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

Newsletter

ANNO 2021 **N. 7/ 2021** **Luglio-Agosto 2021**

Unità cibernetica congiunta

La Commissione Europea già da tempo ha rilevato la necessità di collegare gli interventi dei singoli stati membri nel campo della sicurezza cibernetica per dare una risposta condivisa e coordinata alle crisi ed agli incidenti in questo settore ed evitare eventuali posizioni in contrasto tra loro. Al fine, quindi, di rafforzare la cooperazione tra istituzioni, agenzie, organismi e autorità dell'UE in questo settore, ha istituito una piattaforma comune: la *Joint Cyber Unit (JCU)*. Ha identificato i principali problemi che essa contribuirebbe a risolvere, i suoi obiettivi e le misure necessarie per conseguire l'obiettivo. Essa sarà collocata fisicamente vicino agli uffici di Bruxelles dell'ENISA , l'Agenzia dell'UE per la sicurezza informatica, e del CERT-EU , il Computer Team di risposta alle emergenze per le istituzioni, gli organi e le agenzie dell'UE.
La JCU aiuterà le comunità civili, delle forze dell'ordine, diplomatiche e di difesa informatica a cooperare per prevenire, scoraggiare e rispondere agli attacchi informatici. Potrà così trarre vantaggio dalle competenze di tutti gli attori pertinenti nel campo della sicurezza informatica.
La Commissione (https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit) ha proposto di costruire la JCU in **quattro fasi**:

1. valutare gli aspetti organizzativi e identificare le capacità operative dell'UE entro **il 31 dicembre 2021**;
2. preparare piani nazionali di risposta agli incidenti e alle crisi e avviare attività di preparazione congiunte entro **il 30 giugno 2022**;
3. rendere operativa la JCU mobilitando le squadre di reazione rapida dell'UE, seguendo le procedure definite nel piano di risposta alle crisi e agli incidenti dell'UE entro **il 31 dicembre 2022**;
4. coinvolgere partner del settore privato, utenti e fornitori di soluzioni e servizi di sicurezza informatica, per aumentare la condivisione delle informazioni ed essere in grado di intensificare la risposta coordinata dell'UE alle minacce informatiche entro **giugno 2023.**

Le azioni chiave della JCU, sempre secondo quanto comunicato dalla Commissione, includono:

- creazione di una piattaforma fisica costruita attorno agli uffici adiacenti dell'ENISA e del CERT-EU a Bruxelles ;
- creazione di una piattaforma virtuale composta da strumenti per la condivisione sicura e rapida delle informazioni;
- fornire il piano di risposta alle crisi e agli incidenti di cibersicurezza dell'UE (basato sui piani nazionali proposti nei NIS2)
- produrre relazioni integrate sulla situazione della cibersicurezza nell'UE, comprese informazioni e intelligence su minacce e incidenti;
- istituire e mobilitare squadre di reazione rapida per la cibersicurezza dell'UE;
- conclusione di protocolli d'intesa per la cooperazione e l'assistenza reciproca;

- concludere accordi di condivisione delle informazioni e di cooperazione operativa con aziende del settore privato, sia utenti che fornitori di soluzioni e servizi di sicurezza informatica;
- mettere insieme un inventario delle capacità operative e tecniche disponibili nell'UE;
- definire sinergie strutturate con strumenti di capacità di rilevamento potenziati, in particolare SOC;
- definire un piano pluriennale per coordinare le esercitazioni e organizzare esercitazioni e corsi di formazione congiunti;
- rendicontazione: relazione intermedia sulla valutazione dei ruoli e delle responsabilità dei partecipanti e relazione finale sull'attività.

In definitiva, lo scopo dell'ICU è di far convergere le risorse, le competenze e le conoscenze disponibili in una risposta rapida, efficace e coordinata alle aggressioni cibernetiche.

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.

ATTIVITA' DELL'ASSOCIAZIONE

Rinnovo associativo per l'anno 2021

Si ricorda a tutti i soci che il 31 dicembre 2020 è scaduto il periodo associativo. Invitiamo tutti i soci a rinnovare per tempo l'associazione versando il relativo contributo, ormai inalterato da anni.
La quota per il rinnovo individuale è di euro 40 e può essere versata con bonifico sul c/c presso Banca Intesa Business, Coordinate bancarie IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando "rinnovo socio ordinario nome e cognome anno 2021".

Per i nuovi iscritti l'importo da pagare è di € 60,00. Le quote e le modalità di rinnovo per i soci collettivi – così come le indicazioni per chi vuole iscriversi come nuovo socio - sono contenute nel sito AIIC *http://www.infrastrutturecritiche.it /*

Ricordiamo che la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2021. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione, versando in più il relativo contributo per le spese di segreteria.

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

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

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

NUOVO SITO WEB AIIC

E' finalmente 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.
Nel corso dei prossimi mesi provvederemo ad arricchirlo sempre di più e ad illustrarvi le nuove funzionalità.
Vi terremo informati! Nel frattempo, vi invitiamo a navigare…

NUOVI GRUPPI DI LAVORO AIIC

Il Consiglio Direttivo di AIIC, nella riunione del 4 giugno 2021, ha approvato la costituzione di un nuovo Gruppo di Lavoro sulla "Disciplina normativa della criticità", mentre prosegue la possibilità di aderire al GdL sulla "Protezione degli spazi pubblici". Qui di seguito sono descritti i contenuti e gli obiettivi dei due GdL, riservati ai soci in regola con il versamento delle quote sociali.
Si ricorda che per l'adesione è sufficiente inviare una mail di conferma 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

Gruppo di lavoro
"ICE, ICN, OSE, OSF… La disciplina normativa della criticità"
Coordinatore Luisa Franchina

Il panorama normativo europeo e italiano sulla disciplina della protezione delle Infrastrutture Critiche è divenuto complesso.
Il GdL vuole analizzare le norme in vigore e in itinere con una pubblicazione veloce, sintetica e precisa che supporti il lettore a:

1. comprendere a colpo d'occhio quanto delineato
2. valutare le implicazioni di compliance sulla propria azienda
3. identificare opportunità
4. interpretare le direttrici di ulteriori futuri sviluppi normativi

Si invitano i Soci interessati ad aderire entro il 12 luglio 2021. Il lavoro verrà organizzato in modo da pubblicare la Linea Guida entro fine 2021.

Gruppo di Lavoro
"Principi e Tecnologie per la Protezione di Spazi Pubblici"
Coordinatore Sandro Bologna

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

La rivoluzione digitale ha aperto la possibilità di raccogliere e recuperare immense quantità di dati in tempo reale. Lo sfruttamento delle soluzioni tecnologiche offre numerose opportunità per migliorare la protezione degli spazi pubblici. Applicati e analizzati correttamente, i dati derivati dai dispositivi IoT (Internet of Things) possono fornire informazioni per il rilevamento precoce delle minacce di molteplici scenari (terrorismo, criminalità, disastri naturali, pandemie). La disponibilità di strumenti per raccogliere informazioni più complesse, complete e rapide può aiutare a prendere decisioni più informate e più tempestive. Le applicazioni mobili e le piattaforme di social media possono fungere da forum per coinvolgere i cittadini nella protezione degli spazi pubblici. Migliori canali di comunicazione e sistemi integrati consentono un migliore coordinamento e collaborazione tra le diverse autorità. Queste ampie opportunità sono accompagnate da sfide altrettanto pesanti, che devono essere affrontate dal gruppo di lavoro.

Punti principali su cui concentrarsi: In termini di tecnologia, anche il miglior hardware non sarebbe utile senza un adeguato software di analisi dei dati e il personale addestrato per gestire le informazioni. Sistemi differenti devono essere interoperabili se vogliono consentire l'analisi di dati provenienti da fonti differenti. L'interoperabilità diventa una questione ancora più complessa se applicata a sistemi utilizzati da diverse autorità, diverse città e diversi paesi. Qualsiasi sistema deve rispettare i principi di protezione della privacy sanciti dal Regolamento Generale sulla Protezione dei Dati. La tecnologia è un potente strumento per la sicurezza, ma può essere altrettanto potente come una minaccia, quindi le misure di protezione tecnologica devono evolversi di conseguenza.

Durata e conoscenze richieste ai membri del Gruppo di Lavoro: Un anno dal kick off meeting.
Membri AIIC conoscitori di una o più delle seguenti discipline: tecnologie di protezione fisica e digitale (diversi tipi di recinzioni fisiche e tecnologie IoT), analisi dei dati applicata all'analisi dei social network, interoperabilità, principi etici che regolano le applicazioni di intelligenza artificiale, principi di Protezione dei Dati Personali, progettazione della Sala Controllo di una Smart City con particolare attenzione al Security Control Center (SOC), al profilo degli operatori SOC e alla loro formazione.

Si invitano i soci che lo desiderano di comunicare il proprio interesse a partecipare inviando una mail di adesione a segreteria@infrastrutturecritiche.it.
Ricordiamo che la partecipazione ai Gruppi di Lavoro AIIC è riservata ai soci AIIC in regola con il pagamento delle quote sociali.

NEWS E AVVENIMENTI

Sicurezza zero trust in epoca smart working: verificare sempre, non fidarsi mai - Il diffondersi dello smart working e l'aumento dei dispositivi connessi alla rete aziendale stanno cambiando i paradigmi della cyber security, spingendo sempre di più le aziende verso l'adozione di soluzioni di sicurezza zero trust. Ecco di cosa si tratta e gli strumenti per raggiungere l'obiettivo. La regola del "verificare sempre, non fidarsi mai" su cui si basa la sicurezza zero trust è tornata prepotentemente di attualità in epoca smart working: la pandemia ha infatti profondamente modificato l'ambiente di lavoro e di conseguenza stanno cambiando anche i paradigmi della cyber security. L'everywhere workplace ha infatti letteralmente distrutto i tradizionali perimetri di difesa rovesciando il concetto di network aziendale, che non è più statico e "chiuso" all'interno delle mura aziendali, ma ovunque. In epoca smart working, i dipendenti possono accedere ad applicazioni e dati aziendali utilizzando diversi dispositivi, ovunque si trovino. A fronte di un incremento della produttività, però, l'aumento degli endpoint connessi al network aziendale ha contribuito ad ampliare notevolmente la superficie di attacco aziendale. A questo si aggiunge anche la scarsa consapevolezza dei pericoli e delle minacce cyber da parte dei dipendenti stessi.
Di conseguenza, l'approccio tradizionale alla sicurezza ICT focalizzato sull'impedire a eventuali attaccanti e minacce di entrare nel perimetro aziendale, presupponendo che tutti gli utenti che si trovano all'interno siano affidabili, è di fatto superato. Ora che la maggior parte delle organizzazioni lavora nel cloud e il cyber crimine organizzato riesce ad aggirare facilmente i classici antivirus, ora che le cyber minacce come i ransomware diventano sempre più sofisticate e invisibili, è evidente che un approccio centralizzato basato sulla fiducia è ormai divenuto obsoleto.
Indice degli argomenti

(continua)
https://www.cybersecurity360.it/soluzioni-aziendali/sicurezza-zero-trust-in-epoca-smart-working-verificare-sempre-non-fidarsi-mai/
Cybersecurity360.it *- Paolo Tarsitano – 1 giugno 2021*

Smart factory, l'evoluzione della fabbrica 4.0 - Il processo di evoluzione verso la Smart factory è partito dalla creazione di singole aree di lavoro dove implementare casi di utilizzo isolati. Ora è necessario scalare la sperimentazione all'intero ciclo produttivo, minimizzando l'intervento umano attraverso sistemi cyber-fisici e network di intelligenza artificiale. La Smart factory genera un mercato che a livello mondiale crescerà fino a raggiungere i 1.500 miliardi di dollari nel 2024. Nelle sole piattaforme di produzione intelligenti ha raggiunto 4,4 miliardi di dollari nel 2020 con una crescita previsionale costante nei prossimi 5 anni. Cina, Germania e Giappone sono i primi tre paesi in termini di adozione delle Smart factory, seguiti a stretto giro da Corea del Sud, Stati Uniti e Francia. L'Italia rientra nella "top 10" a livello mondiale per quanto riguarda molte delle tecnologie al servizio dell'Industry 4.0, come la robotica, la comunicazione macchina-macchina e l'utilizzo di tecnologie cloud. Tutto ciò è supportato dal Nuovo Piano Nazionale Transizione 4.0 del MISE, che comprende incentivi e stimoli finalizzati all'investimento in hardware e software per l'innovazione e la trasformazione digitale. Ad esempio, crediti di imposta per investimenti in beni strumentali, quelli per ricerca, sviluppo, innovazione e design e quelli finalizzati alla formazione 4.0. Il processo di evoluzione verso la Smart factory è partito dalla creazione di singole aree di lavoro dove implementare casi di utilizzo isolati. Il passo ora necessario è scalare la sperimentazione all'intero ciclo produttivo minimizzando l'intervento umano attraverso sistemi cyber-fisici e network di intelligenza artificiale. In futuro la Smart factory abbraccerà una visione ancora più ampia che, partendo dagli imperativi strategici aziendali, si estenderà dalla produzione a tutte le attività aziendali fino raggiungere i principali attori della catena del valore creando un vero e proprio ecosistema tra gli stabilimenti e le aziende partner, legate da una piattaforma di interscambio condivisa.

Indice degli argomenti

(continua)

https://www.industry4business.it/smart-manufacturing/smart-factory-levoluzione-della-fabbrica-4-0/

Industry4business - *Claudio Brusatori – 3 giugno 2021*

Lezioni dalla pandemia: dal disaster recovery alla resilienza - Oggi chi ha potere decisionale ha il compito non facile di spostarsi da un approccio tattico alla business continuity verso una strategia a lungo termine, focalizzata sui valori della resilienza e dell'agilità. Una vera resiliency aziendale si basa su una cultura impegnata a offrire a tutto il personale una varietà di mezzi tecnologici, organizzativi e sociali

In ogni crisi esiste un'opportunità per imparare e per crescere. Con l'epidemia di COVID-19 molte aziende hanno capito che alle loro strategie mancava una parte importante: se da un lato, infatti, tutte avevano dei piani di business continuity, molte avevano considerato la business continuity soltanto in termini di disaster-recovery, pensando cioè a un singolo evento, non a situazioni di lungo corso come accade invece con una pandemia. Ma la business continuity è qualcosa di più rispetto al semplice disaster recovery, è la capacità di mantenere la normale operatività senza entrare in una modalità emergenziale. Oggi sappiamo di dover fare ancora un passo avanti: il nostro prossimo obiettivo è la resilienza.

Indice degli argomenti
Scalare in modo agile: alle fondamenta di un'azienda resiliente
Oltre gli aspetti tecnici: per una forza lavoro motivata e resiliente
Scalare in modo agile: alle fondamenta di un'azienda resiliente
(continua)
https://www.industry4business.it/esperti-e-analisti/lezioni-dalla-pandemia-dal-disaster-recovery-alla-resilienza/
Industry4business *- Mario Derba - 3 giugno 2021*

Colonial Pipeline, se è l'infrastruttura IT (non l'OT) il problema per la sicurezza: la lezione
Come ci insegna anche il recente caso Colonial Pipeline, nella stragrande maggioranza degli attacchi informatici la parte del sistema più vulnerabile non è l'infrastruttura di Operational Technology ma la buona vecchia Information Technology. Ecco perché
L'attacco informatico a Colonial Pipeline negli Stati Uniti è arrivato sui giornali, andando quindi ben oltre un pubblico di esperti, anche per gli effetti concreti che tale attacco ha prodotto. Ma non è il primo, e non è un punto di svolta epocale dal punto di vista della metodologia dell'attacco (lo è per le conseguenze e per le reazioni). Occorre dunque fare un po' di chiarezza.
Indice degli argomenti
Perché la sicurezza dell'infrastruttura OT è cruciale per le aziende
I problemi (gravi) sul "versante" IT
Le "connessioni" tra rete operativa e rete informatica gestionale
Conclusioni
(continua).
https://www.agendadigitale.eu/sicurezza/colonial-pipeline-se-e-linfrastruttura-it-non-lot-il-problema-per-la-sicurezza-la-lezione/
Agenda Digitale - *Alberto Berretti - 4 Giu 2021*

Russia behind a massive spear-phishing campaign that hit Ukraine
Ukraine warned of a "massive" spear-phishing campaign carried out by Russia-linked threat actors against its government and private businesses**.** Three Ukrainian cybersecurity agencies (Ukrainian Secret Service, Ukrainian Cyber Police, and CERT Ukraine), including the Ukrainian Secret Service, warned last week of a "massive" spear-phishing campaign conducted by Russia-linked hackers against its government and organizations in the private industry. This is the third massive spear-phishing campaign that the Ukrainian government attributed to Russia-linked threat actors this year. The phishing messages employed in the operation pose as representatives for the Kyiv Patrol Police Department and warn recipients of problems with the payment of local taxes.
"Specialists of the Security Service of Ukraine established that in early June this year, mass e-mails were sent with the sender's address changed. Messages, in particular, allegedly from the Kyiv Patrol Police Department contained malicious attachments and were sent to the addresses of a number of government agencies." reads the alert published by the Ukrainian Secret Service. According to the national CERT, the attackers send messages on behalf of government agencies that use the following statement in their subject: "You didn't pay taxes. Details in the file… »,« a criminal case has been filed against you. Details in the application… »

The messages use a RAR archive as an attachment and trick victims into opening it. Upon downloading and opening the archive, an EXE file with a double extension, filename.**pdf.exe**, is dropped on the system.
When the recipient runs the files will install a modified version of RemoteUtilities, a remote administration software. The software connects to command and control servers located in Russia, Germany, and the Netherlands.
The Ukrainian Security Service shared indicators of compromise for this attack on the platform "MISP-UA".
Below the recommendations by the CERT: *(continua)*
https://securityaffairs.co/wordpress/118675/apt/ukraine-hit-russia-spear-phishing.html
Security Affairs *– Pierluigi Paganini - June 7, 2021*

Agenzia per la cyber security, una svolta per l'Italia digitale: ma ora lavorare sulle competenze
Il decreto-legge sull'Agenzia sulla cybersicurezza, insieme all'uscita in GU del decreto attuativo del perimetro di sicurezza nazionale cibernetica accendono una luce importante sulle prospettive di sicurezza e digitalizzazione del Paese. I temi sul tavolo e il nodo delle competenze
Il puzzle tridimensionale della cyber security italiana sta ormai prendendo forma. Il decreto legge sull'Agenzia sulla cyber sicurezza, formulata con velocità e perizia dopo neanche due mesi dalla dichiarazione dell'Autorità delegata, ha acceso una luce sulle aspettative della comunità che si occupa di sicurezza cibernetica in Italia.
Si veda anche in Gazzetta Ufficiale il decreto sull'Agenzia.
L'Agenzia potrà agire con elasticità, contando su professionalità di alto livello che affrontino la sfida con motivazione e coinvolgimento e su due organismi, il Nucleo e il Comitato Interministeriale, di livello decisionale elevato e con responsabilità chiare.
Quasi contemporaneamente al decreto lege, quasi a essere di buon auspicio, esce in Gazzetta Ufficiale, praticamente invariato rispetto alle ultime bozze circolate, il dpcm 81/2021, decreto attuativo del perimetro di sicurezza nazionale cibernetica, contenente, fra le altre cose, i requisiti minimi di sicurezza per i servizi fondamentali interni al perimetro stesso.
Indice degli argomenti
Agenzia per la cybersecurity, perché è un Dpcm fondamentale
Manca l'organismo per le certificazioni di prodotto
I temi aperti per l'Agenzia
Il nodo delle competenze
Il testo del decreto legge sull'Agenzia cybersecurity in Gazzetta Ufficiale
(continua)
https://www.agendadigitale.eu/sicurezza/agenzia-per-la-cyber-security-una-svolta-per-litalia-digitale-ma-ora-lavorare-sulle-competenze/
Agenda Digitale – *Luisa Franchina, Presidente AIIC - 14 Giu 2021*

NIST Releases Draft of Ransomware Risk Management Framework NIST released a draft of its Cybersecurity Framework Profile for Ransomware Risk Management which aims to help organizations prevent and respond to ransomware attacks.
A preliminary draft the National Institute of Standards and Technology (NIST) released its "Cybersecurity Framework Profile for Ransomware Risk Management," which aims to assist organizations in preventing, responding to, recovering from, and managing risk of ransomware attacks.

The draft is open for comments through July 9th and will have at least one more comment period before it is officially published. The Ransomware Profile contains detailed steps an organization can take to reduce risk levels and prevent ransomware attacks.
NIST identifies some essential first steps to ensuring cybersecurity: using antivirus software, allowing only authorized apps, keeping computers patched, blocking access to known ransomware sites, and restricting personal devices on work networks.
In addition, NIST recommends that organizations take preventative measures so they are prepared in the event of a ransomware attack, including backing up data and making an incident recovery plan.
All recommendations outlined in the framework profile are meant to be used in conjunction with the NIST Cybersecurity Framework and NIST's other specific resources that provide guidance on patching software, improving telework device security, and more.
The detailed Ransomware Profile is split into five categories, informed by the Cybersecurity Framework: identify, protect, detect, respond, and recover. Each category of the profile also contains subcategories with more specialized references that organizations can consult, along with a ransomware application section that explains how each subcategory can help to prevent and respond to ransomware attacks. *(continua)*
https://healthitsecurity.com/news/nist-releases-draft-of-ransomware-risk-management-framework
Healthitsecurity *- Jill McKeon - June,17,2021*

North Korea-linked APT group Kimsuky allegedly breached South Korea's atomic research agency KAERI by exploiting a VPN vulnerability. South Korean representatives declared on Friday that North Korea-linked APT group Kimsuky is believed to have breached the internal network of the South Korean Atomic Energy Research Institute (KAERI). The Korea Atomic Energy Research Institute (KAERI) in Daejeon, South Korea was established in 1959 as the sole professional research-oriented institute for nuclear power in South Korea. The security breach took place on May 14, and the institute discovered it only on May 31, then the research institute reported the incident to the government and launched an investigation.
The investigation into the intrusion revealed the involvement of 13 internet addresses including one traced to the Kimsuky APt group.
"The breach of the Korea Atomic Energy Research Institute (KAERI) took place on May 14 involving 13 internet addresses including one traced to Kimsuky, said Ha Tae-keung, a member of the parliamentary intelligence committee, citing an analysis by Seoul-based cybersecurity firm IssueMakersLab." reported the Reuters.
"The incident could pose serious security risks if any core information was leaked to North Korea, as KAERI is the country's largest think tank studying nuclear technology including reactors and fuel rods," Ha Tae-keung said in a statement.
A KAERI spokesperson revealed that threat actors exploited a vulnerability in a virtual private network (VPN) server to gain access to the network of the institute.
"The Korea Atomic Energy Research Institute checked the history of access to some systems by unknown outsiders through the VPN system vulnerability. In accordance with this, the attacker IP is blocked and the VPN system security update is applied." reads a statement published by the agency. Currently, the Atomic Energy Research Institute is investigating the subject of the hacking and the amount of damage, etc. ○ The statement that "there was no hacking incident" was a mistake in the response of the working-level staff, which occurred in a situation where damage was not confirmed during investigation due to suspected infringement."
The South Korean authorities did not reveal which VPN vendor was targeted by the threat actors.

"The name of the VPN server vendor was redacted in documents presented to South Korean press today at a KAERI press conference." reported The Record. (continua)
https://securityaffairs.co/wordpress/119147/apt/kimsuky-apt-hacked-south-korea-kaeri.html
***Security Affairs** – Pierluigi Paganini - June 19, 2021*

Should making a ransomware payment be illegal? It's complicated. Should ransomware payments be illegal? Policymakers and security professionals have found themselves wrestling with that question after a spree of high-profile ransomware attacks gave criminals multi-million-dollar paydays and crippled organisations in sectors ranging from energy to healthcare. However, despite the simplicity of the question, the answer is complicated.
"Banning payment would cause some huge problems and an even bigger headache for many companies," Jake Moore, cybersecurity specialist at ESET, tells *Verdict*. "Unfortunately, there is no one size fits all for organisations." While officials in the US, UK and elsewhere have strongly advised against paying ransomware demands, governments have so far avoided introducing laws dictating how an organisation should respond.
"In general, we would discourage paying the ransom because it encourages more of these attacks, and frankly, there is no guarantee whatsoever that you are going to get your data back," said FBI director Chris Wray while testifying before a US Senate appropriations panel in June. As ransomware gangs go after increasingly larger targets and demand ever-higher payments – usually made via the cryptocurrency bitcoin – it has raised the question of whether governments should introduce legislation banning companies from making a ransomware payment.
Cybercriminal groups that use malware to hold digital files and systems hostage do so because it is highly lucrative. In June, meat processing company JBS paid $11m to its attackers to draw a line under the hack. Bitcoin records show that prolific ransomware gang Darkside has made at least $90m since last August. And in July, the REvil ransomware syndicate demanded $70m after encrypting the systems of thousands of organisations via the Kaseya supply chain attack. *(continua)*
https://www.verdict.co.uk/ransomware-payment-illegal/
***Verdict** - Robert Scammell - 25th June 2021*

L'intelligenza artificiale per garantire la sicurezza del lavoro ovunque ci si trovi - Per mettere al sicuro tutti i tool, le app, i contenuti e i dispositivi di cui le persone hanno bisogno o che preferiscono usare, garantendo loro la libertà di scegliere il proprio stile di lavoro senza che questo rischi di compromettere i dati dell'azienda, è necessario adottare un approccio basato sull'intelligenza artificiale. I cyber criminali la usano da tempo e in modo efficace, la si può sfruttare anche per identificare tempestivamente le loro minacce in real time. Nell'era dello smart working e dell'IoT, trend entrambi affatto passeggeri, antivirus e soluzioni preconfezionate non bastano più per contrastare attacchi informatici sempre più complessi. Nell'attuale scenario di minacce estremamente sofisticate e perimetri aziendali sempre più difficili da circoscrivere e proteggere, è necessario prepararsi a dare una risposta dinamica ed efficace in termini di data protection non facendosi sovrastare dai cyber criminali ma sfruttando, come loro, tecnologie all'avanguardia basate sull'intelligenza artificiale.
Indice degli argomenti

Nuove vulnerabilità richiedono una nuova consapevolezza: l'AI può aiutare

(continua)
https://www.zerounoweb.it/techtarget/searchsecurity/lintelligenza-artificiale-per-garantire-la-sicurezza-del-lavoro-ovunque-ci-si-trovi/
***ZeroUnoWeb** - Marta Abba' - 30 Giu 2021*

UK, US agencies warn of large-scale brute-force attacks carried out by Russian APT. US and UK cybersecurity agencies published a joint alert about a series of large-scale brute-force conducted by the Russia-linked APT28 group. The joint alert was published by the US National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC). The attacks took place between mid-2019 and early 2021, the Russia-linked threat actor used a Kubernetes cluster to conduct anonymized brute force access against hundreds of government organizations and businesses worldwide, including think tanks, defense contractors, energy firms.
The attackers remained under the radar by routing brute force attacks through the TOR network and commercial VPN services, including CactusVPN, IPVanish, NordVPN, ProtonVPN, Surfshark, and WorldVPN. Authentication attempts that did not use TOR or a VPN service were also occasionally delivered directly to targets from nodes in the Kubernetes cluster.
The government experts attribute the attacks to Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165.
""Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments" details how the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) has targeted hundreds of U.S. and foreign organizations using brute force access to penetrate government and private sector victim networks." reads the advisory published by the NSA.
The advisory provided details about the tactics, techniques, and procedures (TTPs) associated with GTsSS.
The APT group mainly targeted organizations using Microsoft Office 365 cloud services, along with targets using other service providers and on-premises email servers. Experts speculate the activity is still ongoing. *(continua)*
https://securityaffairs.co/wordpress/119595/apt/russia-apt-brute-force-attacks.html
***Security Affairs** – Pierluigi Paganini - July 1, 2021*

Gallerie: metodi e tecniche innovative per la progettazione e la sicurezza dei tunnel - L'innovazione tecnologica assume un ruolo fondamentale nella progettazione e manutenzione delle gallerie.
Grazie all'uso di avanzati software, strumenti digitali, robot e tecnologie di scansione 3D oggi è possibile sia ottimizzare l'intero processo costruttivo di un'opera in sotterraneo sia migliorarne la sicurezza, con attività di monitoraggio costante e ispezioni automatizzate.
Per fare il punto sulle principali tecniche e soluzioni oggi disponibili, Ingenio ha intervistato Silvia Gioja, ingegnere edile, architetto e BIM Manager di Arcadis Belgio.
Lo scorso maggio, l'Ing. Gioja è stata la prima donna italiana insignita del titolo di Best Woman in Tunneling & Underground Construction, nonché la prima a vincere un premio WICE per Arcadis Belgio, dove lavora come ingegnere specializzato in infrastrutture e dove è impegnata, insieme al governo fiammingo, nel rinnovo di 20 tunnel. (continua)

https://www.ingenio-web.it/31288-gallerie-metodi-e-tecniche-innovative-per-la-progettazione-e-la-sicurezza-dei-tunnel
Ingenio *- Samorì Chiara, Gioja Silvia - 01/07/2021*

Cybercrime, i dati del 92% degli utenti LinkedIn sono in vendita sul dark web

I dati del 92% degli utenti LinkedIn sono in vendita sul dark web. Un hacker ha rubato le informazioni di 700 milioni di profili sui 756 milioni totali. Sembra che il data breach sia avvenuto grazie alle API

Le informazioni del 92% degli utenti LinkedIn sono state compromesse e sono in vendita sul dark web. Lo denunciano gli esperti di cybersecurity di E Hacking News, secondo cui i dati sarebbero riferiti a oltre 700 milioni di profili sui 756 milioni totali. Sembra che un hacker sia, infatti, entrato in possesso di un nuovo dataset che contiene i numeri di telefono, gli indirizzi, la geo-localizzazione e i salari. Peraltro, secondo diversi ricercatori, i dati sono autentici e aggiornati a un periodo tra il 2020 e il 2021. La stessa piattaforma ad aprile aveva riportato di aver subito un data breach che impattava 500 milioni di utenti, con le loro informazioni personali esposte online. Il criminal hacker, contattato da 9to5Google, ha affermato di aver ottenuto il data set sfruttando l'API di LinkedIn per raccogliere ciò che gli utenti caricavano sul sito.

https://www.difesaesicurezza.com/cyber/cybercrime-i-dati-del-92-degli-utenti-linkedin-sono-in-vendita-sul-dark-web/
Difesa e Sicurezza *- Francesco Bussoletti* ***-*** *1° luglio 2021*

Cybercrime, la PA in Italia attaccata da 16 campagne la scorsa settimana

La PA in Italia attaccata da 16 campagne la scorsa settimana. Usati i malware Formbook, AgentTesla, Ursnif/Gozi, Rastaf, Lokibot e Raccon. Il phishing punta le banche

Sono 16 le campagne del cybercrime che hanno preso di mira la Pubblica Amministrazione in Italia la scorsa settimana. Tre erano generiche e 13, invece, dirette espressamente contro il nostro paese. Le hanno rilevate gli esperti di cybersecurity del CERT-AgID. Nello specifico sono state osservate sei famiglie di malware:

- FormBook – due campagne veicolate via email di cui una italiana ed una. Il tema utilizzato è "Ordine" in entrambi i casi e gli allegati di tipo ISO e ZIP;
- AgentTesla – due campagne rispettivamente a tema "Delivery" e "Pagamenti". Gli allegati sono di tipo GZ e ZIP;
- Ursnif/Gozi – campagna a tema "Delivery" che sfrutta ancora una volta il brand BRT ed allegati XLSM;
- Rastaf – campagna a tema "Documenti" veicolata verso indirizzi PEC della pubblica amministrazione tramite email PEC contenente un link al download di un documento RTF;
- Lokibot – campagna italiana a tema "Premi" e allegati di tipo GZ;
- Raccoon – campagna generica veicolata tramite email a tema "Pagamenti" e allegati XLSX.

Per il phishing, invece, il tema principale è stato quello "Banking", che ha coinvolto quattro brand: Intesa Sanpaolo (tornato ad essere il brand più sfruttato), Poste Italiane, ING e Unicredit.

https://www.difesaesicurezza.com/cyber/cybercrime-la-pa-in-italia-attaccata-da-16-campagne-la-scorsa-settimana/
Difesa e Sicurezza *- Francesco Bussoletti* ***-*** *5 luglio 2021*

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

Come tutti gli anni, la 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.

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 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.