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. 6/ 2022	Giugno 2022

La sicurezza cibernetica spaziale

L'esplorazione è stata fondamentale per l'esperienza umana e continuerà ad ispirare molte attività umane basilari. Con questo presupposto, lo spazio assumerà sempre più importanza per la sicurezza e la prosperità globale nei decenni e nei secoli a venire.
Lo spazio è stato inestimabile per produrre ricchezza, stimolare il commercio e vincere guerre, ma un aspetto qualitativamente diverso dello spazio sta emergendo e potrebbe essere primario nel prossimo futuro. Questo nuovo paradigma per lo spazio darà priorità alla sicurezza e alle attività economiche che si verificano all'interno dello spazio stesso, non solo a quelle che si sviluppano sulla Terra.
"Lo spazio è un settore emergente di infrastrutture critiche commerciali non più dominio delle sole autorità governative nazionali" (Michael Holden – DSEI 2021). Lo spazio è un ambiente intrinsecamente rischioso in cui operare, quindi i pericoli per la sicurezza informatica che coinvolgono lo spazio commerciale, compresi quelli che interessano i veicoli commerciali satellitari, devono essere considerati e gestiti insieme agli altri tipi di rischi per garantire operazioni sicure e di successo.
I massimi funzionari spaziali statunitensi hanno recentemente affermato che è probabile che l'invasione russa dell'Ucraina si estenderà allo spazio, prevedendo continue interferenze GPS e spoofing e sollecitando gli operatori spaziali militari e commerciali a prepararsi a possibili attacchi informatici. Il direttore del National Reconnaissance Office, Chris Scolese, ha esortato i partecipanti a una conferenza della National Security Space Association ad "assicurarsi che i vostri sistemi siano sicuri e che li stiate osservando da vicino perché sappiamo che i russi sono attori informatici efficaci".
Lo spazio è una frontiera critica della sicurezza informatica, dalla quale stiamo diventando sempre più dipendenti sia per il nostro commercio che per la sicurezza. Nella sicurezza nazionale deve essere inserita una infrastruttura critica prioritaria da proteggere.
Lo spazio sta rapidamente diventando la nuova frontiera da esplorare da parte dei governi nazionali e degli attori del settore privato. Nel processo, le diverse parti si stanno preparando per un ambiente che presenta la stessa competizione e collaborazione che sono tipiche sulla Terra e che richiederà nuovi regolamenti e norme internazionali e creerà nuove opportunità per l'industria e l'innovazione.
La nostra dipendenza dallo spazio è cresciuta esponenzialmente con la trasformazione digitale. Sfortunatamente anche i rischi, di conseguenza la necessità di dare priorità alla sicurezza informatica delle risorse spaziali è urgente. Poiché le capacità e la connettività dei dispositivi informatici sono cresciute in modo esponenziale, anche le intrusioni informatiche e le minacce da malware e hacker richiedono la ristrutturazione delle priorità.
La minaccia informatica include varie imprese criminali e stati nazionali avversari. Proteggere le risorse spaziali dalle minacce informatiche è un imperativo di sicurezza nazionale. Mentre investiamo e continuiamo a costruire la spina dorsale satellitare che guiderà la nostra sicurezza e il nostro benessere economico per i prossimi decenni, la sicurezza cibernetica spaziale già in fase di progettazione non può che essere un requisito indispensabile.

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

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

ASSEMBLEA DEI SOCI E RINNOVO DEL CONSIGLIO DIRETTIVO DI AIIC

Il giorno 8 giugno 2022 alle ore 16.00 in collegamento web, si è svolta l'assemblea ordinaria dei soci AIIC.

Nel corso dell'assemblea sono state illustrate le attività svolte da AIIC durante il mandato del Consiglio Direttivo uscente (dal 2018 al 2021) nonostante le difficoltà create dalla pandemia da Covid-19:
i punti di forza sono stati il rifacimento del sito web, le attività di formazione (Colloquia, webinar e visite aziendali), le attività dei vari gruppi di lavoro che hanno prodotto documenti di alto spessore, senza contare i patrocinii concessi a diverse manifestazioni di carattere nazionale e internazionale, la partecipazione ad eventi anche televisivi e il gruppo AIIC di Linkedin, creato e gestito da Enzo Tieghi, che ormai ha sfiorato il numero di mille partecipanti.

Si è poi passati all'illustrazione del bilancio consuntivo 2021 e del preventivo 2022 che prevede un sostanziale pareggio. L'assemblea ha approvato all' unanimità i due bilanci.

Nel corso dell'assemblea, il presidente del Comitato Elettorale, Paolo Bellofiore, insieme agli altri componenti Priscilla Inzerilli e Tommaso Ruocco, ha comunicato i risultati delle elezioni per il rinnovo del Comitato Direttivo dell'Associazione. Si ricorda che le votazioni si sono svolte nei giorni 6 e 7 giugno 2022, tramite piattaforma online Eligo.
La partecipazione dei soci alle votazioni è stata numerosa (più dell'80% dei soci aventi diritto), pertanto il Consiglio che ne esce eletto è pienamente legittimato.
Sono risultati eletti: Luisa Franchina, Glauco Bertocchi, Silvano Bari, Alberto Traballesi, Gianluca Cipriani, Raffaella D'Alessandro, Andrea Fumagalli, Sandro Bologna, Bruno Carbone, Giuseppe Rinciari.

Il nuovo Consiglio è, pertanto, pienamente operativo. Un particolare ringraziamento va ai componenti uscenti Paolo Bellofiore, Claudio Pantaleo, Priscilla Inzerilli, Angelo Socal per il prezioso contributo fornito nel corso di questi anni.

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

PRIMA RIUNIONE DEL NUOVO CONSIGLIO DIRETTIVO AIIC

Il giorno 15 giugno 2022 si è svolta la prima riunione del nuovo Consiglio Direttivo AIIC, nel corso della quale sono state definite le cariche sociali:

Presidente	Luisa Franchina
Vicepresidente	Alberto Traballesi
Vicepresidente	Silvano Bari
Tesoriere	Glauco Bertocchi
Segretario	Bruno Carbone
Consiglieri	Gianluca Cipriani, Raffaella D'Alessandro, Andrea Fumagalli, Sandro Bologna, Giuseppe Rinciari.

Le informazioni sui singoli consiglieri sono presenti nel sito web dell'associazione
www.infrastrutturecritiche.it
Chi volesse contattarli può farlo inviando una mail alla segreteria AIIC:
segreteria@infrastrutturecritiche.it

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

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

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

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

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

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.

- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

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

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

NEWS E AVVENIMENTI

La sfida OT per la cybersecurity con l'arrivo dell'Industria 5.0 - Mentre siamo ancora impegnati a sviluppare metodi per l'interconnessione, primo passo per la digitalizzazione del processo produttivo e principio base dell'Industria 4.0, una nuova fase è già alle porte. Si tratta dell'Industria 5.0 antropocentrica e collaborativa, che mette sul campo nuove sfide sul piano dei rischi cyber. Il tema è stato oggetto della tavola rotonda "Impatto della Cyber Security sui piani Transizione 4.0 e Industria 5.0" organizzata dal Clusit durante il Security Summit (15 – 17 marzo) con esperti, CIO e CISO di aziende italiane e moderata da Enzo Maria Tieghi del Comitato Scientifico di Clusit e referente per la security di ICS/OT/IIoT. Il confronto ha permesso di fare il punto su come i piani per la trasformazione digitale, tra cui quello più recente Transizione 4.0, abbiano inciso sulla sicurezza delle aziende e comprendere quali rischi di sicurezza dobbiamo aspettarci da un'industria sempre più umano-centrica, sostenibile e resiliente.

Indice degli argomenti

Il cambio di passo di Industria 5.0
Il punto su Transizione 4.0: cosa è stato fatto per la sicurezza
Il ruolo dell'innovazione per accelerare in sicurezza
Security OT la sfida è sulle competenze
L'evoluzione della cyber resilienza
(continua)
https://www.zerounoweb.it/techtarget/searchsecurity/la-sfida-ot-per-la-cybersecurity-con-larrivo-dellindustria-5-0/
Zerounoweb *- Roberta Fiorucci - 12 Apr 2022*

Cybersecurity, Urso: "Contro attacchi hacker poteri al premier" - Il presidente del Copasir: "A fronte di azioni che possono pregiudicare la sicurezza nazionale il Presidente del Consiglio deve avere l'autorità di disporre ogni misura proporzionata per il suo contrasto". Intanto Palazzo Chigi accelera sulla strategia nazionale: entro maggio il via libera.
Più poteri al Presidente del Consiglio contro attacchi hacker che possono pregiudicare la sicurezza nazionale. La proposta arriva dal presidente del Copasir, Adolfo Urso, intervistato dal Corriere della Sera.
"Un attacco hacker su vasta scala deve essere configurato come atto terroristico. Credo inoltre necessario attribuire direttamente al presidente del Consiglio il potere di disporre che, a fronte di una azione configurata come pregiudizio per la sicurezza nazionale, possa disporre ogni misura proporzionata per il suo contrasto – ha spiegato Urso – E va realizzato al più presto il cloud nazionale della Pubblica amministrazione, una politica nazionale sui cavi marittimi e terrestri per fare del nostro Paese un nodo centrale nella rete globale che sempre più connetterà Europa e Occidente con Asia e Africa".
Sui rischi di infiltrazioni nella politica, Urso sottolinea: "Gli attacchi statuali sono ovviamente per loro natura politici. Hacker e macchina di disinformazione russa sono elementi di una 'guerra ibrida' che i sistemi autoritari, Russia ma anche Cina, usano per penetrare le democrazie occidentali".
La proposta di Urso arriva a pochi giorni dell'attacco hacker al sito del Senato e ad altri siti istituzionali su cui stanno indagando i Pm antiterrorismo della Procura di Roma: l'accusa è accesso abusivo a sistema informatico.
Gli accertamenti, a carico di ignoti, sono stati aperti sulla base di una informativa trasmessa ai magistrati dagli investigatori della Polizia postale. Secondo quanto verificato l'azione pirata è stata rivendicata su Telegram dal collettivo filorusso "Killnet".
Secondo quanto ricostruito sinora l'attacco sarebbe stato di tipo DDos (Denial of Service) da parte di più computer 'zombie' controllati a distanza dai pirati informatici.
Indice degli argomenti

https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-urso-contro-attacchi-hacker-poteri-al-premier/
Corriere delle Comunicazioni *- F. Me 13 Mag 2022*

Black Hat Asia: Firmware Supply Chain Woes Plague Device Security The supply chain for firmware development is vast, convoluted, and growing out of control: patching security vulnerabilities can take up to two years. For cybercriminals, it's a veritable playground.
BLACK HAT ASIA 2022 — When it comes to developing the firmware that powers computing devices, the ecosystem consists of complex supply chains that have multiple contributors. For any given device, firmware could be made up of a hodgepodge of components from different sources. And that means that when it's time to address security vulnerabilities, it's far from a straightforward process to get a patch out to the public. During a panel-discussion session at Black Hat Asia on Thursday, entitled "The Firmware Supply-Chain Security Is Broken: Can We Fix It?", Kai Michaelis, co-founder and CTO at

Immune GmbH, outlined what he called the overgrown supply-chain "tree," out of which grows onerous code reviews, and lengthy patching processes when a bug is found. In fact, six to nine months for patches to roll out is the average, according to the panelists — with two years being not uncommon. And that means the supply chain represents a wide attack surface that's ripe for compromise, they warned. Given that vulnerable firmware threatens safety of the operating system and any applications, the potential for cyberattackers to find exploitable vulnerabilities is a serious concern.
A Thorny Tree of Supply-Chain Complexity. The final firmware that vendors incorporate into their hardware is a multisourced affair, explained Michaelis. Stakeholders can include various component vendors, a few open source repositories, reference implementations, original design manufacturers, independent BIOS vendors, and finally, the original equipment manufacturers (OEMs) that create and sell the final product to channel partners and end users. *(continua….)*
https://www.darkreading.com/risk/black-hat-asia-firmware-supply-chain-woes-plague-device-security
Darkreading-*Tara Seals- May 13, 2022*

Nuovo attacco russo a siti istituzionali italiani, disservizi diffusi: cosa sta succedendo - Il sito del Ministero degli Esteri e quello del CSM sembrano essere tra i più colpiti da uno sciame di attacchi contro le istituzioni italiane e aeroporti, annunciati dal gruppo criminale filo-russo KillNet. Ma secondo l'esperto di cyber security Corrado Giustozzi, è solo "rumore di fondo": il peggio potrebbe ancora arrivare.
Ministero degli Esteri, Consiglio Superiore della Magistratura, Senato e Ministero della Difesa sono alcuni dei siti web istituzionali italiani che, in queste ore, stanno soffrendo momenti di grande rallentamento, con anche brevi down che stanno provocando un'altalena di disservizi diffusi, a causa degli attacchi che stanno prendendo di mira il nostro Paese.
Aggiornamento 23.30: l'attacco ha preso di mira i servizi di trasporto pubblico e con essi gli aeroporti italiani. Risultano in queste ore inaccessibili o con gravi rallentamenti i siti web degli aeroporti di Milano Malpensa e Linate, Genova, Rimini, Milano Bergamo e Olbia (società Geasar).
Indice degli argomenti
Il gruppo Legion ha annunciato l'attacco
Alcuni siti web sono già non disponibili
Il nostro CSIRT lancia l'allarme
(continua)
https://www.cybersecurity360.it/nuove-minacce/nuovo-attacco-russo-a-siti-istituzionali-italiani-disservizi-diffusi-cosa-sta-succedendo/
Cybersecurity360 *- Dario Fadda, 20 Mag 2022*

Attacchi DDoS e strategia cyber nazionale: ecco come mettere in sicurezza le nostre infrastrutture - Dal CSIRT un bollettino sulle attività di preparazione ad attacchi DDoS verso le nostre infrastrutture. E nel frattempo, come anticipato nei mesi precedenti, è stata approvata la strategia per la cybersicurezza nazionale. Ecco tutti i dettagli.
È di qualche giorno fa, il 17 maggio per l'esattezza, l'alert pubblicato dal CSIRT, il Computer Security Incident Response Team, "Rilevate attività di preparazione ad attacchi DDoS verso infrastrutture nazionali (AL02/220517/CSIRT-ITA)".
A quanto pare, a partire dall'11 maggio scorso, si sono intensificati gli attacchi DDoS, Distributed Denial of Service, contro soggetti nazionali e internazionali e il CSIRT ha potenziato il monitoraggio di questo tipo di minaccia "identificando attività di "probing" delle misure di protezione attive all'interno della

constituency nazionale. Tali attività, che al momento risultano di bassa intensità e che avrebbero avuto inizio almeno dalla data del 12 maggio u.s., potrebbero preludere a successive azioni di attacco DDoS con impatto sulla disponibilità dei servizi vittima".
Le attività vedranno: "presenza di picchi di traffico UDP e TCP anomalo (in ogni caso superiore alla normale baseline di utilizzo delle risorse interessate); presenza di chiamate HTTP malformate (versione HTTP non valida, assenza del carattere CRLF); presenza di volumi anomali di chiamate provenienti da indirizzi IP appartenenti a servizi di anonimizzazione (rete Tor, proxy anonimi); presenza di chiamate riconducibili ad attacchi di tipo ICMP flood, SYN flood e TCP RST".
Indice degli argomenti
Attacchi DDoS e come difendersi
Le azioni consigliate contro gli attacchi DDoS
La strategia di cybersicurezza nazionale
(continua)
https://www.cybersecurity360.it/cybersecurity-nazionale/attacchi-ddos-e-strategia-cyber-nazionale-ecco-come-mettere-in-sicurezza-le-nostre-infrastrutture/
Cybersecurity360 *- Marco Santarelli - 23 Mag 2022*

La strategia cyber dell'Italia: ecco i punti chiave - Circola un testo non definitivo della strategia e che permette di coglierne l'essenza. Ecco dove punterà il Paese con l'Agenzia della cybersicurezza nazionale
La visione strategica dell'Italia dal punto di vista della sicurezza nazionale cibernetica ha una nuova forma, aggiornata al 2022 e alle nuove sfide che il mondo ci sta ponendo. Sfide che l'ACN, Agenzia per la Cyber security Nazionale, ha identificato nel documento programmatico appena presentato al Comitato Interministeriale Cyber per l'approvazione insieme con il piano attuativo.
La strategia per la cybersicurezza nazionale sarà presentata il 25, anche se nei giorni scorsi tra gli addetti ai lavori ha circolato un documento che l'agenzia ha poi bollato come "non definitivo".
Il testo va preso quindi con le pinze, ma permette di approfondire almeno i concetti cardine di questa svolta.
Indice degli argomenti
I punti chiave della strategia cyber nazionale
Tre binari strategici
Protezione
Risposta
Sviluppo
Nuovi finanziamenti
(continua)
https://www.agendadigitale.eu/sicurezza/la-strategia-cyber-dellitalia-ecco-i-punti-chiave/
Agenda Digitale *- Luisa Franchina, 23 Mag 2022*

Cos'è uno smart building: quando un edificio si può definire "intelligente" - Passiamo più del 90% del nostro tempo all'interno di spazi chiusi. Renderli "smart" diviene quindi un'esigenza imprescindibile. In questo articolo vedremo quando un edificio si può definire smart, quali sono i sei passi chiave per renderlo tale, l'importanza della fiducia degli utenti nella condivisione del dato e un breve elenco dei sistemi 4.0 maggiormente utilizzati in ambito smart.
(continua)
https://www.ingenio-web.it/34727-cose-uno-smart-building-quando-un-edificio-si-puo-definire-intelligente
INGENIO *- Bracci Elisabetta - 23/05/2022*

Smart Building, Domotica e Cyber Security: la vulnerabilità dell'IoT - I sistemi di domotica e smart building aprono le porte "virtuali" delle nostre case e delle nostre aziende a forti vulnerabilità di sicurezza logica, che possono causare danni anche ben più gravi di una incursione fisica. Vediamo insieme ad un esperto di cyber security come fare a difenderci.
L'Internet of Things e la loro sicurezza
L'Internet of Things (Internet delle cose) indica un network di oggetti identificati univocamente e connessi tra loro in grado di comunicare tramite lo scambio di dati. Parliamo quindi di tantissimi dispositivi che incrociamo quotidianamente, dai wearable (come smart-watch e fitness tracker) alle stampanti, agli impianti di videosorveglianza o di climatizzazione e più in generale a tutti i componenti smart e domotici. In quanto oggetti connessi ad una rete, possono essere raggiungibili da remoto e attaccabili, generando quindi una vulnerabilità.
Approfondiamo il tema della cyber security insieme all'Ing. Massimo Carnevali, che ha svolto il ruolo di ICT Manager e di Innovation Manager per oltre 35 anni, prima in azienda e poi come consulente, e che attualmente svolge docenze a contratto all'Università di Ferrara ("Sicurezza dei sistemi informatici") e all'Università di Bologna ("Strumenti multimediali per l'interazione nei servizi digitali").
(continua)
https://www.ingenio-web.it/34745-smart-building-domotica-e-cyber-security-la-vulnerabilita-delliot
***INGENIO** - Bracci Elisabetta - 25/05/2022*

Come difendere dal rischio idraulico una città: il caso di Olbia - A seguito di un evento eccezionale che ha messo in crisi la città di Olbia, si è deciso, dopo un processo di analisi basato su una visione multidisciplinare del problema, di compiere una serie di interventi per la messa in sicurezza dal rischio idraulico del centro urbano. All'interno i dettagli degli interventi.
(continua)
https://www.ingenio-web.it/34777-interventi-per-la-difesa-idraulica-di-olbia
***INGENIO -** Venturini Simone, 26 mag 2022*

Security Summit: il settore energetico e la guerra cyber - L'evento verticale ha sondato lo scenario della sicurezza informatica per le infrastrutture critiche e in particolare per il comparto Energy & Utilities.
La Cyberwarfare è stata il punto di partenza per la discussione sviluppata nel contesto dell'Energy & Utilities Security Summit, la tavola rotonda verticale, ormai alla seconda edizione, organizzata da Clusit (Associazione Italiana per la Sicurezza Informatica), insieme ad AIPSA (Associazione Italiana Professionisti Security Aziendale) e Utilitalia (Federazione delle imprese idriche, energetiche e ambientali).
La crisi tra Russia e Ucraina ha portato all'attenzione pubblica il tema della guerra cibernetica tra Stati, che puntano a piegare il sistema e l'economia degli avversari attraverso gli attacchi informatici.
Le grandi infrastrutture di produzione, trasporto e distribuzione dell'energia, da sempre obiettivi sensibili in termini di cyber risk, diventano i bersagli privilegiati dell'attuale conflitto, visto che le forniture energetiche sono il perno del regime sanzionatorio contro la Russia.
L'argomento, insieme ad alcune tematiche più generali sull'evoluzione della cybersecurity, è stato oggetto del dibattito che ha visto coinvolti alcuni dei principali attori italiani del mercato dell'energia.
Indice degli argomenti
Gli attacchi cyber in Italia e nel mondo

Aumentano gli attacchi alle infrastrutture critiche
Le riflessioni delle imprese del settore Energia
(continua)
https://www.zerounoweb.it/techtarget/searchsecurity/cybersecurity/security-summit-il-settore-energetico-e-la-guerra-cyber/
Zerounoweb - *Arianna Leonardi 07 Giu 2022*

How Do We Secure Our Cities From Attack? Physical access matters in keeping people and buildings safe. Points to consider when establishing a physical security protocol are ways to lock down an area to keep people safe, approaches to communicate clear safety directions, and access control. As organizations around the world fortify their systems against the threat of cyberattacks, it's imperative businesses and cities don't neglect the potential harm from a physical threat. Recent attacks in Sacramento and Brooklyn are horrific examples of the threats that can impact cities without warning. Attacks that occur in broad daylight and outdoors are difficult to protect against, especially in the immediate surrounding areas. How and when should nearby buildings lock themselves down and maintain access control? What protocols should businesses have in place for when sudden violence arises? While every building and business will vary in its risk tolerance and security needs, there are several best practices that all should consider when establishing a physical security protocol.
Understand the Immediate Priorities During Attack
In a situation of sudden violence, the first priority of any building or business in the surrounding area must be to lockdown its premises to keep employees, guests, and customers safe. In any zones in which the threat is unknown or unidentified, locking down is the safest immediate response. Secondly, communicate clear directions to those in your building or campus, especially if it is sprawling. For example, hospitals and college campuses are large areas where it can be difficult to communicate to everyone at once – having an emergency communications mechanism in place such as mass texts or mobile alerts systems alleviate any confusion.
The third and final priority is access control. *(continua….)*
https://www.darkreading.com/physical-security/how-do-we-secure-our-cities-from-attack-
Darkreading **-** *Mark Allen - June 08, 2022*

We still need to talk about data protection
Safeguarding fundamental rights should no longer be a radical dream, but an obvious reality.
When you're a regulatory authority responsible for compliance, being called a "rulebreaker" doesn't happen every day — but it's what happened to me.
Nominated to this year's POLITICO Tech 28 list, my profile read, "Wiewiórowski is making waves." He's "broken a Brussels taboo," "daring to question whether the EU's flagship General Data Protection Regulation is up to scratch."
I remember reading these words for the first time and feeling a sense of pride in the institution I have the honor to lead — and a sense of worry. If questioning how to better bring practices into compliance and pointing out problems in your own backyard are seen as controversial, this says something about the state of public debate — at least with respect to the protection of fundamental rights.
While data protection is sometimes perceived as technical and bureaucratic, the GDPR, which encapsulates Europe's rules for data protection and privacy, probably remains one of the most well-known pieces of legislation in the world — particularly among EU citizens. And though data protection

existed before it, the new regulation was needed to step up compliance across the bloc, using stronger enforcement mechanisms to ensure greater protection of individual rights.
Though enforcement is only a tool for accomplishing this primary objective of the GDPR, the mechanism and means through which it's achieved remain prominently relevant. And what the last four years have shown is that where enforcement lacks, so does an individual's ability to have their rights realized *(continua….).*
https://www.politico.eu/article/eu-data-protection-gdpr-brussels-regulation-supervision/
Politico- *WOJCIECH WIEWIÓROWSKI -June 9, 2022*

Cybersecurity, Bonfanti (Acn): "Rischi crescenti per la sanità" - Il rappresentante dell'Agenzia per la cybersicurezza nazionale: "Il settore vive un inarrestabile processo di digitalizzazione e innovazione tecnologica, che comporta benefici e opportunità ma espone anche a minacce sempre più sofisticate".
"Il settore sanitario vive un inarrestabile processo di digitalizzazione e innovazione tecnologica, e questo se da un lato comporta benefici e opportunità straordinarie per operatori e utenti, dall'altro li espone a rischi, vulnerabilità e minacce sempre più sofisticate perpetrate da attori, statuali e non, che ricorrono allo strumento cibernetico per accedere ai dati o per compromettere l'erogazione di un servizio, spesso chiedendo il pagamento di riscatti di denaro". Lo ha detto Matteo Bonfanti, in rappresentanza dell'Agenzia per la cybersicurezza nazionale, durante il suo intervento al convegno "Cybersecurity e protezione dei dati personali nella sanità" organizzato dalla Fondazione Icsa con Link Campus University.
Rispetto alla tipologia dei rischi a cui il sistema sanitario è e sarà sottoposto Bonfanti sottolinea il fatto che "si tratta di una minaccia in evoluzione, per contrastare la quale va messo in campo un insieme di capabilities che l'Italia sta acquisendo e rafforzando".
Per fronteggiare al meglio le nuove minacce esistono una serie di normative specifiche, come la direttiva Nis 1 (Network and information security), recepita in Italia dal decreto legislativo 65 del 2018, che "stabilisce l'obbligo per l'operatore di adottare in ambito nazionale misure adeguate a fronteggiare il rischio cyber – spiega l'esperto – direttiva che sarà sostituita dalla Nis 2, tesa a migliorare ulteriormente la resilienza e la capacità di risposta del sistema in tutta Europa".
Quanto alle tecnologie necessarie per prevenire gli attacchi informatici, affrontarli e minimizzarne le conseguenze negative "servono soluzioni capaci di proteggere dati e i servizi, ma anche tecnologie mediche concepite e realizzate avendo in mente il rischio cyber che implica un livello di protezione sempre più elevato", prosegue Bonfanti.
Ma non si deve dimenticare l'aspetto culturale: "Va diffusa una consapevolezza della minaccia che sola può accrescere la protezione del dato anche a livello individuale", spiega.
L'approccio con norme, tecnologie e formazione è proprio quello che caratterizza la strategia nazionale di cybersicurezza adottata dal presidente del Consiglio, prosegue Bonfanti, "Perché tutti gli stakeholder del settore – istituzioni centrali e locali, privati, società civile – devono fare fronte comune nell'attivare misure tali da aumentare il livello di cybersicurezza e di resilienza del Paese, tutelando settori nevralgici per l'economia e la sicurezza dello Stato".
https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-bonfanti-acn-rischi-crescenti-per-la-sanita/
Corriere delle comunicazioni *- A. S. - 14 Giu 2022*

Chips Can Boost Malware Immunity

Security is becoming an increasingly important design element, fueled by increasingly sophisticated attacks, the growing use of technology in safety-critical applications, and the rising value of data nearly everywhere.

Hackers can unlock automobiles, phones, and smart locks by exploiting system design soft spots. They even can hack some mobile phones through always-on circuits when they are turned off. Earlier this year, Okta, a security firm that provides authentication services to many companies, also was hacked. The Critical Vulnerability cyberattack, known as *Error! Hyperlink reference not valid.* (mitre.org), and rated at a critical level of 9.9, put 90,000 websites at risk of being completely controlled by hackers. Even more alarming, much of this can slip by security software completely undetected. For example, Enterprise Security Information and Event Management (SIEM), an always-on cybersecurity analytics tool, could not detect 80% of cyberattack techniques, according to CardinalOps.

On the positive side, built-in hardware security will help developers strengthen system defense.

Trust no one

Threat actors always pretend to be somebody else, particularly those with credentials to access networks. Any part of those networks or systems should not grant access to anyone easily until the access request is fully authenticated. After authentication, access should be granted only one time, for a particular asset, at the time when it is requested. Additionally, the authentication must be presented with credible information such as account passwords, account credentials, and keys (API, SSH, encryption).

A relatively new concept called "zero trust" is being deployed to increase cybersecurity at all levels. The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, defines zero trust (ZT), in part, as "an evolving set of cybersecurity paradigms that moves defenses from static, network-based perimeters to focus on users, assets, and resources. A zero-trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows."*(...)*

How chips boost immunity to malware Many of these cybersecurity defense mechanisms (zero trust, secure boot, authentication, secure key management, and side-channel attack protection) that used to be performed by enterprise software are now being done automatically at the chip or firmware level inside the device. That not only increases the overall performance of the system, but it also makes them more secure. It's important to keep in mind, however, that there is more than one way to implement chip security.*(continua...)*

https://semiengineering.com/chips-can-boost-malware-immunity/

SEMIENGINEERING- *JOHN KOON - JUNE 15TH, 2022*

International operation takes down Russian RSOCKS botnet. $200 a day buys you 90,000 victims

A Russian operated botnet known as RSOCKS has been shut down by the US Department of Justice acting with law enforcement partners in Germany, the Netherlands and the UK. It is believed to have compromised millions of computers and other devices around the globe. The RSOCKS botnet functioned as an IP proxy service, but instead of offering legitimate IP addresses leased from internet service providers, it was providing criminals with access to the IP addresses of devices that had been compromised by malware, according to a statement from the US Attorney's Office in the Southern District of California. It seems that RSOCKS initially targeted a variety of Internet of Things (IoT) devices, such as industrial control systems, routers, audio/video streaming devices and various internet connected appliances, before expanding into other endpoints such as Android devices and computer systems. The DoJ said that the RSOCKS botnet operators managed to compromise target devices simply

by conducting brute force attacks rather than taking advantage of any software security vulnerabilities. Security experts and analysts have been warning for many years about the threat posed by IoT devices, especially those aimed at consumers who are unlikely to know or care much about security settings or applying software updates as soon as possible, although even large corporations have been known to get careless too. According to the DoJ, cybercriminals who wanted to use the RSOCKS platform could simply access a web-based storefront which allowed them to pay for access to a pool of proxies for a specified time period, with prices ranging from $30 per day for access to 2,000 proxies to $200 per day for access to 90,000 proxies. (continua…)
https://www.theregister.com/2022/06/17/rsocks_russia_botnet/
THEREGISTER - *Dan Robinson - Fri 17 Jun 2022*

Tregua mai. Dentro le cyber gang di Putin in Ucraina
Come la guerra sul campo, anche la guerra cyber russa contro l'Ucraina si adatta, cambia, evolve. Dagli hacker pluripremiati del Cremlino alle gang bielorusse, chi si muove sul campo per colpire la resistenza. L'analisi di Federico Berger, esperto di social media intelligence
Che la disinformazione in ambienti digitali non sia più un mestiere per pochi amatoriali, desiderosi di racimolare qualche spicciolo in più con articoli sensazionalistici fabbricati ad hoc dai titoli roboanti, è ormai ampiamente sotto gli occhi di governi e istituzioni. A partire dalle elezioni Usa 2016 (vero e proprio spartiacque per quanto riguarda le campagne di influenza informativa online) si è assistito alla progressiva sofisticazione e pervasività di queste attività sia dal punto di vista delle narrative impiegate, sia per quanto riguarda gli aspetti squisitamente tecnici.
Anche se le operazioni di hack and leak al comitato elettorale di Hillary Clinton sembrano un lontano ricordo, la guerra in Ucraina ha dimostrato come le campagne di disinformazione odierne richiedano necessariamente infrastrutture informatiche con un certo costo e capacità di programmazione di buon livello. Due componenti cardine nelle manovre dei cosiddetti gruppi di hacker state-sponsored o Apt, collettivi che vengono finanziati da attori statuali e agiscono per conto di governi o dei servizi di intelligence a vario scopo. Anche se questi avversari si occupano in larga parte di infiltrarsi nei network nemici o di compromettere i sistemi, talvolta possono anche essere impiegati come supporto tecnico nelle InfoOps e nelle attività disinformative strutturate.
Stando quindi a un report pubblicato dal gigante della cybersecurity Mandiant sulle Information Operation del Cremlino durante l'invasione del Paese vicino, il conflitto tra Mosca e Kiev è solo il più recente esempio di come i gruppi Apt abbiano un ruolo di primo piano nel processo, alcuni di questi noti da diverso tempo e riconducibili alla stessa Russia o all'amica Bielorussia.*(continua…)*
https://formiche.net/2022/06/tregua-gang-putin-ucraina/
FORMICHE *- Federico Berger - 18/06/2022 -*

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

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 *ai quali potete inviare suggerimenti e quesiti scrivendo a:* *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