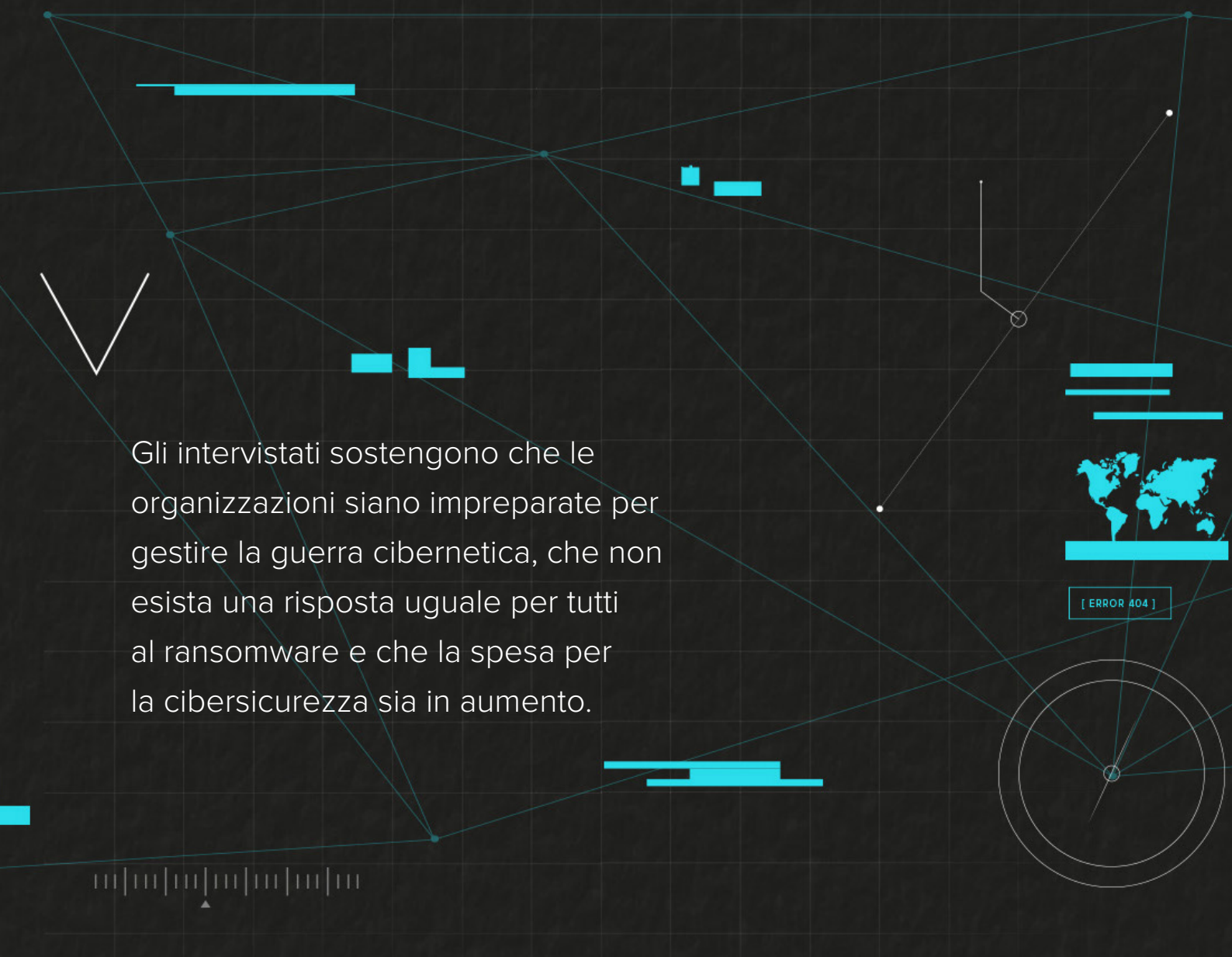
ARMIS®

STATO DELLA
GUERRA CIBERNETICA

# RESOCONTO SULLO STATO DELLA GUERRA CIBERNETICA E SULLE TENDENZE DI ARMIS: 2022-2023

IDENTIFICA L'OPINIONE DEI PROFESSIONISTI IN AMBITO IT E SICUREZZA A LIVELLO GLOBALE SULLA SPESA E SULLA PREPARAZIONE IN MATERIA DI CIBERNETICA.




Gli intervistati sostengono che le organizzazioni siano impreparate per gestire la guerra cibernetica, che non esista una risposta uguale per tutti al ransomware e che la spesa per la cibersicurezza sia in aumento.

# PREFAZIONE DI NADIR IZRAEL

## CTO E CO-FONDATORE DI ARMIS

Armis è lieta di poter condividere con voi i risultati della nostra ricerca sulla guerra cibernetica globale e della nostra analisi di mercato. Ci auguriamo che i contenuti di questo resoconto globale e dei resoconti regionali ad esso collegati siano preziosi e utili.

Consideriamo meglio il contesto in cui operiamo oggi; **gli analisti più importanti**[1] prevedono che entro il 2025 gli hacker avranno armato gli ambienti di tecnologia operativa (OT) per danneggiare o uccidere con successo gli esseri umani. Sebbene questa previsione possa sembrare estrema, è alla base di una tendenza della guerra cibernetica che vede i player delle minacce passare dal campo della ricognizione e dello spionaggio all'applicazione cinetica degli strumenti di guerra cibernetica. Queste armi cibernetiche cinetiche sono già state scoperte sul campo, anche se nessuna in particolare è stata impiegata con effetti letali. Ad esempio, il malware Triton scoperto nel 2017 **ha preso di mira e disabilitato**[2] i controller del sistema di sicurezza strumentale (SIS) di un impianto petrolchimico dell'Arabia Saudita, che avrebbe potuto contribuire a un disastro dell'intero impianto se il problema non fosse stato identificato. E nel **febbraio 2021**[3], un hacker ha tentato di avvelenare l'impianto di approvvigionamento idrico di una piccola città statunitense nello stato della Florida tramite un accesso remoto. Abbiamo già visto attacchi ransomware contro il settore sanitario **causare vite umane**[4]; quindi il potenziale impatto degli attacchi cibernetici, intenzionali o meno, è chiaro.

Mentre le minacce cibernetiche cinetiche sono il futuro della corsa agli armamenti cibernetici, le armi cibernetiche non sono certo un concetto nuovo. Il mondo ha avuto modo di sbirciare nell'arsenale cibernetico della **National Security Agency**[5] (NSA) nel 2016 grazie alle fughe di notizie pubblicate dagli **Shadow Brokers**[6]**,** che hanno messo a nudo alcune delle armi cibernetiche più potenti e invisibili del pianeta. Questo arsenale cibernetico trapelato, che includeva la vulnerabilità EternalBlue, è diventato la base di alcune delle compromissioni più estese della storia, tra cui NotPetya e WannaCry.

Lo sviluppo di queste armi cibernetiche ha anche accelerato un intero settore noto come mercato degli zero-day: un gruppo enigmatico di ricercatori, broker e siti web dedicati a trarre profitto dagli exploit zero-day. Sebbene nessuno conosca l'esatto ammontare in dollari del settore nel suo complesso, i listini prezzi pubblicati apertamente hanno rivelato che il prezzo di un exploit zero-click funzionante è pari a **2,5 milioni di dollari per Android e 2 milioni di dollari per iOS**[7].

Il panorama continua a evolversi in modo significativo ed è cambiato in modo monumentale negli ultimi cinque anni, soprattutto a seguito dell'invasione dell'Ucraina da parte della Russia nel febbraio 2022. In quanto tale, i leader aziendali e IT devono comprendere l'evoluzione del panorama delle minacce, in modo da poter migliorare la propria posizione in materia di cibersicurezza per difendersi da questi attacchi; ed è per questo che abbiamo creato il **Resoconto sullo stato della guerra cibernetica e sulle tendenze di Armis: 2022-2023**[8]. Per la stesura di tale resoconto, Armis ha commissionato uno studio proprietario a 6.021 professionisti in ambito IT e sicurezza in aziende con oltre cento dipendenti in U.S.A., Regno Unito, Spagna, Portogallo, Francia, Italia, Germania, Austria, Svizzera, Australia, Singapore, Giappone, Paesi Bassi e Danimarca. Inoltre, 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. Le domande poste agli intervistati comprendevano:

- Ritenente che la vostra organizzazione sia preparata a gestire una guerra cibernetica?
- In che misura siete fiduciosi, se lo siete, che il governo del Paese in cui ha sede la vostra azienda sia in grado di difendersi dalla guerra cibernetica?
- Qual è la politica della vostra organizzazione in merito al pagamento di riscatti in caso di attacco ransomware?
- Quali sono le pratiche di cibersicurezza implementate nella vostra organizzazione?

Le risposte a queste e ad altre domande sono state utilizzate per determinare l'opinione dei professionisti in ambito IT e sicurezza a livello globale, regionale e nazionale, caso per caso, al fine di avere un quadro delle seguenti tendenze. Diamo uno sguardo più da vicino ai risultati e al loro rapporto con il modo in cui le organizzazioni possono migliorare la propria posizione in materia di cibersicurezza per difendersi dagli attacchi di guerra cibernetica.

# GUERRA CIBERNETICA

cyberwarfare /ˈsʌɪbəˌwɔːfɛː/

SOSTANTIVO:

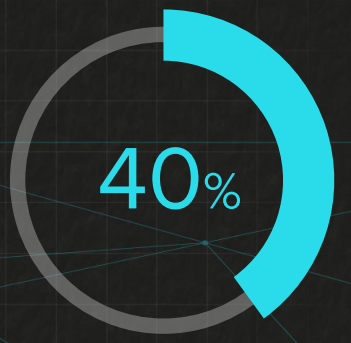
l'utilizzo di attacchi cibernetici che causano danni paragonabili a quelli di una guerra vera e propria e/o interrompono sistemi o servizi vitali. Alcuni esiti previsti potrebbero essere spionaggio, sabotaggio, propaganda, manipolazione dell'opinione pubblica, intimidazione o interruzione di servizi critici.

# INDICE DEI CONTENUTI

# LE ORGANIZZAZIONI SONO PREPARATE AD AFFRONTARE LA TEMPESTA CHE COMPORTA LA GUERRA CIBERNETICA?

## Principali risultati del resoconto globale.

APPROFONDIMENTO




Il 40% dei dirigenti di livello superiore al quadro (CTO, CIO e CISO) ha dichiarato di aver riscontrato una maggiore attività di minaccia nello stesso periodo. Tra gli intervistati di livello dirigenziale superiore al quadro, quelli appartenenti a settori quali alimenti e bevande (44%), telecomunicazioni (44%), automotive (43%), vendita retail/all'ingrosso (42%) e tecnologia (42%) hanno registrato un aumento delle attività di minaccia superiore alla media.

Secondo lo studio Armis, un terzo (33%) delle organizzazioni globali non prende sul serio la minaccia della guerra cibernetica. Queste organizzazioni si dichiarano indifferenti o non preoccupate dell'impatto della guerra cibernetica sulla loro organizzazione nel suo complesso, lasciando spazio a lacune nella sicurezza. Inoltre, le crescenti tensioni geopolitiche derivanti dalla guerra in Ucraina hanno reso molto più plausibile la minaccia di un attacco di guerra cibernetica. Oltre il 64% dei professionisti in ambito IT e sicurezza intervistati da Armis concorda sul fatto che la guerra in Ucraina ha creato una maggiore minaccia di guerra cibernetica e oltre la metà (54%) degli intervistati che sono gli unici responsabili della sicurezza IT ha dichiarato di aver riscontrato una maggiore attività di minaccia sulla propria rete tra maggio e ottobre 2022 rispetto ai sei mesi precedenti. Non sorprende quindi che il 45% degli intervistati abbia dovuto denunciare alle autorità un atto di guerra cibernetica.

## INTERVISTATI DI LIVELLO DIRIGENZIALE SUPERIORE AL QUADRO:

*Negli ultimi sei mesi avete riscontrato una maggiore o minore attività di minaccia, qualora presente, sulla vostra rete rispetto ai sei mesi precedenti?*

| SETTORI VERTICALI | SETTORE INDUSTRIALE | MAGGIORE | UGUALE | MINORE | N/D | NON SAPREI |
|---|---|---|---|---|---|---|
| **Governo** | Governo, autorità locale, ente del settore pubblico | **39%** | 44% | 14% | 3% | |
| **Servizi finanziari** | Servizi finanziari e assicurazioni | **20%** | 70% | 10% | | |
| **Settore sanitario** | Medico, sanitario, farmaceutico | **26%** | 52% | 20% | 2% | |
| **Tecnologia operativa (OT)** | Automotive | **43%** | 33% | 24% | | |
| | Distribuzione, logistica, trasporti | **30%** | 48% | 19% | 4% | |
| | Alimenti e bevande | **44%** | 44% | 11% | | |
| | Produzione, ingegneria | **40%** | 30% | 8% | 22% | |
| | Petrolio, gas, minerario, edilizia, agricoltura | **30%** | 50% | 15% | 5% | |
| | Trasporto | **32%** | 36% | 18% | 14% | |
| | Servizi di pubblica utilità: Energia e acqua | **15%** | 62% | 15% | 8% | |
| **Totale OT** | | **37%** | 35% | 12% | 16% | |
| **Altro** | Beneficenza, no-profit | **29%** | 29% | 14% | 29% | |
| | Altro (specificare) | **33%** | 43% | 5% | 10% | 10% |
| | Tecnologia | **42%** | 25% | 30% | 2% | 1% |
| **Totale altri settori** | | **42%** | 25% | 29% | 2% | 1% |
| **Settore retail** | Servizi di vendita retail/ all'ingrosso | **42%** | 40% | 15% | 3% | |
| **Telecomunicazioni** | Telecomunicazioni, servizi via cavo, servizi satellitari | **44%** | 38% | 18% | | |
| **Totale complessivo** | | **40%** | 31% | 22% | 6% | 0,5% |

I dati proprietari della piattaforma di asset intelligence e sicurezza di Armis, raccolti dal 1° giugno 2022 al 30 novembre 2022, hanno confermato che le suddette tendenze non hanno subito un rallentamento, anzi, sono peggiorate. Le attività di minaccia contro il pacchetto clienti 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.

Il peggioramento del panorama delle minacce ha avuto un impatto tangibile sui progetti di trasformazione digitale a livello globale, rallentando l'innovazione in tutto il mondo. Oltre la metà (55%) degli intervistati dichiara che la loro organizzazione ha bloccato o interrotto i progetti di trasformazione digitale a causa di tali minacce. Questa percentuale è persino più alta in alcuni Paesi, tra cui Australia (79%), Stati Uniti (67%), Singapore (63%), Regno Unito (57%) e Danimarca (56%).

Vista l'ansia per la crescente minaccia di guerra cibernetica e il costo medio di una violazione dei dati negli Stati Uniti di **9,44 milioni di dollari**[9] e di


Sebbene tutti i settori siano a rischio di attacchi cibernetici, si distinguono in particolar modo le infrastrutture critiche, il settore sanitario e le agenzie governative, poiché rappresentano obiettivi interessanti per i player degli stati nazione. Il settore sanitario è interessante per l'ampiezza della superficie d'attacco e per l'effetto che un attacco può avere sui processi critici e sulla salute e sicurezza dei pazienti. Le agenzie governative sono interessanti per i dati che conservano e le infrastrutture critiche continuano a essere una priorità assoluta, data la loro importanza per la sicurezza nazionale ed economica.

4,35 milioni di dollari a livello globale, non c'è da stupirsi che gli analisti del settore **prevedano**[10] che la spesa mondiale per la sicurezza e la gestione del rischio crescerà dell'11,3% nel 2023. I modelli di lavoro ibrido e remoto, la transizione dalle reti private virtuali (VPN) all'accesso di rete Zero Trust (ZTNA) e il passaggio alla fornitura basata su cloud sono tutti fattori che contribuiscono, ma ciò che si riduce in realtà è una superficie d'attacco in continua espansione unita a una preponderanza di Paesi in grado di sviluppare armi cibernetiche sofisticate. In definitiva, le organizzazioni

digitalizzate e realmente connesse possono permettersi di non aumentare la spesa cibernitica?

Sebbene sussista il rischio che la guerra cibernetica abbia un impatto su un'organizzazione, la difesa e la resilienza cibernetica contro tali attacchi rimangono modeste. Sempre più stati nazione hanno spostato la propria attenzione dalle infrastrutture critiche all'attacco di entità commerciali di ogni forma e dimensione. Paradossalmente, questa ricerca ha rilevato che quasi un quarto (24%) delle organizzazioni globali si sente impreparato a gestire la minaccia di guerra cibernetica, eppure l'elemento di sicurezza meno tenuto in considerazione dai professionisti in ambito IT e sicurezza è proprio la prevenzione di un attacco da parte di uno stato nazione. Inoltre, anche per le organizzazioni disposte a investire denaro per un robusto programma di cibersicurezza (approfondiremo le tendenze di spesa più avanti), trovare le persone che ricoprono ruoli di cibersicurezza con le competenze necessarie per monitorare efficacemente le tecnologie e i software correlati continua a essere un problema. Il numero di posti di lavoro non coperti nel settore della cibersicurezza in tutto il mondo **è cresciuto del 350%**[11] tra il 2013 e il 2021, passando da un milione a 3,5 milioni. Si prevede che nel 2025 vi sarà lo stesso numero di posizioni di lavoro ancora aperte.

# QUALI SONO I SETTORI PIÙ VULNERABILI?

## MINACCE ALLE INFRASTRUTTURE CRITICHE

Con il prolungarsi del conflitto in Ucraina, nel 2022 gli enti internazionali hanno lanciato numerosi allarmi sulle operazioni cibernetiche russe dannose che hanno come obiettivo le infrastrutture critiche. Degni di nota sono Industroyer2 e InController/ PipeDream: strumenti di attacco modulari destinati alle tecnologie operative (OT) di tutti i settori che comprendono sistemi di controllo di supervisione e acquisizione dati (SCADA), sistemi di controllo distribuiti (DCS), unità terminali remote (RTU) e ambienti operativi di controller logici programmabili (PLC).

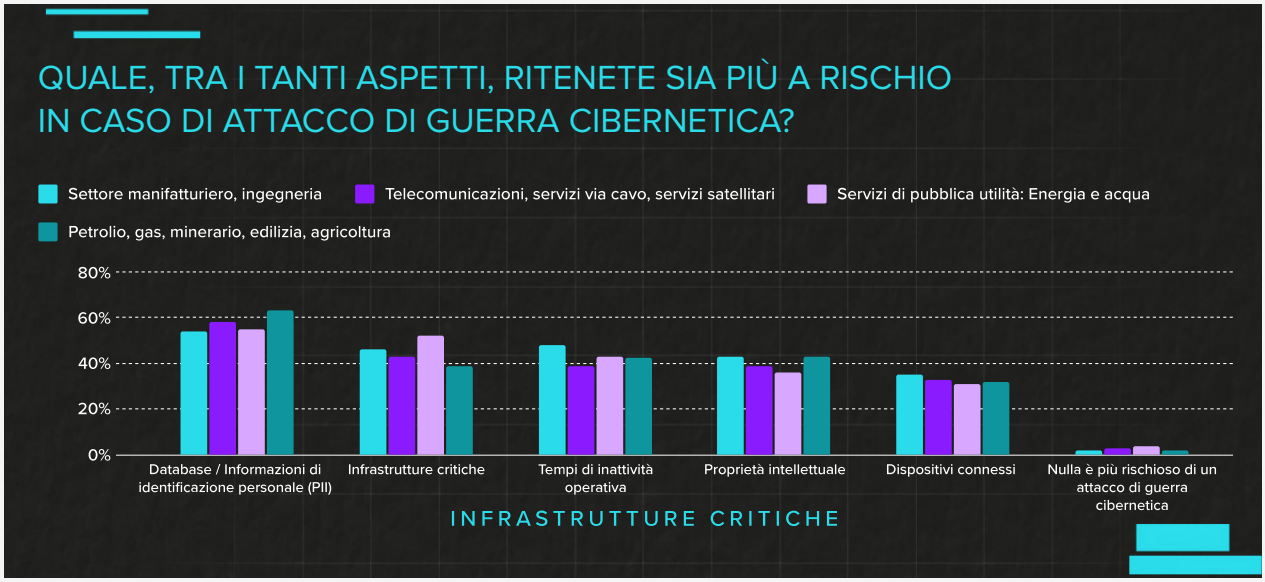
Nel maggio 2021, la **Colonial Pipeline**[12], che controlla quasi la metà della benzina, del cherosene e del gasolio che fluiscono lungo la costa orientale degli Stati Uniti, è stata vittima di un attacco ransomware interno all'IT, che ha colpito le operazioni OT. L'hack di Colonial Pipeline è il più grande attacco cibernetico contro le infrastrutture critiche degli Stati Uniti ad oggi reso noto pubblicamente. Dopo un confronto con il Federal Bureau of Investigation (FBI), il Department of Energy (DOE), il Department of Homeland Security (DHS) e la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti, Colonial Pipeline ha preso la difficile decisione di pagare il riscatto in criptovaluta richiesto dagli hacker di DarkSide.

La società ha ritenuto che pagare per ottenere la chiave di decrittazione fosse il modo migliore per rimettere l'oleodotto in funzione in modo rapido e sicuro. Circa un mese dopo, l'FBI è riuscita a recuperare la maggior parte del pagamento del riscatto sequestrando i bitcoin appartenenti agli hacker.

La guerra cibernetica tra stati nazione non si limita ai vicini confinanti o ai partecipanti attivi al conflitto. Gli aggressori possono prendere di mira altri Paesi per una serie di motivi, legati (ad esempio, la fornitura di armi) o meno al conflitto. Nel 2021, gli Stati Uniti hanno formalmente accusato Nobelium, un player statale dei servizi segreti esteri della Russia, di aver realizzato l'hack SolarWinds per infiltrarsi nelle reti governative degli Stati Uniti e dell'UE. L'attacco Nobelium ha modificato il panorama delle minacce per quasi tutti i settori. Nell'ottobre del 2022, il gruppo di hacker filo-russo Killnet ha lanciato **decine di attacchi DDoS**[13] contro il settore aeronautico statunitense e ha proclamato che tutte le infrastrutture critiche degli Stati Uniti dovrebbero essere sotto attacco persistente.

Le notizie di questi continui e crescenti attacchi di guerra cibernetica e gli sforzi delle organizzazioni pubbliche e private per aumentare la consapevolezza non sono stati ignorati dai leader aziendali. Il resoconto sullo stato della guerra cibernetica e sulle tendenze di Armis: 2022-2023 ha rilevato che il 74% degli intervistati a livello mondiale responsabili di infrastrutture OT critiche concorda sul fatto che i consigli di amministrazione stanno modificando la cultura dell'organizzazione verso la cibersicurezza in risposta alla minaccia della guerra cibernetica.

Se si considerano i settori più comunemente associati alle infrastrutture critiche (vedi tabella seguente), la convergenza dell'IT e della tecnologia operativa (OT) nell'Industria 4.0 risulta evidente dalle risposte. Agli intervistati è stato chiesto di selezionare fino a tre elementi maggiormente a rischio in caso di attacco di guerra cibernetica. In ogni settore, i database e le informazioni di identificazione personale (PII) sono stati classificati come i più preoccupanti. Le infrastrutture critiche (attrezzature e strutture fisiche), i tempi di inattività operativa e la proprietà intellettuale si sono posizionati nella fascia media delle aree a rischio, mentre i dispositivi connessi sono risultati la preoccupazione minore in tutti i settori delle infrastrutture critiche.




Le risposte indicano una serie di preoccupazioni negli ambienti IT[14], OT[15] e dei sistemi di controllo industriale (ICS)[16], il che non sorprende data la recente e rapida convergenza di questi sistemi un tempo disparati. Molti sistemi ICS e OT nelle infrastrutture critiche sono stati costruiti decenni fa e sono ancora protetti in gran parte tramite metodi tradizionali basati sulla progettazione della rete e sull'accesso basato sui ruoli. Man mano che questi ambienti diventano più interconnessi e automatizzati, la superficie d'attacco si espande all'intersezione tra le reti esistenti e le risorse che non sono mai state destinate a connettersi a tali reti.

Tale intersezione di risorse connesse è ciò che spinge Armis a condurre ricerche sulle vulnerabilità di sicurezza per contribuire a diffondere la consapevolezza delle vulnerabilità e degli attacchi che colpiscono le infrastrutture critiche. Nel marzo 2022, il team di ricerca di Armis ha rivelato pubblicamente tre vulnerabilità zero-day che potrebbero avere un impatto su oltre 20 milioni di dispositivi del gruppo di continuità intelligente (UPS) di APC, che forniscono energia di backup di emergenza per le risorse critiche in data center, impianti industriali, ospedali e altro ancora. Queste vulnerabilità, note collettivamente come TLStorm[17], consentono ai player delle minacce di disabilitare, interrompere e distruggere questi dispositivi UPS e le risorse collegate. Lo sfruttamento di queste vulnerabilità può consentire a un aggressore di armare i dispositivi UPS, ad esempio manomettendo la tensione fino a farli bruciare e andare letteralmente in fumo. Queste vulnerabilità si verificano nei sistemi ciberfisici che fanno da ponte tra il mondo digitale e quello fisico. In quanto tali, sono ancora più critiche da identificare, in quanto danno agli attacchi cibernetici la possibilità di avere conseguenze nel mondo reale e pericolose per la vita e/o possono portare alla distruzione fisica dell'infrastruttura presa di mira.

# MINACCE AL SETTORE SANITARIO

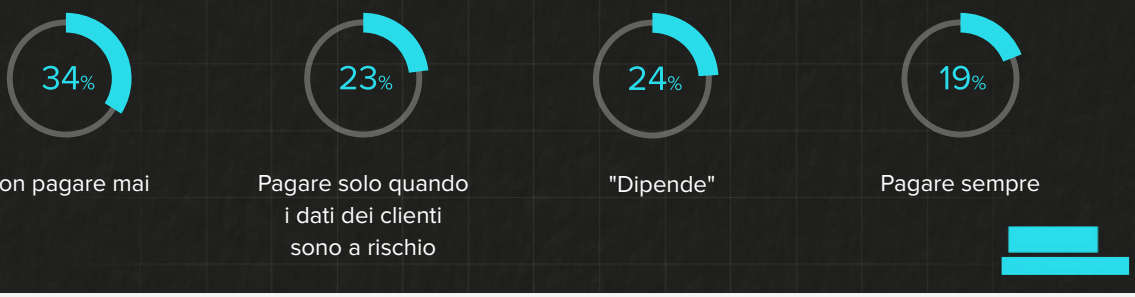
Il settore sanitario è di importanza cruciale per i cittadini di ogni nazione. È vitale per il funzionamento di qualsiasi società e svolge un ruolo fondamentale nello sviluppo di qualsiasi stato moderno. A causa delle conseguenze nel mondo reale e pericolose per la vita, quando la sicurezza dei pazienti è a rischio, il settore sanitario continua a essere uno dei principali obiettivi dei player malintenzionati. Ad esempio, nell'ottobre 2022, **CommonSpirit Health[18]** ha subito un grave attacco ransomware a un sistema che gestisce 140 ospedali e oltre 1.000 siti di cura in tutti gli Stati Uniti. Alla fine del 2022, questo attacco colpiva ancora quasi 20 milioni di americani in 21 stati e, di conseguenza, gli operatori sanitari fornivano assistenza senza le cartelle cliniche dei loro pazienti. Questo, ovviamente, è un modo molto pericoloso di amministrare il settore sanitario. In uno degli incidenti derivanti da tale attacco, un bambino di tre anni dell'Iowa ha ricevuto una "megadose" di farmaci antidolorifici, ma fortunatamente è sopravvissuto. All'inizio del 2020, un **attacco cibernetico molto più piccolo a un ospedale tedesco di Düsseldorf[19]** ha provocato un'interruzione della rete e la necessità di mandare i pazienti ad altri ospedali, causando la morte di un paziente.

Gli attacchi al settore sanitario non solo sono pericolosi per la vita, ma sono anche estremamente costosi per i sistemi sanitari, che già lavorano con budget ridotti e stanno ancora cercando di riprendersi dall'ondata della pandemia di COVID-19. **I CIO del settore sanitario[20]** faticano a trattenere i talenti chiave della tecnologia e della sicurezza, poiché i lavoratori da remoto cercano di ottenere redditi più elevati in altri settori. Questa riduzione del personale qualificato arriva in un momento critico per le organizzazioni sanitarie, che rimangono uno dei settori più bersagliati dalla guerra cibernetica e dalla criminalità cibernetica. (IBM stima che attualmente il costo medio di una violazione nel settore sanitario sia pari a **10,1 milioni di dollari[21]**, superiore ai 9,44 milioni di dollari stimati per tutti i settori). Quando l'**Health Service Executive[22]** irlandese è stata attaccata dal ransomware Conti nel 2021, il sistema sanitario finanziato con fondi pubblici è stato costretto a passare a processi cartacei, con la conseguente cancellazione dell'80% degli appuntamenti dei pazienti e un costo totale stimato di 600 milioni di dollari per la correzione e la sostituzione dei sistemi.

Secondo tale studio, il 72% degli intervistati responsabili dell'IT nel settore sanitario, medico e farmaceutico concorda sul fatto che i loro consigli di amministrazione stanno cambiando la cultura della loro organizzazione tenendo conto della cibersicurezza in risposta alla minaccia della guerra cibernetica. Tale tendenza è determinata dalla prevalenza e dal costante verificarsi di attacchi cibernetici al settore sanitario: il 45% degli intervistati del settore ha dichiarato di aver riscontrato la stessa quantità di attività di minaccia sulla propria rete tra maggio e ottobre 2022 rispetto ai sei mesi precedenti; mentre il 28% ha dichiarato di aver riscontrato una maggiore attività

## APPROFONDIMENTO

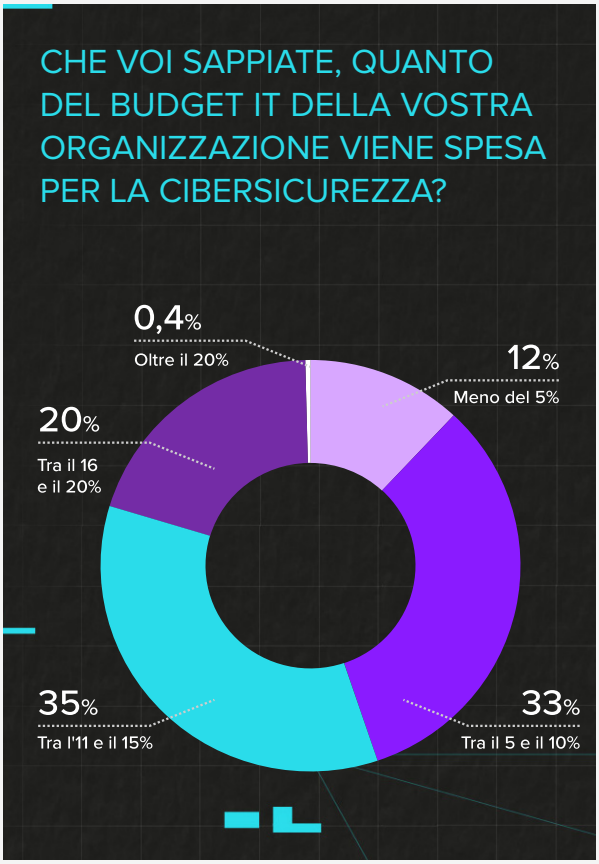
Le organizzazioni sanitarie a livello globale intervistate da Armis hanno indicato che la loro politica sul pagamento dei riscatti in caso di attacco ransomware è la seguente:



di minaccia analizzando gli stessi periodi. Inoltre, gli intervistati hanno dichiarato di essere in qualche modo o molto preoccupati dell'impatto della guerra cibernetica sull'intera organizzazione (70%), sulle infrastrutture critiche della società (72%) e sui servizi della società (68%).

Tuttavia, la spesa per la cibersicurezza delle organizzazioni sanitarie è bassa rispetto ad altri settori a livello globale. Quasi la metà (45%) delle aziende del settore sanitario spende meno del 10% del proprio budget IT per la cibersicurezza. In media, gli intervistati del settore sanitario a livello globale hanno dichiarato di spendere circa l'11% del budget IT della loro azienda per la cibersicurezza, alcuni spendono dall'11 al 15% (35%) o dal 16 al 20% (20%) e pochi spendono il 20% o più (meno dell'1%).

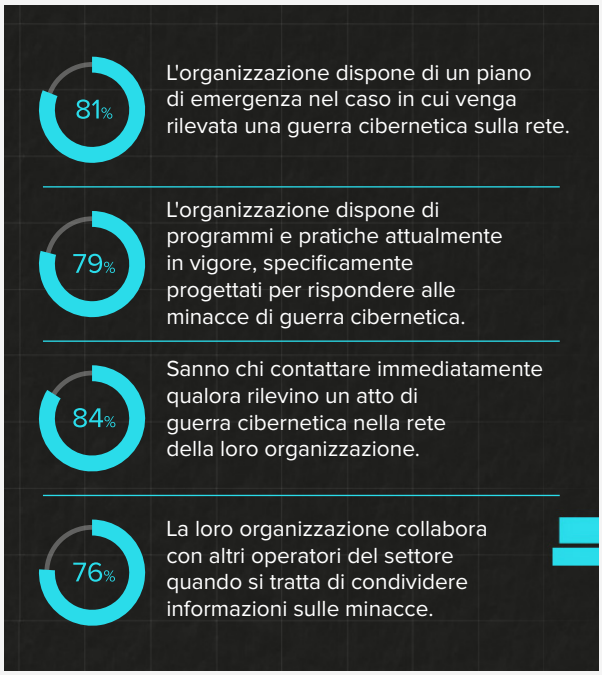
Mentre l'IT del settore sanitario continua a progredire e a digitalizzare l'assistenza ai pazienti, l'innovazione ha il potenziale per affrontare alcune delle principali sfide del settore sanitario, come la carenza di personale, l'aumento dei costi e i problemi di conformità. Tuttavia, il 55% degli intervistati ha dichiarato che la minaccia della guerra cibernetica ha il potenziale per rallentare tale processo di digitalizzazione. Ciò può avere un impatto significativo sulla vita dei pazienti, in quanto il massimo beneficio della digitalizzazione potrebbe venire a mancare se rallentato da attacchi cibernetici. Se la digitalizzazione non viene sfruttata a pieno mettendo la cibersicurezza al primo posto, questi nuovi progetti potrebbero essere sfruttati. Prendiamo ad esempio i sistemi di tubi pneumatici (PTS). Tali sistemi vengono utilizzati in oltre **l'80% degli ospedali del Nord America[23]** e installati in oltre 3.000 ospedali in tutto il mondo, automatizzando la logistica e il trasporto di materiali in tutti gli ospedali attraverso una rete di tubi pneumatici.




Tali sistemi svolgono un ruolo cruciale nell'assistenza ai pazienti e sono utilizzati quasi costantemente. I ricercatori di Armis hanno identificato nove vulnerabilità in questi dispositivi già nel 2021, soprannominate **PwnedPiper[24]**, che, se prese di mira dai criminali cibernetici, potrebbero consentire a un aggressore non autenticato di assumere il controllo completo di un ospedale preso di mira per sferrare un sofisticato attacco ransomware o far trapelare informazioni sensibili dell'ospedale.

# MINACCE ALLE AGENZIE GOVERNATIVE

Le risorse sono il denominatore comune del nostro mondo digitale moderno, globale e sempre più frammentato. E nessuna entità possiede più risorse (persone, dispositivi o software) delle agenzie governative e delle persone che cercano di servire e proteggere. Nonostante quanto accaduto negli ultimi anni, gli intervistati del settore pubblico sono apparentemente sicuri di sé quando si tratta di gestire una guerra cibernetica:




Forse questa maggiore fiducia deriva da una maggiore condivisione delle conoscenze tra le alleanze globali. Le nazioni del Five Eye[25] (Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti), ora condividono in modo proattivo le risorse di intelligence per rafforzare la loro posizione in materia di sicurezza complessiva, in particolare quando si tratta di proteggere le risorse. E, aspetto ancora più interessante, nel caso in cui uno di questi Paesi fosse coinvolto in un conflitto cibernetico, il 63% degli intervistati a livello globale ha dichiarato che sarebbe favorevole all'arruolamento in un'alleanza di difesa cibernetica.

Questa schiacciante dimostrazione di fiducia da parte degli enti viene confermata ancora una volta, in quanto questo sondaggio ha rilevato che 9 intervistati governativi su 10 (90%) sono fiduciosi che la nazione di appartenenza sia in grado di proteggersi dalla guerra cibernetica. Tuttavia, una volta rilevate le violazioni, il 55% degli intervistati a livello globale ritiene che la loro agenzia governativa non sia in grado di affrontare e infine rimediare agli impatti negativi dei criminali cibernetici. Una dimostrazione di ciò si è avuta nell'aprile 2022, quando gli aggressori del gruppo russo di ransomware noto come Conti hanno spodestato il governo del Costa Rica[26]. Il loro sfacciato attacco ha congelato i sistemi fiscali del Paese subtropicale, creando scompiglio nelle esportazioni e ritardando i pagamenti ai lavoratori locali. Tramite l'attacco, Conti è riuscito a far trapelare il 97% di tutti i dati rubati[27]. Nel maggio del 2022, la situazione è peggiorata, tanto da richiedere al governo costaricano di dichiarare lo stato di emergenza.

Negli Stati Uniti, le agenzie governative, le istituzioni e i sistemi educativi hanno risentito dell'effetto "trickle-down" globale dei gruppi di guerra cibernetica. Durante l'apice della pandemia del 2020 negli Stati Uniti, sono stati effettuati 79 attacchi ransomware contro agenzie governative. Si stima che tali enti abbiano perso circa 18,8 miliardi di dollari[28] per i costi di ripristino e il tempo di inattività. Di conseguenza, nel terzo trimestre del 2021 il governo degli Stati Uniti ha lanciato una missione aggressiva per ridurre il volume complessivo del ransomware con StopRansomware.gov[29]. La speranza è che con i partenariati pubblico-privati le agenzie governative, come quelle degli Stati Uniti, possano iniziare a proteggere, rilevare e rimediare meglio all'impatto del ransomware.

## APPROFONDIMENTO

Le organizzazioni governative sono le meno propense, rispetto a qualsiasi altro settore, a pagare un riscatto in caso di attacco ransomware, con il 43% degli intervistati a livello globale che afferma che la politica della propria organizzazione è di non pagare mai (significativamente superiore alla media globale (26%) degli intervistati le cui organizzazioni hanno politiche di non pagare mai).

# QUALI SONO LE TENDENZE DELLA CIBERSICUREZZA A LIVELLO MONDIALE?

## NON ESISTE UNA RISPOSTA UGUALE PER TUTTI AL RANSOMWARE

Molti scambiano gli attacchi ransomware per tentativi di furto di dati critici. La verità, tuttavia, è che la maggior parte delle organizzazioni sono bersagli facili e i criminali cibernetici sono opportunisti. Dopo tutto, è molto più efficiente e redditizio estorcere a queste aziende un riscatto multimilionario per riottenere l'accesso alle propria attività, piuttosto che esfiltrare e vendere centinaia di migliaia di singoli dati sul mercato nero.

Che siano i player degli stati nazione o i criminali cibernetici a distribuire il ransomware, l'anatomia di un attacco ransomware è relativamente la stessa. L'attacco inizia con l'ingresso, che spesso avviene attraverso un sito web compromesso, il phishing o un attacco mirato. Una volta entrati, gli aggressori si muovono lateralmente attraverso la rete, aumentando i privilegi e scavando nella rete. Attraverso l'uso del tunneling, gli aggressori stabiliscono una connessione di comando e di controllo che alla fine porta all'esfiltrazione dei dati di un'organizzazione e al lancio del ransomware che cripta i dati sul sistema bersaglio.

DarkSide è un gruppo di criminali cibernetici dell'Europa dell'Est che ha sviluppato REvil, uno strumento ransomware nato originariamente come variante di GandCrab e che è una delle piattaforme ransomware-as-a-service (RaaS) più note grazie al già citato attacco di Colonial Pipeline del 2021. È apparso per la prima volta nell'aprile 2019 ed è stato al culmine della sua attività fino all'ottobre 2021, quando i server di REvil sono stati violati in un'operazione che ha coinvolto più Paesi e sono stati messi offline. Fino a questo momento, DarkSide forniva il proprio malware agli "affiliati" e divideva il riscatto con i clienti che conducevano gli attacchi. Oltre al malware stesso, DarkSide forniva il meccanismo di decrittazione (che è tuttora considerato uno dei sistemi di decrittazione più sofisticati di tutte le famiglie di malware), l'infrastruttura per le chat darknet, i siti di fuga di notizie darknet e i servizi di riciclaggio di denaro. Con l'aiuto dei broker di accesso iniziale, una categoria emergente di criminali cibernetici che vende l'accesso a una rete compromessa, gli affiliati ottengono l'accesso a una rete bersaglio, lanciano il payload di REvil e negoziano con l'organizzazione colpita un riscatto per ripristinare i dati crittografati.

### APPROFONDIMENTO

**Chi paga e chi non paga?**

Poco più di 3 professionisti IT su 10 (31%) intervistati in una società con oltre 500 dipendenti hanno dichiarato che la politica della loro organizzazione sul pagamento dei riscatti in caso di attacco ransomware è di non pagare mai, mentre oltre un quinto (23%) dei professionisti IT intervistati in una società con un numero di dipendenti compreso tra 100 e 249 ha dato la stessa risposta. Queste risposte differiscono se si confrontano i Paesi: quasi la metà (47%) dei professionisti IT intervistati negli Stati Uniti ha dichiarato che la politica della loro organizzazione in merito al pagamento dei riscatti in caso di attacco ransomware è di pagare sempre, rispetto a 1 su 14 (7%) in Giappone che ha affermato la stessa cosa.

Se la proliferazione del ransomware e del mercato degli zero-day non fosse sufficiente, il Segretario Generale dell'Interpol, Jurgen Stock, a maggio 2022 ha dichiarato di temere che nei prossimi due anni le armi cibernetiche sviluppate dagli stati diventino disponibili su darknet. "Si tratta di un aspetto molto preoccupante nel mondo reale: armi che vengono usate sul campo di battaglia, un domani saranno usate da gruppi di criminalità organizzata", ha asserito Stock durante un panel **moderato dalla CNBC[30]** al World Economic Forum di Davos, in Svizzera.

Alla domanda del sondaggio agli intervistati in merito a quale fosse la politica della loro organizzazione in merito al pagamento di riscatti in caso di attacco ransomware, i professionisti IT a livello globale hanno risposto in modo discordante. Il 24% degli intervistati ha dichiarato che la propria organizzazione paga sempre, il 31% che paga solo quando i dati dei clienti sono a rischio, il 26% che non paga mai e il 19% che dipende.

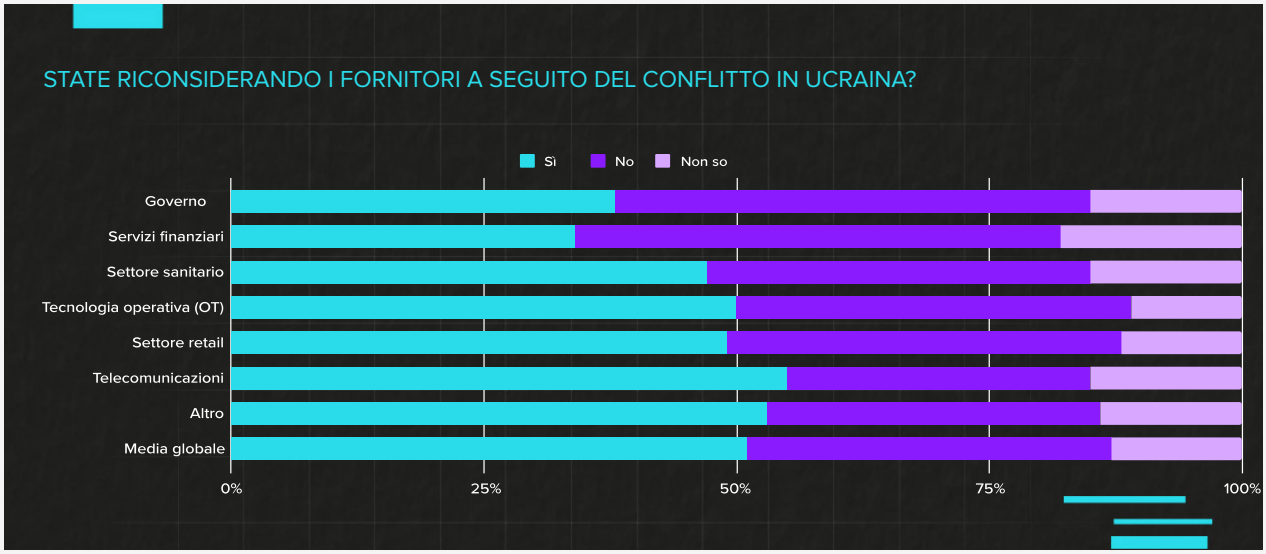
## LA SPESA PER LA CIBERSICUREZZA CONTINUA AD AUMENTARE

Se cercate informazioni su dove le aziende spenderanno i loro budget per l'IT, non vi sorprenderà sapere che le aziende aumenteranno la spesa per i servizi di difesa, resilienza e protezione cibernetica.

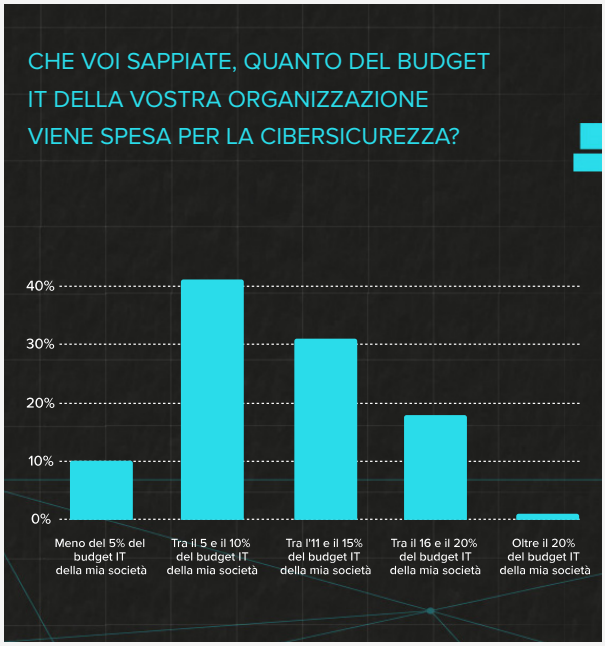
Poco più di tre quarti (76%) dei professionisti IT intervistati concordano sul fatto che i consigli di amministrazione stanno cambiando la cultura della loro organizzazione tenendo in considerazione la cibersicurezza in risposta alla minaccia della guerra cibernetica. Si tratta di un dato significativo, in quanto tale supervisione da parte del consiglio di amministrazione è stata raramente presente in precedenza e tali individui stanno ora iniziando a condividere le loro responsabilità nel migliorare la posizione in materia di cibersicurezza di un'organizzazione.

Di conseguenza, poco oltre la metà (51%) degli intervistati a livello globale ha dichiarato di aver riconsiderato i fornitori a seguito del conflitto ucraino e di prevedere che la loro organizzazione acquisirà nuovi fornitori di cibersicurezza o fornitori di servizi di sicurezza gestiti (MSSP) immediatamente (31%) o nei prossimi sei mesi (29%). È fondamentale che i fornitori siano consapevoli delle tendenze di spesa e dei settori in cui le organizzazioni hanno più bisogno dei loro servizi, in modo da poter garantire la fornitura delle soluzioni più adeguate.

> *"La mancanza di competenze nel settore della cibersicurezza rappresenta ancora una problematica enorme, in quanto la carenza di personale aumenta la domanda di servizi o di pacchetti di soluzioni, che si adattano molto bene alle capacità di valore dei partner. La mancanza di competenze rende il mercato forte nel settore della cibersicurezza, soprattutto per gli MSSP e per quei partner che cercano di ridurre i rischi di impatto sull'attività sviluppando servizi internamente per ottenere risultati migliori".*
>
> **TIM MACKIE**
> VP WORLDWIDE CHANNEL DI ARMIS

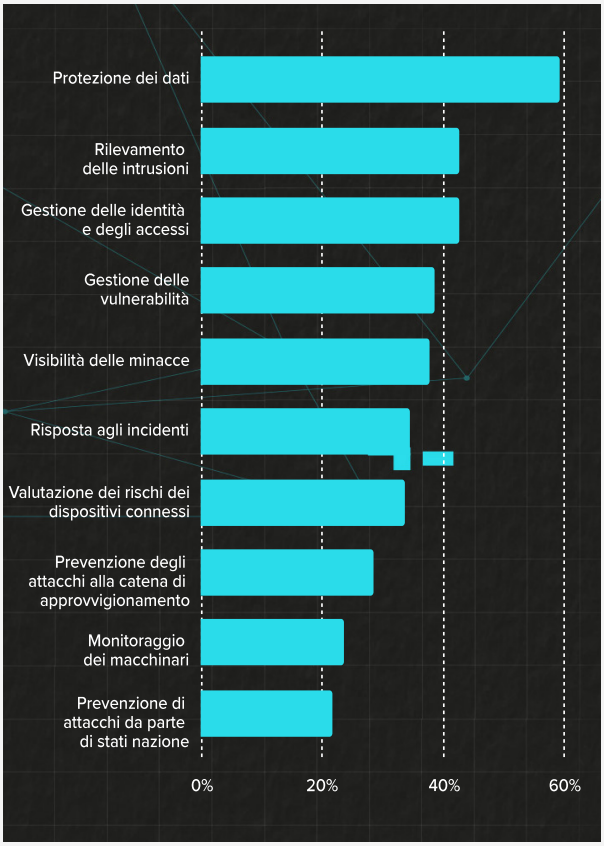



Analizzando i dati, quasi 4 professionisti IT su 5 (78%) intervistati hanno dichiarato che, pensando agli eventi globali verificatisi improvvisamente, sia recenti sia in corso (come la pandemia, il conflitto in Ucraina, ecc.), è probabile che la loro azienda investa una parte maggiore del proprio budget nella cibersicurezza, con quasi 2 su 5 (37%) che lo ritengono molto probabile. Quindi, quanto spendono le organizzazioni e per cosa spendono? L'indagine ha rilevato che, a livello globale, la percentuale media dei budget IT destinati alla cibersicurezza è dell'11%, con la seguente ripartizione:




Tra coloro che spendono di più, il 37% ha dichiarato di essere molto propenso ad aumentare gli investimenti a breve e il 41% ha dichiarato che è abbastanza probabile. Tuttavia, le società che hanno meno investimenti sono meno propense ad aumentare la spesa a breve.

Alla richiesta di selezionare gli elementi di sicurezza in ordine di priorità assoluta, è stata data la seguente risposta a livello globale:



Oltre 2 professionisti IT su 5 (42%) intervistati prevedono che la loro organizzazione investirà nella gestione delle vulnerabilità[31] immediatamente, mentre quasi 3 su 10 (28%) hanno risposto entro sei mesi. Per quanto riguarda gli investimenti nella gestione delle risorse[32], il 37% degli intervistati ha dichiarato che la loro società effettuerà investimenti immediatamente, mentre il 30% ha affermato che investirà entro sei mesi.

Non solo le aziende investono in soluzioni di cibersicurezza, ma adottano anche principi di cybersecurity-first a livello dell'organizzazione e investono nella formazione in materia di cibersicurezza. Un terzo (33%) dei professionisti IT intervistati prevede che la propria organizzazione adotti immediatamente modelli "zero-trust[33]", mentre il 28% dichiara entro sei mesi. Per quanto riguarda la formazione sulla cibersicurezza, il 41% degli intervistati a livello globale ha dichiarato che la loro organizzazione investirà immediatamente in una maggiore formazione sulla cibersicurezza, mentre il 46% ha affermato che investirà nel corso del prossimo anno. Solo il 4% delle organizzazioni ha dichiarato che non intraprenderà alcuna azione per aumentare la formazione in materia di cibersicurezza.

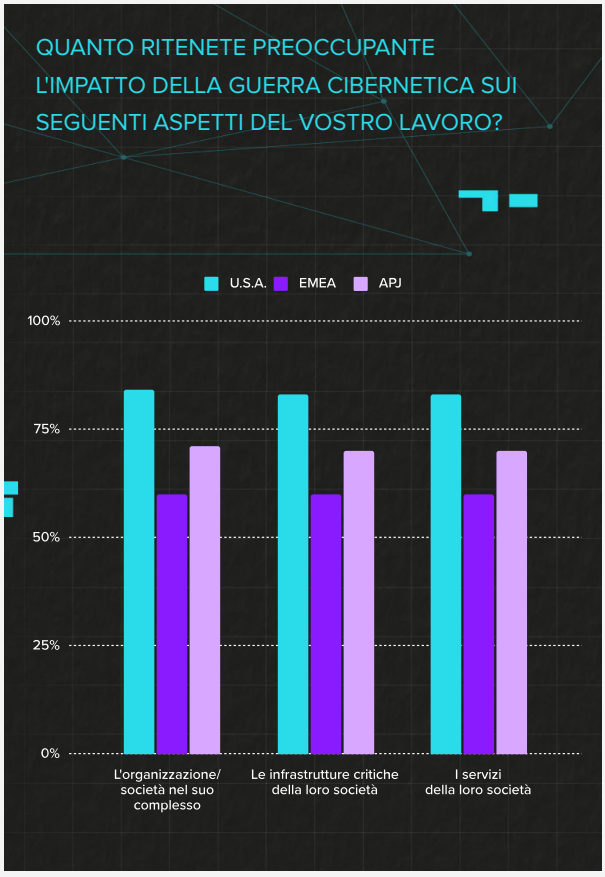
> *"I team di sicurezza hanno una netta necessità di avere un elevato grado di visibilità contestualizzata nell'intero panorama operativo tecnologico per poter operare in modo efficace. Il livello di visibilità offerto ai team di sicurezza che utilizzano le moderne tecnologie sta aiutando i CISO e i loro team a identificare opportunità reali, contestuali al business e comprovate dai dati, per eliminare dall'ambiente le soluzioni più vecchie e concorrenti e tutte le spese correlate."*
>
> **CURTIS SIMPSON**
> CHIEF INFORMATION SECURITY OFFICER (CISO)
> DI ARMIS

# QUALI SONO LE DIFFERENZE A LIVELLO REGIONALE (U.S.A., EMEA E APJ)?

Oltre alle tendenze globali evidenziate in precedenza, differenze a livello regionale sono emerse anche raggruppando le risposte di U.S.A., EMEA e APJ (Australia, Giappone e Singapore). Ad esempio:

## PREOCCUPAZIONE PER L'IMPATTO DELLA GUERRA CIBERNETICA

Agli intervistati di U.S.A., EMEA e APJ è stato chiesto quanto ritengano preoccupate l'impatto della guerra cibernetica sui vari aspetti del loro lavoro. Gli intervistati dell'EMEA hanno indicato una minore preoccupazione rispetto alle loro controparti dell'APJ, che sono più preoccupate e una preoccupazione significativamente minore rispetto ai professionisti IT statunitensi, che hanno il livello più alto di preoccupazione.




## ATTIVITÀ DI MINACCIA E NUMERO DI VIOLAZIONI SUBITE

- Secondo questo sondaggio, gli intervistati dell'area APJ hanno subito il minor numero di violazioni della cibersicurezza, con il 53% degli intervistati dell'area APJ che ha dichiarato che la propria società ha subito una o più violazioni della cibersicurezza. In confronto, quasi 3 intervistati su 5 (58%) in EMEA e 7 intervistati su 10 (73%) negli U.S.A. hanno indicato che la loro organizzazione ha subito una o più violazioni di cibersicurezza.
- Le organizzazioni statunitensi sono anche quelle che hanno registrato il maggior numero di attività di minaccia negli ultimi mesi (45%) rispetto alle controparti APJ (36%) ed EMEA (25%).

## FIDUCIA NELLA PREPARAZIONE DELL'ORGANIZZAZIONE

Gli intervistati statunitensi sono i più fiduciosi sul fatto che la loro società abbia stanziato un budget sufficiente per i programmi, le persone e i processi di cibersicurezza, con quasi 9 intervistati su 10 (88%) che si sono dichiarati fiduciosi negli U.S.A., rispetto al 78% dell'APJ e al 76% dell'EMEA. Inoltre, il 90% degli intervistati statunitensi ha indicato che i dipendenti della loro organizzazione saprebbero a chi rivolgersi se notassero attività cibernetiche sospette, rispetto a 4 su 5 (82%) di quelli con sede nell'area EMEA o APJ.

## PRATICHE DI CIBERSICUREZZA GIÀ IMPLEMENTATE

- Quando si tratta di investire in un'assicurazione per la cibersicurezza, le società statunitensi sono le più propense ad aver investito (45%), seguite da quelle dell'area APJ (37%) e dell'area EMEA (31%).

- Per quanto riguarda l'importanza della formazione dei dipendenti, tutte e tre le regioni hanno dato risposte simili: U.S.A. (51%), EMEA (49%) e APJ (45%).
- Per quanto riguarda la creazione di una cultura lavorativa incentrata sulla sicurezza, il 44% degli intervistati negli U.S.A. ha indicato che la propria azienda sposa una cultura in cui la sicurezza è al primo posto, rispetto al 37% degli intervistati in EMEA e al 33% in APJ.
- Gli U.S.A. sono i più propensi a implementare uno scenario di riferimento per il rischio cibernetico (43%), mentre il 34% degli intervistati dell'APJ ha implementato uno scenario di riferimento e il 31% degli intervistati dell'EMEA ha uno scenario di riferimento.

## PROTEZIONE DEI DATI SENSIBILI E SMART WORKING

Agli intervistati è stato chiesto se fossero d'accordo o meno con un elenco di affermazioni:

- *"La mia organizzazione detiene dati sensibili, ci sono normative da rispettare e vogliamo ridurre al minimo gli effetti negativi di un evento di sicurezza".*
  - » Tra coloro che si sono dichiarati d'accordo: 91% U.S.A., 84% APJ e 83% EMEA.
- *"La questione della sicurezza IT è diventata più importante per i dipendenti con l'adozione dello smart working".*
  - » Tra coloro che si sono dichiarati d'accordo: 91% U.S.A., 85% APJ, 81% EMEA.

## ANALISI PAESE PER PAESE

Per coloro che desiderano approfondire le differenze regionali sopra evidenziate, il team di Armis ha preparato un'analisi unica paese per paese, più rilevante per le nazioni e i territori analizzati come parte di questo resoconto.

Per leggere i resoconti sui singoli Paesi, accessibili in inglese e in alcune versioni tradotte, consulta https://www.armis.com/cyberwarfare.

1. **Stati Uniti**
2. **Regno Unito**
3. **Francia**
4. **DACH** (Austria, Svizzera, Germania)
5. **Iberia**
6. **Italia**
7. **Danimarca**
8. **Paesi Bassi**
9. **APJ** (Australia, Giappone, Singapore)

# CONCLUSIONE

## Perché questi risultati sono importanti e cosa può fare la vostra organizzazione per proteggersi?

I leader mondiali dell'IT e della sicurezza ammettono di non prendere sul serio la minaccia della guerra cibernetica, di sentirsi poco preparati a gestirla e che l'elemento di sicurezza meno importante ai loro occhi è la prevenzione degli attacchi da parte degli stati nazione. Inoltre, stanno assistendo a un aumento delle minacce di guerra cibernetica a seguito della guerra in Ucraina, come risulta evidente dall'aumento dell'attività di minaccia riscontrata sulla loro rete tra maggio 2022 e ottobre 2022 rispetto ai sei mesi precedenti. Non solo si nota una maggiore attività (e non la si prende sul serio) ma si permette anche che la minaccia della guerra cibernetica abbia un impatto sull'innovazione, ammettendo di aver bloccato o interrotto i progetti di trasformazione digitale come diretta conseguenza. È chiaro che queste minacce non possono essere evitate, perché devono essere affrontate di petto per essere difese.

Prima, nel resoconto, gli intervistati che già spendono di più per la cibersicurezza hanno affermato che il 37% è molto propenso ad aumentare gli investimenti a breve e il 41% ha dichiarato che è abbastanza probabile. Oltre 2 professionisti in ambito IT e sicurezza su 5 (42%) intervistati prevedono che la loro organizzazione investirà nella **gestione delle vulnerabilità**[34] immediatamente, mentre quasi 3 su 10 (28%) hanno risposto entro sei mesi. Per quanto riguarda gli investimenti nella **gestione delle risorse**[35], il 37% degli intervistati ha dichiarato che la loro società effettuerà investimenti immediatamente, mentre il 30% ha affermato che investirà entro sei mesi.

Che un attacco alla rete sia il risultato di un player di uno stato nazione o di criminali cibernetici poco importa: l'impatto sulle operazioni e sulla reputazione di un'organizzazione è lo stesso. Inoltre, il protocollo di desktop remoto, le reti "bring your own device", le vulnerabilità delle reti private virtuali e le errate configurazioni dei protocolli stanno diventando il punto d'ingresso più comune per gli aggressori. Tale fenomeno è stato esacerbato dalla pandemia e nel 2021 gli attacchi ransomware **sono quasi raddoppiati**[36] a livello globale.

Disporre degli strumenti corretti e di un piano di risposta agli incidenti (IR) è solo il primo passo. Testare regolarmente il piano può aiutarvi a identificare in modo proattivo i punti deboli della vostra cibersicurezza e a rafforzare le difese per proteggere i dati critici di aziende e consumatori. Senza contare che ciò può far risparmiare alle organizzazioni milioni di euro in costi di violazione dei dati.

Armis consiglia le seguenti misure per tutte le organizzazioni:

- Indipendentemente dagli strumenti e dalle tecniche che un'organizzazione sceglie di mettere in atto, molte organizzazioni avranno bisogno di assistenza per mitigare gli effetti di un attacco attraverso l'esecuzione di un piano di risposta agli incidenti. Spesso è buona norma per un'organizzazione affidarsi a un team specializzato nella risposta agli incidenti per ridurre i costi e aumentare la velocità della risposta agli incidenti.
- Una volta individuato un attacco, è essenziale ridurne al minimo l'impatto. La sorveglianza o l'isolamento continuano a essere la strategia predominante per la maggior parte delle organizzazioni. Esistono diverse tecniche di isolamento e la maggior parte degli strumenti di rilevamento e risposta degli endpoint offre funzionalità di isolamento sul dispositivo. In questo modo, coloro che dovranno far fronte all'incidente avranno la possibilità di isolare le singole macchine dal resto della rete.

- Inoltre, una buona strategia e un buon processo di backup sono una linea di difesa di prima linea contro gli attacchi degli stati nazione e dei criminali cibernetici. Le organizzazioni devono assicurarsi che la soluzione scelta sia resistente agli attacchi e che includa il monitoraggio continuo e il controllo dell'integrità.
- Un'organizzazione ciber-resiliente investirà anche nella formazione dei propri dipendenti in materia di sicurezza. Assicurarsi che i dipendenti siano regolarmente istruiti su come identificare il traffico di e-mail dannose e fornire meccanismi di segnalazione facili da usare.

Le organizzazioni dovrebbero lavorare secondo il principio per cui i player degli stati nazione o i criminali cibernetici riusciranno nel loro intento. Dopotutto, ai player malintenzionati basta avere successo una volta sola tra tutti i loro tentativi di accedere alla rete di un'organizzazione, mentre i team di sicurezza e IT devono avere successo il 100% delle volte nella loro difesa per prevenire tali attacchi.

Vista la situazione, cosa possono fare le organizzazioni? Il rilevamento precoce e il monitoraggio continuo sono il modo migliore per migliorare la posizione 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 cibernetici 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 cibernetica o da altro.

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

Per approfondire i risultati del resoconto sullo stato della guerra cibernetica e sulle tendenze di Armis: 2022-2023 su scala globale, potete visitare il sito web: **armis.com/cyberwarfare.**

# RESOCONTO DEMOGRAFICO

Per la stesura del presente resoconto, Armis ha commissionato uno studio a Censuswide intervistando 6.021 professionisti in ambito IT e sicurezza in aziende con oltre cento dipendenti in U.S.A., Regno Unito, Spagna, Portogallo, Francia, Italia, Germania, Austria, Svizzera, Australia, Singapore, Giappone, Paesi Bassi e Danimarca. Le risposte sono state raccolte tra il 22 settembre 2022 e il 5 ottobre 2022.

| INTERVISTATI PER PAESE | |
|---|---|
| **Australia** | 511 |
| **Austria** | 100 |
| **Danimarca** | 50 |
| **Francia** | 501 |
| **Germania** | 501 |
| **Italia** | 500 |
| **Giappone** | 501 |
| **Paesi Bassi** | 52 |
| **Portogallo** | 251 |
| **Singapore** | 501 |
| **Spagna** | 500 |
| **Svizzera** | 50 |
| **Regno Unito** | 1003 |
| **Stati Uniti** | 1000 |

| INTERVISTATI PER TITOLO/RUOLO | |
|---|---|
| **Chief Information Officer (CIO)** | 432 |
| **Chief Information Security Officer (CISO)** | 241 |
| **Chief technology officer (CTO)** | 530 |
| **Specialista dell'assistenza informatica** | 229 |
| **Amministratore di database** | 457 |
| **Analista della sicurezza delle informazioni** | 392 |
| **Responsabile di progetto di tecnologia dell'informazione (IT)** | 1831 |
| **Amministratore di rete** | 394 |
| **Architetto di rete** | 260 |
| **Altro** | 346 |
| **Analista di sistemi** | 493 |
| **Sviluppatore web** | 416 |

| INTERVISTATI PER SETTORI VERTICALI | |
|---|---|
| **Governo, autorità locale, ente del settore pubblico** | 369 |
| **Servizi finanziari e assicurazioni** | 120 |
| **Settore sanitario, medico, farmaceutico** | 255 |
| **OT** (automotive, distribuzione, logistica e trasporti, alimenti e bevande, settore manifatturiero, petrolio, gas, edile, settore minerario, agricoltura, trasporti) | 1415 |
| **Tecnologia e altri settori** | 3133 |
| **Vendita retail e all'ingrosso** | 295 |
| **Telecomunicazioni** | 434 |

# NOTE FINALI

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.armis.com/cyberwarfare/
9. https://www.ibm.com/reports/data-breach
10. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
11. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
12. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
13. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
14. https://www.armis.com/cybersecurity-asset-management/
15. https://www.armis.com/ot-device-security/
16. https://www.armis.com/ics-risk-assessment/
17. https://www.armis.com/research/tlstorm/
18. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
19. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
20. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
21. https://www.ibm.com/reports/data-breach
22. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
23. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
24. https://www.armis.com/research/pwnedpiper/
25. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
26. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
27. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
28. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
29. http://stopransomware.gov
30. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
31. https://www.armis.com/avm/

32. https://www.armis.com/armis-asset-management/
33. https://www.armis.com/zero-trust/
34. https://www.armis.com/avm/
35. https://www.armis.com/armis-asset-management/
36. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

STATO DELLA

# GUERRA CIBERNETICA

## INFORMAZIONI SU ARMIS

Armis, azienda leader nella visibilità e nella sicurezza delle risorse, fornisce la prima piattaforma intelligente sulle risorse unificata del settore, progettata per affrontare la nuova ed estesa superficie d'attacco creata dalle risorse connesse. Le aziende della Fortune 100 si affidano alla nostra protezione continua in tempo reale per poter vedere, con il pieno contesto, tutte le risorse gestite e non gestite tramite IT, cloud, dispositivi IoT gestiti, dispositivi medici (IoMT), tecnologia operativa (OT) e sistemi di controllo industriale (ICS) e 5G. Armis fornisce capacità passive di gestione delle risorse cibernetiche, gestione del rischio e applicazione automatizzata. Armis è un'azienda privata con sede in California.

armis.com

info@armis.com

20230110-1



ARMIS®