Capgemini press contacts:
Laura Muratore
Marketing & Communication Director
laura.muratore@capgemini.com

Michela Cotich
Marketing & Communication
michela.cotich@capgemini.com
+39 347 3620244

Community Group:
Michele Bon
michele.bon@communitygroup.it
+39 338 6933868

Carlo Carboni
carlo.carboni@communitygroup.it
+39 348 9412226

Il 69% delle organizzazioni ritiene che senza l'Intelligenza Artificiale non sarà in grado di contrastare le nuove minacce informatiche

Due organizzazioni su tre intendono implementare l'IA già nel 2020 per supportare i propri meccanismi di difesa da attacchi informatici

Milano, 11 luglio 2019 – Secondo il nuovo studio del Capgemini Research Institute, le imprese stanno incrementando gli investimenti in sistemi di intelligenza artificiale per difendersi dagli attacchi informatici di nuova generazione. Due terzi (69%) delle imprese riconoscono di non essere in grado di rispondere alle minacce critiche senza il supporto dell'IA. Con l'incremento del numero di dispositivi, di reti e di interfacce utente dovuto ai progressi in ambito cloud, IoT, 5G e nelle tecnologie di interfaccia conversazionale, le aziende devono affrontare con urgenza la necessità di incrementare e migliorare costantemente la loro sicurezza informatica.

Allo studio dal titolo "Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security", hanno partecipato 850 dirigenti senior in ambito IT con responsabilità nella sicurezza delle informazioni, nella cybersecurity e nelle operations in 10 paesi e sette settori di business. Inoltre, sono state condotte interviste approfondite con esperti del settore, startup in ambito cybersecurity e rappresentanti del mondo accademico.

Queste le principali evidenze:

L'IA è ormai un abilitatore necessario per la cybersecurity
Oltre la metà (56%) dei dirigenti intervistati afferma che i cybersecurity analyst della loro azienda si sentono sotto pressione a causa della vasta gamma di dati da monitorare al fine di rilevare e prevenire gli attacchi informatici. Inoltre, sono notevolmente aumentati i tipi di attacchi informatici che richiedono un intervento immediato o che i cyber analyst non sono in grado di risolvere abbastanza rapidamente, come attacchi hacker che interessano applicazioni time-sensitive (il 42% dichiara di aver assistito a un incremento, in media del 16%) e attacchi automatizzati e machine-speed, che si trasformano tanto velocemente da non poter essere neutralizzati attraverso i tradizionali sistemi di risposta (il 43% degli intervistati ha dichiarato di aver registrato un aumento, in media del 15%).

Trovandosi di fronte a queste nuove minacce, una netta maggioranza delle aziende intervistate (69%) ritiene di non essere in grado di rispondere agli attacchi informatici senza l'utilizzo dell'IA, mentre il 61%

dichiara di aver bisogno dell'IA per identificare le minacce più critiche. Un dirigente su cinque ha affermato che la propria azienda ha subito una violazione della sicurezza informatica nel 2018, il 20% delle quali ha comportato per l'azienda un costo di oltre 50 milioni di dollari.

Aumentano gli investimenti in IA per la sicurezza informatica

Una netta maggioranza dei dirigenti è d'accordo sul fatto che l'IA sia fondamentale per il futuro della sicurezza informatica:

- Il 64% ha dichiarato che l'IA permette di ridurre il costo di rilevazione degli attacchi informatici e delle azioni di risposta agli stessi, in media del 12%
- Il 74% ha affermato che questa tecnologia consente di avere tempi di risposta più brevi, infatti riduce del 12% il tempo necessario per rilevare le minacce, intervenire per bloccare le violazioni informatiche e implementare le patch
- Il 69% degli intervistati ha dichiarato che l'IA migliora l'accuratezza del rilevamento delle violazioni, mentre il 60% che la tecnologia permette di incrementare l'efficienza dei cybersecurity analyst, riducendo il tempo di analisi dei falsi positivi e migliorando la produttività

Di conseguenza, emerge che quasi la metà degli intervistati (48%) ha affermato che nel 2020 i budget a disposizione per l'implementazione dell'IA per la sicurezza informatica aumenteranno di quasi un terzo (29%). In termini di implementazione, il 73% delle aziende sta eseguendo dei test sugli use case dell'IA nel quadro della cybersecurity. Solo un'azienda su cinque ha utilizzato l'IA prima del 2019, ma l'implementazione è destinata a incrementare in maniera esponenziale: quasi due imprese su tre (63%) prevedono di utilizzare l'IA entro il 2020 per rafforzare i propri meccanismi di difesa dagli attacchi informatici.

"L'IA offre enormi opportunità in tema di sicurezza informatica", ha affermato Oliver Schererer, CISO di MediaMarktSaturn Retail Group, principale rivenditore europeo di elettronica di consumo. *"Questo avviene perché le attività di rilevazione, reazione e risanamento passano da manuali ad automatizzate, un miglioramento che le aziende vorrebbero raggiungere entro i prossimi tre o cinque anni"*.

Permangono ostacoli significativi all'implementazione dell'IA su scala

La sfida principale per l'implementazione dell'IA legata alla sicurezza informatica è la mancanza di comprensione sul processo per passare dal proof of concept a una completa implementazione su larga scala degli use case: il 69% degli intervistati ha infatti ammesso di aver incontrato delle difficoltà proprio in questo senso.

Alessandro Menna, Cybersecurity Lead di Capgemini Business Unit Italy, ha affermato: *"Le aziende si trovano ad affrontare un volume e una complessità di minacce informatiche senza precedenti e si sono rese conto dell'importanza dell'IA come primo elemento di difesa. I cybersecurity analyst sono fortemente sotto pressione per la mole di dati da monitorare e quasi un quarto dichiara di non essere in grado di analizzare con successo tutte le violazioni identificate. Diventa quindi fondamentale che le aziende incrementino gli investimenti e inizino a concentrarsi sui benefici che l'IA può apportare in termini di rafforzamento della cybersecurity delle loro aziende".*

Inoltre, per la metà delle aziende intervistate le sfide più significative riguardano l'integrazione con infrastrutture, sistemi di dati e applicazioni esistenti. Nonostante la maggior parte dei dirigenti affermi di aver ben chiari gli obiettivi che si vogliono raggiungere con l'introduzione dell'IA nella sicurezza informatica, solo la metà (54%) degli intervistati ha identificato i dati necessari per rendere operativi gli algoritmi di IA.

Continua Menna: *"Le organizzazioni devono fronteggiare gli ostacoli che impediscono all'IA di raggiungere il pieno potenziale per la sicurezza informatica. Questo rende necessario creare una roadmap per affrontare le principali barriere e concentrarsi sugli use case che possono essere scalati più facilmente e offrire maggiori ritorni. Solo attraverso queste misure le aziende potranno essere pronte ad affrontare le nuove minacce informatiche, riducendo i costi e la probabilità di una violazione dei dati fortemente impattante."*

Per scaricare una copia del report cliccare qui.

Metodologia di ricerca

La ricerca ha coinvolto 850 dirigenti senior operanti in sette settori: Consumer Products, Retail, Banking, Insurance, Automotive, Utilities e Telecom. Un intervistato su 5 ricopre l'incarico di CIO, mentre uno su dieci è CISO nelle rispettive organizzazioni, con sede in Francia, Germania, Regno Unito, Stati Uniti, Australia, Paesi Bassi, India, Italia, Spagna e Svezia. Capgemini ha inoltre condotto interviste con leader del settore e rappresentanti del mondo accademico, esaminando lo stato attuale e l'impatto dell'IA nella sicurezza informatica.

Capgemini

Leader mondiale nei servizi di consulenza e tecnologia, Capgemini è all'avanguardia nell'innovazione per consentire ai suoi clienti di orientarsi al meglio in un mondo costantemente in evoluzione del cloud, del digitale e delle piattaforme. Forte di 50 anni di esperienza e di una profonda conoscenza degli specifici settori di mercato, Capgemini sostiene le organizzazioni nel realizzare le proprie ambizioni di business, offrendo una gamma di servizi che vanno dalla strategia alle operations. Capgemini è mossa dalla convinzione che il valore di business della tecnologia sia creato dalle e attraverso le persone. Con un'organizzazione multiculturale di oltre 200.000 dipendenti presenti in più di 40 paesi nel mondo, nel 2018 il Gruppo Capgemini ha registrato ricavi per 13,2 miliardi di euro.
Visita il nostro sito www.it.capgemini.com. *People matter, results count.*

Capgemini Research Institute

Il Capgemini Research Institute è il think-tank interno di Capgemini dedicato a tutto ciò che è digitale. L'istituto pubblica lavori di ricerca in merito all'impatto delle tecnologie digitali sulle grandi società tradizionali. Il team fa leva sul network mondiale di esperti Capgemini e lavora a stretto contatto con partner accademici e tecnologici. L'istituto possiede centri di ricerca dedicati in India, nel Regno Unito e negli Stati Uniti. Recentemente, è stato nominato il miglior istituto di ricerca al mondo per la qualità dei suoi lavori da una giuria di analisti indipendenti.
Per saperne di più consultare il sito https://www.capgemini.com/researchinstitute/