attraverso una verifica automatica delle credenziali e dell'indirizzo DNS, ci consentono di analizzare gli accessi ad una rete bloccandoli automaticamente nel caso vengano rilevate anomalie. Abbiamo poi sviluppato il sistema ETA che consente di analizzare anche il traffico cifrato, al cui interno sempre più spesso passano le minacce, il tutto senza accedere al contenuto dei dati. E questi sono solo alcuni di quelli sviluppati da **Cisco**, parte di un sistema più grande pensato per proteggere non una sola fetta di traffico, anche perché in quel caso sarebbe come non avere nessun tipo di difesa. Resta un dato di fatto: nessun sistema è sicuro al 100% e per questo si deve essere in grado di reagire e isolare gli attacchi che riescono a superare le barriere protettive esterne».

L'imponderabile rischio del fattore umano

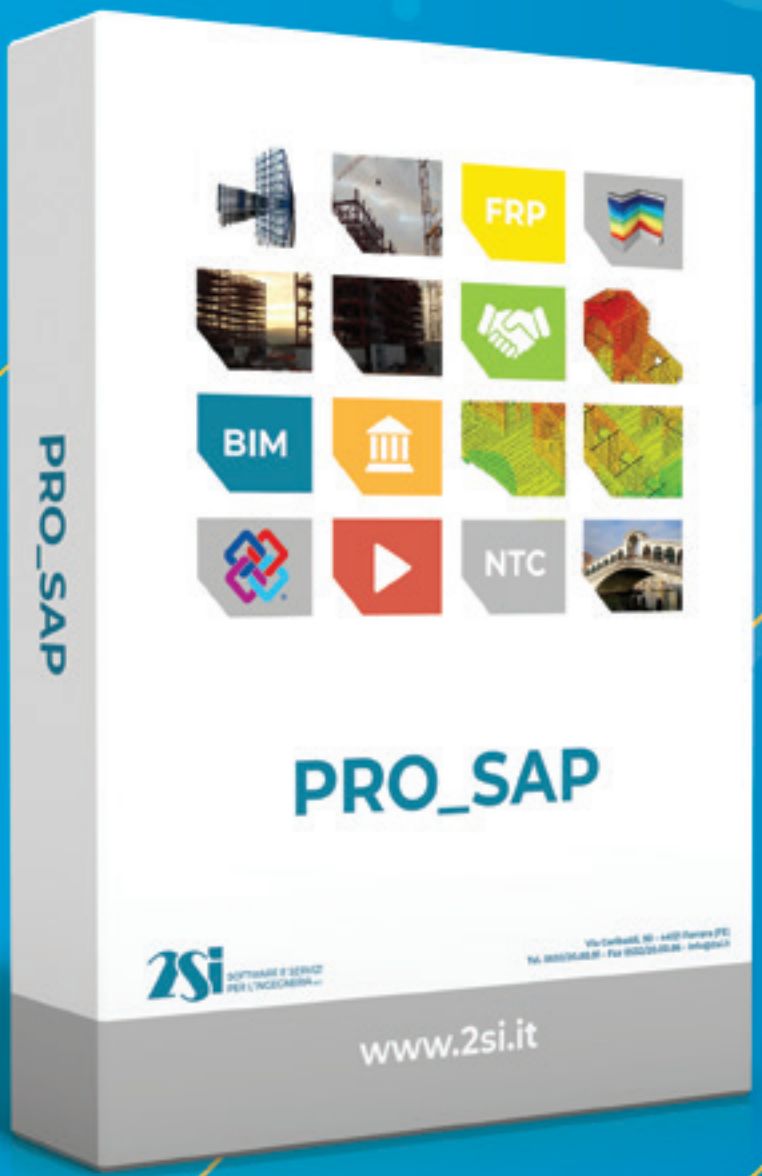
– «A volte un utente "distratto" rappresenta il vulnus di un dispositivo di protezione. Se si chiude una casa per tenerla al riparo dai ladri, ma ci si dimentica una finestra aperta, si possono utilizzare tutti gli accorgimenti del mondo, ma la protezione viene meno. In questo senso ci stiamo concentrando, non solo a Torino, sulla formazione del personale rispetto i nuovi processi aziendali. La scarsa conoscenza del mezzo, infatti, può portare le persone a creare dei passaggi pericolosi e che potrebbero essere soggetti al furto di informazioni. Con **Cisco Academy** organizziamo corsi generalisti e specialisitici per i dipendenti sia del settore pubblico che di quello privato. Nostro ulteriore obiettivo è quello di formare anche gli studenti degli istituti superiori e delle università con programmi ad hoc pensati per diffondere il più possibile la conoscenza dei mezzi informatici».

Il compromesso tra privacy e protezione dati

Si tratta d un tema molto dibattuto. La necessità di proteggere i sistemi informatici e di trasmissione dei dati e insieme di rispettare la privacy si avvantaggia della possibilità di «difendere le reti senza accedere ai contenuti: è quindi quella la strada da seguire. Nelle città si sta molto lavorando sempre di più sull'installazione di sensori definiti di sicurezza fisica, come le telecamere nelle zone sensibili o quelle per il controllo del traffico. Vista la sensibilità delle informazioni, tutto il materiale raccolto deve essere necessariamente abbinato a una modalità di tutela virtuale. A Milano, ad esempio, stiamo affiancando il Comune proprio a questo scopo».

PRO_SAP

ESALTA
i tuoi progetti!



SCOPRI DI PIÙ

www.2si.it

2Si
SOFTWARE E SERVIZI
PER L'INGEGNERIA

blumatica
Software Edilizia e Sicurezza

UNI/TS 11300-2:2019 e FAQ del MiSE:
Blumatica Energy è già in linea!

Lo scorso 7 febbraio è stata pubblicata la UNI/TS 11300-2:2019 "*Prestazioni energetiche degli edifici - Parte 2: Determinazione del fabbisogno di energia primaria e dei rendimenti per la climatizzazione invernale, per la produzione di acqua calda sanitaria, per la ventilazione e per l'illuminazione in edifici non residenziali*".

La nuova norma sostituisce la versione del 2014 e, rispetto a quest'ultima, apporta le seguenti novità:

- adeguamento a carattere editoriale alla premessa e all'introduzione raccordandole alle UNI/TS 11300 pubblicate nel 2016
- conversione a testo "normativo" di una nota "informativa" sui sistemi di regolazione
- aggiunta di un'appendice sul calcolo dei fabbisogni energetici di acqua calda sanitaria in presenza di recuperatori di calore dai reflui delle docce
- eliminazione dell'appendice E (calcolo della prestazione energetica di edifici non dotati di impianto di climatizzazione invernale e/o di produzione di acqua calda sanitaria) poiché superata dalle indicazioni dei Decreti Ministeriali del 26 giugno 2015.

Si tratta pertanto - spiega il Comitato Termotecnico Italiano (CTI) - di un aggiornamento con un impatto minimo sulla metodologia di calcolo che, seppure debba essere necessariamente recepita dagli operatori entro 90 giorni dalla pubblicazione (quindi l'8 maggio 2019), non si ritiene tale da richiedere una nuova procedura di verifica dei software commerciali e degli strumenti di calcolo della prestazione energetica degli edifici (ai sensi dell'art.7 del DM 26 giugno 2015, cosiddetto 'Requisiti Minimi') rispetto a quella attualmente in vigore.

Infatti, l'unica sostanziale modifica riguarda la **nuova metodologia di calcolo introdotta nell'Appendice E** che riguarda **la valutazione dei fabbisogni di energia termica utile per acqua calda sanitaria nel caso di presenza di sistemi di recupero di calore dai reflui di scarico delle docce**.

Tale metodologia può essere applicata a tutte le tipologie di edifici, siano essi residenziali o non residenziali.

Requisito fondamentale per tener conto di tale recupero è l'installazione di un sistema che prevede uno scambio diretto all'utilizzo, cioè nel caso in cui l'energia termica recuperata preriscalda l'acqua fredda che sarà utilizzata dall'utente.

Si precisa, infine, che la UNI/TS 11300-2:2019 costituisce solo un aggiornamento editoriale e tecnologico rispetto alla precedente versione e pertanto non rientra nel processo di recepimento delle nuove norme EN sviluppate sotto mandato M/480. Quest'ultimo è attualmente in corso e prevede la redazione di specifiche appendici nazionali alle norme EN e di una serie di moduli aggiuntivi che costituiranno il nuovo pacchetto UNI/TS 11300.

Altra importante novità riguarda le FAQ 3ª serie, pubblicate dal MiSE il 20 dicembre 2018.

Il documento, che integra le FAQ già pubblicate nel mese di ottobre 2015 (1ª serie) e nel mese di agosto 2016 (2ª serie), fornisce ulteriori chiarimenti per l'applicazione delle disposizioni previste dal D.M. Requisiti Minimi recante modalità di applicazione della metodologia di calcolo delle prestazioni energetiche e dell'utilizzo delle fonti rinnovabili negli edifici, nonché dell'applicazione di prescrizioni e requisiti minimi in materia di prestazione energetica.

I principali chiarimenti riguardano:

- Le verifiche FER nel caso di ampliamento
- Il calcolo della quota rinnovabile per le pompe di calore
- La verifica di formazione della condensa interstiziale per le strutture opache
- La verifica di trasmittanza delle strutture.

Blumatica Energy è già aggiornato alla nuova UNI/TS 11300-2:2019 ed alle nuove FAQ del MiSE!

PROVALO GRATIS e passa a Blumatica!

www.blumatica.it/energy

Via Irno snc - 84098 Pontecagnano Faiano (SA) - Tel: 089.848601 - Fax: 089.848741 - Email: info@blumatica.it

TORINO LABORATORIO D'INNOVAZIONE

La sperimentazione nella prospettiva di Paola Pisano, assessore all'innovazione

Torino City Lab (TCL) è un laboratorio d'innovazione aperto e diffuso su tutta l'area cittadina. Promosso dal Comune, coinvolge soggetti pubblici e privati interessati a testare le nuove tecnologie. L'amministrazione agisce come facilitatore per la creazione di sinergie che, sul proprio territorio, consentano di sperimentare nel campo del 5G, IoT, della robotica e della sensoristica avanzate.

«TCL segue una regola: se c'è un'azienda che sta sviluppando un servizio innovativo che può essere assimilato allo sviluppo della città viene da noi – sottolinea Paola Pisano, Assessora all'Innovazione della città della Mole –. Il motivo è semplice. A Torino abbiamo un team di esperti che sta studiando l'applicazione del 5G e abbiamo piattaforme adatte alla sperimentazione. In sostanza vogliamo attrarre aziende in cerca di un partner istituzionale disposto a testare le nuove tecnologie legate alla smart city. La nostra politica non è diretta alle start up, ma alle imprese in crescita perché abbiamo i tempi stretti della Legislatura. L'obiettivo è quello di rapportarci con realtà già strutturate e in grado di realizzare progetti che ci aiutino a dimostrare che questa politica di apertura ai privati funziona».

E sotto il profilo della Cyber Security?

«La nostra struttura interna ha due livelli di sicurezza. Uno è gestito dal CSI Piemonte, un consorzio di enti pubblici che dal '77 opera nel campo delle tecnologie dell'informazione e della comunicazione e si occupa di proteggere i nostri database da eventuali attacchi hacker. Abbiamo poi il progetto di infrastruttura tecnologica, aperta e utilizzabile a livello nazionale, che stiamo creando per Torino City Lab in partnership con Intel, Tim e Cisco. Questa si baserà su 5G e cloud computing e, proprio con Cisco, stiamo realizzando un progetto di layer di Cyber Security che loro stanno finanziando con un milione di euro. Stiamo cercando di dar vita ad uno standard replicabile a livello nazionale, anche attraverso il Mise che osserva con attenzione l'andamento della sperimentazione».

Elena Pasquini (PPAN)

Smart building

Dal progetto alla gestione: la chiave di volta dell'integrazione

La sicurezza costituisce uno dei principali driver dell'automazione dell'edificio e dell'utilizzo di soluzioni appartenenti all'IoT. Oltre a garantire efficienza dal punto di vista fisico, però, la sfida è rappresentata dalla raccolta e protezione del dato, chiamata a rispondere anche alle nuove norme sul Gdpr, e soprattutto dalla sua corretta interpretazione.

Le tecnologie non si limitano più a percepire un allarme, ma monitorano e legano tra loro processi diversi, raccolgono e gestiscono dati e sono in grado di interpretarli in maniera intelligente. Le azioni di sistema - dalle operazioni più semplici come l'apertura di una serranda o l'accensione del riscaldamento sulla base della temperatura percepita da un termometro o da quelle più complesse come la reazione a un allarme incendio in ambienti tenuti a particolari condizioni e con gradi di rischio elevati - sono la nuova frontiera della gestione dell'edificio. Definito "smart" per semplicità, il building sui cui sono installati una serie di sistemi automatizzati è in effetti un organismo complesso e complicato che fin dalla sua progettazione dovrebbe avvantaggiarsi dalla scelta di componenti tra loro dialoganti.

Se il "dato", inteso come informazione, è il valore principe degli smart building, la sua interpretazione è fondamentale per la sua efficacia. Tanto più in un'ottica di sicurezza.

L'utilizzo di intelligenza artificiale o soluzioni avanzate di tracciabilità e riconoscibilità sulla base di dati univoci (come quelli biometrici) da un lato aumentano performance e adattabilità dei sistemi ma dall'altro diventano porte d'accesso al dato e di conseguenza alle reti su cui è veicolato, tanto per le aziende quanto per le abitazioni.

Il risk assessment - «È la gestione intelligente di tutte le informazioni che si possono raccogliere a fare la differenza, a permetterci di ottimizzare l'esistente o agire sui sistemi», spiega **Stefano Cremonini**, system engineering director e responsabile dell'area Ricerca & Sviluppo per Kireti, brand dedicato a soluzioni per la gestione della sicurezza e dell'innovazione di **Site**. Per questo, «l'approccio per progettare una piattaforma di controllo dell'edificio si basa sul risk assessment – gli fa eco **Pierluigi Marrocu**, solutions & products engineer per la stessa azienda – per identificare i vari livelli di sicurezza cui mi voglio riferire su un determinato compound, che si tratti di un campus universitario o di un impianto produttivo». Rispetto ai quattro livelli di sicurezza che in genere vengono individuati – dalle vie d'ingresso agli edifici ad accesso controllato ed elevata sensibilità – è il confronto con il committente a indirizzare il posizionamento dei sistemi, la tipologia di sensoristica da installare e il relativo costo. «Una sonda che trasmette da un'area esterna un dato semplice come la temperatura – specifica Marrocu – ha necessità di livelli di sicurezza minimi e solo nella congiunzione con l'unità di connessione. Diverso il caso di una centrale che immagazzina particolari categorie di dati, come quelli nevralgici di consumo: qui entra in campo pesantemente la sicurezza dell'infrastruttura di rete, con per esempio protocolli Sql o che criptano la comunicazione tra i dispositivi. A livello logico viene poi progettata sempre l'atomicità, individuando l'unità chiave dell'edificio».

L'analisi del rischio valorizza, gli aspetti logici e i profili fisici come decidere dove far passare gli apparati o quali mezzi trasmissivi usare (wifi, fibra ottica, rame) per evitare falle nel sistema dettate da valutazioni sommarie. L'esempio potrebbe essere quello di un sistema di sicurezza che dialoga in wifi al suo interno: bisogna tener in conto che sarebbe possibile effettuare il jamming (un "disturbo intenzionale" sulla rete) dall'esterno e creare dei blocchi che impediscono gli accessi anche a chi ne sarebbe qualificato. Il risultato? Nel caso di un'attività commerciale, la perdita del fatturato fino a quando il problema non è risolto. Gli stessi impianti che garantiscono la sicurezza non devono diventare di per sé un fattore di rischio. «Stiamo lavorando con importanti catene di supermercati – afferma Marrocu – ma oltre a bloccare gli accessi ai malintenzionati dobbiamo riuscire a evitare che si intervenga su cavi e centralina, per esempio, bloccando le attività con ricadute economiche pesantissime».

Il caso pratico - L'altro esempio è il campus dell'Università della Calabria (si vedano le specifiche a pagina 100) su cui si sta terminando il rilascio del sistema. È costituito da un insieme di edifici chiamati cubi per la loro forma dislocati lungo un asse centrale. «Per noi il cubo non è solo un accentratore di informazioni ma un edificio con una logica, dotato di una centrale di acquisizione intelligente. In caso di fail del singolo cubo, esso viene escluso seguendo logiche di gestione e protocolli di sicurezza che affiancano quelli di scambio dati; le altre strutture non vengono influenzate né lo è il funzionamento della piattaforma di gestione dell'intero Ateneo», spiega Marrocu.

La valorizzazione del sistema - Il valore dei sistemi interoperabili è slegato da quello delle singole componenti sensoristiche: l'evoluzione tecnologica ha permesso di avere una media di sensori performanti anche senza acquistare il top di gamma mentre è sempre più funzionale investire sulle piattaforme di gestione cui chiedere la semplificazione della lettura aggregata delle informazioni raccolte. Con un duplice obiettivo: avere dei report che realizzano uno schema di coordinazione, garantiscono accessi molteplici (da web, tramite client certificato..) e fanno viaggiare su un binario funzioni di controllo e sicurezza del sistema da un lato; evitare di assegnare personale specializzato a funzioni che possono essere automatizzate dall'altro.

«In genere sono tre le variabili che influiscono sul costo: in primo luogo l'aspettativa del cliente – semplifica l'ingegner Cremonini – per cui la consapevolezza dell'interlocutore di una relazione tra livelli di sicurezza e investimento permette di orientarsi fin da subito su soluzioni efficienti, prima che economiche; le dimensioni del compound; la compartimentazione dei livelli di sicurezza e il posizionamento voluto per l'impianto». Variabili ampissime che fanno oscillare i preventivi da poche decine a centinaia di migliaia di euro.

Sistemi in evoluzione - Sicurezza fisica e tecnologica degli impianti vanno a braccetto con le scelte delle persone che vi si interfacciano. Come sempre, l'azione umana può vanificare un sistema perfetto: basta una password non sicura o condivisa con tutti gli abilitati al sistema. L'importanza della formazione, nell'approccio come nella gestione, è supportata anche da modelli di implementazione dell'installato per l'affinamento del modello inizialmente individuato e il rilascio di release successive.

Quello adottato in Kireti *(Figura 1)* ha sei step verticali declinati orizzontalmente e mappa le azioni di sviluppo del sistema tecnologico da affiancare con scelte interne da parte del committente. Come la realizzazione del piano di cambiamento organizzativo per l'assegnazione di nuove mansioni quando si è definito il modello di sistema o la formazione del personale.

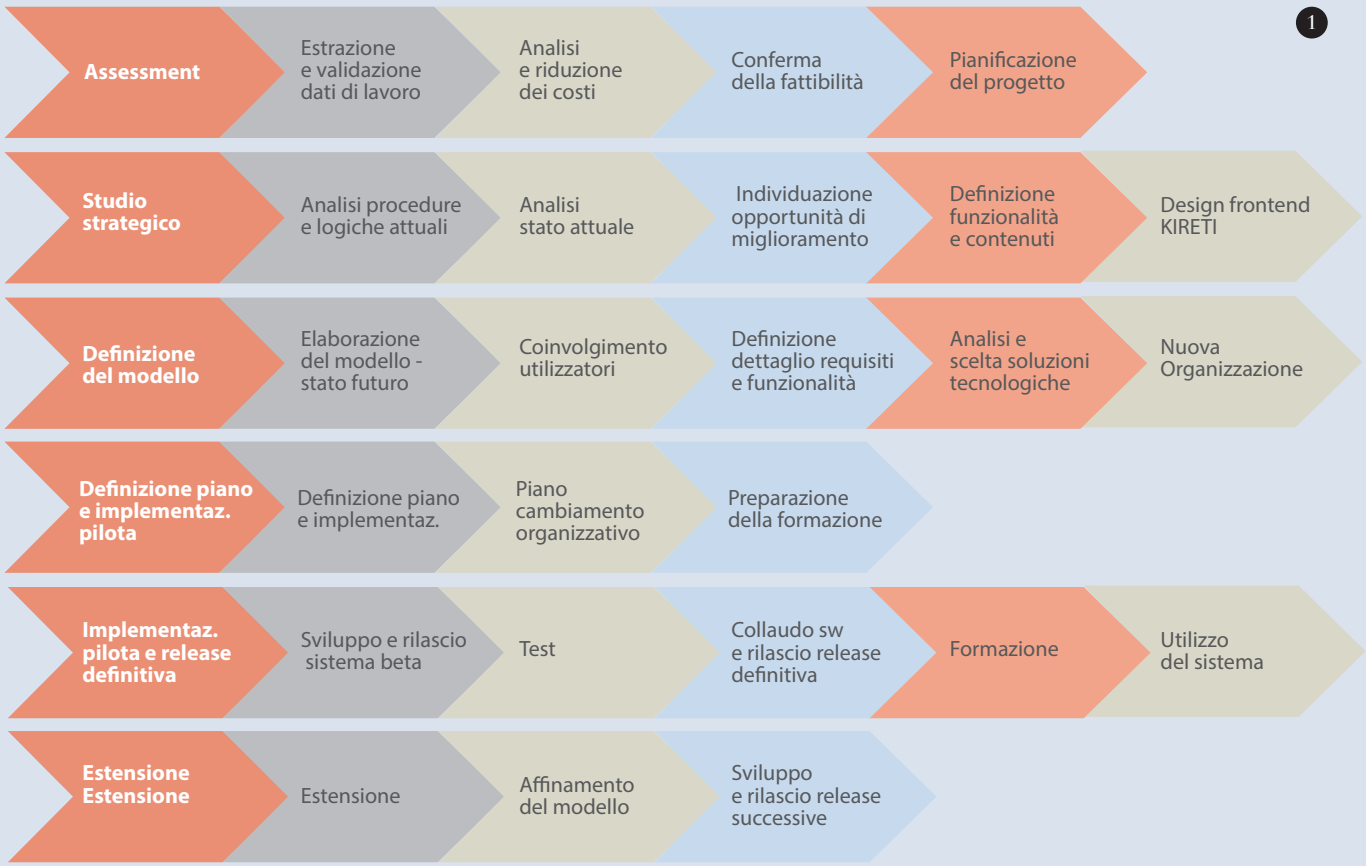
Il progetto

Il campus dell'Università della Calabria ad Arcavacata di Rende, in provincia di Cosenza, si estende su una superficie di circa 200 ettari sui quali sono dislocati 14 centri dipartimentali e 170 aule.

Con il più grande sistema bibliotecario del Mezzogiorno (500mila volumi, 900 postazioni di lavoro e 300 accessi telematici), l'Ateneo mette a disposizione un Auditorium da 500 posti, due sale cinema da 250 posti ciascuna, un centro sanitario, un ufficio postale, un asilo che ospita circa cento bambini, tre centri di servizi comuni, un Museo di storia naturale, l'orto botanico, il centro Arti musica e spettacolo oltre al centro linguistico d'Ateneo.

Per la realizzazione del campus fu organizzato alla fine degli anni '60 un concorso vinto dal gruppo con Vittorio Gregotti come capofila. Il progetto ha previsto, lungo un tracciato rettilineo di oltre 2 km una serie di "cubi" (lato di 25,5 metri), con altezze che seguono l'andamento collinare di Arcavarcata, all'interno dei quali sono collocati i dipartimenti.

Quattro i blocchi: quello delle Maisonettes comprende i primi alloggi per studenti realizzati per l'ateneo, il Martensson, ulteriormente diviso in Martensson nuovi e Martensson vecchi, che prendono il nome dal progettista Dänen Martensson; il Molicelle e il Chiodo, ultimato e aperto nel settembre 2007. All'interno dei blocchi Maisonettes e Martensson sono presenti le strutture di ristorazione.



1 – Il modello di implementazione (@ Kireti)

Gli edifici sono smart quando i sistemi dialogano tra loro

Parola all'ingegnere Stefano Cremonini

Il primo obiettivo di uno smart building è leggere "dentro" o "tra" le informazioni, così come l'etimologia della parola intelligenza suggerisce: mettere in relazione i dati presenti nei sistemi installati sugli edifici, eterogenei e molto diversi tra loro e che tipicamente non comunicano anche per l'uso di modi e linguaggi molto differenti.

Essere in grado di relazionare i dati provenienti da tali sistemi ed attuare delle conseguenti azioni, è la capacità di trasformare un edificio, magari attrezzato con le migliori tecnologie disponibili ma "normale", in un "edificio intelligente". In stretta correlazione al tema dei big data, quindi, la nostra visione di smart building è orientata alla gestione intelligente di tutte le informazioni che si possono raccogliere da sensori, dispositivi e impianti. L'edificio sarà tanto più smart quanto più sarà in grado di raccogliere, aggregare, correlare ed elaborare i dati raccolti, fornendo informazioni, allarmi, statistiche utili alla sua gestione e manutenzione efficiente.

Come ultima finalità, laddove i sistemi presenti lo consentano, ci deve essere poi l'attuazione di azioni predefinite basate sulla correlazione di uno o più eventi, anche in ottica di sicurezza ed efficientamento.

Appuntamento in fiera

La sicurezza di dati, cose e persone diventa un asset strategico per garantire l'utilità e l'efficacia di ogni tecnologia. Parlare di security non vuol dire più affrontare una tematica tecnica, ma dibattere di un tema di governance. Con questo approccio si sta preparando "Sicurezza", l'esposizione in Fiera Milano che dal 13 al 15 novembre 2019 si svolgerà in parallelo con Smart Building Expo e presenterà soluzioni per le aziende insieme a occasioni di formazione per tutta la filiera.

Che si tratti di aziende, città o centri commerciali, infatti, le scelte di security sono sempre più un valore, intorno al quale si gioca l'indice di affidabilità dello stesso committente. In questo contesto di grande cambiamento diventa fondamentale la competenza degli operatori perché la sicurezza è ormai un tema irreversibilmente nelle mani di più soggetti: costruttori, progettisti e installatori (anche alla luce del Gdpr), ma anche grandi utilizzatori e privati, che oggi possono integrare i propri sistemi di sicurezza rappresentando una risorsa per tutta la comunità. La "cultura della sicurezza" rappresenta, così, sempre più un vero e proprio patrimonio cui i costruttori e tutti i rappresentanti della filiera sono chiamati continuamente a contribuire.

TG Soft
Cyber Security Specialist
www.tgsoft.it

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

Ransomware

MONDO | GIOVEDÌ 20 GIUGNO 2019

La città di Riviera Beach, in Florida, ha deciso di pagare 600mila dollari per provare a liberarsi da un attacco informatico

Ransomware

cosa sono e come mi difendo!

Centro Ricerche Anti-Malware di TG Soft

Sicurezza

"WannaCry e le aziende? La disattenzione alla sicurezza è paradossale"

ITALIA

Non aprite quella mail: attenzione al Cryptolocker

Cosa sono i Ransomware:

sono dei malware in grado di cifrare i file di dati del computer o aree critiche dei PC/Server (tipo la MfT Master file Table), rendendo inaccessibili i file di lavoro e/o l'intero computer. Per il recupero dell'accessibilità ai dati e/o al PC/Server, viene richiesto un riscatto, generalmente in BitCoin (BtC) o altre cryptovalute.

Come avviene la cifratura dei file o delle aree critiche dei PC/Server:

attraverso vari stratagemmi di ingegneria sociale (social engineering) i cyber-criminali procedono ad operare campagne massive di e-mail (malspam), che cercano di indurre il ricevente a cliccare sul/i link o ad eseguire l'allegato. Cadendo nel tranello, si attiva il processo di cifratura che utilizza algoritmi molto robusti di derivazione militare quali RSA, AES, SALSA20.
Di fatto la cifratura, se non vi sono errori nell'implementazione dell'algoritmo, è di difficile, se non **impossibile, decifratura** anche con il Brute Force.

I Ransomware sono quindi un pericolo per il nostro prezioso lavoro!

#PROTEGGIAMOiTuoiDATI

Preservare i dati da questi attacchi è possibile!

Le nostre tecnologie AntiRansomware sono in grado di bloccare la cifratura dei file di dati nella fase iniziale dell'attacco, con la possibilità di ripristinare in brevissimo tempo i pochi file cifrati prima del blocco.

Si tratta di un approccio MultyLayer che **TG Soft** Cyber Security Specialist ha sviluppato a partire dal 2014 con tecnologie proprietarie che sono state integrate in Vir.IT eXplorer PRO AntiVirus-AntiSpyware-AntiMalware e AntiRansomware.

VirIT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

Abbiamo le TECNOLOGIE *per* PROTEGGERTI

Vir.IT Backup
File di backup protetti anche dai Ransomware di nuova generazione

VirIT Backup permette di proteggere i file di backup da questo generati e periodicamente aggiornati in modo automatico non solo dai ransomware già noti, ma anche e, soprattutto, da quelli di nuova generazione, non ancora intercettati da alcun software AntiVirus-AntiMalware.

Protezione Crypto-Malware Anti-Ransomware

Vir.IT eXplorer PRO integra tecnologie euristico-comportamentali in grado di riconoscere un processo di cifratura in atto e mitigarne gli effetti, salvaguardando dalla cifratura mediamente non meno del 99,63% dei file di dati presenti nel PC/Server da attacchi ransomware anche di nuova generazione.

I pochi file che dovessero venire cifrati nella fase iniziale dell'attacco potranno essere decifrati/ripristinati attraverso:

- L'intercettazione in memoria della chiave di cifratura nella fase iniziale dell'attacco che permetterà di de-codificare i file recuperandoli senza perdere alcuna modifica;
- Backup On-The-Fly che effettua automaticamente copie di sicurezza dei file di dati in via preventiva.

Grazie a queste tecnologie è possibile ripristinare fino al 100% dei pochi file di dati cifrati nella fase iniziale dell'attacco.

Non lasciare che i tuoi dati vengano cifrati dai Ransomware.
Affidati a **Vir.IT eXplorer PRO**, l'**AntiVirus ITALIANO,** per difenderli al meglio da questi attacchi e da tutte le altre tipologie di virus&malware realmente circolanti.

TG Soft S.r.l. Cyber Security Specialist
Via Pitagora, 11/b - 35030 Rubàno (PD) - ITALIA
Tel. **049.8977432**
E-mail: segreteria@tgsoft.it
commerciale@viritpro.com
https://www.tgsoft.it/italy/antiransomware.asp

Elena Pasquini (PPAN)

I datacenter moderni? Ecosistemi per siti interconnessi

Sicurezza ed economie di scala tra gli elementi di valutazione nella scelta di costruire un proprio centro di elaborazione dati piuttosto che rivolgersi a siti di colocator. Una tendenza all'esternalizzazione legata all'esigenza di rapida connessione più che di storage del dato, come avveniva in passato.

La sicurezza del dato in un data center viene considerato quasi "scontato" perché è il punto di partenza nella progettazione di qualsiasi sito dedicato. A spiegarci il rapporto tra architettura e cloud computing, con le relative ricadute in termini di sicurezza, è **Alberto Caccia**, director **CAP DC Italia**, brand del Gruppo **Lombardini22** specializzato nella progettazione di data center.

«Il vero ragionamento è sull'architettura degli impianti, più che su quella fisica – afferma Caccia – perché di fatto l'involucro è al servizio dell'attività prevista al suo interno». Gli elevati livelli di sicurezza – fisica, logica, operativa – si perseguono fin dalla scelta della localizzazione quando si tratta di strutture "colocator" (che ospitano quindi datacenter di terzi) mentre è diverso l'approccio dei clienti corporate che scelgono di avere un data center proprietario.

«Sono cambiate le esigenze e con esse la strategia prevalente – sottolinea Caccia –. Il mondo della colocation è nato per rispondere a un'esigenza di archiviazione del dato con tematiche di backup, vulnerabilità, presidio dei luoghi e prevenzione incendi. Adesso si propongono sempre più come luoghi dove altissima è la connettività per rispondere alla progressiva creazione di ecosistemi a livello di information technology che consentano di avere siti interconnessi agli ambienti cloud dei clienti. In questo senso, il ragionamento da seguire è certamente legato alla sicurezza ma molto più spostato sulla connettività con la previsione di doppi collegamenti in fibra, doppio provider e, in generale, un'ampia e rapida accessibilità al dato».

Prospettive Future

Sulla spinta del 5G e dell'Internet of Things cambierà la tendenza a costruire hyperscale data center?

Le opinioni sono discordi e molto dipenderà dalla capacità tecnologiche di sopportare le richieste del mercato. Nel mentre, chi pensa che lo sviluppo delle applicazioni IoT andrà di pari passo con la collocazione diffusa dei data center inizia a investire sugli "edge", strutture con il volume di un container.

Una risposta alla domanda di alte prestazioni ed alta latenza che portano a distribuire sul territorio i servizi cloud e di elaborazione dati per tagliare i pur già brevissimi tempi di latenza del dato dal suo invio alla ricezione: micro data center per l'edge computing.

Equinix è proprietaria di 200 data center nel mondo. Ha un Pue (Power Usage Effectiveness) a livello globale pari a 1,2 mentre in Italia – per via del clima mite - sale 1,6.

Tra le metriche da tenere in considerazione, quindi, oltre alla scelta di siti lontani da luoghi considerati "a rischio" (come con ferrovie e autostrade nelle vicinanze), è la progettazione di impianti elettrici ridondanti e resilienti – in grado di operare anche in casi di interruzione del flusso di corrente, meglio ancora se interamente manutenibile senza interruzione – e di paralleli impianti di raffreddamento che permettano di mantenere all'interno un predeterminato grado di temperatura e umidità.

In parallelo si procede con la valutazione dei rischi e la definizione degli impianti antincendio e antitrusione, collegati, insieme ai sistemi di monitoraggio e supervisione dell'ambiente e degli impianti, a un cruscotto di gestione.

La criticità, anche in questo caso, è legata al fattore umano. «La maggior parte dei problemi di non connettività (e quindi di tenuta in sicurezza del dato) è dovuto a errori del personale – conferma Caccia – e per questo dopo il collaudo consegniamo un manuale d'uso e manutenzione molto ricco e dettagliato che contiene le specifiche per tutte le manovre sugli impianti, tanto in situazioni di allerta quanto nella normale amministrazione. Per evitare che lo spegnimento di alcuni interruttori di impianti elettrici secondo una sequenza non corretta provochi un fail del sistema nel complesso».

Tra le questioni da sciogliere resta quella dell'efficienza energetica (misurata in Pue, Power Usage Effectiveness), nonostante le condizioni di efficientamento interne ai colocator abbassino i consumi. In questo caso tecnologia e design possono collaborare a tendere verso l'obiettivo di un Pue pari a 1 (l'energia assorbita dall'impianto è utilizzata per gli apparati It senza ulteriore consumo per raffreddamento e distribuzione di energia alle apparecchiature). Anche solo separando corridoi caldi e freddi per ottimizzare i flussi.

La localizzazione in Italia

- 75 colocator / 29 città
- 24 a Milano / 7 a Roma / 4 torino

Il rating sull'infrastruttura

TIA-942-A

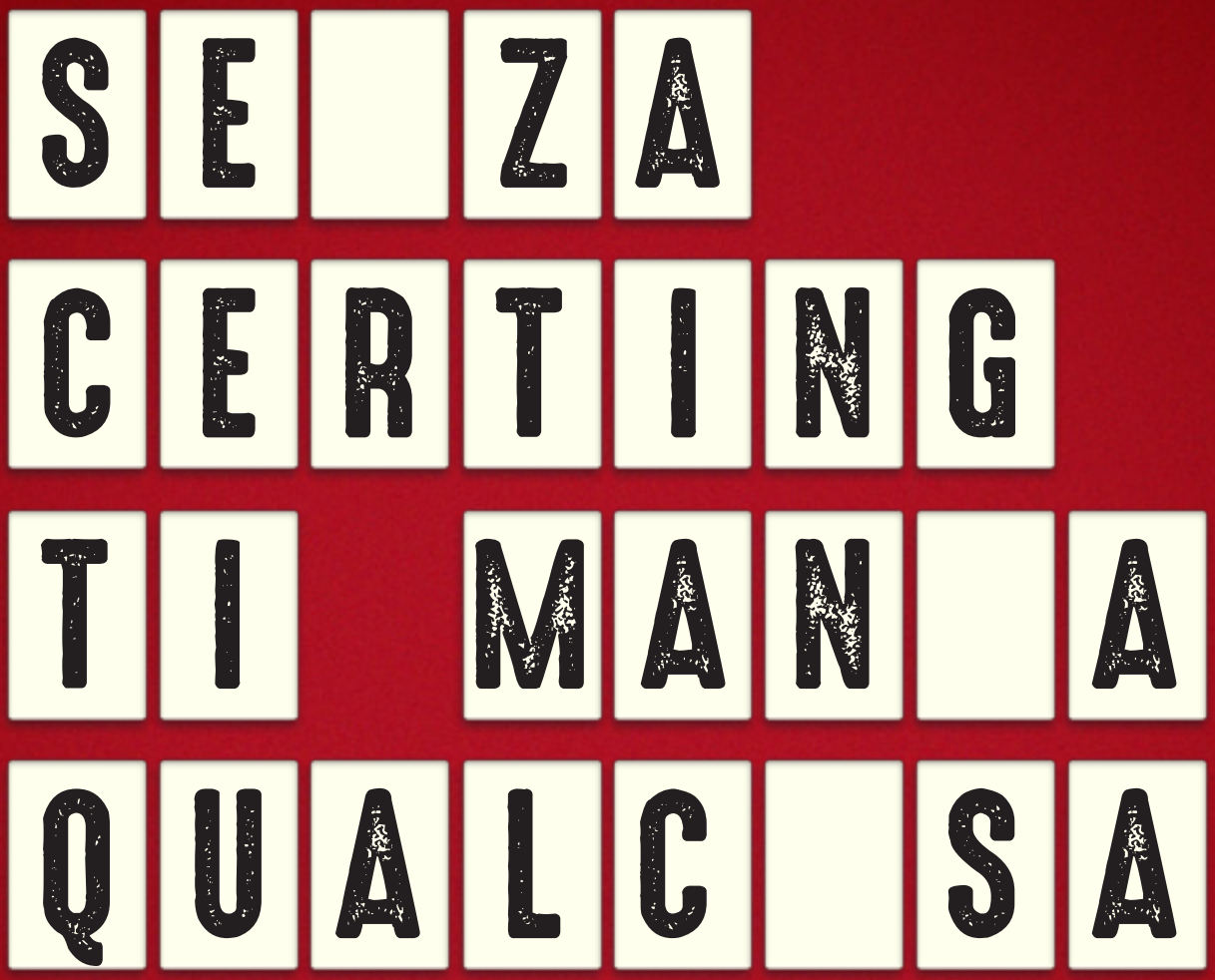
È lo standard di riferimento per i data center della pubblica amministrazione. Stabilisce le norme per la progettazione dei data center e specifica i requisiti in materia di architettura di rete, progettazione elettrica, ridondanza dei sistemi, controllo dei rischi, controllo ambientale, risparmio energetico e molto altro.

Il rating è determinato in base alla disponibilità attesa del dato (dalla ridondanza alla localizzazione) e si compone di quattro livelli incrementali rispetto alla resilienza del sito.

TIER di Uptime Institute

Precedente rispetto al TIA, il Tier è più orientato al mercato e focalizzato sui sistemi. Oltre al rating convenzionale su una scala a quattro livelli (da I a IV), ha una ulteriore griglia supplementare di tre livelli (Gold, Silver, Bronze) per valorizzare le pratiche operative e di sostenibilità del data center oltre alle iniziali norme di progettazione.

freedot



cni-certing.it

LA CERTIFICAZIONE PROFESSIONALE PER INGEGNERI NELL'ICT.

Il tassello che mancava per il tuo lavoro è qui. CERTing è la certificazione che racconta tutto della tua carriera professionale: i progetti, le capacità, le tue reali esperienze. L'agenzia CERTing è un ente di certificazione accreditato ISO 17024: un marchio autorevole che premia la tua professionalità, ti inserisce nel grande data base degli ingegneri certificati e ti rende più credibile, visibile e competitivo sul mercato del lavoro.

CERT'ing
AGENZIA NAZIONALE
CERTIFICAZIONE
COMPETENZE INGEGNERI

X-PAD
ULTIMATE

X-PAD Ultimate

Tutto in un unico software

X-PAD Ultimate è un software modulare, facile da usare per lavori topografici e del cantiere, come rilievi, tracciamenti, catasto, controlli BIM, strade, mappe, batimetria e GIS.

Il software è disponibile sulla piattaforma Android e porta le migliori tecnologie direttamente in campo nella tua mano: una completa visualizzazione 3D ed un sistema CAD per visualizzare e modificare i disegni, integrazione dei tuoi dati con tutte le tipologie di mappe, supporti per la realtà aumentata e molto altro. XPad Ultimate ti assicura la produttività e ti permette di avere una perfetta integrazione con tutti gli strumenti.

Disponibile in due versioni, una dedicata a chi lavora nel campo della topografia ed una dedicata alle imprese di costruzioni, offrendo ad entrambi delle caratteristiche dedicate.

Part of HEXAGON

geomax-positioning.it

Per trovare un distributore nella vostra zona, visitate il nostro sito web: geomax-positioning.it

gli autori di questo numero

Angelo Tofalo

Sottosegretario di Stato alla Difesa con delega Cyber. È stato componente del COPASIR, il Comitato Parlamentare per la Sicurezza della Repubblica. Laureato in ingegneria civile presso l'Università degli Studi di Salerno, da ingegnere ha lavorato per circa cinque anni nell'ambito della progettazione di opere strategiche per la sicurezza, principalmente telecomunicazioni e videosorveglianza.

Luciano Floridi

Filosofo italiano naturalizzato britannico, è professore ordinario di filosofia ed etica dell'informazione all'Università di Oxford, presso l'Oxford Internet Institute, dove dirige il Digital Ethics Lab. È stato UNESCO Chair of Information and Computer Ethics. Floridi è principalmente conosciuto per il suo lavoro in due aree di ricerca filosofica: la filosofia dell'informazione e l'etica informatica.

Michele Colajanni

Professore ordinario presso il Dipartimento di Ingegneria "Enzo Ferrari" dell'Università di Modena e Reggio Emilia. È fondatore e direttore del CyberLab istituito tra l'UniMoRE e la Tel Aviv University con il patrocinio del Ministero degli Affari Esteri e della Cooperazione Internazionale, e responsabile dei Master universitari in "Cyber Defense" e in "Digital Forensics" per lo Stato Maggiore della Difesa presso la Scuola delle Telecomunicazioni di Chiavari.

Simone Crolla

Consigliere Delegato della American Chamber of Commerce in Italy ("AmCham") dal 2009. Fondata nel 1915, AmCham è un'organizzazione non a scopo di lucro, che ha l'obiettivo di facilitare lo sviluppo di relazioni economiche e politiche tra gli Stati Uniti e l'Italia. Dal novembre 2018, guida l'Advisory Board in Italia della Veneranda Fabbrica del Duomo di Milano. È stato tra i fondatori del Padiglione USA a Expo 2015 per il quale ha ricoperto il ruolo di Director of Italian Relationships.

Davide Lamanna

Ingegnere in Telecomunicazioni, con dottorato di ricerca in Ingegneria Informatica, è esperto di architetture cloud e infrastrutture IT basate su OpenStack, Docker, Kubernetes e Ansible. Attivo fin dal 2001 nella progettazione e realizzazione di cluster, sistemi distribuiti e virtualizzazione, vanta esperienze di alto profilo in ambito Cyber Security come formatore tecnico, consulente e PM in contesti internazionali, con un'esperienza di più di 2 anni a Londra. Attualmente è CTO di Binario Etico e consulente della Pubblica Amministrazione.

Gianluca Di Fusco

Dottore magistrale in Marketing & Management Internazionale è specializzato nel settore privacy come Data Protection Specialist, area governance e procedure. Nella recente esperienza ha lavorato come stageur nel settore bancario sui temi inerenti alla data protection. Tra il 2015 e il 2016 ha maturato esperienza nel settore commerciale come intermediario assicurativo impegnato nella gestione di portafogli clienti. Attualmente collabora con la società Hermes Bay come consulente negli ambiti cyber governance e privacy.

Luisa Franchina

Ingegnere elettronico con dottorato e post dottorato di ricerca in ingegneria elettronica (Università di Roma la Sapienza) e master in geopolitica (IASD) del Centro Alti Studi Difesa. Ha conseguito la qualifica militare CBRN presso la Scuola Militare di Rieti. È stata ricercatrice in università estere, Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013), Direttore Generale del Nucleo Operativo per gli attentati nucleari, biologici, chimici e radiologici (Dipartimento della Protezione Civile, PCM, 2006-2010) e Direttore Generale dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Ministero delle Comunicazioni 2003-2006). Saggista e docente in temi di sicurezza presso master specialistici in diverse università, ha fondato un'azienda che eroga servizi di gestione del rischio e gestione dell'informazione e reporting.

gli autori di questo numero

Agostino G. Bruzzone

Professore ordinario presso l'Università di Genova. È presidente del Simulation Team, chair del corso di Laurea magistrale in Engineering technology for Strategy&Security e direttore del Master internazionale in Impiantistica MIPET presso l'Università di Genova. Membro del CdA della Society for Modeling and Simulation International, ha ricoperto il ruolo di Responsabile M & S presso il centro NATO STO CMRE. È stato allievo dell'Accademia Navale di Livorno.

Fabio Lazzini

Responsabile della Funzione Security Governance & Data Protection di Sogei, il partner tecnologico del Ministero dell'Economia e delle Finanze. È laureato in Ingegneria delle Telecomunicazioni all'Università degli studi di Pisa, con un Master CEFRIEL in Tecnologia dell'Informazione al Politecnico di Milano.

Giovanni Lagorio

Ricercatore in Informatica presso il DIBRIS dell'Università degli Studi di Genova, dove tiene corsi su sistemi operativi, crittografia, analisi di programmi binari e sviluppo di codice sicuro. Appassionato di sicurezza informatica ed ethical hacking, nel 2017, assieme ad alcuni colleghi, ha fondato la squadra CTF ZenHack, di cui è tuttora membro. Dal 2019 fa parte dello steering committee per l'European Cyber Security Challenge (ECSC).

Marina Ribaudo

Professore associato di Informatica presso il DIBRIS dell'Università degli Studi di Genova, dove tiene corsi sullo sviluppo delle applicazioni web e sull'analisi di reti/grafi di grandi dimensioni. I suoi interessi di ricerca si focalizzano sullo studio/sviluppo di applicazioni e servizi innovativi (Web, IoT, basati su blockchain). Dal 2018, grazie al progetto CyberChallenge.IT, ha cominciato ad interessarsi al tema dell'ethical hacking.

Emilio Coppa

Assegnista di ricerca presso il Dipartimento di Ingegneria Informatica, Automatica e Gestionale della Sapienza Università di Roma. Ha ricevuto un dottorato in Informatica nel 2015 e i suoi interessi di ricerca si focalizzano su tecniche di analisi statica e dinamica del software. Dal 2017 fa parte del comitato organizzativo di CyberChallenge.IT ed è uno dei responsabili della squadra nazionale per l'European Cyber Security Challenge (ECSC).

Alessandro Mollo

Dal 2009 svolge attività di consulenza tecnica in sicurezza informatica per importanti realtà della pubblica amministrazione. Lavora come Analista di Sicurezza Cibernetica e ricopre il ruolo di coordinatore delle attività del CERT-PA (Computer Emergency Response Team PA) presso AgID.

Biagio Tagliaferro

Ha conseguito la Laurea Magistrale in Ingegneria Informatica, è membro della Commissione di Sicurezza Informatica dell'Ordine degli Ingegneri di Roma. Lavora come Analista di Sicurezza Cibernetica presso il CERT-PA (Computer Emergency Response Team PA) all'interno di AgID.

Paola Rocco

Laureata in Ingegneria Informatica presso l'ateneo Federico II di Napoli, svolge attività di consulenza nell'ambito della sicurezza delle informazioni e della privacy. Lead Auditor ISO 27001, ISO 22301, DPO UNI 11697, Valutatore Privacy 11697, R.S.P.P. Dal 2013 è Presidente della Commissione Sicurezza Informatica presso l'Ordine degli Ingegneri della provincia di Roma, dove ha tenuto interventi tecnici in numerosi seminari e corsi. Ha partecipato a conferenze internazionali e pubblicato diversi articoli sul tema della sicurezza informatica ed è docente nel Master "Competenze digitali per la protezione dei dati, la Cyber Security e la privacy" di Tor Vergata.


SOFT.LAB
SOFTWARE PER L'EDILIZIA
Da più di 30 anni,
gli esperti del
calcolo strutturale
in Italia
Scopri il nuovo sito web:
www.soft.lab.it
Ti aspettiamo al SAIE
Bari | 24 – 26 Ottobre 2019
SAIE
BARI 24-26 Ottobre 2019
0824 87 43 92

2 2019 #376 € 10.00

ISSN 0020-0913

CONSIGLIO NAZIONALE
DEGLI INGEGNERI

L'Ingegnere Italiano
2 2019

n. 376 dal 1966 - n. 2 della nuova versione quadrimestrale
a cura del Consiglio Nazionale degli Ingegneri
Registrazione del Tribunale di Roma
n. 46/2011 del 17 febbraio 2011

Editore
Consiglio Nazionale degli Ingegneri
via XX Settembre 5, 00187 Roma

Poste Italiane SpA
Spedizione in abbonamento postale - 70%
Aut. GIPA/C/RM/16/2013