G L /X Q H Gu I H E E U D L R

Sommario Rassegna Stampa

CORRIERE DELLA SERA

Quotidiano Data 06-02-2023
Pagina 2
Foglio 1

L'intervista

«Colpiti sistemi molto diffusi Chi non li aveva aggiornati ha aperto la porta all'assalto»

L'esperto di sicurezza: così hanno agito i cyber criminali

ROMA «Già due anni fa la casa madre Vmware, e quindi la linea di prodotto ESXi, ha scritto ai clienti di utilizzare le *patch* di aggiornamento, ma a oggi molte aziende non l'hanno fatto. Un po' di sano allarmismo non fa mai male in questo campo, però bisogna tenere presente che gli hacker stanno scansionando il web alla ricerca di obiettivi da colpire». A spiegare quello che sta accadendo è Remo Marini, presidente della Fondazione F3rm1, che si occupa di ricerca e sviluppo nell'ambito della cybersecurity e dell'innovazione tecnologica.

Chi c'è dietro questi attacchi?

«Due gruppi cyber criminali, Black Basta (che ha già colpito Acea, *ndr*), di origine russa, e ESXiArgs, che potrebbe trattarsi di una joint venture fra criminalità russa e cinese. Hanno sviluppato un tool, ovvero un sistema automatico, che sfrutta le vulnerabilità dei server e inietta un malware: così cercano le vittime sul web per colpirle».

Al momento chi è più a rischio?

«Per sfruttare la vulnerabilità bisogna trovarsi di fronte a due errori commessi dai dipartimenti di *information technology* delle aziende. Innanzitutto non aver aggiornato i sistemi usando le *patch* fornite dalle aziende produttrici. Inoltre aver esposto direttamente su internet senza protezioni di sicurezza, i servizi vulnerabili, rilevabili così attraverso le scansioni degli hackers attaccanti».

Perché tutto è partito dalla Francia?

«Proprio perché sono state rilevate le vulnerabilità a seguito delle non corrette procedure di sicurezza da parte dei clienti del provider Ovh. Non sono stati utilizzati i sistemi di sicurezza raccomandati e gli hacker hanno potuto dilagare. È accaduto il 3 febbraio scorso, sono bastati due giorni per scatenare il panico. Del resto i due sistemi in questione sono molto diffusi, non c'è ditta che non li usi: ottimizzano l'utilizzo delle risorse informatiche, permettendo quello di più sistemi contemporaneamente in un unico server fisico. Improponibile al giorno d'oggi, anche a livello economico, non usare macchine virtuali. L'importante, come detto, è aver una gestione dei sistemi orientata alla sicurezza e con relativi piani di *patching*».

L'intenzione degli hacker è solo chiedere un riscatto?

«Una volta entrati in un sistema possono fare ciò che vogliono, dalla gestione dei sistemi all'esfiltrazione dei dati o la loro criptazione».

Secondo lei, c'è un collegamento con la guerra in Ucraina?

«Non penso, questi sono criminali. C'erano anche prima. Sono russi ma rimbalzano da una parte all'altra del mondo: usano sistemi *command&control* per gestire le *botnet*, ovvero i pc infetti. La loro "firma" si scopre proprio dall'analisi di questo modo d'agire».

Quale altro sistema ha un'azienda per proteggersi?

«Affidarsi a uno specialista in cybersicurezza. Soprattutto oggi per i rischi che si corrono e come evolvono in maniera molto rapida. Bisogna capire che adesso sei mesi in questo settore corrispondono a un'era geologica. Leggere costantemente come si muovono i gruppi criminali è fondamentale».

R.Fr.

Chi è
Remo Marini, 47 anni, presidente della Fondazione F3RM1 che si occupa di sicurezza cibernetica

> È partito tutto dalla Francia perché un fornitore non ha utilizzato i sistemi di sicurezza raccomandati


Attacco hacker nel mondo
Violati migliaia di server
«Colpiti sistemi molto diffusi Chi non li aveva aggiornati ha aperto la porta all'assalto»

159329

L'Economia
del CORRIERE DELLA SERA

Settimanale Data 06-02-2023
Pagina 23
Foglio 1 / 3

CYBERSICUREZZA
TRE GUERRE DA VINCERE E L'ITALIA PROTAGONISTA

L'Europa è in una posizione di leadership con un set di norme che prevedono anche certificazione e responsabilizzazione dei top manager aziendali
Il nostro Paese non era tra i più virtuosi, ma col Pnrr sta facendo grandi passi

di **Daniele Manca** e **Roberto Viola**

L'attacco informatico con richiesta di riscatto alla Royal Mail, le poste inglesi, è arrivato nella seconda metà di gennaio. E le conseguenze si stanno allungando. È forse stato uno degli episodi più eclatanti delle scorse settimane a far tornare il tema della cybersicurezza al centro delle preoccupazioni di aziende e semplici cittadini. Ancora una volta, è decisivo, nell'era digitale, saper riconoscere i rischi della tecnologia per poterli prevedere e contenere. E non certo perché il digitale debba essere sinonimo di mondo sempre più incerto ed insicuro. Da un lato esiste una realtà di transazioni che sono parte di sistemi totalmente decentralizzati, come abbiamo visto nell'articolo del 23 gennaio scorso su *L'Economia* sulle criptovalute. Ma dall'altro la conoscenza del problema permette alle grandi istituzioni, come l'Ue, di poter intervenire a difesa dei cittadini e delle aziende, non solo delineando direttive, regole, e misure alle quali attenersi, ma anche rafforzando la protezione delle infrastrutture critiche come ad esempio le reti elettriche e di comunicazione, le banche o gli ospedali.

Tutte le teste

Tutti i prodotti immessi sul mercato devono essere cyber-sicuri. Purtroppo oggi questo non sempre è garantito. Abbiamo sempre più oggetti connessi in casa. Lo scorso giugno la polizia postale ha smantellato una rete criminale che vendeva immagini catturate illegalmente negli appartamenti di ignari cittadini. Per questo l'Ue si è attivata detenendo – ancora una volta – la leadership mondiale nella regolamentazione della cybersicurezza dei prodotti. A settembre scorso è stato presentato il nuovo Cyber Resiliente Act (Cra). Il Cra fa subito una distinzione tra prodotti a basso e ad alto rischio informatico. I primi possono essere autocertificati. Per i secondi è prevista una certificazione esterna che avviene tramite laboratori accreditati. Abbiamo visto durante il Covid quanto fosse importante la certificazione di un prodotto come le mascherine. Nel futuro, i prodotti immessi in Europa avranno bisogno della certificazione per poter circolare all'interno del mercato unico. Dovranno dunque essere effettuati degli aggiornamenti periodici nella vita del prodotto, individuando e registrando costantemente le possibili vulnerabilità.

Come le molteplici teste dell'idra, esistono tre diversi livelli di at-

tacchi informatici contro cui ci ritroviamo a combattere. Il più immediato sono sicuramente le email. L'Europa ha coniato il termine igiene informatica attraverso diverse campagne informative per impiantare il riflesso istintivo di essere digitalmente cauti, ad esempio nella scelta della propria password o nel prestare maggiore attenzione alle email in odore di truffa. Una sorta di attacchi ingegnerizzati socialmente, sempre più verosimili alle email ufficiali di aziende ed enti. Una prova l'abbiamo avuta durante il Covid con l'esperienza della regione Lazio.

La seconda categoria di attacchi informatici è molto più sofisticata ed organizzata. Si tratta degli attacchi come i *ransomware*. Si entra nel sistema di un ente o azienda o istituzione e si chiede un riscatto, se si vogliono evitare danni. Si ha ragione di credere che questo tipo di operazioni siano molto più frequente di quello che viene dichiarato. Ammettere di essere stati soggetti ad un attacco informatico può intaccare la reputazione di un'azienda. Queste incursioni possono anche degenerare, portando a grandi incidenti come, ad esempio, quello dell'hackeraggio di SolarWinds negli Stati Uniti.

L'ultima testa dell'Idra consiste invece in quegli attacchi sponsorizzati o organizzati da Stati ostili dove gli attaccanti sono gli attori pubblici con scopi offensivi, bellici e tattici. Un campo dove autentiche guerre informatiche si verificano in modo più o meno esplicito. La lezione più importante che ci ha però lasciato la pandemia è la consapevolezza che una crisi sanitaria – così come un attacco informatico – non conosce confini nazionali. Ha ripercussioni che coinvolgono quasi contemporaneamente più Stati. Cosa che stiamo vedendo con il conflitto in Ucraina.

Nella strategia europea per la cyberdifesa comune presentata lo scorso novembre il punto chiave per affrontare questo tipo di crisi è attivare una strategia comune europea basata sull'unione delle forze, la cooperazione e sull'alta tecnologia, anche con gli strumenti avanzati che sono stati messi in pista dall'Europa – quali un sistema satellitare sicuro e la comunicazione quantistica, che offre una crittografia intrinsecamente sicura. Bisogna lavorare insieme per sconfiggere minacce comuni, non esistono alternative.

Come rispondere? Con la triade che governa la cybersicurezza in Europa. Un'altra importante lezione che ci viene dalla pandemia e che possiamo applicare alla cybersicurezza è l'importanza dell'individuare il punto di rischio e di vulnerabilità per poter restringere il campo d'azione e prevedere l'attacco informatico e la sua propagazione. Questo permette alle aziende di avere dei sistemi informativi preparati e pronti a rispondere velocemente. Tuttavia, non è sufficiente. La sicurezza informatica deve essere presa sul serio dalle aziende.

La legge fondamentale che regola la cybersecurity in Europa si chiama direttiva Nis (network and information system security). Nella profonda revisione operata lo scorso anno è significativo che si richieda esplicitamente la responsabilizzazione del top management all'interno delle aziende e una particolare attenzione alle catene di approvvigionamento in termini di prodotti che non introducano rischi informatici. E questo con l'introduzione di sanzioni nel caso in cui le aziende non facciano il proprio dovere, soprattutto nei settori più critici.

La triade di norme che governa la cyber security in Europa è composta dalla direttiva Nis, il futuro regolamento sulla sicurezza informatica dei prodotti (Cra) di cui abbiamo parlato sopra, e dal Cybersecurity Act (Csa).

Il Csa introduce procedure per certificare la qualità di determinanti prodotti e servizi particolarmente rilevanti sul piano della sicurezza informatica soprattutto per quanto riguarda i sistemi complessi, come il cloud, ma anche i chip, le smart card che si usano nei documenti, e così via.

Il fattore umano, l'imprudenza o imperizia del personale preposto alla sicurezza è stata la causa per cui tanti recenti attacchi hanno purtroppo avuto successo. Per questo mettere in sicurezza prodotti e servizi non basta. Il personale che opera nell'ambito dei sistemi informativi di un ospedale, nei settori produttivi più delicati per la sicurezza delle persone o di aziende impegnate nei servizi di pubblica utilità, deve poter possedere delle competenze che siano verificabili e rilasciate da enti autorizzati allo scopo. Per pilotare un aereo non basta un corso on-line, bisogna prendere un brevetto. Un quadro europeo per educare ed affermare operatori della cybersicurezza è uno snodo fondamentale.

L'Ue si sta già muovendo in questa direzione. Il 2023 sarà l'anno europeo delle competenze digitali la cui carenza è plateale. A livello nazionale, l'Italia non era di certo nel gruppo di testa quando è cominciata l'avventura europea della cybersicurezza, ma è stato un allievo che ha appreso rapidamente. Oggi possiamo disporre di un'Agenzia per la cybersicurezza nazionale che si è distinta a livello europeo e che anche grazie al Pnrr dispone di risorse per l'utilizzo di tecnologie più avanzate nel settore come l'uso di intelligenza artificiale e super calcolo: ad attori tecnologici sofisticati bisogna rispondere con tecnologia ugualmente sofisticata. Questa è la sfida forse più importante.

Non bastano norme, comportamenti virtuosi e prevenzione, serve la tecnologia: soprattutto l'intelligenza artificiale e le tecnologie quantistiche. È grazie a questi tipi di strumenti e potenza di calcolo che un comportamento informatico anomalo può essere reso evidente anche in pochissimo tempo. La priorità europea è quindi quella di investire in una rete di centri di sicurezza avanzati interconnessi fra loro che creeranno una sorta di scudo informatico europeo. Con questo modello è stata creata la rete di supercomputer europei, e come nel supercalcolo anche nei sistemi di cybersicurezza avanzati l'Italia ha le carte in regola per essere protagonista.

ItaliaOggi Sette

Settimanale Data 06-02-2023
Pagina 44
Foglio 1

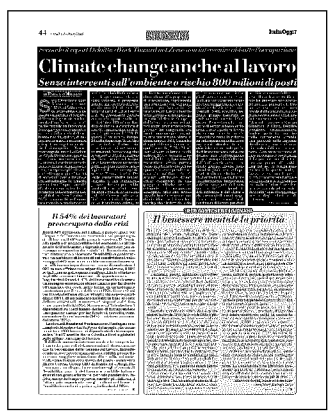
Secondo il report Deloitte «Work Toward net Zero» non intervenire abbatte l'occupazione

Climate change anche al lavoro

Senza interventi sull'ambiente a rischio 800 milioni di posti

DI FABRIZIO MILAZZO

Sono 800 milioni i posti di lavoro, pari a circa il 25% dell'attuale forza lavoro globale, altamente vulnerabili al cospetto dell'ormai imperante cambiamento climatico e al suo inevitabile impatto sull'economia. Non agire preventivamente a sostegno della tutela dell'ambiente rischia, quindi, di rallentare la crescita economica e impattare negativamente i livelli di occupazione. È quanto emerge dal report di Deloitte «Work Toward net Zero» in cui si dimostra come affrontare, invece, il cambiamento climatico con una transizione attiva, sinergica e globale consente di raggiungere il target di emissioni zero e favorisce contestualmente la crescita economica e l'espansione del dividendo occupazionale. La riduzione delle emissioni nette globali a "zero" entro il 2050 potrà cambiare l'economia mondiale, trasformando anche il ruolo della forza lavoro. Intraprendendo tale percorso virtuoso, si prospetta, infatti, una crescita dell'economia mondiale di circa 43 mila miliardi di dollari entro il 2070, prevenendo perdite economiche quattro volte superiori (circa 178 mila miliardi di dollari) e la creazione di oltre 300 milioni di posti di lavoro in più entro il 2050. Di questi, 21 milioni in Europa, 26 nelle Americhe, 75 in Africa e 180 in Asia. «La transizione attiva verso il net-zero rivoluzionerà l'economia globale con le attività ad alta intensità di emissioni e i relativi posti di lavoro che verranno impattati in base a nuove tecnologie e industrie emergenti» osserva Franco Amelio, Deloitte sustainability leader, «rispetto a una transizione passiva, che comporterebbe un disallineamento tra competenze e posti di lavoro e impedirebbe la crescita dei settori a basse emissioni, il percorso di transizione attiva, se realizzato con idonee politiche ambientali e programmi di innovazione, rappresenta una situazione win-win per il clima e per l'economia. Da una parte, si riducono le emissioni globali e si mitigano gli impatti del climate change, e, dall'altra, si creano nuovi settori, nuovi lavori e nuove competenze. Se comparata con una transizione passiva, sotto una transizione attiva si stima che solo USA, Cina e India potrebbero generare, rispettivamente, 5, 38 e 74 milioni di posti di lavoro in più entro il 2050». Secondo il report di Deloitte, il percorso di transizione attiva porterà verso una forza lavoro più responsabile, consapevole e ancora più qualificata che gli analisti definiscono «Green collar workforce». In tale gruppo si collocheranno sia categorie di occupazioni emergenti della new economy, che beneficeranno in modo significativo dei cambiamenti globali indotti dalla decarbonizzazione, sia tipologie di lavoro appartenenti alla old economy che risulteranno essere maggiormente esposte ai rischi climatici e ambientali. Nello specifico, nel primo gruppo rientrano le professioni altamente richieste con l'emergere e l'espansione di settori a basse emissioni, i nuovi posti di lavoro che emergeranno durante la transizione verso la riduzione delle emissioni nette, le occupazioni attualmente esistenti che, nel corso del periodo di transizione ecologica, vedranno una trasformazione dei propri requisiti e della modalità di svolgimento. Il secondo gruppo, invece, comprenderà professioni collegate ad attività con alta intensità di emissioni che subiranno un'interruzione temporanea o definitiva e posti di lavoro con attività dipendenti dall'ambiente e dal clima e che saranno influenzati negativamente in termini sia di condizioni di lavoro più dure sia di interruzione delle attività. «Il cambiamento climatico ha generato uno scenario in cui le persone e le loro competenze non saranno create dall'economia, ma saranno esse stesse a condurre la transizione e a dar vita al futuro del lavoro» aggiunge Gianluca Di Cicco, Deloitte workforce transformation leader, «pertanto, investire nelle competenze diventa una priorità delle imprese che devono pensare ad azioni mirate e calibrate sul contesto. Non sarà richiesto di fare un completo re-training delle persone, ma di intraprendere percorsi di up-skilling del set di competenze esistenti. In questo modo, i lavoratori avranno la possibilità di mantenere l'attuale occupazione e le imprese potranno beneficiare di una forza lavoro pronta ad essere indirizzata verso il raggiungimento degli obiettivi di net-zero».


Climate change anche al lavoro
Senza interventi sull'ambiente a rischio 800 milioni di posti
Il 54% dei lavoratori preoccupato dalla crisi
Il benessere mentale la priorità

Il Sole 24 ORE

Quotidiano Data 06-02-2023
Pagina 11
Foglio 1

PANORAMA

IL BILANCIO

Tregua fiscale, Casse schierate per il no

La rottamazione delle cartelle non piace alle Casse dei professionisti: alla proposta di stralciare i debiti previdenziali sotto i mille euro hanno detto «no» tutti gli enti di previdenza privati, mentre solo poche Casse hanno deciso di permettere la definizione agevolata.

Una chiusura totale che sembra lasciare poco spazio a una eventuale riapertura dei termini: il Governo ha infatti depositato un emendamento al decreto Milleproroghe (non ancora approvato) che riaprirebbe le possibilità di adesione, spostando la scadenza dal 31 gennaio al 31 marzo per le decisioni delle Casse. Ma dopo un «no» così compatto di tutti gli enti una marcia indietro sembra difficile.

Gran parte delle Casse ha scelto di non consentire ai propri iscritti morosi alcun tipo di sanatoria: oltre alla chiusura totale verso il saldo e stralcio dei debiti sotto i mille euro, in poche, infatti, consentiranno la rottamazione delle cartelle affidate alle Entrate dal 2000 al 30 giugno 2022, pagando solo la quota capitale (di fatto i contributi). La chance sarà possibile per avvocati, biologi, giornalisti, ragionieri e veterinari che potranno fare domanda alle Entrate entro il 30 aprile (salvo proroghe del termine al momento in discussione in Parlamento).

La strada della rottamazione, invece, è preclusa agli altri, compresi commercialisti, architetti e ingegneri, notai, attuari, chimici, fisici e geologi. Le casse di questi professionisti infatti hanno optato per la non adesione alla nuova sanatoria. Altre categorie, come i consulenti del lavoro, i periti industriali o gli psicologi, non potranno comunque partecipare, in quanto non affidano la riscossione delle cartelle all'agenzia delle Entrate.

—V.Uv.


Professioni 24

Per l'equo compenso importi vecchi e incompleti

Il Sole 24 ORE

Quotidiano Data 06-02-2023
Pagina 1
Foglio 1 / 5

Primo Piano
I movimenti migratori

I DATI DEL VIMINALE: +2,2% NEL 2022

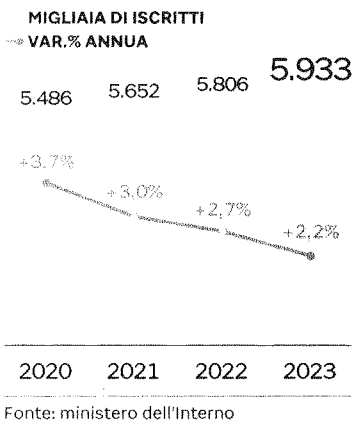
In sei milioni dall'Italia all'estero Bassa padana, uscite in crescita

Sono 5,93 milioni gli iscritti all'Anagrafe degli italiani all'estero al 1° gennaio 2023. I dati aggiornati, anticipati dal ministero dell'Interno, certificano un aumento del 2,2% delle fughe all'estero durante lo scorso anno, anche se il trend è rallentato dopo la pandemia. A emigrare di più sono ancora i giovani. Mantova è la provincia di origine da cui crescono di più le iscrizioni, ma l'impatto più significativo dell'esodo resta al Sud.

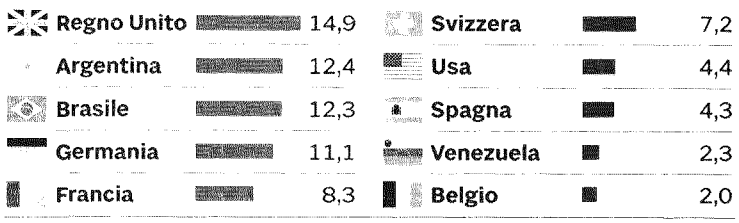
Casadei e **Finizio**

—*a pagina 6*

GLI ISCRITTI ALL'AIRE
Dati al 1 gennaio



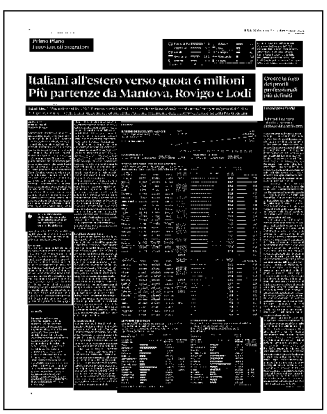
Fonte: ministero dell'Interno



Fonte: Italiani nel mondo - Migrantes

LE DESTINAZIONI PIÙ RECENTI
A gennaio 2022 erano 197.406 gli italiani iscritti da meno di un anno all'Anagrafe degli italiani all'estero. I primi Paesi di destinazione delle emigrazioni più recenti sono Gran Bretagna, Argentina, Brasile, Germania e Francia (in percentuale sul totale).


Lavoratori extra Ue, più posti e più settori


Italiani all'estero verso quota 6 milioni
Più partenze da Mantova, Rovigo e Lodi