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 2022	N. 11/ 2022	Dicembre 2022

La prova della cyber-security per il nuovo governo*

Perseguire la strategia di cyber-security con una visione unitaria e di insieme per il Paese sarà sicuramente un'istanza fondamentale che la comunità che si occupa di cyber-security richiederà al nuovo Governo. La sicurezza cibernetica non è solo una questione tecnologica, ma è un insieme multidisciplinare di processi, prodotti, tecniche e tecnologie che necessita una strategia nazionale di cooperazione tra le Istituzioni e tra le Istituzioni e le aziende private, per creare economie di scala e per rendere la sicurezza pervasiva.
L'autonomia digitale, punto cardine delle politiche strategiche di cybersecurity di tutti i Paese del mondo, passa necessariamente per la creazione di uno strato industriale altamente specializzato sia dal punto di vista tecnico sia tecnologico, in grado di realizzare sia software sia hardware. Un tessuto specializzato di tale natura si basa su un processo completo di innovazione che parte dalla ricerca e arriva all'industrializzazione. È un processo inverso alla globalizzazione e tenta di fermare l'azione fagocitante delle multinazionali a favore della nascita e della crescita di realtà nazionali in grado di soddisfare, almeno in parte, il mercato interno. Gli investitori sono molto attratti dall'innovazione in cyber-security e questo spinge numerose aziende a cercare di consolidare i fatturati per attrarre finanziamenti. Le piccole imprese e le start up si trovano in svantaggio costante perché non ricevono tutele, anche solo di defiscalizzazione, per assumere o per investire nella ricerca applicata e vengono facilmente inglobate dai grandi gruppi che attraggono investimenti con maggiore facilità. Un processo, questo, che non favorisce l'autonomia digitale perché va inevitabilmente verso globalizzazioni multinazionali.
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.
La creazione di professionalità legate alla sicurezza cibernetica anche al di fuori dell'ambito universitario è la prima risposta alle istanze delle industrie e delle aziende pubbliche e private italiane. L'autonomia digitale "soft", quella che considera la parte "human", ossia i cervelli e la loro formazione, è quella che ci interessa in modo più urgente.
Gli esperti concordano sul ruolo fondamentale che potranno giocare gli Istituti tecnici superiori (Its). Gli Its sono scuole di eccellenza ad alta specializzazione tecnologica che permettono di conseguire il diploma di tecnico superiore. Rappresentano un'opportunità di assoluto rilievo nel panorama formativo italiano in quanto fondati sulla connessione tra le politiche d'istruzione e di formazione-lavoro e le politiche industriali: l'obiettivo è sostenere interventi formativi destinati ai singoli settori produttivi, con particolare riferimento ai fabbisogni di innovazione e di trasferimento tecnologico delle piccole e medie imprese. Attraverso gli Its si possono offrire, infatti, percorsi su metodi e tecnologie per lo sviluppo di sistemi software, su organizzazione e fruizione dell'informazione e della conoscenza e su

architetture e infrastrutture per i sistemi di comunicazione, nonché su gestione della supply chain digitale, cybersecurity, cyber threat Intelligence, gestione dei Big data, cloud, architetture digitali per Industria 4.0.

* AirPress, n.138, novembre 2022

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 in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nell'anno 2023.

Anzitutto, l'accordo con IsacaRoma consentirà 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 questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle 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.

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

Riprendendo il nostro programma di visite sul campo dopo la pausa forzata dovuta ai noti problemi epidemici, abbiamo contattato lo Stato Maggiore dell'Aeronautica Italiana che ci ha dato la disponibilità di massima ad organizzare una visita guidata presso il **Reparto Sperimentale di Volo** della **Divisione**

Aerea di Sperimentazione Aeronautica e Spaziale (D.A.S.A.S.), situato presso l'aeroporto militare "Mario de Bernardi" di Pratica di Mare (Roma).

Il programma di massima prevede:

- presentazione delle principali attività del Reparto Sperimentale di Volo e dei Gruppi componenti, in particolare il Gruppo Gestione Software ed il Gruppo Ingegneria per l'Aerospazio;
- illustrazione delle attività per il biocontenimento dei velivoli per l'emergenza Covid-19;
- le caratteristiche dei velivoli presenti;
- la funzione di Entry Point sanitario nazionale per la gestione delle emergenze epidemiologiche.

La visita potrebbe essere effettuata nel periodo metà febbraio-marzo 2023, durata prevista 3 ore, luogo di incontro Aeroporto di Pratica di Mare (Roma) da raggiungersi con mezzi propri.

Poiché la visita è soggetta ad un numero minimo ed uno massimo di partecipanti, e bisogna prevedere i tempi per i permessi di ingresso in zona militare, chiediamo di **esprimere il proprio interesse – non vincolante – a partecipare, rispondendo a questa mail entro il giorno 20 dicembre p.v.**

Qualora si raggiunga il numero minimo di interessati, procederemo con l'organizzazione, e l'apertura delle iscrizioni.

Attenzione! **La visita è riservata 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 scadrà 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 aumentato 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.
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.

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

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.

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 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.

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

Competenze digitali: quali sono e che importanza hanno per le aziende – Il Parlamento europeo ed il Consiglio UE hanno definito la competenza digitale come il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC (tecnologie dell'informazione e della comunicazione): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet". Tra queste competenze digitali, da ritenere di particolare importanza e necessità per conservare la competitività sul mercato del lavoro, primeggiano l'individuazione dei sostegni previsti dal Governo per questo ambito e la definizione dei compiti specifici di lavoratori e imprese. Il governo ha messo a punto *il Piano operativo per la strategia nazionale per le competenze digitali*, per formare figure sempre più professionali e adeguate ai mutati fabbisogni nella Pubblica amministrazione. Tra i traguardi – si legge **sul sito del** Ministero dell'Innovazione tecnologica e transizione digitale:

- Dare al 70% della popolazione almeno le competenze digitali di base e colmare il divario di genere;
- Raddoppiare il numero di persone con competenze digitali avanzate;
- Triplicare i laureati in ICT e in questo ambito quadruplicare le laureate;
- Fa crescere del 50 per cento la quota di PMI che utilizzano specialisti ICT;
- Portare i servizi digitali della pubblica amministrazione al 64%, e avvicinando all'utilizzo di Internet i meno giovani.

Si chiama Syllabus, "competenze digitali per la PA", ed è il documento realizzato dall'Ufficio per l'innovazione e la digitalizzazione del Dipartimento della funzione pubblica, che puntualizza **quali sono le minime conoscenze e abilità di base che tutti i dipendenti pubblici devono avere in campo digitale**. Tra gli strumenti a disposizione, sono decisivi quelli di comunicazione e condivisione dei documenti digitali. Oltre alla posta elettronica, entrano in campo l'intranet aziendale, il sapersi muovere con le cartelle disponibili online, la corretta utilizzazione della video conferenza e le varie applicazioni di instant messaging. Senza tralasciare i social media, sempre più sempre più utilizzati dalla pubblica amministrazione per interloquire con i cittadini.
La sicurezza è garantita in primo luogo dalla protezione dei sistemi informatici e dei dati in essi contenuti. Per questo, il dipendente pubblico deve conoscere le regole che vanno rispettate per evitare usi non consentiti nella gestione di dati e informazioni. Avendo presenti le minacce alle quali deve far fronte mentre gestisce questo flusso di dati che spesso riguardano da vicino i cittadini. (continua…)
https://www.agendadigitale.eu/cultura-digitale/competenze-digitali/competenze-digitali-quali-sono-e-che-importanza-hanno-per-le-aziende/
Agenda Digitale *– Redazione - 20 Ott 2022*

Introduzione al mondo dei DRONI: normativa, abilitazioni e regolamento delle categorie Open, Specific, Certified - Per entrare nel mondo dei droni ed eventualmente pilotarne uno in applicazioni professionali, occorre conoscerne i riferimenti normativi, gli ambiti applicativi, le tipologie e i regolamenti delle varie certificazioni, di cui in questo articolo se ne fa una sintesi.
I droni e il loro sviluppo
Il mondo dei sistemi di volo, comunemente chiamati "droni" o APR, e con diversi acronimi nella nomenclatura internazionale, come UAV, RPV, etc., non si può dire sia una novità degli ultimi tempi, ma è pur sempre un tema in forte evoluzione in numerosi scenari operativi e professionali. Dal punto di

vista futuribile possiamo inoltre affermare che insieme ai sistemi di volo, vedremo sempre più applicazioni e sistemi di tipo autonomi un po' in tutti i settori, ivi comprese ispezioni e mappature.
(continua)
https://www.ingenio-web.it/articoli/introduzione-al-mondo-dei-droni-normativa-abilitazioni-e-regolamento-delle-categorie-open-specific-certified/
INGENIO - *Alessio Grassi, Domenico Santarsiero - 28.11.2022*

La digitalizzazione dei servizi nel PNRR e la necessità di una visione condivisa - Senza un'adeguata comunicazione digitale, saranno impossibili molte delle funzioni dell'edificio, come il controllo dell'energia, la sicurezza e la ricarica dei veicoli elettrici. A livello politico si deve dunque comprendere che, in assenza di questa digitalizzazione dell'edificio, le iniziative previste nel PNRR resteranno sulla carta.
Se ne è parlato recentemente nell'evento "Summit for Territories", organizzato dall'associazione Smart Building Alliance Italia (SBA) presso la sede dell'ANCE a Milano.
Molte delle funzioni dell'edificio sono ormai implementate digitalmente, o comunque supportate da tecnologie di comunicazione, e questa tendenza non accenna a fermarsi. Controllo dell'energia, sicurezza, ricarica dei veicoli elettrici, solo per fare qualche esempio, sarebbero impossibili senza una adeguata comunicazione digitale.
Tutto questo richiede ovviamente una adeguata infrastruttura di scambio veloce dei dati, che sia però appartenente all'edificio stesso e non solo ai singoli utenti.
(continua)
https://www.ingenio-web.it/articoli/la-digitalizzazione-dei-servizi-nel-pnrr-e-la-necessita-di-una-visione-condivisa/
INGENIO *- Ernesto Santini - 29.11.2022*

Data analytics applicati ai servizi alla cittadinanza: Singapore esempio di smart nation -Ogni giorno ognuno di noi produce e consuma una mole indefinita di **dati**. Entro certi limiti**, qualsiasi nostra azione, anche quella più quotidiana, può essere quantificabile:** i minuti che aspettiamo per prendere un bus, il numero di persone che incontriamo quando andiamo al parco, il tempo che impieghiamo per attraversare la strada, il numero di transazioni che dobbiamo compiere per ottenere un certificato dalla Pubblica Amministrazione, e così via.
Eppure, molto del potenziale racchiuso in questi dati rimane tutt'oggi in gran parte inesplorato. La domanda, dunque, è: come possiamo organizzare e sfruttare i dati prodotti nella nostra quotidianità, per pianificare e sviluppare soluzioni che migliorino il modo in cui viviamo nella nostra città?
In questo contesto, Singapore rappresenta un caso studio di come l'analisi dei dati può contribuire all'azione di pianificazione e di allocazione di risorse dell'amministrazione centrale.
(continua…)
https://www.agendadigitale.eu/smart-city/data-analytics-applicati-ai-servizi-alla-cittadinanza-singapore-esempio-di-smart-nation/
Agenda Digitale*- Giulia Geneletti - 01 dic. 2022*

Infrastrutture critiche in rete per gestire le emergenze
Nell'ambito del progetto Interreg Sicurezza delle Infrastrutture Critiche transfrontaliere (SICt) è stato siglato oggi a Giornico un accordo tra la Polizia cantonale ticinese, rappresentata dal capitano Marco

Guscio, e Regione Lombardia, rappresentata dal Direttore pro-tempore della Direzione Generale Territorio e Protezione Civile Roberto Laffi. L'accordo è relativo all'utilizzo, alla promozione e all'adesione da parte di soggetti interessati alla Piattaforma Infrastrutture Critiche.
La Piattaforma è uno strumento informatico di supporto alle decisioni riguardanti la sicurezza delle infrastrutture critiche, in particolare a quelle dedicate al trasporto (stradale e ferroviario) poiché consente la consultazione, l'elaborazione e lo scambio di informazioni, al fine di promuovere la gestione condivisa degli eventi che possono avere impatti sulla continuità del loro servizio. Serve pure per elaborare, nell'ambito delle attività ordinarie finalizzate alla prevenzione dei rischi, strategie operative e documenti di pianificazione. L'accordo prevede che le parti contraenti si impegnino a promuovere attivamente l'adesione alla Piattaforma da parte dei soggetti coinvolti nella gestione e nella sicurezza delle infrastrutture critiche.
(*continua*)
https://www4.ti.ch/tich/area-media/comunicati/dettaglio-comunicato?NEWS_ID=214782&cHash=db6493b460afd85fc60c2474db33fb54
Repubblica e Cantone Ticino *- Comunicato stampa, Dipartimento delle istituzioni, 06 dicembre 2022*

Single-Pair Ethernet, i vantaggi per le imprese 4.0: ecco perché potrebbe diventare uno standard
A distanza di pochissimi anni dalla sua concezione, Single-Pair Ethernet sta suscitando sempre più interesse, soprattutto negli operatori industriali che vedono in questa innovazione la possibilità di dare vita, in un futuro imminente, a reti dati di campo universali, performanti e di facile implementazione
Nuove applicazioni in ambito Industria 4.0 come l'IIoT sono alla base della spinta **verso nuovi standard per la connettività cablata nell'automazione e nelle fabbriche intelligenti**. L'introduzione della tecnologia IoT nell'ambiente industriale prevede nodi di sensori che, sebbene non richiedano potenze o larghezze di banda elevate, siano in grado di comunicare in maniera efficace e affidabile quasi in tempo reale o, almeno, entro intervalli di tempo accettabili e garantiti. In questo scenario, sta crescendo l'interesse per la tecnologia Single-Pair Ethernet, che potrebbe rappresentare uno standard per le reti dati.
Come funziona la tecnologia Single-Pair Ethernet
Agli albori di Ethernet si utilizzavano cavi coassiali, ma, a partire dal 1984, si passò a cavi a coppie ritorte che portarono all'introduzione di 10BASE-T e, nei decenni a seguire, di 100BASE-T, 1000BASE-T, 10GBASE-T, 25GBASE-T e 40GBASE-T. Non solo: tre anni fa, attraverso lo standard IEEE Std 802.3cg-2019, sono state ratificate due ulteriori varianti di Ethernet per trasmissioni a 10 Mb/s su singola coppia ritorta, note come 10BASE-T1S e 10BASE-T1L. La prima è ideale per l'industria automobilistica e **per altre applicazioni a breve distanza** in cui è presente un notevole rumore elettrico, mentre la seconda supporta connessioni su distanze fino a 1.000 metri. Così è nata la nuova tecnologia Ethernet a singola coppia, denominata, appunto, Single-Pair Ethernet o SPE.
SPE significa cavi con una singola coppia di conduttori di rame in grado di trasmettere dati a velocità fino a 1 gigabit al secondo su brevi distanze, **fornendo contemporaneamente un'alimentazione elettrica** di tipo Power over Data Line (PoDL). Infatti, supporta fino a 52 watt di potenza CC e si presta a un'ampia gamma di dispositivi e sistemi in ambito sia industriale che civile. (continua…)
https://www.agendadigitale.eu/industry-4-0/single-pair-ethernet-i-vantaggi-per-le-imprese-4-0-ecco-perche-potrebbe-diventare-uno-standard/
Agenda digitale- *Maurizio Truglia- 06 Dic 2022*

Cyber Warfare, le istituzioni in Italia sotto attacco DDoS per il sostegno all'Ucraina

Le istituzioni in Italia sotto attacco DDoS per il sostegno all'Ucraina. Gli esperti di cybersecurity del CSIRT Italia: Escalation di aggressioni degli hactivisti. Il 3 dicembre il gruppo pro-Russia NoName057(16) ha colpito il MIPAAFC'è un aumento di attacchi di tipo DDoS soggetti istituzionali nazionali. Lo rilevano gli esperti di cybersecurity del Computer Security Incident Response Team – Italia (CSIRT Italia) dell'Agenzia per la Cybersicurezza Nazionale (ACN), che ritiene ci siano gruppi di hactivisti dietro all'escalation di aggressioni. Allo stato, comunque, non risulta che gli attacchi – a quanto appare attualmente di carattere "dimostrativo" – abbiano intaccato l'integrità e la confidenzialità delle informazioni e dei sistemi interessati. L'offensiva di cyber warfare, infatti, ha prodotto solo una indisponibilità del sito per alcune ore. Il 3 dicembre il gruppo hacker pro-Russia, NoName057(16) ha lanciato un attacco DDoS contro il Ministero delle Politiche Agricole, Sovranità Alimentare e Forestale italiano. (continua…)

https://www.difesaesicurezza.com/cyber/cyber-warfare-le-istituzioni-in-italia-sotto-attacco-ddos-per-il-sostegno-all-ucraina/

Difesa e Sicurezza- *Francesco Bussoletti- 6 Dicembre 2022*

What Will It Take to Secure Critical Infrastructure?

There's no quick fix after decades of underinvestment, but the process has started. Cybersecurity grants, mandatory reporting protocols, and beefed-up authentication requirements are being put in place.

Securing critical infrastructure is complicated because of the vast network of facilities and management systems. Threats targeting this sector can have dire consequences, and when attacks do happen, they're often accompanied by a media storm. This generates interest among concerned citizens, which prompts a reaction from politicians, who are spurred into action to ensure the necessary cyber protections are implemented to calm the concerned citizens — the electorate.

The 2021 ransomware attack on Colonial Pipeline, which caused long lines at gas stations, followed this very timeline and served as a much-needed wake-up call to protect critical infrastructure services against cyberattacks. The attack prompted action at the highest levels of US government, causing the president to expedite an executive order aimed at strengthening US cybersecurity defenses. The executive order, in brief, requires disclosure of incidents, creates a federal playbook for incidents, mandates cybersecurity upgrades, creates a review board, and, importantly, encourages an ethos of cyber-intelligence sharing between government agencies and the private sector.

Wake-Up Call

The emphasis on cybersecurity due to the increased threats to critical infrastructure — including cybercriminals attempting to monetize their efforts, terrorism, and the conflict in Ukraine — is unprecedented. In the current budget proposal, the Cybersecurity and Infrastructure Security Agency (CISA) will receive $2.93 billion, $417.1 million more than it requested. There are numerous grants available to critical infrastructure organizations to assist funding the much-needed improvements to cybersecurity; in April 2022, CISA and FEMA began rolling out the first $1 billion from the Rescue Act to help state and local entities improve cybersecurity. Testifying before the House Homeland Security Subcommittee, Jen Easterly, director of the CISA, used the cyberattack on the Oldsmar, Fla., water utility plant as an example of an attack on critical infrastructure to justify the original request.

Enormous would be an underestimate of the task of upgrading the cybersecurity of water supply and wastewater systems in the US. According to American Water, there are 53,000 water supply and sanitation providers in the US. The Environmental Protection Agency (EPA) calculates this differently, and lists 148,000 public water systems (not companies). (continua….)

https://www.darkreading.com/ics-ot/what-will-it-take-to-secure-critical-infrastructure
***Darkreading**- Tony Anscombe- December 06, 2022*

Antwerp's city services down after hackers attack digital partner

The city of Antwerp, Belgium, is working to restore its digital services that were disrupted last night by a cyberattack on its digital provider.

The disruption has affected services used by citizens, schools, daycare centers, and the police, which have been working intermittently today. An investigation is ongoing, but the little information available points to a ransomware attack from a threat actor that has yet to be disclosed.

According to Het Laatste Nieuws (HLN), the hackers were able to disrupt Antwerp's services after breaching the servers of Digipolis, the city's digital partner that provides administrative software. The publication also notes that almost all Windows applications have been impacted.

Phone service for some departments was also unavailable. Alexandra d'Archambeau, a councilor member for the district of Wilrijk, said earlier today that the city's email service was down.

De Standaard reports that it received confirmation that ransomware was the cause of the disruption from an actor that has yet to be determined. The problems also extend to the city's reservation system, which has been shut down, leaving people unable to receive their identity cards. Today, only travel cards could be collected.

Residential centers impacted

Among other the services affected by the attack are those from the Antwerp Healthcare Company (Zorgbedrijf Antwerpen), which provides residential care services to seniors in the province. Johan De Muynck, the general manager of Zorgbedrijf said that the attack made unusable the software that kept track of who should receive medication.

This forced the staff in 18 residential care centers to switch to pen and paper and rely on traditional paper prescriptions for the seniors needing them. (continua…)

https://www.bleepingcomputer.com/news/security/antwerps-city-services-down-after-hackers-attack-digital-partner/
***Bleepingcomputer -**Ionut Ilascu- December 6, 2022*

"Interventi chirurgici rimandati". Sistemi spenti a causa di un attacco ransomware.

Pensa se stai per recarti all'ospedale per una operazione salvavita, e arrivi una telefonata dall'ospedale dove ti viene detto: "Ci spiace ma l'operazione è rimandata. Siamo stati colpiti da un attacco informatico e tutti i sistemi sono stati fermati". Quale sarebbero le tue sensazioni? Sembra qualcosa di incredibile, ma stiamo iniziando sempre di più ad assistere a questo genere di "tragedie" e questa volta è il turno di un ospedale dei nostri cugini francesi. Nel fine settimana, l'ospedale André Mignot di Versailles è stato colpito da un attacco ransomware che ha costretto i tecnici a spegnere tutti i sistemi informatici e telefonici, e ha costretto i medici a cancellare gli interventi chirurgici e trasferire alcuni pazienti in altre strutture mediche. Il consiglio di sorveglianza dell'ospedale ha detto ai media locali che gli autori dell'incidente avevano chiesto un riscatto. L'importo esatto non è stato divulgato, ma la direzione dell'ospedale Andre Mignot ha già dichiarato che non pagherà gli estorsori.

(*continua*)

https://www.redhotcyber.com/post/interventi-chirurgici-rimandati-sistemi-spenti-a-causa-di-un-attacco-ransomware/
***Red Hot Cyber** – Redazione RHC - 8/12/2022*

Gli Stati Uniti stanno per invadere la Cina attraverso il Golden Shield

Cloudflare ha trovato un modo per distribuire alcuni dei suoi servizi attraverso il Great Firewall of China (Golden Shield). Secondo Cloudflare, i pacchetti che attraversano il confine cinese spesso incontrano problemi di accesso, congestione, perdita e latenza. Molti aspetti della rete in Cina sono spesso considerati separati dal resto della rete globale a causa delle loro sfide uniche. Per risolvere questi problemi, Cloudflare sta lavorando con "partner locali" sconosciuti che "instradano il traffico locale verso una destinazione in Cina in modo sicuro al data center Cloudflare disponibile più vicino al di fuori della Cina". Cloudflare esegue la sua suite di servizi nel data center, tra cui un firewall-as-a-service e un gateway web sicuro (Secure Web Gateway). Le policy applicate a questi servizi possono quindi essere propagate dagli uffici dell'organizzazione in tutto il mondo, attraverso il Great Firewall, e nelle reti cinesi. In teoria, ciò dovrebbe significare che le politiche di sicurezza dell'organizzazione applicate altrove potrebbero essere estese alla Cina. Inoltre, gli sforzi di Cloudflare per semplificare le operazioni in Cina saranno apprezzati dalle organizzazioni internazionali e dalle società offshore cinesi. Vale la pena notare che i partner cinesi di Cloudflare non avrebbero partecipato a questo accordo transfrontaliero senza il consenso di Pechino. Altrimenti sarebbero stati puniti. Inoltre, la collaborazione attiva di Cloudflare con gli operatori di telecomunicazioni cinesi potrebbe attirare l'attenzione delle autorità statunitensi sulla società.

https://www.redhotcyber.com/post/gli-stati-uniti-stanno-per-invadere-la-cina-attraverso-il-golden-shield/

Red Hot Cyber – *Redazione RHC- 8/12/2022*

Agrius Iranian APT Group Cuts Into Diamond Industry

The supply chain attack is piggybacking off an earlier breach to deploy new wiper malware.

A previous cyberattack on an Israeli software developer is being used by Agrius Advanced Persistent Threat (APT) group to launch wiper attacks against various organizations in the diamond industry.

Although Agrius and its attack against Israeli IT and HR companies last February was previously known, using the "Fantasy" wiper in attacks is new, according to researchers at ESET.

Fantasy is a modified iteration of the Apostle malware, the team said. But while its predecessor Apostle masqueraded as ransomware, Fantasy dispenses with the charade and moves directly to destroying files.

So far, ESET reported, Fantasy victims have been found in Hong Kong, Israel, and South Africa. (continua….)

https://www.darkreading.com/attacks-breaches/agrius-iranian-apt-group-cuts-into-diamond-industry

DARK READING *Dark Reading Staff- December 08, 2022*

La sveglia europea agli Stati membri. Più attenzione alle infrastrutture critiche

Dopo la Nis2 è il momento della Direttiva Cer, che sta per critical entities resilience. Accompagnata da una raccomandazione che mette fretta alle capitali europee. Il prof. Setola: "Questi atti vanno nella direzione di migliorare la resilienza delle infrastrutture critiche sviluppando una strategia di forte cooperazione pubblico/privato"

Pandemia e conflitto in Ucraina hanno mutato lo scenario relativo alla sicurezza per gli Stati e le singole infrastrutture: anche per questa ragione dopo l'approvazione della **Direttiva Nis2** avvenuta a metà novembre, il Consiglio Europeo lo scorso 8 dicembre ha approvato anche la **direttiva Cer** sulla

resilienza fisica delle infrastrutture critiche. Queste due direttive sono alla base di uno schema che invita gli stati membri a dare maggiore attenzione ai temi della resilienza dei sistemi che erogano servizi essenziali alla popolazione.

Premessa

Si tratta di una necessità che deriva da una constatazione: la complessità intrinseca di queste infrastrutture impone un diverso approccio alla loro protezione superando le visioni settoriali (a silos) per un approccio maggiormente intersettoriale e, nel contempo, dalla constatazione che le minacce contro questi sistemi sono sempre più sofisticate e numerose includendo sia eventi naturali legati in particolare all'estremizzazione dei fenomeni climatici, ma anche di origine dolosa.

Ciò parte dalla considerazione che le infrastrutture critiche sono diventate sempre più interconnesse e reciprocamente dipendenti: sono quindi più efficienti ma anche più vulnerabili in caso di incidente.

Non va dimenticato che il **conflitto russo-ucraino** ha portato nuovi rischi, attacchi fisici e informatici, spesso combinati come una minaccia ibrida. Più in generale, il panorama dei rischi è sempre più complesso, con una minaccia terroristica in evoluzione, pericoli interni, disastri naturali e cambiamenti climatici che possono ridurre la capacità e l'efficienza di determinati tipi di infrastrutture, qualora non siano in atto misure di prevenzione. La **pandemia da Covid-19** ha mostrato la vulnerabilità delle nostre società sempre più interdipendenti di fronte ai rischi a bassa probabilità.

La direttiva

A tal fine la **direttiva Cer** impone che ogni stato individui i propri operatori dii infrastrutture critiche, identifichi le minacce che potrebbero comprometterne la capacità operativa considerando tanto le minacce antropiche che quelle di origine naturali definendo una specifica strategia nazionale di resilienza delle infrastrutture critiche. In questo quadro un ruolo fondamentale deve essere svolto dagli operatori che gestiscono le diverse infrastrutture critiche che dovranno effettuare una dettagliata analisi dei rischi implementando conseguentemente specifici piani di resilienza. (continua…)

https://formiche.net/2022/12/direttiva-cer-setola/

Formiche *-Paolo Falliro -10/12/2022 –*

The US Department of Health and Human Services (HHS) warns healthcare organizations of Royal ransomware attacks.

The human-operated Royal ransomware first appeared on the threat landscape in September 2022, it has demanded ransoms up to millions of dollars.

The Health and Human Services (HHS) is aware of attacks against the Healthcare and Public Healthcare (HPH) sector.

Unlike other ransomware operations, Royal doesn't offer Ransomware-as-a-Service, it appears to be a private group without a network of affiliates.

"Royal is a human-operated ransomware that was first observed in 2022 and has increased in appearance. It has demanded ransoms up to millions of dollars. Since its appearance, HC3 is aware of attacks against the Healthcare and Public Healthcare (HPH) sector. Due to the historical nature of ransomware victimizing the healthcare community, Royal should be considered a threat to the HPH sector." reads the report published by HHS.

Once compromised a victim's network, the threat actors deploy the post-exploitation tool Cobalt Strike to maintain persistence and perform lateral movements. (continua…)

https://securityaffairs.co/wordpress/139486/cyber-crime/us-hhs-royal-ransomware-attacks.html

Securityaffairs *-Pierluigi Paganini - December 10, 2022*

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

Questa è l'ultima newsletter del 2022.
Cogliamo l'occasione per augurare a tutti i nostri soci e simpatizzanti
un Natale sereno e un buon inizio di Anno Nuovo.
Arrivederci al 2023!

Il Comitato di Redazione

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 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 *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.