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 2023 **n. 3/ 2023** **Marzo 2023**

Il Prefetto Frattasi nominato Direttore della ACN

Il Prefetto Bruno Frattasi è il nuovo Direttore della Agenzia per la Cyber Security Nazionale. La guida della Agenzia è stata ritenuta un tema profondamente istituzionale e le istanze di visione strategica sono state poste a pari livello rispetto alla operatività tecnica. L'Agenzia aumenta la propria connotazione strategico istituzionale che verrà espressa dalla guida posta nelle mani di un uomo di Stato con una lunga esperienza nella gestione della res publica.

Un primo obiettivo sul quale le Infrastrutture Critiche saranno molto sensibili è la creazione di professionalità di cyber security a tutti i livelli, compreso quello dei diplomati. L'autonomia digitale "soft", quella che considera la parte "human", ossia i cervelli e la loro formazione, è quella che ci interessa di più.

Una autonomia tecnologica implica una capacità autonoma di produzione che copra tutto il flusso della catena del valore, comprese materie prime e logistica, quindi comprese, per esempio, le fonderie dei microchip. Il perimetro di tale autonomia non può che essere europeo, tuttavia l'"europeità" si garantisce a parità di capacità tecniche e tecnologiche, quindi passa prima di tutto per uno sviluppo di capacità nazionali e poi per una corretta postura di cooperazione internazionale. L'autonomia digitale, punto cardine delle politiche strategiche di cyber security di tutti i Pease del mondo, passa necessariamente per la creazione di uno strato industriale altamente specializzato sia dal punto di vista tecnico che tecnologico, in grado di realizzare sia software che hardware.

Un altro punto da affrontare velocemente è legato allo sviluppo degli schemi di certificazione di prodotto in cyber security. Nell'ambito del percorso avviato per la valutazione e la certificazione dei prodotti, percorso che trova nel CVCN il proprio elemento cardine a livello nazionale, è necessario promuovere la tempestività della definizione degli schemi di certificazione sia a livello nazionale che a livello europeo. Il terzo decennio di questo millennio sarà sicuramente dedicato, in tema di cyber security, alla standardizzazione e alla individuazione di tecniche di valutazione e certificazione che rendano la sicurezza "minima" misurabile e comprovabile. L'Europa ha intrapreso un cammino ambizioso in questo senso, prevedendo di identificare un metodo di certificazione per ogni tecnologia e per ogni settore specifico. Il percorso di identificazione di tali schemi va terminato il più velocemente possibile per dare attuazione alle norme.

Infine, un terzo punto riguarda la gestione dei finanziamenti del PNRR con una accelerazione significativa per poter usufruire di questa opportunità. Supportare e agevolare le PA centrali e locali nella spesa dei finanziamenti in ambito PNRR per la cyber security resta un obiettivo essenziale

Il percorso avviato nell'ultimo periodo in tema di cyber security dal nostro Paese ha già consentito di raggiungere risultati tangibili che abbiamo sperimentato durante la pandemia e in questo ultimo anno, reso particolare dagli eventi geopolitici internazionali. Ora dobbiamo rendere stabili e consolidati questi primi obiettivi raggiunti.

Luisa Franchina

Presidente dell'Associazione Italiana esperti in Infrastrutture Critiche

Luisa Franchina È stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono riprese le attività di formazione per soci e simpatizzanti che si svolgeranno nell'anno 2023.

L'accordo con IsacaRoma consente ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Stiamo valutando le modalità di svolgimento di altri eventi possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, come avrete notato, abbiamo ripreso le visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

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

VISITA GUIDATA PRESSO LA DIVISIONE AEREA DI SPERIMENTAZIONE AERONAUTICA E SPAZIALE (AEROPORTO DI PRATICA DI MARE)

Giovedì scorso 2 marzo si è svolta la prevista visita alla Divisione Aerea di Sperimentazione Aeronautica e Spaziale (DASAS), presso l'Aeroporto militare "Mario de Bernardi" di Pratica di Mare.
Hanno partecipato 10 soci, alcuni provenienti in aereo o auto da diverse città (Varese, Luino, Perugia, Civitavecchia, Campobasso, ecc.).

All'arrivo, i soci AIIC - guidati dal vicepresidente Silvano Bari - sono stati accolti dal Comandante della Divisione, Generale D.A. Alessandro De Lorenzo, che ha spiegato i vari reparti componenti. Successivamente il Colonnello Fabio De Michele, Comandante il Reparto Sperimentale di Volo, ha illustrato le attività del reparto ed ha accompagnato i soci AIIC nelle visita ai vari Gruppi, in particolare al Gruppo Ingegneria per l'Aerospazio, e permettendo la salita – particolarmente emozionante – al posto di guida degli aerei in quel momento disponibili. Infine, è stato possibile visitare il Reparto Medicina e l'Infermeria, dove il Colonnello Cerini e i suoi collaboratori hanno spiegato il funzionamento dell'Entry Point Sanitario Nazionale per la gestione delle emergenze epidemiologiche, quali sono state le attività per la gestione della pandemia da Covid19, come sono stati attrezzati i velivoli per il trasporto in sicurezza degli ammalati ed hanno poi accompagnato i soci nella visita della struttura in biocontenimento dedicata al transito dei contagiati.

La visita, iniziata alle ore 9.00, si è conclusa dopo 4 ore con una sosta "mangereccia" ad una trattoria adiacente alla base.

Tutti i componenti del gruppo hanno espresso grande soddisfazione perché oltre alla visita interessantissima di per sé, hanno avuto l'occasione di prendere contatti con esperti militari nelle varie specialità (tra le quali molte di interesse dell'Associazione come, ad esempio, la valutazione e la gestione dei rischi) che potranno essere contattati in futuro.
Inoltre è stata importante la ripresa, dopo il periodo di pandemia, dei rapporti personali tra i soci che hanno avuto anche l'occasione di esprimere consigli per i prossimi eventi e suggerimenti per quanto riguarda la vita associativa.

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 anche le visite previste nel prossimo futuro saranno riservate ai soli soci AIIC in regola con il pagamento delle quote sociali. I signori non-soci che volessero partecipare, possono iscriversi all'Associazione AIIC usufruendo di una quota di associazione minima (euro 50 anno + 10 una tantum). Le modalità per l'iscrizione si trovano sul sito www.infrastrutturecritiche.it o si possono richiedere inviando una mail a segreteria@infrastrutturecritiche.it

RINNOVO ASSOCIATIVO ANNO 2023

Il 31 dicembre 2022 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La partecipazione associativa inalterata da anni, pari ad euro 40, con delibera del Consiglio Direttivo del 19.9.2022 è stata aumentata di una modesta quota pari ad euro 10 per l'aumento generale dei costi di gestione.
La nuova quota per il rinnovo individuale è quindi adesso di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2023".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

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 2023. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.**

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.
Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

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

Infrastrutture critiche e utilizzo di Internet - Sono numerose le infrastrutture critiche che abbisognano, per funzionare correttamente, di efficienti collegamenti a Internet per esigenze di comunicazioni e operative. Uno studio mette in evidenza alcuni aspetti critici di questa funzionalità.
Le infrastrutture critiche nazionali fanno affidamento su sistemi elettronici, tra i quali si trova l'Internet of Things (IoT) e le tecnologie operative (OT).
IoT per solito fa riferimento a tecnologie ed apparecchiature che consentono le interconnessioni di rete e l'interazione con un gran numero di "oggetti", nel mondo delle infrastrutture del trasporto, delle abitazioni, delle costruzioni e simili.
Per contro, con l'espressione OT si fa riferimento a sistemi programmabili o apparecchiature che interagiscono con l'ambiente fisico, come ad esempio sistemi di automazione di edifici, movimentazioni ascensori, gestione di impianti di condizionamento e trattamento dell'aria e via dicendo.
Per aiutare le agenzie federali e gli enti privati a gestire i rischi di sicurezza informatica associati con questi due mondi, il Dipartimento della sicurezza nazionale, ed in particolare l'agenzia per la sicurezza informatica delle infrastrutture, ha pubblicato un prezioso documento e ha messo a disposizione risorse specifiche.
In particolare, vengono lanciati, quando appropriato, dei segnali di allerta per la presenza di criticità, che coinvolgano sia i sistemi IoT, sia i sistemi OT.
In particolare, gli investigatori hanno analizzato in profondità tre particolari categorie di infrastrutture critiche, rispettivamente legate alla gestione dell'energia, della salute pubblica e dei sistemi di trasporto.
Per quanto riguarda il settore dell'energia, sono stati avanzati suggerimenti afferenti alla messa sotto controllo dei sistemi di distribuzione dell'energia attraverso la rete, che permettono di aggirare interruzioni temporanee o potenziare l'invio di energia durante periodi di picco della richiesta.
Per quanto riguarda il settore della salute pubblica, gli specialisti hanno avanzato tutt'una serie di raccomandazioni, da trasmettere a tutti coloro che sviluppano apparati medici, come ad esempio apparati diagnostici, perché introducano dei criteri di sicurezza intrinseca, in grado di diminuire la probabilità che un attacco via Internet possa compromettere la funzionalità degli apparati.
Per quanto riguarda i sistemi di trasporto, è stata messa a punto una serie di strumenti, che possono mettere sotto controllo il rischio informatico, mettendo ad esempio sotto stretto monitoraggio gli aspetti meccanici dei dispositivi di trasporto, con particolare riferimento ai sistemi utilizzati nelle linee ferroviarie critiche.
Il documento è completato da alcuni esempi di tipi di attacchi informatici e della illustrazione delle modalità con le quali è possibile effettuare interventi di prevenzione e mitigazione del rischio.
Il documento, composto da 72 pagine, rappresenta una preziosissima guida per tutti gli esperti di sicurezza informatica, che operino nell'ambito di infrastrutture critiche, che facciano riferimento significativo alle due architetture informatiche illustrate. (*continua*)
https://www.puntosicuro.it/sicurezza-informatica-C-90/infrastrutture-critiche-utilizzo-di-internet-AR-*23052*
Punto Sicuro *– Adalberto Biasiotti - 17/02/2023*

AI TRiSM, ecco il framework per gestire l'intelligenza artificiale senza rischi

L'intelligenza artificiale gestita in modo errato può indurre le organizzazioni a prendere decisioni sbagliate: le aziende devono quindi imparare a gestirne rischi e sicurezza. AI TRiSM è un framework che include soluzioni, tecniche e processi per supportare un'adozione corretta dell'IA. Ecco di cosa si tratta

Gli algoritmi di intelligenza artificiale sono ormai in ogni ambito e mercato, utilizzati e utilizzabili da individui e organizzazioni: la musica che ci viene consigliata studiando i nostri gusti preferiti, i percorsi suggeriti sulle mappe per raggiungere una destinazione, le analisi delle frodi bancarie, le autovetture a guida autonoma, i sistemi in grado di accettare o rifiutare domande di prestito di denaro, non ultima la possibilità di fare domande su qualsiasi tipo di argomento (qualcuno sta pensando a ChatGPT?).

Attorno a essi nascono nuove professioni, nuove idee di business, nuovi casi di utilizzo.

Partendo da questo presupposto, Gartner ha recentemente pubblicato un paper centrato su "AI TRiSM" nel tentativo di fornire una migliore comprensione dell'emergente ecosistema incentrato sull'intelligenza artificiale.

Indice degli argomenti

Cos'è l'AI TriSM

AI TRiSM, acronimo di Artificial Intelligence (AI) Trust, Risk, and Security Management, è un framework sviluppato per consentire la governance, l'affidabilità, l'equità, l'efficacia e la privacy dell'IA. Si preoccupa di garantire che vengano impiegate adeguate salvaguardie e politiche di governance al fine di evitare l'uso inappropriato dell'intelligenza artificiale. (continua…)

https://www.agendadigitale.eu/cultura-digitale/ai-trism-ecco-il-framework-per-gestire-lintelligenza-artificiale-senza-rischi/

Agenda Digitale - *Andrea Benedetti-02 Mar 2023*

150 operazioni cancellate al Clinic Hospital di Barcellona a causa di un ransomware

Un attacco informatico ransomware su uno dei principali ospedali di Barcellona ha paralizzato il sistema informatico del centro che ha costretto la cancellazione di 150 operazioni non urgenti e fino a 3.000 controlli dei pazienti, hanno detto lunedì i funzionari.

(continua)

https://www.redhotcyber.com/post/150-operazioni-cancellate-al-clinic-hospital-di-barcelona-a-causa-di-un-ransomware/

Red Hot Cyber *– Redazione RHC – 07/03/2023*

Biden vara la nuova strategia cyber: focus su cooperazione internazionale e infrastrutture critiche

La Casa Bianca ha presentato la nuova National cybersecurity strategy: colpisce, prima di tutto, la consapevolezza che solo rafforzando la cooperazione internazionale è possibile raggiungere livelli alti di sicurezza e protezione del sistema Paese e delle infrastrutture critiche. Ecco i punti cardine del piano Biden per rafforzare la cyber security USA

Biden ha pubblicato il 2 marzo la nuova strategia di sicurezza cibernetica USA (National cybersecurity strategy) che si basa su due visioni strategiche: ribilanciamento delle responsabilità nel difendere il cyber space e riallineamento degli incentivi per favorire investimenti a lungo termine.

Entrambi i punti, già nel titolo, esprimono una volontà di differenziarsi dal passato e dare una impronta decisamente nuova nell'approccio alla cyber security da parte degli Stati Uniti.

Indice degli argomenti

USA, i pilastri della nuova strategia cyber

La nuova strategia cyber USA è basata su cinque pilastri.

Difesa delle infrastrutture critiche

Il primo riguarda la difesa delle infrastrutture critiche. Intanto si parla di difesa e non di protezione.

Al suo interno, il primo obiettivo strategico è "stabilire i requisiti di cyber security per supportare la security nazionale e safety pubblica". Nuove regole che siano sostenibili, controllate, applicate. Si enfatizza la collaborazione tra il settore pubblico il settore privato anche in ambito normativo e in generale norme che supportino la collaborazione tra i vari attori. (continua…)

https://www.cybersecurity360.it/cybersecurity-nazionale/biden-vara-la-nuova-strategia-cyber-focus-su-cooperazione-internazionale-e-infrastrutture-critiche/

***Cybersecurity360**- Luisa Franchina- 07 Mar 2023*

Attenzione ai modelli ingannevoli che violano la privacy nelle interfacce dei social media: pubblicate le Linee Guida 03/2022

Il 24 febbraio 2023 l'European Data Protection Board ha pubblicato le Linee Guida 03/2022 per aiutare gli utenti a riconoscere i modelli di progettazione ingannevoli nelle interfacce delle piattaforme dei social media. Rispetto alla prima versione che era stata pubblicata lo scorso anno per la consultazione pubblica, adesso le Linee Guida 03/2022 in versione definitiva 2.0 vedono sostituito nel titolo il termine "dark pattern" con "deceptive design patterns", andando così ad estendere la portata di questa subdola tipologia di violazioni del GDPR. *(continua)*

https://www.federprivacy.org/informazione/primo-piano/attenzione-ai-modelli-ingannevoli-che-violano-la-privacy-nelle-interfacce-dei-social-media-pubblicate-le-linee-guida-03-2022

***Federprivacy** – 08/03/2023*

5 Critical Components of Effective ICS/OT Security

These agile controls and processes can help critical infrastructure organizations build an ICS security program tailored to their own risk profile.

It's no secret that the industrial control system (ICS) attack surface is rapidly expanding (PDF). From advancements in business digitalization, IT-OT convergence, and Internet of Things (IoT) adoption to the ripple effects of escalating geopolitical tensions, organizations in critical infrastructure sectors must be positioned to combat accelerating ICS attacks that, in addition to forcing prolonged operational downtime, can potentially put people and communities at severe risk. After all, there's a clear differentiator regarding the nature of ICS/OT threats. Unlike traditional attacks against enterprise IT networks that are primarily rooted in monetary gain or data theft, state-sponsored adversaries often target critical infrastructure systems with the malicious intent to disrupt operations, inflict physical damage, or even facilitate catastrophic incidents that lead to loss of life.

This isn't fable or fiction — it's reality. In early February, leaders of two US House subcommittees called on the US Energy Department to provide information regarding three nuclear research laboratories targeted by the Russian hacking group Cold River last summer. Or take the Russian state-sponsored Crashoverride incident (PDF) of 2016, which manipulated ICS equipment through the abuse of legitimate ICS protocols to disrupt the flow of electricity across Ukraine's power grid at the transmission substation level. As a result, part of Ukraine's capital, Kyiv, experienced a one-hour outage overnight.

The incident served as a microcosm to an evolving era of cyber-risk, signifying the importance of trained defenders with engineering backgrounds who can effectively monitor ICS networks and actively respond to attacks before impact. After all, a weak ICS/OT security posture can pose risk to public health, environmental safety, and national security.(continua…)

https://www.darkreading.com/ics-ot/5-critical-components-of-effective-ics-ot-security-

***DarkReading**- Dean Parsons- March 09, 2023*

Sicurezza IoT, come evitare i rischi: le norme tecniche e la privacy

Per garantire la protezione e la messa in sicurezza sia dei dispositivi IoT sia dei dati da essi trattati, e per minimizzare il rischio di abusi, ci si può affidare anche a norme internazionali e a regolamenti, quali la norma tecnica ISO/IEC 27400 e il GDPR.

I dispositivi IoT sono molto diffusi e utilizzati in diversi ambiti che riguardano la vita quotidiana di tutti noi, non solo per migliorare la qualità della vita delle persone nella gestione quotidiana della casa, degli edifici e delle città, ma anche come dispositivi medici. Per questo motivo e per evitare possibili rischi di sicurezza è di fondamentale importanza proteggere e mantenere sicuri sia i dispositivi stessi che i dati da essi trattati, considerando sempre centrale il ruolo dell'utente. Un altro elemento messo a rischio dall'IoT o, meglio, che è collegato all'uso dell'IoT, è la privacy: i dispositivi "connessi" generano dati che potrebbero essere stati raccolti o condivisi senza il nostro consenso.- Per garantire la protezione e la messa in sicurezza sia dei dispositivi IoT sia dei dati da essi trattati, e per minimizzare il rischio di abusi, ci si può affidare anche a norme internazionali e a regolamenti, quali ad esempio la norma tecnica ISO/IEC 27400 e il Regolamento Generale per la Protezione dei Dati personali (GDPR).

Indice degli argomenti

- ISO/IEC 27400
- Controlli di sicurezza per i fornitori di servizi IoT e per gli sviluppatori di sistemi IoT
- Controlli di sicurezza per gli utenti di sistemi IoT
- Controlli sulla privacy per i fornitori di servizi IoT e gli sviluppatori di sistemi IoT
- Controlli sulla privacy per gli utenti di sistemi IoT

- L'applicazione del GDPR
- Conclusioni

ISO/IEC 27400
Con l'obiettivo di fornire delle linee guida per la sicurezza informatica e la privacy dei sistemi IoT, a giugno 2022 è stata pubblicata la norma tecnica ISO/IEC 27400:2022 nella sua prima versione. Questa norma non contiene requisiti, e quindi la sua applicazione non può essere resa obbligatoria, però fornisce delle linee guida utili per garantire la sicurezza informatica e la privacy dei sistemi IoT. (continua…)
https://www.agendadigitale.eu/sicurezza/le-norme-tecniche-e-la-privacy-per-la-sicurezza-nelliot-cosa-sapere-per-evitare-rischi/
***Agenda Digitale**- Beatrice Ridolfi -Anna Vaccarelli- 09 Mar 2023*

TikTok introduce il limite di un'ora per i ragazzi sotto i 18 anni e un parental control per i genitori
Sembrerebbe un passo in avanti concreto verso la salute mentale dei ragazzi e verso il controllo da parte dei genitori nella gestione dei contenuti. TikTok, la popolare app di social media nota per i suoi video di breve durata, ha introdotto i controlli sul tempo di visualizzazione per affrontare le preoccupazioni sugli utenti adolescenti e al suo potenziale impatto sulla loro salute mentale. La nuova impostazione predefinita limita gli utenti di età inferiore ai 18 anni a un'ora al giorno. (*continua*)
https://www.redhotcyber.com/post/tiktok-introduce-il-limite-di-unora-per-i-ragazzi-sotto-i-18-anni-e-un-parental-control-per-i-genitori/
***Red Hot Cyber** – Redazione RHC – 09/03/2023*

Tra bando per la Pa e nuovi data center per l'Ue, a che punto è il caso TikTok?
Non sembra esserci alcun piano per bloccare TikTok, app di proprietà della cinese ByteDance Ltd, ai dipendenti pubblici italiani in tempi brevi. A dirlo è stato Paolo Zangrillo, ministro della Pubblica amministrazione, lo stesso che nei giorni scorsi aveva aperto il dossier.
LE PAROLE DI FINE FEBBRAIO…
"Su questo argomento si sta già impegnando il Copasir, ma è evidente che il mio ministero, avendo 3,2 milioni di dipendenti, è fortemente coinvolto", aveva detto il ministro a *Repubblica*. "Le opzioni possono essere di muoversi come si è mossa la Commissione europea o eventualmente assumere una decisione diversa. È una scelta che non posso compiere in solitaria, mi devo confrontare con le altre istituzioni e insieme concorderemo una linea".
… E QUELLE DI QUESTA SETTIMANA
Durante una nuova intervista all'evento Raduno per la transizione digitale, ha spiegato: "Quindici giorni fa mi sono limitato a dire che ho notato che sia nella comunità europea che in diversi stati federali americani viene vietato ai dipendenti pubblici l'utilizzo di TikTok. Ho sollevato il problema e detto che è opportuno approfondire il tema e capire se effettivamente esistono dei rischi legati alla sicurezza degli utenti di questo social". Al momento, quindi, nessun piano per bloccare l'app in tempi brevi: "Assolutamente no anche perché, peraltro, non è decisione che spetti a me", ha replicato il ministro.
LA POSIZIONE DI TIKTOK
Dopo le prime parole del ministro, **Giacomo Lev Mannheimer**, responsabile delle relazioni istituzionali per il Sud Europa di TikTok, aveva dichiarato: "Così come per la decisione della

Commissione Europea, vorremmo rimarcare la nostra piena disponibilità a chiarire i dubbi del governo italiano, auspicando in un confronto dettato da regole e processi certi e trasparenti".

IL PROGETTO CLOVER

Mercoledì, poi, TiKTok ha annunciato i dettagli del progetto Clover. Oltre al data center di Dublino annunciato lo scorso anno ma ancora non attivo, ne dovrebbero essere aperti altri due: un altro a Dublin e uno nella regione di Hamar in Norvegia. "TikTok ha già iniziato a conservare i dati degli utenti europei in Irlanda e proseguirà il processo nel 2023 e 2024", si legge in una nota. (continua…)

https://formiche.net/2023/03/bando-pa-tiktok-progetto-clover/

***Formiche**- Federica De Vincentis -10/03/2023 –*

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

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.

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 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il 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 Gianluca Cipriani Andrea Agostino Fumagalli

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

ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.