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

Newsletter

ANNO 2022	N. 7/ 2022	Luglio 2022

Il Ransomware

Il ransomware è un tipo di software dannoso, che inibisce l'apparato informatico della vittima e lo mantiene bloccato sino a quando non viene pagato all'attaccante un riscatto.
La realizzazione di un attacco ransomware normalmente procede attraverso tre passaggi, come codificato da IBM (https://www.ibm.com/au-en/topics/ransomware) :
Passaggio 1: Ricognizione. Gli aggressori eseguono la scansione del sistema infetto per comprendere meglio l'apparato e la rete, nonché scoprire i file sui quali concentrare l'attenzione. Sono ricercate anche credenziali aggiuntive che potrebbero consentire agli attaccanti di diffondersi nella rete, propagando il ransomware a più dispositivi.
Passaggio 2: Attivazione. Il ransomware inizia a identificare e crittografare i file. La maggior parte dei ransomware di crittografia implementa la crittografia asimmetrica, utilizzando una chiave pubblica per crittografare il ransomware e conservando una chiave privata in grado di decrittografare i dati. Poiché le vittime non hanno la chiave privata, non possono decrittografare autonomamente i dati. Alcuni ransomware disabilitano anche le capacità di ripristino del sistema per aumentare la pressione per pagare la chiave di decrittazione.

Passo 3: La richiesta di riscatto. Una volta che l'apparato è stato disabilitato, il ransomware avvisa la vittima dell'infezione e richiede il riscatto con le relative istruzioni per pagarlo ed avere una chiave per ripristinare le operazioni standard.

Pagare il riscatto è accettato dalla maggioranza degli utenti. In uno studio dell'IBM del 2021, è evidenziato che il 61% delle aziende, che sono state interpellate e che hanno confermato di aver subito un attacco ransomware, ha dichiarato di aver pagato il riscatto.
Però, le forze dell'ordine federali statunitensi scoraggiano le vittime di ransomware dal pagare richieste di riscatto:
"The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered."

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.
Secondo l'AGI (Agenzia Giornalistica Italia), non c'è mai la certezza che dopo il primo pagamento i criminali cederanno la chiave crittografica per sbloccare dati o sistemi in ostaggio. Per giunta i dati liberati dopo un attacco possono risultare corrotti.

Il modus operandi dei banditi è che una volta attaccata la vittima e aver ottenuto un riscatto, continuerà a farlo, per molte volte. Le varie gang potrebbero poi passarsi le informazioni sulle vittime affinché possano essere attaccate di nuovo da altri gruppi, ancora e ancora. Queste anche secondo Yoroi, società che si occupa di sicurezza informatica, alcune delle ragioni per cui le vittime di ransomware non dovrebbero mai pagare il riscatto.
Inoltre, la stessa società ha rilevato che Kisa, agenzia per la cybersecurity della Corea del Sud, ha rilasciato il decryptor per Hive Ransomware, un gruppo che ha attaccato anche aziende italiane come Ferrovie dello Stato, portando al blocco delle biglietterie.
Avere a disposizione il decryptor potrebbe salvaguardare numerose organizzazioni che a causa di attacco ransomware hanno visto rallentare la produzione o, in alcuni casi, arrivare al suo blocco totale.
Secondo vari studi circa l'80% delle organizzazioni e società che hanno pagato il riscatto dopo l'attacco, secondo Yoroi, sono state colpite dal ransomware una seconda volta. "Il nostro consiglio – ha spiegato Marco Ramilli, ad di Yoroi - è di essere preparati a un attacco ransomware e a non pagare in nessun caso il riscatto. Se è stato fatto un adeguato backup, l'azienda o l'ente colpito, possono riavviare le normali attività, mentre l'autorità giudiziaria provvederà a fare il suo lavoro"

Alberto Traballesi
In servizio presso l'Aeronautica Militare Italiana dal 1958 al 1995, ha lasciato il servizio attivo con il grado di Generale di Brigata Aerea. Sino al 2013 ha servito come esperto presso la Presidenza del Consiglio dei Ministri. Laureato in Matematica, Ingegneria elettronica e Scienze Aeronautiche. Attualmente è parte attiva in ricerche sulla protezione delle IC e sulle tematiche spaziali.
E' vice-presidente AIIC.

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nella seconda parte dell'anno 2022.

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

Per quanto riguarda i nostri "Colloquia", abbiamo in cantiere per metà novembre un evento molto interessante sulla protezione delle infrastrutture critiche tramite "droni" mentre stiamo organizzando, con una startup del settore, un evento di illustrazione di soluzioni innovative di predizione e anticipazione degli eventi negativi per tendere al rischio minimo nelle realtà RIR (Rischio Incidente Rilevante) e in generale dove il Real Time Risk Management e la Resilience Engineering rappresentano aspetti qualificanti e determinanti nella gestione.
Stiamo valutando le modalità di svolgimento di questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

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

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

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

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical

Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).

- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

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

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

NEWS E AVVENIMENTI

La resilienza cyber è anche un problema di interventi nel settore delle imprese: quali obiettivi - Per aumentare la resilienza del Paese è necessario prevedere interventi in materia di cyber security al fine di migliorare la capacità complessiva di far fronte ad attacchi massivi volti a bloccare la produzione. Un obiettivo concreto da inquadrare in uno schema di Governance che richiede idonee politiche di investimento da indirizzare anche verso le imprese e il lavoro privato.
Come noto, la tutela e la messa in sicurezza dei sistemi di rete e di informazione nazionali e dell'Unione dipendono dalla realizzazione di quelle azioni indirizzate sia dalle politiche europee in materia di sicurezza contro le minacce cyber, inquadrate perciò nel piano delle strategie per la resilienza collettiva dell'Europa, sia dagli specifici orientamenti nazionali.
Se la nascita dell'Agenzia per la Cybersicurezza Nazionale ha segnato un traguardo per la sicurezza cyber nazionale, dall'altro canto il Paese è di fronte a un appuntamento improrogabile: quello di portare avanti le proprie scelte e impostazioni per condurre istituzioni, enti e imprese verso un punto di svolta.
L'Agenzia funge da "faro" e da "catalizzatore" per il piano di difesa del Paese, ma complessivamente l'intero sistema e singolarmente ciascun soggetto pubblico e privato, dovranno affrontare un impegno elevato, specie se consideriamo il deficit strutturale, infrastrutturale e soprattutto culturale da colmare nel contesto della cyber security.

Indice degli argomenti

Un "cambio di passo" nella strategia nazionale di cybersicurezza
Servono politiche di investimento per la resilienza dei sistemi
I nuovi strumenti agevolativi
Il voucher per consulenza in innovazione
Piano di defiscalizzazione per gli investimenti in cyber security
Il portale online per gli incentivi a professionisti, imprese e PA
(continua)

https://www.cybersecurity360.it/cybersecurity-nazionale/la-resilienza-cyber-e-anche-un-problema-di-interventi-nel-settore-delle-imprese-quali-obiettivi/

Cybersecurity360 - *Giancarlo Samele, Giuseppe Tulli - 15 Giu 2022*

Internet delle cose sotto i mari: ecco perché è il futuro e l'Italia lo domina Il mare è un bene prezioso ma anche una risorsa. Quando saremo 10 miliardi sulla Terra, è da lì che trarremo gran parte di ciò che ci servirà per vivere. I grandi player mondiali lo hanno capito e, per una volta, la tecnologia italiana è in pole position: le reti wireless dell'italiana WSense sono il principale enabler**.** Si scrive **IoUT** (Internet of Underwater Things) si legge **evoluzione della specie**. Già, perché portare in mare la tecnologia dell'Internet delle cose significa scrivere un capitolo completamente nuovo della storia umana, consentendole di accedere in maniera più sicura e meno impattante ad un ambiente per definizione 'ostile'. Ottima notizia, dunque, alla luce delle opportunità di cui parleremo, che in uno scenario in cui il mare sarà al centro della nostra vita il principale enabler tecnologico sia italiano: si chiama WSense, ha il suo quartier generale a Roma e una branch in Norvegia, impiega oltre quaranta persone ed è in rapida crescita.

Indice degli argomenti

Cosa vuol dire "connettere" i mari e gli oceani
La rete wireless sottomarina realizzata a Roma
Conoscere gli abissi marini e le reti wireless e i dispositivi di IoT
La tecnologia italiana in aiuto all'acquacoltura norvegese
(continua)

https://www.agendadigitale.eu/infrastrutture/internet-delle-cose-sotto-i-mari-ecco-perche-e-il-futuro-con-tecnologia-italiana-in-pole-position/

Agendadigitale - *Marco Merola Chiara Petrioli -16 Giu 2022*

Come il citizen engagement cambia le piattaforme per l'erogazione dei servizi pubblici - Qual è il punto di incontro tra le soluzioni tecnologiche per l'erogazione di servizi pubblici e la cultura human-centered che caratterizza la nostra epoca? Il ruolo centrale delle MarTech alla luce del think tank europeo.

L'erogazione di servizi pubblici digitali al cittadino rappresenta il punto di arrivo della digitalizzazione delle amministrazioni pubbliche. In particolare, il macro-obiettivo della PA è la digitalizzazione dell'80% dei servizi essenziali entro il 2026, come richiesto dal Ministero per l'innovazione tecnologica e la transizione digitale retto da Vittorio Colao. Altrettanto importante, però, è che i servizi online siano ben accolti e apprezzati da chi li deve utilizzare. Imporne semplicemente l'obbligo d'uso, infatti, non sarebbe indice di successo.

Per massimizzare l'appeal dei servizi digitali occorre di conseguenza investire in adeguate tecnologie, ma anche e soprattutto in strategie di citizen-centric design. Conoscere i bisogni, le aspettative e gli insight dei cittadini, infatti, è vera chiave di volta della trasformazione digitale della PA. Marketing e tecnologia, quindi, devono incontrarsi fin dalle prime fasi di sviluppo delle piattaforme di erogazione e gestione dei servizi.
Oggi, il PNRR Missione 1 (investimento 1.4) mette a disposizione oltre 2 miliardi di euro per sviluppare il concetto di "cittadinanza digitale"; migliorare la user experience dei servizi digitali pubblici e, infine, aumentare l'accessibilità e la platea degli utilizzatori.
Alla luce di questi target, i Responsabili della Transizione al Digitale (RTD) della PA sono chiamati a predisporre progetti di digitalizzazione degli Enti che tengano conto del necessario approccio human-centered.
A questo scopo, nel corso degli ultimi anni, si sono fatte strada le MarTech (Marketing Technology). Si tratta di software e soluzioni hi-tech che permettono di offrire ai cittadini una vera citizen experience omnicanale, in grado di fare la differenza nello sviluppo dei servizi pubblici.

Indice degli argomenti

https://www.zerounoweb.it/cio-innovation/pa-digitale/come-il-citizen-engagement-cambia-le-piattaforme-per-lerogazione-dei-servizi-pubblici/

Zerounoweb - *Paola Orecchia - 16 Giu 2022*

Dal mare al sottosuolo fino allo spazio: le nuove frontiere dell'IoT - Non solo tecnologie e casi d'uso oggi ampiamente noti, come quelli della domotica e della telemedicina. L'Internet of Things oggi sta ampliando le sue possibili applicazioni abbracciando sempre più settori e allargando i confini in cui implementare sensoristica, piattaforme e servizi di connettività. Ecco una breve panoramica dei 3 nuovi ambiti di espansione dell'IoT.
Nel 2021 l'Internet of Things (IoT) ha raggiunto un valore pari a 190,26 miliardi di dollari. La pandemia in sostanza ha avuto un duplice effetto: da un lato ha fatto registrare, soprattutto nel 2020, una battuta d'arresto sugli investimenti nei grandi progetti IoT; dall'altro ha accelerato i processi di digitalizzazione rendendo sempre più pervasiva l'adozione di hardware, piattaforme, software e servizi di connettività. Solo con riferimento all'Italia, l'anno scorso il mercato ha superato i 7 miliardi di euro, con un incremento del 22% rispetto al 2020 e con 110 milioni di oggetti connessi, che corrispondono a 1,8 per abitante. Segno che la maturità delle tecnologie IoT oggi vede una diffusione costante in svariati casi d'uso come la smart factory, la telemedicina, la smart city, lo smart building e la smart grid, solo per citare gli stessi settori dell'Internet of Things che anche il PNRR prevede di supportare da qui al 2026.
Accanto a questi ambiti ormai ampiamente noti, esistono alcune sperimentazioni che stanno cercando di portare l'IoT oltre i confini sinora conosciuti e che si possono suddividere in 3 macro categorie:
Internet of Underwater Things (IoUT)
Internet of Underground Things (IoUGT)
Internet of Space Things (IoST)

Indice degli argomenti

L'Internet of Space Things (IoST)
(continua)
https://www.internet4things.it/iot-library/dal-mare-al-sottosuolo-fino-allo-spazio-le-nuove-frontiere-delliot/
Internet4things *- Carmelo Greco - 23 Giugno 2022*

Gli orientamenti Ue su mobilità multimodale e sistemi di trasporto intelligenti - Dal progetto Orchestra, che ha l'obiettivo di creare un ecosistema di gestione del traffico che abbraccia diversi mezzi di trasporto, ai finanziamenti che incentivano la smart mobility, passando per la proposta di modifica alla normativa sul quadro generale degli Intelligent Transport Systems nel vecchio continente. Uno sguardo alla mobilità del futuro secondo l'Unione europea
Si chiama Orchestra e ha l'ambizione di progettare un ecosistema di gestione del traffico multimodale che abbraccia diversi mezzi di trasporto: stradali, ferroviari, aerei e navali. Finanziato dall'Unione europea nell'ambito del programma Horizon 2020 con un ammontare pari a 5 milioni di euro, che coprono gran parte dell'importo complessivo di 5,2 milioni, vede tra i 16 partner appartenenti a 8 Stati membri Ue la presenza rilevante dell'Italia con 5 realtà che, nel loro insieme, compongono il Living Lab nell'aeroporto di Milano Malpensa: FSTechnology (Gruppo Ferrovie dello Stato), ENAV, Techno Sky, SEA Aeroporti Milano e Deep Blue. Il coordinamento è affidato a ITS Norway, l'associazione nazionale norvegese che promuove l'uso delle nuove tecnologie per il settore dei trasporti. Norvegia e Italia sono i due paesi nei quali saranno effettuati due test di validazione da qui alla primavera del 2024, data presunta di conclusione del progetto. I pilastri su cui verte Orchestra coincidono con le tre caratteristiche che dovrà avere la mobilità del futuro secondo il documento Sustainable and Smart Mobility Strategy pubblicato dalla Commissione europea nel dicembre 2020. Lo mobilità dovrà essere sostenibile, smart e resiliente. Caratteristiche suddivise, a loro volta, in 10 flagship che vanno dall'incremento nell'adozione di vettori di trasporto a emissioni zero all'accelerazione di una mobilità intelligente con l'ausilio di AI e big data.
Indice degli argomenti
Le risorse Ue per la mobilità smart del futuro
La proposta di modifica della Direttiva 2010/40 sugli ITS
(continua)
https://www.internet4things.it/smart-city/gli-orientamenti-ue-su-mobilita-multimodale-e-sistemi-di-trasporto-intelligenti/
Internet4things *- Carmelo Greco - 23 Giugno 2022*

Sardegna, dal maxi-furto di dati l'occasione per ripensare la cybersecurity *Spero che i vertici dell'Agenzia per la cybersicurezza nazionale portino trasparenza nelle zone digitali opache, inaugurando una fertile collaborazione con università e istituti di ricerca aiutando anche il Copasir. Il commento di Marco Mayer* Per la nuova Agenzia per la cybersicurezza nazionale guidata da **Roberto Baldoni** e da **Nunzia Ciardi** il *leak* di quasi 170.000 file della Regione Sardegna costituisce un *case study* di particolare rilevanza in materia di politica digitale delle regioni italiane. È un caso ancora più interessante del celebre precedente della Regione Lazio. La Regione a statuto speciale della Sardegna ha, infatti, alcune connessioni internazionali che meritano di essere studiate nella loro peculiarità. La Regione e altri enti sardi di ricerca hanno, infatti, coltivato sin dal 2015 un rapporto speciale con il colosso cinese Huawei, noto in tutto il mondo per le accuse (in corso di accertamento) di spionaggio industriale e di rapporti obliqui con l'Iran. La prima pagina di oggi della *Nuova Sardegna* scrive che la Regione tende a minimizzare quanto sarebbe accaduto con i recenti attacchi informatici. Vedremo se la

difesa di SardegnaIT, la società *in house* della Regione, è fondata su basi solide. Il *breach* è presumibilmente iniziato nel gennaio di questo anno e per la prima volta segnalato nel febbraio scorso dal giornalista **Raffaele Angius**. È presto per stimare l'entità dei danni del gigantesco *leak*. Tuttavia, colpiscono le dichiarazioni dell'assessore regionale **Valeria Satta**: "Ecco perché si stava operando prima ancora di questo attacco alle Academy di formazione, tra cui quella sulla Cyber dedicata ai referenti informatici della Regione e degli enti locali, la prima rivolta alla P.A in collaborazione stretta con la Polizia Postale e l'università di Cagliari, Facoltà di Ingegneria Indirizzo Cybersicurezza e intelligenza artificiale" (continua…).
https://formiche.net/2022/06/sardegna-furto-dati-cybersecurity/
FORMICHE - Marco Mayer *- 26/06/2022*

Attacchi cyber, ecco le prime lezioni da trarre dalla guerra in Ucraina. Aziende che combattono oltre a fornire strumenti per combattere, IT Army al limite della legalità, minacce ibride e attacchi advanced persistent manipulator. Sono diverse le novità e le lezioni che si possono trarre sul conflitto in corso da una lettura "trasversale" del recente report Microsoft**.** Nei giorni scorsi **Microsoft** ha pubblicato un rapporto[1] con quelle che a suo giudizio sono **le prime lezioni che possiamo trarre dall'invasione russa dell'Ucraina dal lato cyber**. Un rapporto indubbiamente interessante ma che mescola considerazioni strategiche con altre più tipicamente commerciali sull'efficacia dei vari prodotti Microsoft utilizzati dai difensori ucraini.
Proviamo allora a darne una lettura trasversale e personale nel tentativo di distinguere tra le lezioni imparate e le altre considerazioni. A mio giudizio, la considerazione più interessante e che ne genera molte altre è un po' nascosta nella parte finale e può essere così tradotta: "Se la guerra in terra, cielo e mare è un dominio degli stati, il dominio cyber è proprietà anche delle aziende. Ciò rende la guerra in Ucraina diversa dalla maggior parte delle guerre del passato".
Indice degli argomenti

(continua…)
https://www.agendadigitale.eu/sicurezza/guerra-in-ucraina-le-prime-lezioni-da-trarre-sul-fronte-cyber/
Agendadigitale- *Fabrizio Baiardi- 27 Giu 2022*

Agenzia cyber. Cosa farà il Cvcn per mettere il 5G al sicuro *Il Centro di valutazione e certificazione nazionale è operativo da oggi. Si tratta di un altro pilastro del Perimetro di sicurezza nazionale cibernetica. Tutti i dettagli*
Il Centro di valutazione e certificazione nazionale è operativo da oggi presso l'Agenzia per la cybersicurezza nazionale diretta dal professor **Roberto Baldoni**. Si tratta di un altro pilastro del Perimetro di sicurezza nazionale cibernetica. È incardinato nel Servizio certificazione e vigilanza diretto dall'ingegner **Andrea Billet**.
IL RUOLO DEL CVCN

Il Cvcn, originariamente istituito presso il ministero dello Sviluppo economico e trasferito all'interno dell'Agenzia, avrà il compito di valutare la sicurezza di beni, sistemi e servizi Ict destinati a essere impiegati nel contesto del Perimetro e che rientrano nelle categorie previste dal Dpcm 15 giugno 2021, il cosiddetto Dpcm 3. La procedura di valutazione potrà prevedere l'esecuzione di test hardware e software sui componenti della fornitura. In questo processo, al Cvcn faranno riferimento i Centri di valutazione presso i ministeri della Difesa e dell'Interno e potrà avvalersi del supporto di una rete di Laboratori accreditati di prova che saranno regolamentati da apposito decreto in fase di pubblicazione in *Gazzetta Ufficiale*.

FARO SUL 5G

Inoltre, il Cvcn svolgerà un ruolo di supporto tecnico per le attività connesse all'esercizio dei poteri speciali (Golden power) in ambito 5G, così come previsto dalle recenti modifiche apportate al decreto-legge 21/2012 dal "decreto Ucraina". In particolare, opererà sia nella fase istruttoria, a supporto del Gruppo di coordinamento, sia nella fase di monitoraggio, come organo di cui si avvale il Comitato preposto allo scopo. È tramite il rafforzamento di questi strumenti che l'Italia ha deciso di affrontare la minaccia cinese (Huawei e Zte). (continua…)

https://formiche.net/2022/07/agenzia-cyber-cvcn-5g/

Formiche- *Gabriele Carrer - 01/07/2022*

Cloud Misconfig Exposes 3TB of Sensitive Airport Data in Amazon S3 Bucket: 'Lives at Stake' The unsecured server exposed more than 1.5 million files, including airport worker ID photos and other PII, highlighting the ongoing cloud-security challenges worldwide. A misconfigured Amazon S3 bucket resulted in 3TB of airport data (more than 1.5 million files) being publicly accessible, open, and without an authentication requirement for access, highlighting the dangers of unsecured cloud infrastructure within the travel sector.

The exposed information, uncovered by Skyhigh Security, includes employee personal identification information (PII) and other sensitive company data affecting at least four airports in Colombia and Peru. The PII ranged from photos of airline employees and national ID cards — which could present a serious threat if leveraged by terrorist groups or criminal organizations — to information about planes, fuel lines, and GPS map coordinates.

The bucket (now secured) contained information dating back to 2018, the report says, noting Android mobile apps also were contained within buckets, which security personnel tap to help with incident reporting and data handling.

"Airport security protects the lives of travelers and airport staff," the report explains. "As such, this breach is extremely dangerous with potentially devastating consequences should the bucket's content end up in the wrong hands."

As travel picks up dramatically following restrictions during the pandemic, Fortune Business Insights found that the global smart airport market size is set to be driven by the rising preference of the masses for air travel. The report also says that the expansion of commercial aviation is set to affect the market positively in the coming years, as airports increasingly turn to cloud service providers to house and process massive amounts of passenger and operational data. (continua….)

https://www.darkreading.com/application-security/cloud-misconfig-exposes-3tb-sensitive-airport-data-amazon-s3-bucket

Darkreading -*Nathan Eddy -July 06, 2022*

NIST Picks 4 Quantum-Resistant Cryptographic Algorithms The US Department of Commerce's National Institute of Standards and Technology has announced the first group of encryption tools that will become part of its post-quantum cryptographic standard. At long last, the National Institute of Standards and Technology (NIST) has announced the first four quantum-resistant algorithms that will become part of the post-quantum-cryptographic standard. The chosen algorithms are CRYSTALS-Kyber for general encryption to access secure websites and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.

The post-quantum cryptographic standard, expected to be finalized in about two years, will help enterprises prepare their environments for the time when quantum computers will be powerful — and readily available — enough that they will be able to break present-day encryption. Researchers estimate that post-quantum threats could be reality as soon as 2030.

Attackers are also harvesting and hoarding sensitive information with the expectation that they can crack it later when quantum computing methods become available.

"Since the standardization project began in 2016, there's been a shift in attitudes towards PQC, and it is now understood as a critical part of a secure future. Now, it is going to be exciting to see more and more applications and systems transition to this next generation of asymmetric cryptography," said Peter Schwabe, cryptographic engineering professor and PQShield advisory board member, in a statement.

The NIST announcement comes after a busy few months. US President Joe Biden has issued two related directives: to foster better quantum technology research within government and to guide agencies to a post-quantum cryptographic standard. Any digital system that uses public standards for public-key cryptography could be vulnerable to an attack by quantum computers in the future. A White House memo in January called for government agencies to identify any encryption not compliant with quantum-proof standards and provide a timeline towards transition.

The agency plans to include four additional algorithms before finalizing the cryptographic standard. The schemes BIKE, Classic McEliece, HQC, and SIKE are expected to be considered. (continua…)

https://www.darkreading.com/emerging-tech/nist-picks-four-quantum-resistant-cryptographic-algorithms

Dark Reading *- Dark Reading Staff -July 06, 2022*

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

Come ogni anno, la nostra Newsletter AIIC va in vacanza. Ci rivedremo a settembre. Buone ferie!

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*

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