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. 6/ 2019	GIUGNO 2019

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

A un anno dall'entrata in vigore del GDPR

Il nuovo regolamento generale sulla protezione dei dati, il GDPR (General Data Protection Regulation), Regolamento Ue 2016/679, è entrato in vigore un anno fa, il **25 maggio** 2018. In questo periodo le relative sanzioni emesse in tutta Europa nei confronti delle imprese sono ammontate a circa 56 milioni di euro. L'Italia è quinta in Europa nella classifica per sanzioni emesse ai sensi del GDPR guidata dalla Francia. Per quanto riguarda il numero complessivo delle decisioni emesse dai garanti europei ai sensi del GDPR, il Paese con maggiori decisioni è la Germania, con 21 procedimenti, seguita dall'Ungheria con 7 procedimenti.
Inoltre, la classifica sul numero di notifiche di data breach è guidata dall'Olanda con 15.000 eventi, seguita dalla Germania con 12.600 e 10.600 del Regno Unito. Il numero di notifiche di data breach in Italia sfiora il migliaio secondo gli ultimi dati pubblicati dal Garante.
Tutto questo è emerso dalla survey della Dla Piper, presentata durante un incontro presso l'università Lumsa di Roma sull'efficacia del GDPR e sui possibili scenari futuri[1].
Da osservare che la maggior parte delle aziende hanno iniziato a conformarsi alla direttiva, dopo un avvio minimalista, dovuto principalmente alla risposta non particolarmente favorevole da parte delle piccole e medie imprese, che l'hanno visto come un freno allo sviluppo dell'economia digitale in generale e alla loro competitività in particolare.
Il GDPR ha anche portato benefici per i consumatori dell'Unione Europea: le aziende hanno intensificato notevolmente l'impegno per guidare il pubblico nelle pratiche di controllo dell'utilizzo dei loro dati personali. Si contrappone, tuttavia, il fatto che l'attenzione degli utenti è scarsa. Il 78%, a livello globale, non legge l'informativa di consenso nella sua interezza, mentre il 52% degli utenti a livello mondiale afferma che, anche leggendo tale policy, non comprende come verranno effettivamente utilizzati i dati. La percentuale è ancora più elevata nei Paesi Europei dove la GDPR è in vigore da un anno: ben il 58%.
E le imprese? Se alcune aziende sono ora conformi al nuovo regolamento, molte altre ci stanno ancora lavorando e l'allerta sul tema data security resta massima. Stando agli ultimi dati italiani resi noti dal Garante della Privacy, nel 2018 ci sono state infatti 630 notificazioni di Data breach, 4.704 reclami e segnalazioni (ben 1326 in più rispetto al 2017), 43.269 comunicazioni dei dati di contatto dei Responsabili Protezione Dati e 13.835 contatti con l'ufficio relazioni con il pubblico (ovvero 5504 in più rispetto all'anno precedente)[2].
Lo scorso martedì 7 maggio, l'Autorità Garante, attraverso le parole del suo Presidente, Antonello Soro, ha presentato alla Camera dei Deputati la Relazione annuale relativa al 2018.

[1] Redazione "*Privacy, un anno di sanzioni da GDPR*" BitMAT, 30 maggio 2019, https://www.bitmat.it/blog/news/85947/a-un-anno-dal-gdpr-cosa-e-successo-e-cosa-succedera
[2] Stefania Prando "*GDPR, riflessioni dopo dodici mesi*" Channel City, 30 maggio 2019, https://channelcity.it/mercato/16501/gdpr-riflessioni-dopo-dodici-mesi.html

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

Cruciali sono stati i passaggi programmatici relativi alle indifferibili ed urgenti sfide da raccogliere per dare e mantenere equilibrio all'Infosfera in cui viviamo e per iniziare ad usare gli strumenti che il GDPR offre rispetto alla regolamentazione dell'intelligenza artificiale e al corretto riposizionamento dell'uomo al centro delle triangolazioni indispensabili con **l'**Internet delle cose e la robotica.
Che il Regolamento abbia superato la prova più ardua, ovvero quella della fase di lancio, è ormai un dato di fatto: le imprese sembrano aver reagito bene all'introduzione della nuova normativa, ed anche nella Pubblica Amministrazione vi è una maggiore consapevolezza dei temi posti dal GDPR.

Alberto Traballesi

In servizio presso l'Aeronautica Militare Italiana dal 1958 al 1995, ha lasciato il servizio attivo con il grado di Generale di Brigata Aerea. Sino al 2013 ha servito come esperto presso la Presidenza del Consiglio dei Ministri. Laureato in Matematica, Ingegneria elettronica e Scienze Aeronautiche. Attualmente è parte attiva in ricerche sulla protezione delle IC e sulle tematiche spaziali.

ATTIVITA' DELL'ASSOCIAZIONE

ASSEMBLEA ORDINARIA DEI SOCI AIIC IL 25 GIUGNO 2019

E' convocata il giorno 19 giugno c.a. alle ore 23,00 in prima convocazione ed il giorno martedì 25 giugno, alle ore 17.30 in seconda convocazione presso la Sala Conferenze del Dipartimento di Ingegneria dell'Università Roma Tre, via Vito Volterra 62, Roma, l'assemblea ordinaria dei Soci AIIC.
E' un appuntamento importante, in quanto, oltre alla presentazione del bilancio consuntivo dell'anno passato, verranno illustrate le linee guida che indirizzeranno le attività per i prossimi anni ma soprattutto sarà l'occasione affinché i Soci possano fornire il loro contributo per quanto riguarda aspettative e indirizzi strategici dell'Associazione. Nel corso dell'assemblea saranno trattati i seguenti argomenti:
relazione del Presidente;
approvazione bilancio consultivo 2018;
approvazione bilancio preventivo 2019;
varie ed eventuali.
l'agenda potrà subire variazioni che saranno comunicate in anticipo a tutti i soci.
L'assemblea sarà preceduta da un Colloquia dove verranno presentati i risultati del GDL sulle Smart City. In questa occasione verrà distribuita ai soci la relativa pubblicazione. Tramite mail verranno fornite notizie sull'orario di inizio del Colloquia e sul relativo programma.

Vista l'importanza degli argomenti trattati, il Consiglio Direttivo auspica una numerosa e fattiva partecipazione da parte dei Soci.

Si ricorda che ai sensi dello Statuto dell'Associazione (riportato nel sito dell'Associazione) tutti i Soci ordinari in regola con la quota sociale per l'anno 2019 possono partecipare all'assemblea con diritto di voto. È consentita l'espressione del voto per delega. Ciascun socio può delegare esclusivamente un altro

socio ed essere latore di massimo tre deleghe. Le deliberazioni dell'Assemblea ordinaria sono prese a maggioranza dei voti. I Soci collettivi e sostenitori, in regola con la quota sociale per l'anno 2019, possono partecipare all'assemblea mediante un proprio rappresentante con diritto di voto.

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:

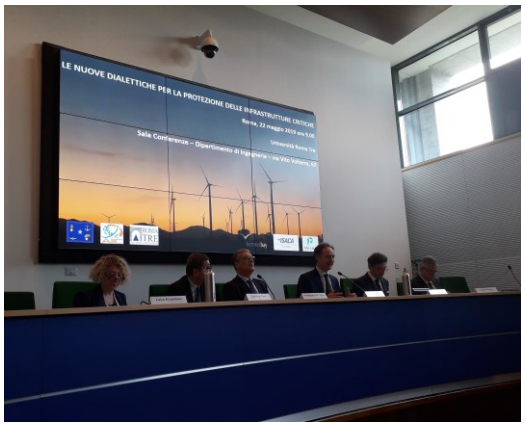
- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare 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.

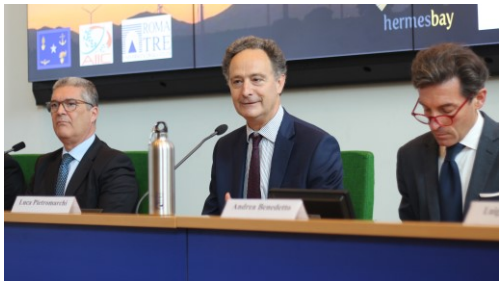
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente 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.
- **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 concluso lo 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.
Il report è scaricabile dal sito di AIIC tramite il seguente link
https://www.infrastrutturecritiche.it/a-set-of-good-practices-and-recommendations-for-smart-city-resilience-engineering-and-evaluation-2019/

Convegno del 22 maggio 2019 su "Le nuove dialettiche per la protezione delle infrastrutture critiche"

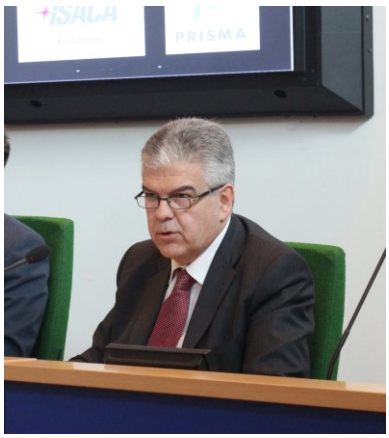


Si è tenuto lo scorso mercoledì 22 maggio a Roma il convegno "Le nuove dialettiche per la protezione delle infrastrutture critiche". L'evento, organizzato congiuntamente da AIIC, IsacaRoma e Università Roma Tre, ha visto – in una folta cornice di pubblico – i saluti del Magnifico Rettore dell'Università Roma Tre, prof. **Luca Pietromarchi**, e del Direttore del Dipartimento di Ingegneria, prof. Ing. **Andrea Benedetto**, seguiti dal Presidente di AIIC, ing. **Luisa Franchina**, dall'Amministratore Delegato di Terna, dott. **Luigi Ferraris**, dal Presidente di Enea, prof. **Federico Testa**.



In particolare, l'amministratore delegato di Terna, **Luigi Ferraris**, ha annunciato un accordo con il Ministero della Difesa, una collaborazione importantissima soprattutto nell'ambito della nuova strategia di "approccio duale delle Forze Armate al servizio del Paese". La collaborazione tra Difesa e Terna prevede:

- progetti per l'incremento della resilienza energetica e della sicurezza nazionale;
- progetti pilota finalizzati all'efficientamento energetico di siti militari;
- sfruttamento di possibili sinergie tra le rispettive infrastrutture.



Il comparto della Difesa, infatti, costituisce uno dei settori più "energivori" delle articolazioni dello Stato e, attraverso il Dipartimento "Struttura di Progetto Energia", il cui Direttore è il Gen. Isp. Ing. **Francesco M. Noto**, sviluppa gli strumenti più efficaci per garantire: la riduzione dei costi energetici, l'abbattimento delle emissioni inquinanti e la sicurezza energetica attraverso le nuove tecnologie.

Quello della sicurezza nel settore energetico, con i rischi di attacco cyber, è un fronte strategico per la struttura SPE diretta dal gen. Noto il quale, a sua volta, nella sua presentazione, ha illustrato la criticità delle infrastrutture energetiche e l'Energy Management System.

Altri interessanti interventi sono stati quelli di:

prof. **Stefano Panzieri** (Coord. Laboratorio Infrastrutture Critiche di Roma Tre) su "Progetti H2020 CockpitCI e Atena: effetti di attacchi cyber sulle infrastrutture elettriche";

ing. **Luca Marchisio** (Responsabile Strategie di sistema di Terna) su "H2020 OSMOSE: Optimal System-Mix of flexibility Solutions for European";

ing. **Luisa Franchina** (Presidente di AIIC) su "Uno scenario in cambiamento tra cyber security act, direttiva NIS e Raccomandazioni EU per Energy e cyber security".

La seconda parte del convegno ha visto gli interventi di:

dott. **Constantinos Hadjisavvas** (European Defence Energy) su "Contribution of CF SEDSS II in the protection of Defence-Related Critical Energy Infrastructure";

dott. **Georgios Theodoridis** (DG Joint Research Centre, European Commission) su "Protection of Defence-Related Critical Energy Infrastructure against Hybrid Threats";

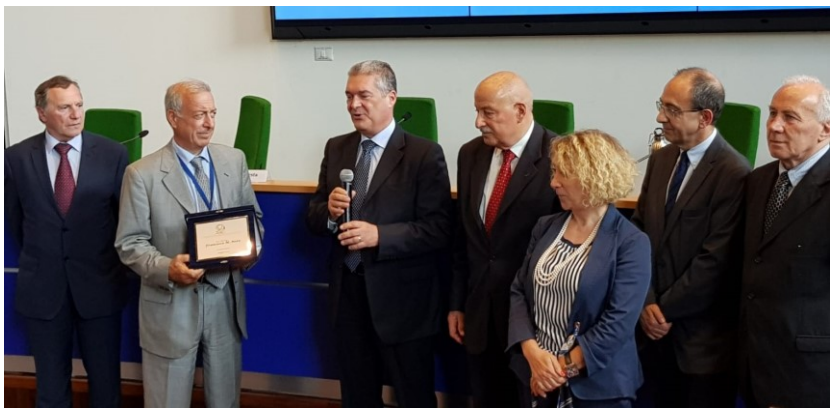
dott. **Vittorio Rosato** (ENEA) su "EISAC.IT: il primo nodo dell'iniziativa European Infrastructure Simulation and Analysis Center – tecnologie, servizi e prospettive";

William Nonnis (Ministero della Difesa) su " Blockchain e possibili applicazioni per la protezione delle infrastrutture critiche".

A chiusura del convegno, un light lunch è stato offerto dalle società sponsor Hermes Bay e Prisma.

Nel sito web di AIIC, www.infrastrutturecritiche.it, sotto la voce eventi AIIC, sono presenti tutte le informazioni sulla conferenza: programma, foto, presentazioni dei relatori (che hanno concesso la pubblicazione), discorsi e articoli.

Il Generale Isp. Francesco M. Noto nuovo socio onorario di AIIC



Nel corso del convegno del 22 maggio 2019 su "Le nuove dialettiche per la protezione delle infrastrutture critiche" si è svolta una simpatica cerimonia nella quale è stata consegnata al Generale Noto una targa con la nomina a socio onorario dell'Associazione Italiana esperti in Infrastrutture Critiche.

Francesco M. NOTO, Generale ispettore del Genio aeronautico, è attualmente in carica nel ruolo di Direttore della Struttura di Progetto Energia del Ministero della difesa. Laureato in Ingegneria civile indirizzo idraulica presso il Politecnico dell'Università Federico II di Napoli, ha ricoperto nella sua lunga carriera importanti incarichi sia all'interno della Forza armata di appartenenza che in ambito interforze, in Patria come all'estero.

NEWS E AVVENIMENTI

Sicurezza dati sanitari. Garante privacy: "Nel 2018 cyber attacchi aumentati del 99%"

07 MAG - "Il 2018 è stato definito, dal Clusit, l'anno peggiore relativamente alla sicurezza cibernetica, così costantemente esposta a minacce da configurare una sorta di cyber-guerriglia permanente. E se nel settore pubblico in generale gli attacchi sono cresciuti nell'ultimo anno del 41%, in ambito sanitario l'incremento ha toccato l'acme del 99% rispetto all'anno precedente, con effetti tanto più gravi che in altri settori perché l'alterazione dei dati sanitari può determinare - come abbiamo sottolineato anche rispetto al fascicolo sanitario elettronico - errori diagnostici o terapeutici". È quanto ha affermato il Garante della Privacy, Antonello Soro nel suo discorso di presentazione della Relazione al Parlamento.

"La carente sicurezza dei dati e dei sistemi – ha rilevato Soro - che li ospitano può rappresentare, in altri termini, una causa di malasanità. O, come nel caso di cui ci siamo occupati, degli embrioni scambiati, la violazione delle regole essenziali di protezione dati può avere effetti deleteri nei processi medici, tanto più gravi ove quei processi incidano su aspetti qualificanti l'esistenza individuale: la nascita, la morte, la genitorialità. …..

http://www.quotidianosanita.it/governo-e-parlamento/articolo.php?articolo_id=73718&fr=n

IoT in the Enterprise. An analysis of traffic and threats report. Enterprises around the globe have been adopting the use of IoT products to improve organizational efficiency, enhance communications, and to gain insight into system performance.
According to Gartner, 20.4 billion IoT devices will be in use worldwide by 2020, and more than 65 percent of enterprises will adopt IoT products. The rapid adoption of these IoT devices has opened up new attack vectors for cybercriminals. As such, the ThreatLabZ research team began studying the use of IoT devices in the enterprise by analyzing IoT traffic across the Zscaler cloud. The team analyzed one month of data for recent IoT device footprints based on traffic in the Zscaler cloud. This analysis looked at the types of devices in use, the protocols they used, the locations of the servers with which they communicated, and the frequency of their inbound and outbound communications, as well as IoT traffic patterns. This report details the results of this analysis.
https://www.zscaler.com/resources/white-papers/iot-in-the-enterprise-2019.pdf
Zscaler *-Zscaler™ ThreatLabZ™- May 2019*

Cybersecurity nelle reti elettriche 4.0: stato dell'arte e tendenze L'introduzione delle tecnologie digitali amplifica il livello di interconnessione delle reti elettriche. E introduce ulteriori dimensioni di rischio cyber, che gli stakeholder devono gestire insieme. Ecco una panoramica del settore e le strategie da adottare per garantire misure di difesa delle infrastrutture energetiche
Di questi giorni la notizia di un attacco cyber (denial of service) che ha causato blackout delle reti elettriche in California, Utah e Wyoming.Il punto è che le reti di nuova generazione richiederanno un uso più spinto dell'ICT: e saranno pertanto potenzialmente più esposte a minacce cyber. E' necessario che la progettazione delle nuove reti elettriche faccia leva sulle best practice sviluppate in ambito internazionale per la protezione cibernetica dei sistemi ICT distribuiti, adattandole alle specificità del dominio applicativo.
A differenza delle reti elettriche attuali, sarà la sicurezza cibernetica a dover guidare la progettazione e lo sviluppo delle reti elettriche di nuova generazione. La condivisione di best practices contribuirà a una maggiore consapevolezza dell'impatto dei rischi cyber nelle aziende energetiche……..
https://www.agendadigitale.eu/sicurezza/cybersecurity-nelle-reti-elettriche-4-0-stato-dellarte-e-tendenze/
Agenda Digitale- *Paola Girdinio, 09 Mag 2019*

6G, a che serviranno le reti post 5G: comincia la gara tra nazioni Mentre ancora si attende di sapere quando il 5G sarà pienamente operativo, i ricercatori di tutto il mondo stanno già guardando al 6G con obiettivo 2030. Vediamo i target e le tempistiche in fatto di standardizzazione, partendo da una domanda: perché ne abbiamo bisogno?
Obiettivo 2030: per quella data dovrebbero essere finalizzati gli standard per il 6G. Si,è vero, gran parte del mondo si sta ancora chiedendo quanto tempo ci vorrà per avere reti 5G pienamente operative e cosa potrebbe significare per le loro vite ed economie, ma i ricercatori delle telecomunicazioni stanno guardando più avanti, al 6G, spinti anche dal fatto che la solita Cina e la Corea del sud sono già in pole position. E l'Europa non vuole stare a guardare……
https://www.agendadigitale.eu/infrastrutture/6g-a-che-serviranno-le-nuove-reti-post-5g-comincia-la-gara-tra-nazioni/
Agenda Digitale - *Enrico Martini -15 Mag 2019*

Cisco risolve due vulnerabilità alte, che potrebbero coinvolgere milioni di dispositivi Cisco ha rilasciato aggiornamenti di sicurezza per la risoluzione di due vulnerabilità di livello "high" che potenzialmente potrebbe interessare milioni di dispositivi, come router, switch e firewall. Lo rendono noto gli esperti di cyber security del CERT-PA. Un attore malevolo potrebbe sfruttare queste falle per installare un malware, una backdoor, e ottenere il controllo persistente del sistema-bersaglio. A scoprirle sono stati i ricercatori di Red Balloon…..Al momento Cisco non ha rilevato attacchi che sfruttano le due vulnerabilità. Si consiglia, comunque, di installare al più presto gli aggiornamenti di sicurezza.
https://www.difesaesicurezza.com/cyber/cisco-risolve-due-vulnerabilita-alte-che-potrebbero-coinvolgere-milioni-di-dispositivi/
***Cyber, Difesa e Sicurezza**-Francesco Bussoletti -17 Maggio 2019*

Cybercrime, una delle armi più pericolose è il ransomware RobbinHood Il ransomware RobbinHood è più pericoloso degli altri malware dello stesso tipo. Prima di cominciare a criptare i dati, blocca 181 servizi di Windows che potrebbero ostacolarlo e disconnette le condivisioni di rete dalla macchina della vittima.Il ransomware RobbinHood è molto più pericoloso degli altri malware dello stesso tipo. Lo hanno confermato i ricercatori di cyber security di Carbon Black, rilevando che il codice malevolo prima di cominciare a criptare i dati blocca 181 servizi legati a Windows. In particolare quelli legati agli antivirus e ai software che permettono di bloccare la cifratura dei files. In questo modo non ha "nemici" che lo possono ostacolare. Inoltre, disconnette tutte le condivisioni di rete dal computer della vittima e cerca nel sistema la chiave di codifica RSA. Se non c'è ferma il processo e si auto cancella. Se, invece, è presente lo porta a termine. Secondo gli esperti, gli attori del cybercrime potrebbe non essere diffuso con i metodi tradizionali (campagne spam). Ma piuttosto attraverso altri sistemi come il protocollo hacked remote desktop (RDP). Gli esperti di cyber security: RobbinHood prende di mira utenze Windows in lingua inglese, ma potrebbe cominciare a colpire anche altri. La sua pericolosità è confermata da quanto accaduto a Baltimora
https://www.difesaesicurezza.com/cyber/cybercrime-una-delle-armi-piu-pericolose-e-il-ransomware-robbinhood/
***Cyber, Difesa e Sicurezza**-Francesco Bussoletti- 22 Maggio 2019*

Cybercrime, l'Italia è presa di mira con una nuova versione di JasperLoader Cisco Talos: Cybercrime prende di mira l'Italia con una nuova versione di JasperLoader per infettare sistemi con payload aggiuntivi, come Gootkit. Questa ha diverse modifiche e miglioramenti rispetto alla versione iniziale. Il cybercrime prende di mira l'Italia con una nuova versione di JasperLoader. Lo hanno scoperto gli esperti di sicurezza informatica Cisco Talos. Il malware loader, sfruttato per infettare sistemi con payload aggiuntivi che possono essere utilizzati per estrapolare informazioni sensibili, danneggiare i sistemi o avere un impatto negativo sulle organizzazioni, ha colpito l'Italia e altri paesi europei con trojan bancari come Gootkit negli ultimi mesi. Di recente, l'attività di distribuzione associata a queste campagne è stata interrotta. Ma dopo diverse settimane di volumi relativamente bassi, i ricercatori hanno scoperto la diffusione di una nuova versione del codice malevolo. Questa presenta diverse modifiche e miglioramenti rispetto a quella iniziale. Gli esperti di cyber security: JasperLoader ha implementato meccanismi aggiuntivi per controllare dove il malware può diffondersi e ora sta prendendo provvedimenti per evitare l'analisi da parte di sandbox e società antivirus.
https://www.difesaesicurezza.com/cyber/cybercrime-italia-e-presa-di-mira-con-una-nuova-versione-di-jasperloader
***Cyber, Difesa e Sicurezza**-Francesco Bussoletti- 27 Maggio 2019*

Cyber Security, scoperta nuova vulnerabilità 0-day in Windows 10 Il CERT-PA: Nuova vulnerabilità 0-day per Windows 10, che con opportune modifiche potrebbe funzionare su tutte le versioni del sistema operativo. L'ha pubblicata la ricercatrice SandboxEscaper
Nuova vulnerabilità 0-day per Windows 10. Lo ha scoperto la ricercatrice di cyber security chiamata SandboxEscaper, che ha pubblicato le informazioni relative su GitHub. La falla, come riporta il CERT-PA, risiede nel processo "Utilità di pianificazione di Windows" e permetterebbe ad un utente malintenzionato di eseguire un file .job non valido che sfrutta un difetto nel modo in cui tale processo modifica le autorizzazioni DACL (Elenco Controllo Accesso Discrezionale)per un singolo file…... Lo 0-day è stato testato e funziona solo su sistemi Windows 10 a 32 bit. Tuttavia tale codice, con opportune messe a punto, potrebbe funzionare anche su tutte le versioni del sistema operativo, XP e Server 2003 compresi.
……..Peraltro, ricorda il CERT-PA, ad oggi non esiste ancora una soluzione per risolvere quest'ultima vulnerabilità di Windows 10. Di conseguenza, c'è l'elevato pericolo che il cybercrime cerchi di sfruttarla per trarne profitti. A proposito, gli esperti di cyber security consigliano di non aprire file ricevuti da fonti sconosciute e di attuare azioni di mitigazione/informative verso gli utenti, nell'attesa del rilascio della patch ufficiale e/o del prossimo patch Tuesday di Microsoft previsto, l'11 giugno 2019……..
https://www.difesaesicurezza.com/cyber/cyber-security-scoperta-nuova-vulnerabilita-0-day-in-windows-10/
Cyber, Difesa e Sicurezza*-Francesco Bussoletti- 28 Maggio 2019*

Sicurezza digitale, la grande corsa allo standard quantum-proof In corso la competizione internazionale lanciata dall'agenzia Usa Nist per l'individuazione di algoritmi crittografici in grado di proteggere le informazioni nell'era del computer quantistico. Ecco il quadro in cui si muovono ricerca e industria**.** In vista dell'affermazione dei computer quantistici industria e ricerca stanno preparandosi ad alzare l'asticella delle difese per la cybersecurity. Per scongiurare che gli "scudi" rappresentati dagli attuali sistemi crittografici possano crollare sotto la potenza del "qubit". Per questo l'agenzia Usa National Institute of Standards and Technology ha lanciato una competizione internazionale: l'obiettivo è la messa a punto di standard quantum-proof. Ecco le tappe della gara e lo scenario in cui si sta muovendo. Se il secolo scorso è ricordato come il secolo che ha visto la nascita del calcolatore elettronico, o computer, questo secolo sarà probabilmente ricordato come quello ha visto la nascita del computer quantistico, ovvero del computer basato sulla fisica quantistica anziché su quella classica. E' noto da tempo che il computer quantistico, o quantum computer, rappresenta un'innovazione capace di rivoluzionare molti aspetti della nostra vita. I computer quantistici saranno infatti capaci di risolvere problemi che richiederebbero migliaia di anni per essere risolti con i computer classici. Questo perché il computer quantistico non è limitato a lavorare su bit che possono valere soltanto 0 oppure 1, come il computer classico, ma lavora invece sui cosiddetti "qubit", che possono valere 0 ed 1 simultaneamente, sfruttando i principi della fisica quantistica. Ciò consente di avere un'accelerazione esponenziale nell'esecuzione di alcune tipologie di calcoli, rendendo così agevole l'esecuzione di alcuni algoritmi, quali ad esempio quelli necessari alla sintesi di molecole, alla simulazione di fenomeni climatici oppure alla soluzione di alcuni problemi matematici noti come fattorizzazione di grandi numeri e calcolo di logaritmi discreti…..
https://www.agendadigitale.eu/sicurezza/sicurezza-digitale-la-grande-corsa-allo-standard-quantum-proof/
Agenda Digitale*-Marco Baldi- 29 Maggio 2019*

Assistenti vocali, doppio rischio privacy e security: quali soluzioni Alexa, Google Home, Cortana le star del nuovo mercato che solo in Italia vale 380 milioni di euro. Ma il loro ingresso nelle abitazioni pone in modo sempre più marcato la gestione di una serie di rischi. Ecco come proteggersi dai vari tipi di minacce. Siamo entrati quasi senza accorgerci nell'era degli assistenti vocali. Se da un lato le possibilità offerte sono molteplici, dall'altro non mancano i dubbi su come l'utilizzo di questi dispositivi possa esporci a rischi quali la violazione della nostra sicurezza e della nostra privacy. Grazie anche alla capacità di governare scenari di "smart home" (centralizzando accensione, spegnimento e regolazione delle luci smart, regolando temperatura e climatizzazione, gestendo agende, sveglie, promemoria, timer, diffondendo contenuti multimediali, aprendo e chiudendo serrande, tende, serrature intelligenti… solo per fare alcuni esempi), la loro diffusione nelle nostre case sta crescendo a ritmo esponenziale. Ho espressamente citato l'abilitatore di Smart Home in quanto quest'ultimo pare essere un argomento piuttosto sexy, che sta facendo da driver dell'adozione delle tecnologie ad attivazione vocale.
……Nel 2018, il mercato italiano valeva 380 milioni di euro, con una crescita di più del 50% anno su anno; se consideriamo che solo da quell'anno gli smart speaker si sono affacciati definitivamente al mercato italiano, tutto lascia pensare che la crescita sarà molto più importante a partire da quest'anno. È sufficiente analizzare i dati di altri paesi che hanno avuto prima di noi la possibilità di utilizzare questi strumenti per ben comprendere le potenzialità di questo mercato: un esempio per tutti è la Germania, dove questo mercato vale già quasi due miliardi di euro…….
https://www.agendadigitale.eu/cultura-digitale/assistenti-vocali-tutelare-privacy-e-security-quali-soluzioni/
***Agenda Digitale**-Paolo Ballanti - 29 Maggio 2019*

Sicurezza delle infrastrutture critiche: è il fattore umano il punto debole Per la sicurezza delle infrastrutture critiche bisogna agire soprattutto su dipendenti, collaboratori e fornitori. I programmi di security awareness hanno come scopo quello di rendere l'individuo da anello debole a ingranaggio più affidabile nei processi di sicurezza. Tuttavia, le iniziative risultano ancora poco efficaci**.** Quella delle infrastrutture critiche è una realtà sempre più interconnessa, interdipendente e tecnologicamente avanzata. Tale complessità ha da una parte reso i servizi più efficaci e immediati, ma dall'altra ha creato nuove debolezze e vulnerabilità. Tra queste, il "fattore umano" è considerato sia l'elemento di maggiore forza ma anche l'anello debole dei processi di sicurezza e negli ultimi tempi sono state avviate delle campagne di Security Awareness. Campagne che risultano però ancora limitate sia livello quantitativo che qualitativo, quando invece sarebbero essenziali per trasformare il personale da anello debole a punto di forza della sicurezza delle infrastrutture critiche…….
https://www.agendadigitale.eu/sicurezza/sicurezza-delle-infrastrutture-critiche-e-il-fattore-umano-il-punto-debole/
***Agenda Digitale**-Giacomo Assenza-Roberto Setola - 29 Maggio 2019*

Facebook removes fraudulent Iranian accounts Facebook has removed dozens of accounts, pages and groups that had thousands of followers that were created by Iranians in the hope of swaying public opinion during the 2018 election cycle. The social media giant said on May 28 it had removed 51 accounts, 36 pages and seven groups from Facebook, along with three Instagram accounts that were involved in coordinated inauthentic behavior, which is Facebook-speak for groups of pages or people using the site working together to mislead others about who they are and what they are doing, according to Nathaniel Gleicher, Facebook's head of cybersecurity policy. About 21,000 accounts

followed one or more of the pages, about 1,900 accounts joined one or more of the groups and 2,600 people followed one or more of these Instagram accounts. "They purported to be located in the US and Europe, used fake accounts to run Pages and Groups, and impersonated legitimate news organizations in the Middle East. The individuals behind this activity also represented themselves as journalists or other personas and tried to contact policymakers, reporters, academics, Iranian dissidents and other public figures," Gleicher wrote this week…… Iran is not the only nation causing problems for Facebook. Rep. Nancy Pelosi, D-Calif., on May 29 expressed her displeasure with the company for allowing video of her that was edited to make her appear drunk to remain on its site, according to KQED News. Pelosi said the fact that Facebook knows the videos in question are fake and has not removed them from the far right ……..
https://www.scmagazine.com/home/security-news/government-and-defense/election-coverage/facebook-removes-fraudulent-iranian-accounts/
***SCmagazine**- Doug Olenick- May 30, 2019*

Nansh0u cryptomining malware hits 50,000 servers. Researchers describe it as more than just a typical cryptomining attack due to its use of fake certificates and privilege escalation exploits. China-based cryptomining malware campaign dubbed Nansh0u has targeted and infected up to 50,000 servers Windows MS-SQL and PHPMyAdmin servers worldwide. Guardicore researchers disclosed in a blog post on 29 May that the campaign took place between 26 February and 11 April. The researchers described it as more than just a typical cryptomining attack due to its use of fake certificates and privilege escalation exploits. When the attacks were first spotted, all three had source IP addresses originating in South-Africa and hosted by VolumeDrive ISP. In addition, the incidents shared the same attack process, focusing on the same service and using the same breach method and post-compromise steps. Researchers spotted 20 versions of malicious payloads and said new payloads are created at least once a week and are used immediately after their creation time in attacks that have targeted companies in the healthcare, telecommunications, media and IT sectors. Once a server is compromised, the targeted servers are infected with malicious payloads …….
https://www.scmagazineuk.com/nansh0u-cryptomining-malware-hits-50000-servers/article/1586133
***SCmagazineUK**- Robert Abel- May 31, 2019*

Che cosa stanno facendo le banche per diventare cyber sicure. I numeri dell'Abi. Gestione e mitigazione del rischio informatico, sicurezza dei pagamenti online, sensibilizzazione della clientela e del personale bancario sono alcune delle priorità in termini di investimento. C'è, però, ancora molta strada da fare. E, per questo, l'intelligence italiana avvierà una campagna di sensibilizzazione nei confronti del mondo economico-finanziario sul tema della cyber security Banche e finanza sono sempre più nel mirino degli hacker. E così corrono ai ripari. *SENSIBILIZZAZIONE E INFOSHARING* Sul tema della sensibilizzazione verso la clientela sui rischi del cyber crime, l'Associazione bancaria italiana (l'Abi), spiega che le banche italiane hanno "sviluppato campagne attraverso il portale di Internet Banking (per l'89% delle banche rispondenti), attraverso le informative contrattuali o presso le filiali (per il 67%) e si sono fatte promotrici di collaborazioni intersettoriali, come il CERTFin, l'iniziativa cooperativa pubblico-privata diretta dall'associazione e da Bankitalia finalizzata a innalzare la capacità di gestione dei rischi cyber degli operatori bancari e finanziari". ……
https://formiche.net/2019/06/banche-cyber-security-investimenti-misure/
***FORMICHE**-Michele Pierri- 01/06/2019*

Come si espande la cyber guerra (e perché è così conveniente) Dal momento che la guerra non cinetica offre un potenziale d'impatto senza perdere la vita, anche il campo di battaglia si allarga in un modo che non si è visto dall'avvento dell'aereo. L'analisi di Carlo Scuderi del Center for Cyber Security and International Relations Studies UniFi .

Con l'evoluzione della guerra non cinetica come forma di conflitto a bassa intensità durante il tempo di pace si pone un grande problema: dal momento che la guerra non cinetica offre un potenziale d'impatto senza perdere la vita, anche il campo di battaglia si allarga in un modo che non si è visto dall'avvento dell'aereo. E ancora peggio, ha esteso il campo di battaglia a organizzazioni che non sono mai state responsabili prima di difendersi dalle aggressioni degli stati nazionali. La maggior parte dei conflitti in tutto il mondo è considerata "a bassa intensità", il che significa che prendono la forma di guerriglia, insurrezioni, operazioni speciali e altri mezzi simili. Anche le recenti guerre tra gli Stati Uniti e i suoi nemici in Iraq e Afghanistan possono essere considerate tali, dal punto di vista dei suoi nemici, poiché essi stessi non si impegnano in grandi manovre militari su fronti definiti. Non sono più i tempi in cui due grandi eserciti ammassavano le loro forze per affrontare un campo di battaglia con chiare linee di combattimento, tranne che tra due potenze minori in un conflitto regionale di interesse solo locale. Ciò significa in termini più ampi che le principali potenze del mondo hanno un incentivo e un modello attraverso cui condurre una guerra non cinetica contro potenziali avversari, anche in tempo di pace…….

https://formiche.net/2019/06/cyber-warfare-sviluppi/

***FORMICHE**-Carlo Scuderi- 02/06/2019*

PROSSIMI EVENTI

Cyber Crime Conference – Atti del convegno

La 10a edizione della Cyber Crime Conference, svoltasi lo scorso 17 aprile nell'Auditorium della Tecnica a Roma, ha registrato una straordinaria partecipazione di pubblico con oltre 1200 visitatori, confermando la propria autorevolezza quanto a rilevanza e attualità dei contenuti trattati.

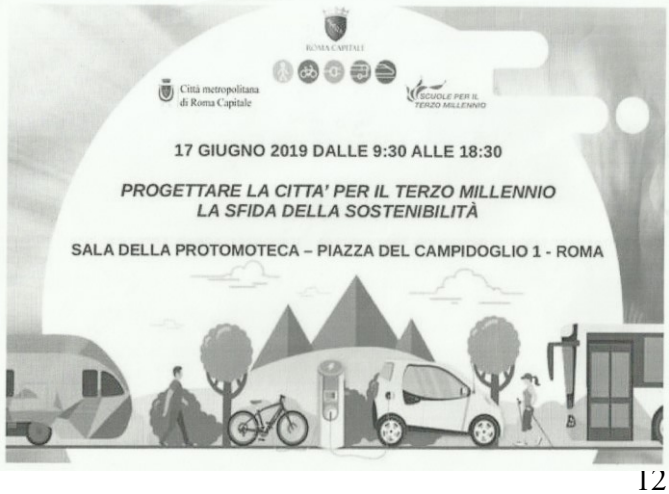
Al seguente link è possibile effettuare il download degli atti del convegno:

http://bit.ly/2I1l45f

Il prossimo evento in programma, la 20a edizione del Forum ICT Security si terrà il 16 ottobre 2019 a Roma.

Convegno "Progettare la città per il terzo millennio" a Roma in Campidoglio il 17 giugno

Si svolgerà a Roma il prossimo lunedì 17 giugno il convegno "Progettare la città per il terzo millennio. La sfida della sostenibilità". L'appuntamento è dalle ore 9.30 alle 18.30 presso la Sala della Protomoteca, in piazza del Campidoglio, 1.



Il convegno affronta temi strutturali per la progettazione di una città sostenibile, pronta ad affrontare le sfide del terzo millennio: una mobilità per tutti, accessibile, a basso costo ed ecologica,

sicurezza infrastrutturale e sostenibilità ambientale.

E' previsto un intervento del dr. **Claudio Pantaleo**, membro del Consiglio Direttivo di AIIC, sul tema "**L'Accessibilità dell'Infrastruttura Critica del Trasporto Pubblico Locale**", dove verrà trattato il valore che il TPL può dare alla vita quotidiana di tutte le persone che vivono e frequentano la città, ovviamente anche gli individui con disabilità. Claudio Pantaleo, nel suo ricco curriculum, vanta anche un trascorso di Direttore Sistemi e Tecnologie a Protezione del Patrimonio in ATM-Milano.
Altri interventi saranno relativi a:
- La rete integrata delle metropolitane possibili, accessibili e a basso costo
- Cambiamento climatico e pianificazione urbanistica per uno sviluppo sostenibile ed inclusivo
- Interventi per migliorare la sicurezza antisismica di strutture pubbliche, abitative e industriali.
- Ambiente urbano e analisi di vulnerabilità ai cambiamenti climatici
- Una città più resiliente e più aperta alla disabilità
- Prospettive di utilizzo di tecniche di realtà aumentata nella presentazione dei progetti

Il programma completo del convegno, promosso dall' Associazione "Scuole per il terzo Millennio" insieme all'Ordine degli Ingegneri della Provincia di Roma, si trova a questo link:

http://www.scuoleperilterzomillennio.it/6-convegno-progettiamo-roma

NOTIZIE D'INTERESSE:

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 provveduto, 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.

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 (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

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@InfrastruttureCritiche.it

o visitate il sito

www.InfrastruttureCritiche.it

ATTENZIONE

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

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

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Palestro 95 – 00185 ROMA Tel. +39 06 64871209 Email segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente cliccare questo link: http://www.linkedin.com/ groups/96335
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*