Investimenti venture cap in cybersecurity ai massimi storici, 15 miliardi di dollari attesi per il 2021

Il 2020 si è chiuso con un volume record di investimenti *venture capital* (VC) nel mercato delle imprese di **cybersecurity**, con 665 accordi a livello globale e una spesa complessiva di **7,8 miliardi di dollari**.

Venture cap per la cybersecurity globale

Si tratta di fondi di investimento specializzati nel settore della cybersecurity, che hanno aumentato la propria capacità di spesa al seguito dell'incremento della domanda di sicurezza informatica, proveniente proprio dal mondo delle imprese e dell'industria, in particolare, ma anche da quello della finanza e delle banche.

La pandemia di **Covid-19** ha cambiato drasticamente il modo di lavorare, di effettuare la formazione, di portare avanti le relazioni sociali e professionali, esponendo le imprese a sempre nuovi e più minacciosi attacchi informatici.

Secondo il rapporto "***Rise Of Global Cybersecurity Venture Funding***", pubblicato da Crunchbase, solo negli Stati Uniti **la spesa degli investitori in sicurezza informatica è cresciuta del +22% nel 2020**.
L'accordo più rilevante a riguardo è stato quello chiuso a 340

milioni di dollari per Netskope.

Nel 2018 si è registrato il più alto numero di accordi degli ultimi 10 anni, ben 729 (il 10% in più rispetto al 2020), ma a fronte di un volume di investimenti VC di 5,3 miliardi di dollari, il 50% in meno di quanto speso nel 2020.

Geografia degli investimenti

"*A seguito dell'aumentare degli attacchi informatici che continuano a minacciare le imprese e le amministrazioni pubbliche, mettendo a repentaglio non solo la sicurezza delle stesse organizzazioni, ma anche la privacy dei singoli cittadini, è divenuto un imperativo investire in cybersecurity per qualsiasi industria o Governo*", si legge nel commento ai dati del Rapporto.

Misura di questa nuova fase espansiva degli investimenti in aziende di cybersecurity è la **nascita di nove nuovi unicorni negli Stati Uniti (società valutate oltre 1 miliardo di dollari) nel 2021**, che si aggiungono ai sei registrati nel 2020.

Il 90% di tutti i finanziamenti VC in cybersecurity sono stati destinati a imprese americane e israeliane, durante l'anno passato, con le prime che hanno raccolto 5,9 miliardi di dollari, il 76% del totale, e le secondo poco più di un miliardo di dollari. Circa 262 milioni di dollari, o il 3% del totale, invece, è stato destinato ad aziende britanniche.

Nuovo record di spesa per il 2021

Nei primi mesi del 2021 sono state concluse diverse transazioni, per un valore complessivo di 3,7 miliardi di dollari a livello mondiale.

Secondo lo studio, è possibile attendersi **investimenti VC in cybersecurity per oltre 15 miliardi di dollari entro la fine**

del 2021, con particolare concentrazione nei settori delle biotecnologie (45 miliardi di dollari circa stimati), della fintech (27 miliardi di dollari), del settore immobiliare (9 miliardi di dollari) e della robotica/automazione (8,6 miliardi di dollari).

https://www.key4biz.it/investimenti-venture-cap-in-cybersecurity-ai-massimi-storici-15-miliardi-di-dollari-attesi-per-il-2021/355720/

Phishing. R. Cazzola (Trust Italia): “In arrivo per le email il VMC per certificare il mittente”. Come il badge blu su Twitter

Se i siti fraudolenti sono “l’esca” per farci abboccare al phishing, “l’amo” è lanciato, spesso, via email. Per evitare che il phishing arrivi attraverso la posta elettronica, *“tra un paio di mesi sarà disponibile la soluzione Verified Mark Certificates (**VMCs**)”,* ha sottolineato **Riccardo Cazzola**, ceo di **Trust Italia**, nella videointervista trasmessa, in live streaming, questa mattina da **Key4biz**.

La videointervista

[embedded content]

Come funziona Verified Mark Certificate per certificare con un logo il mittente delle email

“Il Verified Mark Certificate permetterà”, ha spiegato Cazzola, *“di visualizzare su tutti i client di posta elettronica, che utilizzeranno il nuovo protocollo, il brand dell’azienda certificata. Nella lista delle email in arrivo, prima di aprirle, vedremo un logo per indicare, in modo immediato, che il mittente dell’email corrisponda realmente a quello indicato”.*

Ecco 3 esempi. Accanto al nome mittente dell’email il logo di Comcast, CNN e Groupon

Il Verified Mark Certificate è l’equivalente del segno di spunta blu utilizzato da **Twitter** per indicare un profilo-utente verificato e come il badge verificato su **Instagram**. Ecco 3 esempi. Accanto al nome mittente dell’email il logo di **Comcast**, **CNN** e **Groupon**.

In fase di test negli Usa

“Il Verified Mark Certificate”, ha concluso **Riccardo Cazzola**, ceo di **Trust Italia,** azienda specializzata nei certificati SSL, *“potrà essere utilizzato dalle aziende titolari di un marchio registrato e che noi potremo verificare nel processo di rilascio dell’VMC. È in fase di test negli USA e* ***Google****, per esempio, lo sta sperimentando in* ***Gmail****: il servizio sarà disponibile in un paio di mesi”.*

Key4biz oggi con Riccardo Cazzola ha aperto un filone interessante su sicurezza online, pagamenti digitali e strategie contro il phishing. È un tema che tocca da vicino ognuno di noi e per questo ne parleremo in modo più

approfondito in un webinar che si terrà prossimamente. Vi faremo conoscere la data e l'agenda con i relatori.

Per vedere l'intervista

GUARDA SU YOUTUBE

[embedded content]
https://www.key4biz.it/phishing-r-cazzola-trust-italia-in-arrivo-per-le-email-il-vmc-per-certificare-il-mittente-come-il-badge-blu-su-twitter/355679/

Gabrielli: "Modificare Dpcm del perimetro sicurezza cibernetica. Si rischia legge inapplicabile da aziende"

Oltre a proporre "*un'Agenzia ad hoc per gestire in modo olistico la sicurezza cibernetica, che non può essere più affidata al Dis*", come affermato in esclusiva a **Cybersecurity Italia**, **Franco Gabrielli**, Sottosegretario alla Presidenza del Consiglio con delega all'Intelligence, auspica anche una revisione del Dpcm che disciplina il perimetro di sicurezza nazionale cibernetica: lo "scudo" governativo dagli attacchi informatici per proteggere circa 150 infrastrutture critiche del Paese, tra enti pubblici, aziende statali e private.

Sulle regole in caso di attacchi informatici alle aziende inserite nel perimetro di sicurezza nazionale, per Gabrielli "*Dobbiamo stare in ascolto delle esigenze dei soggetti destinatari. Altrimenti facciamo editti, grida manzoniane. E ci confermiamo il Paese delle leggi perfette rivelatesi inapplicabili".* Il Sottosegretario alla Presidenza del Consiglio con delega all'Intelligence l'ha dichiarato nel corso del convegno "*Le Nuove Reti per l'industria italiana e per i consumatori",* che si è svolto l'8 aprile a Roma.

Il videointervento di Franco Gabrielli nel panel con Adolfo Urso, Vicepresidente Copasir, e Stefano Mele, Comitato Atlantico Italiano

[embedded content]

Quale processo si attiva in caso di incidente o attacco informatico alle aziende nel perimetro di sicurezza cibernetica?

Il riferimento di Gabrielli è alla norma nel Dpcm, secondo la quale, il caso di incidente, l'azienda violata è tenuta a informare, entro 6 ore al massimo (e non, come previsto dalla direttiva europea Nis, entro le 24 ore successive dal malfunzionamento) il **Csirt** (Computer security incident response team) cioè il gruppo di esperti istituito presso il Dis. Quando l'intrusione è grave, si attiva il Nucleo per la sicurezza cibernetica, che propone al presidente del Consiglio delle ipotesi di risposta all'attacco e coordina il ripristino

del servizio.

1,5 milioni di euro se non comunicano l'incidente o attacco informatico

I soggetti inseriti nel perimetro di sicurezza nazionale cibernetica **rischiano sanzioni fino a 1,5 milioni di euro se non comunicano l'incidente o attacco informatico**.

"Il Dpcm che andrà ora all'analisi parlamentare", ha aggiunto Gabrielli nel suo intervento al convegno, "*fortunatamente, stabilisce un tempo di sperimentazione*", durante il quale, si augura il sottosegretario la norma possa essere migliorata.

Il Nucleo per la sicurezza cibernetica è composto da tutti gli attori nazionali dell'architettura cyber: delegati del Dis, di Aise e Aisi, dei ministeri, dell'Agenzia per l'Italia digitale, della Protezione Civile, della Postale e il consigliere militare del premier.

Un'Agenzia come la francese ANSSI

E per quanto riguarda la gestione della cybersecurity, secondo Franco Gabrielli è l'ora di creare un'Agenzia ad hoc, come, per esempio, quella francese **ANSSI** (National Agency for the Security of Information Systems). Ha motivato così la sua proposta.

"Dal 2017 il comparto dell'Intelligence ha svolto una funzione importante, anche se a mio avviso di supplenza, come la definizione del perimetro di sicurezza cibernetica, il Centro di valutazione e certificazione nazionale (CVCN), di certo è stato fatto molto".

Ma ora per Gabrielli bisogna concepire un'Agenzia *"fuori dal comparto dell'Intelligence, perché quest'ultima si occupa di*

un aspetto, ma non della complessità della resilienza cibernetica”.

“*Credo*”, ha detto il sottosegretario con delega ai servizi di informazione e sicurezza, nella videointervista in esclusiva a **Cybersecurity Italia**, “*sia arrivato il tempo di creare una struttura, un’Agenzia che tratti in maniera olistica il tema della sicurezza cibernetica e della crescita culturale in questo settore. Dobbiamo affrancarci da una modalità emergenziale ed affrontare il tema in modo più strutturale e ordinario*”.

https://www.key4biz.it/gabrielli-modificare-dpcm-del-perimetro-sicurezza-cibernetica-si-rischia-legge-inapplicabile-da-aziende/355066/

This Data Privacy Filter Can Help Protect Your Small Business From Cybercrime

Small businesses are frequent cybercrime targets. Protect yours today.

April 11, 2021 2 min read

Disclosure: Our goal is to feature products and services that we think you’ll find interesting and useful. If you purchase them, Entrepreneur may get a small share of the revenue from the sale from our commerce partners.

When it comes to small businesses and cybercrime, the statistics are frightening. Forty-three percent of all cyber attacks worldwide target small businesses, and 60 percent of small businesses that are victims of a cyber attack go out of business within six months. Cybercrime costs businesses more than $2.2 million every year and, in 2019, there was a 424 percent increase in new small-business cyber breaches. Simply put, the digital world is dangerous for entrepreneurs.

Of course, that’s not going to stop you trying to push your business to the top, so you might as well take some precautions. For instance, the Winston Privacy Filter.

[embedded content]

Winston is a plug-and-play device that gives you control over your digital privacy. Unlike VPNs, anti-malware, and other subscription cybersecurity products, with Winston, you only pay once and you’re covered whenever you plug in. Not only does Winston cloak your location and identity from anyone creeping on your network, but it also blocks malware and adult content, filters out ads and trackers, and more. The end result is a cleaner, faster, more secure browsing experience that keeps your small business safe.

Winston works on every device in your home or office, from computers and smart TVs to tablets. You can protect mobile devices with the iOS and Android apps and encrypt your internet to prevent hacks and identity theft. Winston uses smart cloaking to route high-risk traffic over a zero-logging, proprietary distributed Privacy Mesh network, making it extremely difficult for your location and identity to be tracked. Best of all, there are no subscription fees.

Protect your digital life and improve your browsing experience on every device. Get the Winston Privacy Filter for 10 percent off today at $179.

Don’t forget to check out DiversyFund to start investing in

private real estate in 2021. You don’t have to be in the 1% to get started. Invest today for as low as $500.

Prices subject to change.

https://www.entrepreneur.com/article/368878

Gabrielli: “Creare un’Agenzia per la cybersecurity, non più affidata al Dis”

“È il momento di dar vita a un’Agenzia ad hoc per gestire a 360° la Cybersecurity, che non può essere più affidata al Dis che deve occuparsi di Intelligence”. L’annuncio di **Franco Gabrielli,** Sottosegretario alla Presidenza del Consiglio, in questa intervista esclusiva di **Cybersecurity Italia,** a margine del convegno “*Le nuove reti per l’industria italiana e per i consumatori*” organizzato a Roma l’8 aprile 2021.

[embedded content]
https://www.key4biz.it/gabrielli-creare-unagenzia-per-la-cybersecurity-non-piu-affidata-dis/354377/

Attacco ransomware contro le scuole italiane, bucato il registro elettronico di Axios

Ransomware mette sotto scacco le scuole italiane

"A seguito dell'attacco subito dalla nostra piattaforma, inviamo di seguito le istruzioni per gestire il registro di emergenza del protocollo", così è scritto sul sito web di **Axios**, società che sviluppa software per la gestione della segreteria scolastica, in questo caso si parla del **registro scolastico elettronico**.

Da venerdì tale programma non sta più funzionando in molte scuole italiane. L'applicativo *cloud based*, accessibile anche tramite app, che registra assenze, voti, giudizi, argomenti delle lezioni e altre annotazioni giornaliere, è stato quindi oggetto di un cyber attacco.

Axios fornisce servizi online di segreteria al 40% delle scuole del nostro Paese, quindi parliamo di criticità piuttosto estese.

Nessuna perdita di dati (sembra)

Dopo i primi disservizi, il giorno 5, lunedì Dell'Angelo, la società rendeva noto che "*a seguito delle approfondite verifiche tecniche messe in atto da Sabato mattina in parallelo con le attività di ripristino dei servizi, abbiamo*

avuto conferma che il disservizio creatosi è inequivocabilmente conseguenza di un ***attacco ransomware*** *portato alla nostra infrastruttura*”.

Dagli accertamenti effettuati, si legge ancora nel comunicato, “***al momento, non ci risultano perdite e/o esfiltrazioni di dati***”.

Nel tanto atteso giorno di rientro a scuola per più di 5 milioni di studenti italiani, si pone quindi il problema di come affrontare anche questo disservizio. Probabilmente saranno stati riesumati i registri cartacei, ma c’è anche una procedura la gestione in emergenza del registro elettronico, sia per l’apertura, sia per la compilazione e la chiusura.

L’azienda prevede di ristabilire i servizi per la didattica, al momento non accessibili, entro domani. Eccesso di ottimismo forse, più probabile ancora qualche giorno di criticità.

Dad sotto attacco informatico anche in Francia

Anche in Francia da ieri si registrano numerose criticità, che per il ministro dell’Educazione, **Jean-Michel Blanquer**, sono frutto di attacchi informatici provenienti da Paesi esteri.

Da ieri gli studenti francesi sono tornati a scuola, ma in gran parte in didattica a distanza (12 milioni di loro), non in presenza, come conseguenza delle nuove misure di lockdown prese dal Presidente **Emmanuel Macron**.

Come riportato da *orizzontescuola.it*: “*Sono in corso attacchi informatici* – ha detto Blanquer ad alcuni giornalisti – *questa mattina sembra arrivino dall’estero, per impedire ai server di funzionare. I tecnici sono al lavoro per ripristinare il servizio. Fortunatamente non tutti i server sono coinvolti*”.

Oggetto dei cyber attacchi il Centro nazionale per la

didattica a distanza (Cned), che per il momento non sta funzionando regolarmente, cioè non per tutti.

Gli attacchi sono stati multipli, di tipo DDoS, si legge sul sito d'informazione francese *bfmtv.com*, soprattutto si segnalano guasti massicci nelle regioni della Loira e dell'IIe-de-France.

https://www.key4biz.it/attacco-ransomware-contro-le-scuole-italiane-bucato-il-registro-elettronico-di-axios/354085/

Il Piano Biden da 2 trilioni di dollari si dimentica della cybersecurity

Gli **Stati Uniti d'America** hanno bisogno di un grande piano di ammodernamento, recupero e innovazione delle sue principali infrastrutture, soprattutto quelle strategiche, dagli ospedali alle scuole, dall'energia ai trasporti, fino alla mobilità elettrica e le reti di ricarica, ma in termini di Difesa pare che ci si sia dimenticato del fondamentale capitolo della **cybersecurity**.

Cybersecurity fuori dal piano annunciato da Joe Biden

A ricordarlo in un articolo pubblicato da *politico.com* gli stessi responsabili della **Cisa**, l'Agenzia per la sicurezza

informatica e la sicurezza delle infrastrutture (*Cybersecurity and Infrastructure Security Agency*), che è da tempo sottoposta ad un crescente carico di lavoro, proprio dovuto all'aumento degli attacchi e degli incidenti informatici, soprattutto a livello governativo, a cui corrispondono un organico insufficiente e risorse finanziarie troppo limitate.

"*In questo momento il Governo sta sottofinanziando il settore della sicurezza informatica, mentre sarebbero necessari investimenti molto più consistenti a livello nazionale*", ha spiegato nell'articolo **Tatyana Bolton**, direttrice della sicurezza informatica e delle minacce emergenti per l'R Street Institute ed ex responsabile della politica informatica dell'*Office of Strategy, Policy and Plans* presso la CISA.

In quel mega piano per il lavoro e le infrastrutture d'America che è stato annunciato da **Joe Biden**, con un programma di investimenti pari a 2.000 miliardi di dollari, incredibilmente non si è menzionata la cybersecurity delle stesse infrastrutture.

Servono più fondi, più personale e più strumenti tecnologici

Alla loro cyber protezione non è stato dato lo spazio necessario, soprattutto non sono state definite le risorse necessarie. "*Non è che non siano stati stanziati fondi in assoluto, ma sono troppo esigui: 2 miliardi di dollari per la Cisa e 10 miliardi per il Cyber Command*", ha spiegato Bolton.

Più che dimenticato, secondo diversi esperti, Biden ha considerato la sicurezza informatica più in termini impliciti che espliciti. Stando ad ulteriori valutazioni, alla Cisa servirebbero altri 5 miliardi di dollari entro il 2030 per portarsi ad un livello operativo sufficientemente efficace.

Tre, secondo l'Agenzia, sono le strade da percorrere sin da

subito per migliorare i livelli di cyberdifesa e per potenziare la capacità di resilienza delle infrastrutture: mitigare gli attacchi ransomware in aumento, aumentare il personale e le loro competenze tecniche e tecnologiche presso le Agenzie e i centri chiave, proteggere i sistemi e le reti industriali.

https://www.key4biz.it/il-piano-biden-da-trilioni-di-dollari-manca-della-cybersecurity/353754/

Il mondo spenderà 166 miliardi di dollari per la cybersecurity nel 2021. Ancora di più dal 2024

Gli attacchi informatici crescono e si diffondono a macchina d'olio da un continente all'altro, senza tregua. In molti casi mancano le più elementari soluzioni di **cybersecurity** per farvi fronte.

Il **Covid-19** ha rappresentato un'ulteriore opportunità per i **cyber criminali** di sviluppare nuove tattiche, tecniche e più dannosi strumenti di attacco informatico.

Crescono gli investimenti globali

in cybersecurity

Per questo gli **investimenti in cyber sicurezza** sono andati crescendo di pari passo con le minacce, in ogni parte del mondo. Secondo stime Fortune Business Insights, **entro la fine del 2021 la spesa in questo tipo di soluzioni tecnologiche dovrebbe raggiungere i 165,8 miliardi di dollari** a livello globale.

Una spesa in **crescita del +7,8%** rispetto al 2020, quando gli investimenti raggiunsero i 153 miliardi di dollari.

Le piattaforme *ecommerce*, i sistemi dell'internet delle cose, sia a livello industriale, sia ospedaliero, ad esempio, ma anche le infrastrutture cloud e quelle energetiche, sono stati più volte considerati dei bersagli primari dai cyber criminali.

Boom della spesa dal 2024

Per questo, secondo lo studio, **gli investimenti in soluzioni di cybersecurity aumenteranno ad un tasso medio annuo composto (Cagr) del +12%** nel periodo di tempo 2021-2028.

In particolare, seguendo i grafici illustrati nella ricerca, la spesa in tecnologie per la protezione informatica di sistemi, processi, reti, device e servizi, è attesa in **decisa crescita a partire dal 2024**, soprattutto per l'industria manifatturiera 4.0, la transizione digitale delle amministrazioni pubbliche e del comparto medico ospedaliero, nonché dell'intero sistema educativo nazionale.

Durante lo scorso anno, è specificato dal Report, circa **il 20% del mercato globale delle soluzioni di cybersecurity è stato rappresentato dal segmento Bfsi, cioè dei servizi bancari-finanziari-assicurativi**, attorno al 15% per il segmento telecomunicazioni & *information technologies*, un altro 15% circa per la sanità, la Pubblica Amministrazione centrale e

per il manifatturiero.

https://www.key4biz.it/il-mondo-spendera-166-miliardi-di-dollari-per-la-cybersecurity-nel-2021/353748/

Vendita illegale di vaccini sul dark web: anche in Italia si comprano dosi a 155 euro via Telegram

È da qualche settimana che in tutto il mondo si raccolgono denunce relative alla **vendita illecita di vaccini tramite i marketplace del dark web**. Anche in **Italia** è accaduto, grazie ad un apposito canale **Telegram**.

Il giro di vendite illecite è stato scoperto a seguito di un'indagine condotta dal **Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza**, da cui è emerso che nel nostro Paese era possibile via social acquistare dal mercato nero di internet sia singole dosi, sia interi stock di fiale.

Vaccini sul mercato nero italiano

Il listino prevedeva **155 euro per la singola dose e fino a 20 mila euro per uno stock di 800 fiale**.

Si garantiva anonimato, riservatezza, tracciabilità della

spedizione, imballaggio alla giusta temperatura sempre controllato e in alcuni casi si offriva anche la dose di richiamo.

"*Un business redditizio che ha attratto migliaia di persone interessate ad immunizzarsi dal virus senza attendere le tempistiche della campagna vaccinale in corso*", si legge nel comunicato che accompagna la notizia.

Per accaparrarsi i vaccini si doveva entrare nel canale Telegram preposto alle vendite, ma ci si riusciva solo previa autorizzazione del gestore.

Una volta entrati si poteva dare un'occhiata ai tanti annunci, quindi sbirciare alla vetrina dell'attività, dopo di che si veniva indirizzati verso i fornitori del prodotto desiderato, **si pagava in criptovalute** e si chiudeva l'affare prendendo nota delle garanzie e i tempi di consegna.

Per qualsiasi problema c'era anche un servizio clienti tramite messaggistica privata.

Indagine ancora in corso

Le indagini della GdF, coordinate dal Procuratore Aggiunto presso la Procura

della Repubblica di Milano, **Eugenio Fusco**, e dirette dai Sostituti Procuratori, **Bianca Maria**

Baj Macario e **Maura Ripamonti**, sono ancora in corso e dovranno cercare di capire in che modo si concretizzava la commercializzazione dei vaccini.

C'è da scoprire la provenienza della merce e la rete dell'organizzazione criminale, presentata come "*intenta unicamente a monopolizzarne il traffico clandestino e truffare gli ignari acquirenti*".

Al di fuori del giudizio etico, chi cerca di procurarsi vaccini in questo modo, tramite canali illegali del dark web, non solo è fortemente soggetto a truffe e frodi economiche, ma deve essere pienamente consapevole che **si tratta nella stragrande maggioranza dei casi di vaccini contraffatti**, non solo inefficaci contro il Covid-19, ma **potenzialmente pericolosi per la salute** del singolo e per la salute pubblica.

Un mercato nero sempre più globale

Una minaccia alla sicurezza della nostra salute e di quella pubblica che è stata rilanciata dai media internazionali già nei giorni scorsi, quando sulla Bbc si informava della **vendita illegale tramite marketplace del dark web di dosi di vaccino AstraZeneca, Sputnik o Johnson & Johnson** per un prezzo che variava tra 500 e 1000 dollari a dose.

Non solo, gli annunci pubblicizzavano anche la possibilità di **acquistare per 150 dollari false certificazioni di vaccinazione** o falsi test negativi a 25 dollari l'uno.

https://www.key4biz.it/vendita-illegale-di-vaccini-sul-dark-web-in-italia-a-155-euro-via-telegram/353713/

Dad nel mirino dei cyber criminali, moltiplicati gli attacchi al sistema educativo britannico

Con l’arrivo della pandemia di **Covid-19** si sono moltiplicate le opportunità per i gruppi criminali che operano online di attaccare diverse tipologie di istituzioni, tra cui scuole ed università.

La **didattica online**, misura necessaria per mitigare l’effetto del virus, è stata sfruttata a pieno per sferrare cyber attacchi di varia natura, attraverso **malware e ransomware** principalmente, che sono andati aumentando durante gli ultimi 12 mesi.

Nuova indagine sui cyber attacchi al sistema educativo britannico

È quanto emerso da una nuova indagine pubblicata dal **National cyber security centre** (Ncsc) sugli attacchi subiti da scuole di ordine e grado, college ed università tra dicembre 2020 e febbraio 2021.

Secondo i dati forniti dalla **Scottish Qualifications Authority** (SQA), nel periodo considerato, sono state individuate circa **860 mila email contenenti una qualche tipologia di minaccia informatica** per le scuole e le università destinatarie.

Solo a gennaio 2021 se ne sono contate più di 360 mila, oltre 291 mila a febbraio e circa 211 mila a dicembre 2020.

Proprio in questi giorni la **Harris Federation**, che gestisce 50 accademie tra primarie e secondarie nell’area metropolitana di Londa, ha denunciato **un attacco informatico che ha bloccato l’accesso alla posta elettronica di 37 mila studenti**.

Le nuove linee guida dell’Ncsc

Per questi motivi l’Ncsc ha rilasciato delle **linee guida** aggiornate che mirano ad aiutare le organizzazioni del settore pubblico e privato a gestire gli effetti del malware e a suggerire “azioni concrete per aiutare le organizzazioni a prevenire un’infezione da malware”, nonché misure volte a mitigare gli effetti di un attacco già avvenuto.

Paul Chichester, direttore delle operazioni presso l’Ncsc, ha dichiarato: “Qualsiasi attacco al settore dell’istruzione da parte dei criminali informatici è del tutto inaccettabile”.

“*Questa è una minaccia crescente e incoraggiamo fortemente le scuole, i college e le università ad agire in base alla nostra guida e ad aiutare a garantire che i loro studenti possano continuare a lavorare senza interruzioni*”, ha aggiunto il direttore.

“*Ci impegniamo a garantire che il settore dell’istruzione nel Regno Unito resti resiliente contro le minacce informatiche* – ha infine detto Chichester – *e abbiamo pubblicato risorse pratiche per aiutare le istituzioni a migliorare i loro livelli di sicurezza informatica e nella risposta stessa agli incidenti informatici*“.

https://www.key4biz.it/dad-nel-mirino-dei-cyber-criminali-moltiplicati-gli-attacchi-al-sistema-educativo-britannico/353599/