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. 03/2018	APRILE 2018

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

Protezione Infrastrutture Critiche: dove guardare e dove investire

Le soluzioni per la protezione di Infrastrutture Critiche, come ogni attività umana, sono determinate dalle minacce dalle quali ci si vuole proteggere. Facendo tesoro di quanto riportato nel Rapporto del World Economic Forum "The Global Risk Report 2017"[1] i fattori di rischio da considerare possono essere individuati essenzialmente in:

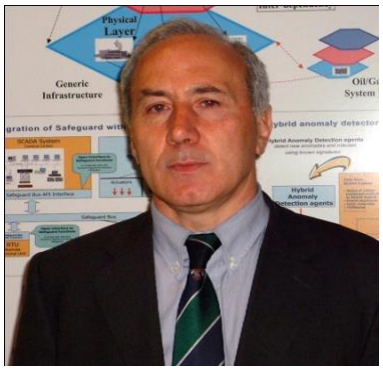
- Minacce da eventi naturali come conseguenza dei cambiamenti climatici e delle attività umane che provocano dei danni ambientali, urbanizzazione crescente e continui spostamenti della popolazione verso veri e propri attrattori ambientali.
- Attacchi terroristici, sia di tipo fisico che di tipo cyber.
- Politiche sociali non adeguate con conseguente disparità economiche che danno origine a comportamenti violenti.
- Aumento della superficie di attacco dovuto all'uso delle nuove tecnologie IT, in particolare dei dispositivi mobili, all'aumento della complessità dei sistemi e alla loro interdipendenza. Destinato ad aumentare con l'implementazione dei concetti di *smart city*, IoT, IIoT.
- Virtualizzazione delle infrastrutture IT dovuta all'aumento delle applicazioni "*in the Cloud*" anche per le Infrastrutture Critiche con conseguente "*outsourcing*" dei dati e delle informazioni.
- Mancanza o scarsa applicazione di adeguate soluzioni ingegneristiche del tipo "*safety & security by design*".
- Mancanza di cicli educativi dedicati agli operatori di Infrastrutture Critiche con particolare riferimento agli aspetti di *cyber security* e allo sviluppo di competenze nel campo della valutazione dei pericoli e dei rischi conseguenti.
- Scarsa cultura della sicurezza, non solo tecnologica ma anche personale e organizzativa e mancanza di forti vincoli legislativi.
- Scarsa attenzione agli eventi "*low frequency high consequence*" con conseguenze catastrofiche e iniziatori di effetti a cascata, che potrebbero trarre insegnamento da incidenti come Fukushima.
- Scarsa diffusione della cultura della modellistica e simulazione dei sistemi da proteggere, finalizzata a sviluppare misure di sicurezza, protezione, e resilienza.

I modelli di sicurezza, protezione, resilienza di 10 o 15 anni fa oggi sono inadeguati e poco rispondenti alle realtà realizzative e alle nuove sfide. Siamo passati da sistemi limitati perimetralmente a sistemi distribuiti, non solo negli aspetti fisici ma anche e soprattutto negli aspetti organizzativi, con la possibilità di lavorare in remoto (*homeworking*) e con l'aumentare delle

[1] http://www3.weforum.org/docs/GRR17_Report_web.pdf

soluzioni "*outsourcing*". La risposta è stata un uso diffuso di tecnologie per la sicurezza, ma ognuno degli strumenti proposti ha una validità limitata nel tempo e alla singola minaccia, perché basato su un approccio frammentato, non un approccio "*risk based*" che guarda a tutta l'organizzazione aziendale. Manca una metodologia basata su una continua analisi del contesto, che solo conseguentemente propone delle soluzioni tecnologiche e organizzative e ne individua la loro evoluzione. Negli ultimi anni si è cercato di far fronte a queste deficienze derivanti dalla segmentazione delle responsabilità con approcci più olistici basati sul concetto di resilienza della infrastruttura, o della città nel caso di una "*smart city*", o della nazione nel caso di una "*smart valley*".

AIIC cerca di creare una rete nazionale, ma anche internazionale, che affronta il tema della protezione delle Infrastrutture Critiche nella sua globalità, superando le tendenze del momento.



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

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 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.

Security Guidelines for Smart City – **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 provvisoria dello studio, che sarà svolto in lingua inglese, prevede al momento queste sezioni, di cui i soci indicati tra parentesi sono gli attuali coordinatori:

1. How to model a Smart City as a complex System-of-Systems (*Sandro Bologna*)
2. How to take advantage of the previous Guidelines produced by AIIC to secure the resilience of utility infrastructures such as power, telecommunications, gas, water, etc., making a Smart City (*Sandro Bologna*)
3. How to limit the consequence of cyber-attacks on a smart city's infrastructure (*Luisa Franchina*)
4. How to design products (IoT, IIoT, OT, IT) and systems making a Smart City with authentication and certification in mind (*Alessandro Lazari*)

5. How to securely design the interfaces between devices or services composing the Smart City (*Alberto Traballesi*)
6. How to limit permissions to get access to services offered by the Smart City (*Silvano Bari*)
7. How to make data security a priority from the beginning by encrypting sensitive data, and deploying network intrusion mechanisms that regularly scan for suspicious activity (*Raffaella D'Alessandro)*
8. How to monitor and control where and when vendors come in, monitor contractors while they're there, and turn it all off when they're gone (*Luigi Carrozzi*)
9. How to take advantage of readily available security tools and modeling techniques developed in different projects (*Glauco Bertocchi*)
10. How to take advantage of risk management principles to guarantee more resilient smart cities (*Priscilla Inzerilli*)

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

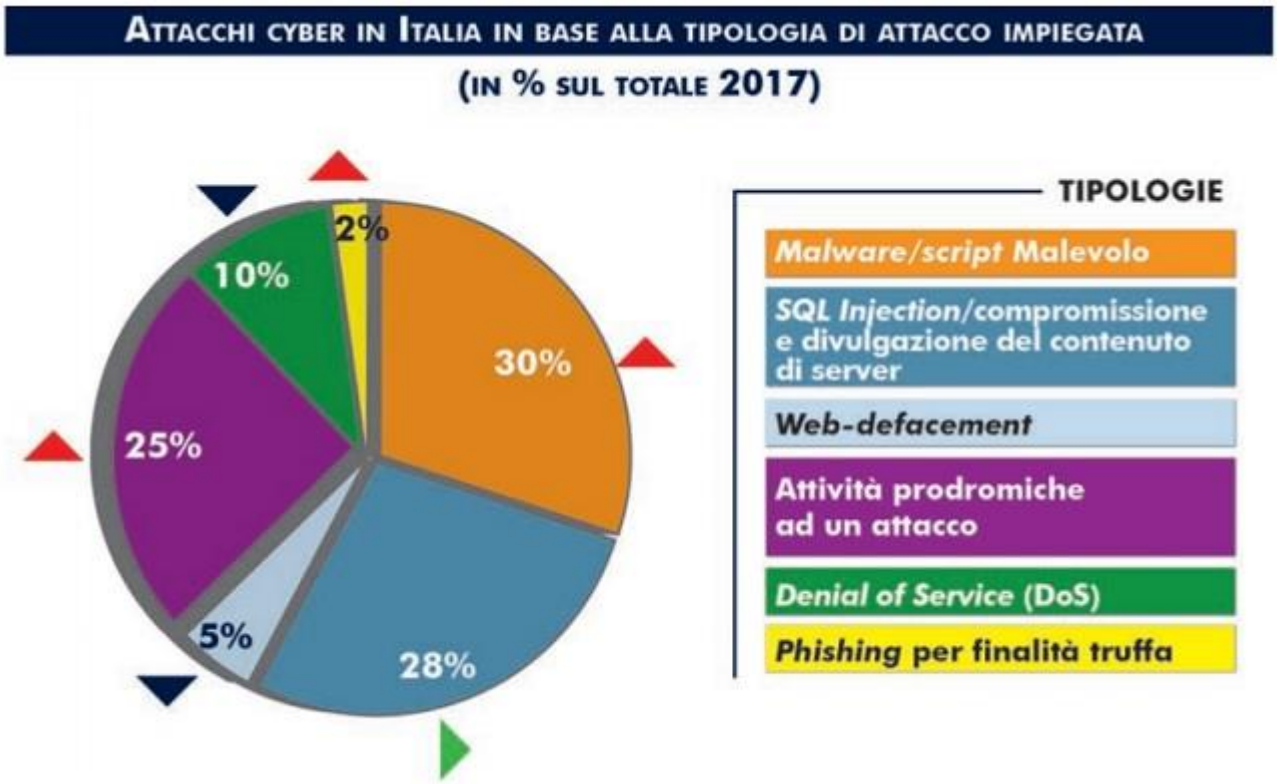
NEWS E AVVENIMENTI

Sensori, fabbriche in rete e dispositivi di controllo: "Ecco come come l'Internet delle cose rivoluzionerà l'industria" — Telecamere connesse in rete, termostati intelligenti, strani oggetti parlanti posizionati al centro del soggiorno. Il primo approccio dei consumatori con il mondo dell'Internet delle cose è fatto di dispositivi ultratecnologici che sembrano indirizzati a patiti della tecnologia e poco più. La vera rivoluzione però si può già vedere poco lontano, mettendo a fuoco cosa si sta muovendo nel mondo delle imprese. Ne é convinto Maciej Kranz, vicepresidente del Corporate Strategic Innovation Group di Cisco Systems, autore di un libro che già dal titolo mette in chiaro dove e in che modo l'internet delle cose si prepara a innescare grandi cambiamenti: "Connetti la tua impresa all'IoT - Come introdurre nuovi modelli di business, sbaragliare i concorrenti e trasformare il tuo settore" (ed. Franco Angeli). I numeri testimoniano che qualcosa sta cambiando e molto velocemente. Secondo le stime più recenti….
http://www.repubblica.it/economia/2018/03/10/news/maciej_kranz_cisco_iot-190522888/?ref=RHPPBT-VE-I0-C6-P11-S4.2-T1
La Repubblica – Flavio Bini – 3 marzo 2018

Cybersecurity nell'internet delle cose: tutte le caratteristiche fondamentali – Mentre nel mondo gestionale le entità da proteggere sono le informazioni (nei loro aspetti di integrità, disponibilità e riservatezza), nel mondo embedded (iot) si tratta di proteggere le funzioni (correttezza). Un mondo dove safety e security sono strettamente connesse. Ecco tutte le analogie e differenze tra i due mondi…
https://www.agendadigitale.eu/sicurezza/cybersecurity-nellinternet-delle-cose-tutte-le-caratteristiche-fondamentali/
Agenda digitale – Alberto Berretti, Giulio Carducci – 7 marzo 2018

Relazione sulla politica dell'informazione per la sicurezza 2017 – È stata presentata al Parlamento l'ultima edizione del documento redatto annualmente dal Sistema di informazione per la sicurezza della Repubblica. Ampio spazio è stato dedicato al tema della cyber security che si è

confermata settore centrale per l'intelligence italiana. Intelligence che è stata modificata per adeguarla alle esigenze di difesa cibernetica del Paese.
In particolare il nuovo Decreto del Presidente del Consiglio dei Ministri, "Direttiva recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", ha posto il Dipartimento Informazioni per la Sicurezza (DIS) al centro della governance nazionale in materia di cyber security. Tra le ulteriori misure tese ad elevare gli standard di sicurezza dei sistemi e delle reti italiane, sono state previste – anche in vista del recepimento della Direttiva NIS – l'unificazione del CERT Nazionale (CERT-N) e del CERT della Pubblica Amministrazione (CERT-PA), al fine di acquisire maggiore capacità di rilevazione, allarme e prima analisi degli incidenti cibernetici, e l'istituzione di un Centro di Valutazione e Certificazione Nazionale (CVCN) allo scopo di dotare il Paese di una capacità di verifica sull'affidabilità delle componenti ICT destinate ad essere impiegate nei sistemi di soggetti titolari di funzioni critiche o strategiche.
La minaccia più significativa è stata rappresentata ancora una volta dallo spionaggio digitale, appannaggio quasi esclusivo di attori strutturati, che hanno colpito target critici per sottrarre loro know-how pregiato ed informazioni sensibili da impiegare in sede di negoziazione di accordi di natura politico-strategica. Altro filone d'interesse è quello connesso con la minaccia ibrida, che si traduce in campagne di influenza che, prendendo avvio con la diffusione online di informazioni trafugate mediante attacchi cyber, mirano a condizionare l'orientamento ed il sentimento delle opinioni pubbliche. Il 56% degli attacchi rilevati dal DIS ha avuto come target soggetti pubblici, il 44% rimanente soggetti privati.



http://www.anra.it/portal/contenuti/mercato/1548/relazione-sulla-politica-dell-informazione-per-la-sicurezza-2017
ANRA (Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali) – Redazione ANRA – 2 marzo 2018.

Microsoft Security Intelligence Report Volume 23 – L'ultimo rapporto di Microsoft sulla security intelligence è disponibile per il download all'indirizzo www.microsoft.com/sir . Il malware vecchio e

nuovo continua ad essere propagato attraverso enormi botnet, gli hacker si stanno concentrando sempre più sui metodi di attacco semplici, come il phishing, e gli attacchi di ransomware si sono evoluti per essere più rapidi e distruttivi. Il report di Microsoft si tuffa in profondità in questi temi chiave e offre informazioni approfondite sull'intelligence delle minacce. Con particolare attenzione ad argomenti come:
- le botnet continuano ad avere un impatto su milioni di computer a livello globale;
- metodi facili come il phishing sono comunemente usati dai cyber criminali,
- il ransomware rimane una forza da non sottovalutare.
https://cloudblogs.microsoft.com/microsoftsecure/2018/03/15/microsoft-security-intelligence-report-volume-23-is-now-available/
Microsoft – 15 marzo 2018

La strategia di Cambridge Analytica si chiama Programmatic Adv – Dopo l'oscuramento da parte di Facebook della società Cambridge Analytica, specializzata nell'analisi di big data e nelle relazioni tra comportamenti e tratti della personalità, la cosiddetta scienza comportamentale, è necessario fare luce sulla potenza dei big data nel marketing predittivo e nella scienza comportamentale.
Utilizzando le tecnologie di programmatic advertising, i marketer della politica possono mostrare il giusto messaggio, al giusto consumatore/elettore, nel giusto contesto interattivo. Se aggiungiamo anche le fake news e la difficoltà di distinguere la verità dalle balle spaziali, il contesto di utilizzo dei big data nel programmatic advertising politico è una vera e propria bomba nucleare.
In una breve presentazione di 10 minuti al Concordia Summit di New York del 2016, il Ceo di Cambridge Analytica Alexander Nix aveva già spiegato al mondo intero il potere dei big data nell'utilizzo congiunto con la psicografia, l'analisi della personalità, e le possibilità di invio personalizzato di messaggi pubblicitari (Programmatic Advertising).
http://formiche.net/2018/03/cambridge-analytica-facebook-adv/
Formiche.net – Alessandro Sisti – 22 marzo 2018

Boeing colpita da virus Wannacry, verifiche su software aerei. "Attivate contromisure" Anche la Boeing è finita nel mirino degli hacker. La compagnia che produce aerei è stata colpita dal virus WannaCry, il ransomware che ha infettato migliaia di sistemi operativi lo scorso maggio in 150 Paesi del mondo - tra i quali l'Italia - e che è in grado di bloccare l'accesso ai dati dei computer fino a quando non si paga un riscatto. La notizia dell'attacco informatico è stata rilevata dal *Seattle Times*, che ha divulgato una nota scritta da Mike VanderWel, ingegnere capo del dipartimento per la produzione di aerei commerciali.
Il top manager ha mobilitato tutti gli esperti dell'azienda invitandoli a collaborare per mitigare l'effetto del virus. L'infezione avrebbe avuto origine a North Charleston. "Ho sentito che i 777 (bracci robotici di assemblaggio) potrebbero essere bloccati", ha messo in guardia il manager, indicando che il virus potrebbe estendersi alle funzioni di produzione e di test degli aerei ed eventualmente agli stessi software dei velivoli.
http://www.repubblica.it/tecnologia/sicurezza/2018/03/29/news/boeing_colpita_da_virus_wannacry_verifiche_su_software_aerei_attivate_contromisure_-192483707/
La Repubblica - 29 marzo 2018

La NATO e l'UE rafforzano il loro partenariato per la cyber security – Le due organizzazioni cercano di aumentare la rilevanza dei dati condivisi e stanno discutendo sul potenziale di condivisione delle informazioni classificate. Anche se hanno missioni molto diverse, la NATO e l'Unione Europea (UE) affrontano una minaccia simile nel cyberspazio, dicono i funzionari. La NATO si occupa di missioni di mantenimento della pace, umanitarie e militari, mentre l'UE si concentra

sull'economia in tutto il continente. Ma entrambe furono costrette a difendere le loro reti critiche quando il ransomware WannaCry e il malware NotPetya iniziarono a infettare i sistemi in tutto il mondo. I funzionari dell'UE stimano che le imprese abbiano dovuto affrontare oltre 4.000 attacchi di ransomware al giorno l'anno scorso, e l'80% delle aziende europee ha avuto almeno un incidente di sicurezza informatica. L'impatto economico della criminalità informatica è aumentato di cinque volte negli ultimi quattro anni, secondo la documentazione dell'UE.
https://www.afcea.org/content/cyber-ties-bind?utm_source=Informz&utm_medium=Email&utm_campaign=Informz+Email
Signal AFCEA – George I. Seffers – 1° aprile 2018

Guerre di spie. Gli occhi sugli agenti di Pechino e non solo sugli ex Kgb – *L'apparato di intelligence di Pechino è molto diffuso e l'Occidente potrebbe non essere preparato*
"Con tutta l'attenzione sull'ingerenza russa nelle elezioni del 2016, il danno fatto dal vigoroso e continuo spionaggio della Cina contro gli Stati Uniti è passato in secondo piano", attacca così un op-ed di David Wise pubblicato all'inizio di marzo dal *New York Times* (dunque ancora al netto delle tensioni attuali con la Russia).Basterebbe già da sé questo inizio firmato dal decano del giornalismo spionistico del *Nyt* (suo "Tiger Trap: America's Secret Spy War with China" del 2011, il libro zeppo di testimonianze dei funzionari del controspionaggio sulla presenza di spie cinesi sul territorio americano) per inquadrare la situazione che fa da contorno al confronto a tutto campo tra Stati Uniti e Cina; si passa dal settore commerciale ….
http://formiche.net/2018/04/cina-spie-pechino-kgb/
Formiche.net – Emanuele Rossi – 1° aprile 2018

Sicurezza energetica, ecco perché gli hacker del Cremlino puntano alle infrastrutture critiche
- A metà marzo, l'Fbi e il Dipartimento di Sicurezza interna degli Stati Uniti hanno lanciato un'allerta riguardante una nuova ondata di cyber-attacchi da parte di hacker riconducibili al Cremlino contro rete elettrica, impianti di trattamento delle acque e servizi di trasporto. L'annuncio rappresenta la prima conferma ufficiale che gli hacker, appartenenti, secondo un rapporto Symantec, ad un gruppo chiamato Dragonfly, hanno cominciato a prendere di mira infrastrutture critiche, da cui milioni di persone dipendono per i servizi di base.
Secondo il rapporto pubblicato dalle due agenzie, attacchi di questo tipo sarebbero in atto negli Stati Uniti "almeno dal marzo 2016". Già nel luglio 2017 c'era stata un'allerta riguardante attacchi ad impianti energetici sul suolo Usa, comprendenti anche un cyber-attacco contro una centrale nucleare in Kansas e riprendenti il modus operandi di svariati attacchi condotti in Ucraina e Georgia.
http://formiche.net/2018/04/sicurezza-energetica-hacker-cremlino/
Formiche.net – Anita Porta e Giuseppe Fersini – 2 aprile 2018

Iran 'the New China' as a Pervasive Nation-State Hacking Threat -- Security investigations by incident responders at FireEye's Mandiant in 2017 found more prolific and sophisticated attacks out of Iran.
Of the four new advanced persistent threat (APT) groups christened by FireEye last year, three were out of Iran.Mandiant, the incident response services arm of FireEye, witnessed a major increase in nation-state hacking activity by Iranian attackers in 2017, especially on the cyber espionage side of things. Iranian groups now are maintaining and keeping a foothold in victim organizations for months and sometimes years, demonstrating their sophistication, according to Mandiant's newly published M Trends Report on its incident investigations in 2017."In a way, it felt like Iran was the new China," notes Charles Carmakal, a vice president at Mandiant. "There were so many Chinese threat actors

in operations [in previous years], it felt like everyone had at least one Chinese actor" attacking them, he notes.
http://www.darkreading.com/perimeter/iran-the-new-china-as-a-pervasive-nation-state-hacking-threat/d/d-id/1331450
Darkreading.com – Kelly Jackson Higgins – 4 aprile 2018

Natural gas pipeline operators in the United States have been affected by a cyber attack that hit a third-party communications system. - The hackers targeted the Latitude Technologies unit at the Energy Services Group, but the attack did not impact operational technology. At least four US pipeline operators were affected by the attack on their electronic systems, the Energy Transfer Partners was the first company that reported problems with its Electronic Data Interchange (EDI) system.The Electronic Data Interchange platform used by businesses to exchange sensitive documents, including invoices and purchase orders. Latitude currently provides EDI services to more than 100 natural gas pipeline firms, storage facilities, utilities, law firms, and energy marketers across the US. The companies in the energy industry use it to manage key energy transactions.
https://securityaffairs.co/wordpress/71040/hacking/gas-pipeline-operators-hack.html
Securityaffairs.co – Pierluigi Paganini – 4 aprile 2018

PROSSIMI EVENTI

Cyber Crime Conference – Verso un Modello di Cyber Difesa Globale – La 9a edizione della **Cyber Crime Conference** si svolgerà il prossimo **18 Aprile 2018** nella splendida cornice dell'**Auditorium della Tecnica**, centro congressi di Confindustria nel quartiere EUR di Roma.
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 nona edizione 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**". 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/levento
L'evento è patrocinato da AIIC
ICT.Security – Auditorium della Tecnica Viale Umberto Tupini 65 – *Roma, 18 aprile 2018*.

Cybersecurity Summit Milano 2018 – The future of Cybersecurity in the AGE OF Digital Transformation - Giunto alla sua sesta edizione, il **"CYBERSECURITY SUMMIT 2018"** si terrà il prossimo **31 maggio 2018 a Milano** con la partecipazione di Keynote Speaker e dei migliori Esperti italiani e internazionali. Il Cybersecurity Summit di **The Innovation Group** crea un'occasione unica di scambio di esperienze e di networking, di discussione ed approfondimento, per comprendere come stanno evolvendo le esigenze di sicurezza ICT, quali sono le contromisure più attuali da adottare, come progettare e sviluppare soluzioni innovative di Cyber Risk management.

Inoltre, sarà presentata e discussa durante il Summit la ***Cyber Risk Management 2018 Survey***, indagine annuale di **The Innovation Group**, rivolta ai CISO/Risk Officer della sua Community, che verte sui temi dell'ottimizzazione delle strategie di prevenzione e risposta agli attacchi cyber.
https://www.theinnovationgroup.it/events/cybersecurity-summit-2018-2/?lang=it
L'evento è patrocinato da AIIC**.**
The Innovation Group – Enterprise Hotel Milano*, 31 maggio 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 ACCADUEO 2018 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*

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

PUBBLICAZIONI AIIC

Good Practices and Recommendations on the use of Big Data Analytics for Critical Infrastructure Resilience– *febbraio 2018*
http://www.infrastrutturecritiche.it/new/media-files/2018/04/AIIC_BigDataCIPR_FINALE.pdf

Guidelines for Community Resilience Evaluation- *marzo 2017*
http://www.infrastrutturecritiche.it/new/media-files/2017/03/COMMUNITY_Resilience_AIIC.pdf

Prospettive strategiche della protezione cibernetica nazionale- *aprile 2016*
http://www.infrastrutturecritiche.it/new/media-files/2016/04/Prospettive_strategiche_protezione_cibernetica.pdf

Guidelines for Critical Infrastructures Resilience Evaluation- *aprile 2016*
http://www.infrastrutturecritiche.it/new/media-files/2017/03/RESILIENCE_Guidelines_AIIC.pdf

Piano di Sicurezza Operatore – Data Model – *aprile 2013*
http://www.infrastrutturecritiche.it/new/media-files/2016/04/GDL-data-Model-v10-07-02-2013.-1-1.pdf

Aspetti legali per la redazione del Piano di Sicurezza dell'Operatore - *febbraio 2013*
http://www.infrastrutturecritiche.it/new/media-files/2016/02/OSP_legal-1.pdf
http://www.infrastrutturecritiche.it/new/media-files/2016/02/Carìa_ASPETTI-LEGALI-SU-PSO-1.pdf

Infrastrutture Critiche Europee Piano di Sicurezza dell'Operatore Proposta di linee guida operative – *febbraio 2012*
http://www.infrastrutturecritiche.it/new/media-files/2016/02/piano_operativo_sicurezza_19.12.2011-1.pdf

Incidenti di Cyber Security Industriale- *settembre 2009*
http://www.infrastrutturecritiche.it/media-files/2016/02/Incidenti-di-Cyber-Security-Industriale-1.pdf

Scheda Tecnica sulla direttiva UE- *giugno 2008*
http://www.infrastrutturecritiche.it/new/media-files/2016/02/DirettivaUE_short_28mag08-1.pdf

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.

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*