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. 08/ 2020	Settembre 2020

Smart Working e Sicurezza

Lo Smart Working, il Lavoro Agile, è – come specificato dal Mistero del Lavoro e delle Politiche Sociali - una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'**assenza di vincoli orari o spaziali** e **un'organizzazione per fasi, cicli e obiettivi**, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività. In particolare, la sua applicazione in modo estensivo si è avuta durante il lockdown ed è stata mantenuta significativamente anche dopo.
Lo smart working – come spiegato dal Prof. Mariano Corso del Politecnico di Milano - *è **un modello di organizzazione del lavoro che si basa sulla maggiore autonomia del lavoratore** che, sfruttando appieno le opportunità della tecnologia, ridefinisce orari, luoghi e in parte strumenti della propria professione. È un concetto articolato, che si basa su un pensiero critico che restituisce al lavoratore l'autonomia in cambio di una responsabilizzazione sui risultati*.
Lo Smart Working, oltre a dare maggior flessibilità al lavoro dipendente, offre maggior attenzione all'ambiente. Permette di evitare, ad esempio, l'abbandono di particolari territori e di limitare gli spostamenti con conseguente riduzione delle emissioni di CO2. *È una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato* – ha evidenziato sempre il Ministero del Lavoro - *dall'**assenza di vincoli orari o spaziali** e **un'organizzazione per fasi, cicli e obiettivi**, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività*.
Lo smart working pone però rilevanti problematiche per quanto riguarda i possibili rischi per la privacy. In ossequio alle norme del **GDPR**, il datore di lavoro deve garantire la sicurezza dei dati trattati in modo da evitare rischi per i diritti delle persone fisiche. Deve rispettare il principio di ***accountability*,** ovvero adottare politiche e misure adeguate a garantire che il trattamento dei dati personali sia conforme ai dettami del GDPR.
Il rispetto della sicurezza delle connessioni è quindi fondamentale e non può essere trascutato se si lavora da remoto, ovvero in un contesto che è senz'altro meno controllato e protetto di quello di un ufficio.
Alla luce di quanto sopra esposto, e per concludere la rapida panoramica sui diversi aspetti di *privacy* e *cybersecurity* connessi al ricorso allo *smart working* per effetto dell'emergenza sanitaria legata alla diffusione del Covid-19, gli Avvocati Federica Lamoratta e Mario Valentini ci ricordano quanto essi richiedano una specifica focalizzazione, nonché **un'apposita regolamentazione da parte del Datore di lavoro**[1]. "*Al riguardo è fondamentale per il Datore di Lavoro rivedere le proprie procedure, ovvero predisporre o integrare policy o istruzioni già esistenti ai fini del compimento delle attività sui dati in regime di lavoro agile. Inoltre, è opportuno che il Titolare predisponga moduli di formazione specifici sull'argomento, affinché gli smart worker siano pienamente consapevoli delle specifiche modalità tramite cui sono chiamati a svolgere le mansioni a distanza e dei rischi riconnessi al contesto extra-aziendale*".

[1] Federica Lamoratta e Mario Valentini "*Smart working e privacy, ecco le regole per lavorare in sicurezza*" Cybersecurity360, 27 agosto 2020.

In sintesi, il Titolare deve nominare un referente *al quale si possa adire per esporre i propri dubbi o segnalare criticità in atto. Delocalizzare il posto di lavoro può significare, infatti, per il Datore di lavoro, perdere una significativa quota di controllo su quello che accade nella sua organizzazione, e per il lavoratore,* ***perdere i riferimenti tipici di un contesto fisico*** *frequentato magari per anni.*

Concludendo, sarà importante poter capire applicare dei migliorativi e, quindi, come si possano assecondare meglio le nuove necessità.

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 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.

Attività del Gruppo di lavoro

Il Gruppo di Lavoro. "**Internet of Things (IoT) in the context of Critical Infrastructures: Cybersecurity and Privacy concerns and possible solutions**" ha concluso la sua attività. Il Gdl è

stato coordinato da Sandro Bologna e ha visto la partecipazione dei soci Silvano Bari, Glauco Bertocchi, Luigi Carrozzi, Luisa Franchina, Francesco Ressa, Angelo Socal, Alberto Traballesi.
E' stato stampato il report e a breve sarà disponibile sul sito dell'Associazione.

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

AIIC ha dato il suo patrocinio per la creazione di un nuovo Master organizzato dall'Università di Roma Tre

E' quindi con piacere che informiamo dell' apertura delle iscrizioni al Master di II livello di Roma Tre "**La cybersecurity per la protezione dei sistemi di controllo nell'industria 4.0 e nelle infrastrutture critiche**" (http://industrialsecurity.it)

ROMA TRE UNIVERSITÀ DEGLI STUDI — iNGEGNERIA DIPARTIMENTO DI ECCELLENZA — accenture

SIEMENS Ingegno per la vita — Life Is On Schneider Electric — BECKHOFF — Rockwell Automation — GE Digital

ServiTecno — ISACA Rome Chapter — ANIE AUTOMAZIONE — ANIPLA A.N.I.P.L.A. ASSOCIAZIONE NAZIONALE ITALIANA PER L'AUTOMAZIONE — Ordine degli Ingegneri della Provincia di Roma — UNINDUSTRIA UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE ROMA • FROSINONE • LATINA • RIETI • VITERBO — AIIC

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

NEWS E AVVENIMENTI

Smartphone in grado di rilevare terremoti: Google annuncia una funzione per i telefoni Android - Col nuovo aggiornamento per i telefonini Android, Google pensa ad una rete su larga scala per il monitoraggio dei terremoti, che sfruttando i sensori già presenti negli smartphone possa avvisare tempestivamente gli utenti dell'arrivo del sisma. Google prevede di lanciare i primi avvisi basati sulle letture dell'accelerometro l'anno prossimo. In realtà la nuova funzione annunciata da Google riguarda la possibilità, da parte di telefoni Android, di rilevare il terremoto e di inviare tali dati ad un centro di elaborazione, che una volta esaminati potrebbe procedere ad avvisare, tramite una notifica, gli utenti dell'imminente arrivo del sisma. Si tratterebbe di alcuni secondi prima dell'arrivo del terremoto ma comunque molto importanti per mettere in salvo se stessi e i nostri cari. Nella nota di Google si legge che se il telefono rileva un possibile terremoto, invia un segnale ad un server dell'azienda che tiene conto anche della posizione approssimativa. Riguardo il funzionamento del server, Google informa che questo "analizza le informazioni di molti telefoni, per capire se effettivamente è in corso un terremoto e, nel caso, inviare le notifiche istantanee".
L'**idea** è quella di utilizzare gli **accelerometri** - sensori che misurano la direzione e la forza di movimento - già presenti sugli smartphone e che ora sono utilizzati principalmente per determinare se un utente tiene in mano un telefono in modalità orizzontale o verticale.
Il principio di funzionamento Un terremoto genera onde simiche di due tipi: onde P e onde S. Le prime sono definite "compressionali" e fanno oscillare le particelle di roccia che attraversano, in maniera parallela alla loro direzione di propagazione. Questa tipologia di onda è molto veloce, più delle Onde S, per questo sono le prime a essere avvertite.
Le Onde S vengono invece definite "trasversali", e fanno vibrare le particelle di roccia che attraversano in maniera trasversale alla loro direzione di propagazione. Queste onde sono molto più lente delle Onde P ma al tempo stesso molto più pericolose.

……
https://www.ingenio-web.it/27994-smartphone-in-grado-di-rilevare-terremoti-google-annuncia-una-funzione-per-i-telefoni-android?utm_term=38931+-+https%3A%2F%2Fwww.ingenio-web.it%2F27994-smartphone-in-grado-di-rilevare-terremoti-google-annuncia-una-funzione-per-i-telefoni-android&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3726+-+1988+%282020-08-24%29
***Ingenio** - Alessandrini Stefania - 21/08/2020*

Parlando di obsolescenza dei ponti e viadotti italiani: il punto di vista del progettista
Dopo il crollo del Polcevera si è scatenata la paura per tutte le opere coeve che sono più della metà dei ponti italiani. Nell'articolo si forniscono alcune indicazioni su cosa i progettisti fanno e possono fare.
Quando ci è stato chiesto un intervento sul tema del **degrado dei ponti** la mente è corsa a oltre venti anni di esperienze vissute e alla attualità drammatica. Nell'ultimo anno non c'è giornale che non abbia ospitato il parere dell'esperto ed è impossibile risolvere un tema sconfinato, per tipologie, problematiche e risoluzioni, come quello dell'**invecchiamento del nostro patrimonio infrastrutturale**; abbiamo scelto, allora, di elaborare piuttosto un **racconto metodologico** che fornisca semplicemente spunti di approfondimento ed organizzi le conoscenze e le esperienze secondo un percorso unitario. Chiaramente alcune semplificazioni faranno sorridere i veri esperti ma l'intenzione reale è quella di permettere una individuazione delle macrotematiche a tutti coloro che pur tecnici del settore non si occupano quotidianamente di ponti.

Cosa c'è in giro oggi, il tema del degrado L'invecchiamento dei ponti attanaglia l'intero occidente, per limitarci al mondo a noi vicino e che conosciamo meglio anche mediaticamente. È un fenomeno noto da qualche decennio sia in relazione all'incedere dell'età delle strutture sia in relazione all'incrementarsi delle conoscenze sui materiali sia, infine, perché enfatizzato dagli episodi recenti e drammatici che lo hanno sbattuto in prima pagina come un mostro, ricordando Bellocchio. Poi, a ben vedere, i quattro casi recenti più famosi italiani sono molto diversi e solo a Genova si può parlare in modo corretto di invecchiamento, molto probabilmente, ma per un'opera del tutto eccezionale sulla quale non era in ogni caso sufficiente applicare le procedure e le attività ispettive semplici proprie delle opere correnti. Infatti il cavalcavia di Lecco sulla SS36, primo di questa recente serie, è crollato a causa del transito di troppi carichi eccezionali; il cavalcavia 167 della A14 è crollato durante alcune attività di cantiere, probabilmente non corrette, e il ponte sulla tangenziale di Fossano, in fondo recente, era figlio di una tecnologia di prefabbricazione sicuramente poco conservativa e forse non correttamente applicata……..
Argomenti:
Ponti in cemento armato precompresso tipici
Le famigerate selle Gerber
Le cose strane
Tutto invecchia
Cosa sappiamo di quello che vediamo
……..
https://www.ingenio-web.it/24864-parlando-di-obsolescenza-dei-ponti-e-viadotti-italiani-il-punto-di-vista-del-progettista?utm_term=39024+-+https%3A%2F%2Fwww.ingenio-web.it%2F24864-parlando-di-obsolescenza-dei-ponti-e-viadotti-italiani-il-punto-di-vista-del-progettista&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3734+-+2065+%282020-08-27%29
Ingenio – *Bartolomei Marco - Isani Stefano, Studio MATILDI+PARTNERS, Bologna 25/08/2020*

Manutenzioni ordinarie e straordinarie delle strutture ferroviarie. Con il termine manutenzione nell'ambito ferroviario s'intende la combinazione di tutte le *azioni tecniche, amministrative e gestionali*, durante il ciclo di vita del corpo ferroviario, volte a mantenere, riportare o ricostituire tale corpo in uno stato tale da poter esercire la rete ferroviaria al miglior livello funzionale, prestazionale e di sicurezza al livello di conoscenza attuale o innovativo. Questa definizione deriva dal fatto che, nel corso degli ultimi anni, l'impostazione dell'attività di manutenzione ha subito una sostanziale trasformazione da attività prevalentemente operativa di intervento, a complesso sistema gestionale orientato alla prevenzione del guasto e al miglioramento continuo del servizio. L'obiettivo principale delle attività che rientrano nel processo di manutenzione è quello di **mantenere in efficienza l'infrastruttura ferroviaria**, assicurando i massimi standard di qualità, sicurezza e affidabilità, garantendo la compatibilità dei costi di manutenzione con il quadro dei costi di gestione aziendale.
La rete ferroviaria italiana
La rete ferroviaria italiana consta di:

- 16.200 km di linee a semplice binario, due terzi delle quali elettrificate;
- 6.300 km a doppio binario per un totale di **22.500 km** di sviluppo complessivo;
- 1.064 km linee a AV;
- 2.270 stazioni per il servizio passeggeri;
- 479 impianti per il servizio merci;
- 1.380 km di gallerie;
- 530 km tra ponti e viadotti.

Il Gruppo Ferrovie dello Stato S.p.a. assicura al sistema dei trasporti la circolazione di circa **9.200 treni al giorno**, per un totale di 472 milioni di viaggiatori e 88 milioni di tonnellate di merci trasportate in un anno.
Esso dispone di un parco di circa 75.000 rotabili ed effettua anche un servizio traghetti per la Sardegna e attraverso lo Stretto di Messina.

……
https://www.ingenio-web.it/27852-manutenzioni-ordinarie-e-straordinarie-delle-strutture-ferroviarie?utm_term=39048+-+https%3A%2F%2Fwww.ingenio-web.it%2F27852-manutenzioni-ordinarie-e-straordinarie-delle-strutture-ferroviarie&utm_campaign=La+Gazzetta+di+INGENIO&utm_medium=email&utm_source=MagNews&utm_content=3737+-+2066+%282020-08-28%29
Ingenio *- Caposio Guido - Politecnico di Torino 26/08/20200*

Cyber attacchi via Linkedin, ecco come funzionano: l'esempio di Inception La piattaforma social Linkedin può essere sfruttata da malintenzionati per veicolare attacchi alle aziende. Un caso è dato da Inception.dll**:** i laboratori di ricerca di Eset, azienda produttrice di software antivirus, hanno reso pubblico di aver individuato un malware finalizzato al compimento di intrusioni informatiche proprio a partire dalla rete LinkedIn. L'operazione "In(ter)ception", com'è stata battezzata proprio da Eset, ha individuato una lunga serie di cyber attacchi compiuti fra i mesi di settembre e dicembre 2019, finalizzati da un lato alla sottrazione di dati sensibili e dall'altro al puro guadagno economico.
Indice degli argomenti

- L'attacco del malware Inception
- Lo sfruttamento di Linkedin
- Il precedente

L'attacco del malware Inception

Tutto ha origine dalla ricezione di uno specifico messaggio di posta su LinkedIn contenente un'offerta di lavoro ben congeniata e proveniente da note società multinazionali attive in specifici settori d'assoluto rilievo pubblico, come il comparto delle telecomunicazioni o dell'energia rinnovabile. Inutile sottolineare in questa sede quanto l'offerta di lavoro fosse in realtà falsa, così come falso era il profilo aziendale collegato all'offerta stessa. Non solo: come sottolinea Dominik Breitenbacher, a capo dell'indagine condotta nei laboratori Eset, il messaggio di posta ricevuto attraverso lo spazio LinkedIn conteneva file allegati dannosi collegati alla piattaforma OneDrive, dove – attraverso false e-mail – erano stati aperti spazi di cloud storage associati ai falsi profili aziendali aperti su LinkedIn. L'allegato dannoso consisteva in un documento in formato PDF dov'era riassunta la posizione lavorativa ricercata; all'apertura del file veniva tuttavia installato sul PC della vittima proprio il malware in questione, garantendo così agli aggressori la piena connettività con il dispositivo colpito.
Quali, dunque, le finalità di simili incursioni? Dominik Breitenbacher ritiene gli attacchi avessero tutti i segni dello spionaggio, con diversi indizi che suggeriscono un eventuale collegamento con il gruppo Lazarus. Spiega però che né l'analisi del malware né l'indagine hanno permesso di ottenere informazioni sui file a cui gli aggressori miravano. Il Gruppo Lazarus abbia già avuto modo di presentarsi alle cronache internazionali come uno dei collettivi hacker più prolifici in circolazione, con decine di attacchi attribuiti divenuti ormai celebri, come il caso WannaCry **e il** Sony Breach……
https://www.cybersecurity360.it/nuove-minacce/cyber-attacchi-via-linkedin-ecco-come-funzionano-lesempio-di-inception/
Cybersecurity360 *- Stefano Ricci* **-** *26 Ago 2020*

Non solo Anonymous: chi sono i cyber-hacktivisti e perché crescono

Dietro le azioni dei "cyber-hactivisti" c'è un antagonismo antico, figlio della scena tecno-underground degli anni '90 e "nipote" della cultura punk: vediamo chi sono e i trend in atto. Vediamo come nasce il fenomeno e gli obiettivi

I servizi segreti li hanno definiti come la minaccia cyber "numericamente più consistente" a target strategici nazionali: sono i cyber-hacktivisti. Un fenomeno molto complesso e che è molto più del ribellismo romantico di film come "V per vendetta". Proviamo a esaminare il movimento che origina dalle derive anti-sistema anni '80 e che fa della tecnologia uno strumento di battaglia politico-sociale. Con un forte impatto sulla cybersecurity…..

Cominciamo col dire che è impossibile comprendere il ruolo che il cyber-hacktivismo ricopre oggi nella società contemporanea se non si conoscono Hakim Bey, al secolo Peter Lamborn Wilson, e le sue visionarie (per l'epoca, oggi decisamente attuali) riflessioni su come il personal computer e internet avrebbero fornito "un'arma" di liberazione e auto-liberazione per anarchici e libertari. Quello che Bey, ormai più di 25 anni fa, consegnava alla storia, era infatti una visione che ha influenzato migliaia di giovani che reperivano i suoi scritti inizialmente tramite riviste circolanti nel mondo della sottocultura underground, poi sistematizzati da case editrici minori.

"La Rete sarà danneggiata dal caos, mentre la Tela potrà prosperare con esso. Sia attraverso semplice pirateria-dati, oppure con uno sviluppo più complesso del rapporto reale con il caos, l'hacker della Tela, il cibernetico della TAZ (Temporary Autonomous Zone), troverà maniere per avvantaggiarsi di perturbazioni, collassi e guasti della Rete (modi di fare informazioni dall'"entropia"). Come un bricoleur, un raccoglitore di schegge d'informazione, contrabbandiere, ricattatore, forse anche cyberterrorista, l'hacker della TAZ lavorerà per l'evoluzione di connessioni frattali clandestine".

Era il 1995, il contesto è quello in cui questa "Rete", come la definisce Bey, sempre più controllata dagli Stati, avrebbe sviluppato una "Contro-Rete" e una "Tela" opposte al regime di controllo oppressivo messo in atto da sistemi di alleanze istituzionali in cui l'individuo sarebbe finito in "elettro-galere" e tirannie lavorative, in cui saremmo stati sottomessi ad un'architettura digitale in cui il computer diventava il fine ultimo dell'economia……

https://www.agendadigitale.eu/sicurezza/non-solo-anonymous-chi-ha-paura-dei-cyber-hacktivisti/

Agenda Digitale *- Federico Sergiani* ***-*** *27 Ago 2020*

Cybercrime, la Polizia esca per un ransomware lockscreen in Italia *JAMESWT scopre un tentativo di truffa del cybercrime che usa la Polizia e un ransomware lockscreen. L'esca è il falso blocco del dispositivo con richiesta di pagare una multa per aver scaricato materiale pedo-pornografico. Per risolvere il problema basta chiudere il browser o riavviare il sistema*

Il cybercrime usa la Polizia di Stato per diffondere un ransomware lockscreen. L'ha scoperto il ricercatore di cyber security JAMESWT. Un falso sito del Corpo appare sullo schermo in maniera permanente e spiega alla vittima che il suo dispositivo è stato bloccato, a seguito dell'accusa di aver scaricato e distribuito materiale pedo-pornografico. Di conseguenza, si intima di pagare una multa di 673 euro entro 12 ore. Altrimenti "la Polizia verrà a casa vostra per arrestarvi e vi saranno mosse delle accuse penali". Ovviamente si tratta di una truffa, il cui obiettivo è rubare le credenziali della carta di credito, con cui in teoria si può pagare la sanzione sul sito. Attenzione! La frode è costruita bene e il testo è scritto in italiano corretto. Inoltre, non è chiaro cosa attivi il redirect alla pagina malevola. Risolvere il problema, comunque, è semplice. Basta chiudere il browser o riavviare il sistema.

https://www.difesaesicurezza.com/cyber/cybercrime-la-polizia-esca-per-un-ransomware-lockscreen-in-italia/
Difesaesicurezza *- Francesco Bussoletti - 4 Settembre 2020*

L'evoluzione del ransomware, la doppia estorsione: ecco di cosa si tratta Il ransomware rimane una delle cyber minacce più temute nel vasto arsenale in possesso dei criminal hacker: probabilmente, tra i cyber incident, l'unico pericolo comparabile è il **data breach** (ovviamente tenendo presente che questo può essere talvolta anche accidentale). Ma l'ultimo trend tra gli operatori del ransomware potrebbe aver creato la tempesta perfetta, **unendo il potere *disruptive* dell'infezione alla possibilità di dover fare i conti allo stesso tempo con una violazione e divulgazione dei propri dati**: stiamo parlando della **doppia estorsione**. In quello che è diventato un vero e proprio modus operandi a partire dal primo trimestre del 2020, i criminal hacker stanno aggiungendo un'ulteriore fase ai loro attacchi. Prima di criptare i database delle vittime, gli aggressori estraggono grandi quantità di informazioni sensibili e minacciano di pubblicarle a meno che non vengano pagate le richieste di riscatto. Di fatto aggiungono un altro layer di pressione nei confronti delle vittime, aumentando parallelamente il valore della richiesta economica che viene recapitata……..
Ovviamente la prima domanda che viene spontaneo porci di fronte all'insorgere di questo nuovo fenomeno è cosa abbia spinto i criminal hacker a compiere questo step, intensificando il livello di minaccia portato dal ransomware. Dopotutto non è certo da quest'anno che questi hanno avuto la possibilità di accedere ai dati delle organizzazioni prese di mira.
L'ipotesi più concreta è che questo metodo sia una risposta alla presa di posizione delle aziende di fronte ai ransomware, meno inclini a pagare, e alla maggiore efficacia delle misure di recovery.Testimonianza di come le best practice contro queste infezioni stiano finalmente prendendo piede in maniera diffusa, costringendo i criminal hacker ad attacchi ancora più intensi.La tattica della doppia estorsione, però, potrebbe non rivelarsi la carta vincente per gli aggressori, come vedremo più avanti nell'articolo, anzi potrebbe metterli ancor di più in difficoltà……..
Il primo caso rilevato di doppia estorsione – nel novembre 2019 – riguardava la Allied Universal, una grande società di sicurezza americana…….
https://www.cybersecurity360.it/nuove-minacce/ransomware/levoluzione-del-ransomware-la-doppia-estorsione-ecco-di-cosa-si-tratta/
Cybersecurity360- *Pierguido Iezzi- 08 Set 2020*

Critical Flaws in 3rd-Party Code Allow Takeover of Industrial Control Systems Researchers warn of critical vulnerabilities in a third-party industrial component used by top ICS vendors like Rockwell Automation and Siemens. Six critical vulnerabilities have been discovered in a third-party software component powering various industrial systems. Remote, unauthenticated attackers can exploit the flaws to launch various malicious attacks – including deploying ransomware, and shutting down or even taking over critical systems. The flaws exists in CodeMeter, owned by Wibu-Systems, which is a software management component that's licensed by many of the top industrial control system (ICS) software vendors, including Rockwell Automation and Siemens. CodeMeter gives these companies tools to bolster security, help with licensing models, and protect against piracy or reverse-engineering.
Wibu-Systems made patches available for all of the flaws in version 7.10 of CodeMeter, on Aug. 11; however, the flaws were only recently disclosed by researchers on Tuesday. Many of the affected

vendors have been notified and added – or are in the process of adding – fixes to their installers, said researchers with Claroty who discovered the glitches.
"Successful exploitation of these vulnerabilities could allow an attacker to alter and forge a license file, cause a denial-of-service condition, potentially attain remote code-execution, read heap data and prevent normal operation of third-party software dependent on the CodeMeter," according to a Tuesday advisory published by ICS-CERT.
……
https://threatpost.com/severe-industrial-bugs-takeover-critical-systems/159068/
THREATPOST - *Lindsey O'Donnell -09 settembre 2020*

Data center giant Equinix discloses ransomware incident. Equinix says ransomware hit internal systems but that data centers are OK.Equinix, one of the world's largest providers of on-demand colocation data centers, has disclosed today a security breach.In a short statement published on its website, Equinix said it found ransomware on its internal systems, but that the main core of its customer-facing services remained unaffected. "Our data centers and our service offerings, including managed services, remain fully operational, and the incident has not affected our ability to support our customers," the company said. There is no suggestion that the company is downplaying the incident, with no major outages being reported at the time of writing, and no wave of customer complaints flooding social media. "Note that as most customers operate their own equipment within Equinix data centers, this incident has had no impact on their operations or the data on their equipment at Equinix," the company added. Details about the ins and outs of the attack are not available, with Equinix citing an ongoing investigation. Equinix is just the latest in a long list of ransomware incidents that have impacted web hosting and data center providers. The list also includes CyrusOne, Cognizant, A2 Hosting, SmarterASP.NET, Dataresolution.net, and Internet Nayana. Such companies are ripe targets for cyber-criminals, and especially for ransomware gangs. The reasons are simple and involve the immediate effect of their attacks, which often bring down services for impacted companies, but also for their respective customers, all of whom are expecting near-perfect uptime. This usually puts the pressure on the data center or web hosting provider to restore services right away, which may sometime include paying huge ransom demands. Equinix is listed on the NASDAQ stock exchange as EQIX and had around 8,000 employees. Earlier this year, Equinix entered into an agreement to purchase a portfolio of 13 data center sites, representing 25 data centers across Canada from BCE Inc. for approximately $750 million.
https://www.zdnet.com/article/data-center-giant-equinix-discloses-ransomware-incident/
ZDNET*- Staff- 09 settembre 2020*

Zoom Brings Two-Factor Authentication to All Users. This marks the latest step Zoom has taken to improve user security as more employees work from home. Zoom today confirmed two-factor authentication (2FA) will now be available for all users of the videoconferencing platform, which has come under intense security scrutiny as employees around the world continue to work from home to curb the spread of COVID-19. Zoom's 2FA will let users opt for authentication apps such as Google Authenticator, Microsoft Authenticator, and FreeOTP, which support the time-based one-time password (TOTP) protocol. Alternatively, users could have Zoom send a code via SMS or phone call as the second factor. The platform offers authentication methods such as SAML, OAuth, and/or passwords, which individuals can enable or disable on their accounts. To enable 2FA for password-based authentication, users should first sign in to the Zoom dashboard, access the navigation menu,

click Advanced > Security, and ensure Sign in with Two-Factor Authentication is enabled. There, users can choose to enable 2FA for all users on an account, for users with specific roles, or for users belonging to specific groups.This marks Zoom's latest effort to improve security for all users as researchers continue to find the gaps where attackers can break in. Earlier this summer, the company announced plans to offer end-to-end encryption (E2EE) for both paid and free users. It had previously said this would only be available to paid users of the platform.
https://www.darkreading.com/application-security/zoom-brings-two-factor-authentication-to-all-users/d/d-id/1338885
Darkreading *– Staff- 10 settembre 2020*

New cyberattacks targeting U.S. elections In recent weeks, Microsoft has detected cyberattacks targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns, as detailed below. We have and will continue to defend our democracy against these attacks through notifications of such activity to impacted customers, security features in our products and services, and legal and technical disruptions. The activity we are announcing today makes clear that foreign activity groups have stepped up their efforts targeting the 2020 election as had been anticipated, and is consistent with what the U.S. government and others have reported. We also report here on attacks against other institutions and enterprises worldwide that reflect similar adversary activity.
We have observed that:

- Strontium, operating from Russia, has attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants
- Zirconium, operating from China, has attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community
- Phosphorus, operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign

The majority of these attacks were detected and stopped by security tools built into our products. We have directly notified those who were targeted or compromised so they can take action to protect themselves. We are sharing more about the details of these attacks today, and where we've named impacted customers, we're doing so with their support……..
https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/
Microsoft blog *- Tom Burt - Sep 10, 2020*

Così l'intelligenza artificiale cambierà il modo di combattere. Il punto del Pentagono
È in corso l'evento del dipartimento della Difesa Usa dedicato all'intelligenza artificiale. A fronte dell'attivismo cinese per "una nuova era di autoritarismo digitale", e di quello russo per "ridurre la sovranità altrui", Mark Esper promette per gli Stati Uniti "standard rigorosi per i test e più alte aspettative etiche". Ma Washington non vuole perdere la sfida...
"L'intelligenza artificiale ha il potenziale per cambiare ogni campo di battaglia". Parola di Mark Esper, capo del Pentagono, che ieri ha aperto la sessione pomeridiana del "2020 department of Defense Artificial intelligence symposium and exposition", evento organizzato dal Joint Artificial Intelligence Center (Jaic), il centro di eccellenza della Difesa Usa istituito nel 2018. A febbraio dello scorso anno, il Jaic ha prodotto la prima "Ai Strategy" del Pentagono, una tabella di marcia per accelerare l'impegno militare nel campo, discendente dalla più ampia National Defense Strategy. Tutto in modalità virtuale

a causa delle restrizioni da Covid-19, il simposio sta riunendo le varie ramificazione della Difesa a stelle e strisce, l'industria, le istituzioni e il mondo della ricerca. L'obiettivo è fare il punto sull'avanzamento dei piani americani.

Cambierà tutto

"La storia ci insegna che i primi a sfruttare le tecnologie irripetibili spesso hanno un vantaggio decisivo sul campo di battaglia per gli anni a venire", ha detto il segretario Usa. "L'ho sperimentato in prima persona durante l'operazione Desert Storm, quando le bombe intelligenti dell'esercito degli Stati Uniti, gli aerei invisibili e il Gps abilitato dai satelliti hanno aiutato a decimare le forze irachene e le loro attrezzature sovietiche". L'intelligenza artificiale, ha notato Esper, può fare ancora di più: "A differenza delle munizioni avanzate o delle piattaforme di nuova generazione, l'Ia è unica, con il potenziale per trasformare quasi ogni aspetto del campo di battaglia."

La corsa per il primato

Già lo scorso anno, quando al Congresso gli chiesero quale fosse la priorità di modernizzazione per il suo dipartimento, Esper rispose "l'intelligenza artificiale". La convinzione, d'altra parte, non si ferma entro gli Stati Uniti. Era settembre 2017 quando **Vladimir Putin** affermò che "chi svilupperà la migliore intelligenza artificiale diventerà il padrone del mondo". La Cina sembrava averlo già capito. Tre mesi prima delle parole iconiche del presidente russo, il Consiglio di Stato cinese aveva rilasciato il Piano di sviluppo per una nuova generazione d'intelligenza artificiale (Aidp), identificando un obiettivo chiaro: diventare entro il 2030 il principale centro d'innovazione nel campo dell'intelligenza artificiale…….

https://formiche.net/2020/09/intelligenza-artificiale-pentagono-confronto/

Formiche *- Stefano Pioppi – 10/09/2020*

PROSSIMI EVENTI

A causa dell'emergenza Covid 19 tutti gli eventi sono stati rinviati a data da destinarsi. Stiamo riprogrammando l'attività dei Colloquia con alcuni interessanti argomenti. Vi terremo informati.

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*