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. 3/ 2019	MARZO 2019

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

5G: l'esplosione di IoT, IIoT, BIG DATA? Luci e ombre.

La tecnologia di rete 5G viene annunciata come uno dei principali fattori abilitanti di moltissime applicazioni quali la guida autonoma, la telemedicina, i sistemi di sicurezza molto avanzati, le Smart Cities, la realtà aumentata e le nuove applicazioni per intrattenimento.
Possiamo sintetizzarla come una piattaforma di rete trasparente con accesso ultra-broadband (a partire da 1Gbps) fisso e mobile, in grado di abilitare servizi con requisiti eterogenei. Avrà una funzionalità, il Network slicing, con cui ogni operatore di telecomunicazioni potrà fornire dinamicamente servizi di tipo diverso e condividere con altri operatori la stessa infrastruttura di rete fisica. Questa architettura aprirà a una condivisione del 100% dello spettro a disposizione di vari operatori in maniera dinamica.
Le specifiche 5G prevedono 3 tipologie di servizi:

1. *enhanced Multimedia BroadBand*, servizi a alto throughput, (in futuro sino a 10Gbps) per applicazioni video e di realtà aumentata
2. *massive Machine Type Communications*, servizi a bassa energia, per servizi di tipo massive IoT per sensori con batterie a lunga vita (15 anni)
3. *Ultra Reliable Low Latency Communications*, servizi a bassa latenza (sino a 1ms) e alta affidabilità per servizi di tipo IoT mission critical.

La definizione dello standard 5G è prevista solo per la fine del 2019, siamo quindi in dirittura di arrivo per l'avvio della disponibilità al pubblico cui seguiranno probabilmente alcuni anni di progressiva diffusione. Le funzionalità e i servizi di una rete 5G sono realizzabili solo con la realizzazione di software molto complesso, molto veloce, modulare.
Una parte del mondo aspetta questo tipo di rete per poter rendere reali applicazioni e servizi sempre più evoluti.

In sintesi, la rete 5G è definibile come un'autostrada molto complessa e veloce cui si connetteranno oggetti IoT (Internet of Things) e IIoT (Industrial Internet of Things) sempre più numerosi e variati.

IoT è l'insieme degli oggetti, più o meno "intelligenti", (automobili, elettrodomestici, scarpe, interruttori della luce, ecc.) che si collegano a Internet e connettono il mondo fisico a quello digitale generando e ricevendo dati.

IIoT differiscono da IoT per l'ambito di uso. Mentre l'IoT è più comunemente usato da parte dei consumatori, IIoT è usato per scopi industriali come, ad esempio, in ambito di produzione, per il monitoraggio delle forniture e nei sistemi di gestione degli impianti.

IoT e IIoT sono spesso correlati ai Big Dat**a**, ossia alla tipologia di dati strutturati, non strutturati o semi-strutturati generati da sensori e dispositivi digitali che generano grandi quantità di dati. Questa massiccia generazione di dati produce i Big Data.

Dal punto di vista di un utente le aspettative rispetto alla rete 5G sono quelle di maggiori prestazioni e del rispetto dei livelli di servizio ma anche sicurezza dei dati trasmessi e ricevuti, ossia almeno lo stesso livello di sicurezza delle reti attuali.

Anche riguardo agli IoT e IIoT connessi ad una rete 5G le aspettative dell'utenza appaiono sintetizzabili come: garanzia di corretto funzionamento, ridotta vulnerabilità alle minacce, capacità di reazione agli attacchi. Tali attese sono già oggi frequentemente non corrisposte a causa dell'esigenza di contenere costi e di essere velocemente presenti sul mercato che comportano troppo spesso il sacrificio delle caratteristiche di sicurezza.

Apparentemente nulla di nuovo rispetto alle reti attuali, si deve però evidenziare che la rete 5G consente di sviluppare molti più servizi (ad esempio: automotive, medicina robotica a distanza) che possono impattare molto più direttamente con l'incolumità delle persone e quindi i requisiti devono essere più stringenti.

Consideriamo quindi alcune ipotizzabili problematiche di funzionamento e sicurezza provenienti dalla stessa rete 5G:

- Malfunzionamenti (down grading o blocchi) dovuti alla complessità ed alla velocità.
- Vulnerabilità del software di gestione della rete, un software così complesso e distribuito avrà sicuramente dei difetti di progettazione o di realizzazione (vulnerabilità).

Anche l'attuale rete 4G presenta tali minacce ma la nuova rete è molto più complessa e performante. Inoltre, il suo corretto funzionamento è affidato a software molto più complesso, conseguentemente aumenta la probabilità della presenza di vulnerabilità.

Un tipico esempio di minaccia attualmente veicolata dalla rete è il DDoS (Distributed Denial of Service). È un attacco che può essere difficile contrastare, già sperimentato con utilizzo fraudolento di telecamere (IoT), è basato sulla disponibilità di banda trasmissiva.

La rete 5G è un'autostrada veloce nella quale la banda trasmissiva disponibile aumenta di 10-100 volte rispetto ad oggi, gli "oggetti" utilizzabili in rete per attaccare saranno più performanti in termini trasmissivi; gli "oggetti" saranno più numerosi di alcuni ordini di grandezza

Con la rete 5G saranno quindi possibili attacchi di questo tipo di una potenza oggi impensabile

Rispetto alle minacce possibili anche con le reti attuali, la rete 5G introdurrà ulteriori complessità poiché vedrà sicuramente un moltiplicarsi di nuove tipologie di "oggetti" (IoT e IIoT), un enorme aumento del loro numero e delle interconnessioni, aumenterà quindi la superficie d'attacco.

A chi spetta la difesa nella futura realtà 5G?

La difesa dalle vulnerabilità della rete spetta ai costruttori e ai gestori. Attacchi da quella parte sembrano, per ora, oltre la portata del normale crimine informatico ma sono possibili per strutture di possibile origine governativa.

La difesa degli utenti spetta a loro stessi ed appare opportuno che l'uso del 5G da parte di una organizzazione venga preceduto da una approfondita analisi dei rischi, sicuramente dovranno essere sviluppati nuovi strumenti di protezione.

La difesa degli "oggetti" (IoT e IIoT) in rete spetta agli utenti e ai costruttori. È necessario che si accelerino i lavori di definizione di standard di sicurezza per gli "oggetti" da connettere in rete. (come ad esempio ISO 27030 "Information technology -- Security techniques -- Guidelines for security and privacy in Internet of Things (IoT)").

Glauco Bertocchi
Laurea in Fisica all'Università di Roma "La Sapienza". Più di 40 anni di esperienza in Informatica e Sicurezza all'interno di Università e istituzioni nazionali. Certificato CISM and 27001 LA. Membro del CD di AIIC e Vice Presidente di ISACA Rome Chapter. L'attuale attività di ricerca è orientata alla protezione e alla resilienza delle Infrastrutture Critiche.

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

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***

Il Presidente ed il Consiglio Direttivo di AIIC hanno proposto al **Gen. Isp. GArn Francesco NOTO** la nomina a Socio Onorario dell'Associazione. Il Gen. Noto, che è il Direttore della Struttura di Progetto Energia del Ministero della Difesa, ha accettato la nomina. Un affettuoso benvenuto al Gen. Noto con l'augurio di sicura e fattiva collaborazione.

La socia **Ing. Roberta Loreto (TASI)** ha gentilmente segnalato un interessante link (https://www.illusivenetworks.com/technology/platform/attack-intelligence-system) sulla Interactive Cyber Intelligence. A Roberta un sentito ringraziamento.

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.

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

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Asociation 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.

A set of Good Practices and Recommendations for Smart City Resilience Engineering and Evaluation

AIIC ha avviato un gruppo di studio su questo argomento, coordinato dal socio Sandro Bologna, 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 contributori:

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. Cyber supply chain risk management for smart cities critical information infrastructures (Luigi Carrozzi)
9. Personal data protection and the ethic challenge of Artificial Intelligence systems (Luigi Carrozzi)

NEWS E AVVENIMENTI

Making a DDoS Protection Plan - The impact of a distributed denial of service (DDoS) attack is easy to see – your websites and applications are unavailable or slow. Your call center lights up urgently with unhappy, frustrated customers. Your IT dashboards alert and indicate an ominous and confusing situation. Panic ensues at unprepared organizations when a DDoS attack hits. IT teams scramble in an attempt to keep websites and applications available in the face of malicious actors and multiple attack

vectors. As the attacker changes denial of service vectors to exploit different network vulnerabilities, IT personnel attempt to triage the unfolding situation and figure out why network anomalies are occurring
https://www.bitpipe.com/data/demandEngage.action?resId=1545345562_388white-aper%20%282%29.pdf
AKAMAI White Paper *– February 20, 1919*

Proteggere le infrastrutture critiche con il cloud, come vincere la sfida – Ai vantaggi delle soluzioni cloud nell'ambito delle infrastrutture critiche, con particolare riferimento alle reti elettriche intelligenti, fanno da contraltare importanti sfide legate alla sicurezza di questi sistemi, sui quali un attacco potrebbe avere conseguenze economiche e sociali molto gravi. La necessità di proteggere le infrastrutture critiche da attacchi informatici è divenuta quindi una priorità assoluta – sia in Europa che negli Stati Uniti – e le Smart Grid risultano essere un dominio di particolare interesse. Soluzioni pratiche ai principali problemi di sicurezza del cloud sono fornite dal progetto *SecureCloud*, co-finanziato dalla Commissione europea, Brasile e Svizzera. …..I principali problemi di sicurezza delle Infrastrutture Critiche in generale e delle Smart Grid in particolare sono dunque:

- La violazione dei dati (*Data Breach*).
- La sottrazione dell'account o del traffico.
- Il *Denial of Service* (DoS).

SecureCloud fornisce soluzioni concrete ai principali problemi di sicurezza del cloud, con particolare riferimento al dominio applicativo delle Smart Grid .
https://www.agendadigitale.eu/infrastrutture/proteggere-le-infrastrutture-critiche-con-il-cloud-come-vincere-la-sfida/
Agenda Digitale *– 19 febbraio 2019*

EU gathers momentum in cyber security legislation and cooperation - There has been significant progress in cyber security-related legislation in the European Union (EU) in the past two years, according to Carl-Christian Buhr, deputy head of cabinet for Mariya Gabriel, European commissioner for digital economy and society. "Since European Commission president Jean-Claude Juncker set the stage in his state of the union address in 2017, a lot has happened, including the transposition of the directive on security of network and information systems (*NIS Directive*) into law in member states," Buhr told the *CyberSec Brussels Leaders' Foresight 2019* event.
Although scheduled to leave the EU on 29 March 2019, the UK is among the member states to have completed the process, with the introduction of *the Network and Information Systems Regulations 2018* on 10 May last year, with most other EU member states having done the same since then. ……
"He said the NIS Directive brings a common baseline across member states when it comes to the authorities that exist, the responsibilities these public authorities have in the area of cyber security and the cooperation they have across the EU."
https://www.computerweekly.com/news/252458268/EU-gathers-momentum-in-cyber-security-legislation-and-cooperation?asrc=EM_EDA_108680093&utm_medium=EM&utm_source=EDA&utm_campaign=20190226_EU%20gathers%20momentum%20in%20cyber%20security%20legislation%20and%20cooperation

ComputerWeekly *- Warwick Ashford – 25 feb 2019*

IoT e 5G, combinazione micidiale per gli attacchi DDoS - Dove ci sono oggetti connessi c'è, purtroppo, anche terreno fertile per gli attacchi DDoS. IL caso eclatante della botnet Mirai nel 2016 è arrivato come una secchiata d'acqua fredda a mostrare come l'Internet of Things (e nella fattispecie milioni di webcam domestiche configurate in modo non sicuro) possa diventare uno strumento offensivo capace di mettere a tappeto intere porzioni del Web. Con l'avvento di nuovi servizi basati sul

5G il numero degli oggetti connessi è destinato a sbocciare e, con esso, anche quello degli attacchi Distributed-Denial-of-Service automatizzati, attacchi in cui dispositivi IoT infettati svolgono il lavoro sporco.
"Osserveremo attacchi DDoS di dimensioni sempre maggiori", scommette Paul Nicholson, senior director of product marketing di A10 Networks….Incontrato a Barcellona in occasione del Mobile World Congress, Nicholson non può dribblare il tema del 5G, vero protagonista dell'edizione di quest'anno della fiera: "*Mirai ha mostrato come sia possibile compromettere e usare gli oggetti connessi, magari privi di patch, per sferrare attacchi. Con il 5G aumenterà ancora il numero di dispositivi IoT alla base di nuove applicazioni, ma già oggi un po' tutto può diventare un oggetto connesso: un drone, un pallet in legno dotato di sensori e persino una mucca"…….*
http://www.ictbusiness.it/cont/news/iot-e-5g-combinazione-micidiale-per-gli-attacchi-ddos/42609/1.html#.XIZ6gxvsZPY
IctBusiness *– Valentina Bernocco – 27 febbraio 2019*

Pol. Postale: nuovi tentativi di truffa tramite WhatsApp - Alla **Polizia Postale** sono giunte numerose segnalazioni da utenti del **servizio di messaggistica WhatsApp** che sono stati contattati da un fantomatico **"reparto Tecnico" di Vodafone** il quale, con la scusa della certificazione del buon funzionamento della linea telefonica da parte di un tecnico o della possibilità di aumento della tariffa del piano telefonico, richiedeva con varie scuse, copia dei documenti di riconoscimento e, in alcuni casi, anche del passaporto e del codice fiscale.
La Polizia Postale ricorda che gli operatori telefonici **non richiedono mai** copie di documenti per interventi di assistenza né tantomeno utilizzano il servizio "WhatsApp" per comunicare con la propria clientela. In alcuni casi invece i truffatori informano gli utenti di inesistenti rincari della loro tariffa telefonica invitando gli stessi a passare ad altro operatore telefonico.
Nel dubbio è opportuno **sincerarsi attraverso il call center** dedicato all'assistenza. Vodafone Italia, anche a tutela della propria clientela, ha presentato denuncia all'Autorità giudiziaria.
https://www.bitcity.it/news/36110/pol-postale-nuova-ondata-di-truffe-su-whatsapp.html
BitCity *- Redazione – 28 febbraio 2019*

GDPR: in Italia oltre 630 notifiche di data breach - Dall'inizio dell'applicabilità del GDPR, ci sono state *in Italia solo 630 notifiche di data breach*, mentre ne sono avvenute oltre 10.000 in Paesi come l'Olanda, la Germania e la Gran Bretagna; a livello di Stati membri dell'Unione europea si contano invece più di 59.000 notifiche di violazione dei dati personali (data breach) eseguite da quando il GDPR è entrato in vigore il 25 maggio 2018.
Secondo il *GDPR Data Breach survey pubblicato da DLA Piper*, Paesi Bassi, Germania e Regno Unito hanno contato rispettivamente circa 15.400, 12.600 e 10.600 notifiche di data breach e i Paesi Bassi comandano ancora la classifica dei dati pro capite con 89,8 segnalazioni ogni 100.000 persone, seguiti da Irlanda e Danimarca. Questi numeri sono di gran lunga superiori rispetto al numero di notifiche ricevute secondo i dati pubblicati dal Garante per il trattamento dei dati personali italiano che risultano inferiori al migliaio…..
…..La survey completa sui data breach notificati nell'Unione europea può essere scaricato al seguente **link:**http://www.dlapiper.com/gdpr-data-breach-survey.
https://www.bitcity.it/news/36116/gdpr-in-italia-oltre-630-notifiche-di-data-breach.html
BitCity *- Redazione - 1° marzo 2019*

Tutti i rischi del jihad per l'Europa e l'Italia nella relazione dei Servizi - La minaccia del terrorismo jihadista non è mai venuta meno, assumendo un andamento carsico, e la gestione dei familiari dei foreign fighter rischia di diventare complicata per l'Occidente come quella dei

combattenti di ritorno. L'analisi complessiva del fenomeno terroristico contenuta nella relazione annuale dell'intelligence al Parlamento, presentata il 28 febbraio, contiene numerosi spunti anche in chiave prettamente italiana: dal numero e qualità degli espulsi per motivi di sicurezza nazionale ai problemi legati all'immigrazione.
Presi da problemi politici ed economici quotidiani, è difficile avere memoria dei tanti episodi avvenuti l'anno scorso. L'eccezione è l'attentato dell'11 dicembre a Strasburgo perché, oltre a 11 feriti, tra i 5 morti ci fu il giovane giornalista Antonio Megalizzi. Eppure in Europa ce ne sono stati almeno altri cinque: il 23 marzo a Carcassone (3 morti e 16 feriti), il 12 maggio a Parigi (1 morto e 4 feriti), il 29 maggio a Liegi (3 morti), tutti rivendicati dall'Isis come quello di Strasburgo. Nessuna rivendicazione è arrivata invece per l'attentato del 31 agosto ad Amsterdam, con 2 accoltellati, e per quello del 31 dicembre a Manchester, con altri 3 feriti a colpi di coltello. Esempi che confermano come il Vecchio Continente sia sempre un obiettivo, ma a Melbourne a novembre un somalo uccise il ristoratore italiano Sisto Malaspina e ferì altre due persone, così come a dicembre due turiste scandinave furono uccise in Marocco. Più o meno legati a bande di terroristi sono anche i sequestri di italiani che la relazione ricorda: il missionario Pierluigi Maccalli (il 17 settembre in Niger), la cooperante Silvia Costanza Romano (il 20 novembre in Kenya) e Luca Tacchetto con la compagna canadese Edith Blais "di cui si sono perse le tracce in Burkina Faso da metà dicembre"……..
https://formiche.net/2019/03/jihad-europa-italia-intelligence/
Formiche *– Stefano Vespa – 3 marzo 2019*

Small Business Cybersecurity Corner – The vast majority of smaller businesses rely on information technology to run their businesses and to store, process, and transmit information. Protecting this information from unauthorized disclosure, modification, use, or deletion is essential for those companies and their customers.
With limited resources and budgets, these companies need cybersecurity guidance, solutions, and training that is practical, actionable, and enables them to cost-effectively address and manage their cybersecurity risks. This NIST Small Business Cybersecurity Corner puts these key resources in one place.

Congress has given NIST responsibility to disseminate **consistent, clear, concise, and actionable** resources to small businesses. All resources are free and draw from information produced by federal agencies, including NIST and several primary contributors, as well non-profit organizations and several for-profit companies. These resources will be updated and expanded regularly.
The website does not provide operational assistance to individual companies, but it does list federal agency and some non-profit contacts (*Credit: Shutterstock*) that can offer that assistance. Small businesses should immediately report any threats and incidents to the FBI's *Internet Crime Complaint Center (IC3)*.
https://www.nist.gov/itl/smallbusinesscyber
NIST (National Institute of Standards and Technology) *– 04/03/2019*

Ultrasound Machine Diagnosed with Major Security Gaps. Check Point researchers investigate security risks and point to implications for medical IoT devices. RSA CONFERENCE 2019 – San Francisco – Vulnerabilities in connected medical devices could have massive implications for patients and the healthcare industry as a whole. The Internet of Medical Things (IoMT) is poised to broaden the attack surface for healthcare organizations, according to Check Point experts. Eighty-seven percent of healthcare institutions are expected to use IoT technologies by the end of 2019, with nearly 650 million IoMT devices in use by 2020, states a new Check Point study. The study underscores the danger of what could happen if these devices are poorly secured. IoT devices collect vast stores of data and are commonly built on outdated software and legacy operating systems. This makes them a simple gateway for cybercriminals, who could break in and move laterally across the target network. Consider ultrasound technology. Researchers explain how "huge advancements" have been made to provide detailed health data to doctors and patients. Unfortunately, they report, this innovation hasn't made its way to the security of IT environments where ultrasound machines sit. To prove this point, they went "under the hood" of a real ultrasound device. What they found was a tool running on Windows 2000. Like many IoMT devices, this no longer receives updates or patches, and leaves both the machine and its data exposed to intruders. It wasn't hard to exploit vulnerabilities and access its database of ultrasound images, they explain. An attacker with this access could launch a ransomware campaign on the hospital system or swap patients' images. "Think how much chaos that can do in the hospital," said Oded Vanunu, head of product vulnerability research at Check Point, in an interview with Dark Reading here at the RSA Conference……
http://www.darkreading.com/threat-intelligence/ultrasound-machine-diagnosed-with-major-security-gaps/d/d-id/1334118
DARK READING *-Kelly Sheridan 08 March-2019*

Italia-Cina. Gli allarmi dell'intelligence inascoltati dal governo - Le mire espansionistiche della Belt and Road Initiative (Bri) – il progetto infrastrutturale e politico della Cina foriero di nuove tensioni tra Pechino e Washington, e al quale l'Italia ha annunciato di voler aderire nonostante la netta contrarietà manifestata ufficialmente dagli Usa – sono da tempo monitorate dalla nostra intelligence.
Nell'ultima relazione del Dis al Parlamento, presentata a fine febbraio dai vertici del dipartimento alla presenza del presidente del Consiglio Giuseppe Conte, ci sono alcuni passaggi che sintetizzano le mosse della Repubblica Popolare e gli effetti nazionali e internazionali derivanti dal suo attivismo. "La Cina", spiega il documento, "ha ribadito la crescente capacità di incidere profondamente sulla ridefinizione degli equilibri mondiali: non esistono, di fatto, aree del pianeta […], dove la sua influenza non si sia consolidata o non risulti in rapido incremento. Il progetto Made in China 2025 (il piano con cui la Cina intende diventare autosufficiente nell'alta tecnologia, ndr) e la Bri", prosegue il documento, "sono i principali strumenti cui Pechino affida la propria affermazione nelle molteplici dimensioni in cui si articola oggi il potere moderno". Disegni, aggiungono i Servizi, "di lungo periodo e di portata assolutamente epocale" e che hanno portato a "interlocuzioni critiche a distanza" con l'Occidente, "soprattutto con gli Usa", su temi "che hanno fatto riferimento non solo all'ambito commerciale, ma anche al dominio tecnologico (e quindi alla sfera della sicurezza nazionale), delineando i contorni di un confronto strategico suscettibile di declinarsi anche in una dimensione geopolitica".
In questo quadro, rispetto all'eventualità che l'Italia aderisca all'iniziativa cinese con la firma di un memorandum d'intesa, Washington non ha usato giri di parole. L'account Twitter ufficiale del Consiglio per la Sicurezza nazionale statunitense (i cui tweet vengono registrati e archiviati come atti governativi) ha scritto: "L'Italia è una grande economia globale e una grande destinazione per gli investimenti. L'approvazione della Bri conferisce [invece] legittimità all'approccio predatorio cinese agli investimenti e non porterà alcun beneficio agli italiani", aggravata, secondo l'amministrazione

Usa, dal fatto che Roma è un membro del G7 e sarebbe il primo di questo "club" ad avallare politicamente a livello governativo i piani espansionistici di Pechino.
L'analisi delle ripercussioni della Bri riportate dalla relazione dell'intelligence appare in questo senso molto chiara, ma tocca solo di striscio un altro dei dossier che secondo svariati esperti vede mettere a repentaglio la collocazione internazionale dell'Italia e il suo rapporto con gli Stati Uniti: il caso Huawei. Gli Usa hanno più volte lanciato moniti ai loro alleati su questo dossier, l'ultimo dei quali giunto dal segretario di Stato Mike Pompeo, che in una recente intervista a *Fox Business Network* ha ribadito che Washington potrebbe non condividere più informazioni con gli Stati (soprattutto quelli che ospitano basi Nato, come l'Italia) che adotteranno tecnologia della compagnia di Shenzhen per l'implementazione della loro rete 5G, auspicando che "comprendano il rischio non solo per i loro cittadini, ma anche per la collaborazione con gli Stati Uniti per garantire la sicurezza globale".
Dopo il 'warning' americano, il Copasir – il Comitato parlamentare di vigilanza sull'intelligence – è intenzionato a raccogliere maggiori informazioni sull'intera vicenda. A suo tempo i servizi segreti italiani "avevano messo in guardia il governo dall'avanzata della multinazionale hi-tech, che è privata ma nondimeno riceve cospicui finanziamenti da alcune delle più grandi banche governative cinesi come Bank of China e Industrial & Commercial Bank of China e ha come fondatore un ex ufficiale dell'Esercito di liberazione popolare cinese, Ren Zhengfei.
https://formiche.net/2019/03/italia-cina-usa-bri-huawei-intelligence-governo/
Formiche *– Michele Pierri – 10 marzo 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

Trend Micro Cyber Conference - È l'appuntamento gratuito annuale, organizzato da Trend Micro, per conoscere i nuovi paradigmi della sicurezza Informatica. Lo scenario, esempi concreti, casi di successo ed esperienze di aziende e alleati tecnologici porteranno i partecipanti a conoscere come approcciare la sicurezza nel 2019. Quest'anno i temi saranno strettamente legati ai topic del futuro,

come le migrazioni nel cloud e le tecniche di social engineering; e agli ambiti che si pensano meno attaccabili come gli impianti industriali e lo smart working. Come aziende e singoli utenti bisogna essere preparati ad affrontare ogni genere di nuove minacce e i rischi. Oggi le minacce presenti nell'universo di Internet sono tantissime e riuscire a difendersi non è semplice. Ma grazie alle soluzioni più aggiornate la battaglia contro questi pericoli può essere combattuta con le migliori armi. Un passo importante è comprendere quali possono essere i rischi, affidarsi alle best practice, considerare sempre la security all'interno di ogni progetto, personale e aziendale, oltre che adottare una condotta di cittadinanza digitale.
Partecipando alla Cyber Conference di Trend Micro avrai la possibilità di rimanere aggiornato sulle nuove modalità e soluzioni legate alla lotta contro il cybercrime, perché le tue informazioni e quelle della tua azienda sono risorse strategiche che devono essere tutelate e protette dai migliori e più aggiornati sistemi di protezione."
Roma – Salone delle Fontane Via Ciro il Grande 10/12 – 00144 Roma RM, Italia – 21 marzo 2019
https://resources.trendmicro.com/IT-TME-Cyber-Conference-2019_Registration-page-Rome.html?_ga=2.104305992.957000573.1552327306-1071895357.1552327306

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.*

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

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* 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

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.

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

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
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*