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 2020	N. 03/ 2020	Marzo 2020

Stato dell'arte sulle Certificazioni Cyber

Il Regolamento UE 2019/881 dell'Unione Europea (Cybersecurity Act) del 2019 ha stabilito "un quadro per l'introduzione di sistemi europei di certificazione della sicurezza informatica. Tale schema di certificazione prevede che i prodotti, servizi e processi ICT valutati nel loro ambito siano "conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita". Un "programma di lavoro progressivo dell'Unione", in cui saranno individuate le priorità strategiche, sarà pubblicato entro il 28 giugno 2020[1].

L'idea alla base della creazione di uno schema di certificazione di un prodotto ICT è quella di controllare un insieme di requisiti minimi di sicurezza, una singola volta, e per tutti i clienti, fermo restando che questi ultimi dovranno effettuare una propria attività di investigazione al momento dell'acquisto.

Prendendo in esame i principali studi di settore, regolamenti nazionali ed europei è possibile analizzare lo stato di avanzamento delle normative inerenti agli schemi di certificazione cyber.

Dalla metà degli anni '90 esiste in Italia una struttura per la certificazione della sicurezza di sistemi/prodotti ICT, ma tale struttura, denominata Schema Nazionale, è utilizzabile esclusivamente nell'ambito della sicurezza nazionale. Con il DPCM del 30 ottobre 2003 è stato istituito un secondo Schema Nazionale il quale è idoneo a fornire servizi di certificazione a tutti i settori della PA che non afferiscono al contesto della sicurezza nazionale. Entrambi questi Schemi sono stati definiti secondo quanto previsto dalle normative internazionali nell'ambito della certificazione di sistema/prodotto ICT, tanto che la loro struttura è fortemente condizionata da alcune caratteristiche degli standard Common Criteria ed ITSEC[2].

Il processo di certificazione nazionale è diviso in due parti: la valutazione, e la certificazione. Una volta terminata la prima parte, è possibile esaminare il Rapporto Finale di Valutazione e utilizzare quest'ultimo come base per produrre un Rapporto di Certificazione, che attesta che l'analisi è stata condotta secondo criteri stabiliti, e il relativo Certificato, valido solo per la specifica versione e configurazione del prodotto[3].

Nel novembre del 2019 è stato approvato anche il Perimetro di Sicurezza Nazionale Cibernetica, che ha confermato il ruolo del Centro di Valutazione e Certificazione Nazionale (CVCN) nell'assicurazione delle garanzie di sicurezza e dell'assenza di vulnerabilità di prodotti destinati a essere impiegati sulle reti, sui sistemi informativi e sui servizi informatici dei soggetti interni al perimetro nazionale. In aggiunta, attraverso l'utilizzo di poteri speciali, il Governo italiano può imporre specifiche prescrizioni o condizioni in relazione "alla stipula di contratti o accordi aventi ad oggetto l'acquisizione di beni o servizi basati sulla tecnologia 5G[4]. Il Governo italiano può quindi richiedere un determinato livello di certificazione o attuare il potere di veto.

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32019R0881&from=EN
[2] http://www.ocsi.isticom.it/index.php/organismo
[3] http://www.ocsi.isticom.it/index.php/organismo/lo-schema
[4] https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg

Proprio relativamente alla tecnologia 5G, il provvedimento più recente in ambito europeo è l'EU Toolbox, del gennaio 2020, con il quale la Commissione Europea è intenzionata a far fronte al rischio di interferenze da parte di un paese terzo attraverso la catena di approvvigionamento del 5G. La Commissione ha invitato i membri a porre condizioni specifiche in tal senso, compresi schemi di certificazione.

Oltre alle tecnologie 5G, un altro settore che merita un'analisi è quello delle Certificazioni Cloud. I servizi di cloud computing, infatti, sono complessi e costruiti a partire da diverse componenti ICT risultando quindi di difficile valutazione per i clienti. A tale riguardo, nel 2012 la Commissione Europea ha pubblicato la comunicazione "Strategia europea per il cloud computing - liberare il potenziale del cloud computing in Europa" per assistere lo sviluppo di sistemi di certificazione a livello europeo per crearne un elenco[5].

ENISA, incaricata di supportare lo studio, ha realizzato la Cloud Certification Schemes List (CCSL), attraverso la quale è in grado di offrire una panoramica dei diversi schemi di certificazione esistenti e le relative caratteristiche[6]. Sempre sotto il dominio di ENISA è presente anche il Cloud Certification Schemes Metaframework (CCSM), un tool online che rappresenta una mappatura che prenda contemporaneamente in esame i requisiti di sicurezza della rete e dell'informazione desiderati dal cliente, e gli obiettivi di sicurezza degli schemi di certificazione cloud esistenti, in modo tale da facilitarne la scelta[7].

Infine, per completare lo stato dell'arte riguardo alle certificazioni, è opportuno menzionare lo studio IACS Cybersecurity Certification Framework, un rapporto che ha avuto come scopo quello di presentare gli esperimenti del componente IACS (Industrial Automation and Control Systems) Cybersecurity Certification Framework (ICCF) eseguiti nel 2017 dalle squadre nazionali di esercitazione (NET) di Francia, Polonia e Spagna. Basato su casi reali di utilizzo e simulazioni di attività ICCF, tale rapporto documenta le attuali pratiche di certificazione dei paesi menzionati e le opinioni dei membri delle squadre NET in relazione alla certificazione della sicurezza informatica dei prodotti IACS[8].

,

Luisa Franchina Cofondatore di AIIC ne è attualmente Presidente.
È stato Direttore Generale del Segretariato per le infrastrutture critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche

[5] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
[6] https://resilience.enisa.europa.eu/cloud-computing-certification
[7] https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework
[8] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111611/the_iacs_cybersecurity_certification_framework.pdf

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

Matteo Taraborelli Laureato in Relazioni Internazionali e specializzato negli studi di sicurezza e difesa. Per la tesi di laurea magistrale ha svolto un periodo di ricerca presso i National Security Archive di Washington, D.C. Ricopre il ruolo di Junior Analyst and Consultant presso la società Hermes Bay

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2020

Si ricorda a tutti i soci che il 31 dicembre 2019 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 2020".

Per i nuovi iscritti l'importo da pagare è di € 60,00 mentre per i soci attuali la quota di rinnovo rimane sempre fissata a € 40,00. 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 2020. 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.

Informiamo i sigg. Soci e i followers di AIIC che, a seguito delle disposizioni volte a contrastare la diffusione del virus COVID-19 (Coronavirus), l'Associazione ha deciso di annullare fino a nuova comunicazione tutti i seminari e le attività di formazione previste. Confidiamo di riprenderle presto!

Vi terremo informati, per il momento vi auguriamo buona lettura!

Attività del Gruppo di lavoro

Il nuovo Gruppo di Lavoro. "**Internet of Things (IoT) in the context of Critical Infrastructures: Cybersecurity and Privacy concerns and possible solutions**" ha iniziato la sua attività ed ha svolto riunioni nei mesi di novembre, dicembre e febbraio Il Gdl è coordinato da Sandro Bologna e vede la partecipazione dei soci: Silvano Bari, Glauco Bertocchi, Luigi Carrozzi, Luisa Franchina, Francesco Ressa, Angelo Socal, Alberto Traballesi.

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 Association 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.

NEWS E AVVENIMENTI

Perché la cybersecurity by design salverà l'Ict - La rapida espansione dell'Ict, dagli utilizzi più complessi agli oggetti di uso quotidiano, comporta un aumento del rischio di attacchi cyber e di furto dei dati personali. La cyber security svolgerà, dunque, un ruolo centrale per proteggere i sistemi Ict fin dalla loro progettazione.
La quarta rivoluzione industriale ha definitivamente sancito la dipendenza dalle *Information and communication technologies (Ict)* dell'economia e degli altri settori e infrastrutture critiche considerati essenziali per il funzionamento di un Paese (energia, trasporti, sanità, finanza).
Il fenomeno dell'internet of things descrive l'ulteriore espansione delle Ict all'ambiente "non biologico" che implica la connessione alla grande rete di oggetti, impianti, strumenti, processi, ma anche l'ampliamento del perimetro di violazione offerto a eventi e comportamenti (hacking "non etico", errore umano, fenomeni naturali)……..
https://formiche.net/2020/02/ict-cybersecurity-design/
Formiche.net *– Giovanni Crea – febbraio 2020*

Sanità e geografia - Il mondo della "Science of Where" e quello della Sanità spesso si sono incrociati e il valore aggiunto della georeferenziazione è innegabile: ma questo non basta. In questi giorni in cui il Coronavirus è al centro dell'attenzione mediatica, abbiamo visto le mappe di Esri Italia su tutti gli organi di informazione, inclusi quelli televisivi. Però il contributo che può dare la Science of Where va ben oltre a una rappresentazione dei casi su mappa: può essere di grande ausilio per capire i movimenti che sono avvenuti tra le persone infette e capire provenienza e diffusione.
Già nell'Ottocento si iniziano a usare le mappe per circoscrivere la diffusione delle malattie, ma è alla fine del secolo scorso che diventano fondamentali per capire la correlazione tra l'incidenza di alcune malattie e la componente geografica. Agli inizi del 2000, come Esri Italia, abbiamo supportato la più grande azienda internazionale che analizza dati sulla vendita dei farmaci, georeferenziando ospedali, farmacie e medici di base di tutta Italia……..
https://www.esriitalia.it/38-eventi/656-sanita-e-geografia-un-connubio-imprescindibile
Esri Italia *– Emilio Misuriello – 02 febbraio 2020*

IoT e Security: cosa c'è dietro un attacco Cyber? Come gestire e mitigare il rischio - Intelligenza artificiale e Internet of Things, ricopriranno un ruolo sempre più importante nelle attività quotidiane e nei settori produttivi. Tuttavia, i sistemi intelligenti e gli oggetti connessi in rete potrebbero comportare dei rischi da non sottovalutare…….
https://www.ingenio-web.it/25751-iot-e-security-cosa-ce-dietro-un-attacco-cyber-come-gestire-e-mitigare-il-rischio?utm_term=34973+-+https%3A%2F%2Fwww.ingenio-web.it%2F25751-iot-e-security-cosa-ce-dietro-un-attacco-cyber-come-gestire-e-mitigare-il-rischio&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3332+-+1839+%282020-02-10%29
***INGENIO** - Marco Baldi - - 06/02/2020*

Le cause tecniche del crollo del cavalcavia di Annone - La memoria presenta le cause tecniche del crollo del cavalcavia di Annone, avvenuto nell'ottobre del 2016. L'articolo sintetizza le prove svolte per identificare le caratteristiche dei materiali impiegati per la costruzione, i calcoli di verifica che hanno condotto alla identificazione del meccanismo di collasso e le prove sulla membratura ritenuta critica all'atto del collasso. La memoria mette in evidenza le criticità sopraggiunte in concomitanza del passaggio del trasporto eccezionale, il coefficiente di sicurezza nei confronti dei carichi di progetto all'atto della costruzione e quello all'atto del passaggio del convoglio eccezionale. Nella nota si mettono in luce anche alcune criticità del sistema infrastrutturale nazionale, con particolare riferimento al trasporto eccezionale e alle modalità che potrebbero essere impiegate per evitare futuri incidenti in assenza di macro-errori progettuali…….
https://www.ingenio-web.it/24090-le-cause-tecniche-del-crollo-del-cavalcavia-di-annone?utm_term=35166+-+https%3A%2F%2Fwww.ingenio-web.it%2F24090-le-cause-tecniche-del-crollo-del-cavalcavia-di-annone&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3346+-+1846+%282020-02-14%29
***INGENIO -** Martinelli Paolo - Colombo Matteo - Di Prisco Marco - 09/02/2020*

Nasce SICURO+, il portale del rischio sismico della Protezione Civile. Che cosa è e come funziona - Nasce la piattaforma SICURO+ (Sistema Informativo di ComUnicazione del RischiO, sito di SICURO+), finanziata dal Dipartimento della protezione civile e realizzata dalla Fondazione Eucentre. SICURO+ si propone di comunicare il rischio sismico, nelle sue diverse sfaccettature, a cittadini, tecnici e amministratori pubblici, che potranno così consultare le valutazioni del rischio sismico a livello comunale relative al patrimonio edilizio residenziale italiano……..
https://www.ingenio-web.it/25834-nasce-sicuro-il-portale-del-rischio-sismico-della-protezione-civile-che-cosa-e-e-come-funziona?utm_term=35163+-+https%3A%2F%2Fwww.ingenio-web.it%2F25834-nasce-sicuro-il-portale-del-rischio-sismico-della-protezione-civile-che-cosa-e-e-come-funziona&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3346+-+1846+%282020-02-14%29
***INGENIO** AA.VV. - 17/02/2020*

Smart Home: il mercato italiano vale 530 milioni di euro e cresce del 40% - L'Osservatorio Internet of Things della School of Management del Politecnico di Milano ha presentato i risultati della ricerca sulla Smart Home: la crescita è buona, ma in valore assoluto l'Italia rimane ancora indietro rispetto a Germania, UK e Francia.

Il consumatore sembra più ricettivo alle nuove offerte per la casa, ma è preoccupato per i rischi privacy e sicurezza informatica. Nel frattempo il mercato è pronto per lanciare servizi più evoluti…..
https://www.ingenio-web.it/25895-smart-home-il-mercato-italiano-vale-530-milioni-di-euro-e-cresce-del-40?utm_term=35362+-+https%3A%2F%2Fwww.ingenio-web.it%2F25895-smart-home-il-mercato-italiano-vale-530-milioni-di-euro-e-cresce-del-40&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3359+-+1856+%282020-02-21%29
INGENIO *- Samorì Chiara - 20/02/2020*

Coronavirus, l'intelligenza artificiale individua i contagi in real time - Bloccare il contagio da coronavirus usando l'intelligenza artificiale per individuare i cittadini cinesi potenzialmente contagiati. È sul mercato un software realizzato dalla malese Myeg Services che mira ad automatizzare il riconoscimento dei casi di coronavirus riducendo i rischi di contagio. Il software è stato presentato ai governi di Kuala Lumpur e Manila per essere utilizzato per contrastare la diffusione del virus.
In Malaysia infatti i casi di infezione da coronavirus resi pubblici sono 22, mentre nelle Filippine ne sono stati registrati tre, di cui uno mortale. La Malaysia ha imposto un blocco temporaneo ai visitatori cinesi che provengono dalle province che sono state messe in quarantena da Pechino……..
https://www.corrierecomunicazioni.it/digital-economy/coronavirus-lintelligenza-artificiale-individua-i-contagi-in-real-time/
Corcom *– Antonio Dini – 20 febbraio 2020*

IoT data lifecycle adapts to AI at the edge - The IoT data lifecycle, as a topic of planning, design and management, doesn't get nearly the discussion it warrants in most enterprise IT departments or the C-suite. And that's unfortunate because the flow of data in and out of the enterprise may be the single biggest driver of institutional change.
Before there were clouds, the enterprise data lifecycle was simple and essentially invariable and circular. IT pros could easily implement, master and maintain the data lifecycle. Data was more structured, less varied and traveled on only a handful of channels to a few destinations. Each step in the traditional data lifecycle is conceptually straightforward:

1. **Plan.** Determine the data required to support existing business processes. Use the most current data available for operational planning and process support.
2. **Acquire.** Input data into application systems via data entry and integration with external systems.
3. **Process.** Validate through authentication and error-check the data, enriching it as needed.
4. **Analyze.** Apply the data to the appropriate business processes and study it for implications and insights that support decisions.
5. **Integrate.** Merge the results of data analysis into decision-making processes and subsequent analyses.
6. **Store.** Store the data in transactional systems for access by ongoing applications and processes and long-term archives.

The simple, orderly scheme had already been groaning under the weight of the internet before the advent of the cloud. With clouds came new possibilities for connecting the IT core of the enterprise to a geometric explosion of new devices, and manufacturers wasted no time in taking advantage of that opportunity.
The global IoT device population will pass 20 billion this year. That doesn't just stress the old data lifecycle, it shatters old-school architecture like an eggshell. Even the easy connectivity of clouds doesn't begin to open enough channels for the data generated by IoT. The massive increase in traffic calls for new architecture……..

https://internetofthingsagenda.techtarget.com/feature/IoT-data-lifecycle-adapts-to-AI-at-the-edge?track=NL-1843&ad=932552&src=932552&asrc=EM_NLN_124075637&utm_medium=EM&utm_source=NLN&utm_campaign=20200225_IoT%20data%20lifecycle%20adapts%20to%20AI%20at%20the%20edge
Tech Target IoT Agenda *- Scott Robinson, Lucina Health – 20 feb 2020*

How software-defined perimeter authentication ups security – The software-defined perimeter (SDP) is an emerging security model that has a set of specific characteristics defined by the Cloud Security Alliance (CSA). The two most important of these SDP characteristics are the following:

- The two ends of the connection must be authorized before any traffic can pass between them.
- SDPs essentially hide devices and traffic from the public internet, even while using it as a transport mechanism.

Within an SDP architecture, before establishing a connection, devices at either end of a connection must authenticate with one another using single-packet authentication, a lightweight security protocol that validates a device or user's identity before permitting a connection to be established.
Specifically, the information for a connection request, including the requester's IP address, is encrypted and authenticated in a single network packet. It is essentially caller ID for network packets: "Hello, this is Alice calling Bob. Will you accept a call from me?"
But how is Bob to know that Alice is who she claims to be? Enter authorization.
The senders' and receivers' identities can be authorized via a range of standard authorization mechanisms, including public key infrastructure services, device attestation, geolocation, SAML, OpenID, OAuth, LDAP, Kerberos, multifactor authentication, identity federation and other similar services. To continue the example, with software-defined perimeter, Alice and Bob must both be authenticated before the connection is established.
This authenticate-then-connect approach is the exact opposite of native TCP/IP, which follows a connect-then-authenticate model. By forcing a sender and receiver to authenticate before passing traffic between them, a software-defined perimeter can avoid a host of difficulties, including man-in-the-middle attacks, distributed denial-of-service attacks and other forms of identity hijacking……
https://searchsecurity.techtarget.com/tip/How-software-defined-perimeter-authentication-ups-security?src=6037440&asrc=EM_ERU_124059336&utm_content=eru-rd2-rcpB&utm_medium=EM&utm_source=ERU&utm_campaign=20200225_ERU%20Transmission%20for%2002/25/2020%20(UserUniverse:%20678619)
Tech Target *– Johna Till Johnson – 25.02.2020*

AZORult, il malware che si spaccia per una nuova versione di ProtonVPN e ruba dati riservati: i dettagli – È in atto una campagna di malvertising che i criminal hacker usano per diffondere una variante di AZORult, un trojan che si nasconde dentro un finto installer del famoso tool di sicurezza ProtonVPN e il cui scopo è quello di rubare credenziali di posta elettronica ed FTP (memorizzate nel tool FileZilla), informazioni riservate, cookie e cronologie dei browser delle vittime. In questa nuova versione del malware, inoltre, i criminal hacker hanno implementato alcune routine per carpire criptovalute da wallet installati in locale (tra cui Bitcoin, Electrum ed Etherium). Il malware AZORult risulta essere uno dei trojan più acquistati e venduti sulle Darknet russe, grazie sicuramente al costo davvero irrisorio (circa 100 dollari), ma soprattutto per la sua ampia versatilità di utilizzo, nonché per le sue elevate prestazioni. Tra le sue peculiarità si annovera quella di poter essere adoperato come downloader di altri ceppi malware. Solo nel primo trimestre del 2019 il numero di utenti italiani colpiti da questo trojan, la cui firma virale è stata identificata con Trojan-PSW.Win32.Azorult, sono stati più di 2.000.

Secondo i ricercatori di sicurezza di Kaspersky che ne hanno individuato le prime tracce fin dal mese di novembre del 2019, il malvertising usato per la diffusione del codice malevolo di AZORult sfrutta l'onorabilità del servizio ProtonVPN, noto fornitore di servizi VPN (Virtual Private Network) ed e-mail open source incentrati sulla sicurezza sviluppati e gestiti dalla società svizzera Proton Technologies AG La campagna malevola sarebbe iniziata con la comparsa di un nuovo dominio **protonvpn[.]Store** che altro non è se non un finto sito Web clonato mediante un noto crawler open source HTTrack per richiamare in tutto e per tutto l'home page di ProtonVPN…..
https://www.cybersecurity360.it/nuove-minacce/azorult-il-malware-che-si-spaccia-per-una-nuova-versione-di-protonvpn-e-ruba-dati-riservati-i-dettagli/
Cybersecurity 360 *– Salvatore Lombardo – 26 febbraio 2020*

Intercettazioni, più spazio all'uso dei trojan – Sono soprattutto i trojan – ovvero i captatori informatici "iniettati" nei telefonini o nei dispositivi portatili – e in particolare il loro uso, i nuovi protagonisti del decreto intercettazioni**.** L'utilizzo dei trojan, era già previsto dalla riforma dell'ex Guardasigilli, ma lo circoscriveva alle inchieste riguardanti reati gravissimi, come mafia e terrorismo. Inoltre le intercettazioni erano conservate e custodite dalla polizia investigativa e potevano infine essere utilizzate esclusivamente nell'ambito del procedimento per cui erano state disposte. La nuova formulazione introduce significative novità. I captatori informatici sono equiparati alle intercettazioni ambientali e viene introdotto l'obbligo di motivazione ulteriore che ne giustifichi l'utilizzo per i reati diversi da quelli di mafia e terrorismo purché si tratti di reati punibili con la reclusione oltre i 5 anni.
Inoltre, sarà possibile utilizzare i trojan non solo per i reati contro la pubblica amministrazione commessi dai pubblici ufficiali, ma anche per quelli commessi dagli "incaricati di pubblico servizio". Infine l'intercettazione attraverso captatore, come avviene nel caso di reati che coinvolgono pubblici ufficiali, potrà avvenire anche dentro le mura di casa….
https://www.corrierecomunicazioni.it/digital-economy/intercettazioni-piu-spazio-alluso-dei-trojan-ecco-le-novita/
Corcom *– Federica Meta – 26 febbraio 2020*

La protezione delle infrastrutture critiche dalle minacce cyber: rischi, soluzioni e competenze
La protezione delle infrastrutture critiche dalle minacce cyber impone agli Operatori di Servizi Essenziali di dotarsi di un'efficace gestione del rischio cyber tramite l'adozione di misure tecniche e organizzative atte a prevenire e minimizzare l'impatto degli incidenti. Ecco gli scenari e le tematiche da affrontare….
https://www.cybersecurity360.it/soluzioni-aziendali/la-protezione-delle-infrastrutture-critiche-dalle-minacce-cyber-rischi-soluzioni-e-competenze/
Cybersecurity360 *- Nicola Scarnera – 2 marzo 2020*

Smart working e cyber security: best practice per mettere in sicurezza le infrastrutture aziendali - Non si può parlare di smart working senza tenere in debita considerazione le problematiche relative alla cyber security correlate al lavoro agile: l'accesso remoto alla rete aziendale, infatti, amplia la superfice d'attacco. Ecco i fattori da tenere presente per garantire la sicurezza dei lavoratori e delle infrastrutture aziendali…..
https://www.cybersecurity360.it/soluzioni-aziendali/smart-working-e-cyber-security-best-practice-per-mettere-in-sicurezza-le-infrastrutture-aziendali/
Cybersecurity360 *- Sergio Cazzaniga– 3 marzo 2020*

Most Cyberattacks in 2019 Were Waged Without Malware If the "malware-free" attack trajectory continues, it could mean major trouble for defenders, according to experts from CrowdStrike and other security companies.
A modern spin on the old-school hacker-behind-the-keyboard attack exceeded malware-borne ones worldwide last year, new incident report data from CrowdStrike shows. Seasoned cybercriminals and nation-state attackers for some time now have been upping their game with new methods to mask their activities from security tools by blending in and posing as real users in the targeted organization's network - using stolen credentials and running legitimate tools to dig through victim systems and data, for instance. And for the first time in CrowdStrike's research and incident response engagement reporting, so-called "malware-free" attacks edged ahead of malware-based ones, at 51% to 49% in 2019. In 2018 and 2017, malware accounted for around 60% of all attacks globally, and malware-free attacks around 40%, according to CrowdStrike's data. A malware-free attack in CrowdStrike's parlance is one where the method to gain entry into a victim organization doesn't employ a malicious file or file fragment to a computer disk. In addition to stolen credentials or legitimate tools, this type of attack also can execute code from memory and can only be detected with higher-level tools and techniques that spot unusual behavior, or via threat hunting…..
https://www.darkreading.com/threat-intelligence/most-cyberattacks-in-2019-were-waged-without-malware/d/d-id/1337239
DARK READING - *Kelly Jackson Higgins - 04-03-2020*

Alleged Vault 7 leaker trial finale: Want to know the CIA's password for its top-secret hacking tools? 123ABCdef Tales of terrible security, poor compartmentalization, and more, emerge from the Schulte hearings. **Analysis** The fate of the man accused of leaking top-secret CIA hacking tools – software that gave the American spy agency access to targets' phones and computer across the world – is now in the hands of a jury. And, friend, do they have their work cut out for them. Joshua Schulte stands accused of stealing the highly valuable materials directly from the CIA's innermost sanctum and slipping them to WikiLeaks to share with the rest of the planet. Federal prosecutors have spent the past four weeks explaining exactly why they believe that to be the case. And Uncle Sam's lawyers have developed a compelling case to send Schulte away for virtually the rest of his life. But Schulte's lawyer, Sabrina Shroff, has picked away at that seemingly watertight case, and pointed out, countless times, that the evidence against her client is dangerously thin. Schulte is the fall guy, she argues; the victim of an agency that decided he was responsible, and then used its extraordinary analytical focus to nail him regardless of his innocence. The CIA may have wished the trial never happened, because, in the course of events, the picture of what actually happens in the darkest corners of what may be the most powerful institution on Earth is not one of the highest caliber of professionals working in their nation's best interests. Instead, the leak of the world's most dangerous hacking tools, code-named Vault 7, may have stemmed from a rubber-band fight that got out of hand……
https://www.theregister.co.uk/2020/03/05/cia_leak_trial/
THE REGISTER *- Kieren McCarthy - 5 Mar 2020*

Securing Our Elections Requires Change in Technology, People & Attitudes
Increasing security around our election process and systems will take a big effort from many different parties. Here's how. The security of our elections is top of mind for practically every voter in the US.

With the state primaries underway, all eyes are on our electronic (and in some cases mobile) voting systems to understand if malicious attacks are happening — and if our systems are able to defend against them. Most experts agree that we are unprepared and underfunded when it comes to securing our elections — which should concern us all. A big problem is that when we look at the entire ecosystem of the national election process, we don't treat it the same way we treat business systems. This is a mistake. Voting is a business of our state governments. And the most valuable asset for states is voter information — similar to the customer information and data assets of a for-profit business (which are increasingly safeguarded by data privacy regulations). To modernize our current model of election management, trust, and security, it's important to examine three interrelated pillars for state governments: technology, people, and attitudes……..
https://www.darkreading.com/attacks-breaches/securing-our-elections-requires-change-in-technology-people-and-attitudes/a/d-id/1337200
DARK READING - *Earl D. Matthews- 06/03/2020*

PROSSIMI EVENTI

.NEXT on tour Roma - Sfrutta la potenza del cloud - alle tue condizioni
Tu e il tuo team IT lavorate costantemente per aumentare la produttività dei dipendenti, garantire customer experience eccezionali e favorire la crescita, ma la pressione si fa sentire. Le aziende vincenti adottano catalizzatori che accelerano la trasformazione del cloud. Hai a disposizione la tecnologia, i processi e le competenze che ti servono per portare avanti una strategia di cloud ibrido di successo? Scopri in che modo le soluzioni software di Nutanix per il cloud, la gestione dei dati e l'end user computing possono aiutarti a creare cloud semplici, intelligenti e resilienti. Unisciti a noi per scoprire:
Le principali competenze necessarie per sviluppare una strategia di cloud ibrido di successo
Come utilizzare la gestione del ciclo di vita basata sull'intelligenza artificiale e l'apprendimento automatico per garantire esperienze ideali a clienti e dipendenti
Le pratiche di consolidamento dello storage per raccogliere informazioni dai dati nel rispetto della conformità
https://www.impresacity.it/calendario.php?eventi=1843
Nutanix *- Auditorium della Tecnica ,Viale Umberto Tupini, 65 – Roma –* ~~*19 marzo2020*~~ ***RINVIATO***

Cybersecurity Summit Roma 2020 – L'economia globale dipende sempre di più dal Digitale, ma Internet, il software e le infrastrutture ICT sono fragili, vulnerabili anche ad attacchi di semplice attuazione. C'è il rischio che una diffusa mancanza di Trust, legata all'escalation delle minacce, inibisca in futuro la crescita del mercato Digitale oltre che dell'economia nel suo complesso. Durante il "**CYBERSECURITY SUMMIT 2020**", The Innovation Group farà luce sul livello di maturità della Cybersecurity raggiunto nelle organizzazioni italiane presentando la Survey "*Cyber Risk Management 2020*". Quest'anno è stato valutato: come cambia il ruolo del CISO; il programma per la Cybersecurity e sua efficacia; aspetti legati all'organizzazione, misurazione e reporting al top management; adeguamento al GDPR; sicurezza degli ambienti OT. La partecipazione al "CYBERSECURITY SUMMIT 2020" delle Istituzioni che si occupano della Cyber Defense nazionale e dei migliori Esperti italiani e internazionali, crea un'occasione unica di scambio di esperienze e di networking, per approfondire le esigenze emergenti di sicurezza, il nuovo panorama delle minacce, e per comprendere come abilitare un utilizzo più sicuro degli ambienti impattati dalle innovazioni digitali quali cloud, mobile, IoT, Industria 4.0, intelligenza artificiale.
https://www.theinnovationgroup.it/events/cybersecurity-summit-roma-2020/?lang=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

The Innovation Group *- Roma Eventi Fontana di Trevi, Piazza della Pilotta, 4 Roma –**14 maggio 2020***

FORUM PA 2020 for a smart nation - Partendo dall'**innovazione della PA**, gli innovatori italiani, le amministrazioni, le imprese innovative di ICT e servizi avanzati, i decisori politici si confrontano sull'**ecosistema digitale del Paese**, sullo **sviluppo equo e sostenibile** della comunità nazionale e delle comunità locali sulla base degli obiettivi dell'**Agenda 2030** e del paradigma dell'openness, della **partecipazione**, della partnership pubblico-privato.
https://www.forumpa.it/scopri-forum-pa-2020/
FPA *- Roma Convention Center La Nuvola Viale Asia – 9/11 giugno 2020*

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.

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

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 Email 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 cliccare questo 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*