

Rassegna del 05/07/2019

Sole 24 Ore	16 Sia, Cdp attende l'ok per salire all'85% Più spazio a Sarmi	<i>Festa Carlo</i>	1
Sole 24 Ore	10 Panorama - Auto connesse, no in Ue al WiFi preferito al 5G	<i>Biondi Andrea</i>	2
Mf	8 La Cina agli Usa: rispettate le promesse su Huawei	<i>Costantini Francesca</i>	3
Giornale	35 Alta definizione - Quelli che ci difendono dai (web)cavalli di Troia	<i>Lombardo Marco</i>	4
Giornale	36 Alta definizione - Il gioco è finito I pirati di Internet ora sono diventati veri delinquenti	<i>Marino Giuseppe</i>	6
Giornale	36 Alta definizione - Il tempo dei Nuovi Eroi - Il nemico è la paura Più educazione è l'arma per batterlo	<i>di Montigny Oscar</i>	9
Giornale	37 Alta definizione - Intervista a Gianvittorio Abate - «Servono poliziotti del web Facciamo fatica a trovarli»	<i>GMar</i>	10
Corriere della Sera	27 Visti da lontano - Hacker mobilitati per le elezioni Usa	<i>Gaggi Massimo</i>	11
Italia Oggi	17 Chessidice in viale dell'editoria - Publicis, nuovo Digital Hub	<i>...</i>	12
Italia Oggi	19 Niente ponti per le news online	<i>Secchi Andrea</i>	13
Sole 24 Ore	17 Media. Vivendi ricorre al Tribunale sui diritti di voto di Mediaset - Mediaset, Vivendi in Tribunale per i diritti di voto	<i>Olivieri Antonella</i>	15

Sia, Cdp attende l'ok per salire all'85% Più spazio a Sarmi

SISTEMI DI PAGAMENTO

A settembre il benessere di Bankitalia all'acquisto della quota delle banche

Carlo Festa

MILANO

È previsto per settembre il via libera di Banca d'Italia all'acquisto, da parte di Cassa Depositi e Prestiti, delle quote azionarie possedute dalle banche (Intesa Sanpaolo e Unicredit) nel gruppo Sia.

Una volta ufficializzato l'accordo, probabilmente dopo l'estate, è prevedibile che ci possa essere un assestamento anche ai vertici del gruppo. A Massimo Sarmi, attuale vicepresidente, ma anche presidente del comitato sviluppo della società ed entrato a far parte del comitato remunerazioni, potrà infatti essere assegnato un incarico esecutivo, a fianco dell'amministratore delegato Nicola Cordone. È il caso di notare che l'attuale presidente Giuliano Asperti non ha deleghe operative.

L'ex numero uno di Poste è entrato in Sia in rappresentanza proprio della Cassa Depositi e Prestiti, ormai azionista di riferimento del gruppo. Non è così da escludere che in settembre, con l'ufficializzazione dell'acquisto delle quote delle banche, possa essere convocata una nuova assemblea dei soci.

A fine luglio ci sarà invece un consiglio di amministrazione dell'azienda, che dovrebbe occuparsi soltanto della semestrale, mentre non dovrebbero essere toccati temi più strategici.

Il nuovo corso di Sia è iniziato due mesi fa quando la Cassa Depositi e Prestiti ha rilevato sia le quote dei fondi di private equity (cioè F2i e Hat) e successivamente quel-

le degli istituti di credito, per salire complessivamente a circa l'85% del capitale di Sia.

Il benessere dell'Authority è fondamentale per dare il via al riassetto futuro del gruppo, tra i leader europei nella progettazione, realizzazione e gestione di infrastrutture e servizi tecnologici dedicati alle istituzioni finanziarie, banche centrali, imprese e pubbliche amministrazioni, nelle aree dei pagamenti, della monetica, dei servizi di rete e dei mercati dei capitali.

Le attese sono soprattutto di due tipi. Da una parte Cdp, una volta salita al quasi pieno controllo, potrebbe cercare concretamente di mettere le basi per una delle opzioni di crescita del gruppo.

Le ipotesi, a propria volta, sono essenzialmente tre: avviare la strada per la quotazione a Piazza Affari, cercare a livello europeo una fusione (si parla della francese Worldline, anche se le dimensioni del gruppo transalpino sembrano troppo elevate) o un'acquisizione e, infine, ridiscutere un'aggregazione con Nexi.

Cdp punta infatti a fare di Sia un campione non solo italiano ma europeo in un settore, quello dei pagamenti, che continua a crescere a tassi elevati. Le premesse ci sono tutte, anche alla luce delle ultime importanti commesse vinte da Sia. L'ultima delle quali nello scorso giugno, quando la Bce ha scelto Sia e Colt per la rete di accesso ai sistemi di pagamento, titoli e garanzie dell'Eurosistema. Nel frattempo, ieri Sia ha inaugurato a Verona un nuovo centro specializzato per le carte di pagamento in grado di gestirne ogni fase di emissione, dall'ideazione alla distribuzione, attraverso un sistema di monitoraggio conforme ai più elevati standard di sicurezza.

© RIPRODUZIONE RISERVATA



PANORAMA**TLC****Auto connesse, no in Ue
al WiFi preferito al 5G**

«Si è fatta una scelta giusta, correggendo un errore». Pietro Guindani, presidente di Assotelecomunicazioni Asstel commenta così la decisione della Ue di bocciare la proposta di adottare il WiFi in qualità di "standard" per la connettività a bordo auto, a scapito del 5G. A votare contro è stata anche l'Italia. «L'approccio della Commissione – spiega una nota del Ministero dei Trasporti – non garantisce la dovuta neutralità tecnologica rispetto all'esigenza di mettere a punto infrastrutture digitali integrate a livello europeo». Da qui la decisione del Mit con l'Italia che «ha scelto di votare contro il vincolo tecnologico che conduce a una soluzione le cui prospettive di mercato sono peraltro ancora labili e lontane e che comunque non garantisce la possibilità di sfruttare appieno tutte le potenzialità del 5G».

Il fatto che l'Italia in sede Ue abbia votato contro è stato accolto con soddisfazione dall'associazione che riunisce la filiera delle Tlc. «Questa decisione – aggiunge Guindani – è un precedente importantissimo che segna il consenso per l'utilizzo delle reti 5G quale infrastruttura di base aperta e interoperabile per soddisfare le esigenze di potenzialmente tutte le imprese nei vari settori "verticali" dell'economia e dei cittadini nella fruizione di servizi intelligenti, sia pubblici sia privati». Adesso l'iter dovrà ripartire, ma «il lavoro fatto – dice ancora Guindani al *Sole 24 Ore* – non si butta via. Bisogna ricostruire un consenso intorno a una rigorosa neutralità tecnologica».

La scelta di bocciare l'atto europeo che avrebbe conferito una corsia preferenziale al WiFi a scapito del 5G è stata presa da 21 Paesi della Ue nel quadro di una querelle in cui Bru-

xelles ha difeso la preferenza per il WiFi puntando il ragionamento sull'immediata disponibilità e dunque sulla possibilità di offrire sin da subito servizi innovativi, laddove per il 5G bisognerà aspettare. Ma questo avrebbe anche voluto dire porre una seria ipoteca sullo sviluppo del 5G in uno dei settori più promettenti. Non il massimo, quindi, dopo che gli operatori, in Italia e non solo, hanno messo e dovranno mettere pedantemente le mani nel portafogli per lo sviluppo della rete 5G, fra frequenze e realizzazione del network. I detrattori del provvedimento Ue, come riporta la nota di Asstel, hanno poi fatto leva sulle potenzialità della quinta generazione mobile in termini di affidabilità e immediatezza. «A confronto con il WiFi – si legge nella nota dell'associazione – le tecnologie di telecomunicazioni 4G-LTE e 5G-NR sono migliori in termini di prestazioni, copertura, costi e sicurezza». I in più: «I sistemi cellulari consentono una maggiore ricchezza di prestazioni nelle comunicazioni dei veicoli tra di loro (V2V) e verso l'infrastruttura (V2I), i pedoni (V2P) e verso la rete (V2N). Al contrario, la tecnologia WiFi esclude la comunicazione verso le persone fisiche e copre aree limitate, non consentendo una supervisione completa del territorio». Senza contare che «in caso di attacchi informatici, i dispositivi di cybersecurity sulle reti di telecomunicazioni sono in grado di inoltrare dei segnali che bloccheranno l'accesso ai sensori attaccati. Al contrario, la tecnologia WiFi, in assenza di un nucleo centrale di rete (core network), non consente il controllo e l'identificazione degli accessi».

—Andrea Biondi

© RIPRODUZIONE RISERVATA

**Pietro Guindani.**

Per il presidente
Asstel «si è fatta
la scelta giusta»



La Cina agli Usa: rispettate le promesse su Huawei

di Francesca Costantini (MF-DowJones)

La Cina ha esortato gli Stati Uniti a mantenere la promessa di rimuovere alcune delle limitazioni imposte a Huawei Technologies per l'acquisto di attrezzature high-tech prodotte da società americane, come annunciato dal presidente Donald Trump dopo l'incontro con l'omologo cinese Xi Jinping avvenuto margine del G20 in Giappone la scorsa settimana. «Speriamo che gli Stati Uniti porranno fine ai provvedimenti contro le aziende cinesi il prima possibile», ha detto il portavoce del ministero del Commercio cinese, Gao Feng. Giorni dopo che Trump ha promesso di attenuare il divieto di vendita alla società cinese il dipartimento del Commercio degli Stati Uniti ha affermato che le richieste da parte delle compagnie americane per esportare prodotti a Huawei sono soggette al «più alto livello di controlli sulla sicurezza nazionale». Una dichiarazione che fa pensare che Huawei continuerà a essere trattata come se fosse ancora nella lista nera. Gao ha anche ribadito che tutte le tariffe punitive dovranno essere revocate per poter raggiungere un accordo con Washington. «La Cina si compiace che gli Stati Uniti abbiano deciso di non imporre nuovi dazi sui prodotti cinesi e di non aumentare le tariffe esistenti», ha affermato il portavoce. (riproduzione riservata)



ALTA DEFINIZIONE

LE MINACCE DI MALWARE, PROGRAMMI SPIA ED ESTORSIONI DIGITALI

Quelli che ci difendono dai (web)cavalli di Troia

Miliardi di pericoli sono dentro i nostri device. Giampaolo Dedola, unico italiano nel gruppo GReAT di Kaspersky, spiega come evitarli. Anche grazie a lui

Marco Lombardo

■ Voi che pensate che Ulisse sia solo nei libri di storia, sappiate che ci sono miliardi di suoi seguaci pronti a infiltrarsi nel vostro computer. O, ancor di più, nello smartphone che avete in tasca. Il Cavallo di Troia insomma esiste ancora, solo che viaggia per la Rete ed è pronto a sconfiggere la vostra (e la nostra) privacy. Non resta che difendersi, e per fortuna rispetto ai tempi andati i mezzi moderni ne danno la possibilità. E se Ulisse oggi si chiama malware, il suo nemico è un gruppo di angeli custodi del web che lavorano 24 ore su 24 per non farlo entrare dalla porta principale.

Il GReAt, ovvero «Global Research and Analysis Team», è un gruppo mondiale di ricercatori che Eugene Kasperky

ha messo insieme fin dal 2008. La sua azienda è sinonimo di sicurezza digitale, e il livello della minaccia è così alto che serve appunto un insieme di più di 40 esperti che lavorano in tutto il mondo: Europa, Russia, Americhe, Asia e Medio. Questo perché le minacce informatiche, infatti, non hanno frontiere, né orario: arrivano 24 ore su 24. Di questo gruppo di specialisti fa parte un italiano, Giampaolo Dedola, che è security researcher di Kaspersky da maggio di 2017, dopo aver ricoperto un ruolo simile in Telecom. Dedola per il GReAT fornisce attività di intelligence e di difesa sulle minacce persistenti che arrivano da internet, e i report delle operazioni di prevenzione vengono utilizzati dalle aziende e dalle istituzioni per migliorare la propria strategia di sicurezza. Il tutto in coordinamento con le forze di polizia di tutto il mondo, e l'ultimo accordo firmato da Kaspersky è stato con Interpol. Perché - come dicono quelli del GReAT - «non esiste un malware buono. Mai».

I numeri che racconta Dedola sono d'altronde chiari: «Se guardiamo le statistiche del 2018, ci sono stati nel mondo 1 miliardo e 877 milioni di attacchi informatici e sono stati scoperti più di 500 milioni di indirizzi internet malevoli. Noi stessi lavoriamo ogni giorno su oltre 400 mila nuovi casi». Siamo circondati, quindi, di cavalli ce ne sono a bizzeffe. E quindi sta a noi affidarci ai consigli di esperti come Dedola: «E questo lavoro è una passione, ovviamente senza orario». Ma come difenderci? «Innanzitutto con il buon senso - dice lui -: se ci arriva una mail che annuncia una vincita di una lotteria a cui non abbiamo mai partecipato, è ovvio che dobbiamo capirlo subito. Ma siccome le minacce sono davvero sofisticate, si possono usare alcuni accorgimenti. In considerazione soprattutto del fatto che il maggior veicolo di pericolo è diventato appunto lo smartphone, che non sempre ha ancora gli stessi software che vengono installati sui computer. E allora, per esempio: se vi collegate a una linea wifi di un hotel, usate un programma Vpn per schermare il vostro indirizzo. E poi utilizzate sempre programmi aggiorna-



ti, presi da vendor affidabili. Come quelli di Kaspersky insomma. Infine: in caso di tentativi di estorsione, non cedete mai. E denunciate sempre».

Intanto loro, quelli del GReAT vigilano, anche se non sempre la prevenzione può sventare una minaccia: «È una lotta continua, l'importante è capire il livello, risalire da chi arriva e intervenire subito. Il nostro compito principale è tutelare le persone, se poi sono coinvolti soggetti importanti ovviamente trattiamo le informazioni con molta attenzione.

Ma ripeto: le persone vengono prima». Ulisse insomma vive, ma Giampaolo (e il GReAT di Kaspersky con lui) non cederà mai, anzi, cerca nuovi alleati: «Le minacce sono in evoluzione globale, è una lotta che non avrà fine. Per questo abbiamo bisogno di nuovo esperti e per fortuna molti giovani cominciano a capire che questo non è un gioco. È un lavoro, che a volte può anche salvare delle vite».

ALTA DEFINIZIONE

GLI HACKER SI STANNO ESTINGUENDO?

Il gioco è finito I pirati di internet ora sono diventati veri delinquenti

IL REPORT «X FORCE» DI IBM
Il gruppo più famoso di corsari informatici nel 2018 ha ridotto l'attività del 95%

I DATI DI CLUSIT
Il giro d'affari dei software di difesa in Italia è stato nel 2017 di 1 miliardo di euro

Giuseppe Marino

■ «È impossibile che un ragazzo del liceo metta un gettone nel telefono e penetri il nostro sistema! Quindi sicuramente lavora con altri. Per forza!». Ci avevano visto lungo gli sceneggiatori di *Wargames*. Era il 1983 quando uscì il film che raccontava l'impresa immaginaria di un adolescente americano che era riuscito a violare le

difese informatiche del sistema di difesa nucleare americano portando il mondo sull'orlo del conflitto finale con i russi.

Come spesso accade, la fiction aveva anticipato un fenomeno poi diventato molto più comune di quanto si potesse immaginare all'epoca, sebbene non con conseguenze così estreme: nessuna guerra nucleare. La frase a effetto pronunciata nel film da un incre-

dulo «dottor John McKittrick» era azzeccata. Gli hacker che per gio-



co o per ideologia violano le difese informatiche di importanti istituzioni per anni sono diventati una preoccupazione reale. I dati più recenti raccontano però di un'inversione di tendenza. Il più famoso gruppo di pirati del web, Anonymous, ha ridotto del 95 per cento gli attacchi, secondo il report «X Force» di Ibm. Dai 35 incidenti del 2015, si è scesi ai soli due del 2018. Il dato è particolarmente significativo perché Anonymous è responsabile del 45 per cento di tutti gli attacchi informatici.

E c'è un riscontro anche in Italia. Secondo il dossier Clusit 2019, il più importante registro degli attacchi informatici pubblicato nel nostro Paese, il numero delle incursioni dovute ad «hacktivism», cioè azioni a sfondo ideologico, è in continuo calo. Nel 2018 c'è stato un ulteriore picco negativo del 23 per cento.

E la comunità tecnologica da qualche tempo si interroga su questa nuova tendenza. Va detto che spesso non è facile distinguere tra le azioni di comune cybercrime, volte a rubare informazioni o a bloccare l'attività di un'azienda per ricattarla, e quelle di vero e proprio «attivismo politico» internetiano. Il furto di dati e la divulgazione a scopo dimostrativo o di protesta politica possono favorire anche l'attività di cybercriminali, sempre in cerca di vulnerabilità.

In Italia ci sono stati casi recenti che sono diventati pubblici e hanno fatto scalpore. Come le azioni di un hacker che si fa chiamare Rogue0 e ha preso di mira più volte Rousseau, la piattaforma di voto elettronico del Movimento 5 Stelle, divulgando dati privati de-

gli «elettori» del Movimento, inclusi i loro numeri di telefono, al solo scopo di dimostrare quanto vulnerabile e poco affidabile fosse lo strumento politico gestito da Davide Casaleggio. Anche attacchi «idealisti» come questi possono portare a danni notevoli. Sia per chi vede i propri dati diventare di dominio pubblico, sia per le aziende coinvolte. Rousseau ha visto minata la propria credibilità e ha accettato di pagare una multa di 50mila euro comminata dal Garante della Privacy (saldata con lo sconto del 50 per cento perché pagata senza fare ricorso).

A questi tipo di azioni si può affiancare l'attività dei cosiddetti «hacker buoni», appassionati di informatica con grandi capacità di operare sulla Rete: la loro attività classica è penetrare le difese come sfida e poi avvisare le aziende coinvolte, segnalando loro le vulnerabilità su cui intervenire. Anche in questo caso la piattaforma Rousseau è riuscita a far parlare di sé quando ha denunciato un «hacker buono», Luigi Gubello, in «arte» Evariste Galois. Il 27enne di Portogruaro (Venezia) era penetrato nel sistema e aveva avvisato i gestori, ma l'associazione Rousseau non ha apprezzato e si è rivolta alle autorità, salvo poi ritirare la denuncia in extremis, alla vigilia del processo.

La «fuga» degli hacker «attivisti» colpisce soprattutto perché allo stesso tempo il fenomeno del cybercrime sta esplodendo.

Sempre secondo Clusit, nel 2018 si sono verificati in Italia 1.232 attacchi, un picco del 43 per cento in più rispetto al 2017. Particolarmente frequente è diventata l'attività di «spionaggio»: estrarre dati per gli scopi più vari, dai ricatti informatici al furto di informazioni utili a scopi industriali, politici, militari (sebbene di quest'ultima categoria si sappia ben poco, perché raramente gli incidenti vengono resi pubblici). Il risultato è che il business della cybersecurity è in continuo aumento negli ultimi anni, arrivando nel 2017 in Italia a oltre un miliardo di euro di giro d'affari, con un tasso di crescita di oltre il 10 per cento.

Nessuno può dirsi veramente al riparo. Gli attacchi a strutture sanitarie sono aumentati in modo vertiginoso (il Garante della privacy ha parlato di incursioni in aumento del 99% nel 2018). Nel mirino gli obiettivi più diversi, dai tentativi di bloccare infrastrutture critiche come le centrali elettriche (c'è il dubbio che anche il black out che ha oscurato mezza America Latina sia opera di cybercriminali), ai ransomware, software che criptano dati importanti nei computer (in Italia è successo anche a piccole aziende) e lo sblocco solo in cambio di un riscatto.

Il business attira malintenzionati e rende tutto più difficile per gli «hacktivist», spesso infiltrati da veri criminali o finiti nel mirino delle forze dell'ordine. Assai meno indulgenti del dottor McKittrick di Wargames.



1,5

In miliardi di euro, è la spesa globale in cybersecurity delle aziende italiane nel 2018. È stato un anno d'oro per il settore. Secondo il report Context, l'Italia è quarta al mondo per aumento di spesa: ha pesato l'entrata in vigore del Gdpr, nuova norma sulla privacy

20mila

Nel 2018, secondo l'Osservatorio delle Competenze Digitali, il fabbisogno di personale specializzato per l'information security in Italia oscillava tra 12.800 e 20mila unità. Ma i laureati sono stati solo 8.800, in aumento di mille rispetto al 2017, ma ancora largamente insufficienti

*Erano attivisti,
violavano i pc
per ideologia
Le loro incursioni
nell'ultimo anno
si sono ridotte
e perfino l'attività
di Anonymous
è molto calata*

*Di contro si è
moltiplicato
il fenomeno del
cybercrimine:
furti di dati,
obbiettivi politici
e militari. E
nessuno può
sentirsi al sicuro*

ALTA DEFINIZIONE



di Oscar di Montigny

Il tempo dei Nuovi Eroi

Il nemico è la paura Più educazione è l'arma per batterlo

Di recente ho letto un articolo in cui l'intervistato ha usato una figura che mi è rimasta in mente perché realisticamente immaginifica. Ha affermato che quella della cybersecurity è la classica corsa tra guardie e ladri a chi arriva prima. Ma se superiamo il primo istinto di ridacchiare immaginando le vecchie comiche con il ladro in calzamaglia nera, inseguito da una guardia impacciata, armata di fischietto e manganello, scopriamo che il tema è serissimo e cruciale per il nostro futuro sotto diversi punti di vista, personali, sociali e di mercato. Il mercato italiano, per esempio, secondo l'Osservatorio del Politecnico di Milano, vale 1,19 miliardi di euro ed è un settore che l'anno scorso è cresciuto del 9% rispetto a quello precedente. Ma, siccome il 77% delle aziende non ha ancora o non ha mai avuto un efficiente sistema di gestione del cyber risk, il mercato è dunque suscettibile di enormi margini di sviluppo. Un dato che, pur nella sua sola dimensione nazionale, ce la dice lunga su scenari e prospettive di carriera e di business. Sappiamo anche che, sebbene gli attacchi nell'ultimo anno siano stati prevalentemente truffe (phishing, estorsioni ecc.) a crescere saranno sempre di più lo spionaggio e l'influenza manipolatoria dell'opinione pubblica. Dunque, le attenzioni si concentreranno soprattutto sugli smartphone.



Se da un lato, pensare che entro il 2025 nel mondo saranno connessi tra loro e su internet circa 75 miliardi di dispositivi (un mercato di 11 trilioni di dollari), e che molti di questi dispositivi sono IoT, ci lascia capire che l'enorme prateria di opportunità per il mondo del crimine. Dall'altro, ci conforta sentire Steve Schmidt, capo dell'Information Security di Amazon Web Services, dire all'apertura dalla recente «Re:Inforce», una conferenza organizzato a Boston che ha raccolto migliaia di addetti ai lavori delle più grandi aziende del settore della cybersecurity e del cloud, che

fare leva sulle paure del cliente è una pratica inutilmente negativa che l'industria del cloud. E della sicurezza informatica dovrebbe abbandonare per preferirle quella di insegnare concretamente come difendersi.

Tutti sappiamo vagamente, perché è già accaduto, che con sistemi non in sicurezza è possibile paralizzare un ospedale o spegnere una centrale elettrica. Gli scopi posso essere vari. Creare agitazione politica per destabilizzare governi, gettare una nazione nel caos. Tra l'altro un'arma cibernetica costa meno di una cinetica. Ma in quanti abbiamo contezza che non è l'arma quella che miete le vittime ma, appunto la paura? È la paura di ciò che sarà e che non conosciamo che ci fa sentire oggi sbalottati tra la sensazione che si sia veramente sull'orlo del precipizio di questo nuovo medioevo, più oscuro del precedente poiché ci ha mangiato le coscienze, e la netta percezione che ci sia un'infinità di menti, cuori, corpi, anime di uomini e donne dediti e focalizzati sulla possibilità di un necessario rinascimento. Allora la chiave è appunto concederci al Ri-nascimento che deve essere prima dentro affinché possa poi prendere forma fuori. In questa direzione le aziende, intese come sistemi organizzativi sociali in grado di aggregare persone che viaggiano verso uno scopo comune, possono e devono fare molto. Un cambio di paradigma, come ad esempio quello indicato da Schmidt che sollecita l'abbandono della leva della paura per quella dell'educazione, degli strumenti e della consapevolezza, è un primo, importante passo. È quel momento di rottura degli schemi che io definisco dello 0.0. Senza il quale non si passa da un «prima» a un «dopo».



ALTA DEFINIZIONE

L'INTERVISTA Gianvittorio Abate

«Servono poliziotti del web Facciamo fatica a trovarli»

Il titolare di Innovery: «Ci sono buone scuole per un mestiere sicuro. Ma le famiglie le snobbano»

DON CHISCIOTTE

Finalmente le aziende capiscono i pericoli della Rete. Ma per anni...

IL COMPUTER

Troppi giovani pensano sia solo divertirsi. Invece di garantirsi uno stipendio

PREVENZIONE

Un mio amico ha perso 3 anni di dati. Correre ai ripari è dura. E costoso...



■ «Gli investimenti in sicurezza sono aumentati, ma manca il personale preparato». Il racconto del mercato del lavoro della cybersecurity fatto dall'ingegner Gianvittorio Abate sembra fatto apposta per accendere la speranza dei ragazzi che non si rassegnano al reddito di cittadinanza. Vent'anni fa Abate, napoletano con esperienze nelle Tlc, si occupava di cavi in fibra ottica, quando intuì che la sicurezza informatica per le aziende sarebbe diventata importante quanto quella fisica. La sua creatura, Innovery, è nata dal lavoro di quattro soci. Oggi è un'azienda con sedi in Italia, Spagna e Messico, conta su 240

dipendenti e un fatturato di 27 milioni, raddoppiato negli ultimi tre anni. E quest'anno ha attirato un importante investimento da parte del fondo Wise Equity, che ha rilevato il 69% delle quote azionarie. «Per anni ho dovuto combattere i mulini a vento come Don Chisciotte, ora le aziende cominciano a capire quanto è importante proteggere i propri dati», dice Abate.

Voi vi occupate di grandi aziende, dall'energy alla farmaceutica, ma l'Italia è soprattutto un Paese di Pmi. Rischiano anche loro?

«La piccola azienda di progettazione ed edilizia di un amico è stata colpita da un ransomware. Ora è in lacrime: si ritrova con i dati di tre anni di contabilità criptati e inutilizzabili e chi l'ha infettato chiede un riscatto. Anche i piccoli rischiano e sono particolarmente indifesi perché spesso a gestione familiare, con scarse competenze informatiche e si rivolgono ad aziende che al massimo si occupano di installare software e fare la manutenzione ai computer. Ma correre ai ripari dopo essere stati colpiti può essere molto difficile e costoso».

Manca la cultura informatica nel nostro Paese?

«La cybersecurity è un settore che sta accelerando tantissimo negli ultimi anni e sicuramente manca personale specializzato, ma credo che il problema riguardi anche altri Paesi».

Può essere uno sbocco lavorativo interessante?

«Un 28enne con un po' di preparazione in media arriva a una Ral (retribuzione annua lorda) di 28mila euro. A 40 anni puoi tranquillamente portare a casa più di 65mila euro».

Avrete la coda davanti alla porta, con la fame di lavoro che c'è.

«Al contrario. Purtroppo ci sono tanti ragazzi che usano il computer e gli smartphone per divertirsi e non approfondiscono. Oppure ci sono comunità di giovani che si divertono a violare difese informatiche per sfida, l'equivalente delle ragazzate che facevamo noi per strada un tempo. Ma non capiscono che potrebbero farne un mestiere».

Come bisogna prepararsi per entrare in questo settore?

«Noi abbiamo talmente bisogno di personale che una volta andavamo a cercare i neolaureati con competenze informatiche. Ora pure quel bacino non basta più. E ci rivolgiamo agli istituti professionali. A Roma, Napoli o Milano ci sono buone scuole che spesso vengono snobbate dalle famiglie ma che invece fanno un buon lavoro. Poi alla formazione specifica ci pensiamo noi».

GMar



Visti da lontano

Hacker mobilitati per le elezioni Usa

di Massimo Gaggi

«**M**i raccomando, non ti intromettere nelle elezioni americane!». L'avvertimento sarcastico pronunciato da Donald Trump davanti alle telecamere, pressato dai giornalisti al vertice di Osaka, è parso più una presa in giro della stampa che un monito reale. Così, almeno, l'ha percepito Vladimir Putin che ha sorriso, per nulla irritato. Le interferenze russe via Internet, insomma, continueranno. Ma, dopo quanto accaduto tre anni fa, nelle presidenziali Usa del 2020 assisteremo a un salto di qualità nelle tecniche usate per influenzare in modo fraudolento gli elettori. E stavolta non si tratterà solo di *hacker* russi. Nei partiti Usa si sta delineando, a destra come a sinistra, lo scenario di una diffusione capillare dei metodi più fantasiosi per falsare non solo il voto per la Casa Bianca ma anche quelli per la conquista dei seggi-chiave di Camera e Senato. I centri di ricerca specializzati, ma anche istituzioni autorevoli come la Brookings, disegnano scenari da incubo: le informazioni false sui candidati sono la cosa più banale. Ben più insidiosi i video falsificati per far dire in modo credibile a un politico, usando le tecniche *deepfake*, cose che non ha mai detto e che offendono parte dell'elettorato, una razza o una religione. Messaggi che possono anche essere inviati solo alla platea di utenti del *web* più sensibile a quegli argomenti o più vulnerabile. Magari scegliendo certi gruppi Facebook. Un ex militare da far eleggere può diventare un eroe di guerra, o si può denigrare l'avversario in mille modi: sesso, soldi, razza. Il «non è una vera nera» scagliato contro Kamala Harris e condiviso, a caldo, anche dal figlio di Trump dà l'idea di cosa si prepara. Ma si può anche cercare di non far votare gente dall'orientamento ostile fornendo false informazioni su orari, ubicazione dei seggi, documenti richiesti o, addirittura, minacciando rappresaglie legali per chi andrà alle urne. Il voto 2020 sarà *Ground Zero* della manipolazione digitale delle elezioni. L'America ha tutti gli incentivi: è in gioco la Casa Bianca, ci sono una enorme quantità di denaro che gira nella campagna, le tecnologie digitali più sofisticate, un'infinità di società di consulenza che offrono servizi di protezione e di attacco informatico. Il Congresso non sa come regolare, i partiti non sanno come difendersi. Uno spettacolo da osservare con attenzione: presto toccherà a noi.

© RIPRODUZIONE RISERVATA



CHESSIDICE IN VIALE DELL'EDITORIA

Publicis, nuovo Digital Hub. *Publicis Media riorganizza le sue attività digitali in un nuovo Digital Hub, che offrirà, alle agenzie del gruppo supporto nella gestione delle campagne pubblicitarie digitali, consulenza nell'utilizzo dei dati e sviluppo di prodotti innovativi derivanti dalla digitalizzazione dei media tradizionali. A capo ci sarà Cristina Ughes, già nel gruppo, con un team di sessanta professionisti.*



L'Audiweb di aprile. Business Insider +29%, TuttoMercatoWeb +8,3%, Il Post +6%

Niente ponti per le news online

Libero +14%, Messaggero +8,4%, Adn +8%, Leggo +5,6%

DI ANDREA SECCHI

Con una tale sfilata straordinaria di ponti festivi aprile sarebbe potuto essere il mese più fiacco della prima metà dell'anno per i siti Internet. Eppure non è stato così: Pasqua, 25 aprile e primo maggio separati da uno o due giorni non hanno impattato granché sul traffico online secondo i dati rilasciati da Audiweb. È plausibile pensare che a sollevare le sorti dell'audience del giorno medio siano stati i due maggiori fatti di cronaca del mese. Da una parte l'incendio a Notre Dame de Paris del 16 aprile, dall'altra l'attentato in Sri Lanka del 21 il cui bilancio finale è stato di oltre 250 vittime. Gli utenti unici giornalieri totali, così, sono rimasti uguali a quelli di marzo, mentre i visitatori mensili sono calati dello 0,9%, e le news, che nei periodi di vacanza hanno meno seguito, hanno comunque tenuto con un -0,8% mensile.

Nella top ten dell'audience giornaliera sul perimetro organico si muove poco rispetto a marzo. *Repubblica*, sempre prima, cala dell'1% a 2,68 milioni di utenti unici, mentre

il *Corriere*, secondo, scende del 3,7% a 2,12 milioni di utenti (da considerare il paywall). Al terzo posto torna *TgCom24* (-0,8%) riprendendosi la posizione che era passata a *Upday*, l'app aggregatore di Axel Springer per i cellulari Samsung ora quarta (-5,3%). Dal quinto posto in poi tutto invariato: *Fanpage* +2%, *Gazzetta dello Sport* +0,8%, *Fatto* -1,6%, poi il *Messaggero* con un +8,4%, *Stampa* a -1,9% e *Leggo* a +5,6%. Quest'ultima testata diretta da **Davide Desario**, già al decimo posto il mese precedente, è stata protagonista di una crescita costante nell'ultimo anno ed è passata dal veleggiare intorno alla 20esima posizione all'ingresso nella top ten e dai 462 mila utenti di luglio 2018 (il primo mese di distribuzione pubblica dei dati Audiweb 2.0) ai 985,5 mila attuali.

Per quanto riguarda le altre testate nazionali, scorrendo la classifica si trova *Il Giornale* a +3,3%, *Sole 24 Ore* -7,7%, *Libero* +14%, *Milano Finanza* +10,2%.

In crescita i siti dedicati al calciomercato come *TuttoMercatoWeb* (+8,3%) e *Calciomercato.com* (+70%, ma l'incremento dipende anche dall'introduzione del tag di

Google Amp ad aprile). Sempre per lo sport, bene *Corriere dello Sport* (+3,2%) e *Tuttosport* (+3,1%).

Da segnalare inoltre *Business Insider* (+29%), *Tpi* (+8%), *Adnkronos* (+7,9%), *Il Post* (+5,9%).

Sui siti della tv, Mediaset Play continua a essere in testa e cresce del 4,4% a 886,3 mila utenti unici mentre al secondo posto *SkySport* supera seppur di poco *RaiPlay* (-11,5% e -14,8% rispettivamente). Nel gruppo aumentano *Eurosport* (-17,1%), *Fox* (+2,5%), *Rai.it* (+21,2%) e *Witty Tv* (+9%), il sito della Fascino di Maria De Filippi.

Invariate le posizioni fra le radio: *Deejay* prima con 173,7 mila utenti in calo dell'11,36% e *Radio 105* a 96,2 mila utenti (-7%).

Qualche nota sulla parte della classifica non pubblicata in questa pagina, quella dei portali e degli altri siti. Il dato più eclatante è quello dei siti sulle previsioni meteorologiche, molto battuti ad aprile in vista dei ponti e del tempo ballerino: *ilMeteo.it* è cresciuto del 60,7% a 3,6 milioni di utenti, mentre *3BMeteo* ha registrato un progresso del 51,3% a 1,8 milioni.

—© Riproduzione riservata—

Così i siti di informazione, tv e radio

		Aprile 2019 (dati quotidiani) perimetro organico (senza aggregazioni - Tal)					
Brand		Utenti unici totali	Computer	Tablet	Smartphone	Pag. tot.	Var. mar. 2019*
I siti di informazione e della carta stampata							
1	La Repubblica	2.682.255	702.103	235.513	1.892.637	9.657	-1,0%
2	Corriere della Sera	2.124.408	616.238	231.794	1.361.074	6.534	-3,7%
3	TGCOM24	1.872.618	295.777	104.720	1.543.772	6.797	-0,8%
4	Upday	1.866.214	0	0	1.866.214	3.602	-5,3%
5	Fanpage	1.659.922	109.937	89.386	1.477.057	4.432	2,0%
6	La Gazzetta dello Sport	1.544.934	359.362	116.473	1.129.345	5.628	0,8%
7	Il Fatto Quotidiano	1.295.376	204.062	73.023	1.041.712	2.990	-1,6%
8	Il Messaggero	1.278.450	172.972	82.186	1.043.839	2.441	8,4%
9	La Stampa.it	1.009.243	234.235	87.790	710.638	2.753	-1,9%
10	Leggo	985.546	65.023	47.072	880.568	1.912	5,6%
11	TuttoMercatoWeb.com	815.236	92.549	53.545	688.236	4.670	8,3%
12	ANSA	774.650	254.645	61.593	484.642	2.427	-0,7%
13	Il Giornale	690.707	128.081	62.045	506.545	1.734	3,3%
14	Huffington Post Italia	608.918	68.775	24.943	518.676	1.144	-3,2%
15	Donna Moderna	604.446	91.954	49.348	467.163	1.085	4,9%
16	Il Sole 24 ORE	596.925	223.214	38.306	342.553	1.501	-7,7%
17	Il Mattino	560.688	71.676	33.658	462.870	1.514	13,8%
18	Quotidiani Espresso	506.372	102.230	41.392	371.627	1.532	2,6%
19	Calciomercato.com	406.582	44.667	22.939	341.957	1.468	70,0%
20	Libero Quotidiano	394.354	103.826	39.090	256.181	1.296	14,0%
21	Il Post	392.423	49.785	22.710	321.590	659	5,9%
22	Vanityfair.it	389.256	30.461	23.648	335.865	782	4,4%
23	Termometro Politico	378.444	44.534	20.146	314.892	670	-55,2%
24	Corriere dello Sport	365.774	73.364	23.977	271.967	997	3,2%
25	Il Gazzettino	352.854	58.432	34.675	266.659	1.192	5,8%
26	Tiscall	311.680	185.300	17.375	116.177	5.039	-9,5%
27	TuttoSport	310.720	72.620	26.447	218.753	1.128	3,1%
28	TPI	253.944	10.357	5.538	238.388	412	8,0%
29	Blitzquotidiano.it	236.151	9.175	16.088	211.936	377	-15,0%
30	DagoSpla	176.175	57.650	24.955	94.916	1.476	-6,3%
31	Affaritaliani.it	150.399	21.161	10.698	118.703	288	3,6%
32	Business Insider Italia	147.211	22.059	9.419	116.152	242	29,0%
33	Grazia.it	142.483	13.834	8.995	120.027	329	-11,3%
34	Wired.it	137.999	23.581	8.725	106.082	202	4,5%
35	LaSicilia.it	136.784	22.899	9.251	105.173	228	42,4%
36	ELLE IT	132.207	10.596	6.301	115.507	212	32,1%
37	La Cucina Italiana	127.676	19.182	10.642	98.075	215	1,3%
38	Lettera43	126.916	28.419	9.523	89.169	187	-33,9%
39	Adnkronos	123.131	21.366	10.204	91.845	222	7,9%
40	Milano Finanza	110.579	53.301	8.826	50.434	635	10,2%
41	Focus.it	107.048	21.589	7.244	78.421	188	7,6%
42	Alvolante.it	105.178	26.936	12.116	66.227	392	-14,3%
43	UnioneSarda	98.096	31.317	10.228	59.368	352	-0,6%
44	Giornale di Sicilia	88.741	13.148	5.376	71.611	220	6,5%
45	Corriere Adriatico	85.381	14.186	7.339	66.575	326	14,8%
46	La Nuova Sardegna	83.964	15.849	4.642	64.336	309	3,2%
47	Glamour.it	80.413	5.981	4.632	69.894	125	14,3%
48	FCInternews.it	67.513	14.916	4.761	48.931	472	1,4%
49	La Gazzetta del Mezzogiorno	66.886	10.379	4.926	51.988	114	46,5%
50	Cosmopolitan.it	65.567	8.365	4.625	52.704	104	17,1%
51	Esquire	55.913	4.743	2.745	48.448	74	56,0%
52	Marie Claire IT	55.283	6.556	3.103	45.654	79	25,1%
53	Il Centro	54.626	10.284	3.120	41.796	151	5,4%
54	L'Arena	54.285	10.382	3.755	40.850	205	5,1%
I siti della tv							
1	Mediaset Play	886.279	158.687	73.508	668.121	2.196	4,4%
2	SkySport HD	568.206	60.961	24.951	485.759	1.416	-11,5%
3	RaiPlay	566.527	236.058	95.145	243.706	2.162	-14,8%
4	Sky TG24 HD	330.197	33.074	18.320	280.199	523	-2,1%
5	Eurosport	265.666	17.385	18.179	234.565	952	17,1%
6	Fox Networks Group Italy	158.016	29.507	14.371	114.709	410	2,5%
7	Rai News	147.819	37.858	12.873	97.970	561	-16,0%
8	LA7	96.291	22.258	9.107	65.371	265	-6,6%
9	Rai.it	73.871	29.117	8.230	36.711	150	21,2%
10	Witty Tv	72.190	35.520	4.285	32.392	217	9,0%
11	Viacom Global Ent. Group	70.489	24.760	2.909	42.823	139	-16,8%
12	Sky GuidaTV	53.856	12.135	5.099	36.796	131	-5,6%
I siti della radio							
1	Radio DeeJay	173.697	23.978	11.408	142.689	296	-11,6%
2	Radio 105	96.242	14.602	5.689	76.159	184	-7,0%

Fonte: elab. ItaliaOggi su dati Audiweb. *La variazione può risentire dei cambiamenti di perimetro

Media**Vivendi ricorre
al Tribunale
sui diritti di voto
di Mediaset****Dopo l'esposto Consob,
Vivendi deposita un atto di
citazione per annullare le****delibere di cda e assemblea sul
voto multiplo.****Biondi e Olivieri — a pag. 17****Mediaset, Vivendi in Tribunale per i diritti di voto****MEDIA****Citazione per annullare le
delibere di cda e assemblea:
il 26 novembre l'udienza****Antonella Olivieri**

Vivendi e Simon fiduciaria – che complessivamente detengono il 28,8% del capitale di Mediaset – si appellano al Tribunale di Milano per recuperare i diritti di voto che il cda del Biscione ha negato loro, ritenendo l'intera partecipazione acquisita irregolarmente e in violazione del contratto su Premium del 2016, che doveva portare la pay-tv sotto le insegne francesi ma non è stato onorato. I tempi della giustizia però non sono quelli degli affari e l'udienza è stata fissata per il 26 novembre quando l'operazione Media for Europe, che prevede il trasferimento delle azioni di Mediaset Italia e Spagna sotto una nuova holding di diritto olandese, sarà già decollata.

Le mosse legali di Vivendi non hanno messo finora in discussione il trasferimento ad Amsterdam, ma se il gruppo che fa capo a Vincent Bolloré recuperasse i diritti di voto – con un intervento d'urgenza del Tribunale – avrebbe la possibilità di bloccarlo, in quanto nelle assemblee straordinarie è necessaria la maggioranza dei due terzi del capitale presente e gli impegni depositati da Vivendi – in ottemperanza alla delibera Agcom che fa di-

vieto di detenere più del 10% contemporaneamente in Mediaset e Telecom (delibera peraltro anch'essa contestata davanti al Tar/Corte europea) – prevedono l'esercizio del diritto di voto sull'intera partecipazione in caso di operazioni straordinarie, come appunto il trasferimento della sede.

Dopo tre anni di liti e tentativi di ricomposizione andati a vuoto, è chiaro che né Mediaset né il suo azionista Fininvest si fidano più di Vincent Bolloré. Tant'è che da tempo non ci sono più contatti tra le parti e i rapporti sono stati relegati alle aule dei Tribunali. Tuttavia le ultime iniziative legali – il dossier per i francesi è curato da Giuseppe Scassellati dello studio Cleary Gottlieb, mentre dalla parte del Biscione c'è lo studio BonelliErede – sembrerebbero aprire uno spiraglio per un compromesso che ponga fine alla diatriba.

L'operazione consegnata da Mediaset sotto il profilo finanziario offre intelligentemente una via d'uscita a Vivendi che, tra buy-back, dividendo straordinario e rivalutazione delle azioni, potrebbe recuperare buona parte di quanto perso finora, considerato che il prezzo medio del rastrellamento era stato di 3,7 euro per azione, quasi un euro in più delle attuali quotazioni di Borsa. Una chance che – a quanto risulta – non sarebbe sfuggita al fronte francese che potrebbe puntare a uno stop loss sul 20% che per le autorità italiane non può detenere per resta-

re invece col rimanente 10% nella holding olandese e mantenere così un posto d'osservazione privilegiato sugli sviluppi del progetto "federativo" di Mediaset.

Ammesso che lo scenario sia praticabile – bisogna vedere anche cosa ne pensa la famiglia Berlusconi – Bolloré non vuole essere un azionista di serie B, privato dei diritti di voto e della possibilità di chiederne la maggiorazione.

Di qui l'istanza al Tribunale di Milano per recuperare i diritti di voto, che è la premessa per il riconoscimento in Olanda, visto che lo statuto della holding prevede espressamente che la maggiorazione possa essere richiesta solo da chi i voti "semplici" li può esercitare. L'atto di citazione – che Mediaset ieri ha confermato di aver ricevuto – chiede di annullare le delibere di assemblea e cda del Biscione che a metà aprile hanno approvato il voto doppio di diritto italiano e, in subordine, di accertare e dichiarare che Vivendi ha diritto a essere iscritta nell'apposito albo per il voto maggiorato (ma col trasferimento in Olanda questa parte sarà superata). Inoltre, e in ogni caso, di accertare e dichiarare che Vivendi può esercitare tutti i diritti sul 9,61% del capitale Mediaset direttamente detenuto e fornire istruzioni a Simon fiduciaria sul restante 19,19% per le operazioni straordinarie previste negli impegni depositati in Agcom.

© RIPRODUZIONE RISERVATA





Battaglia legale. È ripartito lo scontro fra Vivendi e Mediaset (in foto la sede)