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 2021 **N. 6/ 2021** **Giugno 2021**

ATTACCO COLONIAL PIPELINE E ORDINE ESECUTIVO PER LA SICUREZZA INFORMATICA

Nelle ultime settimane, l'intera comunità della sicurezza informatica è stata allertata dall'attacco ransomware a uno dei più importanti oleodotti degli Stati Uniti, noto come Colonial Pipeline dal nome della società che lo gestisce. È uno degli attacchi più importanti alle infrastrutture critiche degli ultimi anni e ha avuto un impatto diretto e indiretto su più settori dell'economia statunitense. Per fortuna, le operazioni sono ritornate attive e funzionanti dopo un'interruzione di circa una settimana e il pagamento di un riscatto di 5 milioni di dollari americani.
DarkSide, il Ransomware as a Service (RaaS) usato contro Colonial Pipeline, è un buon esempio di malware usato per portare attacchi informatici a diverse organizzazioni in tutto il mondo. Preparato e usato con cura dagli esperti, utilizza una combinazione di tecniche per estorcere con successo le sue vittime.
L'attacco Colonial Pipeline è diventato di dominio pubblico il 10 Maggio, 2021. In data 12 Maggio, 2021, il Presidente degli Stati Uniti ha firmato l'Executive Order (EO) *on Improving the Nation's Cybersecurity* 14028[1]. Alcuni media hanno suggerito che l'EO sia stato una risposta all'attacco della Colonial Pipeline, ma ciò è poco credibile sul piano pratico. Esso è un documento enorme e complesso, con ricadute ad oggi difficili da ipotizzare. La lunghezza media di un EO è inferiore a 3 pagine e mezzo; la maggior parte sono solo 1 o 2 pagine, questo è un documento di 18 pagine.
Un documento di queste dimensioni e profondità non avrebbe potuto essere scritto durante il fine settimana tra quell'attacco e il momento in cui l'EO è stato rilasciato. La sua portata è semplicemente molto più ampia rispetto all'attacco ransomware al centro del problema Colonial Pipeline.
L'ordine esecutivo 14028 è 18 pagine, ma non è solo la lunghezza che è senza precedenti: l'ordine include 74 direttive. Quarantacinque di tali direttive hanno scadenze ben definite, molte delle quali sono legate al completamento di altre direttive. Aggiungete a tutto questo una pletora di acronimi e abbreviazioni comuni al mondo della sicurezza informatica e il risultato è un documento che richiederà mesi agli esperti di sicurezza informatica per essere decifrato completamente, e capire tutte le sue conseguenze.
Il nuovo ordine richiama ripetutamente la Tecnologia Operativa (OT), che nel mondo del controllo di processo coesiste con la Tecnologia dell'Informazione (IT), sia nell'introduzione all'EO che nella scheda FACT[2] che costituisce una Appendice dell'EO. Tuttavia, sposta l'attenzione su un termine più generale, Software Critico, enunciando l'elenco dei requisiti e delle direttive che saranno obbligatori per tutto il software venduto al governo degli Stati Uniti. E questo avrà un impatto sia nel mondo OT che nel mondo IT, tra loro legati e fortemente interdipendenti.
Cosa si intende esattamente per software critico? In questo momento non c'è certezza nella definizione. Tuttavia, dopo il recente incidente della Colonial Pipeline, è lecito ritenere che il software OT sia incluso in questa categoria. Tuttavia, una risposta definitiva non è lontana: il direttore del CISA (*Cybersecurity and Infrastructure Security Agency*) ha il compito di fornire un elenco delle categorie di software che soddisfano la definizione di software critico, entro 45 giorni dalla data di pubblicazione dell'EO. Per

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

adesso, l'EO si limita a formulare *"The security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern".*
Le aziende della "*Supply Chain*" interessate da questo ordine esecutivo non hanno molto tempo per capire come esso avrà un impatto su di loro. Devono capirlo il più presto possibile, in modo da poter implementare un piano per soddisfare i nuovi requisiti. Ciò è particolarmente vero per le aziende che forniscono il suddetto software critico al governo degli Stati Uniti.
La sicurezza della catena di fornitura (*supply chain*) del software è probabilmente l'obiettivo principale di questo EO. Quasi un terzo delle dichiarazioni di policy del documento si trovano nella sezione *Enhancing Software Supply Chain Security*. Questa non è una sorpresa dopo che l'attacco di SolarWinds a Dicembre 2020 si è infiltrato in tutti i rami dell'esercito americano, il Pentagono, il Dipartimento di Stato, l'Agenzia per la sicurezza nazionale, la Casa Bianca e molti altri obiettivi significativi.
I fornitori di prodotti ICS/OT, ma anche IT, al governo degli Stati Uniti (o più semplicemente i fornitori di un'azienda che rifornisce il governo) hanno un bel lavoro da fare per adeguarsi. Ci sono precise scadenze per le varie direttive della catena di fornitura, alcune delle quali hanno un impatto sui fornitori di software che nessun'altra legislazione informatica degli Stati Uniti ha mai avuto. Si estenderà anche ben oltre gli Stati Uniti, in particolare il Medio Oriente, dove le compagnie petrolifere sovrane stanno cercando di duplicare questi requisiti per la loro catena di fornitura del software OT. Anche se la tua azienda non vende direttamente al governo degli Stati Uniti, aspettati di sentire gli effetti di questo EO nei prossimi anni.

Sandro Bologna, laureato in fisica alla Sapienza, Università di Roma, Socio fondatore, Presidente nel triennio 2011 – 2013, e attuale Membro del Consiglio Direttivo AIIC. Tra le principali attività di ricerca attuali si citano la valutazione della resilienza di infrastrutture critiche, con particolare riferimento agli aspetti di analisi delle vulnerabilità alle minacce di origine naturale e umana e alla modellistica dei diversi fattori che concorrono a costituire una infrastruttura. Nel campo delle Smart City sta conducendo attività di ricerca afferenti agli aspetti etici nell'uso delle tecnologie di Machine Learning e Intelligenza Artificiale per la protezione di spazi pubblici.

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2021

Si ricorda a tutti i soci che il 31 dicembre 2020 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 2021".

Per i nuovi iscritti l'importo da pagare è di € 60,00. 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/*

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 2021. 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.

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.

ATTIVITA' DELL'ASSOCIAZIONE

ASSEMBLEA DEI SOCI AIIC

Il giorno 20 giugno 2021 alle ore 23.59 in prima convocazione e il giorno **30 giugno 2021 alle ore 16.30** in seconda convocazione è indetta l'assemblea generale dei soci con il seguente ordine del giorno:

- Comunicazioni del Presidente;
- Approvazione bilancio consuntivo 2020;
- Approvazione bilancio preventivo 2021;
- Rinvio data elezioni per rinnovo Consiglio Direttivo;
- Varie ed eventuali.

L'assemblea si terrà in modalità webinar, la comunicazione con le modalità previste saranno comunicate in tempo utile.

Si rammenta che la partecipazione all'assemblea con diritto di voto è riservata ai soci in regola con il pagamento delle quote sociali per l'anno 2021 e ai nuovi soci che abbiano effettuato il pagamento almeno 30 giorni prima della data dell'assemblea e, quindi, entro il 31 maggio 2021.

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

NUOVI GRUPPI DI LAVORO AIIC

Il Consiglio Direttivo di AIIC, nella riunione del 4 giugno 2021, ha approvato la costituzione di un nuovo Gruppo di Lavoro sulla "Disciplina normativa della criticità", mentre prosegue la possibilità di aderire al GdL sulla "Protezione degli spazi pubblici".
Qui di seguito sono descritti i contenuti e gli obiettivi dei due GdL, riservati ai soci in regola con il versamento delle quote sociali.
Si ricorda che per l'adesione è sufficiente inviare una mail di conferma a segreteria@infrastrutturecritiche.it.

Gruppo di lavoro
"ICE, ICN, OSE, OSF… La disciplina normativa della criticità"
Coordinatore Luisa Franchina

Il panorama normativo europeo e italiano sulla disciplina della protezione delle Infrastrutture Critiche è divenuto complesso.
Il GdL vuole analizzare le norme in vigore e in itinere con una pubblicazione veloce, sintetica e precisa che supporti il lettore a:

1. comprendere a colpo d'occhio quanto delineato
2. valutare le implicazioni di compliance sulla propria azienda
3. identificare opportunità
4. interpretare le direttrici di ulteriori futuri sviluppi normativi

Si invitano i Soci interessati ad aderire entro il 30 giugno 2021. Il lavoro verrà organizzato in modo da pubblicare la Linea Guida entro fine 2021.

Gruppo di Lavoro
"Principi e Tecnologie per la Protezione di Spazi Pubblici"
Coordinatore Sandro Bologna

Il Gruppo di Lavoro si riferisce alla protezione di spazi pubblici quali - ad esempio - stazioni ferroviarie, sale aeroportuali, imbarchi portuali, stadi per concerti, ecc.

La rivoluzione digitale ha aperto la possibilità di raccogliere e recuperare immense quantità di dati in tempo reale. Lo sfruttamento delle soluzioni tecnologiche offre numerose opportunità per migliorare la protezione degli spazi pubblici. Applicati e analizzati correttamente, i dati derivati dai dispositivi IoT (Internet of Things) possono fornire informazioni per il rilevamento precoce delle minacce di molteplici scenari (terrorismo, criminalità, disastri naturali, pandemie). La disponibilità di strumenti per raccogliere informazioni più complesse, complete e rapide può aiutare a prendere decisioni più informate e più tempestive. Le applicazioni mobili e le piattaforme di social media possono fungere da forum per coinvolgere i cittadini nella protezione degli spazi pubblici. Migliori canali di comunicazione e sistemi integrati consentono un migliore coordinamento e collaborazione tra le diverse autorità. Queste ampie opportunità sono accompagnate da sfide altrettanto pesanti, che devono essere affrontate dal gruppo di lavoro.

Punti principali su cui concentrarsi: In termini di tecnologia, anche il miglior hardware non sarebbe utile senza un adeguato software di analisi dei dati e il personale addestrato per gestire le informazioni. Sistemi differenti devono essere interoperabili se vogliono consentire l'analisi di dati provenienti da fonti differenti. L'interoperabilità diventa una questione ancora più complessa se applicata a sistemi utilizzati da diverse autorità, diverse città e diversi paesi. Qualsiasi sistema deve rispettare i principi di protezione della privacy sanciti dal Regolamento Generale sulla Protezione dei Dati. La tecnologia è un potente strumento per la sicurezza, ma può essere altrettanto potente come una minaccia, quindi le misure di protezione tecnologica devono evolversi di conseguenza.

Durata e conoscenze richieste ai membri del Gruppo di Lavoro: Un anno dal kick off meeting, previsto entro fine settembre 2021.
Partecipanti: soci AIIC conoscitori di una o più delle seguenti discipline: tecnologie di protezione fisica e digitale (diversi tipi di recinzioni fisiche e tecnologie IoT), analisi dei dati applicata all'analisi dei social network, interoperabilità, principi etici che regolano le applicazioni di intelligenza artificiale, principi di Protezione dei Dati Personali, progettazione della Sala Controllo di una Smart City con particolare attenzione al Security Control Center (SOC), al profilo degli operatori SOC e alla loro formazione.

Si invitano i Soci interessati ad aderire entro il 15 settembre 2021. Il lavoro verrà organizzato in modo da pubblicare i risultati entro un anno dall'inizio lavori.

NEWS E AVVENIMENTI

Microsoft warns of BadAlloc flaws in OT, IoT devices Microsoft researchers are warning of major security vulnerabilities affecting OT and IoT devices and high-risks for businesses using them. Researchers from Microsoft's Section 52 team recently uncovered several critical memory allocation flaws, collectively tracked as **BadAlloc**, affecting IoT and OT devices. The vulnerabilities could be exploited by attackers to bypass security controls to execute malicious code or trigger DoS conditions. Experts found more than 25 RCE vulnerabilities that potentially affect a wide range of domains, from consumer and medical IoT to Industrial IoT, Operational Technology (OT), and industrial control systems. The full list of vulnerabilities is available in an advisory (ICSA-21-119-04) published by the US DHS. *"Our research shows that memory allocation implementations written throughout the years as part of IoT devices and embedded software have not incorporated proper input validations. Without these input validations, an attacker could exploit the memory allocation function to perform a heap overflow, resulting in execution of malicious code on a target device." reads the advisory published by Microsoft.* According to Microsoft, the BadAlloc vulnerabilities resides in standard memory allocation functions spanning widely used real-time operating systems (RTOS), embedded software development kits (SDKs), and C standard library (libc) implementations. Microsoft, along with the U.S. Department of Homeland Security (DHS), disclosed the issues with all the affected vendors. IOT/OT devices sold by Amazon, ARM, Cesanta, Google Cloud, Samsung, Texas Instruments and Tencent, along with many other open-source products are affected. *"Given the pervasiveness of IoT and OT devices, these vulnerabilities, if successfully exploited, represent a significant potential risk for organizations of all kinds. To date, Microsoft has not seen any indications of these vulnerabilities being exploited. However, we strongly encourage*

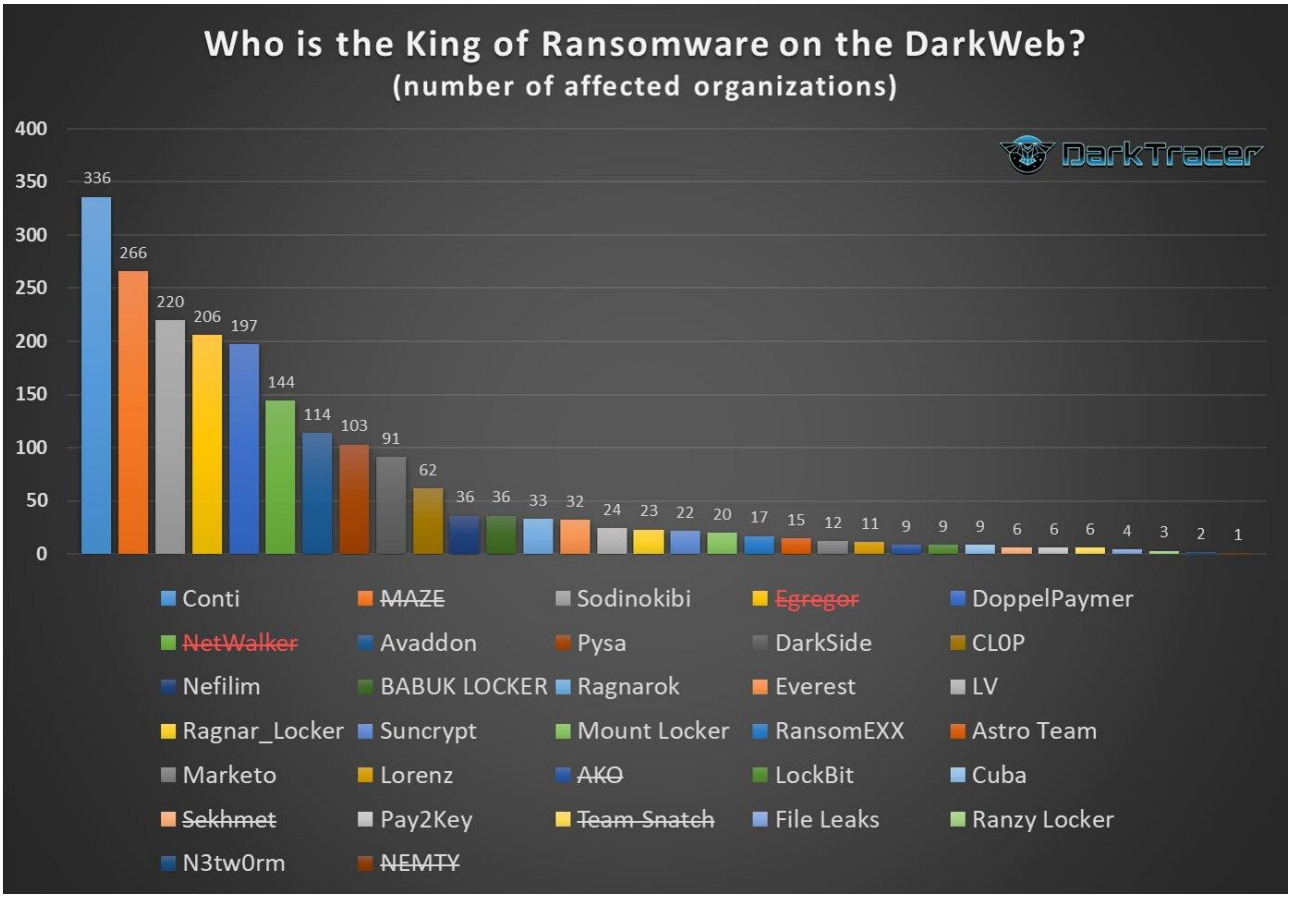
organizations to patch their systems as soon as possible," continues the report. Microsoft provides the following recommendations to mitigate the risk of attacks on their IoT and OT infrastructure (segue)
https://securityaffairs.co/wordpress/117372/iot/badalloc-vulnerabilities-ot-iot.html
***Security Affairs** Pierluigi Paganini -April 30, 2021*

Operation Management in ambito IIoT: come superare gli ostacoli nello sviluppo dei progetti - Quando si parla di progetti nell'ambito dell'Industrial Internet of Things, il rischio è quello di trovarsi di fronte a vere e proprie "opere incompiute", che non riescono a scalare dal PoC alla messa in produzione. Ma quali sono gli ostacoli e come si superano? Il ruolo di Axulus di Industrie Reply
Nonostante l'Industrial IoT sia considerato da molti analisti come uno dei segmenti in più forte crescita nel mondo manifatturiero e nonostante anche i dati più recenti dell'Osservatorio Internet Of Things del Politecnico di Milano sottolineino come le imprese che hanno un forte commitment in questo ambito sono in grado di estendere la propria offerta con servizi a valore aggiunto e, in alcuni casi, di rivoluzionare il proprio modello di business, ancora oggi molti dei progetti avviati in questo ambito fanno fatica a decollare e a uscire dalla fase del PoC (Proof of Concept).
I benefici, sulla carta, sono chiari a tutti: collegare le operational technologies ai sistemi IT aiuta a semplificare le attività, ridurre i tempi di fermo, migliorare la produttività, generare nuovi flussi di reddito e alimentare l'innovazione.
Ma nel passare dalla definizione teorica dei benefici alla loro realizzazione concreta, il passo è tutt'altro che breve. (segue)
https://www.internet4things.it/industry-4-0/operation-management-in-ambito-iiot-come-superare-gli-ostacoli-nello-sviluppo-dei-progetti/
***Internet4things** - Maria Teresa Della Mura - 4 maggio 2021*

UE, in arrivo il nuovo Regolamento Macchine - Salute e sicurezza nella progettazione, costruzione e commercio dei macchinari all'interno dell'Unione, perché siano aggiornati al progresso tecnologico e applicati in modo uniforme da tutti gli Stati membri: con questi scopi la Commissione Europea ha elaborato una proposta ufficiale per un nuovo Regolamento Macchine (i.e. Regulation of the European Parliament and of the Councilon machinery products). Esso andrà a sostituire l'attuale Direttiva macchine 2006/42/CE. La trasformazione della direttiva in un regolamento comporterà non solo un'attuazione più uniforme, riducendo le differenze di interpretazione tra gli Stati membri, ma anche minori problematiche di recepimento e una maggiore certezza del diritto. (segue)
https://www.industry4business.it/esperti-e-analisti/ue-in-arrivo-il-nuovo-regolamento-macchine/
***Industry4business -** Federica Maria Rita Livelli - 7 Mag 2021*

Ransomware gangs have leaked the stolen data of 2,100 companies so far. Since 2019, ransomware gangs have leaked the stolen data for 2,103 companies on dark web data leaks sites.When modern ransomware operations began in 2013, the attacker's goal was to encrypt as many companies as possible and then demand a ransom payment for a decryptor.Since the beginning of 2020, ransomware operations began conducting a new tactic called double-extortion. Double-extortion is when ransomware operations steal unencrypted files before encrypting a network. The attackers then threaten to publicly release the stolen files on dark web data leak sites if a ransom is not paid. Between the threat of not recovering their encrypted files and the additional concerns of data breaches, government fines, and lawsuits, threat actors are banking on the idea that this would force victims to

more readily pay a ransom. A dark web security researcher known as DarkTracer has been keeping track of the data leak sites for thirty-four ransomware gangs and told BleepingComputer that they have now leaked the data for 2,103 organizations. The 34 ransomware gangs followed by DarkTracer are Team Snatch, MAZE, Conti, NetWalker, DoppelPaymer, NEMTY, Nefilim, Sekhmet, Pysa, AKO, Sodinokibi (REvil), Ragnar_Locker, Suncrypt, DarkSide, CL0P, Avaddon, LockBit, Mount Locker, Egregor, Ranzy Locker, Pay2Key, Cuba, RansomEXX, Everest, Ragnarok, BABUK LOCKER, Astro Team, LV, File Leaks, Marketo, N3tw0rm, Lorenz, Noname, and XING LOCKER.
Of these thirty-four operations, the top five active operations are Conti (338 leaks), Sodinokibi/REvil (222 leaks), DoppelPaymer (200 leaks), Avaddon (123 leaks), and Pysa (103 leaks). Three groups that are no longer active and have more leaks than some of those in the top five are Maze (266 leaks) and Egregor (206 leaks).The data for all the ransomware gang's data leak sites are represented in the chart below created by DarkTracer from May 4th, 2021.



Who is King of Ransomware on the Dark Web?
Source: DarkTracer

Some of the listed ransomware gangs are no longer in operation, such as NetWalker, Sekhmet, Egregor, Maze, Team Snatch, or rebranded to a new name, such as NEMTY and AKO. The data-extortion industry has become a significant money-maker for ransomware gangs who have told BleepingComputer that victims worry more about their data being leaked than the loss of encrypted files. Other threat actors are seeing this trend and have begun launching new data leak marketplaces over the past couple of months that exist solely to sell stolen data. While it may seem better to pay a ransom to prevent a data leak, there is no guarantee that the data won't be released or sold to other threat actors. (segue).....

https://www.bleepingcomputer.com/news/security/ransomware-gangs-have-leaked-the-stolen-data-of-2-100-companies-so-far/
BleepingComputer *- Lawrence Abrams - May 8, 2021*

Elisabetta Belloni al DIS: che c'è dietro e l'impatto sulla cyber italiana - Ci sono motivi politici ma non solo dietro alla successione di Vecchione a capo Dipartimento delle informazioni per la sicurezza (DIS), con Elisabetta Belloni. C'è anche la volontà di ristrutturare la cyber e aprire di più ai rapporti con Paesi extra UE.
Il mondo della sicurezza è stato scosso da una notizia, che era un evento già nell'aria anche se la sua maturazione è accelerata nelle ultime ore: l'ambasciatore Elisabetta Belloni nuovo direttore generale del Dipartimento delle informazioni per la sicurezza (DIS). Attuale segretaria generale della Farnesina. Il Premier Draghi ha avuto l'ok del Copasir e del Comitato interministeriale per la sicurezza della Repubblica.
Andiamo a vedere in dettaglio motivi e implicazioni di questa scelta. (segue)
https://www.agendadigitale.eu/sicurezza/elisabetta-belloni-al-dis-che-ce-dietro-e-limpatto-sulla-cyber-italiana/
Agenda Digitale *- Marco Santarelli -13 mag 2021*

Non aspettiamo un disastro come Colonial Pipeline per rafforzare la cyber italiana - Gli Usa hanno colto l'occasione dell'incidente ransomware all'oleodotto per un ordine esecutivo utile a rivedere la strategia cyber. Noi che aspettiamo? Un disastro nostrano per rafforzare la cyber security?
L'oleodotto Colonial Pipeline è tornato in funzione – pagando 5 milioni di dollari di riscatto agli autori dell'attacco ransomware – ma mica è finita qui. L'incidente riapre una questione sempre più pressante: quella delle guerre cyber e delle strategie Paese che vanno adottate per fronteggiarle. Gli Usa hanno colto l'occasione per un ordine esecutivo utile a rivedere la strategia cyber. E da noi? Ancora non ci siamo. Non è il caso di correre ai ripari, rafforzando la cyber, solo dopo un grave incidente. Facciamolo prima. (segue)
https://www.agendadigitale.eu/sicurezza/non-aspettiamo-un-disastro-come-colonial-pipeline-per-rafforzare-la-cyber-italiana/
Agenda Digitale *- Alessandro Longo, Marco Santarelli - 14 mag 2021*

Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. (Bloomberg) -- Colonial Pipeline Co. paid nearly $5 million to Eastern European hackers on Friday, contradicting reports earlier this week that the company had no intention of paying an extortion fee to help restore the country's largest fuel pipeline, according to two people familiar with the transaction. The company paid the hefty ransom in difficult-to-trace cryptocurrency within hours after the attack, underscoring the immense pressure faced by the Georgia-based operator to get gasoline and jet fuel flowing again to major cities along the Eastern Seaboard, those people said. A third person familiar with the situation said U.S. government officials are aware that Colonial made the payment.
Once they received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. The tool was so slow that the company continued using its own backups to help restore the system, one of the people familiar with the company's efforts said. A representative from Colonial declined to comment. Colonial said it began to resume fuel shipments around 5 p.m. Eastern time Wednesday. When Bloomberg News asked President Joe Biden if he was briefed on the

company's ransom payment, the president paused, then said: "I have no comment on that." The hackers, which the FBI said are linked to a group called DarkSide, specialize in digital extortion and are believed to be located in Russia or Eastern Europe. On Wednesday, media outlets including the Washington Post and Reuters, also based on anonymous sources, reported that the company had no immediate intention of paying the ransom.
Ransomware is a type of malware that locks up a victim's files, which the attackers promise to unlock for a payment. More recently, some ransomware groups have also stolen victims' data and threatened to release it unless paid -- a kind of double extortion.
The FBI discourages organizations from paying ransom to hackers, saying there is no guarantee they will follow through on promises to unlock files. It also provides incentive to other would-be hackers, the agency says (segue……)
https://finance.yahoo.com/news/colonial-pipeline-paid-hackers-nearly-141548661.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cyLnNtYXJ0YnJpZWYuY29tLw&guce_referrer_sig=AQAAAHNpbRDo5BAfe9YwWEtU5N3771tvp-wyZuHL0I4Xu5nCn3qEzoe6hkea-8TV5Sct1FDesWSDzPFQth5XSHVC9XdxCwQNYeYeKYWAAZ7PYj_YPX1l9WrzXGx_yLhWMgpmIi3r9BfXkKLaGtUbzeoQ3TqMLbfi-uh0VL02mmZLybSu
Finance Yahoo-*William Turton, Michael Riley and Jennifer Jacobs May 14, 2021*

How penetration testing can promote a false sense of security. Penetration testing in and of itself is a good way to test cybersecurity, but only if every nook and cranny of the digital environment is tested; if not, there is no need to test.
Rob Gurzeev, CEO and co-founder of CyCognito, a company specializing in attack-surface management and protection, is concerned about blind spots—past and present. In his DarkReading article Defending the Castle: How World History Can Teach Cybersecurity a Lesson, Gurzeev mentioned, "Military battles bring direct lessons and, I find, often serve as a reminder that attack surface blind spots have been an Achilles' heel for defenders for a long time."
As an example, Gurzeev refers to the 1204 siege of Château Gaillard—the castle was thought to be impenetrable. After nearly a year of failed attempts, the attackers somehow determined the latrines and sewer system were poorly defended. Plans were made, and on the next moonless night, the medieval equivalent of a special-ops team made their way through the sewers, gained entry, set fires to the inner workings of the castle, and, in short order, the siege was over.
"Cybersecurity attackers follow this same principle today," wrote Gurzeev. "Companies typically have a sizable number of IT assets within their external attack surface they neither monitor nor defend and probably do not know about in the first place."
Some examples are programs or equipment:

- Set up without the knowledge or involvement of security, sometimes even without the knowledge of IT
- No longer used and forgotten about
- Used for short-term testing that are not decommissioned

"Assets and applications are constantly created or changed, and the pace of change is fast and dynamic," added Gurzeev. "It is a monumental task for any security organization to stay apprised of all of them."
Cybercriminals understand this tendency (segue..)
https://www.techrepublic.com/article/how-penetration-testing-can-promote-a-false-sense-of-security/
Techrepublic *- Michael Kassner - May 17, 2021*

Auto connesse, le linee guida EDPB: focus sul trattamento dati dei veicoli - La rivoluzione digitale dell'industria automobilistica procede speditamente e richiede una rapida risposta alle nuove sfide del mercato in una logica d'insieme che tenga conto dei molteplici profili, regolatori, antitrust, IP e data protection. Le indicazioni dello European Data Protection Board. (segue)
https://www.agendadigitale.eu/sicurezza/auto-connesse-le-linee-guida-edpb-focus-sul-trattamento-dati-dei-veicoli/
Agenda Digitale *- Laura Liguori, Irene Picciano - 18 mag 2021*

Tecnologie IoT, come possono potenziare la sicurezza delle persone - L'analisi in tempo reale di dati video, rilevati da telecamere e sensori, fatta attraverso algoritmi di AI e l'uso di una infrastruttura 5G e edge computing sono fattori di moltiplicazione della sicurezza. Gli esempi di un progetto italiano e di uno europeo.
Telecamere e sistemi di allarme fungono già da utili dissuasori contro malintenzionati e potenziali aggressori. L'integrazione con i servizi offerti all'interno delle Smart City, lo sviluppo di app per smartphone, l'utilizzo delle tecnologie IoT, così come dell'infrastruttura 5G, dell'edge computing e di sensori, possono aumentare enormemente l'efficacia delle soluzioni per la sicurezza. Elemento cruciale in questo panorama sono gli algoritmi di intelligenza artificiale per l'analisi dello streaming video delle telecamere di quartiere. (segue)
https://www.internet4things.it/sicurezza-iot/tecnologie-iot-come-possono-potenziare-la-sicurezza-delle-persone/
Internet4things *- Antonino Albanese - 21 maggio 2021*

Protezione attiva e protezione passiva: breve panoramica delle due misure di Prevenzione Incendi - Nel presente articolo, vengono descritte a grandi linee le strategie di protezione attiva e protezione passiva, seguendo le strategie antincendio riportate nel DM 3 Agosto 2015 e successivi aggiornamenti.
Per ognuna delle strategie riportate dal Codice di prevenzioni incendi vengono brevemente descritte le soluzioni più comuni adottate. (segue)
https://www.ingenio-web.it/30819-protezione-attiva-e-protezione-passiva-breve-panoramica-delle-due-misure-di-prevenzione-incendi
Ingenio *- Cecchinato Diego - 21/05/2021*

50 persone della cybersecurity italiana da seguire. E non finisce qui *Seguendo criteri generali tipo "la capacità di costruire qualcosa che resta", come imprese, enti, associazioni, e quello di "essere capace di modellare le idee, la cultura", abbiamo provato a costruire una sorta di Who's Who del settore. Ma è solo la prima puntata*
L'Italia è un paese ricco di competenze, creatività e spirito imprenditoriale. Anche nel campo della cybersecurity. Un po' a digiuno di storia, forse, e con una limitata proiezione internazionale, ma è un paese dove "la cyber" non è più considerata un passatempo. Per questo abbiamo provato a fare una prima mappa di queste competenze a partire dalle personalità più in vista del settore ma senza la pretesa di fare un elenco definitivo, sapendo che si tratta di un *work in progress* e che anche nel campo della cybersecurity le classifiche basate sulla bravura sono impossibili. Del resto ogni elenco non mette mai nessuno d'accordo. E neanche parole come "Cybersecurity", che qui usiamo nell'accezione ombrello di Data security, Information security, CyberThreat Intelligence e via di questo passo.

Ma seguendo criteri generali, in particolare "la capacità di costruire qualcosa che resta", come imprese, enti, associazioni, e quello di "essere capace di modellare le idee, la cultura", abbiamo lo stesso provato a costruire una sorta di*Who's Who* della cybersecurity italiana. Per farlo abbiamo valutato la visibilità delle persone considerate, la presenza a convegni internazionali, agli eventi accademici, la presenza a conferenze, le citazioni sui giornali, le interviste alla radio, in tv, ma abbiamo escluso i social tranne LinkedIn dove abbiamo chiesto che ne pensano quelli che nella cyber ci lavorano. E lo abbiamo fatto sapendo che le teste pensanti stanno spesso un passo indietro, non amano la visibilità, sono tenute alla discrezione, praticano il silenzio, soprattutto con la stampa. Lo abbiamo fatto sapendo che le figure aziendali hanno un ruolo importantissimo nel proteggere il proprio perimetro, ma che i Cyber security officer, i Ciso, sono più spesso figure politico-manageriali che tecnici di grido: quelli stanno spesso in retrovia e difficilmente diventano "personalità". Per mettere a punto questa prima lista inoltre non ci siamo basati soltanto sui titoli e sulla bravura tecnica, quella che capiscono i colleghi di lavoro o gli appassionati della tua cerchia ristretta e nemmeno sugli anni di esperienza. Abbiamo invece provato a valutarla. (segue)
https://www.repubblica.it/tecnologia/2021/05/23/news/cinquanta_persone_della_cybersecurity_italiana_da_seguire_e_non_finisce_qui-302292340/
Repubblica - *Arturo di Corinto* ***-*** *23 MAGGIO 2021*

Ransomware Hit: Tulsa Promises Recovery, Not Ransom Paying. Mayor Says .
If it feels like ransomware attacks today are stuck on repeat, that's because they are. Criminal syndicates have found an extremely profitable business model, and they're milking it for all it's worth.
"Know that your tax dollars are not going to go into the hands of criminals."
The city of Tulsa, Oklahoma, is yet another public sector victim. But give officials credit for appearing to have strong disaster recovery processes in place and refusing to be victimized, vowing to not engage with the attackers.
"We're not going to pay any ransom," Tulsa Mayor G.T. Bynum said at a Thursday press conference.
The city, which has a population of 766,000, first announced the attack on May 9 via a post to its Facebook page.
Restoration work is continuing. "All of our computer systems - with a few exceptions - are down right now," Michael Derringer, the city's CIO, said at the press conference. Emergency services - including police and fire services - remain fully functional, officials say. But multiple systems have been disrupted, with police, for example, having no way to offload data from their body cameras, which they would typically do via Wi-Fi, except all Wi-Fi is down. Residents also remain unable to pay bills, such as their water bills, but the city has said nothing now will come due until five days after billing systems get restored.
In the meantime, the city's mayor has vowed to "not ... pay a nickel" to attackers. "We have strong systems in place here at the city of Tulsa, and we have no inclination to negotiate with cyber terrorists," he said. "We're not embarrassed to publicly say when we've been a victim, and you're not going to get hush money from us for that, and we're not going to pay to get our systems restored more quickly, when we can go through and do it ourselves."
Bynum added: "We will be completely transparent and do the hard work and avoid rewarding criminal behavior. And I think the most important audience for me that would hear that is the citizens of Tulsa, to know that your data here at the city of Tulsa is secure, and to know that your tax dollars are not going to go into the hands of criminals."
Repeat Target: US Cities

Tulsa joins a growing roster of U.S. cities - including Atlanta, Baltimore, New Orleans and many others - that have seen their systems get hit by extortionists wielding crypto-locking malware and demanding a ransom in return for a decryption tool. (segue….)
https://www.bankinfosecurity.com/blogs/ransomware-hit-tulsa-promises-recovery-ransom-paying-p-3047
BANKINFOSECURITY *- Mathew J. Schwartz - May 24, 2021*

Prevenzione incendi: dalle nuove RTV in arrivo all'applicazione della Fire Safety Engineering
Fabio Dattilo, Capo del Corpo Nazionale dei Vigili del Fuoco, fa il punto sulle novità in arrivo nel settore della prevenzione incendi: dalle Regole Tecniche Verticali (RTV) all'applicazione dell'ingegneria della sicurezza antincendio.
Il Comitato Centrale Tecnico Scientifico dei Vigili del Fuoco sta esaminando diverse RTV che riguarderanno, a esempio, la reazione al fuoco delle facciate degli edifici civili e gli impianti di trattamento rifiuti, nonché nuove regole antincendio per le attività di intrattenimento e spettacolo a carattere pubblico che andranno a integrare la RTO del Codice di prevenzione Incendi. (segue)
https://www.ingenio-web.it/30833-prevenzione-incendi-dalle-nuove-rtv-in-arrivo-allapplicazione-della-fire-safety-engineering
Ingenio *- Samorì Chiara, Dattilo Fabio - 26/05/2021*

The Principles and Technologies Heralding the Next Cybersecurity Revolution
Everyone is always looking for the next big thing but how do you know when the time's up for the current tools?
Over recent years, we have faced increasing incidents of cyber-attacks and unprecedented technologies being used to cause data breaches. It'll only get worse unless organizations adapt their cybersecurity strategies to the principles and technologies of the current transformation in the state of enterprise cybersecurity. Here, we discuss three of these big principles and highlight some of the technologies driving the trend.
Zero-Trust
Basically, this is a principle that strips security authentication systems of the assumption of trust when handling access requests. As against traditional security models, the zero-trust framework aims to ascertain the identity of a user and their legitimacy to be granted the required access. This moves away from dependence on hardware devices and knowledge-based authentication models, all of which may be easily breached/hijacked. By not trusting anything outside the network perimeter until the user's identity is firmly established, organizations can greatly reduce incidents of data breaches.
Least Privilege
One of the principles promoted in the zero-trust model is *least privilege* cybersecurity. The principle means that users do not have access to network resources beyond what's necessary for fulfilling a (legitimate task). The ultimate aim is to manage and reduce the impact of data breaches. Essentially, if even the CEO cannot have access to more network resources than they require to fulfill an assignment, breaching the system through that endpoint limits the amount of damage that a cyber-attacker can wreak. Least privilege_appears to be a cross between smart permission management and advanced network segmentation that reduces a cyber-attack surface. (segue….)
https://www.infosecurity-magazine.com/next-gen-infosec/principles-tech-next-cyber/
infosecurity-magazine - Joseph Chukwube -_28 MAY 2021

China-linked attackers breached Metropolitan Transportation Authority (MTA) using Pulse Secure zero-day

China-linked APT breached New York City's Metropolitan Transportation Authority (MTA) network in April using a Pulse Secure zero-day. The intrusion took place in April, but attackers did not cause any damage because they were not able to gain access to MTA train control systems. The Authority addressed the issue the day after Pulse Secure and US CISA issued an advisory in April to warn of the active exploitation of the flaw in the wild. The security breach was the third cyberattack on the transit network in recent years, officials told The New York Times.

"The breach was the third — and most significant — cyberattack on the transit network, North America's largest, by hackers thought to be connected to foreign governments in recent years, according to transit officials." reported The New York Times. "The M.T.A. is one of a growing number of transit agencies across the country targeted by foreign hackers and the breach comes during a surge in cyberattacks on critical American infrastructure, from fuel pipelines to water supply systems."

Hackers did not access to employee or customer information, said Rafail Portnoy, MTA's Chief Technology Officer.

"The Metropolitan Transportation Authority (MTA) quickly and aggressively responded to this attack, bringing on Mandiant, a leading cyber security firm, whose forensic audit found no evidence operational systems were impacted, no employee or customer information breached, no data loss and no changes to our vital systems," said Portnoy. "Importantly, the MTA's existing multi-layered security systems worked as designed, preventing spread of the attack and we continue to strengthen these comprehensive systems and remain vigilant as cyber-attacks are a growing global threat,"

The flaw, tracked as CVE-2021-22893 is an authentication bypass issue that unauthenticated users could exploit to perform remote arbitrary file execution on the Pulse Connect Secure gateway. (segue….)

https://securityaffairs.co/wordpress/118579/apt/metropolitan-transportation-authority-hack.html

Security Affairs *- Pierluigi Paganini - June 4, 2021*

PROSSIMI EVENTI

WEBINAR • AL VIA LA CERTIFICAZIONE DI COMPETENZE PROFESSIONALI DEGLI OT CYBER SECURITY EXPERT (WEBINAR GRATUITO (Mercoledì 30 giugno 2021 • Ore 10.55 – 12.00) - *CEPAS* srl, ente di certificazione specializzato nella certificazione delle competenze, organizza un webinar per illustrare la figura professionale dell'OT CYBER SECURITY EXPERT.

Con l'avvento della filosofia Industria 4.0 tutte le macchine ed i sistemi di produzione devono poter essere interconnessi, integrati e telemanutenuti. Questo fa sì che gli aspetti di *security* per la prevenzione e l'eventuale gestione di minacce e della vulnerabilità dei sistemi e dei dispositivi di automazione diventino sempre più un punto aperto e che deve essere affrontato.

Inoltre, considerate le evoluzioni del settore produttivo, si rende necessaria la standardizzazione e la valorizzazione di una figura (esattamente come già previsto per i sistemi ICT) che abbia in carico la gestione del rischio di ogni potenziale *cyber* attacco e sia in grado di valutare, intervenire e mitigare il rischio, oltre che le conseguenze di eventuali eventi minacciosi: l'OT Cyber Security Expert.

https://www.cepas.it/webinar-al-via-la-certificazione-di-competenze-professionali-degli-ot-cyber-security-expert/

CEPAS *– Eventi – 4 giugno 2021*

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

A Roma la 7th EDEN Conference on data protection in law enforcement - Si terrà a Roma il 18 e 19 ottobre p.v., all'Auditorium della tecnica, la 7th EDEN Conference on data protection in law enforcement.
E' una interessante conferenza internazionale, organizzata da ERA (Accademia Europea di Diritto) in collaborazione con la Polizia Italiana ed Europol's Data Protection Experts Network (EDEN) diritto, nella quale si affronteranno temi di data protection, AI, machine learning, data bias ecc.
Prossimamente sarà resa nota l'agenda con il programma e la descrizione dei panel. Il link all'evento è il seguente: https://www.era.int/cgi-bin/cms?_SID=885ede4b6519453fd72b2911c71b71b8835ef22000784608450084&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=130784

A causa dell'emergenza Covid 19 gli eventi in presenza sono ancora rinviati a data da destinarsi. Stiamo programmando l'attività dei Colloquia in modalità online. Vi terremo informati.

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

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

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	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente usare il seguente 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*