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. 5/ 2021** | **Maggio 2021**

La sicurezza spaziale e la protezione cibernetica

Le componenti di terra dei sistemi spaziali sono diventate il principale obiettivo degli attacchi cibernetici. Le minacce agli impianti e alle reti di comunicazione, in particolare cibernetiche, sono diventate un serio pericolo per la sicurezza pubblica.
La resilienza dei sistemi di comunicazione è basilare per la sicurezza complessiva delle infrastrutture critiche. Molteplici settori ormai si avvalgono di tali sistemi, ad iniziare dalle telecomunicazioni ed ai servizi meteorologici. Non è chiaro, però, se gli attuali sistemi di protezione e di resilienza nell'ambito dell'Unione Europea sono **adeguati ed in grado di contrastare le minacce fisiche, ma soprattutto informatiche.**
Proprio per cercare di affrontare in modo reale ed efficiente le questioni relative alla cybersecurity delle applicazioni spaziali, la Commissione Europea nell'ambito del programma **Horizon 2020** ha lanciato il progetto **7SHIELD** (Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats), per arrivare alla definizione di un quadro esaustivo delle minacce informatiche e fisiche alla resilienza dei segmenti terrestri dei sistemi spaziali europei. Il meccanismo di allerta precoce ipotizza preventivamente il livello di rischio in caso di un attacco informatico o fisico. Un piano di mitigazione viene progettato e aggiornato automaticamente per poter reagire tempestivamente ad un attacco o ad una avaria del sistema. La sicurezza e la resilienza delle installazioni private dei segmenti terrestri spaziali sono inoltre indirizzate a scenari di continuità operativa[1].
A tal fine saranno costruiti scenari di continuità operativa che permetteranno l'implementazione di servizi innovativi per la protezione dei segmenti di terra. Sarà, quindi, innalzata la protezione di questi sistemi, integrando le **protezioni già esistenti nelle installazioni a livello nazionale e sovranazionale**. Il quadro risultante perfezionerà tecnologie innovatrici indirizzate all'integrazione, all'elaborazione e all'analisi dei dati, ai sistemi di machine learning, alla protezione dalle minacce informatiche e al rilevamento di attacchi informatici[2].
Il progetto 7SHIELD prevede anche un coordinamento con l'Agenzia europea per la difesa (EDA) attraverso la realizzazione di sinergie con i progetti **PYTHIA** (**Predictive methodologY for TecHnology Intelligence Analysis**) e **SOLOMON** (**Strategy-Oriented anaLysis Of the Market fOrces in EU defeNce**), finanziati nell'ambito della *Preparatory Action for Defence Research (PADR)*.
Tramite **PYTHIA** è stata sviluppata una metodologia innovativa per la realizzazione di **previsioni tecnologiche strategiche nel campo della difesa** al fine di individuare le future sfide che emergeranno nel settore della ricerca nei prossimi anni.
SOLOMON intende, invece, **fornire all'Unione europea metodologie e strumenti necessari a garantire che le industrie operanti nel settore della difesa possano contare su un approvvigionamento affidabile**.

[1] https://www.7shield.eu/project/
[2] Luigi Romano "*Cybersecurity, è lo spazio la nuova frontiera: l'Europa schiera 7Shield*", Agenda Digitale, 02 novembre 2020.

In sintesi, l'obiettivo sarà l'attuazione di un **risk-mitigation plan,** a supporto della sicurezza e della resilienza delle installazioni private di segmenti spaziali terrestri, con **scenari di continuità operativa basati sulle più recenti tecnologie di monitoraggio e di previsione**.

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 al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

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

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da inserire, per esempio, in newsletter o nel sito AIIC.
In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIIC: in tal caso – però – la partecipazione di AIIC ad un evento deve

essere decisa dal Consiglio Direttivo, pertanto siete pregati di contattare il CD con ragionevole anticipo, alla mail segreteria@infrastrutturecritiche.it
In caso non fosse possibile la partecipazione a nome AIIC, vi invitiamo ad indicare, nel profilo professionale, la vostra appartenenza ad AIIC.

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

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi ed autonomi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza
- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo)

è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

ATTIVITA' DELL'ASSOCIAZIONE

NUOVO GRUPPO DI LAVORO AIIC
Principi e Tecnologie per la Protezione di Spazi Pubblici

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

Il GdL sarà coordinato dal consigliere Sandro Bologna.

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

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

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

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

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

Industrial Control System (ICS) e sicurezza: 6 cose da sapere - Gli attacchi informatici mirati ai sistemi industriali smartificati spingono fornitori, sviluppatori e produttori a incorporare processi di sicurezza ICS prima, durante e dopo lo sviluppo.
Industrial Control System (ICS) sempre più intelligenti ma anche potenzialmente più vulnerabili. La fusione della Industrial IoT e i sistemi di controllo industriale hanno aperto il fianco alle minacce del cybercrime. I team devono affrontare molte sfide per integrare la sicurezza a livello di processo e di prodotto.
Indice degli argomenti
Quali sono gli attacchi agli Industrial Control System
ICS connessi e comunicanti: come proteggerli?
Sei processi per la sicurezza degli ICS
Comprendere la cyber kill chain
Pianificare la difesa in profondità
Implementare la gestione del ciclo di vita del dispositivo
Secure Software Development Lifecycle: che cos'è e a cosa serve
Modellazione delle minacce
https://www.zerounoweb.it/techtarget/searchsecurity/industrial-control-system-ics-e-sicurezza-6-cose-da-sapere/
Zerounoweb *- Laura Zanotti, 25 Marzo 2021*

IoT e wearable device per il welfare e la sicurezza dei lavoratori
L'IoT e i dispositivi indossabili sono sempre più presenti nell'ambito professionale, per monitorare i rischi derivanti da un'attività lavorativa continua, identificare possibili eventi avversi e migliorare la salute e sicurezza sul posto di lavoro. L'adozione di queste tecnologie apre importanti prospettive per offrire alle persone non soltanto un ambiente lavorativo sicuro ma anche uno stile di vita più sano.
Indice degli argomenti
RFID, dispositivi di protezione individuale e richieste del mercato
Come funzionano i DPI con tecnologia RFID
I dispositivi indossabili per la sicurezza dei lavoratori
L'utilizzo dei dispositivi indossabili
https://www.internet4things.it/edge-computing/iot/iot-e-wearable-device-per-il-welfare-e-la-sicurezza-dei-lavoratori/
Internet4things *- Luca Del Col Balletto, Giuseppe Andreoni – 1 aprile 2021*

Smart car security: rischi cyber e contromisure per viaggiare sicuri nelle auto intelligenti - Con la sempre maggiore diffusione delle smart car, anche la cyber security delle auto si è evoluta di pari passo con gli standard del settore automotive per adeguarsi ai possibili rischi legati alla sicurezza informatica. Ecco quali sono le misure di sicurezza e le necessarie contromisure da adottare.

https://www.cybersecurity360.it/nuove-minacce/smart-car-security-rischi-cyber-e-contromisure-per-viaggiare-sicuri-nelle-auto-intelligenti/
Cybersecurity360 *- Elisa Di Conza, Alessio Pennasilico - P4I - 6 Apr 2021*

Internet of Things: 93 milioni di oggetti connessi in Italia, un mercato da 6 miliardi di euro
I dati dell'Osservatorio Internet of Things del Politecnico di Milano evidenziano un mercato in lieve flessione rispetto all'anno precedente a causa della crisi pandemica e della sopraggiunta maturità di alcuni segmenti. Crescono, e di molto, i servizi: il mercato IoT è pronto a mostrare il proprio valore
Un anno di sostanziale tenuta, chiuso con una lieve flessione (-3%) rispetto al 2019.
Così potremmo sintetizzare il 2020 del mercato Internet of Things, così come raccontato dall'Osservatorio del Politecnico di Milano.
Attenzione, però.
Quella che potrebbe sembrare una brusca frenata, rispetto a un trend che aveva visto il comparto crescere del 24% anno su anno nel 2019 e del 35% l'anno precedente, non solo è perfettamente in linea con quanto accaduto sugli altri mercati internazionali, non solo è comunque la rappresentazione di un mercato che vale 6 miliardi di euro, ma, soprattutto, "è figlia di tante dinamiche, tra le quali deve essere sottolineata la crescita dei servizi, che mettono a segno un +40% complessivo", come spiega Angela Tumino, Direttore dell'Osservatorio, che quest'anno giunge alla sua decima edizione. "L'evidenza è che l'attenzione non è più sulla sola evoluzione tecnologica, ma sulla capacità di mettere a terra il valore che questo comparto ha in sé. Grazie agli oggetti connessi si fa innovazione e si crea valore".
Indice degli argomenti
Non solo COVID: la flessione arriva nei comparti più maturi
Il mercato in Italia: bene smart agriculture, smart car, smart city
È il momento di misurare i benefici dell'Internet of Things
Le tecnologie per l'Internet of Things: e se Internet diventasse "trasparente"?
Un nuovo tavolo di lavoro: la smart city
Industrial IoT: l'open source facilita le PMI
https://www.internet4things.it/smart-city/internet-of-things-93-milioni-di-oggetti-connessi-in-italia-un-mercato-da-6-miliardi-di-euro/
Internet4things *- Maria Teresa Della Mura - 12 Aprile 2021*

Sicurezza negli studi professionali: nuovo protocollo anti Covid-19 e vademecum RPT - La sintesi fornisce ai professionisti le principali raccomandazioni contenute nell'ultimo "Protocollo condiviso di aggiornamento delle misure per il contrasto e il contenimento della diffusione del virus SARS-CoV-2/COVID-19 negli ambienti di lavoro"
La Rete delle Professioni Tecniche fornisce ai professionisti e loro studi professionali, in modo sintetico, le principali raccomandazioni contenute nei protocolli aggiornati per il Covid-19 e le prime indicazioni per le loro applicazioni negli studi professionali e nelle attività presso cui operano i professionisti nell'ambito della sicurezza sul lavoro.
Sulla base degli aggiornamenti dei Protocolli di Aprile 2021, la RPT ritiene infatti utile che i professionisti valutino nei propri contesti lavorativi l'aggiornamento delle procedure e\o protocolli e\o valutazioni adottate.
Il nuovo protocollo Covid-19 per la sicurezza sul lavoro
Il Protocollo aggiorna le misure generali applicabili a tutte le realtà lavorative rimandando in dettaglio, al fine della prevenzione di ogni forma di affollamento e di situazioni a rischio di contagio, ai protocolli di settore per le attività di cui all'Allegato IX al DPCM 2 marzo 2021, che restano dunque sostanzialmente invariati.

Si evidenzia, nello specifico, che:
le norme del protocollo si estendono alle aziende in appalto che possono organizzare sedi e cantieri permanenti e provvisori all'interno dei siti e delle aree produttive;
a livello organizzativo, il protocollo conferma la possibilità di utilizzare il lavoro agile e da remoto, ricorrere all'utilizzo di ammortizzatori sociali, la rimodulazione di orari, livelli produttivi e spazi di lavoro;
relativamente agli spazi di lavoro è fatta salva la possibilità di individuare soluzioni innovative come, ad esempio, il riposizionamento delle postazioni di lavoro adeguatamente distanziate tra loro, l'utilizzo - per un periodo transitorio - anche di spazi generalmente non adibiti ad ufficio quali sali riunioni, etc.
In quest'ottica il ruolo del professionista quale consulente per la sicurezza o RSPP è sicuramente fondamentale in quanto in grado di dare un contributo fattivo nella rimodulazione e riorganizzazione di spazi ed operatività che tengano conto non solo del protocollo ma anche dei rischi per la salute e la sicurezza sul lavoro.
Il protocollo tratta i seguenti punti:
informazione;
modalità di ingresso in azienda/ufficio;
modalità di accesso dei fornitori esterni;
pulizia e sanificazione;
precauzioni igieniche personali;
dispositivi di protezione individuale;
gestione degli spazi comuni (mensa, spogliatoi, aree fumatori, distributori di bevande e/o snack);
organizzazione aziendale (turnazione, trasferte, lavoro agile)
gestione entrata e uscita dei dipendenti;
spostamenti interni, riunioni, eventi interni, formazione;
gestione di una persona sintomatica;
sorveglianza sanitaria/medico competente/RLS;
aggiornamento protocollo di regolamentazione.
https://www.ingenio-web.it/30469-sicurezza-negli-studi-professionali-nuovo-protocollo-anti-covid-19-e-vademecum-rpt
Ingenio – *Peppucci Matteo - Collaboratore INGENIO 21 aprile 2021*

Gestione impianti industriali: l'IoT al servizio di sicurezza e business continuity - Tra le frasi più celebri pronunciate da Albert Einstein ce n'è una che oggi riguarda tutti un po' più da vicino: "Un giorno le macchine riusciranno a risolvere tutti i problemi, ma mai nessuna di esse potrà porne uno".
La riflessione del grande scienziato sulle macchine e dunque, nell'accezione moderna, sulla tecnologia si è rivelata corretta nel tempo. Oggi è più che mai attuale. L'intero comparto manifatturiero italiano, fiaccato dalla pandemia di Covid-19, trova nella tecnologia il suo più grande alleato, per resistere e per rinascere.
Indice degli argomenti
Lavorare sulla resilienza grazie all'uso della tecnologia
Un paradigma nuovo per gli impianti industriali
La chiave è nei sensori intelligenti
Smart sensor e IIoT come risposta alla domanda di sicurezza e business continuity
L'importanza di un partner specializzato
https://www.internet4things.it/smart-manufacturing/gestione-impianti-industriali-liot-al-servizio-di-sicurezza-e-business-continuity/
Internet4things *- Paola Mangiapane, 23 Aprile 2021*

An alleged ransomware attack hit the Italian Banca di Credito Cooperativo causing chaos. Banca di Credito Cooperativo (BCC), one of the largest Italian cooperative credit banks was hit by a ransomware attack. Banca di Credito Cooperativo (BCC), one of the largest Italian cooperative credit banks, was hit by a cyberattack allegedly carried out by one of the most aggressive ransomware gangs, Darkside. The attack paralyzed the operations at 188 branches causing serious problems to the customers of the bank as reported by the Italian newspaper La Repubblica. The Italian newspaper also shared an image of a ransom note that was dropped on the computers of the bank, the attackers claim to be the DarkSide ransomware gang.
The bank attempted to downplay the problem reporting that the root cause of the issue was related to technical issues at the communication systems. The statement published by the bank invites the customers to use the ATMs or the Home Banking service, which according to the bank were not impacted."We inform our customers that the Agencies, albeit with slowed-down operations due to line problems, are regularly open to the public."We also inform you that the technical problems that slowed down normal operations are being resolved and will be gradually restored from Monday 3 May at the latest. Please note that the ATM is active and that the Home Banking services can be used directly from a PC or smartphone, through which it is possible to carry out all information and dispositive operations.
"We inform our customers that the Agencies, albeit with slowed-down operations due to line problems, are regularly open to the public." reads the statement published by the company. "Please note that the ATM is active and that the Home Banking services can be used directly from a PC or smartphone, through which it is possible to carry out all information and dispositive operations." The bank plans to completely restore all the operations by May 3rd. At the time of this writing, the Banca di Credito Cooperativo (BCC) has yet to be included in the list of the victims of the Darkside group that is published on their leak site, likely because there is an ongoing negotiation.
https://securityaffairs.co/wordpress/117360/cyber-crime/banca-di-credito-cooperativo-darkside-ransomware.html
Security Affairs *- Pierluigi Paganini April 29, 2021*

Ransomware Task Force Publishes Framework to Fight Global Threat. An 81-page report details how ransomware has evolved, along with recommendations on how to deter attacks and disrupt its business model. The Ransomware Task Force (RTF) this week published a report detailing recommendations to fight back against the operators and infrastructure that drive ransomware, which its team of experts describes as a "serious national security threat" and "public health and safety concern." More than 60 people from software companies, security vendors, government agencies, nonprofits, and academic institutions teamed up with the Institute for Security and Technology (IST) to create the RTF, which launched last December. Participants include Microsoft, McAfee, Rapid7, Amazon, Cisco, the Cyber Threat Alliance, the Global Cyber Alliance, US Department of Justice, Europol, and the UK's National Crime Agency, among many others. In their 81-page report, "A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," experts share proposed guidance to deter ransomware attacks, disrupt its business model, help organizations prepare, and better respond to the global threat. While other threats, such as business email compromise, also cause tremendous losses for businesses each year, RTF is focusing on ransomware because of its massive impact. "One of the concerns we have is the scope and scale of ransomware," says Megan Stifel, executive director for the Americas at the Global Cyber Alliance and co-chair of the RTF. "It's holding parts of the ecosystem and the economy at risk, particularly aspects of critical

infrastructure, that can give rise to a range of cascading consequences that in some cases individually, or certainly collectively, can create a significant national security problem." RTF's framework arrives as ransomware attackers continue to evolve their strategies. Ransomware targeted the healthcare industry during a global pandemic and has shut down schools, hospitals, police stations, city governments, and US military facilities, its report points out. "The professionalism of the affiliates, and focusing on their ability to attack organizations, is probably the biggest challenge," says Raj Samani, fellow and chief scientist at McAfee, of fighting ransomware. "This has supported the big-game hunting strategy and ultimately the ability to get into organizations and disrupt operations or steal data, [which] has given threat actors the ability to demand a lot more than ever before." The framework outlines 48 actions government and industry leaders can take to disrupt the ransomware business model and mitigate the impact of attacks. (segue)

https://www.darkreading.com/threat-intelligence/ransomware-task-force-publishes-framework-to-fight-global-threat/d/d-id/1340889

Darkreading - *Kelly Sheridan- 4/30/2021*

La Cina si arma hi-tech. Ecco il report dell'Intelligence Usa *La Defense Intelligence Agency degli Stati Uniti ha presentato il report "Worldwide threat assessment". La Cina si conferma in cima alla lista delle sfide. Preoccupano la modernizzazione del Dragone ad ampio spettro, la crescita del suo arsenale missilistico e nucleare e la capacità di proiettarsi in scenari lontani dal Paese. La grande sfida è sull'Intelligenza artificiale*

La Cina si arma in ogni dominio militare, puntando sulle nuove tecnologie e incrementando la capacità di proiezione in aree anche molto lontane dai suoi confini. È quanto si legge nel "Worldwide threat assessment" dell'Intelligence militare degli Stati Uniti, presentato dal direttore della Dia **Scott Berrier** ai membri del Comitato Armed services del Senato. Cinquantasette pagine che certificano il passaggio a "un'era di competizione strategica", in cui Washington affronta "competitor che stanno sviluppando capacità per sfidare, limitare o superare il vantaggio militare degli Stati Uniti". In cima alla lista, dopo l'analisi dello scenario da Covid-19, c'è la Cina, che "resta un competitor strategico a lungo termine".

GLI OBIETTIVI DEL DRAGONE

L'attenzione è su tre trend: il potenziamento ad ampio spettro del Dragone; lo sviluppo di tecnologie innovative per impieghi militare; l'incremento della presenza all'estero delle forze cinesi. Si parte dall'obiettivo scritto a chiare lettere da Pechino nel 2019 all'interno del documento (pubblicato in lingua inglese) "La Difesa nazionale della Cina nella nuova era": avanzare "in modo completo nella modernizzazione" di tutti i segmenti delle Forze armate entro il 2035, così da disporre entro il 2050 di uno strumento militare "world-class". A tendere verso tale obiettivo, spiega l'intelligence militare americana, c'è la leadership targata Xi Jinping, il cui consolidamento registrato nel 2020 ha permesso addirittura di accelerare gli obiettivi strategici. Pechino cerca una modernizzazione "completa" entro il 2027, così da avere "una migliore postura per un conflitto con qualsiasi Paese che vede come una minaccia, compresi gli Stati Uniti".

LE STRATEGIE DI UNA SUPER POTENZA

Certificate le ambizioni di super potenza. L'Esercito popolare di liberazione (Pla), nota la Dia, giustifica la sua modernizzazione non solo con ragioni di sicurezza e difesa, ma anche "per promuovere la stabilità e la prosperità globali, attenuando le preoccupazioni sulle sue intenzioni e per presentare la Cina come leader globale". Eppure, "il Pla afferma chiaramente che ha bisogno di modernizzarsi per colmare le

lacune con potenze militari più forti e per scoraggiare e sottomettere le forze separatiste (principalmente Taiwan), proteggendo la sovranità e l'integrità territoriale della Cina".

LA MODERNIZZAZIONE

Con un budget da 210 miliardi di dollari per il 2021 (+6,8% rispetto al 2019), la modernizzazione copre tutti i domini operativi, con forte spinta inter-forze ed esercitazioni rilevanti volte all'integrazione delle varie componenti. Preoccupano le novità missilistiche (qui un focus sull'arsenale di Pechino): "continuano a rafforzare le capacità di attacco balistico a lungo raggio e missili anti-nave, che conferiscono la capacità di condurre attacchi di precisione nel Pacifico occidentale, nell'Oceano indiano e nel Mar Cinese Meridionale". Prosegue inoltre lo sviluppo dei missili a planata ipersonica (Hgv), con lo schieramento confermato dell'avveniristico vettore DF-17, per ora armato convenzionalmente, anche se si nota che "la Cina sta espandendo e diversificando il suo arsenale nucleare", passando da circa 200 testate a un raddoppio nel giro di un decennio. Eppure, Pechino si dimostra "refrattaria" a discutere di disarmo e di controllo degli armamenti. (segue)

https://formiche.net/2021/05/usa-cina-arma-missili/

Formiche.net- *Stefano Pioppi - 04/05/2021*

Will 2021 Mark the End of World Password Day? We might be leaving the world of mandatory asterisks and interrobangs behind for good. More than a quarter of us have used the words "password" or "qwerty" as our primary password at some point in our lives, according to Google. Even more alarming, six in 10 of us admit to using the same password across multiple online accounts, from email to online banking, and only a third of us bother to change passwords more than once a year. That's why World Password Day was created. In 2005, security expert Mark Burnett wrote a book called *Perfect Passwords*, in which he floated the idea of dedicating one day in the calendar each year when everybody should change their passwords.

By 2013, the idea had really caught on and Intel ran with it, making the first Thursday in May the official World Password Day. In 2021, World Password Day falls on May 6, but is it still relevant in its current form?

From phishing scams to distributed denial-of-service attacks, malware to spyware, the security landscape is a lot more complex than it was back in 2005, or even 2013. Most individuals today have so many different online accounts that to devise and remember a unique and complex password for each one is near impossible. It's why so many of us now rely on authenticator apps and digital "vaults" in which to store our passwords, allowing us to simply remember one to unlock them all. This kind of innovation is good; however, it also leads to a creeping realization that the humble password may no longer be fit for purpose. So, what's next?

Has the Password Outlived Its Usefulness? Bill Gates famously quipped that the password was dead back in 2004. His forecast might have been a little premature, but he was right when he said the traditional password cannot "meet the challenge" of keeping critical information secure. That's as true for businesses as it is for each and every one of you reading this article. As recently as 2018, more than 80% of all data breaches could be attributed to poor passwords. Businesses know this, which is why they're constantly encouraging employees to create ever more complex passwords, layering up password security with things like two-step and certificate-based authentication. But while these technologies might help to mitigate password vulnerability, they can't eradicate it.

Password-Strengthening Technologies Technology hasn't yet evolved to a point where we can do away with passwords altogether. Instead, we keep inventing ways of making passwords more secure, propping them up as a viable way in which to secure our data. Two-step authentication does exactly what it sounds like, requiring an additional step in the login process beyond simply entering a

password. Once a user has entered the password, that person will be sent a text message with a unique code or be asked to generate one via an authenticator app, which is needed to gain access to their account. This kind of multifactor authentication certainly offers an additional layer of security. It means that even if hackers crack your password, they aren't going to get very far without your mobile phone or access to your code generator. However, it's not entirely without flaws. (segue)
https://www.darkreading.com/vulnerabilities---threats/will-2021-mark-the-end-of-world-password-day-/a/d-id/1340911
Darkreading **-** *Jake Madders- 5/5/2021*

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:

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
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