The Innovation Group
Innovating business and organizations through ICT

MSSP IN ITALIA. TUTTI LI VOGLIONO, MA CHI SONO E COSA FANNO?

La crescente complessità tecnologica, soprattutto in ambito cybersecurity, chiama l'aiuto degli MSSP. Esperti che gestiscano in outsourcing e in maniera automatizzata la sicurezza per conto terzi. Questo white paper, frutto di un'indagine qualitativa che ha coinvolto fornitori di servizi di diverse provenienze geografiche e dimensioni, vuole contribuire a disegnare un quadro del fenomeno a fronte di una recrudescenza degli attacchi cyber.

Offrire servizi è ormai l'alternativa alla complessità che le aziende e i partner di canale devono affrontare per gestire una sicurezza che evolve e cresce allo stesso ritmo degli attacchi. Troppi prodotti, meglio i servizi. E che siano tassativamente gestiti in outsourcing, da qualcuno molto esperto. Il canale delle terze parti IT si sta ritagliando proprio questo nuovo ruolo sul mercato, mettendo nel proprio curriculum il "titolo" di MSSP, vale a dire Managed Security Service Provider, evidenziando così di essere in grado di erogare servizi a corredo, o in completa sostituzione, della fornitura di prodotti. In questo caso prodotti per la sicurezza IT.

Si tratta di un fenomeno che sta letteralmente esplodendo, soprattutto nella denominazione dell'offerta dei vendor, dietro il quale si cela una modalità nuova, o in evoluzione, di gestire moltitudini di clienti in maniera centralizzata, semplificata o addirittura automatizzata, per l'utilizzo corretto e in sicurezza di applicazioni e infrastrutture, svincolandoli, lato cliente finale, dalla logica delle licenze.

MSP (Managed Service Provider): un team IT esterno e specializzato

In effetti, l'aumento della complessità delle infrastrutture aziendali, che vede una crescente integrazione di strumenti e soluzioni per fare fronte alle nuove esigenze imposte dal mercato, richiede un'escalation nella quantità e nella qualità delle competenze interne delle organizzazioni che in pochi riescono ormai a gestire e sostenere. Nemmeno le aziende di grandi dimensioni, che hanno a loro disposizione nutriti team dediti alla gestione delle loro reti e asset IT, vi riescono o, meglio dire, trovano conveniente farli gestire internamente, comportando un ampio impiego di risorse poco sostenibile per i costi e l'efficienza.
L'alternativa che sempre più aziende stanno adottando è l'outsourcing di tutti i propri sistemi informativi o parte di essi e delle applicazioni connesse. Si va quindi verso il ricorso agli MSP (Managed Service Provider), i quali erogano servizi di vario tipo a canone, prevalentemente orientati alla gestione dell'infrastruttura, servizi in cloud, applicazioni, backup e via dicendo, fino ad interessare anche l'uso as a service dei device, garantendone funzionamento, aggiornamenti, manutenzioni. In pratica, un MSP può prendersi carico di tutte le mansioni che

solitamente verrebbero svolte da un team IT interno a un'azienda. Con il vantaggio di avere persone totalmente dedicate a queste problematiche, che utilizzano le corrette e più aggiornate tecnologie, con le dovute competenze e le certificazioni sui brand utilizzati.

MSSP (Managed Security Service Provider) specializzati nei servizi di cybersecurity

La parte di tecnologia che maggiormente si è complicata, soprattutto negli ultimi anni, è quella inerente alla cybersecurity.
Una complicazione nella gestione delle numerose soluzioni a rimedio che è figlia diretta dell'incredibile incremento degli attacchi che hanno sfruttato i timori delle persone nei riguardi della pandemia da Covid, della guerra in atto ai confini dell'Europa ma, soprattutto, delle mutate tendenze nella gestione del lavoro, le quali hanno attivato quelle forme di smart o remote working che, da totali che erano in periodo lockdown, stanno diventando ora parte integrante nella nuova era dell'hybrid workplace.
Situazioni nuove che hanno di fatto cancellato la già labile linea dei perimetri aziendali, delegando al cloud l'infrastruttura di accesso alle applicazioni e interazioni aziendali, aprendo nuovi fronti d'attacco a un cybercrime che non aspettava altro.
Tante modalità d'attacco equivalgono a tante soluzioni e modalità di difesa. Una situazione davvero troppo complicata da gestire, con il rischio di non proteggere adeguatamente e in maniera veloce i dati e le informazioni essenziali per la sopravvivenza stessa del business.
Serve quindi rivolgersi a chi queste pratiche le fa di mestiere.
Nel caso della cybersecurity un MSSP è proprio la figura che si prende l'incarico di gestire la sicurezza per conto di un cliente. Anzi, di molti clienti. Contemporaneamente.

Lo fanno da remoto, attraverso console di gestione, acquisendo quantità di licenze a prezzi concorrenziali per monitorare e intervenire grazie a un pannello di controllo alle eventuali anomalie riscontrate presso i tanti clienti che aderiscono ai servizi che l'MSP riesce a erogare.
Una modalità, quella dei servizi gestiti da terze parti, che consente ai clienti di mantenere la propria rete, i propri endpoint e altro ancora, monitorati nella loro integrità, e delegarne il controllo a chi su queste piattaforme, soluzioni specifiche, di nicchia o comunque con funzionalità di base o avanzate, ha sviluppato competenze specifiche. Competenze che, dicevamo, vengono messe a disposizione a un gran numero di clienti contemporaneamente, con una scala di costi che diventa in tal modo accessibile anche alle realtà di piccole e medie dimensioni che altrimenti non avrebbero la possibilità di creare e mantenere professionisti in grado di garantire un controllo di tale efficacia.

Tante modalità d'attacco equivalgono a tante soluzioni e modalità di difesa. Una situazione davvero troppo complicata da gestire, con il rischio di non proteggere adeguatamente e in maniera veloce i dati e le informazioni essenziali per la sopravvivenza stessa del business.

MSSP, partner appetibili cui i vendor di cybersecurity ambiscono. Qualche numero

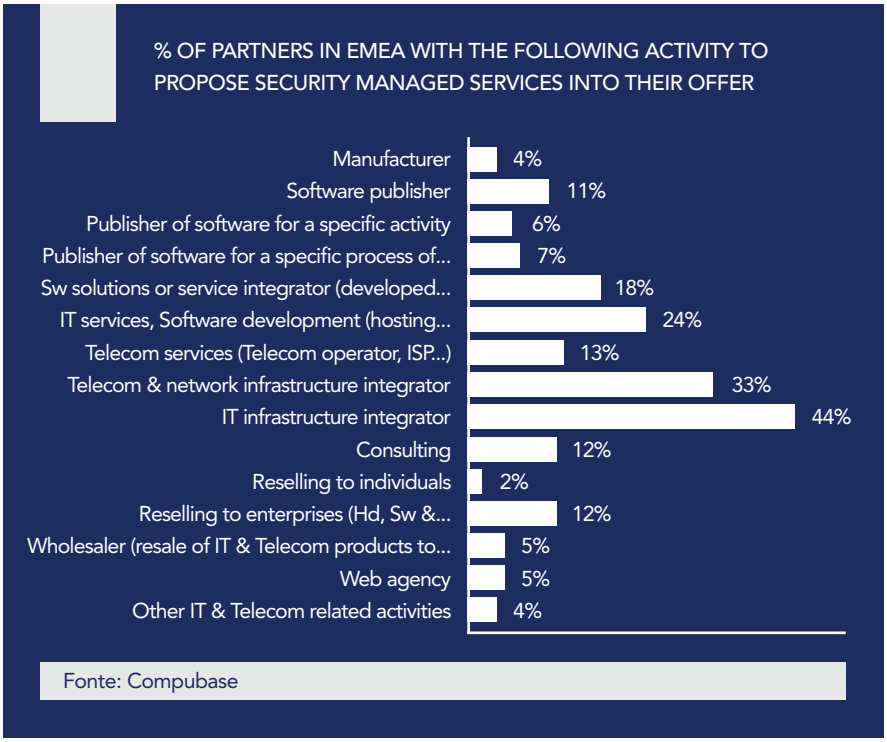
Numerosi vendor di cybersecurity stanno adeguando la propria offerta per essere erogata anche come servizio e cercando così di essere appetibili a quegli MSSP che nel nostro Paese stanno crescendo in misura tale che è difficile averne un quadro numerico preciso.

L'ultimo aggiornamento dato da Compubase (marzo 2023) indica un numero di 57.833 MSSP attivi a livello mondiale, di cui 2.279 già operanti in Italia. Se serve fare un paragone, la sola Francia ne conta quasi il doppio (4.231).

Un numero maggiore (3.509), nella nostra Penisola, riguarda i system integrator in area cybersecurity, potenziali target per i vendor di sicurezza nella loro fase di recruiting di un canale dedito ai servizi oltre, o in alternativa, alla vendita delle licenze. Un destino previsto, sembra, per le realtà del canale che già operano anche sul cloud, visto che gli MSSP rappresentano intorno al 20% degli operatori che offrono servizi in cloud o as a service.

Chi si sta trasformando in MSSP per offrire cybersecurity a canone

Sono infatti in molti in EMEA le figure di canale che si stanno strutturando per offrire servizi gestiti di sicurezza. Sempre gli stessi analisti calcolano che gli MSSP di oggi derivino in parte dai system integrator infrastrutturali di stampo IT (44%), seguiti da quelli di natura telco e network (33%), in generale gli sviluppatori software e chi offre servizi IT (24%) quindi i fornitori di servizi software as a service (18%) e dai rivenditori (12%) e i consulenti (12%), oltre che da altri soggetti.



Una grande varietà di figure del canale, quindi, di diverse provenienze, che si stanno attrezzando per passare a una forma a canone dei propri servizi di sicurezza, in affiancamento o in sostituzione delle licenze dei software di sicurezza. Si tratta di operatori alcuni dei quali anch'essi alle prese con il problema della mancanza di risorse, per i quali poter erogare diversi servizi di security in maniera centralizzata, automatizzata e semplificata, consentirebbe loro di proporsi ai propri clienti con contratti comprensivi di più aspetti giovandone in fidelizzazione dei propri clienti ai quali si proporrebbero con una veste più consulenziale che di venditore.

MSSP, esperti in cybersecurity in lotta con l'industria del cybercrime

L'attività del cybercrime non ha mai rallentato, né in pandemia, né nelle altre condizioni di crisi economica. È un'industria in piena attività e

crescita che proprio nei momenti di difficoltà globali riesce a ottenere i maggiori guadagni, sfruttando elementi e comportamenti sempre più sofisticati, sia tecnologici, sia di approccio emozionale e psicologico nei confronti dei possibili bersagli.
Il confronto, ormai da tempo, non è più con i cani sciolti che nell'hackeraggio traevano soddisfazioni personali fini a sé stesse, ma con soggetti che ambiscono al guadagno economico, ormai strutturati in vere e proprie organizzazioni, le quali hanno capacità d'investimento enormi, proporzionate ai potenziali guadagni. Un potenziale che la crescente digitalizzazione delle imprese sta facendo diventare sempre più appetibile. Il cloud da un lato amplifica enormemente le opportunità e l'ottimizzazione delle operazioni di business delle aziende (e degli individui) ma, dall'altro, per definizione sfuma o elimina i perimetri aziendali, esponendole potenzialmente a innumerevoli e nuove forme di attacco.

Vecchio o nuovo, semplice o sofisticato. Ogni attacco è buono per il guadagno del cybercrime

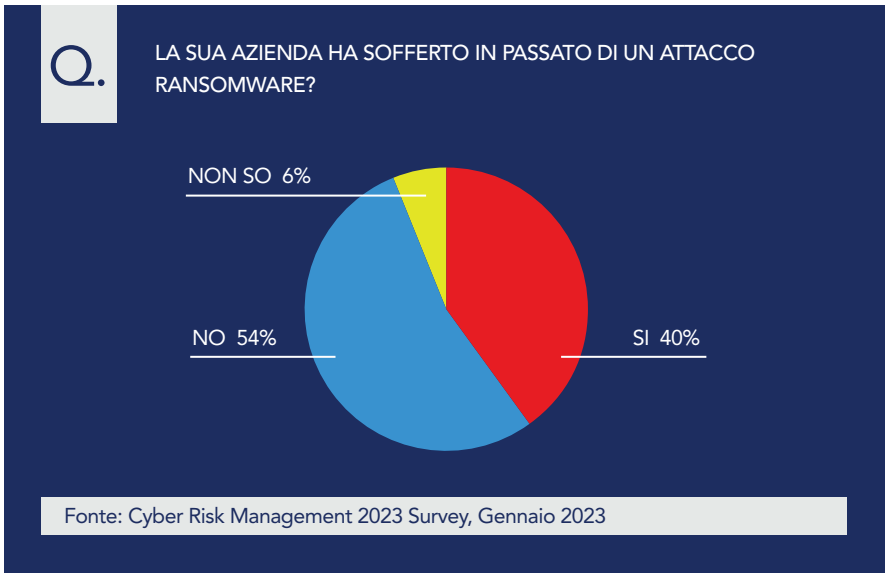
Gli attacchi sfruttano vecchie e nuove forme di trasmissione per veicolare l'elemento malevolo all'interno dell'azienda, dalla classica "pesca a strascico" dell'evergreen phishing, alle forme complesse, addirittura personalizzate, messe in atto da personale criminale altamente specializzato e focalizzato sulla singola azienda dalla quale si prevede di poter trarre un forte guadagno. Un impegno e investimento, quest'ultimo, piuttosto oneroso che il cybercrime non esita a effettuare se solo intravvede la possibilità di ampi guadagni in termini di denaro o, come suggerisce l'attualità geopolitica, per avvantaggiarsi strategicamente mettendo fuori uso infrastrutture o servizi del nemico ingaggiando una vera e propria guerra cibernetica tra i diversi Paesi.

Furto con ricatto. Il ransomware è l'attacco più remunerativo

Nella gran parte dei casi l'effetto finale è il furto dei dati, per utilizzarli a scopo di lucro, o per il loro sequestro a fronte della richiesta del pagamento di un riscatto, con la minaccia portata da nuove famiglie di ransomware, una piaga che rappresenta ancor oggi il principale esito di attacchi che possono anche rimanere silenti per mesi prima che la vittima si accorga della loro presenza, concedendo agli hacker tutto il tempo di ispezionare, scegliere e indentificare i dati più sensibili e, per contro, più appetibili per il loro guadagno.

Dati **TIG (The Innovation Group) e CSA - Cyber Security Angels**, nel loro "Cyber Risk Management Survey 2023" dove sono state sentite oltre 200 aziende di medio/grandi dimensioni, indicano che il 40% di queste ha subito almeno un attacco ransomware, mentre gran parte di queste aziende ha maturato nel contempo una certa consapevolezza del pericolo, al punto solo il 18% ritiene di essere esente dal rischio di poter essere colpite da un attacco ransomware, mentre il 28% lo considera altamente possibile che possa accadere.

Di buono c'è che le aziende stanno imparando a riparare i danni di un attacco in maniera migliore e più velocemente che in passato. Il 70% ritiene addirittura di non avere subito alcun danno a seguito dell'attacco, e il 53% è riuscito a rilevare il malware nel giro di pochi minuti (lo scorso anno erano il 45%) e nelle aziende di grandi dimensioni si arriva addirittura al 71%.



Solo il 18% ritiene di essere esente dal rischio di poter essere colpite da un attacco ransomware, mentre il 28% considera altamente possibile che possa accadere.

La voce degli MSSP italiani a garanzia della cybersecurity

Si tratta di un panorama che presenta ovunque un aumento degli attacchi, ma che nel nostro Paese vede ancora una scarsa reazione in termini di investimenti per la cybersicurezza. L'Italia, infatti, pur avendo aumentato del 18% la spesa per la cybersicurezza rispetto all'anno precedente, arrivando nel 2022 a 1.855 milioni di euro (dati Politecnico di Milano), è il fanalino di coda tra le nazioni del G7 nel rapporto tra spesa in cybersecurity e Pil.
Una situazione che a livello nazionale non è uniforme, e che vede esempi virtuosi che hanno ben presenti i pericoli e sono disposti a spendere in sicurezza riconoscendone il valore strategico per la propria attività, accostati da realtà che non hanno le minime basi di cultura della protezione, nella convinzione di non essere appetibili per il cybercrime. Sottovalutando la "bocca buona" che hanno le organizzazioni criminali che operano nel digitale quando si parla di estorcere denaro. Realtà diverse che a volte risiedono a pochi chilometri di distanza tra di loro, a riprova che l'indifferenza verso la cybersecurity è, purtroppo, trasversale lungo tutto lo Stivale e non concentrata in alcune regioni.

Gli MSSP di cybersecurity alle prese con le diversità e mancanze culturali dei clienti

A queste disparità culturali e di approccio alla sicurezza cercano di porre rimedio i system integrator, dai più grandi e organizzati fino ai più piccoli e locali, proponendosi con una serie di servizi di monitoraggio e risoluzione dei problemi di sicurezza da remoto e in outsourcing per conto dei propri clienti.

Dalla crescente volontà dei clienti di alleggerire i compiti complessi dei propri comparti IT, fino alla delega totale della gestione della cybersecurity per mancanza di competenze interne, il ruolo e l'opzione MSSP stanno diventando note un po' a tutto il mercato e, in particolare, a quegli operatori IT che cercano piattaforme per la gestione centralizzata della sicurezza, nei vari aspetti, di un alto numero di clienti. Meglio ancora se si tratta di piattaforme intelligenti, in grado di attivare funzionalità di difesa e risoluzione in automatico dei problemi che si possono avverare tra i loro clienti.
Serve, ovviamente, un diverso approccio commerciale e di partnership con il cliente, chiedendo un cambio di rotta delle logiche commerciali interne al system integrator stesso, orientato tradizionalmente verso modalità di vendita transazionale rispetto a quanto la logica MSP richiede, ossia il pagamento a canone per l'utilizzo del servizio.

Problemi e opportunità degli MSSP italiani: operatori locali o nazionali di servizi di cybersecurity

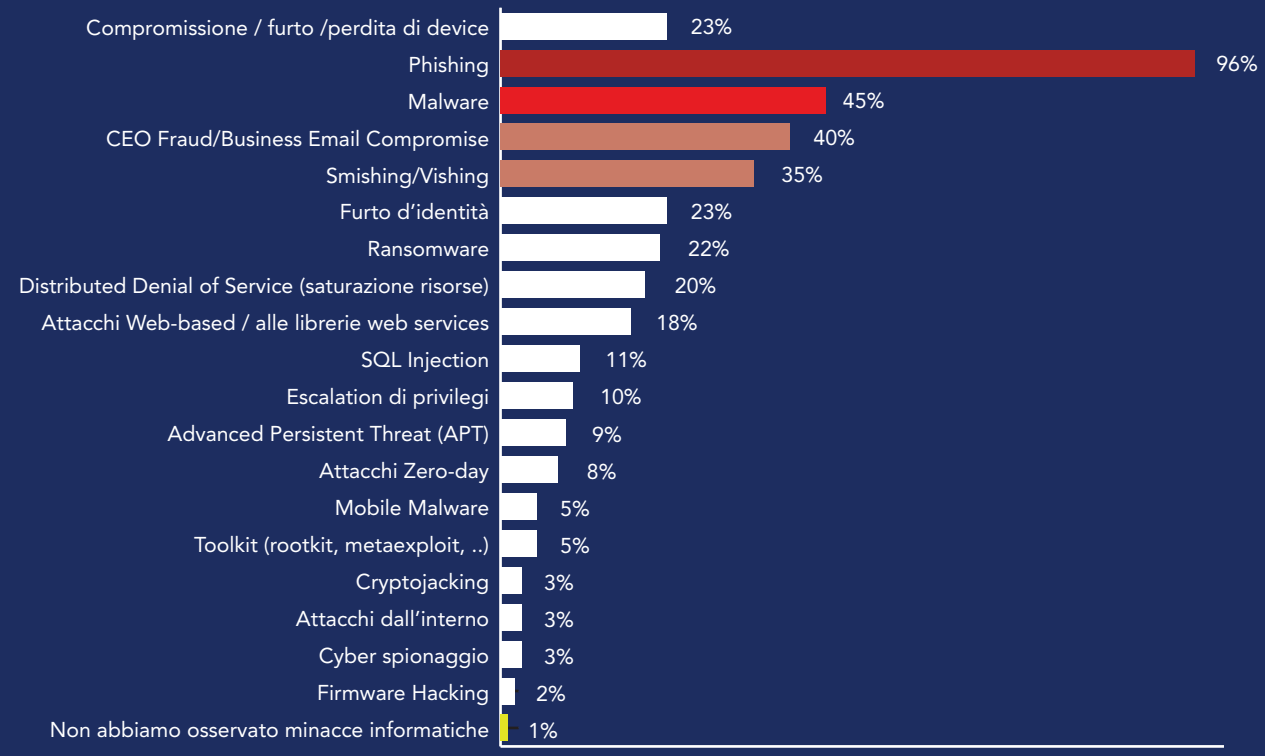
Un cambio di rotta che alcuni operatori delle terze parti vedono con grande favore ma che chiedono sia accompagnato da programmi di supporto adeguati da parte dei vendor oltre che a sforzi per elevare il grado culturale delle aziende clienti, sia in termini di attenzione alla cybersecurity sia a un nuovo modello che si basa non solo sulla validità del prodotto, ma che ha il suo valore nei servizi che il reseller riesce ad aggiungere. Che deve essere valorizzato e non essere dato per scontato.

Intanto il cybercrime non sta a guardare

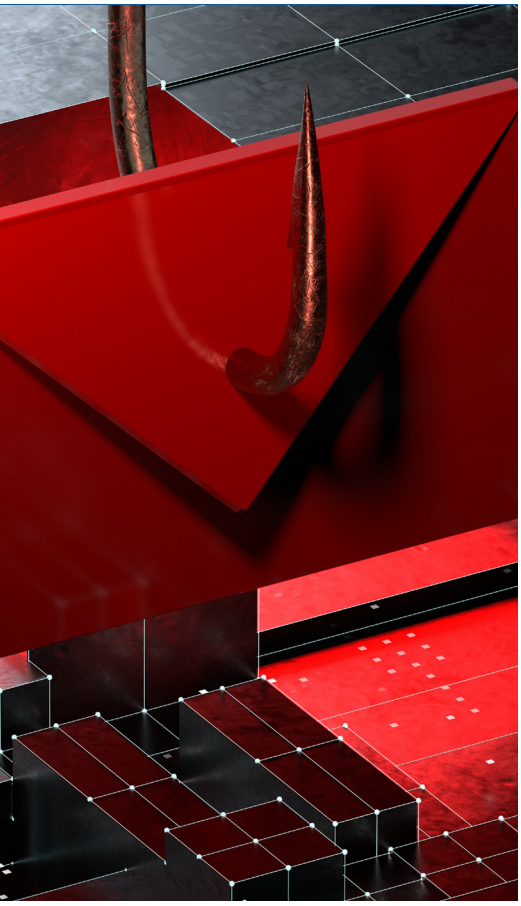
Sempre facendo riferimento alla survey 2022 di The Innovation Group, si evidenzia come nel corso del 2022, gli attacchi di Phishing hanno interessato praticamente tutte le aziende interpellate (96%). Malware e Business Email Compromission, non sono stati da meno, avendo avuto una diffusione, rispettivamente, per il 45% e il 40% degli intervistati. Il secondo, in particolare, è praticamente raddoppiato rispetto a quanto risultava da una survey analoga effettuata l'anno precedente. Rapportando i dati alle dimensioni aziendali delle aziende che hanno composto il panel si è notato che questo tipo di minaccia ha interessato nel 20% dei casi le organizzazioni sotto i 200 dipendenti, aumentando fino al 60% dei casi nelle aziende il cui numero di dipendenti supera le 5.000 unità.

> **La survey 2022 di The Innovation Group evidenzia come nel corso del 2022, gli attacchi di Phishing hanno interessato praticamente tutte le aziende interpellate (96%).**

Q. NEL CORSO DEGLI ULTIMI 12 MESI, QUALI DEI SEGUENTI TENTATIVI DI ATTACCO / TECNICHE DI ATTACCO AVETE RILEVATO NELLA VOSTRA AZIENDA?



Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023



I guai attesi dalle aziende da un attacco cyber

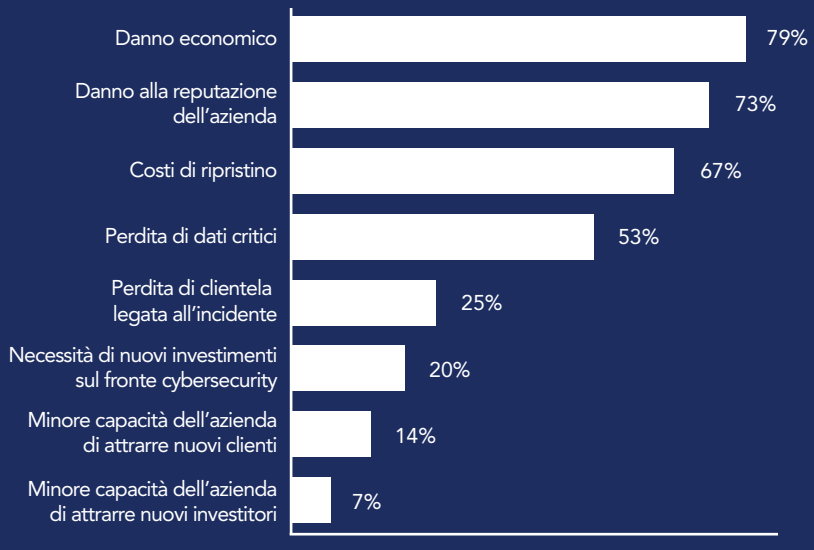
Da un incidente informatico le aziende si attendono grossi guai. La consapevolezza corre tra i partecipanti alla survey, identificando diverse tipologie di danno: il danno economico è quanto la maggior parte (79%) teme, conseguenza del fermo operativo e al relativo calo di fatturato. Ma anche la messa in pericolo della reputazione aziendale non è sottostimata, preoccupando il 73% delle aziende. A seguire, gli oneri di ripristino (67%), la perdita di dati critici (53%) e per un 25% degli intervistati anche il timore che un attacco possa causare una perdita di clientela.

Preoccupazioni che variano in base anche alle dimensioni delle aziende interessate, con le aziende più piccole che temono soprattutto i costi necessari per il ripristino delle attività a seguito dei singoli incidenti e, dopo che è successo, la fatica ad attirare nuovi clienti. Per le aziende di taglio enterprise, oltre ai 5.000 dipendenti, tremano al pensiero del danno economico e della cattiva reputazione che ne conseguirebbe.

Anche la preoccupazione per la perdita di dati critici è in questo caso più alta rispetto alla media.

Le preoccupazioni derivanti da un attacco cyber variano in base anche alle dimensioni delle aziende interessate, con le aziende più piccole che temono soprattutto i costi necessari per il ripristino delle attività a seguito dei singoli incidenti e, dopo che è successo, la fatica ad attirare nuovi clienti.

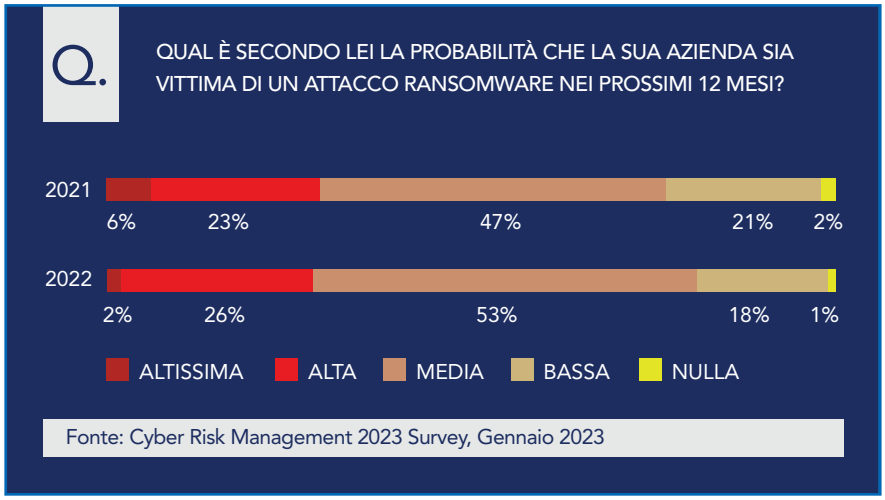
Q. QUALI I PRINCIPALI IMPATTI CHE UN EVENTUALE INCIDENTE DI SICUREZZA INFORMATICA POTREBBE CAUSARE ALLA SUA AZIENDA?

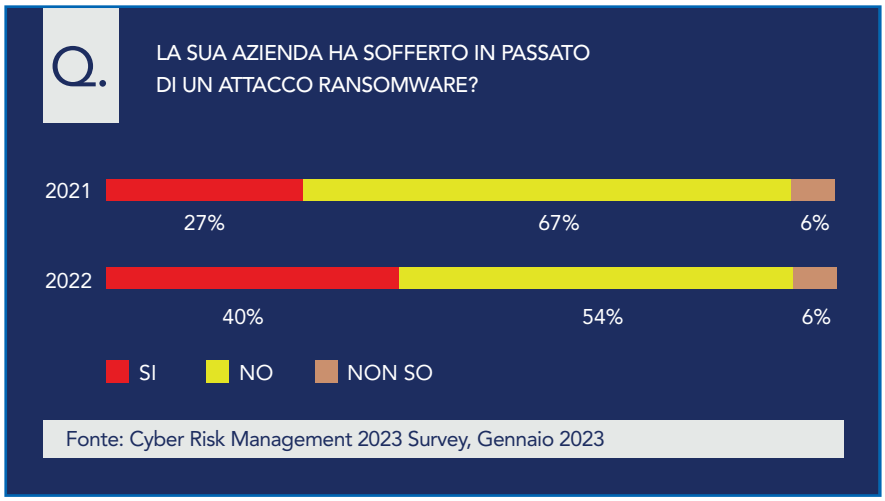


Fonte: Cyber Risk Management 2023 Survey, Gennaio 2023

Attacchi ransomware: analisi di una paura diffusa. A buon ragione

Tornando sul tema del ransomware, va sottolineato il fatto che nel solo lasso di tempo di un anno, la percentuale di aziende che hanno subito attacchi è passato dal 27% al 40%, con una crescita intorno al + 48%.
Ma nonostante i dati, la convinzione media è di non essere troppo esposti a questa forma di ricatto: solo il 28% ritiene, infatti, che la possibilità di esserne vittima sia alta o altissima. Un dato praticamente invariato rispetto allo scorso anno. Ancora più spavalde risultano essere le piccole aziende: solo il 18% pensa di essere altamente a rischio. Le enterprise sono più cute sulla loro invulnerabilità: il 32% dei rispondenti pensa che il proprio rischio di essere esposti ad attacchi ransomware sia alto, se non addirittura altissimo. Da notare che le più spaventate, sono proprio le aziende che hanno già subito un attacco ransomware, considerando alta la probabilità di esserne ancora vittima.





La cifratura dei dati è l'effetto più eclatante osservabile a seguito di un attacco (56%). Ma non è l'unica attività malevola che una violazione del genere si porta in dote.

Ransomware ed effetti collaterali

La cifratura dei dati è l'effetto più eclatante osservabile a seguito di un attacco (56%). Ma non è l'unica attività malevola che una violazione del genere si porta in dote. Il 52% ha notato movimenti laterali, segnali di una ricerca e utilizzo di credenziali con privilegi superiori, mentre per il 34% delle aziende intervistate, il danno ha avuto effetti distruttivi, in alcuni casi anche con il danneggiamento dei sistemi. Il furto dei dati è stato segnalato solo dal 19% del panel. Risultato probabilmente dovuto all'evoluzione del ransomware verso forme di attacchi Double Extortion, che causano allo stesso tempo cifratura ed esfiltrazione di dati. Dati che poi possono essere resi pubblici o, addisittura, entrare nel flusso del mercato del dark web.

Ulteriori componenti osservate con gli attacchi ransomware (16%) sono gli attacchi mirati (APT - advanced persistent threat) e, nel 10% dei casi, l'attacco congiunto di DDoS come diversivo delle forme di difesa aziendali. Un vero e proprio modo per coprire le spalle al ransomware, dove la digitalizzazione degli attacchi si avvicina sempre di più alle tecniche di assalto fisiche degne di strateghi militari.

The Innovation Group
Innovating business and organizations through ICT

Un documento realizzato da

Fondata nel 2009, The Innovation Group (TIG) è una società di servizi di consulenza e di ricerca di mercato indipendente, specializzata nello studio delle evoluzioni del mercato digitale e nei processi d'innovazione abilitati dalle tecnologie e dalla conoscenza. Evento, Ricerca, Advisory e Media le aree di attività. In particolare, ICTBusiness Ecosystem e Technopolis sono le due testate giornalistiche di riferimento del gruppo.

In collaborazione con

WatchGuard Technologies, Inc. è un leader globale nella sicurezza informatica unificata. Il nostro approccio Unified Security Platform è progettato unicamente per i fornitori di servizi gestiti per offrire una sicurezza di livello mondiale che aumenta la portata e la velocità del loro business, migliorando al contempo l'efficienza operativa. Scelti da oltre 17.000 rivenditori di sicurezza e fornitori di servizi per proteggere più di 250.000 clienti, i pluripremiati prodotti e servizi di WatchGuard comprendono sicurezza e intelligence di rete, protezione avanzata degli endpoint, autenticazione a più fattori e Wi-Fi sicuro. Insieme, offrono cinque elementi critici di una piattaforma di sicurezza: sicurezza completa, conoscenza condivisa, chiarezza e controllo, allineamento operativo e automazione. WatchGuard ha sede a Seattle, Washington, con uffici in Nord America, Europa, Asia Pacifico e America Latina.