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. 4/ 2021** | **Aprile 2021**

La convergenza IT/OT. A che punto siamo?

L'ultima mail (31 marzo) proveniente da **ISA** (International Society for Automation) (www.isa.org), riporta l'annuncio di 9 webinar che trattano di Cybersecurity, IIoT, Industrial IT, IT/OT convergence. La convergenza tra il "mondo" **IT** (information Technology) e quello **OT** (Operational Technology) è un argomento che sembra rivestire un sempre maggior interesse, specie in relazione alla cybersecurity che coinvolge sempre più il mondo dell'automazione, una volta regno incontrastato degli specialisti dei sistemi di controllo. La storia di questo "matrimonio", che forse non si è ancora celebrato, inizia oltre 20 anni fa con i primi tentativi di utilizzo delle tecnologie IT in ambito industriale. Allora ci si preoccupava per la possibilità di dotare i **PLC** (Programmable Logic Controller) di una porta Ethernet con tutte le conseguenti possibilità, e i rischi, di agevole connessione al mondo TCP/IP. Da allora la situazione è enormemente evoluta e oggi è normale parlare di sistemi **ICS** (Industrial Control System)/ **SCADA** (Supervisory control and data acquisition) in cloud. In realtà l'evoluzione tecnologica ha reso sempre meno definiti gli ambiti e le definizioni funzionali di tali sistemi

La spinta maggiore a questa progressiva "invasione" è stata ovviamente quella economica. Le tecnologie IT, grazie alla loro diffusione, costano meno sia in termini di acquisizione che di mantenimento e la loro evoluzione tecnologica è più veloce e meno costosa. Quindi grandi opportunità ma anche maggiori rischi derivanti dal cyber crime, nelle sue varie forme, al quale si è improvvisamente aperto un nuovo "mercato".

Negli ultimi 5 anni si sono anche affermate nuove tecnologie e concetti (l'intelligenza artificiale, l'Internet delle cose, Block-chain) che hanno reso sempre meno definito il confine tra IT e OT. In particolare, l'Internet delle cose (**IoT)** ha decisamente esteso il panorama degli "oggetti" connessi includendo anche i sensori e gli attuatori che sino ad alcuni anni fa erano i tipici elementi della OT. In pratica IoT ha abolito i limiti e i perimetri tradizionali con i quali siamo stati abituati a definire, e quindi a difendere, i sistemi informatici, inclusi quelli per uso industriale.

Questa evoluzione non è, ovviamente, sfuggita ai vari enti di normazione e standardizzazione che, con approcci molto differenziati, hanno cercato di "inseguire" il fenomeno e fornire definizioni e metodiche per migliorare l'uso e la sicurezza. Inoltre il mondo IoT ha non solo problemi di sicurezza, intesa nella duplice accezione di safety e security, ma anche di tutela dei dati personali che potrebbero essere presenti o in transito negli apparati IoT.

ENISA (European Union Agency for Network And Information Security) ha sinora dedicato circa 20 documenti al mondo IoT e alle sue declinazioni, tra cui IIoT (Industrial Internet of Things) in particolare in connessione con lo Smart Manufacturing. ENISA definisce IoT come un ecosistema all'interno del quale sono presenti apparati IoT. Ogni settore di applicazione (trasporti, medicina, consumer, ecc.) definisce un ecosistema con le sue minacce e i suoi asset da proteggere. Vengono anche identificati gli standard e le best practices da applicare all'ecosistema considerato.

Molto diverso appare l'approccio dell'americano **NIST** (National Institute of Standards and Technology) il cui focus sono le caratteristiche di sicurezza dell'IoT come apparato. I documenti riguardano gli obiettivi di tutela della sicurezza e della privacy con cui gli apparati IoT devono essere progettati e le raccomandazioni per i costruttori di IoT. Da evidenziare che i documenti NIST esplicitano le misure proposte in termini di controlli specificati dal **NIST SP 800-53 r5** che rappresenta la "Bibbia" dei controlli di sicurezza in ambito forniture IT al governo federale.

L'ISO (International Standard Organization) ha prodotto oltre 150 documenti classificati come IoT ma, il focus varia secondo le finalità del Sottocomitato (SC) coinvolto. ISO sta lavorando sull'IoT in quanto dispositivi e non come ecosistema. Questo approccio è coerente con la storia dell'organizzazione che mira a emettere standard per i prodotti e le industrie correlate. A titolo di esempio si può citare lo SC41 "Internet of Things e tecnologie correlate", creato per esaminare l'IoT. Questo Sottocomitato si concentra principalmente sui sensori IoT (rete, architettura di riferimento, test, sensori specializzati (acustica subacquea, contatore del gas, sottostazioni elettriche, IoT industriale, ecc.)).
Di particolare rilievo appare lo sforzo congiunto **ISA** (International Society for Automation) e **IEC** (International Electrotechnical Commission) per il completamento dell'architettura **ISA/IEC 62443** relativa alla sicurezza degli IACS (Industrial Automation and Control Systems). Questi ultimi sono definiti come: raccolta di personale, hardware, software, e di regole organizzative per il funzionamento del processo industriale che possono influenzare la sicurezza, la protezione e l'affidabilità operativa. L'architettura ISA 62443 include 4 serie di standard articolati sui seguenti livelli General, Policies and Procedures, System, Component.
Come si può desumere dalla quantità di documentazione disponibile la convergenza IT/OT è in corso da tempo. Inoltre, l'evoluzione tecnologica, forse più veloce dei tentativi di classificazione e definizione di architetture, sta rendendo sempre meno definite categorie una volta immutabili.
Forse la domanda da porsi non è quando avverrà questa convergenza ma, piuttosto, quali sono i requisiti irrinunciabili del settore industriale che lo caratterizzeranno anche in futuro.
Sicuramente il primo requisito è quello del rispetto delle normative di safety per assicurare il corretto funzionamento degli apparati ed evitare incidenti che potrebbero causare danni a persone e cose. La cybersecurity viene dopo la safety e comunque dovrebbe evitare che venga compromessa la safety. Analoghe considerazioni valgono per le esigenze di continuità e i vincoli derivanti in termini di manutenzione e aggiornamento software; il ciclo frenetico di patches del mondo IT non è compatibile con la continuità e il mantenimento delle certificazioni di safety proprie delle installazioni industriali. Infine, la vita operativa degli apparti OT è molto superiore ai 10 anni, un'era geologica per il mondo IT.
Personalmente ritengo che l'attuale enfasi sulla convergenza abbia anche origine commerciali (ad esempio, Microsoft ha acquisito società che operano nel campo OT) e in realtà sia anche riconducibile, come evidenziato da alcuni, ad una differenza "culturale" tra i team IT e OT che si sono sviluppati in ambiti paralleli e adesso devono iniziare a "dialogare" e collaborare.
Come al solito il fattore umano è quello più difficile da "governare" e l'evoluzione verso un mondo sempre più complesso comporta, a mio parere, il definitivo riconoscimento della necessità di abbandonare l'approccio settoriale per adottare quello multidisciplinare.

Glauco Bertocchi
Laurea in Fisica all'Università di Roma "La Sapienza". Più di 40 anni di esperienza in Informatica e Sicurezza all'interno di Università e istituzioni nazionali. Certificato CISM and 27001 LA. Membro del CD di AIIC e Vice Presidente di ISACA Rome Chapter. L'attuale attività di ricerca è orientata alla protezione e alla resilienza delle Infrastrutture Critiche.

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

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
Principi e Tecnologie per la Protezione di Spazi Pubblici

Il Consiglio Direttivo di AIIC ha approvato la costituzione di un nuovo Gruppo di Lavoro su "Principi e Tecnologie per la Protezione di Spazi Pubblici (stazioni ferroviarie, sale aeroportuali, imbarchi portuali, stadi per concerti, ……..).

Il GdL sarà coordinato dal consigliere Sandro Bologna.

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.
Membri 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 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

Attacchi hacker contro la Sanità, allarme rosso al Governo - La relazione annuale del DIS (Dipartimento delle informazioni per la sicurezza) al Parlamento, delinea la nuova situazione della minaccia cibernetica in Italia. Attacchi sempre più sofisticati, contro la PA e in particolare aziende sanitarie, farmaceutiche. Speriamo che il Governo ne tenga conto in questa fase decisionale.
L'anno della pandemia ha generato un avanzamento tecnologico proiettandoci in avanti di circa quindici anni nella diffusione delle tecnologie di comunicazione remota a supporto del lavoro agile, ma questo salto in lungo è avvenuto senza le necessarie precauzioni in termini di sicurezza e di consapevole uso degli strumenti e della rete.
Indice degli argomenti
Attacchi cyber più sofisticati e mirati

PA locali bersagliate
Aziende farmaceutiche
Tecniche innovative, intervenga il Governo
https://www.agendadigitale.eu/sicurezza/attacchi-hacker-contro-la-sanita-allarme-rosso-al-governo/
Agenda Digitale - *Luisa Franchina, AIIC - 2 marzo 2021*

Smart city: come l'IoT può essere al servizio dei cittadini - In un futuro molto vicino l'IoT avrà un impatto sempre più significativo sui servizi pubblici e consentirà di generare nuovi modelli di governance e di revenue, ma soprattutto di creare servizi innovativi e personalizzati da quelli della mobilità, fino a quelli legati all'illuminazione pubblica con l'obiettivo, per gli Enti locali, di migliorare la qualità della vita degli utenti e ottenere di più sprecando di meno
IoT e nuove tecnologie al servizio dei cittadini: la "rinascita" delle città passa anche da qui, dalle Smart city, consentendo alle persone di vivere non solo in centri urbani più innovativi ma anche più sostenibili. Come? Rendendo più efficienti i servizi, a cominciare da quelli della mobilità, fino ad arrivare ai consumi legati all'illuminazione pubblica con l'obiettivo, per gli Enti locali, di migliorare la qualità della vita degli utenti e ottenere di più sprecando di meno.
Ci sono decine e decine di buone pratiche in tutta Italia, ma restano ancora poche se confrontate con le sfide dei nostri tempi e per questo diventa fondamentale per le Pubbliche Amministrazioni locali sfruttare al meglio le risorse economiche del Recovery Fund. Questo significa investire sui territori e credere, come l'emergenza Covid-19 ha ampiamente dimostrato, che la "rivoluzione digitale" ormai non è più rinviabile.
Indice degli argomenti
Verso la Mobility as a Service
Smart city: in Sicilia tre comuni sperimentano un progetto di illuminazione pubblica
Conclusioni *(segue)*
https://www.internet4things.it/smart-city/smart-city-come-liot-puo-essere-al-servizio-dei-cittadini/
INTERNET4THINGS *- Carmelo Bonaccorso e Paolo Lanari - 8 Marzo 2021*

Tecnologie per la sanità: le sei aree di modernizzazione definitiva - In tutto il mondo stiamo assistendo a una progressiva modernizzazione nell'ambito dell'assistenza sanitaria: ospedali, cliniche e altre strutture assistenziali che da anni stanno cercando di digitalizzare e automatizzare i processi di acquisizione e comunicazione dei dati hanno compiuto significativi progressi nell'utilizzo delle nuove tecnologie al fine di raggiungere gli obiettivi prefissati.
Il Covid-19 ha innescato il dubbio che ancora non si sia stato fatto abbastanza per migliorare l'assistenza fornita i pazienti in termini di qualità, efficienza e sicurezza.
In questi ultimi mesi c'è stato un più approfondito esame delle politiche, procedure, processi e dei sistemi interni a molte strutture sanitarie per capire se possono esserci margini di miglioramento nell'acquisizione, analisi e distribuzione dei dati in tempo reale.
In molti casi si è optato per accelerare l'effettiva implementazione delle tecnologie o potenziare soluzioni già in uso così da essere pronti ad affrontare qualsiasi scenario. Talvolta però questi cambiamenti non riescono a stare al passo con le effettive necessità del mercato.
L'implementazione immediata di soluzioni innovative ha dimostrato di poter avere un impatto rilevante su diversi aspetti in ambito sanitario: ad esempio si sono mobilitati team di assistenza e

automatizzati flussi di lavoro a livello clinico in tempi record, affrontando così alcuni dei problemi sistemici aggravati dall'epidemia di Covid-19.
È stato anche possibile implementare rapidamente diverse tecnologie mobile per contribuire ad aumentare l'efficienza e l'accuratezza delle procedure di presa in carico del paziente e delle azioni diagnostiche, riducendo inoltre il problema della mancanza di forniture mediche e delle notifiche del trattamento previsto. (*segue)*
https://www.01health.it/tecnologie/tecnologie-sanita-sei-aree-modernizzazione-definitiva/
01Health *- 9 Marzo 2021*

Italia e sicurezza: il 2020 è stato un annus horribilis - L'Italia nel 2020 è risultata a livello mondiale il quinto Paese più colpito dai macro-malware (primo in Europa), il settimo per attacchi malware e l'undicesimo per attacchi ransomware. I dati sono evidenziati in *A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report,* il report di Trend Micro Research sulle minacce informatiche che hanno colpito nel corso dell'anno 2020.
Nell'anno trascorso Trend Micro ha rilevato a livello globale 119.000 minacce al minuto, facendo registrare un +20% rispetto al 2019. Le cause di questo incremento sono conseguenza del lavoro da remoto che ha determinato l'incremento della pressione cybercriminale su molte infrastrutture. Gli attacchi alle reti domestiche sono infatti cresciuti del 210% raggiungendo i 2,9 miliardi. Il phishing continua a essere una delle tattiche più sfruttate dai cybercriminali; il 91% di tutte le minacce è arrivato infatti via email e gli URL unici di phishing intercettati sono stati 14 milioni. Il numero di vulnerabilità pubblicate dalla Zero Day Initiative di Trend Micro è cresciuto del 40%, per un totale di 1.453 vulnerabilità, l'80% delle quali è stato etichettato "ad alto rischio".
https://www.cwi.it/sicurezza/cybercrimine-hacking/italia-e-sicurezza-il-2020-e-stato-un-annus-horribilis-134749
Computer World – *Francesco Destri – 15 marzo 2021*

Smart building e sicurezza aziendale: le tecnologie di social distancing - Un ambiente di lavoro moderno (workplace) è quello spazio di lavoro che senza soluzione di continuità mette a disposizione dei lavoratori digital workplace, accessibili in ogni momento e da qualunque località e dall'altro smart office, uffici che integrano tecnologie digitali per la gestione degli accessi, l'organizzazione degli spazi e la garanzia di sicurezza
Garantire la sicurezza in azienda, adeguarsi alle nuove norme, proteggere la salute delle persone, ripensare i propri spazi, modificare le procedure: nell'ultimo anno le organizzazioni di tutti i settori e di tutte le dimensioni sono state chiamate a mettere in atto numerosi cambiamenti per poter operare in tempo di pandemia da Covid-19. In questa fase di emergenza, molte imprese hanno avviato (o, in altri casi, accelerato) un processo di trasformazione che ha portato allo sviluppo di un ambiente di lavoro moderno, adatto alla gestione della nuova normalità con da un lato la creazione di digital workplace, ambienti di lavoro digitali che favoriscono la gestione delle attività in remoto, dall'altro l'integrazione di tecnologie IoT e soluzioni mobile funzionali alla messa in sicurezza degli spazi fisici, ovvero soluzioni di smart building.
Indice degli argomenti
Dal digital workplace allo smart building
Le tecnologie di social distancing e l'importanza dell'employee empowerment
L'importanza dell'employee empowerment per il modern workplace
(segue)

https://www.internet4things.it/smart-building/smart-building-e-sicurezza-aziendale-le-tecnologie-di-social-distancing/
INTERNET4THINGS *- Andrea Romanello, Fabrizio Bottino, Giovanni Quaranta, 18 Marzo 2021*

Top 3 Cybersecurity Lessons Learned From the Pandemic. Defending an enterprise of fully remote employees and their devices at this scale and speed had never been done before. Now, we do it every day. Cybersecurity professionals are always prepared to adapt. Our function is centered around potential risk and the ability to instantly respond to new threats and events that could put our organizations and their people in harm's way. An enormous amount of preparation and planning always needs to be in place — with a clear process and playbook to execute or a fundamental capability to fall back on in any given scenario. But in March 2020, the world faced a scenario beyond the scope of anything we'd seen before. Companies were forced to move from reasonably well-defined enterprise infrastructures inside office buildings to a wide range of individual remote users signing in from countless access points across the world. From a cybersecurity perspective, the technology was already in place; remote employees have existed for years, as have the cybersecurity measures to keep them protected. The challenge was delivering this protection at unprecedented scale and speed while still maintaining cybersecurity best practices.
One year into the pandemic, there are many lessons we have learned. Here are the top three that made the greatest impact on the new normal of cybersecurity:
1. *In a Crisis, Cyber Resilience Is an Essential Business Enabler*

The pandemic ignited an explosion of digital transformation. Instant pivots to remote operations meant pushing forward with technology investments in cloud, connectivity, automation, and innovation that may have taken months or years to implement in normal times. As the world began relying on these new digital capabilities, new risks and challenges were introduced. Organizations that were well-equipped to extend visibility and control to this new way of working found themselves in a far better situation than those that were scrambling to completely reengineer their security capabilities. The ones that had built an empowered and proactive security team, backed by robust processes and supported by effective technology, were able to adapt and overcome. Organizations that were locked into a rigid operational model, overly reliant on vendor platforms or lacking a defined set of processes to support their new reality, struggled to keep pace. *(segue)*
https://www.darkreading.com/operations/top-3-cybersecurity-lessons-learned-from-the-pandemic/a/d-id/1340375
Darkreading *Joe McMann 21/03/2021*

Industrial security, 5 consigli per una strategia di cyber security resiliente - Quello dell'industrial security è uno dei temi più caldi che le aziende devono affrontare in questo momento. Ecco quali sono le criticità e le strategie che possono adottare per garantire l'integrità delle linee di produzione, proteggendole dai cyber attacchi.
Il settore industriale è sempre più digitalizzato e votato all'automazione. Se questa sua evoluzione garantisce un passo avanti nel business, pone anche un problema: approntare strategie di industrial security che consentano di mettere al riparo le linee di produzione da eventuali attacchi informatici. Un compito che richiede di considerare, in primo luogo, le specificità del settore e delle tecnologie che vengono utilizzate al suo interno.
Indice degli argomenti

1. Separare la rete IT da quella OT
2. Adottare misure specifiche per l'industrial security
3. Garantire la trasparenza e la visibilità dei dispositivi
4. Attenzione ai sistemi legacy
5. Utilizzare sistemi di scansione attivi *(segue)*

https://www.internet4things.it/industry-4-0/come-liiot-sta-cambiando-la-fabbrica/
INTERNET4THINGS *- Marco Schiaffino, 19 Marzo 2021*

Le principali tendenze della sicurezza e della gestione dei rischi per il 2021 - Secondo Gartner i leader della sicurezza e della gestione del rischio devono affrontare otto tendenze principali per consentire una rapida reinvenzione nella loro organizzazione, dal momento che il COVID-19 ha accelerato la trasformazione del business digitale e sfidato le pratiche tradizionali di sicurezza informatica.
"La prima sfida è un divario di competenze. L'80% delle organizzazioni afferma di avere difficoltà a trovare e assumere professionisti della sicurezza e il 71% afferma che ciò influisce sulla loro capacità di fornire progetti di sicurezza all'interno delle loro organizzazioni" ha affermato Peter Firstbrook, vicepresidente della ricerca di Gartner.
Altre sfide chiave per la sicurezza e il rischio nel 2021 comportano la complessa situazione geopolitica e le crescenti normative globali, la migrazione di spazi di lavoro e carichi di lavoro dalle reti tradizionali**,** un'esplosione nella diversità e nelle posizioni degli endpoint e un ambiente di attacco mutevole tra le sfide del ransomware e la compromissione dell'email aziendale. Queste tendenze rappresentano le dinamiche aziendali, di mercato e tecnologiche che si prevede avranno un ampio impatto sul settore e un significativo potenziale nel 2021.
https://www.cwi.it/sicurezza/sicurezza-dei-dati/le-principali-tendenze-delle-sicurezza-e-della-gestione-dei-rischi-per-il-2021-135097
Computer World *– Francesco Destri – 26 marzo 2021*

I HAD A DREAM - Riflessioni a ruota libera sul blocco del Canale di Suez - Una nave portacontainer, lunga 400 metri e larga circa 60, blocca il Canale di Suez. Un nuovo evento imponderabile mette in crisi le catene logistiche mondiali. Dopo Wuhan, cosa abbiamo davvero imparato sulla resilienza delle supply chain?
(segue)
https://www.industry4business.it/risk-management/i-had-a-dream-riflessioni-a-ruota-libera-sul-blocco-del-canale-di-suez/
Industry4Business *- Marco Perona - Università degli Studi di Brescia, 29 Mar 2021*

La gestione della sicurezza antincendio: ruoli, compiti, responsabilità e procedure - Il presente lavoro intende approfondire la misura della gestione della sicurezza antincendio (GSA) nell'attività, con particolare attenzione ai contenuti del codice di prevenzione incendi.
Cosa s'intende per prevenzione incendi
Come sottolineato all'art.13 del D.Lgs. 139/2006 e s.m.i., la prevenzione incendi è:
"una funzione di preminente interesse pubblico diretta a conseguire, secondo criteri applicativi uniformi sul territorio nazionale, gli obiettivi di sicurezza della vita umana, di incolumità delle persone e di tutela dei beni e dell'ambiente attraverso la promozione, lo studio, la predisposizione e la

sperimentazione di norme, misure, provvedimenti, accorgimenti e modi di azione intesi ad evitare l'insorgenza di un incendio e degli eventi ad esso comunque connessi o a limitarne le conseguenze".
Appare evidente, quindi, che la prevenzione incendi si pone come fine il contenimento del rischio di incendio, inteso come probabilità che si verifichi l'evento incendio e che si generino conseguenze ad esso connesse. *(segue)*
https://www.ingenio-web.it/30244-la-gestione-della-sicurezza-antincendio-ruoli-compiti-responsabilita-e-procedure
INGENIO *– Panza Daniele - Direzione Regionale Vigili del Fuoco Lombardia 31/03/2021*

Kansas Man Indicted for Hacking, Tampering With Water Utility System. Attacker disabled water-purification operation systems "with intention of harming" the rural water district**.** A 22-year-old man has been indicted for breaking into a Kansas water utility's computer systems and disabling the cleaning and disinfecting operations for the locality's drinking water supply. Wyatt A. Travnichek allegedly hacked into the Ellsworth County Rural Water District No. 1's computer system on March 27, 2019, according to the US Department of Justice. Travnichek was charged with one count of tampering with a public water system and one count of reckless damage in his unauthorized access to a protected computer. According to the DoJ, his attack was waged "with the intention of harming the Ellsworth Rural Water District No. 1, also known as Post Rock Rural Water District.""By illegally tampering with a public drinking water system, the defendant threatened the safety and health of an entire community," said Lance Ehrig, Special Agent in Charge of EPA's Criminal Investigation Division in Kansas. "EPA and its law enforcement partners are committed to upholding the laws designed to protect our drinking water systems from harm or threat of harm. Today's indictment sends a clear message that individuals who intentionally violate these laws will be vigorously prosecuted."
The two charges combined carry a maximum sentence of 25 years in federal prison and up to $500,000 in fines.
https://www.darkreading.com/attacks-breaches/kansas-man-indicted-for-hacking-tampering-with-water-utility-system/d/d-id/1340572
Darkreading *- Staff - 01/04/2021*

Recovery (China) plan, il Copasir alzi la guardia. Firmato Mayer *Fra le maglie del Recovery plan si nascondono progetti che, invece che aumentare la resilienza istituzionale del Paese, aprono le porte anche in settori chiave ad aziende cinesi legate a Pechino. Il Copasir dovrebbe sorvegliare, ma è vittima di un inaccettabile stallo. Il commento di Marco Mayer*
Nel corso del mese di marzo quasi tutti i ministri del governo Draghi sono stati convocati in audizione dalle commissioni parlamentari competenti per discutere il Piano Nazionale di Ricostruzione e Resilienza (Pnrr), il programma da 196 miliardi destinati all'Italia dalla Ue. Il piano strategico non é ancora definito nei dettagli, ma dai lavori delle Commissioni Parlamentari risulta evidente che il Pnrr avrà implicazioni di rilevanza primaria in materia di sicurezza nazionale, alleanze internazionali e rilancio della vocazione euro-atlantica dell'Italia. Pochi ricordano che una delle priorità fondamentali del programma Next Generation EU (deliberato dal Consiglio Europeo nel luglio 2020) è irrobustire la resilienza istituzionale degli Stati membri. Nelle prossime settimane (esattamente come per il piano dei vaccini) un compito importante e delicato dovrebbe spettare al Copasir che – avvalendosi della preziosa collaborazione dell' Autorità Delegata – potrebbe compiere un esame a 360 gradi dei progetti che il nostro Paese dovrà presentare all'Unione Europea entro il prossimo 30 Aprile. Verificare la coerenza

dei progetti Pnrr rispetto all'obiettivo di irrobustire la resilienza istituzionale dell'Italia è ciò che rende utile e opportuno un esame "trasversale" del Copasir. Per chiarire meglio questo aspetto è sufficiente richiamare all'attenzione dei decisori un solo esempio paradigmatico. A parole tutti concordano sul fatto che per rendere l'Italia più resiliente sia indispensabile ridurre la sua forte dipendenza dalle importazioni tecnologiche dalla Cina, dipendenza testimoniata in modo emblematico dalla rapida e consistente penetrazione delle imprese del Dragone nelle nuove reti 5G e nelle forniture per la *broad band*. Per ragioni di spazio non cito i dati inquietanti (sottolineati proprio dal Copasir) in merito alla crescita dell'influenza economico-finanziaria della Cina nel nostro Paese nell'ultimo quinquennio (2015/ 2020). Mi riferisco in particolare a quanto il Copasir ha segnalato in materia di investimenti diretti (talora abilmente mascherati con etichette europee), *joint ventures*, importazioni di prodotti, componenti, piattaforme e servizi, forniture Pa via Consip o altre migliaia di stazioni appaltanti, accordi con università italiane per la diffusione di tecnologie cinesi di varia natura. *(segue)*
https://formiche.net/2021/04/recovery-china-plan-il-copasir-alzi-la-guardia-firmato-mayer/
***FORMICHE** - Marco Mayer - 04/04/2021 -*

Facebook says leak of 533m accounts is old news. But my date of birth, name, etc haven't changed in years, Zuck. Account info swiped in 2019 via security hole, sold online, now given away for free. Reams of personal data – including phone numbers, email addresses, and birthdays – obtained from 533 million Facebook accounts was offered to all for free on a cyber-crime forum over the weekend. The data dump was flagged up by Alon Gal, co-founder and CTO of infosec startup Hudson Rock. The information – which also includes people's names, marital status, occupation, and location – was siphoned from Facebook in 2019 via a vulnerability in the platform. The data waspackaged up and sold online to miscreants in June 2020. Now that same database is up for grabs to anyone who messages a particular Telegram account and asks nicely. The records were pilfered from hundreds of millions of Facebook profiles spread across 104 countries; that includes 32,315,282 accounts in the US, and 11,522,328 in the UK, according to a post on the underground forum viewed by *The Register*. All of the data amounts to over 70GB. It's reported the price tag on the database has been falling, and now it's free of charge.
All 533,000,000 Facebook records were just leaked for free. This means that if you have a Facebook account, it is extremely likely the phone number used for the account was leaked. I have yet to see Facebook acknowledging this absolute negligence of your data. https://t.co/ysGCPZm5U3 pic.twitter.com/nM0Fu4GDY8
— Alon Gal (Under the Breach) (@UnderTheBreach) April 3, 2021
Facebook is keen to shrug this off. We're told the data theft was in the news in 2019, and the exploited security hole was closed that same year.
That doesn't quite change the fact that people's stolen info has been circulating online for nearly three years, and that even though it all happened in 2019, names, dates of birth, contact details, and other data are unlikely to have changed in that time. *(segue)*.
https://www.theregister.com/2021/04/05/facebook_data_dump/
***THE REGISTER** - Katyanna Quach - 5 Apr 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

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 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

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

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