Da Armis una prospettiva italiana all'interno del suo Armis State of Cyberwarfare and Trends Report: 2022-2023

Il 61% degli intervistati ha registrato una violazione della sicurezza informatica nelle loro organizzazioni

MILANO, ITALIA, January 24, 2023 /EINPresswire.com/ -- Armis, azienda leader per la visibilità e sicurezza degli asset, ha recentemente presentato la ricerca Armis State of Cyberwarfare and Trends Report: 2022-2023, che mostra la percezione della guerra informatica da parte dei professionisti IT e responsabili della sicurezza. Con riferimento alle aziende italiane, il 61% degli intervistati ha affermato di aver riscontrato un attacco informatico alla propria organizzazione. In generale, l'Italia mostra attualmente una discreta attenzione alla cybersecurity, con oltre l'85% degli intervistati che dichiara che la propria organizzazione dispone di misure per rispondere alle minacce informatiche, anche se ci sono molte aree ancora da migliorare.

Le preoccupazioni differiscono dalla realtà rispetto al contesto geopolitico
Rispetto al resto del mondo, l'Italia è mediamente meno preoccupata dell'impatto della guerra informatica sulle infrastrutture critiche dell'azienda e sui suoi servizi. Quando chiesta l'opinione sull'affermazione "La mia azienda considera il cyber come un rischio strategico per l'organizzazione", il 29% degli intervistati italiani si è trovato fortemente d'accordo, un dato che risalta, paragonato al 44% degli intervistati a livello globale. È necessario porre maggiore enfasi sui rischi associati a un evento di questa portata per stimolare la consapevolezza dei professionisti della sicurezza.

La ricerca ha toccato anche il tema della fiducia nel governo per quanto riguarda la difesa di fronte a un cyberattacco, che ha mostrato risultati interessanti. A livello globale, il 33,5% si sente molto fiducioso dell'impegno delle organizzazioni governative, mentre in Italia solo il 18% degli intervistati ha la stessa fiducia.
Il Data Protection Framework italiano e Cybersicurezza: la conformità alle direttive italiane

L'Italia ha redatto il Framework Nazionale per la Cybersecurity e la Data Protection, un benchmark adottato da diverse tipologie di organizzazioni come strumento per coordinare la propria strategia di difesa contro le minacce cyber. Nonostante ciò, oltre 2 aziende su 5 (41%) dichiarano di non aver intrapreso azioni per essere conformi al nuovo quadro normativo, e solo il 7% delle organizzazioni in area governativa dichiara di avere un piano conforme. Il settore più proattivo è quello finanziario e bancario, con il 33% degli intervistati che dichiara di aver

implementato un piano pienamente conforme. In generale, la preoccupazione è debole nelle organizzazioni appartenenti ai settori OT e retail, dato che la percentuale di entità che non hanno ancora implementato un piano, o che stanno pianificando di farlo, è rispettivamente del 25% e del 21%.

Questo dato è forse ancora più preoccupante se si considera che oltre 4 professionisti IT su 5 (84%) intervistati concordano sul fatto che la loro organizzazione detiene dati sensibili, che ci sono regolamenti da seguire e che vogliono ridurre al minimo qualsiasi effetto negativo di un evento di sicurezza. La protezione dei dati è un imperativo per tutti i Paesi dell'UE e, sebbene la consapevolezza della sua importanza sia evidente, sembra esserci uno scostamento con l'effettiva conformità alle norme.

La priorità è rafforzare le proprie misure di sicurezza
Le organizzazioni italiane stanno migliorando il loro approccio alle minacce informatiche, ma ci sono ancora diverse misure da adottare. L'attenzione principale è rivolta alla protezione dei dati, al rilevamento delle intrusioni e alla gestione dell'identità e degli accessi, che gli intervistati hanno indicato come le loro priorità principali, mentre la prevenzione di possibili attacchi alla catena di fornitura e il monitoraggio dei macchinari appaiono secondari.
Le prospettive future sembrano essere rassicuranti e incoraggianti, in quanto il campione di intervistati prevede maggiori investimenti da parte delle proprie organizzazioni in misure di cybersecurity rilevanti. Gli intervistati prevedono investimenti in formazione sulla cybersecurity immediatamente (35%) o entro sei mesi (31%); in nuovi fornitori il 21% immediatamente e il 33% entro sei mesi; e in risorse per la gestione delle vulnerabilità il 40% immediatamente e il 29% entro sei mesi.

"Dai risultati di questo studio emerge chiaramente che le organizzazioni italiane non condividono le preoccupazioni della maggior parte degli altri Paesi riguardo alla minaccia della guerra informatica e hanno ancora molta strada da fare per quanto riguarda la compliance", ha dichiarato Nicola Altavilla, Country Manager Italy & Mediterranean Area di Armis. “Entrambi questi problemi possono essere affrontati con una maggiore visibilità degli asset, la gestione delle vulnerabilità e la valutazione continua dei rischi. Armis è in una posizione unica per assistere le organizzazioni italiane nel raggiungimento della conformità e nel miglioramento delle loro posizioni di sicurezza".

Per maggiori informazioni riguardo allo studio Armis State of Cyberwarfare and Trends Report: 2022-2023, visitare: https://www.armis.com/cyberwarfare/

Metodologia
Armis ha intervistato 6.021 professionisti IT e responsabili della sicurezza in aziende con più di un centinaio di dipendenti negli USA, UK, Francia, DACH (Austria, Germania, Svizzera), penisola Iberica, Italia (500 rispondenti), Danimarca, Paesi Bassi e APJ (Australia, Giappone, Singapore). Questi risultati sono stati raccolti tra il 22 settembre 2022 e il 5 ottobre 2022, e descrivono lo stato della guerra informatica a livello globale in varie regioni e settori.

About Armis
Armis, azienda leader nella visibilità e nella sicurezza degli asset, fornisce la prima piattaforma di asset intelligence unificata del settore, progettata per far fronte alla superficie di attacco ampliata dai nuovi numerosi dispositivi connessi. Aziende Fortune 100 si affidano alla nostra protezione continua e in tempo reale per avere visibilità completa su tutti gli asset gestiti e non gestiti tra IT, cloud, dispositivi IoT, dispositivi medici (IoMT), tecnologia operativa (OT), sistemi di controllo industriale (ICS) e 5G. Armis fornisce una gestione passiva automatizzata e la gestione del rischio di tutti gli asset informatici, Armis è una società privata con sede a Palo Alto, in California.

per Armis
Archetype Agency Srl.
armis-mil@archetype.co
Visit us on social media:
Twitter
LinkedIn
