

RISPARMI, MERCATI, IMPRESE

[FINANZA](#) [BORSA E FONDI](#) [RISPARMIO](#) [TASSE](#) [CONSUMI](#) [CASA](#) [LAVORO](#) [PENSIONI](#) [IMPRESE](#) [MODA](#) [OPINIONI](#) [EVE](#)

09:22 Borsa: l'Europa parte con slancio dopo la Fed, a Milano (+1,2%) giu' Tim

08:36 Borsa: future puntano al rialzo dopo la Fed, corre il petrolio

08:00 *** Borsa Tokyo: Nikkei chiude in netto rialzo (+2,1%) dopo Fed



SICUREZZA ONLINE

Cybersecurity, mancano le competenze: «formazione e ricerca sono fondamentali»



di Alessia Conzonato | 14 dic 2021



PRINCIPALI IN

NOME

DAX 40

DOW JONES

FTSE 100

FTSE MIB

« Il digitale non è da temere, non dobbiamo demonizzarlo», risponde così Ferruccio Resta, rettore del Politecnico di Milano e presidente della Crui (Conferenza dei rettori delle



università italiane), alla domanda su quanto è **importante aderire al progresso innovativo** , nonostante le minacce che quotidianamente arrivano attraverso la rete, sia per gli utenti privati che per le attività produttive e imprenditoriali. «È controindicato non attuare una transizione tecnologica solo perché il digitale è un campo su cui siamo vulnerabili – continua –. Sarebbe come dire che il virus ci rende fragili e quindi non ci impegniamo a trovare un vaccino». **L'evoluzione di sistemi e apparecchi tecnologici a metodi sempre più innovativi è in atto già da tempo** . La crisi pandemica ha inevitabilmente accelerato il processo, entrando a far parte di ogni aspetto della vita privata dei cittadini ma anche dell'economia del Paese e globale. È il motivo per cui i riflettori sono puntati molto più di prima su attacchi informatici volti a danneggiare un'intera filiera produttiva o anche solo a dimostrare la debolezza di un software.

Ecco la nazionale :
tifa per i nostri cyl
di Alessia Cruciar



I MODELLI

Cybersecurity, la lotta diventa trasversale a tutte le funzioni aziendali

di Fabio Savelli



Cybersecurity: i pr
offerte per lavorar
di Irene Consiglie

LinkedIn premi:
italiane più capac
Talenti dell'IT; il

Le statistiche sugli attacchi informatici



Il rettore del Politecnico di Milano, Ferruccio Resta

Come si evince dal più recente rapporto Clusit - Associazione Italiana per la Sicurezza Informatica, nel 2020 si sono verificati, solo in Italia, circa 1.871 attacchi hacker, con una percentuale di crescita pari al 12% rispetto all'anno precedente e del 66% rispetto al 2017. Nei primi sei mesi del 2021, invece, sono stati 1.053 gli attacchi gravi a livello globale: si tratta del 24% in più rispetto allo stesso periodo dell'anno precedente, **per una media mensile pari a 170, contro i 156 del 2020** . Tanto che gli esperti dell'Associazione la definiscono ormai un'«emergenza globale». Il 10% degli attacchi portati a termine ha una relazione con la pandemia: tra i settori più colpiti, infatti, ci sono il sanitario,

quello governativo, il militare e dell'intelligence, la ricerca e l'istruzione e, infine, i servizi online. Le perdite stimate causate dalle falle della cybersecurity sono pari a 6 trilioni di dollari per l'anno in corso. Una previsione che punta al ribasso, dato che **vengono presi in considerazione nello studio solo attacchi di pubblico dominio** e quindi sfuggono tutte le altre tipologie.



Università e azien
dell'IT; il Master d
di Irene Consiglie

FORMAZIONE



Competenze digitali: entro settembre 2022 Microsoft formerà 3 milioni di persone

di Irene Consigliere



Assicurazioni, la n
tech cambierà il b
di Alessia Conzon

Influiscono i comportamenti degli utenti

Oggi più che mai gli strumenti di cybersecurity sono fondamentali. «È chiaro che qualunque studio sul fenomeno non può che partire da un'analisi dei rischi – spiega Resta – che minano o mettono in difficoltà il nostro sistema socio-economico. Lo abbiamo provato sulla nostra pelle con la pandemia: **l'interconnessione mondiale ha portato al diffondersi del Covid**. Si tratta di un attacco virale, ma è pur sempre un attacco. Un altro pericolo è un blocco dei sistemi informatici e dell'analisi dei dati, che sia per un failure doloso o meno. È evidente che la fortissima connessione che c'è tra intere filiere delicate, come il sistema bancario, finanziario, o quello sanitario, **tra le attività produttive e nella vita dei cittadini sia una vulnerabilità**. Ma non per questo se ne deve aver paura. Ci sono anche dei punti di forza: la rete è talmente distribuita che è raro e difficile che avvenga un blackout totale». Insomma, lo sviluppo tecnologico non si fermerà e, per fare in modo che l'incremento sociale ed economico vada di pari passo, è necessario proteggersi da eventuali attacchi hacker. L'elemento tecnico, però, non basta.



«Stipendi inadeguati
laureati stem scap
di Alessia Cruciar

LEGGI ANCHE:

[La sicurezza sulla Rete: il 90% dei server della Pa è vulnerabile agli attacchi hacker](#)

[La superpoliziotta Ciardi: «Donne, puntate sul digitale, lavoro e carriera vi aspettano»](#)

[Cybersecurity, mancano le competenze: «formazione e ricerca sono fondamentali»](#)

[Le imprese a lezione di big data al competence center di BiRex](#)

[Il polo Accenture di Napoli: le armi di difesa](#)

[Engineering, la frontiera dell'internet delle cose](#)

[Il superpolo internazionale di Cisco nella «casa» di Leonardo](#)

[Competenze digitali: entro settembre 2022 Microsoft formerà 3 milioni di persone](#)



Il superpolo intern
Leonardo
di Sergio Bocconi



La sicurezza sulla
vulnerabile agli at

«C'è anche un aspetto sociale e organizzativo che influisce – aggiunge il presidente dei rettori –. Certo, la tecnologia è utile. Ad esempio, **nella protezione degli storage dove i dati**

vengono immagazzinati, nella gestione dei cloud o nella duplicazione di informazioni. Ma spesso i problemi derivano da un comportamento non consono dell'individuo: può succedere che il mio computer recepisca un virus perché io ho cliccato su un sito trojan senza riconoscerlo oppure sono caduto in un phishing (tipologia di truffa in rete per rubare i dati personali degli utenti, spesso avviene attraverso messaggi di posta elettronica ingannevoli, ndr)».

di Federico De Ro

LE GRANDI RETI PUBBLICHE

Engineering, la frontiera dell'internet delle cose

di Marco Sabella



Le imprese a lezione
center di BiRex

di Alessia Conzon

Corso di laurea in cybersecurity

È qui che entrano in gioco due elementi, secondo Resta, imprescindibili dalla trasformazione tecnologica. Oltre a un potenziamento dei corsi di studi e degli insegnamenti specifici già presenti nel programma del Politecnico di Milano, come ingegneria informatica e matematica, proprio in tema di cybersecurity è stato avviato nel 2019 un corso di laurea magistrale in «Cyber risk strategy and governance», nato dalla partnership con l'università Bocconi di Milano. «È il primo esempio di facoltà su questo tema tra due università di eccellenza – racconta il rettore – ed è la dimostrazione che non vogliamo concentrare la formazione solo in ambito tecnologico». Gli studenti, infatti, oltre allo sviluppo di materie come computer science, potranno acquisire le competenze anche su un livello strategico, per valutare, governare e gestire sia i rischi che le opportunità già presenti o in via di sviluppo nel settore digitale e all'innovazione tecnologica. Il programma mira a fornire una solida preparazione per far sì che chi lo ha frequentato sia in grado di valutare e comunicare le minacce prima che si manifestino. «Il corso sta avendo un successo incredibile – continua Resta –. Non solo i due poli universitari, ma anche molte aziende hanno capito da subito la rilevanza di questa opportunità e hanno deciso di dare il loro contributo offrendo borse di studio per gli studenti meritevoli e possibilità di internship presso le loro sedi. Per loro è anche un modo per fare reclutamento. A settembre ci sono stati i primi laureati e sono tutti molto richiesti nel mondo del lavoro. È ovvio che per valutarne l'efficienza servono numeri più alti, ma per adesso il tasso di occupazione è del 100%».



La superpoliziotta
digitale, lavoro e c

di Alessia Cruciar

LE COMPETENZE

Il polo Accenture di Napoli: le armi di difesa

di Marco Sabella



Il ruolo fondamentale della ricerca

Al termine del corso di laurea emergono due figure professionali: il cyber risk manager, che supporterà le attività relative alla gestione del **rischio informatico a livello organizzativo al fine di governare il rischio d'impresa** attraverso la progettazione e l'attuazione di strategie ad hoc, e il data protection and security manager, il quale si occuperà delle attività relative alla protezione dei dati, alla gestione della privacy e alla compliance al fine di governare i rischi sui dati. «**La collaborazione con Bocconi porta da sempre a ottimi risultati** – commenta Resta –, perché abbiamo tutta grande consapevolezza del fatto che la sfida è globale, interessa tutti e riguarda un'attrazione dei talenti che porterà benefici a tutto il sistema sociale ed economico. Soltanto avviando dei percorsi di altissima qualità i ragazzi sono stimolati a sceglierli». A fianco di tutto ciò ci vuole la ricerca, che con il lavoro giornaliero studia le nuove tecnologie presenti sul mercato e ne analizza le controversie e le debolezze. «L'università è tale proprio per l'impegno nella ricerca – conclude il rettore Ferruccio Resta –. Senza i laboratori e un team di professori ed esperti che **ogni giorno studiano e sperimentano nuovi strumenti, soluzioni e tecnologie**, è difficile immaginare un progresso».

BIG DATA

CYBERSECURITY

CYBERSICUREZZA

INNOVAZIONE

TECNOLOGIA

TECNOLOGIE

© RIPRODUZIONE RISERVATA

Raccomandato da Taboola

Velasca, la tradizione artigianale italiana.

[VELASCA](#)

Natale in montagna in Lombardia: dove andare

[INLOMBARDIA](#)

Tutto quello che non sai sul salmone (e che dovresti sapere)

[SEAFOOD FROM NORWAY](#)
