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. 3/ 2021	Marzo 2021

Minacce al dominio Spazio
Le infrastrutture critiche dello spazio e le aziende del comparto a rischio di targetizzazione della minaccia Cyber

Le economie globali, i governi in aggiunta al settore militare, si stanno affidando sempre più alle infrastrutture spaziali e questa tendenza ha portato a una crescente gamma di minacce informatiche destinate ad attaccare i sistemi spaziali come anche le aziende del settore Spazio.
Gran parte delle infrastrutture critiche del mondo dipende fortemente dalle risorse spaziali, per il funzionamento quotidiano. I sistemi essenziali come le comunicazioni, il trasporto aereo, il commercio marittimo, i servizi finanziari, il monitoraggio meteorologico e la difesa si basano sulle infrastrutture spaziali, inclusi i satelliti, le stazioni di terra e i collegamenti dati a livello nazionale, regionale e internazionale. Nell'ambito civile sono molteplici i servizi abilitati dal segmento satellitare: segnali tv (TVsat), app e servizi georeferenziati per fare due esempi comuni e molti altri ne nasceranno. È infatti, notizia di ottobre 2020 l'avanzamento del programma dell'internet satellitare di Space X di Musk per offrire servizi internet a basso costo. Ma nei prossimi anni si prevede che vengano lanciati migliaia di nuovi satelliti commerciali come risultato di una nuova fase della guerra economica globale tra Stati Uniti, Russia, Cina. Proprio la contrapposizione fra stati (Cyberwarfare) potrebbe causare scontri Cyber in ambito Spazio per puntare i satelliti ed interrompere le comunicazioni o i flussi di informazioni vitali per il commercio e la sicurezza. Cina, Russia e altri stati-nazione possiedono già le capacità per eseguire un attacco informatico sull'alta frontiera. Sul fronte del Cybercrime invece, la moltitudine di satelliti, i servizi correlati e soprattutto il traffico di dati conseguente, li renderanno un obiettivo molto attraente per gli i criminali digitali: quanto più le comunicazioni o i servizi si basano sulle tratte satellitari come sistemi abilitanti, tanto maggiore questa porzione di infrastruttura potrebbe essere oggetto di attacchi lucrativi.
Come ogni altra infrastruttura critica sempre più digitalizzata, i satelliti e altre risorse spaziali sono vulnerabili agli attacchi informatici. Queste vulnerabilità informatiche comportano gravi rischi non solo per le risorse spaziali stesse, ma anche per le infrastrutture critiche a terra. Il rischio a livello mondiale riguarda lo sviluppo economico e la sicurezza internazionale. Non stupisce quindi che dal punto di vista militare lo spazio sia già da tempo acclarato come dominio della conflittualità fra Stati, mentre da dicembre 2019, i ministri degli esteri della NATO lo hanno formalmente dichiarato come un "dominio operativo", estendendo la gamma dell'alleanza dalla terra, dal mare, dall'aria e dal cyberspazio alle operazioni nello spazio.

La possibilità di manipolare oggetti remoti come i satelliti rappresenta una nuova sfida per la comunità degli attaccanti e il rischio potenziale è correlato alla possibile interruzione o anomalia dei servizi satellitari e tutte le applicazioni digitali loro connesse. Un cyberattacco nello spazio potrebbe assumere diverse forme, tra cui il furto di dati satellitari e malware per disabilitare fisicamente un veicolo spaziale o tirarlo fuori dall'orbita prevista per danneggiare un altro satellite. In particolare, le minacce informatiche ai sistemi spaziali coprono un'ampia gamma, dalle vulnerabilità nei segmenti fisici di terra

e spazio ai collegamenti dati dei satelliti e alle catene di approvvigionamento. Le minacce ibride (asimmetriche, non tradizionali) diventano l'arma prescelta per attori statali per destabilizzare e sovvertire, mentre il cybrecrime le usa per lucrare.
I sistemi spaziali sono solitamente suddivisi in tre segmenti tecnologici e operativi, che sono responsabili di diverse funzioni e sono quindi esposti a diverse minacce informatiche: il segmento di terra, il segmento spaziale e il segmento di collegamento. Nel **segmento di terra** a causa delle attività di C&C e gestione del satellite e dei dati verso le destinazioni finali, le minacce più impattanti riguardano: l'esfiltrazione di dati (per spionaggio o rivendita), l'interruzione dei servizi o il blocco operativo rispettivamente a mezzo di DDOS o Ransomware; attacchi che sfruttano le vulnerabilità del Web per scaricare malware e trojan con vettori: phishing, smishing, vishing sui computer della stazione di terra. Il **segmento spaziale tipicamente** violato solo dopo il segmento di terra, risente di: vulnerabilità nei componenti di rete o nei ricevitori dei dati dal satellite con il rischio di cambio rotte o di interruzione dei servizi; tentativi di persistenza in cui l'infiltrazione serve per intercettare le comunicazioni a mezzo malware che alterino la catena di trasmissione o di approvvigionamento provocando danneggiamenti non immediati. Nel **segmento di collegamento:** la minaccia fisica riguarda jamming e spoofing. Nel primo la trasmissione è interrotta dai jammer GPS causando lo stop dei segnali e l'interruzione del servizio, nel secondo, incentrato sulla falsificazione di segnale, l'attacco mira a distorcere le comunicazioni creando situazioni ingannevoli a vantaggio degli attaccanti. In ultimo l'intercettazione del traffico non crittografato da parte di un attaccante (MitM) permette l'esfiltrazione di dati.
Progressivamente nuove vulnerabilità sono scoperte nell'ambito dei sistemi spaziali, ma naturalmente cresce anche il numero degli studi specifici che spiegano come hardenizzare i sistemi spaziali. L'attenzione sul tema è così alta che ad esempio l'Air Force e il Defense Digital Service del DOD nel 2020 hanno organizzato un concorso inteso a stimolare l'interesse per la sicurezza informatica aerospaziale. La sfida dal nome "Hack-A-Sat" ha permesso ai partecipanti white di prendere il controllo di un satellite, dimostrando il motivo per cui la protezione delle risorse spaziali dalle minacce informatiche debba essere una nuova priorità.

Tipicamente la mitigazione delle minacce informatiche ai sistemi spaziali può essere suddivisa in soluzioni tecnologiche, che consistono nell'introduzione di nuove tecnologie o nell'aggiornamento di quelle esistenti e in soluzioni in ambito sviluppo di politiche e protocolli di condotta.
A titolo di esempio nel contesto delle soluzioni tecnologiche, si può citare la modernizzazione dei sistemi di controllo a terra GPS per supportare un segnale GPS anti-jamming denominato M-Code, che consentirà all'Air Force americana di continuare a utilizzare la costellazione GPS3 con i sistemi di terra esistenti fino al 2025 o la nuova architettura satellitare definita da software chiamata SmartSat come soluzione per il segmento spaziale, che consentirà maggiori capacità e un maggiore controllo dei satelliti in orbita per gli operatori di terra, una maggiore precisione nella diagnosi di problemi come gli incidenti informatici, oltre a consentire ai satelliti di sostenersi a vicenda. (Lockheed Martin). Nel gennaio 2019, la NASA ha invece annunciato che avrebbe iniziato a testare una piattaforma Blockchain open source per affrontare potenziali problemi di privacy e per prevenire spoofing, DoS e altri attacchi.
In termini di policy una prima soluzione è stata la Cybersecurity Maturity Model Certification (CMMC) che è stata introdotta dal Dipartimento della Difesa degli Stati Uniti per tutti gli appaltatori della difesa, compresi i piccoli fornitori. Un tale modello di standard di sicurezza informatica dovrebbe essere una condizione soglia per le offerte per i contratti governativi. Inoltre, è probabile che l'adozione di standard rigorosi nei contratti governativi introdurrà cambiamenti nell'intero settore e contribuirà quindi a promuovere la sicurezza delle tecnologie commerciali e standard.

Tuttavia, specificatamente per il settore Spazio all'inizio di settembre la Casa Bianca ha pubblicato una nuova direttiva di politica spaziale, volta a migliorare la sicurezza informatica dei sistemi spaziali. I principi della direttiva comprendono l'uso dell'autenticazione e della crittografia nei collegamenti di comando e controllo da e verso i satelliti, la protezione contro il jamming e lo spoofing delle comunicazioni e la protezione dei sistemi terrestri e dei sistemi di elaborazione delle informazioni. Tuttavia, non esistono piani ufficiali per indirizzare le agenzie a codificare questi principi in regolamenti, che potrebbero non essere sufficienti a proteggere l'infrastruttura spaziale dalle nuove minacce emergenti. Il memorandum parla di "*full life-cycle cybersecurity* " e l'Intelligenza Artificiale può essere la soluzione per implementarlo, poiché in grado di comprendere come sono le normali operazioni di un sistema per individuare automaticamente qualsiasi anomalia prima che si verifichino troppi danni.
Per essere più specifici sulle azioni di remediation è possibile consultare un elenco non esaustivo di sette elementi di sicurezza per la difesa di risorse e satelliti spaziali, insieme a reti di volo di controllo a terra adattato da "Defending Spacecraft in the Cyber Domain" e da fonti governative ad opera di Paul Ferrillo and Chuck Brooks in "Protecting Space-Based Assets from Cyber Threats".

Alessia Valentini
Consulente di Cybersecurity, Advisor e Giornalista. Attualmente in Gruppo Daman svolge attività di Advisor, Business Developer e Consulente di Cybersecurity. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016

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/*

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

NUOVO GRUPPO DI LAVORO AIIC
ANALISI DEI RISCHI NELLE INFRASTRUTTURE CRITICHE

Il Consiglio Direttivo di AIIC ha approvato la costituzione di un nuovo Gruppo di Lavoro su "Analisi dei rischi nelle Infrastrutture Critiche". Il GdL sarà coordinato inizialmente dal consigliere Glauco Bertocchi. Si invitano i soci che lo desiderano di comunicare il proprio interesse a partecipare inviando una mail di adesione a segreteria@infrastrutturecritiche.it.
Ricordiamo che la partecipazione ai Gruppi di Lavoro AIIC è riservata ai soci AIIC in regola con il pagamento delle quote sociali.

NEWS E AVVENIMENTI

L'allarme di Clusit: "Serve un piano nazionale Cybersecurity 4.0" - Un Piano Nazionale #CyberSecurity4.0 che premi la componente di cybersecurity in tutti i progetti innovativi e di consolidamento del digitale nelle imprese italiane**,** con voci e misure specifiche, come già accaduto per Industry 4.0. E' la proposta avanzata dal Clusit**, l'**associazione italiana per la sicurezza informatica, durante un'audizione informale alla Commissione Difesa del Senato della Repubblica**.**
All'incontro Clusit ha evidenziato come gli attacchi informatici diretti a Enti Governativi, Infrastrutture Critiche e Government Contractors continuino a crescere: negli ultimi tre anni e mezzo, secondo il rapporto Clusit, sono stati 951 gli attacchi gravi diretti a questi settori. Il 22% del totale degli attacchi rilevati nei primi 6 mesi dell'anno hanno evidenziato una severity che è stato definita "Critica" ed "Alta". A questo, si deve anche associare che il settore militare e quello civile sono caratterizzati da interessi

ed esigenze nazionali convergenti, con la soglia di attenzione che deve rimanere al massimo livello. "Non è pensabile perseguire una resilienza strutturale agli attacchi cyber – ha sottolineato durante l'audizione Gabriele Faggioli , presidente di Clusit – senza che l'intero ecosistema nazionale operi sinergicamente, sia per quanto riguarda la strategia che nelle azioni tattiche".
Tre gli interventi più urgenti che Clusit ha proposto durante l'audizione: provvedimenti per supportare la trasformazione organizzativa delle imprese sui mercati di riferimento. Innanzitutto, l'obbligo di dotarsi della figura di Chief Information Security Officer **(**Ciso**)** e, per determinati contesti, di certificazioni «accountable», come ad esempio l'Iso 27001. Il secondo suggerimento è rivolto a favorire la transizione al cloud con modalità che tengano conto di esigenze di cyber security e data protection, anche grazie a "certificazioni di security", mentre il terzo è rivolto all'accelerazione del processo di assunzione da parte del mercato di prodotti IoT e tecnologie "*cyber sicuri by default*", sia per il cittadino che per le organizzazioni pubbliche e private, visti anche i nuovi requisiti normativi, quali, per esempio, il Cybersecurity Act**.**
https://www.corrierecomunicazioni.it/cyber-security/lallarme-di-clusit-serve-un-piano-nazionale-cybersecurity-4-0/
Corcom *– A. S. – 11 gennaio 2021*

Operatori di servizi essenziali (OSE): chi sono e quali obblighi di sicurezza hanno - Nell'ambito di applicabilità della Direttiva NIS, gli operatori di servizi essenziali sono chiamati a contribuire al raggiungimento di una corretta postura di sicurezza del nostro Paese. Ecco chi sono gli OSE e i loro obblighi in materia di cyber security.
La Direttiva NIS (Direttiva UE 2016/1148), recepita in Italia con D.lgs. 18 maggio 2018 n. 65 con l'intento di conseguire un elevato livello di sicurezza delle reti e dei sistemi informativa e incrementare il livello comune di sicurezza dell'Unione europea, ha stabilito anche i requisiti minimi di sicurezza informatica per gli operatori di servizi essenziali (OSE).
Indice degli argomenti

Chi sono gli operatori di servizi essenziali (OSE)
Si definiscono operatori di servizi essenziali (OSE) i soggetti pubblici o privati che soddisfano i seguenti criteri:
un soggetto fornisce un servizio che è essenziale per il mantenimento di un'attività sociali e/o economiche fondamentali;
la fornitura di tale servizio dipendente dalla rete e dai sistemi informativi;
un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.
(segue)
https://www.cybersecurity360.it/cybersecurity-nazionale/operatori-di-servizi-essenziali-ose-chi-sono-e-quali-obblighi-di-sicurezza-hanno/
Cybersecurity360 *- Serena Nanni - 29 gennaio 2021*

Logistica del freddo: cos'è, come funziona e come viene usata l'IoT - La logistica del freddo è l'insieme delle attività che servono a mantenere la catena del freddo, ovvero la temperatura adeguata

per tutto il ciclo di vita del prodotto. Usata in ambito alimentare e farmaceutico, come può essere migliorata attraverso l'adozione di soluzioni IoT?

Indice degli argomenti

Cos'è la logistica del freddo
Come funziona?
Come viene usata l'IoT nella logistica del freddo e con quali vantaggi
Il controllo dei processi
L'efficienza energetica
L'ottimizzazione della velocità operativa

Cos'è la logistica del freddo

La logistica del freddo è l'insieme delle attività organizzative, gestionali e strategiche che servono a mantenere la catena del freddo.

Il sistema logistico (industrial supply chain) comprende le infrastrutture, le attrezzature, le risorse e le strategie operative che gestiscono il flusso delle merci e le relative informazioni in ogni fase del ciclo del prodotto: dalla fornitura dei materiali alla trasformazione fino alla sua consegna al cliente finale e, se contemplato, al postvendita.

Un sistema complesso, che nel caso della catena del freddo si caratterizza per una sfida aggiuntiva: assicurare in ogni passaggio la continuità della temperatura stabilita, al di sotto dello zero.

La logistica del freddo non riguarda solo il passaggio delle merci dagli impianti di produzione ai centri di distribuzione ma segue tutto il ciclo del prodotto, che necessita delle basse temperature per conservare intatte le proprietà organolettiche, nel caso di alimentari, o curative, nel caso dei farmaci. Gli ambiti in cui viene utilizzata la logistica del freddo sono infatti principalmente l'agroalimentare e il farmaceutico.*(segue)*

https://www.internet4things.it/iot-library/logistica-del-freddo-cose-come-funziona-e-come-viene-usata-liot/

***INTERNET4THINGS** - Josephine Condemi - 26 Febbraio 2021*

Come l'IIoT sta cambiando la fabbrica - Le informazioni generate grazie all'IIoT, creano nuove logiche di analisi degli indici di efficienza da applicare alle prestazioni dei processi, dando la possibilità di scoprire potenziali problemi. L'integrazione con i sistemi ERP permette di avere una migliore pianificazione e un utilizzo efficiente della capacità produttiva

Il mondo dello smart manufacturing è basato su tecnologie, software e componenti hardware che devono integrarsi tra loro per generare le informazioni che permettono alla fabbrica 4.0 di essere competitiva, efficiente e sostenibile. Come si possono raggiungere questi risultati? La risposta sta nel mix di IoT e Industrial IoT (IIoT).

Indice degli argomenti

Cos'è l'Industrial IoT
I vantaggi dell'IIoT
Esempi di applicazione in fabbrica
Il ruolo del digital twin nella fabbrica 4.0
Un nuovo tipo di valore dalle tecnologie connesse
Il futuro dell'IIoT verso il 5G

Cos'è l'Industrial IoT

L'IoT è in continua espansione e diffusione verso più settori, diventando un pilastro dell'interazione nella gestione della produzione. Dall'IoT nasce la sua evoluzione: l'IIoT, che permette di connettere tra loro le macchine intelligenti e sviluppare quei dati preziosi per l'intero processo aziendale. L'IIoT identifica nuove soluzioni tecnologiche come, ad esempio, piccoli sensori ambientali fino ai cobot –

robot collaborativi industriali. Ciò sottolinea l'importanza e la stretta relazione tra IoT, IIoT e tecniche di produzione avanzate verso una rivoluzione industriale che vede protagonista una fabbrica interconnessa, capace di comunicare, analizzare e utilizzare le informazioni per guidare le azioni necessarie. *(segue)*
https://www.internet4things.it/industry-4-0/come-liiot-sta-cambiando-la-fabbrica/
INTERNET4THINGS *- Stefano Massari, 16 febbraio 2021*

Sicurezza nel cloud: come Amazon, Google e Microsoft proteggono i nostri dati con la crittografia - Con l'aumentare delle aziende che si avvalgono di un Cloud Service Provider (CSP) come parte integrante del loro business, aumentano gli interrogativi in merito alla sicurezza nel cloud, a come i dati siano protetti e se queste misure sono sufficienti.
Tutti i grandi attori di questo settore offrono servizi crittografici che permettono di proteggere la confidenzialità e l'integrità dei dati che vengono trasferiti nel cloud.
In particolare, sono due i servizi crittografici messi a disposizione da AWS, GCP e Azure (il cloud di Amazon, Google e Microsoft, rispettivamente), i quali vengono usati in combinazione con gli altri servizi offerti dai vari CSP per aumentare la protezione delle applicazioni e servizi implementati in questi cloud.
In particolare, questi servizi crittografici sono, da una parte, il *Key Management Service (KMS)* e, dall'altra, il *Cloud Hardware Security Module (Cloud HSM).*
Ci si domanda, però, qual è il vantaggio di usare i servizi crittografici di AWS, GCP e Azure rispetto all'implementarsi le primitive crittografiche necessarie da sé. *i*n effetti è vero che occuparsi della crittografia da sé diminuisce la dipendenza del proprio sistema da un sistema terzo che non sarà mai completamente trasparente e vigilato.
Sono moltissime le vulnerabilità introdotte involontariamente dagli sviluppatori di applicazioni che richiedono l'uso di crittografia e che possono venire sfruttate facilmente da terzi per accedere ai dati sensibili. Questo espone tutto il sistema di protezione dati a rischi elevati: l'applicazione potrebbe essere implementata in modo tale da lasciar fuoriuscire delle informazioni verso un'altra applicazione gestita da un altro utente, potenzialmente un hacker. Tale hacker potrebbe agilmente accedere alle chiavi crittografiche usate per la cifratura dei dati sensibili dell'applicazione esponendoli a rischio. Ecco perché molto spesso conviene delegare la parte crittografica di un'applicazione o un servizio a terzi, specialmente nel caso in cui il gruppo di sviluppatori non ha un forte background in crittografia.
Tuttavia, non esiste un servizio di crittografia che sia il migliore in assoluto. Dipende sempre dal tipo di applicazione che si vuole far migrare nel cloud e dal tipo e dalla quantità di dati sensibili o di operazioni critiche di cui si ha bisogno.
Il tutto va scelto anche in termini di costo e del tipo di investimento che si vuole fare per rendere un'applicazione o un servizio sicuro.
https://www.cybersecurity360.it/soluzioni-aziendali/sicurezza-nel-cloud-come-amazon-google-e-microsoft-proteggono-i-nostri-dati-con-la-crittografia/
Cybersecurity 360 *– Giulia Traverso – 18 febbraio 2021*

La telemedicina entra nel Servizio Sanitario Nazionale - A seguito dell'approvazione da parte della Conferenza Stato-Regioni delle Linee guida predisposte dal Ministero della Salute. Un passaggio importante verso la definizione di nuovi standard per l'erogazione della prestazione medica a distanza tramite tecnologie IoT
Dopo una lunga attesa, a dicembre 2020 la telemedicina ha compiuto un passo fondamentale per il suo ingresso nel Servizio Sanitario Nazionale, a seguito dell'approvazione da parte della Conferenza Stato-

Regioni delle Linee guida predisposte dal Ministero della Salute. Un passaggio senz'altro importante verso la definizione di nuovi standard per l'erogazione della prestazione medica, che tuttavia non può prescindere da ulteriori attente valutazioni per una sua completa e corretta attuazione.

Indice degli argomenti

Le opportunità della medicina digitale

Quando si parla di eHealth (o digital health o ancora smarthealth) si fa riferimento, secondo la definizione dell'Organizzazione Mondiale della Sanità (OMS), all'applicazione delle tecnologie dell'informazione e della comunicazione (ICT) in ambito sanitario per la gestione di attività quali, ad esempio, la diagnosi, il trattamento e, più in generale, la gestione della cura del paziente mediante l'uso della rete e delle tecnologie digitali, tra le quali ha un posto d'onore l'Internet of things.

Il modello della digital society, che pervade sempre maggiormente ogni ambito umano, non ha risparmiato quello della sanità che, così come accaduto con lo smart working per la modalità con cui è resa la prestazione lavorativa, ha trovato nell'emergenza pandemica da Covid-19 una valida alleata per accrescere la diffusione della "medicina connessa". (*segue)*

https://www.internet4things.it/smart-health/la-telemedicina-entra-nel-servizio-sanitario-nazionale/

INTERNET4THINGS.IT *- Lorenzo Giannini, 19 Febbraio 2021*

IoT nelle città del futuro: le persone al centro - Finora l'utilizzo dell'IoT combinato con l'AI nelle metropoli è stato "technology driven", le esigenze delle persone sono rimaste in secondo piano ma la pandemia ci dà l'occasione per ripensare un nuovo paradigma che generi di servizi legati al reale benessere dei cittadini. Notevole sarebbe l'impatto non solo socio sanitario, spiega Gian Marco Revel, ma anche economico.

Su scala urbana l'**azione combinata di IoT e intelligenza artificiale** sta abilitando una serie di nuovi scenari ma con l'arrivo della pandemia quelli che abbiamo iniziato ad intravvedere negli scorsi mesi hanno subito "forti ricondizionamenti". Questo momento di discontinuità è l'occasione per ripensare al paradigma che guida l'utilizzo di queste tecnologie per immaginare una città del futuro con al centro le persone. Lo suggerisce Gian Marco Revel, Professore Ordinario di Misure, Università Politecnica delle Marche che, data l'estrema flessibilità di impiego dell'IoT combinato con l'AI, invita tutti a "cercare di comprendere come applicare nel proprio settore la possibilità offerta da questo connubio tecnologico di interpretare sensazioni, reazioni ed esigenze delle persone, partendo dalla grossa quantità di dati generati".

Revel è intervenuto al recente Richmond IT Director Forum, una convention di 3 giorni che solitamente raduna a Rimini decine di CIO, IT manager, Direttori IT e rappresentanti del mondo dell'offerta ma che quest'anno, a causa dell'emergenza sanitaria, si è tenuta interamente online.

Indice degli argomenti

- Da sperimentazioni a business: servono iniziative pilota
- Da technology driven a people driven, un cambio di paradigma urgente

(segue)
https://www.zerounoweb.it/cio-innovation/iot-nelle-citta-del-futuro-le-persone-al-centro/
***ZEROUNOWEB** - Marta Abba' – 4 febbraio 2021*

Sempre più IoT nell'industria - L'internet of things è vista come un'opportunità per rivedere il framework digitale della fabbrica e della supply chain e le strategie di vendita.
Il processo di adozione delle tecnologie IoT nell'industria è ormai avviato verso una piena maturità. Le prime esperienze sono state largamente trainate dal tentativo di dimostrare che l'introduzione di tecnologie IoT nello shop floor portava all'azienda benefici immediati in termini di riduzione dei costi e dei rischi di fermo attraverso progetti tesi a transitare da un modello di manutenzione basato sulla programmazione ciclica rigida e risoluzione dei guasti a un modello predittivo.
Indice degli argomenti
L'Internet of Things nell'industria, opportunità di innovazione
Trasformare il mondo industriale nell'interfaccia di un computer
Le conseguenze della convergenza digitale sulla mediamorfosi
L'evoluzione della fabbrica 4.0
Conclusioni
(segue)
https://www.internet4things.it/iot-library/sempre-piu-iot-nellindustria/
***INTERNET4THINGS** - Nicola Gulli - 29 Gennaio 2021*

Vaccini anti-Covid in vendita nel dark web, fino a 1.200 dollari per dose - Già effettuate centinaia di transazioni in criptovaluta per l'acquisto di Pfizer/BioNTech, AstraZeneca e Moderna. Secondo Kaspersky, il rischio è altissimo: "*Impossibile stabilire che sostanze contengano*". Hanno un prezzo medio di circa 500 dollari a dose. Gli acquisti avvengono tramite app di messaggistica criptate come Wickr **e** Telegram**.** I pagamenti vengono richiesti sotto forma di criptovaluta e principalmente bitcoin, molto più difficile da tracciare. Secondo Kaspersky, la maggior parte dei venditori ha sede in Francia, Germania, Regno Unito e Stati Uniti.
Esaminando 15 diversi marketplace su Darknet, i ricercatori di Kaspersky hanno individuato messaggi pubblicitari per tre dei principali vaccini Covid disponibili, Pfizer/BioNTech, AstraZeneca e Moderna**,** ma anche per altri non certificati.
La maggior parte dei venditori illegali ha effettuato circa 100-500 transazioni di vendita, ma, annota *Kaspersky*, "non è chiaro cosa stiano davvero acquistando gli utenti Darknet". È infatti impossibile stabilire quante delle dosi di vaccino commercializzate online siano reali (molte strutture mediche si sono trovate con dosi avanzate) e quanti annunci siano in realtà una truffa. Non solo per le dosi di vaccino, ma anche per i falsi certificati di vaccinazione: "*Si tratta di documenti che consentono di spostarsi da un luogo all'altro liberamente – dice Dmitry Galov, security expert di Kaspersky -. Raccomandiamo agli utenti di diffidare di qualsiasi "affare" legato alla pandemia e ricordiamo che, naturalmente, comprare un vaccino su una Darknet non è una buona idea*".
Si sconsiglia di comprare dosi di vaccino o altri prodotti nel dark web e si invita a controllare attentamente l'Url dei siti visitati che riportano annunci pubblicitari sul Covid: "*Lettere fuori posto o domini inusuali come .com.tk invece del noto .com* – fa sapere l'azienda – *aiutano a identificare i tentativi di phising. In questo caso, non inserire mai informazioni personali sul sito sospetto*". Per finire, "*prestare attenzione alla grammatica e al layout dei siti visitati e delle e-mail ricevute*".

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

Check Point Research mette in guardia dalle truffe sui siti web legati ai vaccini, poiché ha documentato un aumento del 300% nelle registrazioni di domini legati ai vaccini, negli ultimi 8 mesi, e un aumento del 29% del numero di siti web ritenuti pericolosi. Di recente un hacker ha progettato un sito web spacciandosi per il Cdc, nel tentativo di rubare le credenziali Microsoft.
https://www.corrierecomunicazioni.it/cyber-security/vaccini-anti-covid-in-vendita-nel-dark-web-fino-a-1-200-dollari-per-dose/
Corcom *- L.O. – 5 marzo 2021*

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 — Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo

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

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