AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2019	N. 2/ 2019	FEBBRAIO 2019

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

La Resilienza delle Città Intelligenti

Dopo la locuzione "città intelligente" oggi è diventato di uso comune nel linguaggio della politica la locuzione "città resiliente". Ma cosa si intende con queste due locuzioni e come si conciliano tra loro? Rifacendosi all'Agenda 2030 delle Nazioni Unite, l'obiettivo che meglio sposa questi due concetti sembra essere l'Obiettivo 11, "Città e Comunità Sostenibili".
"Viviamo in un mondo sempre più urbanizzato: il 54% della popolazione globale risiede in città e questa cifra aumenterà, secondo le previsioni, fino al 68% entro il 2050, mentre la Quarta Rivoluzione Industriale sta cambiando il modo in cui le città forniscono servizi ai residenti." Esordisce così il documento "*Agile cities: preparing for the fourth industrial revolution*"[1], del Global Future Council on Cities and Urbanization, promosso dal World Economic Forum, tracciando la cornice entro la quale, continua, "le città, come motori di crescita globali, devono essere agili – capaci di muoversi velocemente e facilmente – permettendo ai loro cittadini di prosperare".
Questo rapporto, che studia come le città possono usare i dati nei settori riguardanti persone, economia, *governance*, infrastrutture e ambiente, evidenzia l'importanza dell'agilità dei centri urbani, nel connubio tra "il mondo biologico, fisico e digitale" attraverso innovazioni come intelligenza artificiale (AI), l' *Internet of things* (IoT) e il 5G. Una città agile, spiega il Rapporto, include edifici multi-funzionali, *policy* di variazione d'uso efficienti, sistemi di trasporto ottimizzati con un sistema di informazione in tempo reale e una rete energetica che massimizza l'utilizzo delle energie rinnovabili, tra le altre caratteristiche.

Il tema dell'agilità delle città è declinato in otto aree specifiche: negli edifici, nel terreno, nella mobilità, nella tecnologia dell'informazione (IT), sicurezza, educazione e settori di amministrazione. Per ogni area è proposto un caso di studio di città esempio, nella quale sono state compiute azioni concrete che attraverso strumenti innovativi hanno trovato soluzioni al passo con il cambiamento richiesto. L'analisi di ogni caso è ulteriormente suddivisa e analizzata su tre livelli:

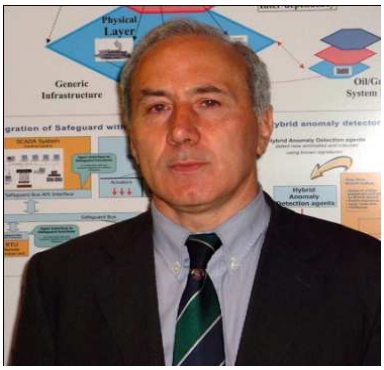
- **Componenti fisici** – le infrastrutture possono adattarsi ai nuovi bisogni ed usi senza abbondare con investimenti, processi a lungo termine o inconvenienti ai cittadini.
- **Componenti digitali** – le nuove tecnologie possono essere utilizzate in maniera migliore per comprendere le tendenze e i bisogni dei cittadini così come fornire opinioni sulle attuali infrastrutture e servizi urbani e ottimizzarne i benefici.
- **Fattori ambientali** – come gli effetti dell'ambiente sulle attività urbane possono mitigare attraverso applicazioni innovative sia nella sfera fisica che digitale.

Queste considerazioni dovrebbero dare un'idea delle difficoltà di far sposare i due concetti di "città intelligente" e "città resiliente": gli edifici servono a diverse funzioni, la resilienza fa leva su strategie

[1] http://www3.weforum.org/docs/WP_Global_Future_Council_Cities_Urbanization_report_2018.pdf

di prevenzione basate sull'utilizzo dei dati, i sistemi di trasporto interoperabili sono ottimizzati grazie ad un sistema di informazione in tempo reale, la rete energetica è organizzata per isole per essere più resiliente, il sistema educativo si adatta velocemente alle richieste di formazione per riflettere i bisogni di un'economia in rapido cambiamento.
Tutto ciò rende il tema delle "città intelligenti e resilienti" estremamente difficile da affrontare, considerato l'alto numero di attori in gioco, sia pubblici che privati, responsabili delle singole infrastrutture che stanno alla base dei servizi offerti al cittadino.
AIIC sta affrontando questo tema con un Gruppo di Lavoro ad hoc, forte della sua esperienza e delle precedenti pubblicazioni sulla definizione di metodologie per la valutazione della resilienza delle singole Infrastrutture, della Comunità, e dell'utilizzo delle tecniche di "*big data analytics & data science*" per l'utilizzo della mole di dati provenienti dal campo. Il tutto, applicando tecniche di "*data security*", "*data protection", "privacy*", in linea con le normative vigenti.

Sandro Bologna



Laureato in fisica alla Sapienza, Università di Roma, è membro del Consiglio Direttivo dell'AIIC. Tra le principali attività di ricerca attuali si citano la valutazione della sicurezza, protezione e resilienza di infrastrutture critiche, con particolare riferimento agli aspetti di analisi delle vulnerabilità alle minacce di origine naturale e umana e alla modellistica dei diversi fattori che concorrono a costituire una infrastruttura.

ATTIVITA' DELL'ASSOCIAZIONE

LE CARICHE SOCIALI DEL CONSIGLIO DIRETTIVO 2018-2021

Il Consiglio Direttivo di AIIC ha eletto le seguenti cariche sociali:

Presidente: ***Luisa Franchina***
Vicepresidente: ***Alberto Traballesi***
Vicepresidente: ***Silvano Bari***
Tesoriere: ***Glauco Bertocchi***
Segretario: ***Bruno Carbone***

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Rinnovo associativo per l'anno 2019

Si ricorda a tutti i soci che il 31 dicembre 2018 è scaduto il periodo associativo. Invitiamo tutti i soci, che non avessero ancora proveduto, a rinnovare l'associazione versando il relativo contributo, ormai inalterato da anni.
La quota per il rinnovo individuale è di euro 40 e può essere versata con bonifico sul c/c presso Banca Prossima, IBAN: IT 61F 03359 01600 100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche indicando "rinnovo socio ordinario nome e cognome anno 2019". Le quote e le modalità di rinnovo per i soci collettivi – così come le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC al link
http://www.infrastrutturecritiche.it/new/per-iscriversi/

Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2019. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione, versando in più il relativo contributo per le spese di segreteria.

Nuova sede AIIC

Si prega di voler gentilmente prendere visione nell'intestazione o alla fine della Newsletter delle coordinate della nuova sede dell'Associazione.

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

Primo Colloquia AIIC del 2019 su "La rete 5G: criticità e prospettive",
il prossimo 14 marzo a Roma Tre, via Vito Volterra 62, dalle 14 alle ore 18.

Ci siamo quasi, il 2020 è la data prevista per il debutto ufficiale del 5G, cioè il nuovo standard di comunicazione mobile di quinta generazione, che permetterà di collegare miliardi di dispositivi in tutto il mondo in contemporanea, ad alta velocità e con tempi di risposta ridottissimi.
Con il 5G, sarà possibile non solo navigare su internet velocemente da smartphone e tablet, ma anche e soprattutto creare una rete velocissima in cui ogni singolo dispositivo potrà essere connesso in tempo reale: di questo ne beneficeranno progetti come – tanto per citarne solo alcuni - le auto a guida autonoma, che potranno dialogare in tempo reale con le infrastrutture stradali le quali, dal canto loro, potranno garantire una migliore gestione del traffico, consigliando percorsi alternativi in base al traffico; le Smart City in cui si potranno gestire simultaneamente tutti i servizi e dispositivi della città; le Smart Home, in cui tutti gli oggetti "smart" della casa potranno essere gestiti da remoto da un unico dispositivo, ed anche dialogare tra di loro.

D'altro canto, se da un lato il 5G potrà portare grandi benefici, è necessario valutare anche i problemi che potrebbero presentarsi, primi fra tutti, la privacy e la vulnerabilità della rete.
La invasività della rete 5G, il fatto di poter collegare praticamente ogni oggetto, potrebbe mettere a rischio la privacy dell'utente, dando la possibilità di accedere nascostamente a dati del singolo cittadino da parte di aziende o di estranei, mentre sarà importante assicurare la protezione della stessa rete da attacchi, per cui ogni dispositivo connesso potrebbe essere potenzialmente acceduto per compiere attività illecite.
Tutte queste problematiche saranno affrontate nel primo Colloquia del 2019, dal titolo "La rete 5G: criticità e prospettive", che si svolgerà il giorno giovedì 14 marzo p.v. presso la sala conferenze del Dipartimento di Ingegneria dell'Università Roma Tre, via Vito Volterra 62, dalle 14 alle ore 18.
Il Colloquia verrà organizzato congiuntamente dall'Università Roma Tre, da AIIC - Associazione Italiana esperti in Infrastrutture Critiche e da IsacaRoma, il Capitolo di Roma di ISACA (Information Systems Audit and Control Association).
L'evento sarà aperto a tutti, e per gli iscritti AIIC è previsto un attestato di frequenza, mentre per i soci Isaca la partecipazione darà diritto ai crediti CPE.
Il programma, che prevede l'intervento di eccelsi relatori del settore, è in corso di definizione e verrà comunicato a breve – come di consuetudine – a soci e simpatizzanti.
Ci auguriamo di vedervi, come al solito, numerosi!

Silvano Bari, vicepresidente AIIC

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi ed autonomi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe

le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.

- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

Mindset of Good Practices and Recommendations for Smart City Resilience Engineering and Evaluation

AIIC ha avviato un gruppo di studio su questo argomento, partendo dalla considerazione che le **Smart Cities** sono alimentate da reti. Dispositivi, persone, aziende e governi devono essere in grado di connettersi in modo sicuro, affidabile e rapido per condividere dati per migliorare il modo in cui le persone vivono, lavorano e gestiscono le loro attività quotidiane. Conseguentemente, come per qualsiasi ecosistema interconnesso, ci sono sfide alla sicurezza ed al rispetto della privacy.

L'agenda dello studio, che è svolto in lingua inglese ed è prossimo alla conclusione, prevede queste sezioni, di cui i soci indicati tra parentesi sono i coordinatori:

1. Introduction *(Sandro Bologna)*
2. How to model a Smart City as a complex System-of-Systems (*Sandro Bologna*)
3. How to take advantage of the previous Guidelines produced by AIIC to secure a Community Resilience (*Sandro Bologna*)
4. How to take advantage of real-time urban data by exploiting IoT, Big Data Analytics and Artificial Intelligence *(Priscilla Inzerilli, Luisa Franchina*)
5. How to combine the Smart City and the historic centre: suggestions from a case study *(Donato Di Ludovico, Donatella Dominici)*
6. How to limit the consequence of cyber-attacks on a Smart City Infrastructure, with particular emphasis to data security (*Alberto Traballesi,Glauco Bertocchi*)
7. How to take advantage of readily available tools and modeling techniques developed in different projects (*Glauco Bertocchi, Alberto Traballesi*)
8. How to monitor and control where and when vendors come in, monitor contractors while they are there, and turn it all off when they are gone (*Luigi Carrozzi*)
9. How to deal with data protection and the ethic challenge introduced by the use of Artificial Intelligence (*Luigi Carrozzi*)

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

E-mail da parte di eventuali interessati a contribuire saranno benvenute (segreteria@infrastrutturecritiche.it)

NEWS E AVVENIMENTI

Gli hacker sfidano la sicurezza dei dispositivi IoT – Ritardi negli aggiornamenti, alto numero di dispositivi IoT collegati a Internet vulnerabili anche alle minacce meno recenti e l'idea che i dispositivi IoT una volta accesi possano essere abbandonati sono alla base della possibilità per gli hacker di disporre velocemente di botnet. La semplicità nell'aggiornamento del codice sorgente dei botnet come il Mirai per sfruttare le vulnerabilità incide notevolmente in questo senso e la capacità di creare botnet di grandi dimensioni in tempi brevissimi e con risorse minime resta alla base della tendenza alla crescita mostrata dai botnet IoT.
La sicurezza dei dispositivi **IoT**, oggi, è decisamente ancora in fase embrionale, e non è inconsueto che si presentino vulnerabilità basilari quali il *command injection*. Per esempio, a novembre 2018 honeypot[2] ha registrato lo sfruttamento di numerose vulnerabilità IoT obsolete quale strumento di diffusione di malware.
Dai dati raccolti emerge quindi che i nuovi dispositivi IoT subiscono in meno di un giorno il tentativo di fare leva sulle vulnerabilità note e sono soggetti in meno di 5 minuti a tentativi di accesso con forza bruta mediante le credenziali IoT predefinite (Dipping Into The Honeypot) .
Le vulnerabilità IoT hanno permesso poi agli autori di botnet di incrementare la presenza quantità di dispositivi nei rispettivi botnet. Pensiamo anche solo alle varianti di Mirai che contenevano vulnerabilità specifiche dell'IoT. Nei dati degli honeypot Netscout si evidenziano tempistiche rapidissime tra il momento in cui una vulnerabilità viene resa nota a quello in cui gli autori di botnet la integrano nelle proprie reti botnet.
https://www.silicon.it/security/gli-hacker-tengono-il-passo-con-la-sicurezza-dei-dispositivi-iot-scenari-di-rischio-127875?utm_source=2019-02-05&utm_medium=email&utm_campaign=it_silicon_security_v2&referrer=nl_it_silicon_security_v2&t=e2299fdce9b02e499ce49ccbde1596b32097967&pos=firstMostSharedArticle_1_chevronRight
Silicon *– Mario De Ascentiis – 22 gennaio 2019*

Sistemi industriali: quando l'attacco è wireless - Quando si parla delle potenziali **vulnerabilità dei sistemi di controllo industriale** (ICS) si pensa ai pericoli che vengono dall'integrazione tra i mondi IT e OT. Ma non è necessario andare così lontano per immaginare nuovi scenari di attacco ad alcuni tipi di impianti. Una ricerca **Trend Micro** si è concentrata sulle unità di telecontrollo wireless a radiofrequenza, o remote controller. I **remote controller industriali** sono in sintesi telecomandi "rugged" che permettono di controllare da remoto il funzionamento di macchinari di vario genere e anche di grandi dimensioni, dalle scavatrici negli impianti minerari alle gru nei cantieri edili. Sono composti da **due unità separate**: un trasmettitore, che viene usato da un operatore umano, e un ricevitore, collegato ai comandi del macchinario.
Il funzionamento dei remote controller industriali è semplice. L'operatore esegue un comando sulla unità trasmittente, di norma premendo uno o più pulsanti. Questa combinazione di comandi **corrisponde a una sequenza di impulsi in radiofrequenza**, che vengono trasmessi all'unità ricevente. Quest'ultima decodifica gli impulsi ricevuti ed esegue i comandi richiesti per il macchinario.

[2] **honeypot** (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici (Wikipedia)

La semplicità del funzionamento permette, secondo lo studio Trend Micro, vari tipi di attacchi. In sintesi, i ricercatori Trend Micro hanno verificato che non è difficile per un ipotetico criminale approfondire il funzionamento di un particolare modello di controller wireless, in particolare **identificare in dettaglio la codifica dei comandi** in segnali radio. Complice il fatto che nessun controller adotta forme particolari di protezione delle trasmissioni wireless, come ad esempio la cifratura, è possibile intercettare quelle di un controller e portare **vari tipi di attacchi.** Trend Micro ne ha identificati quattro.
https://www.impresacity.it/news/21114/sistemi-industriali-quando-l-attacco-e-wireless.html
Impresacity *– Redazione – 30 gennaio 2019*

Blockchain, Poste Italiane entra nel consorzio Hyperledger - In futuro la corrispondenza di **Poste Italiane potrà viaggiare sulla blockchain**. La società, prima nel nostro Paese, è entrata a far parte del consorzio Hyperledger, entità amministrata dalla Linux Foundation che riunisce oltre 260 organizzazioni coinvolte a vario titolo nello sviluppo di standard tecnologici aperti e condivisi per i **registri distribuiti**. *"L'adesione è coerente con le linee strategiche individuate dal Piano industriale Deliver 2022, che mira a rafforzare la leadership digitale di Poste Italiane"*, ha spiegato l'azienda in una nota. L'ingresso nel consorzio *"accelera il percorso di acquisizione di nuove competenze e di sperimentazione della tecnologia blockchain e delle Dlt* (distributed ledger technologies, *ndr*) *per meglio comprenderne potenzialità capaci di generare innovazione nel business"*.
Secondo Poste, la catena di blocchi è destinata a *"cambiare il modello di conservazione e condivisione delle informazioni, con il ribaltamento del paradigma secondo il quale al controllo fisico centralizzato dei dati corrisponde una sicurezza maggiore"*, assolutamente centrale nell'**era digitale**. *"In questo contesto la blockchain si candida a costituire una risposta efficace ai problemi di sicurezza, trasparenza, interoperabilità e privacy"*.
http://www.ictbusiness.it/cont/news/blockchain-poste-italiane-entra-nel-consorzio-hyperledger/42433/1.html#.XGG50RvsZPY
IctBusiness.it *– Redazione – 31 gennaio 2019*

Cyber security nazionale, tutti i dossier aperti in Italia - Nel 2018 sono state gettate le basi normative per molti sviluppi attuativi che contribuiranno a consolidare lo scenario di innalzamento sistemico delle capacità di protezione, reazione e risposta nei confronti dei rischi e delle minacce cibernetiche non solo del nostro Paese ma dell'intera Unione europea. Sono ben tre gli ambiti comunitari strutturalmente interessati dalle varie norme entrate in vigore o comunque perfezionate nel corso del 2018:

- la protezione dei dati personali e dei diritti digitali dei cittadini, grazie al Regolamento generale noto come GDPR;
- la protezione dei servizi e delle infrastrutture tecnologiche cruciali per il buon funzionamento della società, grazie alla cosiddetta Direttiva NIS;
- la protezione dei dispositivi e degli apparecchi informatici e telematici di uso civile e domestico, grazie al nuovo quadro europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali istituito dal cosiddetto *Cybersecurity Act*.

A questo già nutrito pacchetto si è aggiunta altresì, ma solamente per il nostro Paese, la piena entrata in vigore degli specifici obblighi per l'innalzamento della sicurezza informatica della Pubblica Amministrazione.
A coronamento di tutto questo complesso di norme e di iniziative vale la pena di ricordare che nel 2018 l'Europa, sempre mediante il Cybersecurity Act, ha finalmente deciso di dotarsi di una vera e propria Agenzia per la cybersecurity rafforzando il mandato, nonché ampliando il ruolo e i compiti, di

ENISA, la precedente Agenzia per la sicurezza delle reti e dell'informazione. Questa dovrà ora trasformarsi in una struttura operativa e supportare l'Unione e le altre Agenzie (quali ad esempio Europol ed Eurojust) in tutte le iniziative anche operative di innalzamento della sicurezza cibernetica comune.
Il nostro Paese è riuscito a rispettare la fatidica scadenza per la maggior parte degli adempimenti, in particolare per quanto riguarda l'identificazione (con relativa notifica a Bruxelles) delle strutture cui sono affidati gli incarichi di:

- Punto unico di contatto (assegnato al DIS);
- Autorità competenti NIS (assegnati ad alcuni Ministeri chiave);
- CSIRT Italiano (assegnato alla struttura risultante dalla fusione dei precedenti CERT Nazionale e CERT della Pubblica Amministrazione).

Anche per il comparto della Difesa il 2018 è stato un anno importante. Il Comando Interforze per le Operazioni Cibernetiche (CIOC) ha infatti raggiunto la Initial Operational Capability (IOC) dotandosi di personale specializzato e risorse adeguate e partecipando sistematicamente ai competenti tavoli della sicurezza nazionale.
Secondo i piani, il CIOC raggiungerà la Full Operational Capability (FOC) nel corso del 2019, e quindi sarà in grado di operare a pieno regime per assicurare la protezione delle strutture e delle operazioni della Difesa in Italia e all'estero come da mandato ricevuto.
Il 2019 sarà l'anno del consolidamento: con il GDPR oramai a regime, sarà ora la volta degli operatori interessati dalla normativa NIS. Sempre nel corso del 2019 andranno a regime sia lo CSIRT Italiano che il CIOC, due importanti tasselli operativi dell'Architettura nazionale per la protezione dello spazio cibernetico. Vedrà infine la luce il primo schema comune europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali, la cui attuazione nazionale è stata affidata all'Istituto Superiore delle Comunicazioni (ISCOM) del Ministero dello Sviluppo Economico.
https://www.agendadigitale.eu/sicurezza/cyber-security-nazionale-tutti-i-dossier-aperti-in-italia/
Agenda Digitale *– Corrado Giustozzi – 4 gennaio 2019*

NIST: Blockchain Provides Security, Traceability for Smart Manufacturing – Engineers at the *National Institute of Standards and Technology (NIST)* needed a way to secure smart manufacturing systems using the digital thread , so they turned to the new kid on the block … blockchain, that is.
According to a new NIST report, the security system better known for underpinning Bitcoin and other digital currencies not only provides tamper-proof transmission of manufacturing data, it also yields something just as valuable to its users—traceability of that data to all participants in the production process.
"Because blockchain gives us both capabilities, we can build trustworthiness into digital manufacturing networks," said NIST mechanical engineer Thomas Hedberg, one of the authors of the report.
Blockchain, first used for Bitcoin a decade ago, is an expandable list of records, or blocks, that each contain data representing an individual transaction by members of a network. Each block consists of the data set, a time stamp, a cryptographic hash (an algorithm serving as a "cybersecurity fingerprint") and the hash of the previous block to mathematically link the two together. Therefore, each block in the chain is connected to the one after, the one before and all the way back to the original transaction (known as the genesis block). This means that the information contained in any block cannot be altered without changing all subsequent blocks and alerting the record-keepers in the network that f- oul play has occurred.
https://www.nist.gov/news-events/news/2019/02/nist-blockchain-provides-security-traceability-smart-manufacturing

NIST *- S. Krima, T. Hedberg and A.B. Feeney – february 2019*

5G e smart grid, come cambierà il settore dell'energia - Il 5G, insieme agli smart meter, sarà uno dei principali fattori abilitanti della "smartificazione" delle reti energetiche e permetterà una connessione stabile e ultra rapida tra tutte le componenti del sistema. Cosa cambierà in termini di vantaggi per i consumatori, andamento dei prezzi, esigenze strutturali della rete.
Le nuove tecnologie, pur arrivate in ritardo nel settore dell'energia, sembrano avere un ruolo determinante nell'esplosione di fenomeni quali la decentralizzazione, la disintermediazione e la maggior integrazione del sistema.
Le reti 5G sono in grado di coprire in maniera contemporanea tutti i tipi di comunicazione, inclusi quelli di tipo macchina, aprendo importanti scenari nel passaggio verso le smart grid.
Indice degli argomenti:
5G ed energia, cosa cambierà
La gestione delle reti in tempo reale
Efficienza e risparmio energetico
Una stima dei benefici
Smart meter e riduzione dei consumi
https://www.agendadigitale.eu/infrastrutture/5g-e-smart-grid-come-cambiera-il-settore-dellenergia/
Agenda Digitale - *Lorenzo Principali e Domenico Salerno, 12 febbraio 2019*

PROSSIMI EVENTI

Building a smarter organization with Analytics & AI – Un efficiente **ecosistema analitico** è la premessa per sviluppare, distribuire, orchestrare e governare progetti di **AI**. In generale si tratta di applicazioni e servizi che necessitano di maggiore agilità rispetto ai tradizionali processi aziendali, ma, in ogni caso, è indispensabile un governo e una gestione controllata dei modelli/algoritmi analitici sviluppati. L'ideale è trovare dinamicamente il giusto bilanciamento fra capacità di essere agili e veloci e la necessità di governo e controllo, il tutto nella complessità degli attuali **sistemi IT** e nella **varietà di fonti dati disponibili alle aziende**.
Il roadshow **"Building a smarter organization with Analytics & AI"** intende mostrare casi virtuosi di collaborazione tra **IT** e **business** proponendo e mostrando le diverse fasi dell'ecosistema analitico necessarie per passare dalla sperimentazione all'azione in **ambito AI** nel mondo del **DevOps**.
Milano - Centro Congressi - Excelsior Hotel Gallia Piazza Duca d'Aosta 9 (20124) Milano – 13 marzo 2019
Roma - Roma Eventi Piazza di Spagna Via Alibert 5A (00187) –21 marzo 2019
https://www.sas.com/it_it/events/19/analytics-roadshow.html

IOTHINGS 2019 – Milano - **IOTHINGS** è un evento italiano molto importante nell'ambito delle tecnologie IoT, si svolge annualmente in 2 edizioni: in primavera a Milano e in autunno a Roma. Durante **IOTHINGS Milano 2019** si svolgeranno nella medesima location le nuove edizioni di **ITALIA5G, AI+BOTS World e BLOCKCHAIN Now**. Tre eventi riuniti per creare un esclusivo punto di aggiornamento sulle tecnologie più "disruptive" e per favorire lo sviluppo dell'ecosistema IoT. **IOTHINGS** Milano si svolgerà nel nuovo **MIND – MILANO INNOVATION DISTRICT**, realizzato nell'area che ha ospitato Expo 2015 e che si sta trasformando in un parco scientifico e tecnologico di eccellenza

MIND - Via Cristina Belgioioso, 28, 20021 Milano MI – 3 aprile 2019
https://www.impresacity.it/calendario.php?eventi=1408

Conferenza Esri Italia 2019 - Il **10** e **11 aprile** si terrà a Roma, all'Ergife Palace Hotel, la **Conferenza Esri Italia**, l'evento più articolato e completo a livello nazionale nel settore delle soluzioni e delle tecnologie geospaziali. L'edizione 2019 della Conferenza sarà dedicata al tema ***The Science of Where, Envisioning Where Next***.
La **digital transformation** sta cambiando profondamente la nostra società, attraverso continue innovazioni che stanno migliorando il nostro modo di vivere e di relazionarci con la realtà. Durante la Conferenza, sarà possibile scoprire come **The Science of Where** sta ispirando, sostenendo e immaginando tale trasformazione digitale in ambiti strategici per l'economia e la pianificazione del territorio, abilitando nuove forme di collaborazione e opportunità future. Attraverso Keynote Speech di ospiti prestigiosi, eventi speciali, sessioni parallele, workshop tecnologici, iniziative formative e presentazioni di progetti nazionali ed internazionali, scopriremo l'impatto che The Science of Where avrà nello sviluppo della nostra società.
https://www.esriitalia.it/news-ed-eventi/eventi/conferenza-esri-italia/conferenza-esri-italia-2019

Cyber Crime Conference 2019 - L'evento B2B è rivolto ad un pubblico di professionisti ed esperti che avranno occasione di incontrarsi, aggiornarsi e confrontarsi sulle ultime novità in ambito di Cyber Security. Questa decima edizione aprirà con una **Tavola Rotonda** dedicata alla **Blockchain Security**.
La Blockchain è una tecnologia emergente in continua evoluzione progettata per essere sicura e democratica basata su quattro concetti fondamentali: **decentralizzazione, trasparenza, crittografia e immutabilità**. In termini di sicurezza, la Blockchain è considerata una potenziale soluzione per la gestione dei **Big Data**, degli **strumenti finanziari**, della **Supply Chain** e non solo.
Durante la Tavola Rotonda si affronteranno tutti gli aspetti critici della Blockchain.
Verranno inoltre affrontati i temi di maggiore attualità: dal **GDPR** e le sue ricadute in termini di Privacy e Cyber Hygiene ai nuovi, complessi scenari delineati dal **Cyber Warfare** e dalle **Cyber Weapons**; dalle sfide della **Cyber Defense nella IoT Era** alle tecniche di **Digital e Mobile Forensic,** senza tralasciare le loro innumerevoli implicazioni giuridiche, tecnologiche e finanziarie.
Roma - Auditorium della Tecnica Viale Umberto Tupini 65 – 17 aprile 2019
https://www.ictsecuritymagazine.com/eventi/cyber_crime_conference_2019/presentazione

GDPR Day 2019 - Appuntamento il 5 marzo a Milano con GDPR Day 2019. Unico incontro nazionale, fortemente voluto dalla Community, per rispondere alla continua richiesta di formazione di qualità e approfondimenti sul GDPR. Partecipando al GDPR Day 2019 sarà possibile incontrare ed interagire con i maggiori esperti italiani di GDPR, Privacy e Security, che interverranno per spiegare la normativa europea e l'adeguamento nazionale, e soprattutto per chiarire dubbi e lacune dei partecipanti, prevedendo un ampio spazio al confronto e alle domande del pubblico.
Milano - Novotel Ca' Granda Hotel, viale Suzzani 13 – 5 marzo 2019
https://www.impresacity.it/calendario.php?eventi=1411

AWS Summit Milano 2019 – E' tornato l'appuntamento AWS Summit Milano dedicato al Cloud Amazon Web Services. Partecipa per scoprire come il cloud sta accelerando l'innovazione nelle aziende di ogni dimensione e per trasformare tutti i vantaggi del cloud in nuove opportunità per te e per la tua azienda. Durante l'evento avrai la possibilità di confrontarti con gli esperti AWS, il nostro ecosistema di Partner e con persone e aziende che affrontano le tue stesse sfide. Approfondiremo una

vasta gamma di argomenti, nuovi servizi e soluzioni e lo faremo attraverso sessioni dedicate a casi d'uso di clienti, sessioni tecniche e demo della piattaforma AWS.
Milano - MiCo - Centro Congressi – 12 marzo 2019
https://pages.awscloud.com/summit-milan-2019-registration.html

NOTIZIE D'INTERESSE:

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@InfrastruttureCritiche.it

o visitate il sito

www.InfrastruttureCritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria — AIIC c/o NITEL – via Palestro 95 – 00185 ROMA
Tel. +39 06 64871209
Email segreteria@infrastrutturecritiche.it

Gruppo di user all'interno della community — Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente cliccare questo link:
http://www.linkedin.com/ groups/96335

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Versione stampabile della newsletter	Nella sezione "Newsletter" del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*