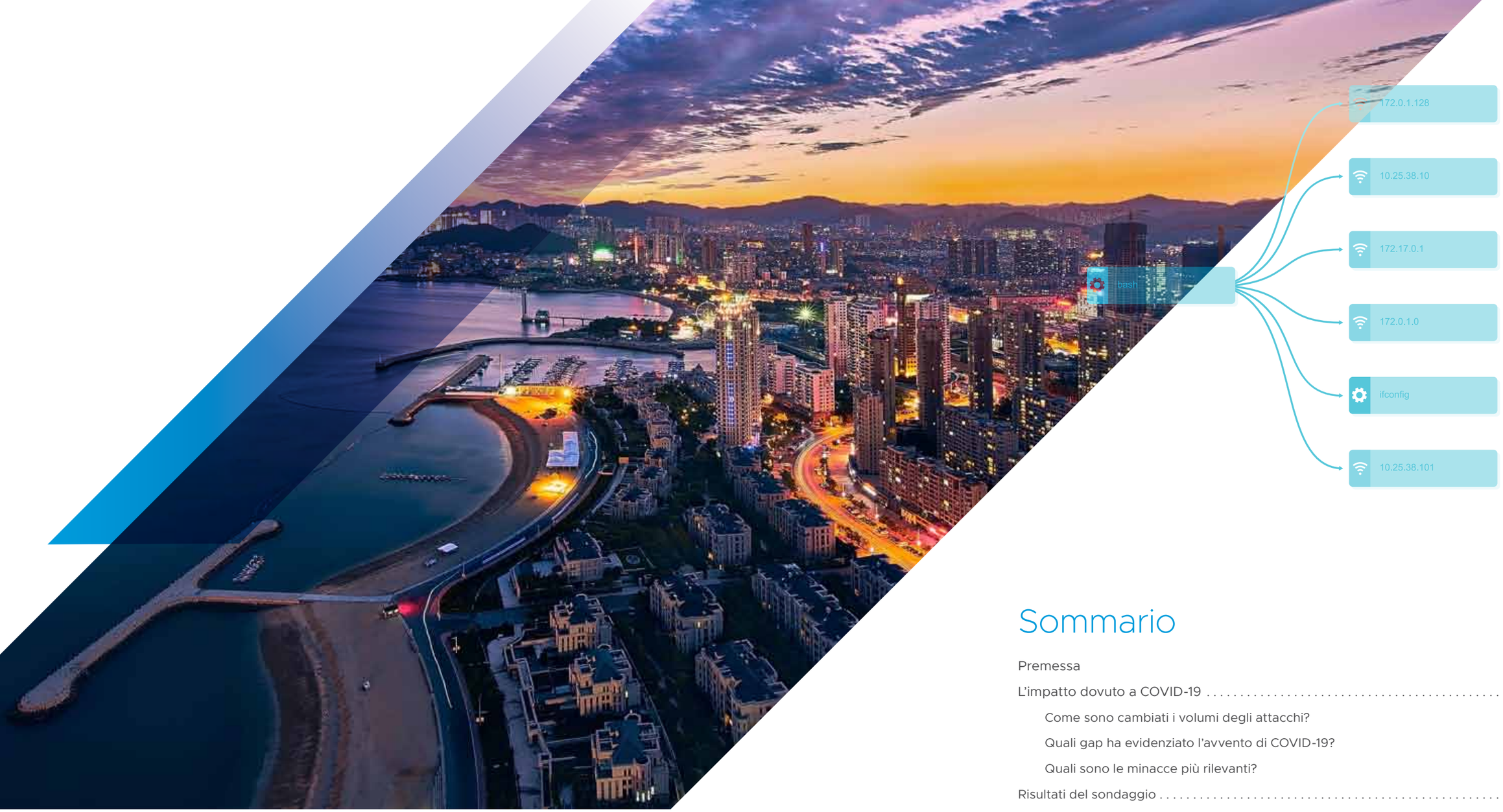
vmware Carbon Black

Italia Threat Report

Le imprese estese sotto minaccia

Giugno 2020



Introduzione preliminare

Questa ricerca è stata condotta per comprendere le sfide e le problematiche che le imprese italiane si trovano a dover affrontare in un contesto nel quale gli attacchi informatici continuano a intensificarsi. La ricerca individua le tendenze della pirateria informatica, le tipologie di attacchi con codici dannosi e l'impatto che eventuali violazioni hanno avuto in termini finanziari e di reputazione. L'indagine prende in esame l'approccio adottato dalle organizzazioni italiane per la messa in sicurezza delle nuove tecnologie, per l'adozione di quadri di riferimento in materia di sicurezza informatica e la complessità dell'ambiente all'interno del quale quest'ultima si debba attualmente gestire.

Sommario

IL PANORAMA DEGLI ATTACCHI INFORMATICI IN ITALIA NEL 2020

Rick McElroy
Cyber Security Strategist, VMware Carbon Black

Prefazione

Il panorama delle minacce informatiche in Italia ha registrato un'escalation. In questo documento, il nostro terzo Rapporto sulle minacce informatiche in Italia, abbiamo rilevato come la frequenza degli attacchi abbia raggiunto livelli senza precedenti: il 98% dei professionisti della sicurezza conferma, infatti, un aumento nel volume degli attacchi rispetto a febbraio e ottobre 2019, quando l'aumento si attestava rispettivamente al 93% e all'89%. Gli autori degli attacchi hanno utilizzato una serie di tattiche e tecniche più diversificata che mai, nel tentativo di estorcere, distruggere e infiltrarsi all'interno delle organizzazioni.

Di conseguenza, le violazioni sono state inevitabili. La nostra ricerca ha rilevato quanto segue:

Il 99% delle aziende italiane partecipanti allo studio ha dichiarato di aver subito una violazione dei dati a causa di un attacco informatico negli ultimi 12 mesi, con una media di 2,20 violazioni per organizzazione.

Il 68% delle aziende interpellate ha ammesso di avere subito una violazione 2 o più volte.

Il notevole aumento nella frequenza degli attacchi rivelato in questa iterazione del rapporto dimostra che, per quanto le imprese italiane si stiano adattando rapidamente a questo contesto di intensificazione, il panorama delle minacce informatiche evolve ancora più rapidamente. L'85% dei professionisti della sicurezza afferma che gli attacchi sono diventati più sofisticati, il 5% afferma che sono diventati significativamente più avanzati, mentre l'80% dichiara che sono diventati moderatamente o leggermente più sofisticati. Questi dati confermano ciò che la ricerca svolta dal team di analisi delle minacce di VMware Carbon Black ha effettivamente riscontrato: gli avversari stanno adottando tattiche più evolute, così come anche la commoditizzazione dei malware sta rendendo disponibili tecniche di attacco sempre più sofisticate a una più ampia coorte di criminali informatici. Le tipologie più prolifiche di attacchi informatici sono state quelle a Google Drive, seguite dal process hollowing (lo svuotamento dei processi) e dall'island hopping (un termine utilizzato per descrivere il processo di indebolimento delle difese informatiche di un'azienda, che consiste nell'attaccare la sua rete vulnerabile di partner, anziché lanciare un attacco diretto) - un cambiamento di passo rispetto all'ottobre dell'anno scorso, quando i custom e commodity malware si collocavano al primo posto.

METODOLOGIA

Nel marzo del 2020 VMware Carbon Black ha commissionato un'indagine a Opinion Matter, una società di ricerca indipendente. Sono stati intervistati 255 CIO, CTO e CISO italiani di aziende operanti in un'ampia gamma di settori verticali, come: servizi finanziari, sanità, pubblica amministrazione statale e locale, retail, produzione e progettazione industriale, alimenti e bevande, servizi di pubblica utilità, servizi professionali, media e intrattenimento. Si tratta del terzo Rapporto sulle minacce in Italia curato da VMware Carbon Black, basato sulle indagini precedenti, condotte a febbraio e ottobre 2019, nell'ambito di un progetto di ricerca globale in diversi Paesi, fra cui: Australia, Canada, Francia, Germania, Giappone, Italia, Paesi Bassi, Paesi Nordici, Regno Unito, Singapore, Spagna e Stati Uniti.

il 98%

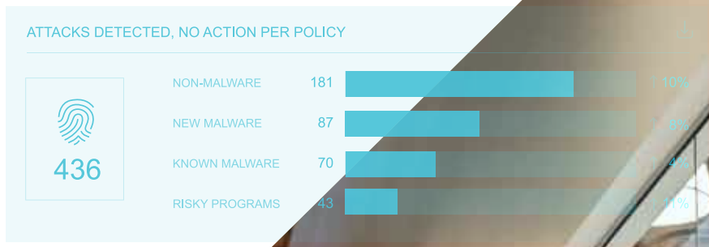
dei professionisti della sicurezza conferma un aumento nel volume degli attacchi

99%

Il 99% delle aziende italiane partecipanti allo studio ha dichiarato di aver subito una violazione dei dati a causa di un attacco informatico negli ultimi 12 mesi

l'85%

dei professionisti della sicurezza afferma che gli attacchi sono diventati più sofisticati, il 5% afferma che sono diventati significativamente più avanzati



26%

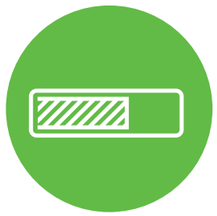
L'island hopping, pur essendo solo al terzo posto tra le tipologie di attacchi più prolifici, è stato la principale causa di violazioni

Rischio di violazioni tramite terzi in crescita

Oltre all'aumento generale dell'intensità, il presente rapporto rivela uno spostamento delle cause delle violazioni riuscite. L'island hopping, pur essendo solo al terzo posto tra le tipologie di attacchi più prolifici, è stato la principale causa di violazioni (26%), seguito dalla vulnerabilità del sistema operativo e dall'attacco alle applicazioni web. Inoltre, l'11% delle imprese violate è stato compromesso attraverso la propria supply chain. Chiaramente, è l'intero ecosistema aziendale a generare notevoli problemi di sicurezza.

Reputazione e profitto sotto tiro

Insieme all'aumento della consapevolezza dell'opinione pubblica circa i diritti in materia di protezione dei dati e l'aumento delle sanzioni per le violazioni di tali diritti, anche l'impatto delle violazioni ha continuato ad aumentare, con una percentuale crescente di intervistati che hanno denunciato gravi danni finanziari e di reputazione.



99%

Tutti i partecipanti al nostro sondaggio tranne due (99%) hanno previsto un aumento della spesa

I budget aumentano ancora, ma si tratta di una spesa strategica o tattica?

I professionisti della sicurezza in Italia stanno rispondendo all'incremento delle minacce informatiche aumentando la spesa per le difese informatiche. Tutti i partecipanti al nostro sondaggio tranne due (99%) hanno previsto un aumento della spesa.

Su cosa si orienterà tale spesa è una domanda interessante. Gli intervistati ci hanno detto inequivocabilmente che la caccia alle minacce (Threat Hunting) sta dando risultati ed è sempre più riconosciuta per il suo valore ai fini dell'identificazione dei soggetti malintenzionati già presenti nel sistema. Sembra quindi probabile che questo investimento continuerà, ma che dire dei rischi emergenti?

Il 49%

afferma di dover aumentare la spesa per la sicurezza informatica

Nel nostro sondaggio dell'ottobre 2019, l'89% degli intervistati dichiarava di avere timori riguardanti la sicurezza nell'ambito dell'implementazione e della gestione della trasformazione digitale e del 5G. Ma, quando si arriva al nocciolo della questione, le opinioni sulla necessità di spendere per la sicurezza divergono. Il 49% afferma di dover aumentare la spesa per la sicurezza e i controlli, mentre il 50% non aumenterà il budget per la messa in sicurezza del 5G.

Un ambiente complesso, affollato e multitecnologico

Forse perché stanno già supportando diverse tecnologie di sicurezza, gli intervistati hanno già messo in campo, in media, più di otto diverse console o agenti per gestire il proprio programma di sicurezza.

Ciò sta a indicare un ambiente di sicurezza che si è evoluto su base reattiva, in quanto gli strumenti di sicurezza sono stati aggiunti per affrontare le minacce emergenti, senza essere integrati. Ciò ha prodotto ambienti a compartimenti stagni, difficili da gestire, che fin dall'inizio prestano il fianco agli aggressori. Poiché quindi il panorama delle minacce informatiche sta raggiungendo la saturazione, è giunto il momento di razionalizzare, di pensare in modo strategico e fare chiarezza sull'implementazione della sicurezza.

Divisi circa il valore dei framework per la sicurezza

La visibilità e la validazione della posizione di sicurezza possono essere notevolmente migliorate con l'applicazione del framework MITRE ATT&CK®, seppure gli intervistati sono divisi sulla rilevanza e sul valore di questo approccio. Il 57% ne è consapevole, e il 39% prevede di utilizzarlo per convalidare la posizione di sicurezza, mentre il 43% non ne è a conoscenza, a dimostrazione del fatto che c'è ancora molto da fare per far sì che questo quadro di riferimento diventi il gold standard tra le imprese.

Il workload / Le applicazioni rappresentano Il più alto rischio di violazioni percepito

Il workload e le applicazioni sono in cima alla lista dei rischi di violazione degli intervistati, con la metà che li associa al rischio principale. Ma a seguire troviamo subito i network, citati come il rischio principale per quasi un terzo delle organizzazioni. Questo dato, forse, non sorprende, alla luce dell'incremento delle violazioni di applicazioni di terze parti. Poiché le aziende gestiscono un numero sempre maggiore di applicazioni nel tentativo di aumentare la flessibilità e la produttività, garantirne la sicurezza diventerà di importanza fondamentale.

Framework MITRE ATT&CK®

57% vs 39%

Il 57% ne è consapevole, e il 39% prevede di utilizzarlo

L’impatto della pandemia dovuta al COVID-19

Quando abbiamo condotto la ricerca principale per questa edizione del Rapporto sulle minacce di VMware Carbon Black, l’impatto della pandemia di COVID-19 stava appena cominciando a farsi sentire in tutto il mondo. Nel frattempo, analizzando i risultati, è emerso chiaramente che, a causa della rapida escalation della crisi, sarebbe stato poco corretto presentare la ricerca senza tentare di includere una misurazione dell’impatto che la situazione sta avendo sulla sicurezza informatica e sullo scenario delle minacce informatiche. Pertanto, siamo tornati dai nostri CISO con domande supplementari per capire l’impatto immediato della crisi e ciò che i professionisti della sicurezza informatica stanno riscontrando sul campo per adattarsi a uno scenario in rapida evoluzione. Siamo grati a tutti coloro che hanno dedicato del tempo a rispondere durante questo periodo critico e crediamo che le informazioni ottenute si riveleranno preziose per orientare la risposta in termini di sicurezza informatica in futuro.

Ci auguriamo che possiate ritenere il nostro terzo Rapporto sulle minacce in Italia utile e ricco di informazioni.

Risultati della ricerca supplementare sulla pandemia di COVID-19

Nel periodo marzo-aprile 2020, 252 intervistati italiani hanno risposto alle seguenti domande supplementari

Si sente spesso dire che nessuna pianificazione possa sopravvivere al contatto con il nemico. In questo caso, il nemico proviene da un luogo inaspettato e l’improvviso spostamento a livello globale verso il lavoro da casa ha sia aumentato l’attività di attacchi informatici, sia messo in luce alcune aree chiave che i team di sicurezza hanno dovuto affrontare, imparando nel mentre. La nostra ricerca sulla pandemia di COVID-19 ha rilevato come la stragrande maggioranza si trovi ad affrontare un aumento dei volumi di attacchi informatici a causa dei dipendenti che lavorano da casa, e il malware correlato alla pandemia COVID-19 sta facendo sentire la sua presenza dannosa.

Le lacune predominanti individuate nella pianificazione del disaster recovery ruotano intorno alla comunicazione con soggetti esterni come clienti, potenziali clienti e fornitori, così come nelle stesse operazioni IT, nelle sfide dovute al lavoro a distanza e nella comunicazione con i dipendenti.

Chi si era dimostrato riluttante verso l’adozione di un’autenticazione multi-factor ha dovuto pentirsene, poiché l’incapacità di implementarla costituisce oggi la più grande minaccia affrontata da più di un quarto dei nostri intervistati in tutto il mondo. Man mano che ci adeguiamo a una nuova normalità caratterizzata dall’aumento del lavoro a distanza e delle minacce ad esso associate, i team IT dovranno affrontare la sfida di estendere la protezione della sicurezza alle case dei dipendenti.

“Gli autori degli attacchi hanno utilizzato una serie di tattiche e tecniche più diversificata che mai, nel tentativo di estorcere, distruggere e infiltrarsi all’interno delle organizzazioni”

Il numero complessivo di attacchi informatici tipici del Vostro sistema é cambiato a seguito dell’aumento del numero di dipendenti che lavorano da casa?

Il **90,5%** degli intervistati italiani ha dichiarato di aver assistito a un aumento degli attacchi informatici complessivi a causa dei dipendenti che lavorano da casa. Poco meno di un sesto (14%) ha riferito che tali attacchi sono aumentati tra il 50 e il 100% e il 39% ha riferito aumenti tra il 25 e il 100%.

L’aumento percentuale medio degli attacchi è stato di **24,24.**

La percentuale media per quanto concerne il settore dei servizi finanziari, pari a **23,34%,** è stata leggermente inferiore alla media complessiva, ma l’11% delle organizzazioni ha registrato un aumento tra il 50 e il 100% e il 21% degli intervistati ha registrato un aumento tra il 25 e il 49%.

Il 72% delle aziende con un numero di dipendenti compreso **tra 251 e 500** ha dichiarato gli incrementi maggiori.

I team IT di dimensioni comprese tra **21 e 30** hanno riportato una media bassa, pari al 15,79%, e questo perché l’85% degli intervistati ha dichiarato solo un aumento inferiore al 25% degli attacchi informatici.

il 90,5%

degli intervistati italiani ha dichiarato di aver assistito a un aumento degli attacchi informatici complessivi a causa dei dipendenti che lavorano da casa.

47%

Poco meno della metà (47%) degli intervistati ha segnalato lacune molto significative in termini di efficacia nella pianificazione del disaster recovery inerenti alla comunicazione con i propri interlocutori esterni

Quali sono le eventuali lacune che lapandemia di COVID-19 ha portato alla luce nella pianificazione del disaster recovery della vostra azienda e quanto sono state significative rispetto all'efficacia del vostro piano di disaster recovery?

Poco meno della metà (47%) degli intervistati ha segnalato lacune molto significative in termini di efficacia nella pianificazione del disaster recovery inerenti alla comunicazione con i propri interlocutori esterni, tra cui clienti, potenziali clienti e partner. Nel complesso, l'81% ha segnalato lacune, di entità da grave a lieve, nella **comunicazione con gli interlocutori esterni.**

Il 41% ha segnalato lacune molto significative nella pianificazione del disaster recovery nelle **attività operative IT**, ivi inclusa la distribuzione di hardware e software. Nel complesso, il 90% ha segnalato lacune di entità variabile (da grave a lieve).

Per quanto riguarda **l'abilitazione di una forza lavoro a distanza**, oltre un terzo (37%) degli intervistati ha avvertito lacune gravi e significative e, nel complesso, l'89% degli intervistati ha ritenuto che vi fossero lacune nella propria pianificazione.

Ben oltre un terzo (38%) degli intervistati italiani ha ritenuto che ci fossero lacune molto significative nella **visibilità relativa alle minacce alla sicurezza informatica**, con un ulteriore 36% che ha dichiarato lacune di lieve entità.

Poco più di un quarto degli intervistati (26%) ha ammesso gravi lacune nella gestione della pandemia in termini di **comunicazione con i dipendenti**; nel complesso, il 77% degli intervistati ha dichiarato che si è trattato di lacune o lievi o molto significative.

Per quanto riguarda il **recovery planning**, il 36% degli intervistati ha individuato lacune molto significative e il 90% ha evidenziato lacune di qualche tipo.

Un intervistato ha scelto di non rispondere a questa domanda.

25%

Un quarto degli intervistati (25%) ha dichiarato che l'incapacità di implementare l'autenticazione a più fattori costituisce la più grande minaccia per la propria azienda

Quale delle seguenti minacce associate alla pandemia di COVID-19 Ha costituito finora la più grande minaccia per la vostra azienda?

Un quarto degli intervistati (25%) ha dichiarato che **l'incapacità di implementare l'autenticazione a più fattori** costituisce la più grande minaccia per la propria azienda. Al secondo posto, con il 21%, il **malware legato alla pandemia di COVID-19**, e al terzo posto le **e-mail di phishing** (11%). Il 9,5% ha citato **inefficienze riguardanti** l'accesso remoto, il 9% **l'impossibilità di distribuire tempestivamente le patch del software** e il 6% il ransomware. Altre minacce degne di nota sono state **l'esposizione all'IoT** (6%), lo **spear phishing** (una truffa tramite comunicazioni elettroniche o e-mail indirizzata a una persona, un'organizzazione o un'azienda specifica) (5%) e il **social engineering** (5%).

L'incapacità di implementare l'autenticazione multi-factor è stata la maggiore minaccia citata dalle organizzazioni legate ai **servizi finanziari** (46%). Anche il **malware correlato alla pandemia di COVID-19** (11%) e le e-mail di phishing (6%) hanno rappresentato un problema per questo settore.

Per le aziende di dimensioni comprese tra **251 e 500** dipendenti, l'impatto maggiore è dovuto all'**impossibilità di implementare l'autenticazione a più fattori** (48%).

Lo stesso fattore è stato evidenziato anche dal 46% delle aziende con un team di 21-30 addetti.

96%

L'aumento più elevato nel cambiamento delle minacce durante la crisi è stato registrato in relazione al malware legato alla pandemia di COVID-19, per cui gli intervistati hanno segnalato un aumento complessivo del 96%.

Come sono cambiate le minacce durante la pandemia e in che misura?

L'aumento più elevato nel cambiamento delle minacce durante la crisi è stato registrato in relazione al malware legato alla pandemia di COVID-19, per cui gli intervistati hanno segnalato un aumento complessivo del 96%. Questo dato è seguito a breve distanza sia dalle **e-mail di phishing** sia dallo **spear phishing**, che hanno rispettivamente registrato un aumento del 94% nelle variazioni delle minacce.

Recentemente è stata rilevata una nuova famiglia di **ransomware** nota come Coronavirus e si è registrata una tendenza all'aumento di questo fenomeno. Purtroppo, non c'è mai stato un momento migliore per gli attaccanti per creare e distribuire **ransomware** e, sebbene l'aumento complessivo sia stato inferiore rispetto ad altre minacce, oltre un terzo degli intervistati (35,8%) ha riferito aumenti nelle categorie dal 51% a oltre il 100%.

Il 92% degli intervistati italiani ha riferito aumenti complessivi delle variazioni delle minacce legati all'**incapacità di adottare l'autenticazione a più fattori** e il 91% l'**impossibilità di distribuire tempestivamente le patch del software**. Analogamente, gli intervistati hanno segnalato un forte aumento delle variazioni delle minacce per l'**esposizione all'IoT** (92%).

I risultati completi della ricerca

Ha riscontrato un aumento degli attacchi informatici nei confronti della sua azienda negli ultimi 12 mesi? Se sì, può quantificare?

Uno sbalorditivo 98% delle organizzazioni italiane ha riscontrato un aumento del numero di attacchi informatici nei confronti della propria azienda nel corso degli ultimi 12 mesi. Si tratta di un aumento considerevole rispetto all'89% dell'ottobre 2019 e al 93% del febbraio 2019, nonché della più alta frequenza di attacchi a cui abbiamo mai assistito.

Il 52% degli intervistati ha riferito un aumento medio dei volumi di attacchi tra il 51 e il 100% e il 16,5% ha affermato che c'è stato un aumento dei volumi di attacchi tra il 101 e il 200%, un salto considerevole rispetto all'ultimo rapporto, in cui solo il 31% riferiva aumenti di tale entità.

Il 61% degli intervistati operanti nel settore **manifatturiero e ingegneristico** ha registrato un aumento del 51-100%, mentre il 62,5% del **settore sanitario** ha registrato un aumento del 51-100%.

Le imprese della fascia 501-1000, 1002-2000 e 2001-5000 si trovano a fronteggiare volumi di attacchi superiori alla media, con un aumento rispettivamente del 54%, 51% e 59%.

Gli attacchi informatici alla sua azienda sono diventati più o meno sofisticati negli altimi 12 mesi?

L'85% degli intervistati dichiara che gli attacchi sono diventati più sofisticati negli ultimi 12 mesi, a fronte del 90% che affermava la stessa cosa nell'ottobre 2019 e del 94% nel febbraio 2019. Di questi, tuttavia, solo il 5% ha dichiarato che gli attacchi sono diventati **significativamente** più sofisticati. Ancora una volta un notevole calo rispetto all'ultimo rapporto, dove il 41% rilevava un significativo aumento della sofisticatezza.

I servizi finanziari hanno registrato la percentuale più alta tra chi ritiene che gli attacchi fossero diventati significativamente più sofisticati (24%).

Oltre la metà (52%) delle imprese della categoria 501-1000 ha dichiarato che gli attacchi sono diventati notevolmente o moderatamente più sofisticati.

98%

Uno sbalorditivo 98% delle organizzazioni italiane ha riscontrato un aumento del numero di attacchi informatici nei confronti della propria azienda nel corso degli ultimi 12 mesi.

85%

L'85% degli intervistati dichiara che gli attacchi sono diventati più sofisticati

il99% dei CISO/CIO che hanno partecipato alla nostra ricerca ha dichiarato di aver subito una violazione a seguito di un attacco informatico negli ultimi 12 mesi.

Nonostante sia presente solo nel 15% degli attacchi, l'island hopping è stato la causa del 26% delle violazioni.

Qual é stata la frequenza delle violazioni dovute ad attacchi informatici alla sua azienda negli ultimi 12 mesi?

Il 99% dei CISO/CIO che hanno partecipato alla nostra ricerca ha dichiarato di aver subito una violazione a seguito di un attacco informatico negli ultimi 12 mesi. Si tratta del dato più alto di violazioni segnalate nella storia della nostra ricerca, con un salto rispetto al 93% di coloro che avevano dichiarato di avere subito violazioni nell'ottobre 2019.

Il numero medio di violazioni subite dalle organizzazioni è di 2,20. Il 68% degli intervistati ha dichiarato di aver subito due o più violazioni. Tuttavia, un preoccupante 6% ha affermato di aver subito cinque o più violazioni. **I servizi di pubblica utilità**, i servizi professionali, il comparto **alimenti e bevande e l'assistenza sanitaria** hanno riportato il più alto numero medio di violazioni; un'organizzazione sanitaria ha addirittura riferito di aver subito più di 10 violazioni.

Anche le dimensioni contano. Oltre la metà delle organizzazioni (57,5%) nella fascia 2001-5000 dipendenti ha subito violazioni due volte. Per quanto riguarda le organizzazioni della fascia 5001-10000, oltre un terzo (37,5%) ha riferito di avere subito violazioni tre volte.

Qual é stata la causa principale di queste violazioni?

La causa principale delle violazioni è stata identificata nel cosiddetto **island hopping**, in quanto i vettori di attacco nella supply chain si rivelano un facile bersaglio per gli hacker. Troviamo poi la vulnerabilità del sistema operativo (18%) e gli attacchi ad applicazioni web (14%).

Le società di **servizi finanziari** (24%) e di **servizi professionali** (24%) sono le più colpite dalle violazioni dovute alla vulnerabilità del sistema operativo.

È interessante notare che, nonostante sia presente solo nel 15% degli attacchi, l'**island hopping** è stato la causa del 26% delle violazioni. Ciò sta a indicare la vulnerabilità delle extended companies agli attacchi provenienti dalle organizzazioni partner/fornitrici. Un'altra ricerca di VMware Carbon Black rivolta ai professionisti dell'incident response ha rilevato che l'island hopping è presente nel 41% dei tentativi di violazione riscontrati.

L'island hopping è soprattutto un problema in settori caratterizzati da grandi ecosistemi di fornitori, come il comparto **manifatturiero e ingegneristico** (37%), l'**assistenza sanitaria** (27,5%) e il segmento **alimenti e bevande** (30%).

Sorprendentemente, gli **attacchi di phishing** sono diminuiti drasticamente tra le violazioni riuscite. Nell'ottobre 2019 il phishing rappresentava la causa del 23% delle violazioni riuscite, mentre ora è sceso ad appena il 2%. Lo stesso può dirsi del **ransomware**, sceso dal 24% al 3%.

l'83%
degli intervistati ha dichiarato di aver subito un impatto negativo sulla propria reputazione a causa di una violazione

99%
Tutti i CISO/CIO interpellati, tranne due (99%), hanno dichiarato di voler aumentare il budget per la difesa informatica

Quali sono state le conseguenze di queste Violazioni Per La Sua azienda, dal punto di vista finanziario e della reputazione?

La percentuale di intervistati che hanno riferito un impatto finanziario a seguito di una violazione è stata del 59%, in leggero aumento rispetto agli intervistati dell'ottobre 2019 (56%); tuttavia, quando le organizzazioni vengono colpite, la gravità dell'impatto è leggermente inferiore (3,5% contro il 6,5% dell'ottobre 2019).

Tuttavia, la percentuale di intervistati che riferisce l'assenza di un impatto finanziario è diminuita, passando dal 39% nell'ottobre 2019 al 32% odierno, un dato che suggerisce come l'impatto finanziario sia in aumento.

L'83% degli intervistati ha dichiarato di aver subito un impatto **negativo** sulla propria reputazione a causa di una violazione, un salto in avanti rispetto al 68% che dichiarava la stessa cosa nell'ottobre 2019. Per il 7% si è trattato di un impatto di **grave** entità.

Poco meno della metà (43%) delle società operanti nel **settore dei servizi finanziari** ha dichiarato di aver subito un grave impatto, in termini di reputazione, a causa di una violazione.

Di quanto intendete aumentare il budget di spesa per la difesa informatica nei prossimi 12 mesi?

Tutti i CISO/CIO interpellati, tranne due (99%), hanno dichiarato di voler aumentare il budget per la difesa informatica nei prossimi 12 mesi, con un aumento medio previsto del 30%. Il 46% afferma che prevede di aumentare il budget del 31-40%, contro il 25,5% che dichiarava la stessa cosa in occasione dell'ultima ricerca. Il 5,5% dichiara che prevede di aumentare il budget fino al 41-50%.

Tra questi, troviamo tre quinti (60%) delle organizzazioni del **comparto manifatturiero e ingegneristico** e il 54% di quelle operanti nel settore dei **media e dell'intrattenimento** che hanno in programma di aumentare il budget del 31-40%.

Le aziende più grandi stanno pianificando gli aumenti maggiori: il 54% nella fascia 2001-5000 e il 52% nella fascia 1001-2000 prevede aumenti del 31-40%.

Nei prossimi 6-12 mesi adotterete il 5g e dovrete aumentare la spesa per la sicurezza e I controlli per poterlo adottare (ossia, state effettuando un nuovo investimento netto sulla base di questo nuovo rischio)?

Ogni CISO/CIO interpellato, ad eccezione di due, ha dichiarato di avere in programma l'adozione del 5G nei prossimi 12 mesi, con il 51% che prevede di farlo nei prossimi sei mesi. Gli intervisti si distribuiscono pressoché equamente per quel che riguarda le implicazioni in termini di sicurezza. Il 49% dichiara che dovrà aumentare la spesa per la sicurezza al fine di gestire l'adozione del 5G, mentre il 50% non crede di dover investire.

Le organizzazioni di servizi finanziari sono maggiormente propense a dichiarare che nei prossimi sei mesi adotteranno il 5G e investiranno nella sicurezza e nei controlli correlati (38%). La pubblica amministrazione e le autorità locali stanno cercando di adottare il 5G e investiranno nella sicurezza e nei controlli correlati nei prossimi 12 mesi (41%). Analogamente, questo dato è risultato simile per gli intervistati del settore manifatturiero e ingegneristico.

Le aziende della fascia 2001-5000 sono state le più propense a dichiarare di avere in programma l'adozione del 5G nei prossimi 12 mesi (46%) e di voler spendere per sicurezza e controlli.

43%
La percentuale che ha trovato evidenze significative di attività dannose è stata del 43%,

Ogni CISO/CIO interpellato, ad eccezione di due, ha dichiarato di avere in programma l'adozione del 5G nei prossimi 12 mesi

il 100%
degli intervistati utilizzano il threat hunting come parte della propria strategia di sicurezza informatica

Negli ultimi 12 mesi, il threat hunting (la ricerca proattiva e iterativa di minacce) ha raggiunto l'obiettivo di rafforzare le difese nei confronti degli attacchi informatici e ha rilevato attivita' malevole che normalmente non sarebbero state rilevate?

Il Threat Hunting sta diventando onnipresente, con il 100% degli intervistati che lo utilizzano come parte della propria strategia di sicurezza informatica, rispetto al 93% dell'ottobre 2019. Si sta inoltre dimostrando più efficace; complessivamente, il 99% ha dichiarato di aver rafforzato le difese della propria azienda, mentre il 14% dichiara di averlo fatto in modo significativo.

La percentuale che ha trovato **evidenze significative** di attività dannose è stata del 43%, mentre nel complesso il 93% ha trovato qualche evidenza di attività dannose grazie al threat hunting (rispetto all'87% dell'ultima ricerca).

Il 51%
degli enti governativi e delle autorità locali prevede di adottare il 5G nei prossimi sei mesi

8.5
Il numero medio di tecnologie implementate è 8,5

57%
La conoscenza del framework MITRE ATT&CK® è relativamente alta: il 57% dichiara di conoscerlo, mentre il 43% non ne ha alcuna conoscenza

Quante diverse tecnologie di sicurezza avete a disposizione per gestire il vostro programma di sicurezza (ad es. console, agenti e strumenti multipli)?

Poco più di tre quarti (76%) delle aziende dispongono di 5-10 diverse tecnologie implementate per la gestione dei propri programmi di sicurezza. Il 14% dispone di 11-25 diverse tecnologie.

Il numero medio di tecnologie implementate è 8,5. I team IT di 51-100 persone utilizzano in media più strumenti: 12,21 rispetto a una media di 8,5.

Conosce e ha in programma di utilizzare il framework mitre att&Ck® per convalidare la posizione di sicurezza?

La conoscenza del framework MITRE ATT&CK® è relativamente alta: il 57% dichiara di conoscerlo, mentre il 43% non ne ha alcuna conoscenza. Fra coloro che ne sono a conoscenza, il 39% ha in programma di utilizzarlo, mentre il 18% ne è a conoscenza ma non ha intenzione di adottarlo.

Il settore dei **servizi finanziari** è quello che conosce meglio il quadro di riferimento; il 95% ne è a conoscenza, ma solo il 43% ha intenzione di utilizzarlo. Per quanto riguarda la **pubblica amministrazione e gli enti locali**, nonché la **sanità**, rispettivamente il 45,5% e il 45% ne sono a conoscenza e hanno in programma di utilizzarlo.

Nel corso degli ultimi 12 mesi quali tra le categorie sotto indicate - se presenti - hanno richiesto un investimento al rialzo o al ribasso (ad es. la riassegnazione delle priorità del budget)

I workload / le applicazioni sono in prima linea per quanto riguarda la necessità di riassegnare le priorità in termini di allocazione del budget per il 77% degli intervistati, seguiti dalle reti (67%), poi dai cellulari (55%) e infine dagli endpoint (50%).

Quale dei seguenti rappresenta il principale rischio di violazione – se presente - del vostro programma di sicurezza?

I workload / le applicazioni sono considerati il rischio maggiore, citato dal 52% degli intervistati, seguiti dalle reti, indicate da poco meno di un terzo (30%). Il rischio successivo citato con maggior frequenza è quello dei dispositivi mobili (10%), mentre gli endpoint come portatili e computer desktop si collocano al 9%.

I **servizi finanziari** vedono un rischio superiore alla media proveniente dai dispositivi mobili (29%), così come la **pubblica amministrazione e gli enti locali** (18%). Il settore **manifatturiero e ingegneristico** vede il rischio maggiore correlato ai workload e alle applicazioni, così come il settore **sanitario**. Il 71% delle organizzazioni della fascia 1001-2000 considera i workload e le applicazioni come soggetti al maggior rischio di violazione.