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 2020	N. 05/ 2020	Maggio 2020

Cambiare tutto per non cambiare niente?

Confessiamolo, questo attuale è stato (e continua ad essere) un periodo di dura emergenza in cui si sono manifestate molte ombre ma fortunatamente anche parecchie luci.
Per quanto riguarda l'infrastruttura sanitaria, l'informatica è corsa in aiuto, avviando numerose attività come risposta al COVID-19: si stanno utilizzando tecniche di Big Data Analytics e di Intelligenza Artificiale per prevedere e gestire richieste di posti letto in terapia intensiva, complicanze mediche, immaginare scenari di medio/lungo periodo e per identificare potenziali trattamenti farmacologici. Ma si stanno sviluppando anche applicazioni per il tracciamento dei contagi tramite tecnologie bluetooth (con conseguenti problemi di privacy e sicurezza), per rispondere in modo più efficace ed efficiente alle numerose richieste di informazioni (permettendo così al personale medico ed amministrativo di dedicarsi alle attività più pressanti), per fornire canali informativi agli utenti sui comportamenti da adottare in caso di sospetta infezione. E potremmo citare anche l'utilizzo di tecniche di matchmaking per avviare nuove collaborazioni nel campo della ricerca medica, ed un maggior ricorso a strumenti di telemonitoraggio per registrare in modalità wireless i parametri vitali dei pazienti in quarantena e tenerli così in osservazione senza affollare le strutture di ricovero.
Nel contempo, i criminali informatici non hanno avuto pietà ed hanno approfittato della situazione di emergenza attaccando le strutture sanitarie già in difficoltà e sfruttando il panico dovuto alla diffusione del coronavirus: si sono continuati a verificare, anzi sono addirittura aumentati i furti di informazioni, la diffusione di ransomware, le e-mail di phishing e la divulgazione di fake-news.
Ma anche in altri campi ci si è dati da fare: in campo lavorativo i webinar, fino a poco tempo fa abbastanza snobbati, ora impazzano in rete mentre si è "scoperto" che – dopo tutto – il telelavoro (il cosiddetto "smart working") consente, in molti casi, di lavorare da casa aumentando addirittura la produttività; alla chiusura dei siti scolastici e universitari si è risposto attivando lezioni on-line ed esami telematici, contribuendo così alla felicità dei produttori di webcam e microfoni.
In altri campi, anche qui notizie positive e meno. Se l'emergenza coronavirus non ha bloccato i lavori del ponte di Genova, che dopo poco più di un anno ha visto completate le sue parti strutturali più importanti, purtuttavia i ponti continuano a crollare, ultimi a citare quello sul fiume Magra (al confine Toscana-Liguria) e quello meno noto in Sardegna a Gonnesa (Sulcis).

Insomma, luci ed ombre. Si dice che ci aspetterà un futuro nuovo, in cui nulla sarà più come prima: i più anziani (tra cui il sottoscritto) forse si considerano più ottimisti, dopo aver conosciuto nel corso della loro vita le varie emergenze sanitarie, dovute alla poliomielite (ormai dimenticata), alle influenze aviarie e suine, all'aids, alla "mucca pazza" e quant'altro: cosa ci hanno lasciato come insegnamento? Sarebbe troppo facile rispondere in modo banale.

Il Presidente della Repubblica, in uno dei suoi recenti discorsi, ha auspicato che si usi la battuta d'arresto che stiamo soffrendo "per accelerare la strada verso un cambiamento che sappia valorizzare e non subire fenomeni come la globalizzazione e la digitalizzazione dell'economia con scelte lungimiranti".

Insomma, l'augurio è che – se è proprio vero che il nostro modo di vita dovrà cambiare – il cambiamento si verifichi in meglio e non si riduca invece – come spesso succede – in un "cambiare tutto per non cambiare niente" di gattopardesca memoria.

Silvano Bari
Vicepresidente AIIC, Professore a contratto di "Valutazione del Rischio" presso l'Università "Campus Bio-medico di Roma".

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2020

Si ricorda a tutti i soci che il 31 dicembre 2019 è scaduto il periodo associativo. Invitiamo tutti i soci a rinnovare per tempo 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 Intesa Business, Coordinate bancarie IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando "rinnovo socio ordinario nome e cognome anno 2020".

Per i nuovi iscritti l'importo da pagare è di € 60,00 mentre per i soci attuali la quota di rinnovo rimane sempre fissata a € 40,00. 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 2020. 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.

Attività del Gruppo di lavoro

Il Gruppo di Lavoro. "**Internet of Things (IoT) in the context of Critical Infrastructures: Cybersecurity and Privacy concerns and possible solutions**" ha iniziato la sua attività ed ha svolto riunioni nei mesi di novembre, dicembre e febbraio 2020. Poi, per l'emergenza Covid 19, i contatti sono proseguiti via e-mail. Il Gdl è coordinato da Sandro Bologna e vede la partecipazione dei soci: Silvano Bari, Glauco Bertocchi, Luigi Carrozzi, Luisa Franchina, Francesco Ressa, Angelo Socal, Alberto Traballesi è nella fase di revisione finale del rapporto.

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.

NEWS E AVVENIMENTI

Gestione dati personali durante le emergenze: perché servono nuove norme. La diffusione del coronavirus dimostra quanto sia assurdo che i dati prodotti dai nostri dispositivi digitali, che sarebbero un grande aiuto alle capacità di affrontare un'emergenza sanitaria, non siano nella disponibilità anche degli enti preposti a tutelare la nostra salute. Le norme vanno cambiate in questa direzione…
https://www.agendadigitale.eu/sicurezza/privacy/gestione-dati-personali-durante-le-emergenze-perche-servono-nuove-norme/
Agenda Digitale *- Massimo Canducci - 06 Mar 2020*

Energia e digitalizzazione: blockchain per il gas naturale - La Cina è uno dei principali importatori di gas naturale. Il suo consumo sta infatti aumentando costantemente come sostituto di altre forme di energia più inquinanti. Questa evoluzione ha creato un grande mercato interno per il gas naturale. Con un conseguente sviluppo delle infrastrutture. E degli scambi commerciali.
È complesso tracciare tutti i movimenti e le transazioni collegati al gas naturale in Cina. Specie del gas importato dall'estero e che arriva nei parchi industriali cinesi. La soluzione scelta da Shanghai Gas è adottare blockchain come piattaforma affidabile.
Il problema principale affrontato da Shanghai Gas sta nel fatto che, lungo la supply chain del gas naturale, le informazioni sono gestite in maniera molto poco omogenea. Blockchan agisce quindi come tecnologia che armonizza e rende affidabili le informazioni**.**
Nei ledger distribuiti della blockchain "energetica" saranno inizialmente inseriti i dati riguardanti ogni serbatoio che viene riempito. Ad esempio in un porto cinese di destinazione di una nave metaniera. Le informazioni memorizzate riguardano sia il gas in sé, sia il trasporto. Con anche dati raccolti periodicamente sul mezzo di trasporto. Ad esempio via sensori e sistemi di posizionamento GPS…..
È importante notare che il progetto cinese è interessante anche per noi**.** La Cina punta infatti allo sviluppo di un mercato del gas naturale che riguardi tutte le nazioni aderenti alla Belt and Road Initiative. Tra cui c'è appunto anche l'Italia.
All'adozione di blockchain nelle nazioni della Belt and Road Initiative è dedicato un progetto specifico. Battezzato Belt and Road Initiative Blockchain Alliance (BRIBA), è guidato tra l'altro da DNV e dalla Tsinghua University. E usa le tecnologie di VeChain, già adottate anche in Italia……
https://www.impresagreen.it/news/9962/energia-e-digitalizzazione-blockchain-per-il-gas-naturale.html
Impresagreen *– o8 marzo 2020*

La resilienza delle Tlc ai tempi del coronavirus Impennata di connessioni a Internet e del traffico sulle reti fisse e mobili. Le infrastrutture stanno tenendo, ma potranno esserci disservizi. L'emergenza sta dimostrando chiaramente il valore e la strategicità dei network. E si auspica che una volta fuori dal tunnel il governo e la politica mettano finalmente il "dossier reti e digitale" fra le priorità-Paese….
https://www.corrierecomunicazioni.it/telco/la-resilienza-delle-tlc-ai-tempi-del-coronavirus/
Corcom *- Mila Fiordalisi - 11 Mar 2020*

Covid-19 crisis shows fragility of food supply system – Richard Tiffin, chief scientific officer and founder of Reading-based agricultural data firm Agrimetrics, says the Covid-19 public health crisis is revealing the fragility of the global food system. He draws an analogy between the global food system and the financial system. Both are complex systems inherently vulnerable to small shocks and lacking a "single point of understanding". The 2008 financial crash was the catastrophic event that drove Tiffin to form the company of which he is now chief scientific officer.
"Our food system is incredibly interdependent, but ironically it's also incredibly disconnected," he says. "We have no idea of the long-term consequences of events like Covid-19. To avoid collapse, we need to understand these connections."
And so the thesis of the company is more about the resilience of the food system than it is about "feeding the world", says Tiffin…….
Agrimetrics has built a graph database using GraphDB, dubbed a "Data Marketplace", which contains global food system information, and which is intended to be used by companies specialising in artificial intelligence (AI) and application development, and focused on agriculture as an industry……..
https://www.computerweekly.com/news/252481018/Covid-19-crisis-shows-fragility-of-food-supply-system?asrc=EM_EDA_126020900&utm_medium=EM&utm_source=EDA&utm_campaign=20200412_Covid-19%20crisis%20shows%20fragility%20of%20food%20supply%20system
ComputerWeekly *– Brian McKenna – 02 apr 2020*

Coronavirus threats ramp up as more hospitals come under attack - An 85% majority of cyber security professionals have been on the receiving end of some kind of phishing email or scam relating to the Covid-19 coronavirus, but not many seem to be landing, with 80% saying they have not seen any organisational downtime as a result. This is according to a preview of figures to be published later this week by the Covid-19 Cyber Threat Coalition, a group of like-minded security specialists who have banded together to put a stop to cyber criminals exploiting the pandemic.
The newly established movement, which was set up as a Slack channel by Sophos's Joshua Saxe in late March, has seen its membership balloon to more than 3,000 in barely a fortnight. Its members said they are united in their feeling that "extraordinary times call for bridging traditional boundaries to operate with unity and purpose".
More statistics from the informal study will be revealed later in the week, but in the first of what is planned to be a series of weekly threat advisories, the group said that the most common coronavirus threats were credential phishing (33%), scams (30%) and malicious documents (18%).
The group said these results suggested that cyber criminals are taking advantage of standard patterns of attack and have simply rebranded them to take advantage of the crisis. This has been borne out by many reports from various suppliers and industry bodies in recent weeks.
The Covid-19 Cyber Threat Coalition is being supported by a number of organisations, including CloudFlare, GitHub, Nvidia, Slack and Sophos, and is still seeking contributors to join its Slack channel and help push threat intelligence data through an Open Threat Exchange group.

It has already published and is now updating a blocklist of compiled and vetted data on indicators that it believes criminal groups are using to go after their targets……..
https://www.computerweekly.com/news/252481298/Coronavirus-threats-ramp-up-as-more-hospitals-come-under-attack?src=6106743&asrc=EM_ERU_125947938&utm_medium=EM&utm_source=ERU&utm_campaign=20200409_ERU%20Transmission%20for%2004/09/2020%20(UserUniverse:%20749422)&utm_content=eru-rd2-rcpB
ComputerWeekly *- Alex Scroxton – 8 apr 2020*

Coronavirus: Zoom restricted or banned at multiple organisations - Organisations around the world are moving to lock down or ban remote workers from using videoconferencing and collaboration application Zoom during the Covid-19 coronavirus pandemic. This comes as concerns about the fundamental security of the service refuse to go away despite repeated attempts by Zoom to assuage them. Among the organisations imposing restrictions on Zoom usage is Google, which has banned it from all its employees' devices, citing security vulnerabilities.
In a statement supplied to *Buzzfeed News*, which first reported the story, Google spokesperson Jose Castaneda said Google had a longstanding policy of not allowing employees to use unapproved apps for work. "Our security team informed employees using Zoom Desktop Client that it will no longer run on corporate computers as it does not meet our security standards for apps used by our employees," said Castaneda. "Employees who have been using Zoom to stay in touch with family and friends can continue to do so through a web browser or via mobile."
Other organisations to have cracked down on Zoom include the US Senate and the German government…….
https://www.computerweekly.com/news/252481432/Coronavirus-Zoom-restricted-or-banned-at-multiple-organisations?asrc=EM_EDA_126176870&utm_medium=EM&utm_source=EDA&utm_campaign=20200414_Coronavirus:%20Zoom%20restricted%20or%20banned%20at%20multiple%20organisations
ComputerWeekly – *Alex Scroxtron – 09 apr 2020*

Crolla un ponte sul fiume Magra: informazioni e video Crolla un altro viadotto. Si tratta di un ponte di circa 270 metri sulla strada provinciale 70, in località Albiano, sul fiume Magra al confine tra Liguria e Toscana. e collega la Sp70 con a Sp62.
L'opera, unitamente a tutta l'arteria, è entrata in gestione ad Anas a novembre del 2018, a seguito dell'emanazione del DPCM 20 febbraio 2018, recante una revisione complessiva della rete stradale di interesse nazionale e della rete stradale di interesse regionale, in particolare quella toscana. Un'altra strada importante che viene nterrotta…….
https://www.ingenio-web.it/26507-crolla-un-ponte-sul-fiume-magra-informazioni-e-video?utm_term=36799+-+https%3A%2F%2Fwww.ingenio-web.it%2F26507-crolla-un-ponte-sul-fiume-magra-informazioni-e-video&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3483+-+1926+%282020-04-09%29
Redazione INGENIO - *09 aprile 2020*

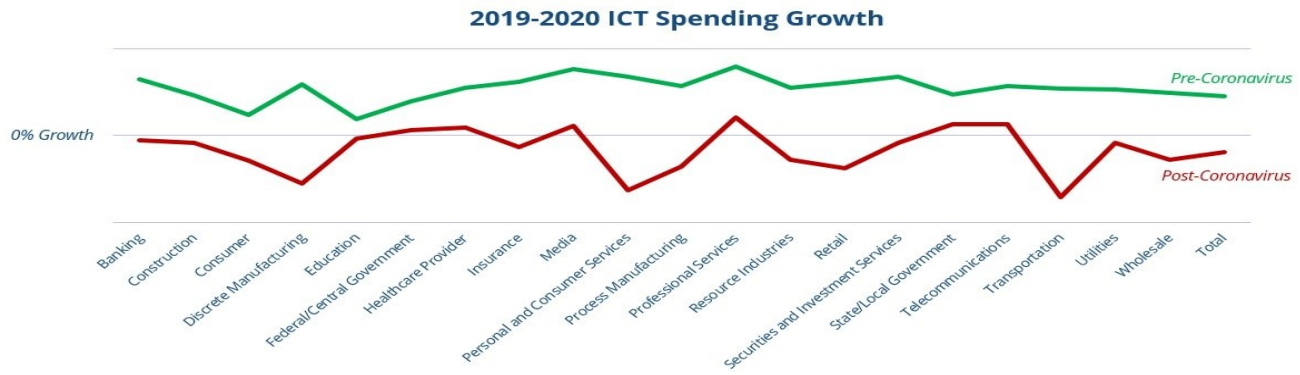
Il phishing al tempo del COVID-19: come difendersi? – Quando si tratta di rischi legati al social engineering e al phishing, gli attacchi che sfruttano COVID-19 rappresentano uno dei maggiori rischi per le organizzazioni di tutto il mondo, indipendentemente dal settore. Già nel febbraio 2020, e con maggiore frequenza a partire da quel momento, Mandiant Threat Intelligence ha osservato che i

Threat Actor si sono orientati sull'argomento COVID-19 per le loro campagne per realizzare crimini finanziari, spionaggio informatico ed operazioni di influenza delle informazioni.
Le organizzazioni del settore privato subiscono sempre più attacchi da parte di criminali informatici motivati da obiettivi finanziari, che cercano di sfruttare il senso di urgenza, paura, solidarietà e la sfiducia. Questi aggressori utilizzano la posta elettronica per diffondere malware nel tentativo di stabilire un punto di accesso alla rete aziendale o sottrarre le credenziali dell'account attraverso tattiche di phishing.
L'email è il principale vettore di attacco e le organizzazioni devono continuare a puntare su una maggiore consapevolezza degli utenti in materia di sicurezza e sull'intensificazione dei controlli tecnici di mitigazione e di rilevamento. Per aumentare la consapevolezza degli utenti, le organizzazioni dovrebbero comunicare i rischi derivanti dalle campagne di phishing e di social engineering COVID-19, fornendo ai dipendenti esempi di cosa osservare con attenzione e di come comportarsi se dovessero imbattersi in tali email.
I responsabili della sicurezza dovrebbero cogliere questa opportunità per ribadire le linee guida sulla consapevolezza della sicurezza, ricordando agli utenti di rimanere vigili sia sulle email di phishing che sui potenziali scenari di frode nei pagamenti. Sia SANS che US CERT forniscono un'importante guida per aumentare la consapevolezza degli utenti, che può essere adottata rapidamente…….
https://www.cwi.it/sicurezza/cybercrimine-hacking/il-phishing-al-tempo-del-covid-19-come-difendersi-127199
Computer World *– Francesco Destri – 09 aprile 2020*

SMART CITY E CYBER SECURITY, UN RAPPORTO SEMPRE PIÙ STRETTO - Tutti speriamo in una veloce digitalizzazione delle nostre città. Una esigenza che in parte è stata acuita dalla pandemia. Abbiamo scoperto in queste settimane che le realtà con un elevato grado di digitalizzazione se la cavano meglio.
Vorremmo che questo si concretizzasse anche per i sistemi e i processi delle città in cui viviamo. Ma la digitalizzazione porta anche nuovi rischi digitali. A partire da quelli di cyber security. Perché una Smart City è potenzialmente un ghiotto boccone per chi è a caccia di informazioni. O magari solo di qualche vittima in più per le sue estorsioni.
La casistica degli attacchi alle realtà pubbliche è già ampia, specialmente Oltreoceano. Mostra una tendenza chiara all'utilizzo di vettori nemmeno troppo sofisticati, come il ransomware. Partendo probabilmente dal presupposto che, più delle imprese, le realtà pubbliche hanno personale meno sensibilizzato rispetto ai pericoli cyber.
Va poi considerato che lo scenario della cyber security in rapporto alle Smart City non è statisticamente del tutto chiaro. Aumentano gli attacchi alle città e alla PA. Ma questo perché c'è un aumento effettivo degli attacchi mirati? O semplicemente perché aumenta la digitalizzazione degli enti pubblici e locali. E quindi la superficie complessiva di attacco? Probabilmente è un insieme dei due fenomeni.
Altro problema da considerare: una Smart City è per forza di cose un ecosistema. Un'azienda no, è un organismo centralizzato. Questa distinzione rende più difficile la protezione delle Smart City. Perché bisogna proteggere molti anelli di più catene - i singoli servizi digitali - che possono essere gestiti da entità distinte. In azienda, quando va bene, c'è un solo dipartimento IT. E al suo interno un Chief Security Officer.
Prendiamo ad esempio, invece, un servizio smart per la gestione della mobilità urbana. E facciamo anche un esempio ideale. Di mobilità urbana multimodale e door-to-door, come dicono i tecnici. Un servizio cioè che consenta al cittadino di pianificare e gestire tutti i suoi spostamenti in città. Da

quando esce di casa a quando arriva alla sua destinazione. Usando sistemi di trasporto differenti, forniti da operatori diversi.
Questo complesso di spostamenti prevede probabilmente servizi di municipalizzate quanto di privati (il car sharing, per dire). E potenzialmente di più fornitori: il car sharing, il bike sharing, e via dicendo. Un servizio integrato - che non è fantascienza, esiste in alcune città - trae dati da tutti i sistemi dei provider coinvolti. Li raccoglie magari in un'app. E idealmente copre in maniera integrata il pagamento di ciascun "vettore" degli spostamenti.
Ecco quindi che un singolo servizio in stile Smart City è fatto da tante IT distinte che collaborano fra loro. E che rappresentano altrettante superfici di attacco. Più una: quella data dalle interazioni fra loro. Perché anche dare per scontata la cyber security di ogni anello della catena non basta a garantire la sicurezza del tutto. Mai come in questo caso l'intero è maggiore della somma delle sue parti. Non è affatto banale garantire la cyber security di sistemi così articolati. …….
https://www.securityopenlab.it/news/402/smart-city-e-cyber-security-un-rapporto-sempre-piu-stretto.html
Securityopenlab *– f.p. – 14 aprile 2020*

IDC: chi investe e chi no nel post-coronavirus – IDC (International Data Corporation) aveva già dato la sua previsione (negativa) per **la** spesa IT mondiale nel 2020. Una spesa in flessione a causa della pandemia da coronavirus. Soprattutto dell'incertezza su tempi e modi in cui le varie nazioni usciranno dalla attuale fase di stallo. Ora gli analisti di IDC cercano di tratteggiare un ritratto più preciso del mercato. Tutti i settori spenderanno meno in IT, quest'anno. Ma per alcuni la minor spesa sarà più contenuta che per altri**.**
Prevedibilmente, spiega IDC, a contenere maggiormente la loro spesa IT saranno i settori più colpiti dalla crisi. Quindi quelli genericamente legati all'ospitalità ed al turismo. Come il settore dei trasporti e quello dei servizi consumer. Qui la flessione della spesa IT sarà superiore al 5%**.** Si tratta però di ambiti relativamente poco importanti per la loro spesa IT. Altri settori investono decisamente di più in IT e saranno comunque impattati dalla crisi. In prima fila il manufacturin**g**, che globalmente muove circa 400 miliardi di investimenti IT. Qui il declino della spesa tecnologica è stimato intorno al 3%**.** Come flessione minima, al momento.
I settori di mercato tradizionalmente resistenti alle recessioni andranno meglio. La spesa IT per la Pubblica Amministrazione potrebbe addirittura aumentare nel 2020. Dovrebbero crescere anche gli investimenti IT della Sanità e del mondo TLC. Questi proprio in risposta alla pandemia, che ha incrementato la richiesta dei loro servizi. La previsione migliore riguarda il comparto dei servizi professionali. Che potrebbe chiudere il 2020 con un +1,7%.



https://www.impresacity.it/news/23328/idc-chi-investe-e-chi-no-nel-post-coronavirus.html
Impresacity *– 21 aprile 2020*

Health Prognosis on the Security of IoMT Devices? Not Good As more so-called Internet of Medical Things devices go online, hospitals and medical facilities face significant challenges in securing them from attacks that could endanger patients' lives.

As COVID-19 continues to turn the world upside down, hospitals are facing unprecedented challenges: Do we have enough staff to treat the influx of patients? Are there enough beds and equipment for those patients? Will patients' lives be threatened by hackers holding the medical devices keeping them alive for ransom?

While that last concern is not unique to the COVID-19 crisis, it's certainly of heightened risk given that hospitals and emergency rooms have been overwhelmed with a massive influx of patients, resulting in even more patient-connected devices going online. While important, every piece of connected medical equipment, referred to as the Internet of Medical Things (IoMT), provides an easy on-ramp for hackers to bring a hospital to its knees.

"We are overdependent on undependable things," says Joshua Corman, former member of the HHS Cybersecurity Task Force under the Obama administration, and co-founder of I Am The Cavalry, a grassroots group focused on the intersection of computer security and public safety. "On the whole, these medical advances are improving lives, making care more available, and curing ailments that haven't been cured before. But I want the trust placed upon those innovations to be worthy of that trust. It's not right now."

The problems with IoMT are, essentially, threefold, with some deeper complications sprinkled throughout: One, the devices tend to run on outdated operating systems, like Windows 95, Windows XP, or Windows 7, and many were never intended to go online so they have no cybersecurity protection whatsoever. Two, hospital networks are often not segmented, allowing attackers to enter anywhere and move around. Three, vulnerable equipment is often not being replaced or patched, and not nearly enough is being recalled.

That combination could literally prove deadly for patients.

"An old, unpatched device that was inadvertently exposed to the Internet can make a great foothold into a network, where attackers can then move around and find more sensitive data," says Charles Ragland, security engineer at Digital Shadows, a San Francisco-based provider of digital risk-protection solutions. "This could also lead to a ransomware attack that could incapacitate infrastructure that is critical for patient care and safety."

https://www.darkreading.com/endpoint/health-prognosis-on-the-security-of-iomt-devices-not-good/d/d-id/1337649

***DARKREADING** -.Nicole Ferraro - 4/25/2020*

La fase sperimentale delle Linee Guida sui ponti: tutti i dettagli - Le Linee Guida sui ponti redatte dal Consiglio Superiore dei Lavori Pubblici prevedono una fase sperimentale che inizierà non appena firmata la convenzione con il soggetto attuatore e si articolerà in sei livelli aventi grado di approfondimento e complessità crescenti. Saranno analizzati tutti i ponti, i viadotti e i cavalcavia ricadenti in 11 tratte di competenza statale, più 7 tratte autostradali, per un totale di 1.046 opere e almeno la metà del campione sarà trattato anche con modellistica BIM. **Giuseppe Catalano,** coordinatore della Struttura tecnica di Missione del Ministero delle Infrastrutture e Trasporti, spiega come si svolgerà la fase sperimentale che servirà, in primo luogo, a calibrare e validare la metodologia definita dalle Linee Guida nazionali…

https://www.ingenio-web.it/26711-la-fase-sperimentale-delle-linee-guida-sui-ponti-tutti-i-dettagli?utm_term=37313+-+https%3A%2F%2Fwww.ingenio-web.it%2F26711-la-fase-sperimentale-delle-linee-guida-sui-ponti-tutti-i-dettagli&utm_campaign=Dossier+Ingenio&utm_medium=email&utm_source=MagNews&utm_content=3536+-+1942+%282020-04-28%29

INGENIO *– Giuseppe Catalano - - Samorì Chiara - – 28 aprile 2020*

Three things in life are certain: Death, taxes, and cloud-based IoT gear bricked by vendors. Looking at you, Belkin. Ubiquitous consumer kit maker EOLs netcam. Oh, AND the cloud services that make it work. Oh look, here's another cautionary tale about buying cloud-based IoT kit. On 29 May, global peripheral giant Belkin will flick the "off" switch on its Wemo NetCam IP cameras, turning the popular security devices into paperweights.

It's not unusual for a manufacturer to call time on physical hardware. Like software, it has a lifespan where, afterwards, it's deemed not economically viable for the vendor to continue providing support.

But this is a little different, because Belkin isn't merely ending support. It also plans to decommission the cloud services required for its Wemo NetCam devices to actually work.

"Although your Wemo NetCam will still connect to your Wi-Fi network, without these servers you will not be able to view the video feed or access the security features of your Wemo NetCam, such as Motion Clips and Motion Notifications," Belkin said on its official website.

"If you use your Wemo NetCam as a motion sensor for your Wemo line of products, it will no longer provide this functionality and will be removed as an option from your Wemo app," the company added.

Adding insult to injury, the ubiquitous consumer network gear maker only plans to refund customers with active warranties, which excludes anyone who bought their device more than two years ago. The window to submit requests is open from now until 30 June.

Customers will also have to provide the company with the original receipt, showing how much they paid for the unit. Though it shouldn't be too hard to fish out an Amazon invoice from an inbox, if you bought the unit from a bricks-and-mortar retailer, there's a chance you won't have that information to provide……..

https://www.theregister.co.uk/2020/04/29/belkin_wemo_eol/

THEREGISTER *- Matthew Hughes - 29 Apr 2020*

Academics demand answers from NHS over potential data timebomb ticking inside new UK contact-tracing app Slurp everyone's details and you create a hugely valuable hacker target. A group of nearly 175 UK academics has criticised the NHS's planned COVID-19 contact-tracing app for a design choice they say could endanger users by creating a centralised store of sensitive health and travel data about them.

In the open letter published this afternoon, the 173 scholars called on NHSX, the state-run health service's app-developing and digital policy quango, to "publicly commit that there will not be a database or databases, regardless of what controls are put in place, that would allow de-anonymization of users of its system."

Due for release in the coming weeks, NHSX's contact-tracing app will be the official way that everyone's contacts with COVID-19-positive people will be tracked. The app will emit an electronic ID from your phone and receive the IDs of other phones with the app installed. If someone develops the coronavirus, everyone who came into contact with that person (i.e. their app came close enough for their ID to be logged by others) will receive an alert.

Controversially, the NHSX app will beam that contact data back to government-controlled servers. The academics who signed today's open letter fear that this data stockpile will become "a tool that enables data collection on the population, or on targeted sections of society, for surveillance."
As we reported yesterday, Britain has abandoned the international consensus on how much data should be collected to fight the COVID-19 pandemic……..
https://www.theregister.co.uk/2020/04/29/academics_open_letter_nhs_coronavirus_app/
THEREGISTER *- Gareth Corfield - 29 Apr 2020*

Healthcare Targeted By More Attacks But Less Sophistication An increase in attacks targeting healthcare organizations suggests that perhaps new cybercriminals are getting into the game. Healthcare organizations are experiencing an increase in probes and fraud attempts against their businesses and suppliers, but the attacks appear not to be very sophisticated, security experts said this week.
Organizations, for example, saw a 30% increase last month in the number of COVID-19-themed phishing sites and lures, but they have not seen a commensurate increase in the number of successful breaches, according to the Healthcare Information Sharing and Analysis Center (H-ISAC). The mix of more but less sophisticated attacks has led to a greater number of investigations – yet about the same number of breaches, says Michael Hamilton, chief information security officer at cybersecurity-response firm CI Security. Half of the company's client base is made up of healthcare firms, he says.
"The downturn in the global economy has likely led some people into cybercrime, so it's not surprising that we are seeing more attacks but not necessarily by more sophisticated actors," he says. "I think there is a reluctance to single out hospitals right now by a lot of the threat actors, however."
Healthcare companies have struggled with securing their networks, and the recent chaos caused by the coronavirus pandemic and managing the response at hospitals and clinics has left cybersecurity as a secondary concern.
More than 80% of healthcare firms, for example, have medical imaging equipment and devices running older, unpatched operating systems, according to Palo Alto Networks.
In addition, external indicators of cybersecurity have dropped, according to SecurityScorecard, a cybersecurity ratings firm that attempts to replicate attacker reconnaissance and rate firms on their apparent cybersecurity posture. The cybersecurity score of the Department of Health and Human Services has dropped from 88 last year to 72 this past month. The healthcare industry as a whole has lower scores than other most other industries, says Alex Heid, chief research officer at the company……..
https://www.darkreading.com/risk/healthcare-targeted-by-more-attacks-but-less-sophistication/d/d-id/1337702
DARKREADING *-.Robert Lemos- 4/30/2020*

Covid-19 e contratti pubblici: l'esperienza inglese delle Procurement Policy Notes - *Come l'Italia, anche altri Paesi hanno previsto misure speciali per la gestione del sistema dei contratti pubblici a fronte dell'emergenza sanitaria causata dal Covid-19.* Ricco di spunti è il caso inglese delle Procurement Policy Notes (PPN) predisposte dal *Cabinet Office*, organismo pubblico di supporto al Governo del Regno Unito, promotore di buone prassi e di vademecum a supporto delle stazioni appaltanti…
https://www.ingenio-web.it/26823-covid-19-e-contratti-pubblici-lesperienza-inglese-delle-procurement-policy-notes
INGENIO – *Studio Legale Valaguzza – 01 maggio 2020*

Covid-19, così l'intelligence può salvare le imprese italiane. Le pmi italiane pagheranno il prezzo più salato della crisi del Covid-19, ha spiegato il consigliere strategico Massimo Franchi in una lezione al Master in Intelligence dell'Università della Calabria diretto da Mario Caligiuri. Ecco come le intelligence può aiutarle

Digitale, economia, lavoro, cyber-security. Non c'è un solo settore al riparto dall'effetto domino della crisi del Covid-19. L'Italia ha gli anticorpi per superare intatta l'impatto? Ne ha parlato, in una lezione al Master in Intelligence dell'Università della Calabria diretto da Mario Caligiuri, il consigliere strategico Massimo Franchi, saggista, docente alla Scuola nazionale dell'amministrazione della Presidenza del Consiglio dei ministri.

"Bisogna affrontare sfide di diversa natura, a cominciare da quelle geopolitiche. L'Italia ricopre una posizione strategica: è affacciata sul Mediterraneo ed è mira di interessi di Paesi Ue ed extra Ue". In questo scenario, ha detto Franchi, "l'intelligence diventa uno strumento di governance che deve essere utilizzato sia dal pubblico che dal privato".

Il primo fronte su cui la crisi del Covid-19 lascerà orme indelebili è quello economico. Presto per fare un bilancio italiano, che comunque sarà drammatico, spiega il docente. "Si prevede il fallimento di 150.000 imprese (circa il 4% delle imprese nazionali), e un tasso di disoccupazione che può arrivare al 20%. In particolare, i settori che soffriranno di più saranno il turismo, il settore Ho.Re.Ca. (Hotellerie, Restaurant e Cafè), mentre altri, come il settore agricolo, rimarranno stabili. I settori alimentari e della distribuzione, anche di prossimità, segneranno invece un aumento di fatturato".

Ma la crisi è globale e così le sue conseguenze sull'economia. "Il Covid19 – ha proseguito Franchi – comporterà un'elevata competizione aziendale all'interno dell'Ue che renderà difficile continuare a parlare di solidarietà". Per l'esperto "i rischi italiani, in questo contesto, derivano soprattutto dalla riduzione e dalla rimodulazione della catena di approvvigionamento e, di conseguenza, dalla diminuzione della produzione, essendo il sistema economico italiano basato principalmente sulle piccole e medie imprese, così come dal calo della domanda di manodopera: insomma, una doppia crisi che incide sia sulla curva dell'offerta che su quella della domanda"……..

. L'Intelligence dovrebbe supportare e tutelare le imprese italiane e sostenere la catena di approvvigionamento. Inoltre, sarebbe necessario un forte stimolo fiscale per la seconda industria manifatturiera d'Europa"…….

https://formiche.net/2020/05/covid-19-intelligence-imprese-italiane/

FORMICHE *- Federica De Vincentis - 02/05/2020*

Biosicurezza, perché serve una strategia nazionale. *Massimo Amorosi, esperto di studi strategici, già consigliere della Farnesina per biosicurezza e minacce Cbrn, spiega perché i biorischi sono l'aspetto più critico con cui fare i conti nel futuro*

Le agenzie di intelligence americane, seguendo quello che viene indicato come "un ampio consenso scientifico", hanno chiuso il capitolo secondo cui il coronavirus potesse avere origine artificiale, creato in un laboratorio di Wuhan. L'affermazione, che va contro uno dei lanci anti-Pechino del presidente Donald Trump, non è superflua: secondo un sondaggio Swg, il 16 per cento degli italiani crede che il virus sia stato creato. Una percentuale ancora più alta invece, il 31 per cento, ritiene che sia sfuggito dal controllo del laboratorio in cui veniva studiato – circostanza che le agenzie di intelligence statunitensi non hanno comunque escluso.

Ossia, il tema che si fa largo è quello della biosicurezza, elemento che amplifica il proprio valore con la cosiddetta "Fase 2", quella delle riaperture, ossia il riavvio verso una forma di normalità e soprattutto la costruzione di un futuro in cui certi "eventi possono accadere in ogni momento, e dunque un Paese deve essere attrezzato per affrontarli. Non parliamo del valore statistico, ma possiamo essere certi che

prima o poi in futuro si riaffacceranno minacce biologiche emergenti", spiega a *Formiche.net* Massimo Amorosi, esperto di studi strategici, già consigliere della Farnesina per biosicurezza e minacce Cbrn, acronimo che raccoglie le sfide chimiche, biologiche, radiologiche e nucleari.
È uno scenario quello che si prospetta di "bio-insicurezza ormai su scala globale". Dice Amorosi: "I governi devono mettere in conto che per preservare i livelli di prosperità dei rispettivi Paesi – intesa come salute pubblica, ma anche resilienza economica e stabilità interna – occorre fare i conti con questo problema". E serve "un cambio di approccio radicale, un cambio di paradigma, dalla portata anche culturale". "Occorre ora – continua l'esperto – una strategia nazionale di biodifesa che tenga conto del fatto che le minacce biologiche emergenti possono avere un'origine naturale, accidentale, oppure deliberata. E questi eventi possono essere molto simili in termini di preparazione e meccanismi di risposta, a prescindere dalla loro origine"…….....
https://formiche.net/2020/05/biosicurezza-minacce-strategia-nazionale-amorosi/
***FORMICHE** - Emanuele Rossi **-**.02/05/2020*

PROSSIMI EVENTI

A causa dell'emergenza Covid 19 tutti gli eventi sono stati rinviati a data da destinarsi

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC al link
http://www.infrastrutturecritiche.it/new/per-iscriversi/

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)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
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 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*