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. 7/ 2019 LUGLIO/AGOSTO 2019

AIIC (Associazione Italiana esperti in Infrastrutture critiche)

Da una situazione potenzialmente pericolosa ad un disastro, ovvero… la storia non insegna mai

Concentrare l'attenzione sulla ricerca delle cause immediate che hanno originato un incendio non serve se lo scopo che ci muove è la prevenzione; è fin troppo chiaro che la causa remota predisponente, sia che ci sia intenzionalità dolosa, sia che ci siano state trascuratezze più o meno gravi ed in ogni caso colpose, è la situazione pericolosa che si realizza quando vengono affidati lavori più o meno impegnativi di restauro o ristrutturazione cioè **interventi lavorativi in appalto**.
Perché?

a) Perché in un ambiente "particolarmente delicato" intervengono estranei
b) Perché le imprese sono capaci di portare a lavorare chiunque, anche personale non formato sulle norme basilari di prevenzione incendi
c) Perché in ogni caso in un ambiente che non è casa loro ne diventano gli esclusivi utilizzatori per un determinato periodo
d) Perché, anche se è rigorosamente vietato, gli operai fumano
e) Perché, quando lavorano più imprese, si offre occasione ad un possibile danneggiatore di intervenire senza essere facilmente scoperto
f) Perché si lavora a prevenzioni ordinarie sospese e non si ritiene mai ripagata la prevenzione straordinaria che sarebbe necessario attivare
g) Perché vi è sempre una abbondanza di materiale combustibile ed una abbondanza di fonti di ignizione
h) Perché l'ordine degli ambienti di lavoro e la pulizia non sono mai giornalieri ma riservati a poco prima della consegna dei singoli lotti di lavorazione
i) Perché è il meccanismo stesso dell'affidamento dell'appalto con gara al ribasso che seleziona le imprese più spregiudicate e più propense a rischiare in campo altrui.
j) Perché il committente che si vuole togliere di dosso alcuni rischi non comprende sufficientemente che gli rimane la responsabilità della maggior parte dei rischi del personale al lavoro oltre al rischio, in corso d'opera, di una mancata funzionalità delle attività adiacenti e di una parziale funzionalità dell'opera consegnata mai compensata a sufficienza da penalità contrattuali.

Chi si deve adeguatamente preoccupare nella **situazione pericolosa di interventi lavorativi in appalto** è in primo luogo il committente. Dovrà attivare **misure preventive** adeguate ai rischi valutati e non venire mai meno alla sua responsabilità "in eligendo" ed "in vigilando".
Classici esempi, che hanno ormai fatto storia ma che dopo qualche tempo vengono dimenticati sono, oltre al recente incendio che ha semidistrutto la Cattedrale di Notre Dame a Parigi, l'incendio della

Basilica di San Paolo Fuori le mura a Roma del luglio 1823 e l'incendio della Cappella della Sindone e di un'ala dell' attiguo Palazzo Reale a Torino dell'11 aprile 1997.

Leo Poggi

Ing. Leo Poggi, socio AIIC, è professore a contratto di Valutazione del Rischio presso Università Campus Bio-medico di Roma. E' stato Responsabile del Servizio di Prevenzione e Protezione del Policlinico Universitario Campus Bio-Medico.

(l'articolo completo si trova al link https://www.infrastrutturecritiche.it/category/documenti/pubblicazioni-aiic/)

ATTIVITA' DELL'ASSOCIAZIONE

ASSEMBLEA ORDINARIA DEI SOCI AIIC IL 25 GIUGNO 2019

Il giorno 25 giugno 2019 alle ore 17.50 presso l'aula magna del Dipartimento di Ingegneria dell'Università di Roma TRE, si è svolta, in seconda convocazione, l'assemblea ordinaria dei soci con all'ordine del giorno l'approvazione del bilancio consuntivo 2018 e preventivo 2019 e varie ed eventuali.

Erano presenti i soci: Luisa Franchina, Alberto Traballesi, Glauco Bertocchi, Sandro Bologna, Priscilla Inzerilli, Silvano Bari, Bruno Carbone, Luigi Carrozzi, Maurizio Fratini, Leo Poggi, Angelo Socal, Stefano Panzieri

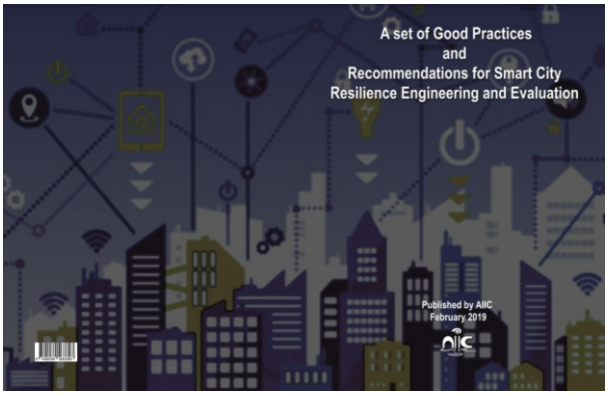
Dopo il saluto ai partecipanti da parte del Presidente Luisa Franchina, il tesoriere Glauco Bertocchi ha illustrato il bilancio consuntivo 2018 e quello preventivo 2019.
In particolare si rileva per l'anno 2018 una piccola perdita d'esercizio, leggermente inferiore rispetto all'anno precedente, dovuta principalmente alle spese fisse di segreteria.
Per quanto riguarda il bilancio preventivo, l'obiettivo per il 2019 sarà quello di raggiungere il pareggio tra entrate e spese fisse (costituite da segreteria, commercialista e costi di gestione): si è già proceduto alla rinegoziazione delle spese fisse di segreteria, riducendone l'importo, ed anche alla rinegoziazione della parcella del commercialista con una riduzione del 25%.
Al termine della presentazione sia il bilancio consuntivo 2018 che quello preventivo 2019 sono stati approvati alla unanimità.

Al termine delle votazioni, si è svolta una ampia discussione sulle opportunità e sulle modalità di coinvolgimento dei soci in modo da favorire la conferma degli attuali associati ed anche di stimolare nuove adesioni.
A tale scopo viene dato mandato al Consigliere Silvano Bari di creare un gruppo di lavoro composto da soci con il compito di individuare quali sono le aspettative nei confronti dell'Associazione, i servizi che i soci si attendono e quali sono i miglioramenti che potrebbero garantire una migliore fidelizzazione ed incremento del corpo associativo, sfruttando anche le possibilità offerte dal nuovo statuto.

Inoltre verrà verificata la possibilità di concedere crediti formativi ai soci che partecipano ai workshop organizzati o patrocinati da AIIC, in particolare il Presidente contatterà in merito l'Ordine degli Ingegneri.

COLLOQUIA SU "SMART CITY RESILIENCE"

L'assemblea del 25 giugno 2019 è stata preceduta da un Colloquia dove sono stati presentati i risultati del GDL AIIC sulle Smart City, coordinato da Sandro Bologna e composto da Glauco Bertocchi, Sandro Bologna, Luigi Carrozzi, Donato Di Ludovico, Donatella Dominici, Priscilla Inzerilli, Luisa Franchina, Alberto Traballesi.
Dopo la presentazione del coordinatore Sandro Bologna si è assistito all'intervento dell'ing. Mauro Annunziato (ENEA), tra i massimi esperti nazionali del tema oggetto del GdL. sui giusti compromessi necessari tra innovazione tecnologica, resilienza, privacy, GDPR, AI.



Alla fine del Colloquia è stata distribuita ai soci la relativa pubblicazione "Smart City Resilience".

Si ricorda che i soci possono ritirare la pubblicazione in oggetto presso la segreteria AIIC, in via Palestro 95, Roma, mentre il documento in formato PDF è scaricabile al link https://www.infrastrutturecritiche.it/a-set-of-good-practices-and-recommendations-for-smart-city-resilience-engineering-and-evaluation-2019/

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

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

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi ed autonomi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

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

NEWS E AVVENIMENTI

Sicurezza dei pagamenti, Swift e blockchain a confronto I possibili utilizzi della blockchain nell'ambito della gestione dei pagamenti transfrontalieri potrebbe porre fine al monopolio del sistema Swift. Molte banche stanno avviando progetti per valutarne le applicazioni e diverse sono le startup attive. Un confronto tra i due sistemi e i possibili scenari

L'infrastruttura critica del sistema finanziario attraversa una fase caratterizzata da profonde trasformazioni e innovazioni dal punto di vista tecnologico. Ciò comporta lo sviluppo di nuove potenziali vulnerabilità a minacce cibernetiche sempre più sofisticate.

Diversi incidenti cyber di alto profilo hanno recentemente riguardato in particolare il sistema dei pagamenti internazionali, scuotendo la comunità finanziaria globale e stimolando nuove iniziative per rafforzare l'integrità dei relativi apparati di sicurezza.

Accanto al modello di gestione dei pagamenti digitali internazionali oggi più diffuso e utilizzato, ossia lo standard di messaggistica finanziaria denominato SWIFT, è emerso negli ultimi anni un approccio innovativo di tipo peer-to-peer basato sulla tecnologia blockchain…..

https://www.agendadigitale.eu/sicurezza/sicurezza-dei-pagamenti-swift-e-blockchain-a-confronto/

Agenda Digitale *G. Carlomagno -L. Franchina 17 Giugno 2019*

5G, il dilemma dell'Europa nel fuoco incrociato Usa-Cina E' conveniente per l'Europa sbarrare le porte al 5G cinese? E quali sarebbero i costi di una eccessiva dipendenza da Pechino? La Ue alle prese con la difficile sfida di bilanciare la necessità di sicurezza e di restare amici degli Usa con quella di tenere il passo con una tecnologia cruciale per il futuro

La competizione tra Stati Uniti e Cina si gioca sempre più nella sfera digitale e l'Europa rischia di rimanere intrappolata nel fuoco incrociato, senza neanche un piano B. Mentre deve seriamente considerare se liberarsi di tutti i fornitori cinesi di 5G sia realistico e conveniente, l'Europa deve anche riflettere sui costi strategici a lungo termine di diventare dipendenti dalla tecnologia 5G cinese. L'Europa, soprattutto, dovrebbe adottare un approccio più strategico e fare fronte comune nei confronti della Cina in generale, per meglio proteggere le risorse e le infrastrutture critiche. Il comunicato dell'Unione europea sulle relazioni UE-Cina è un buon inizio, ma non avrà un grande valore se ogni paese alla fine si muoverà per la propria strada…..

https://www.agendadigitale.eu/infrastrutture/5g-il-dilemma-delleuropa-nel-fuoco-incrociato-usa-cina/

Agenda Digitale*- Enrico Martini, 19 Giu 2019*

Perché Libra è un campanello d'allarme per le banche (e la politica). Parla Damiani

Conversazione di Formiche.net con il professor Ernesto Damiani, presidente del Cini, il Consorzio Interuniversitario Nazionale per l'Informatica Con Libra, Facebook "ha fatto una scommessa: creare un proprio ambito economico in cui può sia operare direttamente come fornitore di servizi, generando ricavi senza costi finanziari per gestire i pagamenti, sia estrarre valore dal funzionamento stesso del sistema attraverso il costo per transazione".Un progetto che – spiega a *Formiche.net* il professor Ernesto Damiani, presidente del Cini, il Consorzio Interuniversitario Nazionale per l'Informatica – potrebbe avere risvolti positivi, soprattutto per gli utenti, ma che, allo stesso tempo, rappresenta un campanello d'allarme per la politica ma soprattutto per le banche, che non possono "combatterlo frontalmente", ma debbono "invece parteciparvi da protagonisti, per tutelare se stesse e la propria clientela". Ecco perché. Professor Damiani, in un momento in cui le Big Tech sono al centro

del dibattito pubblico, Facebook decide di lanciare Libra, che attira ancora di più i timori di chi crede che i colossi del Web stiano accentrando nelle loro mani troppo potere. Come valuta questa lettura?
Se fossi un politico o un banchiere centrale, la creazione di un grande ambito economico internazionale a cui corrisponde una stablecoin sotto il controllo di un'autorità non bancaria – un'operazione molto diversa dallo spirito "democratico" originale delle criptovalute come Bitcoin – non mi farebbe dormire sonni tranquilli. Ma ci vedo lati positivi…….
https://formiche.net/2019/06/libra-facebook-cripto-pagamenti-banche-politica-damiani-cini/
FORMICHE -*Michele Pierri 20/06/2019*

Allarme smartphone in azienda, il bersaglio mobile scatena gli hacker - I telefonini sono ormai veri e propri centri di aggregazione e condivisione di dati, video, messaggi, informazioni critiche di ogni forma e dimensione. Tra le mani, nelle nostre borse abbiamo da tempo veri e propri hub capaci di affrontare e gestire, in tempo reale, operazioni e processi di business spesso di valore incalcolabile. Transazioni bancarie, condivisione di progetti e informazioni riservate o ancora DB clienti. Gli smartphone sono il nuovo centro di gravità permanente del business. Un centro di gravità che sta attirando con una forza irresistibile anche e soprattutto le attenzioni del cybercrime. Il motivo è semplice, da una parte c'è lo scenario appena descritto, dall'altra c'è una percezione del rischio mai così bassa e poco rilevante per manager e utenti. Impariamo ad usarli nella nostra vita personale, impariamo ad affidare loro le foto, i nomi, i volti dei nostri familiari e, allo stesso modo, al momento di varcare la soglia del nostro ufficio pretendiamo di affidare loro tutta la nostra vita lavorativa, nessuno escluso. Una tenenza inarrestabile su cui da tempo il Clusit ha lanciato un allarme preciso "gli utenti mobile sono percentualmente molto più propensi a cadere nelle truffe digitali come phishing, ransomware e hanno contribuito in maniera decisiva nel fare del 2018, e della prima parte del 2019, l'anno peggiore di sempre a livello di attacchi e danni che il cybercrime ha fatto alle imprese italiane. La situazione insomma è seria e i casi di imprese messe al tappeto da attacchi andati a buon fine, sfruttando soprattutto, le vulnerabilità dei device mobili, continuano a susseguirsi.
https://www.impresacity.it/news/21842/allarme-smartphone-in-azienda-il-bersaglio-mobile-scatena-gli-hacker-come-difendersi.html
ImpresaCity *– 20 giugno 2019*

Cybersecurity nel settore energetico, ecco le raccomandazioni della Commissione europea
Garantire la sicurezza delle reti energetiche è uno degli obbiettivi chiave della strategia Ue per la sicurezza cibernetica. Per questo la Commissione europea ha formulato alcune specifiche raccomandazioni sulle misure in materia di cybersecurity che i gestori di reti energetiche dovrebbero adottare.
Il processo di transizione verso le fonti rinnovabili sta comportando grandi cambiamenti nel settore energetico, tra cui la trasformazione delle reti elettriche in "smart grid", ovvero in "reti elettriche intelligenti" integrate con infrastrutture ICT che consentono di gestire in maniera efficiente e decentrata la produzione e la distribuzione di energia elettrica. Questa trasformazione comporta però anche nuovi rischi, visto che la digitalizzazione delle reti elettriche le espone a possibili attacchi ed incidenti informatici che possono compromettere la sicurezza energetica nazionale ed europea. Alcuni dei rischi informatici a cui sono esposte "le reti elettriche intelligenti" sono specifici del settore energetico. Ad esempio, alcune componenti delle smart grid devono operare in tempo reale, eseguendo i comandi in pochi millisecondi, il che rende quasi impossibile, per mancanza di tempo, l'applicazione di misure di sicurezza informatica standard come la cifratura delle connessioni. Le

principali minacce ed i rischi cibernetici a cui è esposto il settore energetico sono state riassunte in uno studio commissionato dalla Commissione europea e pubblicato nel 2018……
https://www.agendadigitale.eu/infrastrutture/cybersecurity-nel-settore-energetico-ecco-le-raccomandazioni-della-commissione-europea/
Agenda Digitale *- Luca Tosoni 21 Giu 2019*

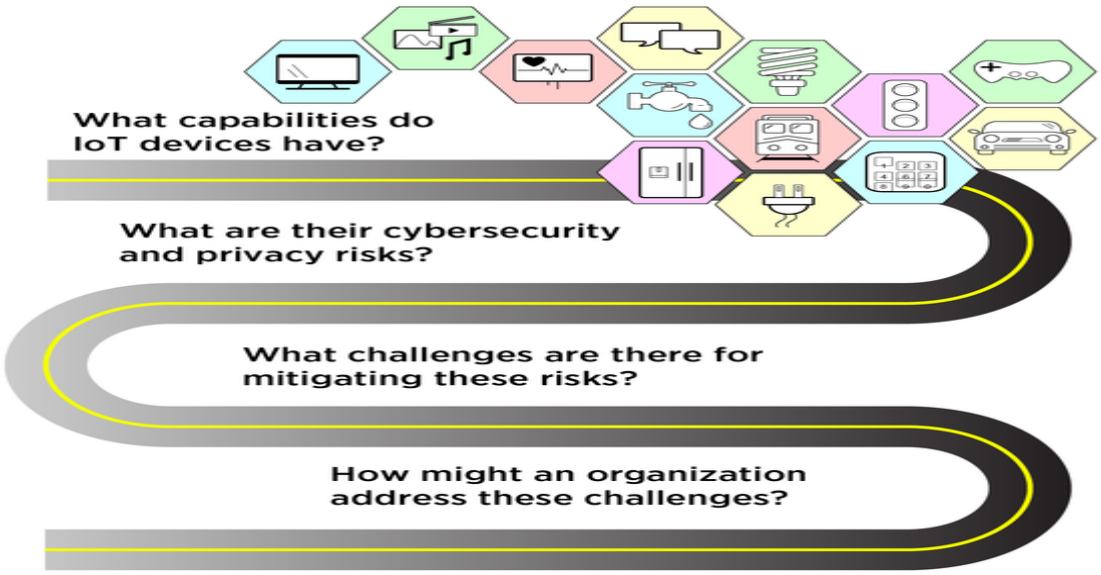
US DHS CISA warns of Iran-linked hackers using data wipers in cyberattacks . The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning of a significant increase in cyberattacks from Iranian hackers spreading data wipers.
US DHS CISA agency warns of increased cyber-activity from Iran aimed at spreading data-wiping malware through password spraying, credential stuffing, and spear-phishing.
The attacks are targeting U.S. industries and government agencies, the statement was also published by the CISA Director Chris Krebs via his Twitter account……The statement warns of targeted attacks carried out by the Iranian affiliated actors that leverage data-wiper specifically designed to permanently destroy data of infected systems. Wiper attacks have been used in the past by state actors or as decoys for other attacks, which are described later in the article. Experts recommend to have secure working backup procedures, in case of attack, victims could simply recover data from a backup. The statement also highlights the risks related to account compromise that could represent the entry point in a targeted network……..
https://securityaffairs.co/wordpress/87500/apt/cisa-warns-data-wipers.html
Security Affairs -*Pierluigi Paganini, June 24, 2019*

Silex malware bricks thousands of IoT devices in a few hours . Security experts warn of a new piece of the Silex malware that is bricking thousands of IoT devices, and the situation could rapidly go worse. Akamai researcher Larry Cashdollar discovered a new piece of the Silex malware that is bricking thousands of IoT devices, over 2,000 devices have been bricked in a few hours and the expert is continuing to see new infections. Cashdollar explained that the Silex malware trashes the storage of the infected devices. The only way to recover infected devices is to manually reinstall the device's firmware. Silex is not the first IoT malware with this behavior, back in 2017 BrickerBot bricked millions of devices worldwide.
According to ZDnet that interviewed the malware's creator, the attacks are about to intensify in the coming days…..
https://securityaffairs.co/wordpress/87609/iot/silex-malware-bricks-iot-devices.html
Security Affairs -*Pierluigi Paganini, June 26, 2019*

Operation Soft Cell – Multiple telco firms hacked by nation-state actor. Operation Soft Cell – Experts at Cybereason discovered that China-linked hackers have breached numerous telco providers controlling their networks. Researchers at Cybereason uncovered an ongoing long-running espionage campaign, tracked as Operation Soft Cell, that targets telco providers. Tactics, techniques, and procedures, and the type of targets suggest the involvement of a nation-state actor likely linked to Chinese APT10. Once compromised the networks of telecommunication companies, attackers can access to mobile phone users' call data records.
"Based on the data available to us, Operation Soft Cell has been active since at least 2012, though some evidence suggests even earlier activity by the threat actor against telecommunications providers. The attack was aiming to obtain CDR records of a large telecommunications provider." reads the report

published by Cybereason. "The threat actor was attempting to steal all data stored in the active directory, compromising every single username and password in the organization, along with other personally identifiable information, billing data, call detail records, credentials, email servers, geo-location of users, and more."……
https://securityaffairs.co/wordpress/87599/hacking/operation-soft-cell-telco-hack.html7
Security Affairs -*Pierluigi Paganini, June 26, 2019*

NIST - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks – The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. Many organizations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may affect cybersecurity and privacy risks differently than conventional information technology (IT) devices do. The purpose of this publication is to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' lifecycles. This publication is the introductory document providing the foundation for a planned series of publications on more specific aspects of this topic.



https://www.nist.gov/news-events/news/2019/06/connecting-iot-device-check-out-new-nist-report-cybersecurity-advice
NIST (National Institute of Standards and Technology) *– june 27, 2019*

L'Europa pensa a "blindare" il cloud: Google&co. potrebbero non avere più vita facile - Le aziende europee temono una crescita del cyber-rischio per i loro dati e, mentre si affidano in misura crescente al *cloud computing* e ai grandi fornitori americani, si premuniscono cifrando il loro patrimonio di informazioni tramite provider europei della *cyber-sicurezza*. Lo ha fatto, per esempio, Veolia Environnement, la utility francese dell'acqua, chiedendo a Atos di cifrarle tutti i dati prima di metterli nel cloud di Google, o ancora la banca francese Societé Generale che usa i servizi dell'olandese Gemalto per mettere in sicurezza i suoi dati spostati sul cloud. È un trend incoraggiato dagli stessi governi e regolatori: in Francia il vice-ministro dell'Economia Agnes Pannier-Runacher ha detto che le

imprese che cedono il controllo dei loro dati pongono un "rischio sistemico", mentre in Germania la Banca centrale ha messo in guardia gli istituti finanziari del paese e dell'Europa intera sulla necessità di un monitoraggio più severo del settore finance perché molti player stanno spostando i dati sul cloud. Queste preoccupazioni si legano alle tensioni geopolitiche e alla guerra commerciale Usa-Cina: i maggiori provider del cloud sono o americani (Amazon, Microsoft, Google, Ibm) o cinesi (Alibaba) …..
https://www.corrierecomunicazioni.it/digital-economy/cloud/aziende-europee-piu-garanzie-su-dati-cloud/
CorCom (Corriere Comunicazioni) *– Patrizia Licata – 28 giugno 2019*

Cloud Hopper operation hit 8 of the world's biggest IT service providers. A long-running operation carried out by China-linked hackers, and tracked as Cloud Hopper, has targeted clients of major companies, including IBM, HPE, Tata CS, Fujitsu, and NTT.
Hackers broke into the internal networks on major companies, such as HPE and IBM, and stole corporate data and trade secrets. Then the attackers used the stolen information to target into customer systems.
The list of victims is long and includes tech giants like HPE, IBM, DXC, Fujitsu, and Tata.
"Teams of hackers connected to the Chinese Ministry of State Security had penetrated HPE's cloud computing service and used it as a launchpad to attack customers, plundering reams of corporate and government secrets for years in what U.S. prosecutors say was an effort to boost Chinese economic interests." reads a report published by the Reuters agency.
"The hacking campaign, known as "Cloud Hopper," was the subject of a U.S. indictment in December that accused two Chinese nationals of identity theft and fraud. Prosecutors described an elaborate operation that victimized multiple Western companies but stopped short of naming them. A Reuters report at the time identified two: Hewlett Packard Enterprise and IBM."…….
https://securityaffairs.co/wordpress/87691/apt/cloud-hopper-service-providers.html
Security Affairs -*Pierluigi Paganini, June 28, 2019*

Decoding America's spies: What does the NSA's cryptic memo really mean? Citizens illegally spied on again The NSA illegally gathered a trove of American citizens' phone and text message records just four months after it promised it had taken steps to literally not do that again.
That's the upshot of a document [PDF] provided to the American Civil Liberties Union (ACLU) and made public this week. The dossier was supplied by the NSA in response to a long-running legal challenge brought by the civil-rights warriors, who ultimately want Section 215 of the USA Patriot Act, which grants spying powers to Uncle Sam's snoops via secret courts, ruled as unconstitutional. There are very few details given about the illegal data harvesting, and the vast majority of the document supplied to the ACLU following a Freedom of Information Act (FOIA) request is redacted. The file is one of a series of quarterly reports produced by the surveillance super-agency for an intelligence oversight board in the United States. What we do know is that the data slurp happened back in October 2018, that it was the 24th issue of 2018 on which a report was written, and that the NSA didn't inform the Department of Defense's senior intelligence oversight official about it until February 1, 2019. This week is the first time anyone outside the intelligence community, and whichever company wrongly sent people's personal information to Uncle Sam's snoops, became aware of the issue……
https://www.theregister.co.uk/2019/06/26/nsa_spy_program_aclu/
The Register *-Kieren McCarthy, 26 June 2019*

Scumbags can program vulnerable MedTronic insulin pumps over the air to murder diabetics – insecure kit recalled Not a particularly sweet ending to the week. Health implant maker MedTronic is recalling some of its insulin pumps following the discovery of security vulnerabilities in the equipment that can be exploited over the air to hijack them. Specifically, the manufacturer is recalling its MiniMed 508 and Paradigm insulin pumps, along with the CareLink USB control hub and some blood glucose monitoring devices used with the at-risk gear. America's medical drug watchdog the FDA also issued an alert this week over the holes, which can be leveraged by nearby hackers to execute commands on the pumps.
These commands can, for instance, tell the pump to inject too much insulin, causing the patient to suffer hypoglycemia and pass out or enter a seizure, or too little insulin and cause the patient to develop serious life-threatening ketoacidosis. It's a bizarre way to kill someone right by you, of course, when hitting them over the head with a wrench will do it, but you never know…..
https://www.theregister.co.uk/2019/06/28/medtronic_insulin_pump_recall/
The Register -*Shaun Nichols, 28 June 2019*

Dalle bombe ai cyber attacchi. La minaccia terroristica alle infrastrutture critiche in Italia. Dal dopoguerra ad oggi l'Italia è sempre stata al centro di numerosi eventi terroristici che ne hanno segnato la storia. Siano stati di matrice interna o esterna, questi, ora condotti anche nel cyberspace, hanno spesso interessato le infrastrutture critiche nazionali. **La Storia.** Uno dei primi e più noti esempi è quello della Notte dei fuochi, ovvero la notte tra l'11 e il 12 giugno 1961, quando un gruppo di terroristi sudtirolesi, aderenti al Befreiungsausschuss Südtirol, movimento che si batteva per l'autodeterminazione dell'Alto Adige, compì numerosi attentati dinamitardi che abbatterono numerosi tralicci della rete di alta tensione, creando molti disagi nell'area. Nel passato le infrastrutture critiche sono state oggetto di attacchi anche da gruppi terroristici internazionali,…… **La Minaccia Oggi.** Oggi la minaccia alle infrastrutture critiche nazionali è più viva che mai. Gli attori interessati capaci di attaccare i centri nevralgici del Sistema Paese sono numerosi, così come i vettori di attacco che spaziano dall'ordigno esplosivo rudimentale al cyber attacco condotto con le più recenti tecniche cibernetiche……..
https://formiche.net/2019/06/minaccia-terrorismo-italia/
Le Formiche - *Domenico Vecchiarino, 29/06/2019*

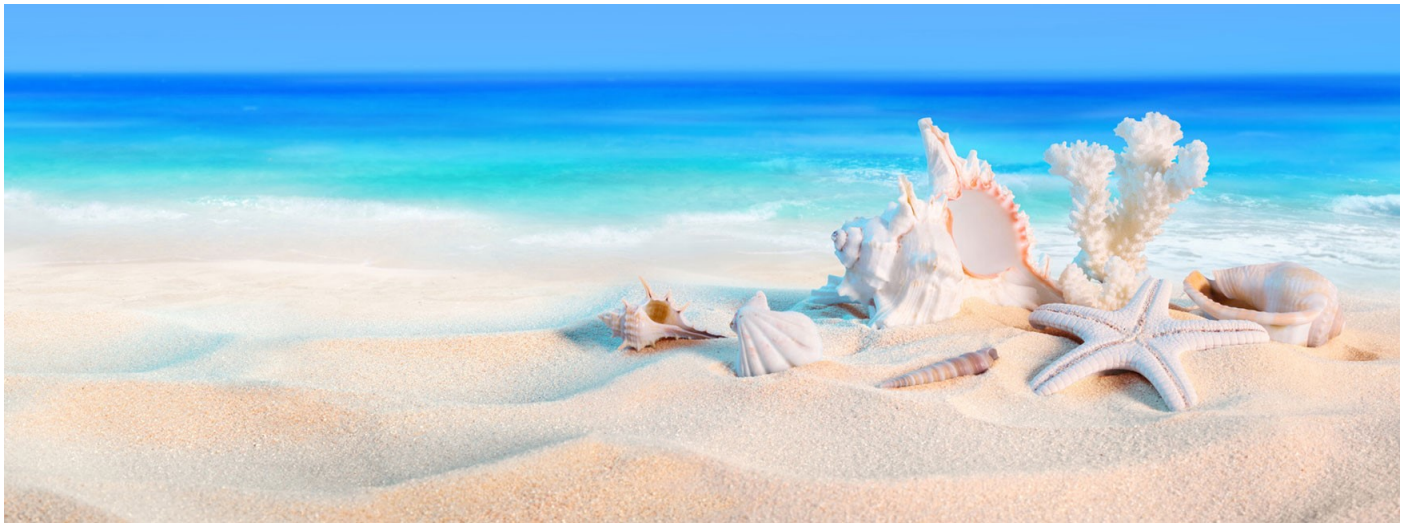
Voto elettronico mediante blockchain - B**lockchain** sta diventando sempre più una buzzword per applicazioni che spaziano dalla finanza, alla logistica e la cyber security. Distinguere le potenzialità della tecnologia dalle semplici illusioni è però critico quando si propone di utilizzarla per il voto elettronico**.** Può essere opportuno analizzare vantaggi e svantaggi di soluzioni digitali per un problema critico come la gestione di una elezione unicamente mediante strumenti informatici. Una premessa fondamentale è che anche il sistema di voto su carta che molti ritengono superiore, offriva inizialmente un livello di sicurezza basso ed è stato migliorato in corso d'opera.
Prima di discutere i potenziali vantaggi di una soluzione basata su blockchain è opportuno premettere alcune considerazioni sulla tecnologia e sulle specifiche soluzioni. Una prima considerazione, a prima vista banale ma spesso dimenticata, è che nessuno Stato, nessuna Regione può accettare che le sue elezioni siano sotto il controllo di un insieme di persone sconosciute. Questo elimina immediatamente tutte quelle soluzioni che propongono di inserire i voti, criptati o no, sulla blockchain di una qualche moneta elettronica. Ad esempio, una qualunque soluzione che usi la blockchain di Bitcoin 13, ha tempi di voto e di calcolo dei risultati non certi che dipendono dal comportamento e dalle convenienze di un

insieme di miner. Inoltre, uno Stato potrebbe interferire con un altro semplicemente utilizzando parte delle sue risorse ICT per ritardare le votazioni producendo nuovi blocchi da inserire nella blockchain. Infine, anche i più strenui sostenitori di e-vote mediante blockchain ammettono che il consumo di energia richiesto da una votazione nazionale sarebbe del tutto improponibile…….
https://www.agendadigitale.eu/documenti/voto-elettronico-mediante-blockchain-problemi-e-possibili-soluzioni/
Agenda Digitale *– Fabrizio Baiardi – 29 giugno 2019*

PROSSIMI EVENTI

Con questo numero la newsletter AIIC va in vacanza. Ci rivedremo a settembre 2019.
Buone vacanze a tutti!

Il Comitato di Redazione



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/

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

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 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*