

EL NINO PIÙ VIOLENTO
Nei prossimi 30 anni, a causa del riscaldamento globale il fenomeno climatico El Nino rischia di diventare molto più regolare e più violento.



COSA È KINDLE TRANSLATE?
È un servizio attualmente riservato a un gruppo selezionato di autori, che usa l’Ai per tradurre un’opera in altre lingue, automaticamente e gratuitamente.

Prove di resistenza digitale, cresce la nicchia anti big tech

Trend. Si moltiplicano app, smartphone e social alternativi rispetto ai grandi ecosistemi. Gli obiettivi sono riappropriarsi della privacy e della libertà di accesso alle informazioni

Claudia La Via

Semplicità di accesso, possibilità di essere sempre connessi, di avere tutto a portata di clic — foto, file, contatti, memoria: la rete ci semplifica la vita e la cataloga, tiene traccia dei nostri spostamenti, delle ricerche, della nostra “cronologia di vita”. Una promessa irresistibilmente comoda, ma anche inquietante. Da questa consapevolezza nasce una fuga silenziosa di chi prova a staccarsi dai grandi ecosistemi digitali per una rivendicazione di libertà: per non essere ridotto a un profilo, a un algoritmo o, peggio, a una previsione di comportamento.

Secondo il documento *Breaking Up with Big Tech* pubblicato lo scorso agosto da Amnesty International, le cinque aziende che controllano il mercato digitale — Google, Meta, Apple, Amazon e Microsoft — «stanno fissando i termini dell’esperienza digitale di miliardi di persone». Un potere che, spiega il documento, non è solo economico, ma anche politico e culturale perché definisce le regole dell’accesso all’informazione, orienta i consumi, condiziona il linguaggio con cui pensiamo la rete e ridefinisce, di fatto, la nozione stessa di privacy. Dalla sveglia dello smartphone al pacco tracciato in tempo reale, l’infrastruttura delle big tech attraversa ogni gesto quotidiano. Nessuno ci obbliga, ma uscire dal loro perimetro è sempre più difficile. Eppure cresce una piccola ma tenace controcorren-

te. E nel turismo, dove dominano Booking e Airbnb, emergono reti più eque come Fairbnb, che devolve parte delle commissioni a progetti locali, Socialbnb, che collega viaggiatori e iniziative sociali, o Ecobnb e Kindred, che promuovono ospitalità sostenibile e scambi tra privati. Un mosaico di soluzioni che dimostra come il “divorzio” da Big Tech non sia isolamento, ma il tentativo di costruire un ecosistema digitale diverso, più umano e condiviso. Non una crociata, ma un cambio di mentalità: scegliere servizi interoperabili, cancellare un account, installare un’app alternativa: piccoli gesti che diventano atti di “resistenza digitale” quotidiana.

Office. E nel turismo, dove dominano Booking e Airbnb, emergono reti più eque come Fairbnb, che devolve parte delle commissioni a progetti locali, Socialbnb, che collega viaggiatori e iniziative sociali, o Ecobnb e Kindred, che promuovono ospitalità sostenibile e scambi tra privati.

Un mosaico di soluzioni che dimostra come il “divorzio” da Big Tech non sia isolamento, ma il tentativo di costruire un ecosistema digitale diverso, più umano e condiviso. Non una crociata, ma un cambio di mentalità: scegliere servizi interoperabili, cancellare un account, installare un’app alternativa: piccoli gesti che diventano atti di “resistenza digitale” quotidiana.

Nuovi attori sul mercato.
A destra Jörg Wurzer, fondatore e direttore generale di Volla, società tedesca che realizza smartphone basati su software libero e filosofia minimalista. Crescono le soluzioni alternative alle big tech, come quelle proposte da Proton, Bluesky, Qwant e Signal



CYBER SECURITY e PROTEZIONE DATI Imprese alla sfida della Trasformazione Digitale

Crescono del 36% gli incidenti informatici nel 2025: l'Italia tra i paesi più esposti

Nel primo semestre del 2025, gli incidenti informatici hanno raggiunto un livello storico, con una crescita globale del 36% rispetto al semestre precedente, e l'Italia si posiziona tra i paesi maggiormente colpiti, rappresentando il 10,2% degli attacchi mondiali. La complessità e la frequenza di queste minacce stanno superando la capacità difensiva delle organizzazioni, con conseguenze che rischiano di travolgere l'intero sistema socio-economico. Come sottolinea Anna Vaccarelli, presidente di Clusit, «la difficoltà crescente nel difendersi porta a un aumento significativo dei rischi e, se questa tendenza dovesse consolidarsi, il problema rischia di espandersi coinvolgendo tutto il sistema organizzativo, industriale e sociale». Il Rapporto Clusit evidenzia inoltre un incremento di attacchi mirati nel nostro Paese a settori strategici, quali quello governativo, militare e delle forze dell'ordine, dei trasporti e della logistica, confermando l'urgenza di rafforzare la resilienza digitale su scala nazionale e globale.

INFORMAZIONE PROMOZIONALE



REEVO integra la sicurezza nel Cloud: Difesa intelligente 24/7

La trasformazione digitale sta agevolando l'adozione del Cloud da parte delle imprese. Questa tendenza ha accelerato l'uso di nuovi paradigmi di difesa abilitando strategie più efficaci di prevenzione, monitoraggio e risposta. Tuttavia, mentre le aziende affidano al Cloud processi mission critical, i Cloud provider tradizionali si assumono solo una parte limitata della responsabilità in tema di sicurezza, lasciando alle imprese l'onere di proteggere dati, accessi e applicazioni. In particolare il provider si occupa della protezione dell'infrastruttura fisica, ovvero delle reti, dei data center, degli spazi fisici e dei sistemi di base; invece l'azienda deve gestire la sicurezza delle applicazioni e dei dati. Questo modello definito “responsabilità condivisa” funziona solo se le organizzazioni sono pienamente consapevoli delle proprie responsabilità e hanno un team e le competenze necessarie allo scopo. Spesso però la consapevolezza è parziale e le risorse tecniche sono limitate, aggravando il rischio in un contesto di minacce in continua evoluzione.

Per questi motivi ReeVo ha adottato un approccio **Secure by Design** tramite il quale integra nativamente un layer di sicurezza in tutta l'offerta cloud, garantendo una protezione di base espandibile con servizi avanzati. Da questo approccio nasce **CyberDome** un sistema di protezione avanzato che analizza il traffico in ingresso e in uscita dai data center per rilevare le minacce in tempo reale e rispondere in modo automatico agli attacchi grazie all'integrazione con il SOC H24/7 e le funzionalità che bloccano IP malevoli o isolano workload compromessi. Con il Secure by Design di ReeVo puoi fare la scelta che rende la tua trasformazione digitale più sicura.

Scopri di più su: <https://www.reevo.it/it/secure-by-design>



NUTANIX rafforza la Sicurezza IT con Infrastrutture integrate e Cloud ibrido

La cybersecurity è oggi una priorità imprescindibile per le imprese italiane. Secondo il rapporto Clusit, l'Italia concentra il 10,1% degli attacchi informatici globali, mentre il 61% delle PMI non dispone di un piano di sicurezza aggiornato. La trasformazione digitale e l'adozione diffusa della GenAI accelerano processi e produttività, ma ampliano anche la superficie d'attacco. Oltre un terzo delle aziende italiane denuncia la mancanza di competenze digitali qualificate, mentre la crescita dei dati non strutturati complica la gestione e la protezione delle informazioni. In questo scenario, il 52% delle imprese ha aumentato gli investimenti in cybersecurity, puntando su piattaforme integrate per garantire una trasformazione digitale sicura. È qui che si inserisce la visione di **Nutanix**, che pone le infrastrutture cloud ibride al centro delle strategie di sicurezza, semplificando la gestione IT e promuovendo un approccio “security by design” dal core al cloud. Alla base di questa architettura c'è **Nutanix AOS**, la piattaforma software per infrastrutture iperconvergenti che integra funzioni di prevenzione, rilevamento e risposta alle minacce, assicurando continuità operati-



Nutanix. Sammy Zoghiani, SVP EMEA

va e protezione dei dati. Soluzioni come **Data Lens** permettono di identificare le minacce in meno di 20 minuti, riconoscendo oltre 5.600 firme di ransomware, mentre **Flow Network Security** introduce la microsegmentazione e i principi Zero Trust per contenere la propagazione del malware. Con **Unified Storage**, infine, backup immutabili e tecnologia WORM garantiscono integrità e compliance normativa. Tutti questi temi saranno affrontati il 18 novembre al **.NEXT On Tour Milano**, occasione unica per esplorare le ultime innovazioni in ambito cloud, sicurezza e resilienza digitale. - www.nutanix.com

vendor. Velocità di risposta, flessibilità progettuale e solidità operativa sono i pilastri che consentono all'azienda di affrontare un mercato in costante evoluzione. Oggi la sfida include la conformità normativa: NIS2, DORA e le implicazioni dell'AI Act ridefiniscono i confini di sicurezza e governance digitale. In questo scenario, tecnologie cloud native e architetture SSE diventano abilitatori chiave per garantire agilità, scalabilità e protezione in ecosistemi sempre più distribuiti. Wellcomm Engineering investe in in-



novazione e competenze per restare partner strategico nella costruzione di un contesto operativo sicuro, sostenibile e affidabile. www.wellcomm.it

Cybersecurity e Governance digitale: l'Expertise WELLCOMM a servizio delle Aziende

Wellcomm Engineering rappresenta la Business Unit Cyber di Sirti Digital Solutions, la Tech Company che abilita il passaggio dalla digital economy alla AI economy del Paese. Nell'era della trasformazione digitale, la sicurezza informatica non è più solo una necessità tecnica, ma un asset strategico per la competitività, la resilienza e la continuità operati-

va delle imprese. Da oltre 30 anni W.E. accompagna aziende italiane e internazionali nel governo della sicurezza, operando come System Integrator specializzato nella protezione di dati, infrastrutture e processi critici. Il modello Wellcomm parte dalla centralità del cliente, con soluzioni su misura costruite su competenze certificate e riconosciute dai principali

ALLNET.ITALIA e SYMBOLIC. Tecnologie e Formazione per una Sicurezza digitale consapevole

La sicurezza digitale è ormai uno degli snodi cruciali per imprese e istituzioni. Gli attacchi crescono in frequenza e sofisticazione, alimentati da reti criminali sempre più organizzate e da strumenti automatizzati che abbassano la soglia di accesso anche per attori meno esperti. Eppure, nonostante la disponibilità di tecnologie sempre più avanzate, l'anello debole rimane il fattore umano. Molti studi confermano che la maggior parte delle violazioni nasce da errori di comportamento: password deboli, man-

canza di aggiornamenti, scarsa consapevolezza nelle procedure quotidiane. È qui che emerge la vera emergenza: la mancanza di competenze diffuse. Senza cultura della sicurezza, anche i sistemi più sofisticati rischiano di rimanere inefficaci. In questo scenario si inseriscono esperienze italiane che cercano di colmare il divario tra innovazione tecnologica e conoscenza. **Allnet.it**, distributore ICT a valore aggiunto, lavora da anni per integrare



nei propri servizi non solo soluzioni avanzate ma anche competenze, favorendo un approccio che mette la sicurez-

za al centro della trasformazione digitale. Accanto ad essa opera la società controllata **Symbolic**, interamente dedicata alla cyber security, che si distingue per la capacità di affiancare alle tecnologie percorsi di formazione specifici per imprese e professionisti. Il messaggio che emerge è chiaro: la protezione dei dati non può più essere considerata un obbligo normativo o un costo da sostenere, ma un investimento strategico. Solo coniugando strumenti affidabili, responsabilità condivisa e preparazione continua sarà possibile costruire un ecosistema digitale resiliente e sostenibile. www.allnet-italia.it - www.symbolic.it

BREVI

SCIENZA/1

Come si misura il ghosting

Interrompere bruscamente una relazione amorosa, amicale o professionale sparendo come un fantasma (il cosiddetto ghosting) può fare più male di un rifiuto esplicito: lo indica uno studio degli psicologi dell'Università di Milano-Bicocca, il primo a misurare sperimentalmente le reazioni psicologiche in tempo reale (mentre le ricerche precedenti erano basate per lo più su ricordi o immaginazione). I risultati sono pubblicati sulla rivista *Computers in Human Behavior*. I ricercatori hanno arruolato un gruppo di volontari chiedendo loro di partecipare a brevi conversazioni quotidiane via chat con un partner (un collaboratore dello studio) per poi compilare ogni giorno un questionario sulle proprie emozioni e percezioni. A metà dell'esperimento, alcuni partecipanti sono stati improvvisamente ignorati (simulando un episodio di ghosting), mentre altri hanno ricevuto un rifiuto esplicito o hanno continuato a dialogare normalmente. Questo approccio, unico nel suo genere, ha consentito di monitorare l'evoluzione quotidiana del disagio emotivo e di evidenziare come il silenzio prolungato del ghosting produca effetti più duraturi rispetto a un rifiuto diretto. I risultati dell'esperimento mostrano che l'interruzione di una relazione è dolorosa, a prescindere dalla modalità tramite cui avviene. Tuttavia, il rifiuto esplicito genera una reazione emotiva intensa ma più immediata e breve, seguita da un progressivo recupero. Il ghosting, invece, lascia le persone in uno stato di incertezza e confusione prolungata, che ostacola l'elaborazione dell'esperienza e mantiene elevate nel tempo stati negativi come dolore e senso di esclusione. —**L.Tre.**

SCIENZA/2

Da un fungo la memoria di un pc

Ottenuta la prima memoria vivente di un computer, utilizzando il micelio di una varietà di funghi molto diffusa in Cina e in Giappone. Il risultato, che potrebbe essere il primo passo verso un'alternativa economica ai chip, si deve alla ricerca pubblicata sulla rivista *Plos One* dal gruppo della Ohio State University guidato da John LaRocco. Utilizzando i funghi shiitake (*Lentinula edodes*), considerati robusti e resistenti allo stress, i ricercatori hanno costruito memristori funzionanti, ossia dispositivi in grado di ricordare gli stati elettrici passati. In particolare hanno utilizzato il micelio, ossia la rete di filamenti simile a una radice che si estende nel sottosuolo in una fitta rete per assimilare sostanze nutritive. I ricercatori hanno utilizzato il micelio perché in esso viaggiano informazioni attraverso segnali elettrici e chimici, come avviene nel cervello. «Essere in grado di sviluppare microchip che imitano l'attività neurale reale significa non aver bisogno di molta energia per lo standby o quando la macchina non è in uso», afferma lo psichiatra John LaRocco, coordinatore della ricerca. Questo risultato, osserva, «può rappresentare un enorme potenziale vantaggio computazionale ed economico». —**L.Tre.**