AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2018	N. 02/2018	MARZO 2018

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

ANNO NUOVO, PROBLEMI VECCHI, SOLUZIONI IN ARRIVO?

E' arrivato l'anno nuovo e immancabilmente si sono ripresentati i soliti vecchi problemi. Maltempo? Troppo spesso basta una nevicata o una forte pioggia e si bloccano strade, autostrade, aeroporti e ferrovie. Per non parlare poi delle occasioni di eventi "eccezionali", purtroppo destinate ad aumentare di frequenza, che richiederebbero un approccio olistico per l'adeguamento delle infrastrutture, il rafforzamento delle organizzazioni e la preparazione dei cittadini. Sono incombenze a lungo termine, che richiederanno impegni e azioni della durata di anni, che il nuovo Parlamento e il suo Governo non potranno eludere. Sempre in tema di tempo meteorologico si aggiungono, tanto per completare il quadro, previsioni sbagliate e allarmistiche e meteo-bufale sul web che danneggiano gli utenti e i cittadini. E, per rimanere in tema di web, malware e altre minacce continuano ad imperversare sulla rete (anche se al momento un po' in sordina) e mettono a rischio non solo i computer delle industrie o dei singoli ma anche la salute dei cittadini, con la possibilità di colpire le cartelle cliniche di milioni di persone ed anche di interferire con il funzionamento dei dispositivi medici impiantati nel corpo dei pazienti. Un po' di incertezza anche nel settore della protezione dei dati personali, dove il 25 maggio diventerà definitivamente operativo il Regolamento europeo meglio noto come GDPR: che fine farà il vecchio Codice Privacy? Il Parlamento italiano ha approvato Il 25 ottobre 2017 la delega al Governo per la revisione del testo ma ce la farà il Governo ad emanare il provvedimento in tempo utile? Senza contare, poi, la grossa confusione che si sta facendo in merito al ruolo e alla figura del DPO, il Data Protection Officer, e alle certificazioni – non approvate e oltretutto discutibili – che si stanno moltiplicando.

Qualche buona notizia? Beh, qualcosa si muove. Entro il prossimo 9 maggio deve essere recepita la "direttiva NIS" 2016/11482 (Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione).Il 22 febbraio scorso il Consiglio dei Ministri ha approvato in via definitiva lo schema di Decreto Legislativo, che dovrebbe attuarla, e ha trasmesso il testo alle Commissioni parlamentari competenti: con le nuove Camere in formazione speriamo siano rispettati i tempi.

Per quanto riguarda le infrastrutture stradali, è stato firmato il Decreto per le nuove "smart road" e la sperimentazione su strada di veicoli a guida automatica, che autorizza la sperimentazione delle soluzioni tecnologiche per adeguare la rete infrastrutturale italiana ai nuovi servizi smart. L'obiettivo è quello di realizzare un miglioramento della rete stradale nazionale attraverso una sua graduale trasformazione digitale, per migliorare e snellire il traffico e ridurre l'incidentalità stradale.

Infine, per quanto riguarda la sanità, emerge qualche soluzione "salva-pazienti" in caso di mancato funzionamento della infrastruttura di rete, funzionamento che forse troppo superficialmente diamo sempre per scontato ma che, ormai è divenuto, al pari dell'energia elettrica, indispensabile per una sanità sempre più digitale e per il controllo e il trattamento di pazienti. Sono infatti numerose le tipologie di guasti che possono mettere a rischio la rete e quelli che vi sono connessi, inclusi i pazienti delle strutture sanitarie.

In questa newsletter troverete una rassegna di articoli su questi argomenti e informazioni su prossimi seminari ed eventi, molti dei quali sponsorizzati dalla nostra associazione: vi segnaliamo in particolare l'evento "Colloquia" del giorno 28 marzo 2018, organizzato direttamente da AIIC con la collaborazione dell'Università Roma Tre. Il tema dell'incontro, di estrema attualità, sarà: **La protezione dei dati personali e le infrastrutture critiche: quali sono i punti di attenzione per l'attuazione del GDPR nelle Infrastrutture Critiche in Italia?** L'appuntamento è a Roma, alle ore 14.30 in via Vito Volterra 62. Vi aspettiamo, non mancate! Ed ora, buona lettura.

Il Comitato di Redazione



Alberto Traballesi

Glauco Bertocchi

Silvano Bari

ATTIVITA' 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.
Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso dell'anno sia nelle sessioni "Colloquia" sia in eventi specifici o nei Gruppi di Ricerca. Chi volesse fornire il proprio contributo è pregato di inviare una mail a: segreteria@infrastrutturecritiche.it, specificando in oggetto "Argomenti di interesse". Nelle prossime newsletter provvederemo ad elencare tutti i temi proposti.

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.

NEWS E AVVENIMENTI

Contro la vera Spectre è inutile chiamare James Bond – Non è il solito malware. Nei microprocessori ci sono gravi falle, non facili da chiudere. Il problema è serio, perché Meltdown e Spectre minacciano soprattutto strutture critiche e sistemi cloud. Ai quali ci obbligano ad affidare i nostri dati. I nomi con cui sono stati battezzate le due vulnerabilità, salite in questi giorni agli onori

delle cronache, suonano sinistri: "Meltdown" richiama il rischio della fusione del nocciolo di una centrale nucleare (chi ricorda "Sindrome cinese", il film del 1979?), mentre "Spectre" è l'agenzia del male, contro la quale combatte da sempre l'Agente 007. Ma questo non è un film, la situazione è reale e James Bond non può farci nulla.
Il problema è semplice: la maggior parte dei sistemi informatici del mondo è a rischio di intrusioni malevole, che possono provocare danni di ogni tipo. Dal furto di informazioni, anche protette da crittografia, alla loro distruzione, al blocco totale dell'attività.
Dicono gli esperti che gli hacker potrebbero prendere di mira più le grandi strutture che i computer di singoli utenti. Significa che a rischio sono i sistemi militari, le centrali elettriche e telefoniche, le grandi basi di dati, i sistemi della sanità con le cartelle cliniche di milioni di persone. E soprattutto i computer che si fa credere siano installati nelle nuvole (*cloud*), e invece sono sulla terra, ma non si sa dove e sotto il controllo di chi.
http://www.interlex.it/privacyesicurezza/meltd-spectre.html
Privacy e sicurezza - Manlio Cammarata - 8 gennaio 2018

Insicurezza dei sistemi informatici, la saga continua – Si fa più presto a contare i sistemi e i dispositivi non affetti da "Meltdown" o "Spectre" che quelli vulnerabili. Da qui la gravità del problema, che richiede azioni decise per obbligare i fornitori a vendere prodotti più sicuri.
La notizia dei giorni scorsi della vulnerabilità di molti dei processori costruiti negli ultimi vent'anni è solo l'ultima di una catena infinita di notizie di vulnerabilità dei sistemi informatici che usiamo tutti i giorni.
Ed è proprio la grande quantità di dispositivi interessati dal problema che pone seri rischi di sicurezza per chiunque. La portata del rischio probabilmente non è ancora completamente chiara. Ovunque si legge che i costruttori e i fornitori di software stanno facendo le corse per rilasciare i correttivi che dovrebbero sanare queste vulnerabilità.
http://www.interlex.it/privacyesicurezza/gelpi18.html
Privacy e sicurezza - Andrea Gelpi - 8 gennaio 2018

GDPR: il nuovo ruolo del Data Protection Officer -Il GDPR obbliga le aziende a nominare un Data Protection Officer, figura molto più articolata di quelle che le aziende hanno sinora associato alla privacy e alla tutela dei dati
L'entrata in vigore del GDPR si avvicina e le aziende stanno rendendosi conto di quanto la normativa impatti sull'organizzazione dei processi interni e non sia semplicemente cosa "da tecnici". Come, purtroppo, in passato sono state affrontate molte altre norme legate alla privacy e alla protezione delle informazioni. Uno degli aspetti che riflettono più chiaramente questa impostazione è la figura del Data Protection Officer, assente nelle normative precedenti e invece assai "presente" nella filosofia del GDPR. Al Data Protection Officer - in italiano "*responsabile della protezione dei dati*" - sono dedicati gli articoli 37 (*Designazione del responsabile della protezione dei dati*), 38 (*Posizione del responsabile della protezione dei dati*) e 39 (*Compiti del responsabile della protezione dei dati*) del GDPR. Viene spontaneo considerare solo l'ultimo articolo per capire quale sia il suo ruolo, ma gli altri contengono indicazioni anche più importanti per valutarne il peso organizzativo.
Un primo elemento che farà tirare un sospiro di sollievo alle piccole-medie imprese è che il DPO va "*sistematicamente*" designato ma non deve necessariamente essere un dipendente. Anzi, data la complessità del suo compito è assai probabile che moltissime imprese, e non solo piccole, si rivolgano a Data Protection Office esterni che abbiano tutte le competenze necessarie. Questo

però non vuol dire che il DPO lo si nomini e poi ci si dimentichi di averlo, è anzi una figura che deve interagire con l'azienda costantemente e ai massimi livelli.
https://www.impresacity.it/gdpr/dettaglio.php?q=19159_0_gdpr-data-protection-officer.html&utm_source=newsletter&utm_medium=email&utm_campaign=MailUp
Impresa City – Francesco Pignatelli – 24 gennaio 2018

Responsabile del trattamento o Data protection officer: c'è differenza? – Dopo la recentissima modifica all'articolo 29 del Codice della privacy che ha riaperto il dibattito in ordine alla configurabilità (o sopravvivenza) del ruolo del responsabile interno anche in epoca successiva al 25 maggio 2018 (data in cui il Regolamento generale sulla protezione dei dati – di seguito anche solo Regolamento o RGPD- sarà pienamente applicabile), è forse opportuno chiarire, per chi non abbia troppa dimestichezza con la normativa, quali differenze ci siano tra il responsabile del trattamento e il responsabile per la protezione dei dati, e se i due ruoli possano essere in qualche modo fungibili o interscambiabili.
Il responsabile del trattamento è definito dal Regolamento europeo come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". L'articolo 28 del Regolamento generale sulla protezione dei dati prevede altresì che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorra unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".
Il Codice della privacy definisce, invece, il responsabile come "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali", e dispone (all'art. 29) che sia "individuato tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza".
https://www.ictsecuritymagazine.com/articoli/responsabile-del-trattamento-data-protection-officer-ce-differenza/
ICT Security Magazine – Francesco Pignatelli – 6 febbraio 2018

Cento giorni al GDPR. E a una nuova privacy. – Man mano che ci si avvicina all'entrata in vigore del GDPR aumenta l'attenzione delle imprese e, parallelamente, anche l'offerta dei vendor che stanno organizzandosi per offrire soluzioni il più possibile "chiavi in mano". Ma ormai la scadenza del 25 maggio sta diventando davvero impellente per le molte aziende che devono prima valutare e poi ripensare i propri processi di gestione dei dati, senza potersi affidare completamente a soluzioni pacchettizzate.
Uno dei temi che le aziende fanno forse più fatica a comprendere è che la privacy deve entrare a fare intrinsecamente parte della gestione delle informazioni, un principio che di solito si esplica nei concetti di *privacy by design* e *privacy by default*. *Privacy by design* significa sostanzialmente che i processi che gestiscono in vario modo le informazioni personali devono essere costruiti in modo da tutelare la privacy. Non si tratta solo di una costruzione tecnologica: l'azienda deve sempre avere sotto controllo la catena di gestione dei dati (chi tratta il dato, perché, con quali strumenti e garanzie di sicurezza) perché deve potere sempre - in caso di una violazione dei sistemi o di un errore umano che portino alla perdita di dati - capire cosa è successo, tutelare i diritti degli interessati e attribuire le giuste responsabilità. Al concetto di *privacy by design* è strettamente collegato quello di *privacy by default*, che è in parte più tecnico. Quando una corretta gestione

delle informazioni è implementata "*by design*" si deve anche garantire che il normale funzionamento dei processi sia quello previsto sulla carta.
http://www.impresacity.it/news/19332/cento-giorni-al-gdpr-e-a-una-nuova-privacy-.html?utm_source=newsletter&utm_medium=email&utm_campaign=MailUp
Impresa City – 13 febbraio 2018

Attuazione della Direttiva NIS, lo stato dopo lo schema di decreto legislativo – Il 23 febbraio u.s. è stato finalmente pubblicato lo schema di Decreto Legislativo che dovrebbe attuare in Italia la Direttiva NIS e che era stato approvato in via preliminare il precedente 8 febbraio e trasmesso alle Commissioni parlamentari il 22 febbraio. Il Governo ha optato per un approccio soft, limitandosi per lo più ad incorporare nello schema di D.Lgs. quanto già stabilito dalla Direttiva. La palla passa ora alle Commissioni parlamentari competenti che dovranno esprimere un parere sullo schema.
Nonostante la Direttiva NIS consenta agli Stati membri di estendere l'ambito di applicazione delle proprie disposizioni anche a settori diversi da quelli elencanti nella Direttiva, il Governo ha scelto di non avvalersi di questa possibilità. I settori che rientrano nell'ambito di applicazione dello schema di D.Lgs. sono infatti solo quelli espressamente previsti dalla Direttiva (ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; nonché motori di ricerca, servizi cloud e piattaforme di commercio elettronico).
https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/
Agenda Digitale – Luca Tosoni – 23 febbraio 2018

Holy See to be 'hacked' by first Vatican hackathon - A "hackathon" is a hacking marathon: a collaborative computer programming event in which a group works under a tight deadline to find software or programming approaches to real-world problems.
On March 8-11, the Vatican is hosting its first hackathon, *VHacks*. 120 young adult programmers, graphic designers, project managers, and others from around the world spend 36 hours "hacking" together over the course of three days.
The Vatican hackathon aims to help leaders develop technological approaches to the needs of social inclusion, interfaith dialogue, and migrants and refugees.
Jakub Florkiewicz, co-chairman of Vhacks and a student at Harvard Business School, told CNA via email that the hackathon's mission is "to inspire young people around the world to collaborate across divisions and to use technology to address social issues."
https://www.catholicnewsagency.com/news/holy-see-to-be-hacked-by-first-vatican-hackathon-74172
CNA – Catholic News Agency – Hannah Brockhaus – 2 marzo 2018

Firmato il Decreto per le nuove smart road e la sperimentazione su strada di veicoli a guida automatica - Il Ministro uscente delle Infrastrutture e dei Trasporti Graziano Delrio ha firmato il Decreto Ministeriale previsto per l'attuazione dell'articolo 1, comma 72, della legge 27 dicembre 2017, n. 205 (Legge di Bilancio 2018), che autorizza la sperimentazione delle soluzioni tecnologiche per adeguare la rete infrastrutturale italiana ai nuovi servizi smart e per i veicoli automatici.
Il decreto Smart Road mira a realizzare un miglioramento della rete stradale nazionale attraverso una sua graduale trasformazione digitale, con l'obiettivo di renderla idonea a dialogare con i veicoli connessi di nuova generazione, anche nell'ottica di rendere possibile l'utilizzo dei più

avanzati livelli di assistenza automatica alla guida, nonché per migliorare e snellire il traffico e ridurre l'incidentalità stradale.
Previsti gli interventi necessari per la comunicazione dei dati ad elevato bit-rate (es.: fibra), la copertura di tutta l'infrastruttura stradale con servizi di connessione di routing verso la rete di comunicazione dati, la presenza di un sistema di hot-spot Wifi per la connettività dei device dei cittadini, dislocati almeno in tutte le aree di servizio e di parcheggio, un sistema per rilevare il traffico e le condizioni meteo e fornire previsioni a medio-breve termine e una stima/previsione per i periodi di tempo successivi. Sulla base dei dati raccolti, poi, il sistema offrirà contenuti per servizi avanzati di informazione sul viaggio agli utenti, permettendo eventuali azioni di re-routing.
Gli interventi saranno realizzati in un primo tempo (entro il 2025) sulle infrastrutture appartenenti alla rete TEN-T (Trans European Network – Transport) e, comunque, su tutta la rete autostradale.
http://www.landcity.it/index.php?option=com_k2&view=item&id=641&Itemid=999
LandCity – Redazione – 5 marzo 2018

Sanità, che guaio se si blocca la rete: ecco le soluzioni "salva-pazienti" - Con una sanità sempre più digitale, i pazienti sono a rischio se il sistema va giù. Servono quindi ridondanza di reti e dati, monitoraggio continuo; procedure di emergenza chiare e condivise, la formazione degli operatori e la pianificazione di collaudi periodici. Alcune tipologie di guasti all'infrastruttura di rete (traffico anomalo dovuto a virus, attacchi hacker di tipo DoS), possono richiedere tempi di diagnosi e ripristino anche di alcune ore. Tempo inaccettabile quando si parla attività critiche per il paziente.
Siamo abituati a pensare a disaster recovery e continuità operativa come argomenti prettamente sistemistici, ovvero ridondanza delle sale server, copia a caldo dei dati e delle macchine virtuali, sistemi di load balancing, tutto quanto serve per garantire la disponibilità dei servizi. Ma quando non funziona la rete?
I servizi sono disponibili, in linea teorica, ma non raggiungibili in nessun modo. L'infrastruttura di rete è ormai data per scontata e, forse proprio per questo, è il punto meno considerato in termini di ridondanza e sicurezza. La rete costituisce infatti l'ossatura sulla quale si basa il funzionamento di tutti i servizi che siamo abituati ad usare nel quotidiano.
https://www.agendadigitale.eu/sanita/sanita-guaio-si-blocca-la-rete-le-soluzioni-salva-pazienti/
Agenda Digitale – Marco Mencacci, Alfiero Ortali – 5 marzo 2018

Solo la collaborazione transatlantica può salvare l'Occidente dalla guerra ibrida di Mosca - Condivisione delle informazioni, sicurezza, trasparenza e investimenti in ricerca e sviluppo su Intelligenza Artificiale e propaganda computazionale, ovvero quella condotta a colpi di bot. Sono questi alcuni dei punti sui quali le due sponde dell'Atlantico dovrebbero, secondo gli esperti, unire le forze per contrastare la moderna 'guerra' condotta contro l'Occidente usando cyber attacchi e disinformazione online. Solo in questo modo sarà possibile preservare le nostre società democratiche, così come le conosciamo.
Il tema è oggetto di un approfondito report della Brookings Institution scritto a quattro mani da **Alina Polyakova**, già direttore di ricerca dell'Atlantic Council, e oggi fellow del think tank americano Brookings Institution e adjunct professor alla Johns Hopkins University, e **Spencer Boyer**, nonresident senior Fellow nel medesimo think tank e Georgetown University, con un passato nelle istituzioni d'oltreoceano.
Nelle 24 pagine del documento, intitolato '**The future of political warfare: Russia, the West, and the coming age of global digital competition**', si pone in evidenza che anche se da un lato gli

strumenti e i metodi esistenti per colpire verranno man mano esposti e neutralizzati, dall'altro la tecnologia continuerà ad avanzare e diventerà finanziariamente più accessibile, gli attori malevoli continueranno a far evolvere le loro tattiche. Diventa pertanto fondamentale, quanto prima (lo studio stabilisce come un tempo limite da qui a 5 anni) accantonare un approccio politico reattivo, che si limita semplicemente a colmare le lacune delle vulnerabilità esistenti o risponde caso per caso – poiché destinato a fallire – e puntare su una strategia collaborativa di portata transatlantica.
http://formiche.net/2018/03/collaborazione-transatlantica-occidente-guerra-ibrida-usa-europa-russia-brookings-institution/
Formiche.net – Michele Pierri – 9 marzo 2018

PROSSIMI EVENTI

COLLOQUIA – Continua il programma di incontri AIIC per l'aggiornamento professionale e lo sviluppo della cultura sulle infrastrutture critiche.

Il 28 marzo p.v. a Roma, dalle ore 14.30 alle 17, si terrà il primo dei nuovi "colloquia" dell'anno 2018, organizzato insieme con l'Università Roma Tre ed ospitato nella sala conferenze del Dipartimento di Ingegneria, sito in via Vito Volterra 62.

Il tema dell'incontro sarà:
La protezione dei dati personali e le infrastrutture critiche: quali sono i punti di attenzione per l'attuazione del GDPR nelle Infrastrutture Critiche in Italia?
Il tema è di grande attualità, in prossimità del 25 maggio 2018, data alla quale, come già sopra evidenziato, il GDPR sarà definitivamente la nuova normativa di riferimento in campo europeo: in questo "Colloquia" si discuterà, con relatori di spicco in campo nazionale, delle principali novità che dovranno essere affrontate dai titolari dei trattamenti - come ad esempio le attività di valutazione dei rischi e di gestione dei data breach - con specifico riguardo alle aziende che operano nel settore delle infrastrutture critiche.
Al momento, hanno confermato la loro presenza i seguenti relatori:

Avv. Rosario Imperiali, (***Applicazione del GDPR nelle Infrastrutture Critiche: principali punti di attenzione***) coFounder of Gruppo Imperiali e Studio Legale Imperiali, editorialista de Il Sole 24 Ore

Ing. Diego Galletta, (***L'esperienza di Società Autostrade per l'Italia nell'applicazione della Data Protection***) IT security & accounting progetti tecnologici – Società Autostrade per l'Italia

Ing. Stefano Moni, (***La Data Protection nelle infrastrutture critiche nazionali governative***). Direttore dell'Ufficio per la Sicurezza dei Dati, Direzione centrale della polizia criminale, Dipartimento della pubblica sicurezza del Ministero dell'Interno

Chairman della sessione sarà Raffaella D'Alessandro, IBM e vicepresidente AIIC.
Concluderà l'incontro un intervento di Luisa Franchina, presidente di AIIC.

Il programma dell'incontro, in corso di aggiornamento, insieme con le indicazioni logistiche, sarà pubblicato sul sito di AIIC www.infrastrutturecritiche.it e verrà inviato agli iscritti alla mail list AIIC entro la prima quindicina del corrente mese.
Università Roma Tre – *Via Vito Volterra 62 – 28 marzo 2018 – ingresso libero*

La Cyber Security per la difesa delle Infrastrutture Critiche - CIAS Elettronica, Betafence Italia e Spark Security in collaborazione con NCP Italy Srl (Networking Competence Provider) organizzano il seminario di formazione su *"la sicurezza delle reti IP per le Infrastrutture Critiche".* Il seminario sarà rivolto a Security Manager, IT manager, amministratori di rete, responsabili di CED e tecnici IT nonché di interesse per network design, system integrator e chiunque altro abbia il bisogno di acquisire valide competenze nel settore della sicurezza. Oggi, infatti, la rete è un asset ormai fondamentale per ogni azienda e il tema della sicurezza della rete è sentito in modo prioritario. Il seminario mira ad evidenziare le problematiche di sicurezza delle reti suggerendo le migliori soluzioni da attuare al fine di proteggersi da accessi e utilizzi indesiderati e/o malevoli.
Durante l'incontro formativo verranno trattati nello specifico gli argomenti relativi alla sicurezza delle reti LAN e delle reti WiFi e dell'accesso Internet, integrando alla teoria una serie di esempi e di casi di studio che hanno l'obiettivo di mostrare le tecniche di difesa relative ad ogni forma di attacco. Verranno altresì illustrate le soluzioni IP specifiche per le Infrastrutture Critiche secondo la direttiva 114/2008CE e la normativa EN50151 e CEI 73-3.
http://www.cias.it/news/cyber-security-roma/
L'evento è patrocinato da AIIC
Auditorium CENTRO CONGRESSI FRENTANI *– Via dei Frentani 4, Roma – 4 aprile 2018*

Cyber-Crime Conference 2018 – **Verso un Modello di Cyber Difesa Globale** - La nona edizione della conferenza aprirà con una Tavola Rotonda dedicata a "Sistemi di Machine Learning, Blockchain, IoT e Big Data nelle mani dei Cyber Criminali - Come evolve il Cyber Terrorismo e quali sono i nuovi rischi per Stati e Industria".
Le nuove tecnologie stanno drasticamente aumentando la nostra superficie di attacco, approcciare correttamente gli aspetti di cyber security e privacy è essenziale come mai prima: Machine Learning, dispositivi dell'Internet delle Cose e Blockchain pervadono l'attuale contesto tecnologico, offrendo opportunità impensabili fino a pochi anni fa e aprendo a nuovi modelli di business e innovativi scenari operativi che devono, però, confrontarsi con una minaccia cibernetica sempre più aggressiva e sofisticata.
Verranno 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, Deanonimizzazione e Blockchain senza tralasciare le loro innumerevoli implicazioni giuridiche, tecnologiche e finanziarie.
https://www.ictsecuritymagazine.com/eventi/cyber_crime_conference_2018/presentazione
Auditorium della Tecnica, centro congressi di Confindustria (EUR) – *Roma - 18 aprile 2018*

CRITIS 2018 – In 2018, the 13th edition of the International Conference on Critical Information Infrastructures Security will be held in Kaunas, Lithuania. CRITIS 2018 will be hosted by the Vytautas Magnus University and the Lithuanian Energy Institute. CRITIS 2018 continues the tradition of presenting innovative research and exploring new challenges in the field of critical (information) infrastructure protection (C(I)IP) and fostering the dialogue between all C(I)I stakeholders.The Projects' Dissemination Session will be an opportunity of dissemination for ongoing European, multinational, and national projects. These presentations will not be submitted

to the reviewing process and will not lead to any publication. The purpose of this activity is sharing experiences among scientist and experts working on different projects in the C(I)IP domain. Similarly, a session will be devoted to CI Operators / sector stakeholders. As for the previous one, one does not expect original scientific work to be presented, open problems and heuristic solutions are expected to be outlined, instead. This specific session is aimed at abridging the gap between academic knowledge and actual policy, organizational and technical applications and challenges.
http://www.lei.lt/critis2018/
Portiamo alla vostra cortese attenzione che i lavori dovranno essere presentati entro il 30 Aprile.
L'evento è patrocinato da AIIC**.**
***Kaunas, Lithuania**, 24-26 settembre 2018*

Mostra Internazionale dell'Acqua – L'evento darà voce a tutti gli operatori in grado di trasferire valore ai diversi ambiti che impattano il settore idrico: il civile, l'industriale, l'agricolo. Con un approccio che guarda all'interesse pubblico e al tempo stesso alla costruzione di una filiera industriale tra le più evolute, in grado di dare slancio al settore.
I focus di ACCADUEO 2018:
• *INNOVAZIONE:* sarà sviluppato il percorso novità per consentire alle aziende di poter comunicare e mostrare i loro prodotti sulla stampa specializzata anche internazionale.
• *INTERNAZIONALE*: saranno costruite delle operazioni di networking internazionale con esperti, progettisti, società ed utilities straniere per gli espositori di ACCADUEO.
http://www.accadueo.com/home-page/1606.html
L'evento è patrocinato da AIIC
***ACCADUEO –** Bologna 17-19 ottobre 2018*

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.

Vi ricordiamo che, salvo eventi speciali riservati ai soli soci, la partecipazione ai Colloquia è libera. Inoltre, ogni socio può suggerire un tema, proporsi come relatore o come organizzatore di un Colloquia: suggerimenti e richieste possono essere inviate al coordinatore dei seminari AIIC, il Vicepresidente Silvano Bari, all'indirizzo e-mail segreteria@infrastrutturecritiche.it , mettendo in oggetto "Colloquia".

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00198 Roma, Via Spalato, 11 c/o Nitel - Tel. +39/06/64003640
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

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 Spalato, 11 – 00198 ROMA Tel. +39 06 64003640 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*