ARMIS®

STATO DELLA
GUERRA INFORMATICA

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

ANALISI PAESE PER PAESE

ITALIA

INDICE DEI CONTENUTI

INTRODUZIONE

Se avete esaminato il Armis State of Cyberwarfare and Trends Report: 2022-2023, saprete che è fondamentale che i leader aziendali e IT comprendano l'evoluzione del panorama delle minacce tipiche di una guerra informatica, in modo da poter migliorare la propria posizione in materia di cybersecurity per difendersi da questi attacchi. Per preparare questo report, Armis ha commissionato uno studio intervistando 6.021 professionisti in ambito IT e sicurezza a livello globale per determinare le tendenze mondiali in relazione alle opinioni dei professionisti del settore sulla guerra informatica, sui modelli di attacco, sulla spesa informatica e altro ancora. Le risposte sono state raccolte tra il 22 settembre 2022 e il 5 ottobre 2022.

Armis ha utilizzato i dati della sua pluripremiata piattaforma di asset intelligence e sicurezza (Armis Asset Intelligence and Security Platform) per verificare i risultati del sondaggio rispetto alle tendenze dei dati reali. I dati proprietari della piattaforma raccolti dal 1° giugno 2022 al 30 novembre 2022, hanno confermato che gli attacchi informatici non hanno subito un rallentamento, anzi, sono aumentati. Le minacce contro il clienti a livello globale di Armis sono aumentate del 15% da settembre a novembre rispetto ai tre mesi precedenti. Inoltre, Armis ha identificato la percentuale maggiore di attività di minaccia contro le organizzazioni di infrastrutture critiche, mentre le organizzazioni sanitarie sono al secondo posto tra i settori più bersagliati.

Oltre a questi risultati globali, Armis ha preparato risultati regionali e analisi paese per paese, per offrire approfondimenti unici e localizzati che possono essere di maggiore impatto per i singoli lettori, a seconda del luogo in cui si trovano fisicamente e delle regioni in cui opera la loro azienda. **Per questa analisi paese per paese, ci concentreremo sui risultati ottenuti dai 500 intervistati che hanno condiviso le loro idee per il nostro sondaggio e che hanno sede in Italia e lavorano in diversi settori, tra cui sanità, industria manifatturiera, retail, servizi finanziari e altri ancora.**

SINTESI DEI RISULTATI

La trasformazione digitale e un nuovo modo di lavorare hanno migliorato la vita di tutti oltre che il flusso di lavoro aziendale. L'approccio digitale è stato implementato in tutti i settori, creando nuove opportunità per concentrarsi sul core dell'azienda, ma come sempre esiste un rovescio della medaglia, che viene illustrato nel report. Analizzando le aziende italiane, il 61% degli intervistati tra i professionisti in ambito IT e sicurezza ha subito un attacco informatico nella propria società. 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.

Complessivamente, Armis ha identificato tre tendenze chiave analizzando le risposte dei professionisti in ambito IT e sicurezza delle società italiane rispetto agli altri intervistati a livello globale di EMEA, U.S.A. e APJ. Di seguito, approfondiamo questi risultati e le tendenze di cui sono indicativi.

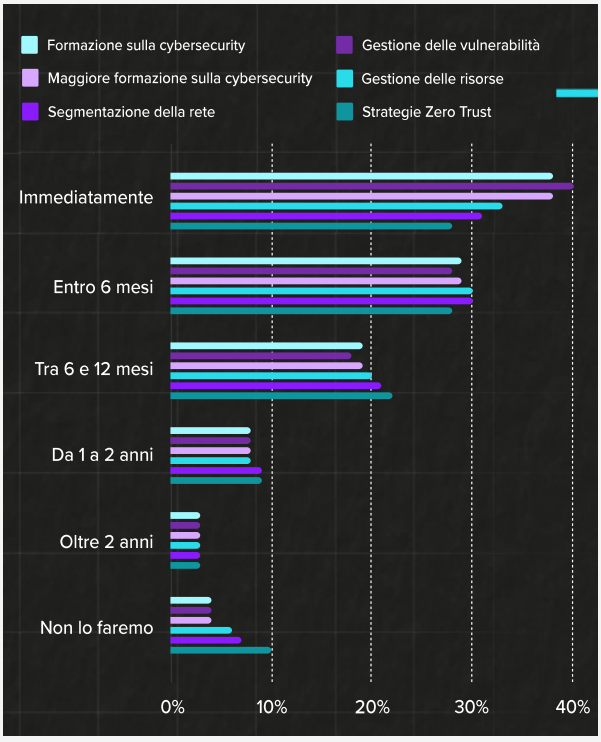
EMEA

Nel corso del 2022, la regione EMEA è stata sconvolta dall'invasione dell'Ucraina da parte della Russia. A causa dell'instabilità geopolitica associata alla guerra sul campo e alla guerra informatica, l'onda d'urto delle conseguenze dell'invasione si fa sentire in tutta l'area. L'imprevedibilità dell'approvvigionamento alimentare, la famigerata crisi energetica e l'ondata di attacchi informatici mirati alle funzioni più critiche della società stanno contribuendo a modificare le spese e le priorità di numerosi settori. Il report conferma l'aumento degli attacchi informatici, evidenziando che quasi 3 organizzazioni su 5 (58%) hanno subito una o più violazioni informatiche. Il 25% degli intervistati ha confermato che il numero di minacce alla propria organizzazione si è intensificato.

Si stanno adottando misure per garantire la protezione, ma a tutt'oggi meno della metà (44%) dei professionisti in ambito IT e sicurezza concorda sul fatto che la propria organizzazione disponga di programmi e pratiche per rispondere alle minacce in ambito cyber. Gli intervistati descrivono la loro società come poco preparata, poiché vi sono alcune questioni rilevanti da affrontare:

- Solo il 46% dei professionisti in ambito IT e sicurezza nella regione EMEA è fortemente d'accordo sul fatto di sapere chi contattare in caso di attività sospette.
- Solo il 76% dei professionisti in ambito IT e sicurezza nella regione EMEA ha dichiarato di collaborare con altri operatori del settore quando si tratta di condividere informazioni sulle minacce, percentuale inferiore alla media di U.S.A. e APJ. Pur essendo un numero elevato, ciò indica che c'è ancora molto lavoro da fare se si vuole proteggere tutti i settori dagli attacchi informatici.
- Solo il 33% dei professionisti in ambito IT e sicurezza nella regione EMEA ha denunciato alle autorità un atto ostile, percentuale inferiore ai livelli di U.S.A. (63%) e APJ (61%).
- Quasi 2 professionisti in ambito IT e sicurezza su 10 (18%) nella regione EMEA hanno dichiarato che la loro organizzazione non dispone di un piano di emergenza in caso di rilevamento di guerra informatica.
- Solo un terzo (33%) dei professionisti in ambito IT e sicurezza dispone di un piano di azione in caso di attacco informatico convalidato che sia appropriato e proporzionato con scenari di riferimento che implementino le migliori pratiche.
- Inoltre, meno della metà (49%) delle società è solita istruire i propri dipendenti o limitare i diritti di amministrazione della rete (40%). Un numero ancora inferiore ha implementato pratiche di cybersecurity quali la creazione di una cultura lavorativa incentrata sulla sicurezza (37%), l'investimento in un'assicurazione per la cybersecurity (31%) e l'implementazione di uno scenario di riferimento per il rischio cyber (31%).

Esiste uno scostamento tra i livelli di fiducia nella preparazione agli attacchi informatici (84%) e la realtà ed è necessario investire per colmare questo divario, sia per gli strumenti sia per i servizi. Alla richiesta di scegliere quando investiranno in determinati aspetti, i professionisti IT hanno dato le seguenti risposte:



LA REGOLAMENTAZIONE SPINGE VERSO IL FUTURO

I governi, i servizi di sicurezza e le relative autorità competenti continuano a porre l'accento sulla necessità di migliorare la posizione in materia di cybersecurity e sulla necessità imperativa di una strategia più resiliente dal punto di vista della cybersecurity. Il recente Cyber Resilience Act dell'UE si basa sull'attuale Direttiva sulla cybersecurity del 2016 e aggiorna quindi i requisiti per una migliore protezione da parte degli Stati membri. Prima del Cyber Resilience Act dell'UE, gran parte della pressione in materia di cybersecurity veniva esercitata sugli utenti di questi prodotti, sia imprese sia privati. Ora anche il produttore condividerà una parte maggiore di questa responsabilità. La responsabilità può contribuire a migliorare la situazione in generale. Anche l'UE ha rilasciato la NIS2, accendendo i riflettori su molti altri settori verticali e introducendo multe, sanzioni e penalità per la mancata gestione del rischio, piano di protezione informatica e i ritardi ingiustificati delle azioni correttive.

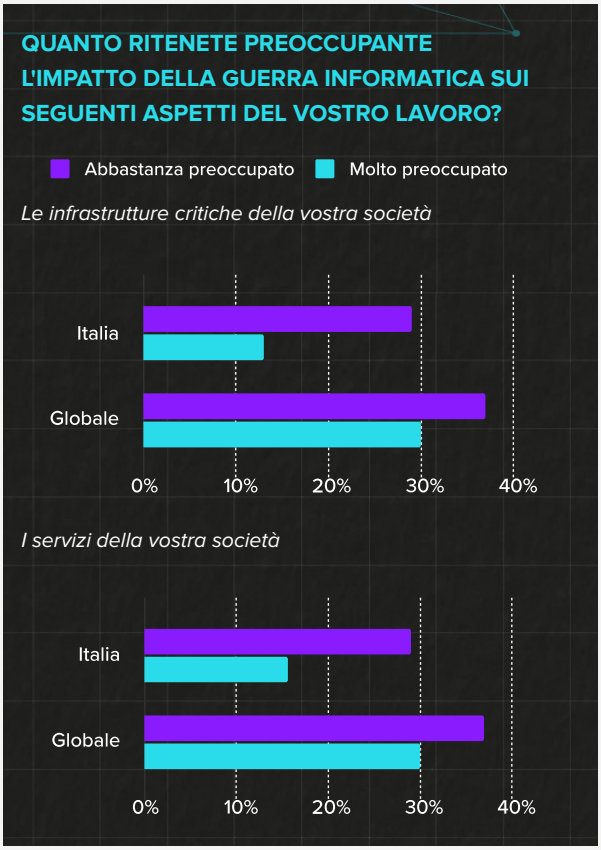
L'emergere di normative è un ottimo spunto di conversazione e sicuramente aiuterà a colmare il divario di investimenti in determinati strumenti e a dare priorità alla loro importanza, ma c'è ancora molta strada da fare per mettere in sicurezza le lacune critiche di vulnerabilità introdotte dalla proliferazione esponenziale di risorse connesse. Il 37% degli intervistati concorda sul fatto che i dispositivi connessi sono una priorità assoluta in caso di attacco di guerra informatica.

Al di là degli sforzi interni, i professionisti IT ritengono che l'Unione Europea e i suoi Stati membri debbano rafforzare la cooperazione con gli altri alleati nel mondo. Oltre la metà (61%) ha dichiarato che sarebbe favorevole alla creazione di una lega di difesa cyber se il proprio Paese fosse coinvolto in un conflitto informatico.

TENDENZE IN ITALIA DAL ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

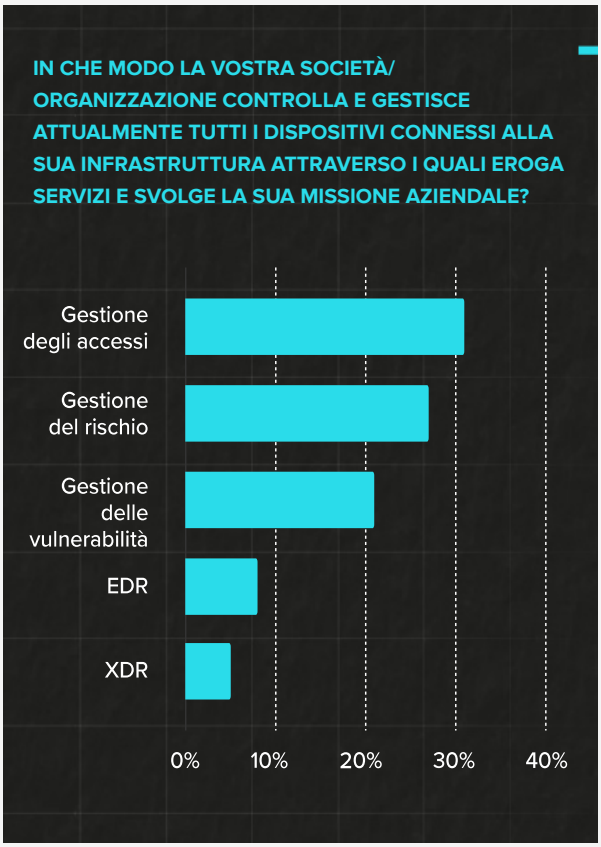
LE PREOCCUPAZIONI DIFFERISCONO DALLA REALTÀ RISPETTO AL CONTESTO GEOPOLITICO

Rispetto al resto del mondo, l'Italia è mediamente meno preoccupata dell'impatto della guerra informatica sulle infrastrutture critiche delle aziende e dei relativi servizi. Alla domanda sulla consapevolezza dei rischi che una guerra di questo genere comporta, il 29% degli intervistati italiani ha riferito di considerare gli attacchi informatici come un rischio strategico trascurabile per l'organizzazione, un dato significativamente inferiore rispetto 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 in ambito di sicurezza.



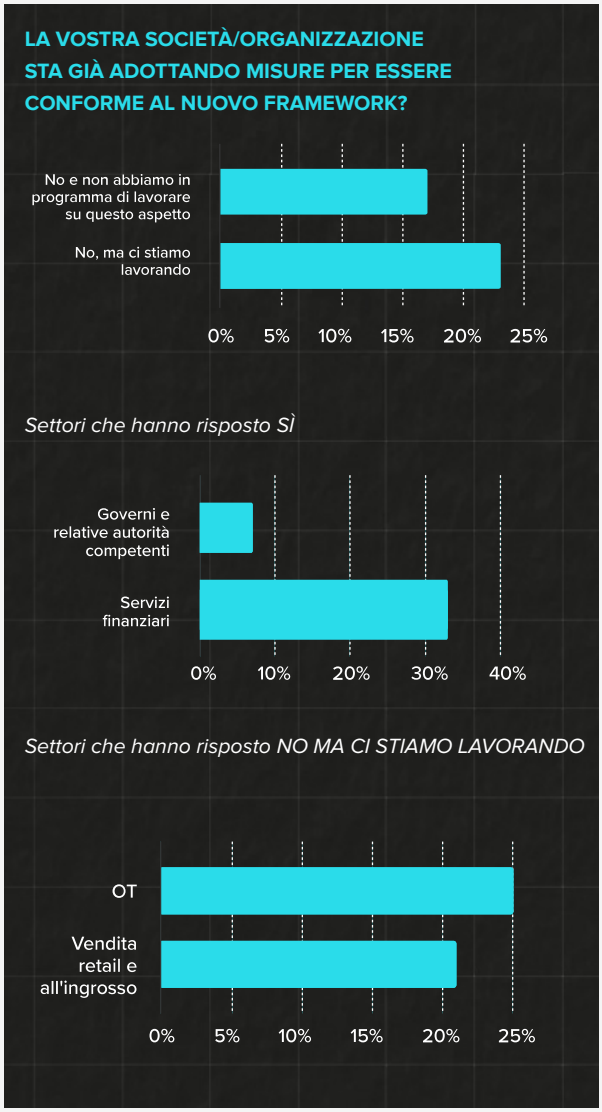
La ricerca ha riguardato anche la fiducia nel governo per quanto riguarda la difesa di fronte a un attacco informatico, con risultati interessanti. A livello globale, il 33,5% si sente molto fiducioso dell'impegno delle proprie organizzazioni governative, mentre solo il 18% degli intervistati in Italia ha la stessa fiducia.

Inoltre, una minoranza afferma che la propria società attualmente controlla e gestisce tutti i dispositivi connessi alla propria infrastruttura tramite i quali eroga servizi e svolge la propria missione aziendale attraverso la gestione degli accessi (31%), la gestione del rischio (27%) o la gestione delle vulnerabilità (21%). Una piccola minoranza lo fa attraverso l'eDR (8%) o l'XDR (5%).



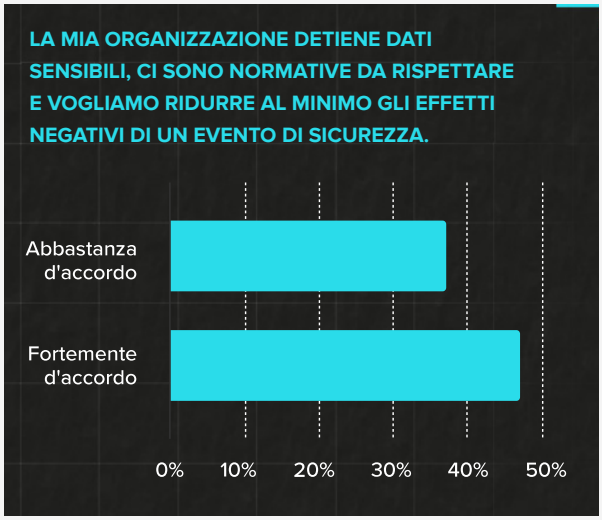
LA CONFORMITÀ NON È UNA PRIORITÀ: LO SCENARIO DI RIFERIMENTO PER LA PROTEZIONE DEI DATI E LA CYBERSECURITY

L'Italia ha creato il Framework nazionale per la Cybersecurity e la Data Protection: uno standard di riferimento adottato da tipologie di organizzazioni molto diverse tra loro come strumento per coordinare la propria strategia di difesa contro gli attacchi informatici. Nonostante ciò, oltre 2 aziende su 5 (41%) dichiarano che la loro società non si sta attivando per essere conforme al nuovo Framework e solo il 7% 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, c'è meno preoccupazione 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, ci sono regolamenti da rispettare e vogliono ridurre al minimo qualsiasi effetto negativo di un

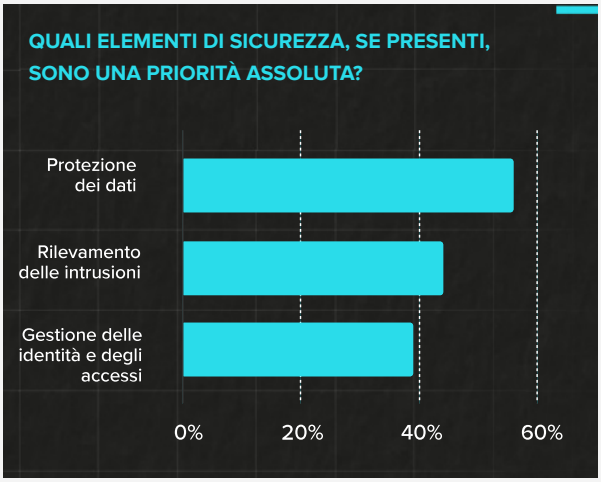
evento di sicurezza. La protezione dei dati è un imperativo per tutti i Paesi dell'UE e, sebbene la consapevolezza della sua importanza sia evidente, sembra esserci uno scostamento con l'effettiva conformità alle norme.

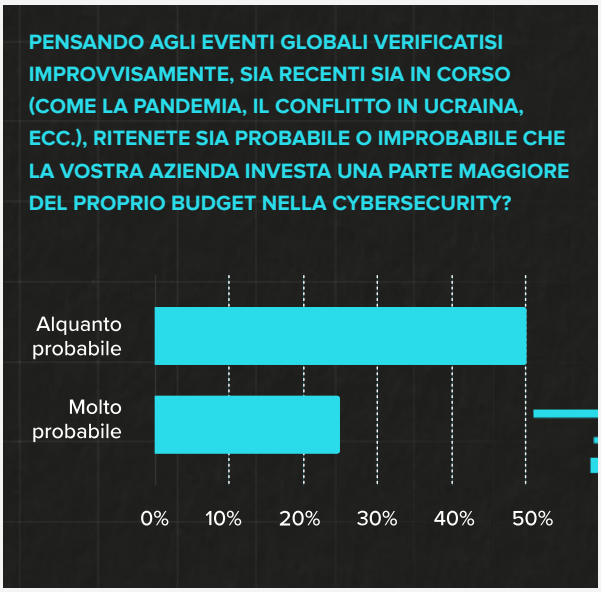


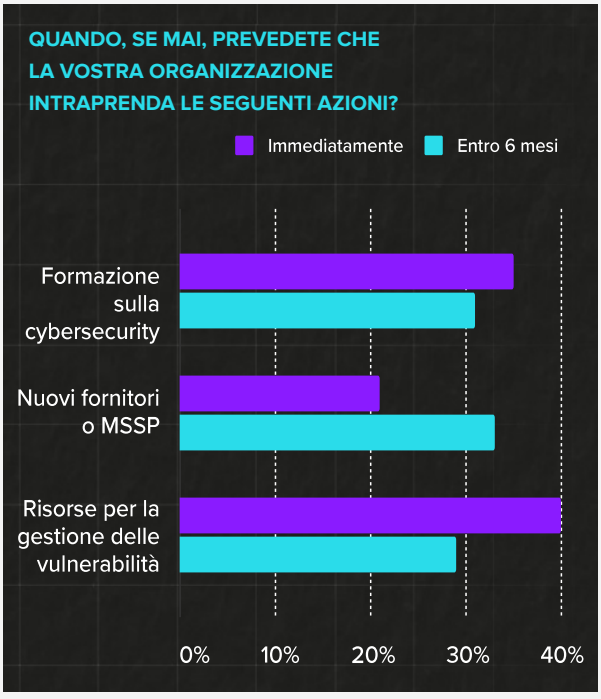
LA POSIZIONE IN MATERIA DI SICUREZZA DEVE ESSERE RAFFORZATA

Le organizzazioni italiane stanno migliorando il loro approccio nei confronti delle minacce informatiche, ma occorre ancora adottare ulteriori misure. L'attenzione principale è rivolta alla protezione dei dati, al rilevamento delle intrusioni e alla gestione delle identità e degli accessi, che gli intervistati hanno indicato come le loro attuali priorità principali, mentre la prevenzione di possibili attacchi alla supply chain e il monitoraggio dei computer 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.







PERCHÉ QUESTI RISULTATI SONO IMPORTANTI?

I risultati del Armis State of Cyberwarfare and Trends Report: 2022-2023 dimostrano la crescente preoccupazione delle organizzazioni per l'aumento della frequenza e della gravità degli attacchi informatici, nonché per la minaccia di una guerra. Il panorama dei rischi, sempre più complesso e sofisticato, ha un impatto su diverse aree aziendali, in tutti i settori. Tuttavia, il ritmo e le priorità nella progettazione e nell'adozione di strategie di cybersecurity sono ancora diversi.

"La guerra informatica è il futuro del terrorismo ai massimi livelli, in quanto fornisce un metodo di attacco asimmetrico ed economicamente vantaggioso che richiede una sorveglianza e una spesa costanti per difendersi". "La guerra informatica clandestina sta rapidamente diventando un ricordo del passato. Oggi assistiamo già a sfacciati attacchi informatici da parte di stati nazione, spesso con l'intento di raccogliere informazioni, interrompere le operazioni o distruggere completamente i dati. Sulla base di queste tendenze, tutte le organizzazioni dovrebbero considerarsi potenziali bersagli di attacchi di guerra informatica e proteggere le proprie risorse di conseguenza".

NADIR IZRAEL
CTO E CO-FONDATORE DI ARMIS

"Dai risultati di questo resoconto emerge chiaramente che le organizzazioni italiane non condividono le preoccupazioni della maggior parte degli altri paesi per quanto riguarda la minaccia della guerra informatica e che hanno ancora molta strada da fare per quanto riguarda la conformità." "Entrambi questi problemi possono essere affrontati con una maggiore visibilità delle risorse, gestione delle vulnerabilità e 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 in materia di sicurezza".

NICOLA ALTAVILLA
COUNTRY MANAGER ITALIA E AREA MEDITERRANEA DI ARMIS

COSA PUÒ FARE LA VOSTRA ORGANIZZAZIONE PER PROTEGGERSI?

Vista la situazione, cosa possono fare le organizzazioni? Il rilevamento precoce e il monitoraggio continuo sono il modo migliore per migliorare la posizione dell'organizzazione in materia di sicurezza e rimediare rapidamente. Dopotutto, se non si sa di avere un problema, non lo si può nemmeno risolvere. Analogamente, se non si riesce a vedere una risorsa, non la si può proteggere. È qui che Armis può aiutarvi.

ARMIS ASSET INTELLIGENCE PLATFORM

La **Armis Asset Intelligence Platform (piattaforma intelligente sulle risorse di Armis)** fornisce una visibilità unificata delle risorse e la sicurezza di tutti i tipi di risorse, incluse la tecnologia dell'informazione (Information Technology, IT), l'Internet delle Cose (Internet Of Things, IoT), la tecnologia operativa (Operational Technology, OT), l'Internet delle Cose del mondo sanitario (Internet Of Medical Things, IoMT), cloud e IoT cellulare, sia gestiti sia non gestiti. La piattaforma di Armis, fornita come piattaforma software-as-a-service (SaaS) agentless, si integra perfettamente con gli stack IT e di sicurezza esistenti per fornire rapidamente i dati contestuali utili che occorrono per migliorare la posizione in materia di sicurezza dell'organizzazione senza influire negativamente sulle operazioni in corso o sui flussi di lavoro. Armis aiuta i clienti a proteggersi da rischi operativi e informatici invisibili, ad aumentare l'efficienza, a ottimizzare l'uso delle risorse e a innovare in modo sicuro grazie alle nuove tecnologie per far crescere il loro business, indipendentemente dalla minaccia, dalla guerra informatica o da altro.

Registratevi oggi stesso per una **valutazione dei rischi per la sicurezza** per sapere quali sono le risorse più vulnerabili agli attacchi. Utilizzate tali informazioni per definire le priorità della vostra strategia di mitigazione dei rischi e garantire la piena conformità agli scenari normativi che richiedono l'identificazione e la definizione delle priorità di tutte le vulnerabilità.

Per richiedere una demo personalizzata ad Armis, potete visitare il sito web: armis.com/demo.

Per approfondire i risultati del Armis State of Cyberwarfare and Trends Report: 2022-2023 su scala globale, potete visitare il sito web: **armis.com/cyberwarfare.**

STATO DELLA

GUERRA INFORMATICA

INFORMAZIONI SU 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 nuova 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 California.

armis.com

info@armis.com

20230110-1

ARMIS®