Digit'Ed

Il Sole 24 ORE Radiocor

16 FEBBRAIO 2023

DigitEconomy.24 – La minaccia dei cyber attacchi

PARLA ROBERTO BALDONI, DIRETTORE GENERALE DI ACN

«Mancati aggiornamenti e ingenuità delle persone alla base degli attacchi hacker»

Alla base dei recenti attacchi di hacker all'Italia ci sono il mancato aggiornamento dei software, i difetti di quest'ultimo e l'ingenuità delle persone. A spiegarlo è Roberto Baldoni, direttore generale dell'Acn, l'Agenzia per la cybersicurezza nazionale. Gli attacchi massicci, che a inizio febbraio hanno colpito prima la Francia, poi l'Italia, sono stati rivolti a aziende e istituzioni, ma grazie all'allerta lanciata dall'Autorità, molte di loro, circa 200, sono riuscite a reagire in tempo e ripristinare la sicurezza. In particolare, si sono registrati

attacchi rivolti a fornitori di connettività per realtà pubbliche; senza una loro reazione tempestiva si rischiava di creare un altro caso Regione Lazio. In Italia a soffrire, in particolar modo, sono le Pmi che spesso non investono perché per loro «la cybersecurity - spiega Baldoni - è un costo», senza considerare i risparmi legati all'investimento nella sicurezza informatica. In generale di cybersecurity,dichiara il direttore generale a DigitEconomy.24, report del Sole 24 Ore Radiocor e di Digit'Ed, nuovo gruppo attivo nella formazione e nel digital learning, si parla molto, ma non sempre «è informazione di qualità». Intanto, nel campo delle competenze, Baldoni conferma la stima già diffusa l'anno scorso: in Italia «c'è una grave carenza di figure professionali», mancano all'appello circa 100mila figure professionali, 3-4 milioni nel mondo.

>> continua a pag. 2

IL PUNTO DI EUGENIO SANTAGATA, CHIEF PUBLIC AFFAIRS & SECURITY OFFICER DI TIM E AD DI TELSY

«Servono più risorse per sostenere la cybersecurity»

Contro i cyber attacchi «servono più risorse per sostenere gli acquisti in tecnologia e sviluppare soluzioni contro la minaccia cibernetica». Lo sostiene Eugenio Santagata, chief public affairs & security officer di Tim e amministratore delegato di Telsy, sottolineando come il ruolo della politica oggi abbia recuperato il gap che c'era in passato nell'ambito della cybersecurity. Occorre tuttavia, spiega nell'intervista a DigitEconomy.24, report del Sole 24 Ore Radiocor e di Digit' Ed, nuovo gruppo attivo nella formazione e nel digital learning, «occorre sensibilizzare le aziende sui rischi informatici», e agire «in ottica preventiva». Quanto alle competenze necessarie per gestire la cybersecurity, Santagata chiarisce che Telsy «nel corso di quest'anno farà assunzioni nell'ordine di alcune decine di unità specializzate. Si cercano esperti in computer science, in matematica, crittografia, ingegneria informatica, ingegneria elettronica, ma anche giovani formati in materie umanistiche».

Eugenio Santagata, chief public affairs & security officer di Tim e ad di Telsy

>> continua a pag. 4

LA POSIZIONE DEL POLITECNICO

«La formazione cyber va completata in azienda»

Donatella Sciutto,
rettrice del Politecnico di Milano

In Italia, nonostante gli sforzi delle università, mancano i profili di cybersecurity richiesti da aziende e istituzioni. «Non è semplice - spiega Donatella Sciuto, rettrice del Politecnico di Milano - ampliare l'offerta perché il numero di docenti in queste materie non si improvvisa». Inoltre, per lavorare nella cybersecurity non basta studiare, serve implementare con la pratica le proprie conoscenze: «Nel campo della cybersecurity - aggiunge la rettrice nell'intervista a DigitEconomy.24, report del Sole 24 Ore Radiocor e di Digit'Ed, gruppo attivo nella formazione e nel digital learning - è molto difficile completare la formazione in aula e laboratorio; bisogna strutturare collaborazioni con le aziende per aiutarle a creare e formare le persone, con percorsi che siano nella dimensione lavorativa».

>> continua a pag. 4

Mancano ancora all'appello circa 100mila figure nella cybersecurity in Italia, 3-4 milioni nel mondo

Che cosa non ha funzionato nell'ultima ondata di attacchi hacker all'Italia che ha preso di mira i server VMware ESXi?
Molte aziende vengono da un secolo analogico e non hanno ancora sviluppato una piena cultura della sicurezza informatica. Gli hacker malevoli approfittano di tre cose: del mancato aggiornamento di software e sistemi e poi dei difetti del software, ma anche dell'ingenuità delle persone. Negli ultimi attacchi il problema è stato che i software deputati a fare un certo lavoro, a fornire servizi digitali, non erano stati aggiornati. Se il software fosse stato aggiornato come indicato da tempo dal produttore, i criminali non sarebbero riusciti a sfruttarne la vulnerabilità.

I mancanti aggiornamenti sono legati al fatto che le Pmi investono ancora poco in cybersecurity? C'è abbastanza informazione sull'importanza di investire in cybersecurity?
Le Pmi non investono perché spesso ritengono la cybersecurity un costo, che però si moltiplica in caso di un attacco. Spieghiamoci meglio. È come l'assicurazione sulla macchina: l'assicurazione ha un costo. Se decido di non pagarla per risparmiare, quando avrò un incidente dovrò spendere molto di più di quanto mi sarebbe costata l'assicurazione. Circa l'informazione, è possibile dire che ormai la cyber è diventata argomento quotidiano, soprattutto, e diciamo, purtroppo, per gli attacchi hacker, ma è anche vero che si sfornano molti libri sull'argomento, ci sono giornalmente convegni ed eventi dedicati al tema, le università offrono corsi, borse di studio e master, sui social se ne parla e tanto. Insomma, non è sempre informazione di qualità, ma l'argomento oramai si è imposto all'attenzione del pubblico.

il 27 febbraio scade il termine per partecipare al programma per le start up nella cybersecurity, che avete lanciato. Che tipo di partecipazione avete avuto e quali gli obiettivi di questo progetto di finanziamento?
Stiamo ricevendo diverse candidature e la procedura è in corso. L'Avviso ha l'obiettivo di selezionare incubatori e/o acceleratori che operano nel campo dell'innovazione e delle tecnologie emergenti dedicate alla cybersicurezza. È questo un primo passo per costruire una rete di collaborazioni, il Cyber Innovation Network, per il lancio di programmi nel campo della cybersicurezza a supporto di start-up che operano in settori di interesse dell'Agenzia come data science, robotica, blockchain, intelligenza artificiale, Internet of things, computazione quantistica e crittografia. Il Cyber Innovation Network fa parte del Programma strategico a sostegno dell'imprenditorialità innovativa e della ricerca pubblica, previsto dalla Strategia nazionale di cybersicurezza 2022-2026, per rafforzare l'autonomia strategica del Paese nel campo della cybersicurezza. Più tecnologia saremo in grado di produrre e di esportare come Italia e come Europa, più saremo in grado di mantenere un processo di trasformazione digitale in "sicurezza" per il Paese. Identificare attraverso Cyber Innovation Network le migliori startup e aiutarle ad avere una crescita costante all'interno di un mercato europeo ancora molto frammentato in un settore che, secondo l'European Investement Bank, ha a livello mondiale un valore di circa 148 miliardi di euro. La seconda area di intervento sarà dedicata al supporto e alla valorizzazione dei risultati della ricerca pubblica. In questa fase, Acn ha l'obiettivo di coinvolgere nel Cyber Innovation Network le strutture universitarie impegnate nel trasferimento tecnologico, mettendo così in circolo l'enorme portafoglio di risultati e di proprietà intellettuale che è proprio del mondo della ricerca.

Roberto Baldoni, direttore generale dell'Acn, l'Agenzia per la cybersicurezza nazionale

L'anno scorso, secondo l'Acn, mancavano in Italia 100mila esperti in cybersecurity, la situazione è migliorata?
Dobbiamo confermare come in Italia ci sia una grave carenza di figure professionali esperte in cybersecurity. Anche se 100mila non è il risultato di un calcolo preciso, si avvicina alle necessità più immediate. Il problema non è italiano ma mondiale. Si stima che manchino a livello globale fra i 3 e 4 milioni di professionisti della cybersecurity. Non ce lo possiamo permettere. Più la nostra vita sarà affidata al software e agli apparecchi digitali, più sarà necessario avere degli esperti in grado di costruire dispositivi inerentemente sicuri, sviluppare software affidabile e di gestire eventuali incidenti. Poi occorre preparare gli esperti in grado di lavorare su fronti che nei prossimi anni assumeranno una rilevanza straordinaria come la crittografia e il quantum computing. L'avviamento massiccio dei giovani alle discipline Stem (Scienza, tecnologia, ingegneria, matematica) è importante per le loro carriere professionali e per il Paese. Infine anche coloro che virano su studi umanistici dovranno essere necessariamente esposti ai concetti e alle regole che il mondo digitale impone, in modo da adattarsi velocemente alle modalità con cui il loro lavoro cambierà nel tempo ad esempio con l'affermarsi della intelligenza artificiale.

PARLA EMMANUEL BECKER, PRESIDENTE DI IDA, PRIMA ASSOCIAZIONE ITALIANA DEI DATA CENTER

«L'Italia in genere non viene attaccata per prima, grazie alla nostra rete informazioni in anticipo»

Data center e cybersecurity sono strettamente legati; se i server non vengono aggiornati frequentemente, il rischio attacco aumenta. Emmanuel Becker, amministratore delegato di Equinix Italia e presidente di Ida (Italian DataCenter Association), la prima associazione italiana dei costruttori e operatori di data center, fa il quadro della situazione alla luce dei recenti attacchi degli hacker. In questo contesto, Ida si pone anche come strumento di aiuto ai suoi membri, essendo in collegamento con reti simili a livello europeo ed essendo gli attacchi in genere collegati tra loro. In genere, infatti, vengono colpiti Paesi vicini e legati economicamente e l'Italia «raramente viene colpita per prima». Ida, nata dal sodalizio fra la stessa Equinix, Microsoft, Rai Way, Data4, Stack Infrastructure, Digital Realty, Vantage Data Centers, Cbre, «è collegata con The european data center association», e in questo modo è informata dei rischi e può avvisare tempestivamente i suoi associati.

L'associazione italiana Ida, collegata alla rete europea, riesce a essere informata in anticipo dei rischi

Gli strumenti per difendersi sono diversi: «innanzitutto, occorre diffondere le informazioni e aiutare le imprese e gli utenti a essere più preparati». Inoltre, nota Becker, «quando gli hacker attaccano preferiscono colpire dove si trovano più facilmente i soldi per riscattare i dati. Si tratta di imprese criminali, dietro alle quali a volte ci sono degli Stati. In genere, si attacca il Paese più ricco, quindi in Europa vengono colpiti dapprima la Francia, come nei recenti casi, o la Germania. Si attaccano Paesi legati tra di loro, commercialmente e digitalmente. L'Italia, quindi, anche se non è oggetto dell'attacco primario, si trova rapidamente sotto attacco».

L'Italia è la terza potenza economica europea ma la quinta digitale, occorre aumentarne l'importanza

Va considerato che «l'Italia è la terza potenza economica e la quinta a livello digitale. C'è, quindi, una discrepanza tra potenza economica e potenza digitale». Ida vuole, dunque, aumentare l'importanza digitale dell'Italia nello scacchiere europeo, federare i professionisti del mondo dei data center provider, ma anche quelli dei costruttori e degli operatori di data center. «Abbiamo studiato quello che esisteva negli altri mercati, in Spagna, Germania, Inghilterra e altri Paesi europei. La creazione effettiva è avvenuta a dicembre, l'annuncio è stato più recente». Il data center, secondo Becker, è paragonale a un aeroporto: «Più è importante per una città e più la città può avere un ruolo a livello locale e globale».

Emmanuel Becker, presidente dell'Italian DataCenter Association (Ida)

Fondata Ida per avere una sola voce comune, per dialogare con gli stakeholder e con il Governo

L'associazione ha una serie di obiettivi pratici, tra i quali quello di parlare con una voce sola, di creare e reclutare assieme i profili e le competenze che servono, di puntare sull'efficienza energetica. «Il primo obiettivo è quello di rappresentare gli interessi del settore di fronte alle autorità locali e internazionali, alla Comunità europea, al consorzio europeo per il cloud Gaia X. In secondo luogo, i data center producono valore ma anche occupazione. Malgrado gli annunci di alcuni giganti del digitale sulla riduzione dell'occupazione, in realtà il bilancio è positivo con la creazione di migliaia di posti ogni anno nel digitale. A volte il mondo dell'istruzione non prepara accuratamente i profili richiesti e, quindi, noi li creeremo al nostro interno, in collaborazione con scuole e università». Un altro punto molto importante è quello relativo all'efficienza energetica, «visto che i data center sono *energy intensive*. Noi vogliamo studiare regole comuni da proporre al legislatore». In quest'ottica Ida, vorrebbe incontrare e instaurare un dialogo «con il sottosegretario all'Innovazione Alessio Butti, con le Regioni, con il ministero delle Imprese e del Made in Italy, attore essenziale per capire in che modo possiamo favorire un impatto positivo sul territorio». Quanto agli associati, al momento Tim non fa parte dei soci fondatori, ma ci sono stati contatti con Noovle e Sparkle, società del gruppo. «Siamo molto aperti a tutti gli attori che pensano di poter portare valore aggiunto nel dialogo e nella creazione di valore sul territorio», conclude il manager.

ALMAVIVA CERCA NUOVE MILLE PERSONE IN AMBITO IT

Lo annuncia Marina Irace, direttrice Risorse umane del Gruppo

Almaviva cerca altre mille persone nell'ambito It per il 2023. Dopo avere assunto mille specialisti l'anno scorso, la società, come annunciato a DigitEconomy.24, report del Sole 24 Ore Radiocor e di Digit'Ed, nuovo gruppo attivo nella formazione e nel digital learning, è in cerca di altre competenze. «Nel settore - spiega Marina Irace, direttrice delle Risorse umane - c'è un *mismatch*: molte aziende si stanno attrezzando con sempre più reparti di informatica, ma il numero di professionalità presenti sul mercato non è elevato. Noi nel 2022 abbiamo già assunto un migliaio di persone nell'It, con profili diversi. Nel comparto, inoltre, c'è un *turn over* molto elevato, con numerose dimissioni spontanee (ne abbiamo contate 350). Fenomeno che, tuttavia, è diminuito negli ultimi tempi».

Marina Irace, direttrice Risorse umane di Almaviva

Va poi considerata la nascita di nuovi profili professionali che vanno a coprire alcune esigenze finora mai presentate. Oggi, spiega Irace, si riscontra «fluidità nei profili professionali che erano più stabili: prima, cioè, si parlava di sviluppatore, analista, architetto di software e così via. Ora, invece, vista la velocità del progresso tecnologico, tutto diventa più fluido. È cambiata l'ottica: in azienda non operiamo per figure professionali, ma per competenza. Nascono, quindi, nuove professionalità ibride». Esemplifica Irace: «nella diagnostica, ad esempio, servono figure nuove, medici che siano anche tecnici informatici. Professionisti chiamati a usare le nuove tecnologie con nuovi profili ibridi». Un'esigenza che Almaviva sente anche nell'ottica delle nuove mille assunzioni nel 2023.

Nel settore della cybersecurity e della mobilità sostenibile Almaviva ha dei reparti *ad hoc*: «facciamo formazione all'interno, con percorsi di crescita. Le figure ricercate possiedono una serie di competenze abbastanza comuni per tanti profili dell'It. Partendo da una base informatica comune, quindi, facciamo crescere le competenze». Almaviva, infine, per la creazione delle competenze necessarie, collabora «con le più grandi università italiane. Inoltre, riteniamo che l'orientamento debba essere svolto fin dalla scuola secondaria, prima della scelta del liceo o dell'istituto tecnico».

«Le donne nelle materie Stem scontano un pregiudizio storico»

In Italia mancano ancora circa 100mila figure nel settore della cybersecurity; le università sono pronte a fornire i nuovi profili?

Le stime mescolano profili molto diversi tra di loro che comprendono ingegneri, informatici, ma anche figure specializzate in ambito legale, e manageriale. Nelle università esistono diversi percorsi che cercano di rispondere a tutte le esigenze. Al Politecnico di Milano, ad esempio, abbiamo una laura magistrale ad hoc in cybersecurity, oltre a un corso di base che frequentano tutti gli ingegneri informatici. Esistono inoltre dei percorsi che puntano a formare figure più innovative che siano un mix tra tecnici, manager, legali. Ad esempio, al Politecnico c'è un corso di laurea in collaborazione con l'università Bocconi che ha proprio l'obiettivo di formare professionisti per il mondo della protezione dei dati personali o per l'organizzazione della cybersecurity nelle aziende. Certo, in generale, quelle della cybersecurity sono figure molto ricercate, e sono ancora mancanti. Purtroppo non è semplice ampliare l'offerta, anche perché il numero di insegnanti in queste materie non si improvvisa. Ossia, i docenti ci sono, ma non sono sufficienti per ampliare la platea di studenti nell'immediato.

Quali sono le figure più ricercate, quelle più difficili da trovare nel contesto italiano?

Tutte le figure tecniche dell'informatica sono molto ricercate. Nel mondo della cybersecurity, per esempio, servono figure come quella del *penetration tester* che ha il compito di provare ad attaccare i sistemi per testarne la resistenza. Nel campo della formazione c'è un progetto nazionale, il Cyber Challenge, un programma per i giovani dai 16 ai 24 anni, che ha l'obiettivo di identificare e attrarre la prossima generazione dei professionisti di cybersecurity anche in collaborazione con le università. Noi partecipiamo come Politecnico di Milano e selezioniamo i ragazzi più bravi per entrare nella squadra nazionale di cybersecurity. E i mHackeroni - nazionale italiana di hacker etici - si sono piazzati quinti a Las Vegas, ai mondiali di cybersecurity.

Quale ruolo possono giocare le istituzioni per agevolare la nascita delle nuove, e sempre più richieste, competenze?

L'Agenzia per la cybersecurity nazionale rappresenta sicuramente un primo passo per mettere a sistema le attività e aiutare le aziende a gestire le tematiche di cybersecurity. Noi, d'altro canto, come Politecnico siamo in collegamento con l'Agenzia e io stessa faccio parte del loro comitato scientifico che sviluppa programmi di assunzione e formazione, ma anche diffusione, disseminazione delle tematiche di cybersecurity.

Quanto è importante e come si può declinare il rapporto tra università e imprese per creare le competenze necessarie?

Le aziende chiedono profili già pronti. Nel campo della cybersecurity è molto difficile completare la formazione in aula e laboratorio; bisogna, quindi, strutturare collaborazioni con le aziende per formare le persone. Poi ci sono altri strumenti, come la Cyber Accademy, che forniscono alle aziende un luogo di incontro con gli studenti, creando un collegamento. Certo, si può sempre fare di più; si potrebbe, ad esempio, trovare il modo di formare gli studenti sugli stessi sistemi software delle aziende e, in questo caso, servirebbe la disponibilità dell'impresa a fornire il software necessario, in forma gratuita, visto che le università non possono permettersi di comprarlo.

L'arrivo sul mercato di sistemi di intelligenza artificiale sempre più completi ha messo in dubbio la validità futura di figure finora molto ricercate come il data analyst. Saranno superati dall'Ai?

La figura del data analyst richiede molte competenze statistiche e informatiche e di natura applicativa. Sono figure molto richieste e rimarranno molto richieste, anche perché aiutano a valutare gli stessi sistemi di Ai e di *machine learning*. Occorre cioè verificare che i dati non siano *bias*, ma siano invece rappresentativi.

Secondo un rapporto Istat del 2021, 16 donne su 100 scelgono una disciplina Stem contro il 35% dei colleghi uomini. Riscontra passi avanti?

I miglioramenti sono lenti, ma ci sono. Avere il dominio tecnologico nell'ambito dell'informatica consente di avere un impatto anche su molte componenti della vita di oggi; questa percezione manca ancora un po' e ciò pesa nella scelta dell'università. Inoltre, scontiamo, nel caso delle donne, un pregiudizio storico e culturale secondo il quale il mondo dell'ingegneria non è un mondo per donne.

IL PUNTO DI EUGENIO SANTAGATA, CHIEF PUBLIC AFFAIRS & SECURITY OFFICER DI TIM E AD DI TELSY

«Occorre sensibilizzare le aziende ai rischi informatici, in chiave preventiva»

Gli ultimi cyberattacchi contro realtà italiane hanno fatto alzare l'asticella della preoccupazione. Cosa non ha funzionato? Occorre maggiore coordinamento anche a livello politico?

Su questo punto credo che la politica abbia recuperato negli ultimi anni il gap che esisteva in passato. Servono però più risorse per sostenere gli acquisti in tecnologia e per sviluppare costantemente soluzioni nuove per contrastare la minaccia cibernetica. In Italia il vento sta cambiando, aziende e istituzioni stanno collaborando proattivamente e i benefici si vedono sul piano normativo e pratico. Negli ultimi due anni Tim ha posto particolare attenzione agli investimenti in competenze e asset necessari a rendere il proprio modello di sicurezza coerente con l'evoluzione dell'architettura di sicurezza nazionale. Gli asset di Tim, infatti, e in particolare Telsy come società leader in crittografia e cybersecurity del gruppo, insieme al Security Operation Center (Soc), al Threat Intelligence Lab, al Vulnerability & Test Lab e al Red Team Research di Tim, sono organizzati per rispondere efficacemente ai requisiti di comunicazione e interscambio informativo con i principali stakeholder governativi, quali l'Acn, la Polizia Postale e le varie articolazioni di sicurezza. Il 'Red Team Research' di Tim, ad esempio, è uno tra i pochi centri italiani di ricerca sui bug di sicurezza non documentati (cosiddetti *bug hunting*) in ambito software, ma anche sulle infrastrutture di rete, come la rete mobile 4G/5G. Identifica elenchi di falle di sicurezza (CVE) pubblicate sul National Vulnerability Database degli Stati Uniti d'America, con l'obiettivo di innalzare gli standard a livello internazionale. In soli 3 anni sono stati rilevati circa 100 bug rilevanti (0-day), di cui 7 molto critici, su prodotti *best-in-class* di valenza internazionale.

Le Pmi hanno oggi le risorse per investire nella cybersecurity? Come aumentare la consapevolezza dell'importanza di investire in cybersecurity?

Occorre sensibilizzare le aziende ai rischi informatici, anche perché spesso si corre ai ripari solo quando i danni sono compiuti, mentre è più importante agire in ottica preventiva. Nell'ultimo anno abbiamo assistito a un aumento esponenziale delle campagne di *phishing* (+200%) e dell'invio di mail fraudolente o con virus. Sono cresciuti anche gli attacchi *ransomware*, quelli che chiedono un riscatto per ripristinare il corretto funzionamento di Pc e applicazioni. Noi in Tim, attraverso Telsy e la rete commerciale di Tim Enterprise, offriamo a nostri clienti servizi di sicurezza informatica per le aziende e la Pa.