cybereason

RANSOMWARE: IL VERO COSTO PER LE ATTIVITÀ

PreventID

Uno studio globale sull' impatto del ransomware sulle attività

INTRODUZIONE
IL PUNTO DI VISTA DEL CEO

Nel maggio del 2021, Colonial Pipeline ha dichiarato di essere caduta vittima di un devastante attacco ransomware che ha portato all'interruzione delle operazioni e ha impedito la fornitura di combustibile a milioni di persone, causando notevoli danni economici in tutta la zona orientale degli Stati Uniti. L'FBI ha confermato che gli attacchi sono stati effettuati dall organizzazione DarkSide, una nuova minaccia che Cybereason ha tenuto d'occhio fin dall'agosto del 2020.

Si stima che avvenga un attacco ransomware contro un'azienda ogni 11 secondi, con un danno globale stimato di 20 miliardi di dollari quest'anno. L'FBI ha comunicato di un aumento di oltre 225% nelle perdite causate da questo tipo di attachi negli Stati Uniti nel solo 2020.

Gestirne le conseguenze è complicato e costoso. Le scoperte di questa ricerca rivelano che la maggioranza delle organizzazioni hanno subito notevoli impatto a causa degli attacchi ransomware, inclusi diminuzione di fatturato e danni al marchio, riduzioni impreviste della forza lavoro e addirittura chiusura dell'attività.

La ricerca sottolinea che la prevenzione è la migliore strategia per la gestione dei rischi associati ai ransomware e per garantire che l'organizzazione non cada vittima di tale attacco.

LIOR DIV
CEO di CYBEREASON

Questa ricerca ha rivelato che la maggior parte delle organizzazioni che hanno deciso di pagare i riscatti in passato non sono state immuni ad attacchi successivi dello stesso tipo e spesso da parte degli stessi autori. Inoltre, possedere una copertura assicurativa informatia non garantisce che un'organizzazione sia in grado di recuperare le perdite associate a un attacco ransomware.

Un aspetto importante di questo report è che fornisce un approfondimento dell'impatto degli attacchi ransomware sull'attività di fasce verticali chiave dell'economia e rivela dati che possono essere utilizzati per migliorare gli approcci di difesa da questa categoria di attacco. La ricerca sottolinea che la prevenzione è la migliore strategia per la gestione dei rischi da ransomware e per garantire che l'organizzazione non cada vittima di uno di questi attacchi.

Cybereason si impegna a individuare le minacce emergenti e a fornire informazioni utilizzabili per migliorare la difesa contro gli attacchi innovativi. Insieme possiamo contrastare il vantaggio che ora è nelle mani degli avversari e posizionarci dietro a una solida difesa.

RISULTATI CHIAVE

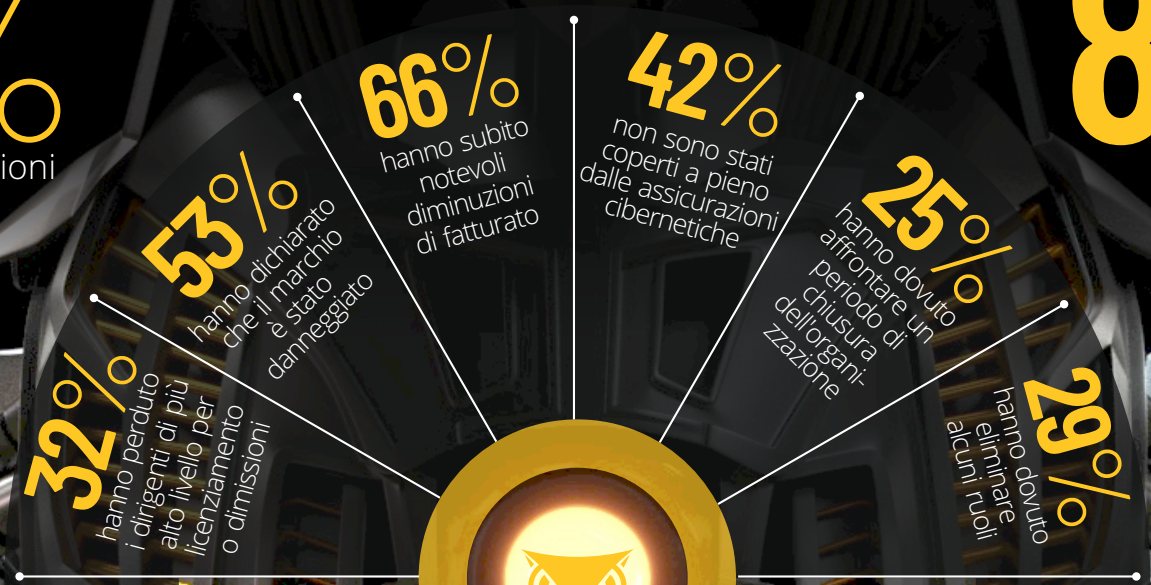
Il rischio è reale

81%
hanno preoccupazioni alte o molto alte di rischio di attacchi ransomware

73%
hanno un piano o procedure specifiche per gestire in modo efficace un attacco ransomware

42%
ritengono di possedere le persone giuste per risolvere il problema

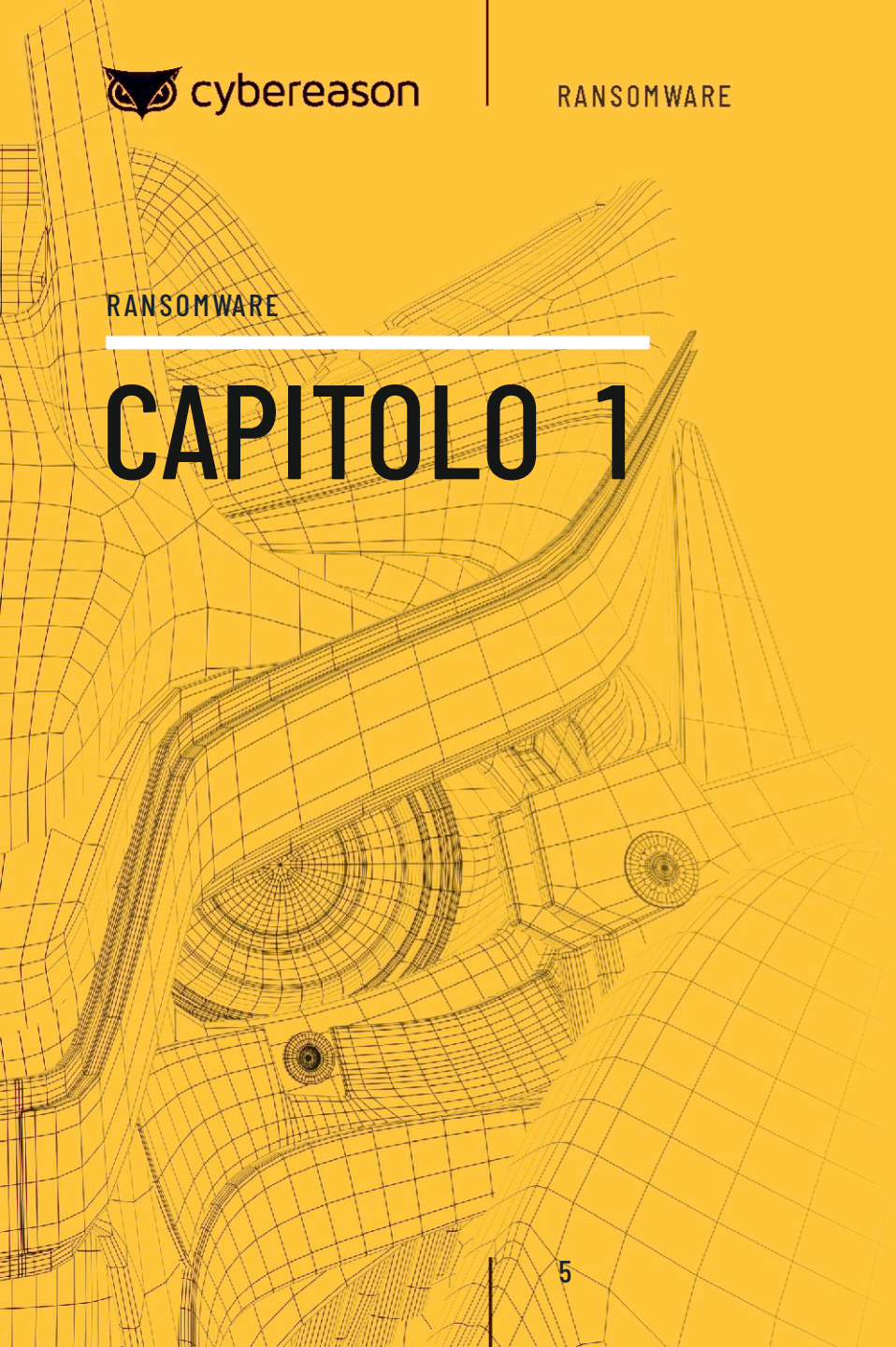
IMPATTO DEL RANSOMWARE SULL'ATTIVITÀ



Non conviene pagare

80%
di coloro che hanno pagato il riscatto hanno subito un altro attacco

46%
hanno riottenuto l'accesso ai dati dopo il pagamento, ma alcuni o tutti i dati sono risultati corrotti



RANSOMWARE

CAPITOLO 1

IMPATTO DEL RANSOMWARE SULL'ATTIVITÀ

Gli attacchi ransomware possono avere un impatto negativo su un'organizzazione in diversi modi, con perdite combinate che possono raggiungere le decine o addirittura le centinaia di milioni di dollari. L'impatto a breve termine può comprendere, tra gli altri, danni ai processi fondamentali dell'attività a causa dell'inaccessibilità dei dati, costi associati alle azioni relative all'incidente e alle attività di mitigazione, interruzione dei processi di sistema, perdita di produttività e il pagamento del riscatto nel caso in cui l'organizzazione decida di acconsentire alla richiesta di estorsione.

L'impatto a lungo termine può includere una diminuzione di fatturato dell'attività, un danno alla reputazione del marchio, la perdita di funzionari chiave e il licenziamento di dipendenti e, in alcune circostanze, avere un impatto sull'intera vita dell'azienda nel suo complesso.

Delle 1263 persone che hanno risposto al sondaggio, il

66%

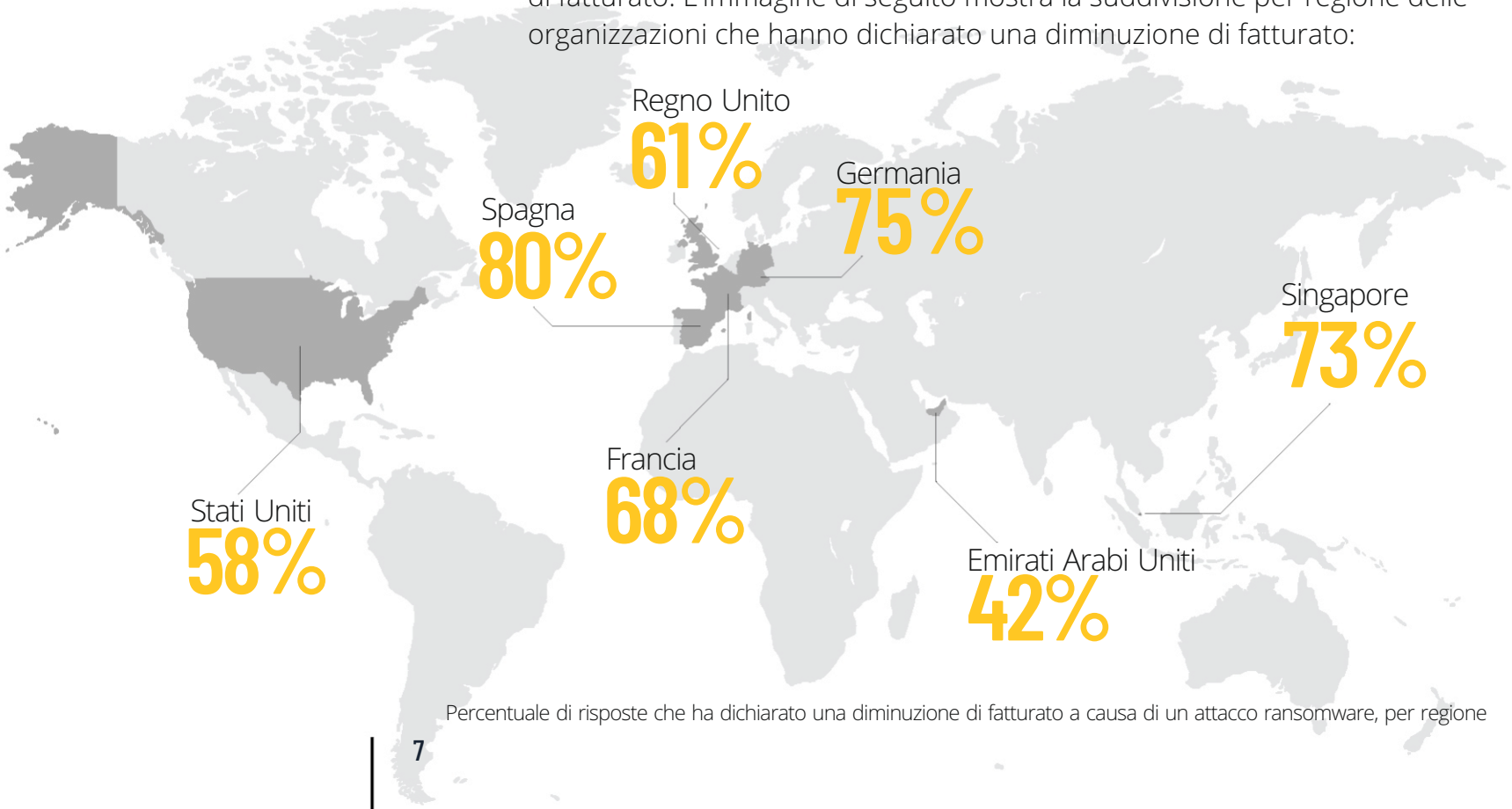
ha subito notevoli diminuzioni di fatturato

DIMINUZIONE DI FATTURATO

FedEx ha dichiarato perdite di circa 300 milioni di dollari come risultato degli attacchi ransomware di NotPetya del 2017 e la città di Atlanta ha dichiarato di aver speso oltre 2,6 milioni di dollari per il ripristino dopo un attacco ransomware di SamSam nel 2018. La città di Baltimora ha dichiarato di aver speso oltre 18 milioni di dollari per ricostruire la propria intera rete IT dopo aver rifiutato di pagare il riscatto dell'ennesimo attacco ransomware di SamSam e Cognizant Technology Solutions ha dichiarato una diminuzione degli utili nel 2020 parzialmente causati dai danni generati da un attacco ransomware di Maze.

DIMINUZIONE DI FATTURATO PER REGIONE

Delle 1263 risposte al sondaggio, due terzi (66%) hanno indicato che la loro organizzazione ha subito notevoli diminuzioni di fatturato come risultato diretto di un attacco ransomware. In base alle risposte del sondaggio, la dimensione dell'azienda sembra avere un impatto minimo sulla diminuzione di fatturato. L'immagine di seguito mostra la suddivisione per regione delle organizzazioni che hanno dichiarato una diminuzione di fatturato:



Percentuale di risposte che ha dichiarato una diminuzione di fatturato a causa di un attacco ransomware, per regione

ORGANIZZAZIONI CHE HANNO DICHIARATO UNA DIMINUZIONE DI FATTURATO, PER SETTORE:

75%
Governo

Servizi finanziari
73%

Vendita
74%

Sanità
64%

Tecnologia
64%

Automobilistico
58%

Manifattura
51%

Legale
50%

Questi risultati mettono in evidenza che ogni settore è vulnerabile, con un rischio statisticamente elevato, a diminuzioni di fatturato in seguito a un attacco ransomware, a causa dei danni generati ai processi dell'attività, ai tempi di indisponibilità dei sistemi, alle differenze tra le rapidità di recupero di risorse e persone, ai danni al marchio e altri effetti.

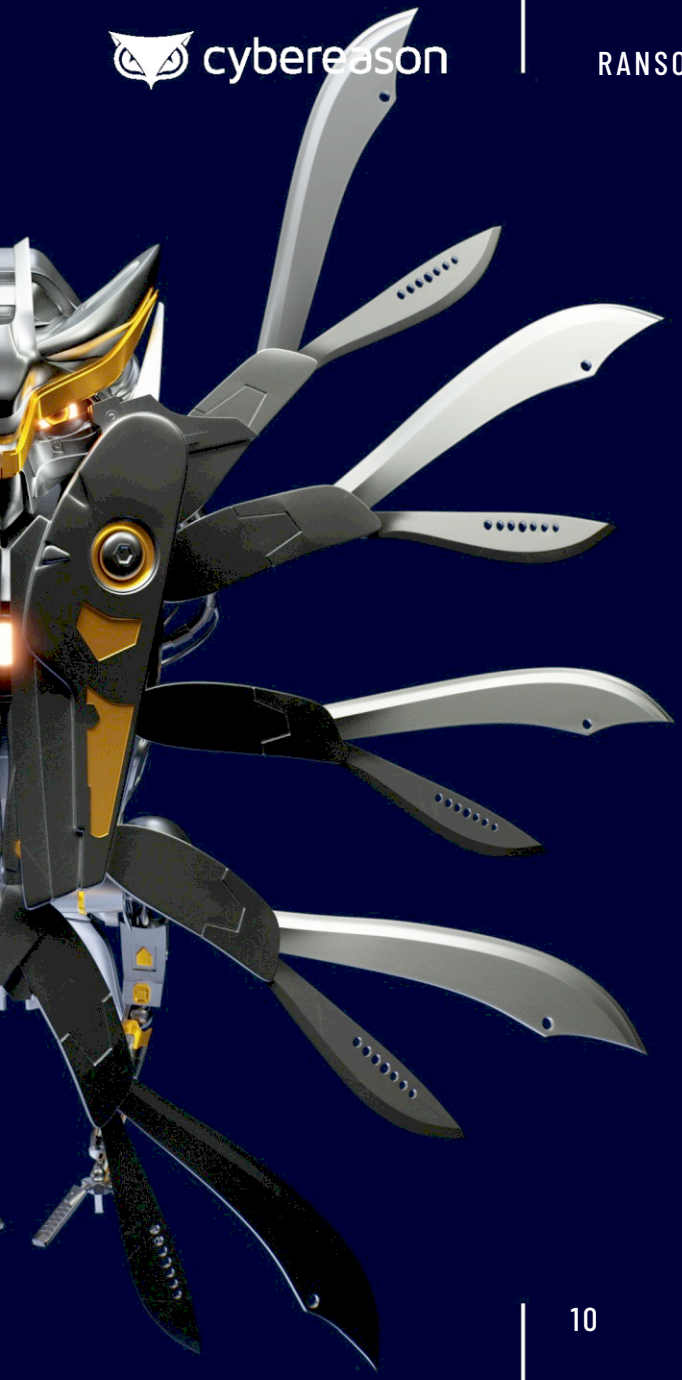
Percentuale di risposte che ha dichiarato una diminuzione di fatturato a causa di un attacco ransomware, per settore

DANNO AL MARCHIO E ALLA REPUTAZIONE

Nessuna azienda desidera seguire le orme di TJ Maxx, Target, Equifax o Microsoft dopo la recente compromissione globale del loro servizio Exchange Server. Tuttavia, anche questi famosi attacchi sono bazzecole in confronto a SolarWinds, il cui marchio stesso. è diventato un sinonimo dell'attacco

Gli attacchi ransomware possono essere e spesso sono, una macchia nei marchi a cui vengono associati. Per esempio, il sistema sanitario nazionale del Regno Unito (National Health Service, NHS) si sta ancora riprendendo dagli attacchi ransomware di WannaCry del 2017, che hanno causato un costo per l'organizzazione di oltre 100 milioni di dollari in perdite combinate e hanno causato oltre 19.000 appuntamenti annullati. Questo livello di danno ai servizi, ha indubbiamente avuto un impatto negativo sull'opinione che i clienti hanno dell'affidabilità del servizio sanitario nazionale.

In questa ricerca, oltre la metà (53%) delle risposte hanno indicato che il marchio delle loro organizzazioni ha subito un danno a seguito dell'attacco ransomware. Le risposte in Singapore (40%), Spagna (44%) e Francia (49%) rappresentano il minori numero di organizzazioni la cui reputazione è stata danneggiata da un attacco ransomware. Più della metà delle risposte in Germania (51%), Emirati Arabi Uniti (54%), Stati Uniti (56%) e Regno Unito (63%) dicono che il marchio delle organizzazioni è stato danneggiato.



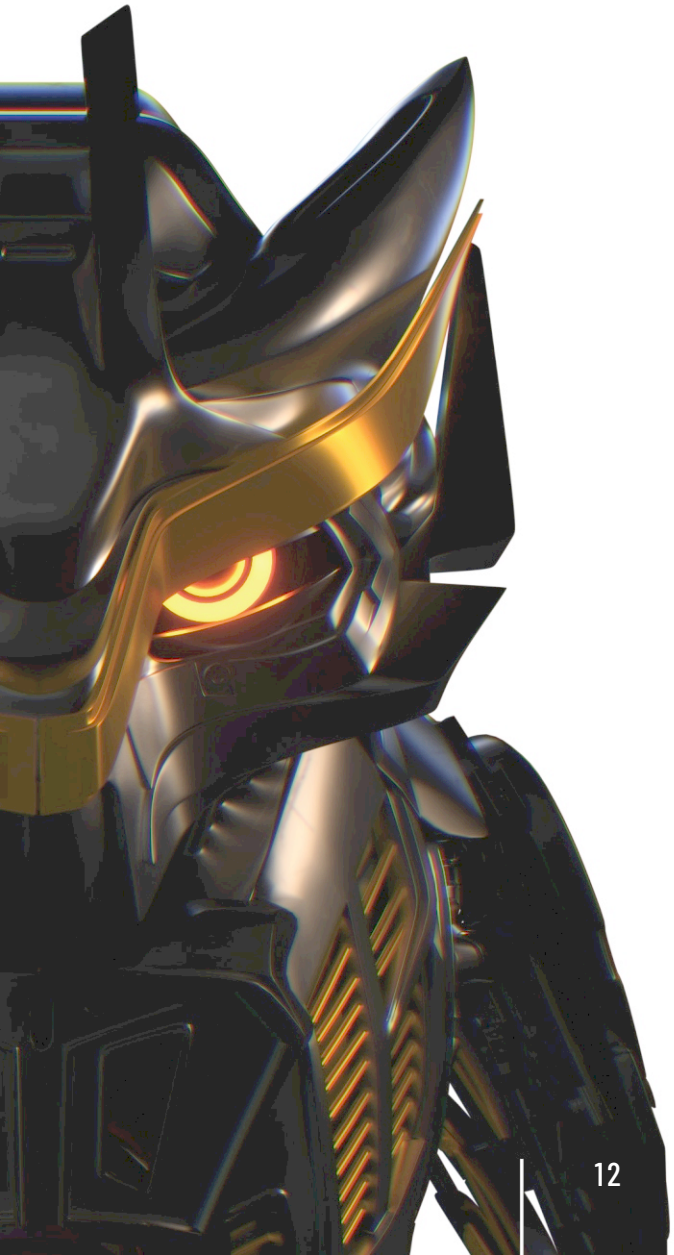
Le organizzazioni potrebbero credere di essere perfettamente preparate a gestire l'impatto di un attacco ransomware avendo una copertura assicurativa informatica, backup di dati e un sistema di ripristino completo in breve tempo. La realtà è che, per quanto un'organizzazione possa essere preparata ad affrontare un attacco, indipendentemente da altri fattori, il rischio di danno al marchio è notevole.

DIMISSIONI E LICENZIAMENTI DEI DIRETTORI

Il responsabile della sicurezza informatica è, sfortunatamente, la persona che più viene colpita dalle conseguenze di questi eventi. La durata media del mandato di responsabile della sicurezza informatica ha continuato a scendere nel corso degli anni ed è al momento tra 18 e 26 mesi. Sebbene abbiano il titolo di "responsabile", la maggior parte dei responsabili della sicurezza informatica non svolge un ruolo di rilievo all'interno della propria organizzazione.

Significa forse che sono immuni in seguito a gravi eventi di sicurezza? Tutto il contrario. I responsabili della sicurezza di Target, Home Depot, Sony e TalkTalk sono stati licenziati o si sono dimessi poco dopo i principali attacchi alla sicurezza andati a segno.

Gli attacchi ransomware rappresentano un rischio per tutti i dirigenti di alto livello, come evidenziato nel 2020, quando Jim Corrigan, direttore generale e presidente di ERT, è stato probabilmente spinto alle dimissioni in seguito a un attacco ransomware che ha portato a ritardi nelle prove vaccinali COVID-19 dell'azienda. Quasi un terzo delle risposte (32%) ha indicato di aver perso i propri dirigenti in seguito a un attacco ransomware, tramite licenziamento o a causa di dimissioni.



Per dirla in modo semplice, i giusti strumenti di prevenzione, rilevazione e risposta allo scopo di respingere i tentativi di attacco ransomware possono avere un effetto diretto sulla durata del mandato dei dirigenti. I risultati di questo sondaggio indicano in modo evidente che un evento di grande impatto a livello di sicurezza come un attacco ransomware aumenta la probabilità di rimozione dal ruolo nelle organizzazioni che ne cadono vittima.

LICENZIAMENTI DEL PERSONALE

I dirigenti non sono le uniche persone che corrono rischi in seguito ad attacchi ransomware; personale di ogni livello può essere vittima delle operazioni di ripristino della stabilità in seguito a un attacco ransomware. Nel 2020, la società produttrice di acciaio Evraz ha annunciato notevoli riduzioni di personale di produzione e in seguito a un attacco ransomware, con un grave danno all'operatività della compagnia nell'America del nord.

Questa ultima ricerca mette in evidenza questa triste conseguenza degli attacchi ransomware, con quasi un terzo (29%) delle risposte che hanno indicato che l'organizzazione è stata costretta a rimuovere alcuni lavoratori in seguito a un attacco ransomware. Le risposte relative a Singapore (13%), Germania (19%) ed Emirati Arabi Uniti (29%) indicano valori medi o al di sotto della media, mentre Regno Unito (31%), Spagna (31%) e Stati Uniti (33%) valori leggermente più elevati della media. La Francia è la nazione con valori più elevati, con 39% delle organizzazioni che sono state costrette e eliminare alcuni lavoratori a causa di attacchi ransomware.

In base alle analisi in funzione del settore, le risposte del settore governativo non hanno indicato perdite di lavoro, mentre i settori automobilistico, vendite e legale hanno avuto molti più casi di licenziamenti in seguito ad attacchi ransomware. L'informazione chiave è che il settore pubblico può essere maggiormente al sicuro per quanto riguarda gli effetti sulla forza lavoro di un attacco ransomware, mentre il settore privato presenta il rischio di una riduzione della forza lavoro come risultato di un attacco ransomware riuscito, in ogni settore:

SETTORE	PERCENTUALE DI CASI CON LICENZIAMENTI
Legale	50%
Vendita	48%
Automobilistico	42%
Manifattura	29%
Tecnologia	29%
Sanità	24%
Servizi finanziari	23%
Governativo	0%

Percentuale di risposte che indicano licenziamenti in seguito a un attacco ransomware, per settore

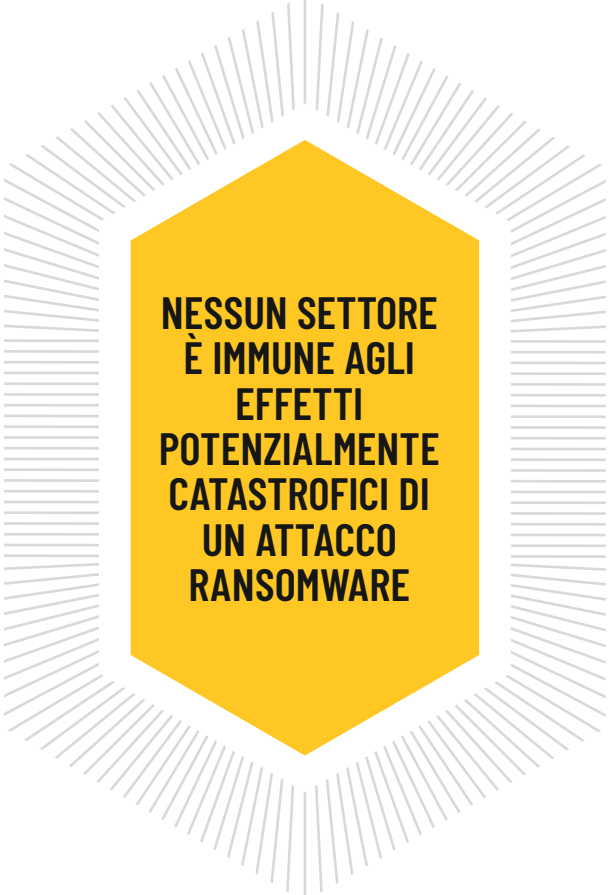
PERCENTUALE DI CHIUSURE DELL'ATTIVITÀ

CHIUSURA FORZATA DELL'ATTIVITÀ

Infine abbiamo il tipo di effetto che un'organizzazione può subire a causa di un attacco ransomware: la chiusura dell'attività. La società di telemarketing The Heritage Company ha informato i suoi 300 dipendenti dell'imminente chiusura e della necessità per loro di trovare nuove opportunità lavorative a causa di un attacco ransomware che aveva colpito i loro server di produzione per un periodo steso; l'annuncio è stato inviato pochi giorni prima del periodo natalizio.

Nonostante la chiusura di un'attività a causa di un attacco ransomware possa sembrare un caso estremo, si tratta di un rischio più concreto di quanto i responsabili delle attività possano credere. Più di un quarto delle risposte (25%) hanno indicato che un attacco ransomware aveva causato la chiusura dell'organizzazione per un periodo. La tabella di seguito mostra una suddivisione per regione:

REGIONE	PERCENTUALE DI CHIUSURE DELL'ATTIVITÀ
Emirati Arabi Uniti	42%
Regno Unito	34%
Stati Uniti	31%
Francia	22%
Germania	21%
Singapore	20%
Spagna	5%



L'analisi dei risultati del sondaggio in funzione del numero di dipendenti ha mostrato risultati misti. Le organizzazioni con 250-500 dipendenti hanno indicato per quasi un terzo (27%) l'impatto più grande, mentre i settori automobilistico e di vendita sono stati quelli più colpiti, rispettivamente al 42% e 33%. Questi risultati dimostrano in modo evidente che nessun settore è immune agli effetti potenzialmente catastrofici di un attacco ransomware.

LE ASSICURAZIONI INFORMATICHE COPRONO I COSTI?

In base agli studi realizzati da uno dei più grandi fornitori del Nord America, gli attacchi ransomware sono stati la causa di quasi metà delle richieste di risarcimento cibernetico (41%) nei primi sei mesi del 2020. Ma un'assicurazione informatica copre sempre l'ampia gamma di costi associati a un attacco ransomware? La risposta non è sempre sì.

La città di New Orleans è stata vittima di un attacco ransomware per una perdita stimata a oltre 7 milioni di dollari. Nonostante le regole dell'assicurazione prevedessero una copertura dei danni degli attacchi ransomware, la città è riuscita a recuperare solo 3 milioni di dollari delle perdite dalla compagnia assicuratrice.

Questa situazione è presente anche nei risultati della nostra ricerca, che ha il 54% delle risposte che hanno indicato che la loro organizzazione ha acquistato una polizza di assicurazione informatica con una copertura contro gli attacchi ransomware negli ultimi 24 mesi e il 21% che hanno indicato che la loro organizzazione ha stipulato una polizza di assicurazione informatica senza l'inclusione dei danni causati da attacchi ransomware.

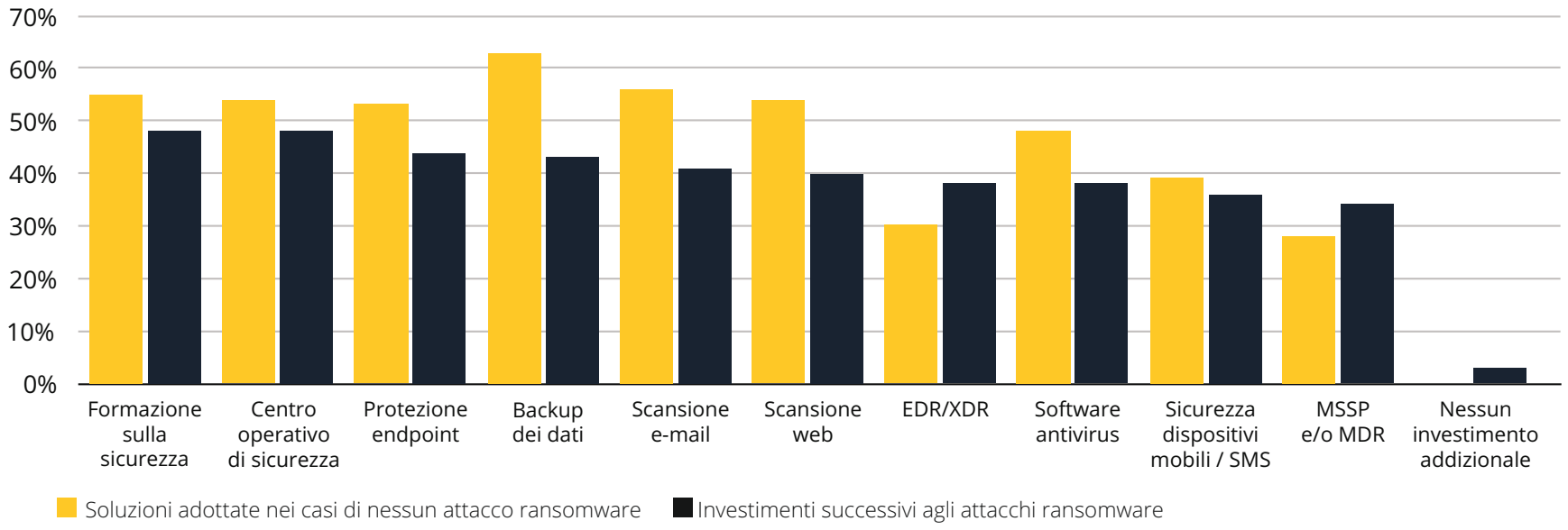
Tra le organizzazioni con assicurazione informatica che hanno subito attacchi ransomware, il 42% ha dichiarato che la compagnia assicurativa ha coperto solo una parte dei danni. Questi risultati suggeriscono un impatto molto elevato per coloro che non erano dotati di un'assicurazione appropriata e un rischio di impatto notevole per le attività che ne erano provviste. La morale è che è necessario verificare che la propria assicurazione informatica offra una valida copertura.

INVESTIMENTI SULLA SICUREZZA DOPO GLI ATTACCHI RANSOMWARE

Esiste da molto tempo un paradosso relativo alla sicurezza, per cui la dimostrazione del successo è legata all'assenza di eventi: se non si presentano particolari problemi, è davvero necessario continuare a investire allo stesso livello nelle soluzioni e nelle procedure di sicurezza? Sfortunatamente, è spesso necessario un evento grave per generare maggiori investimenti verso i programmi, gli strumenti e il personale dedicato alla sicurezza.

Abbiamo chiesto agli intervistati che hanno dichiarato che l loro organizzazione era stata vittima di un attacco ransomware negli ultimi 24 mesi di condividere le soluzioni di sicurezza su cui avevano investito dopo l'attacco, per dare una maggiore protezione alla loro rete in caso di tentativi di attacco futuri.

Il grafico in basso confronta i nuovi investimenti con le soluzioni adottate in precedenza dalle organizzazioni i cui intervistati hanno indicato di non aver subito un attacco ransomware negli ultimi 24 mesi. Questo grafico mostra un confronto tra le soluzioni adottate che potrebbero aver protetto le organizzazioni dagli attacchi ransomware e gli investimenti compiuti



LE 5 PRINCIPALI SOLUZIONI ADOTTATE DOPO UN ATTACCO RANSOMWARE

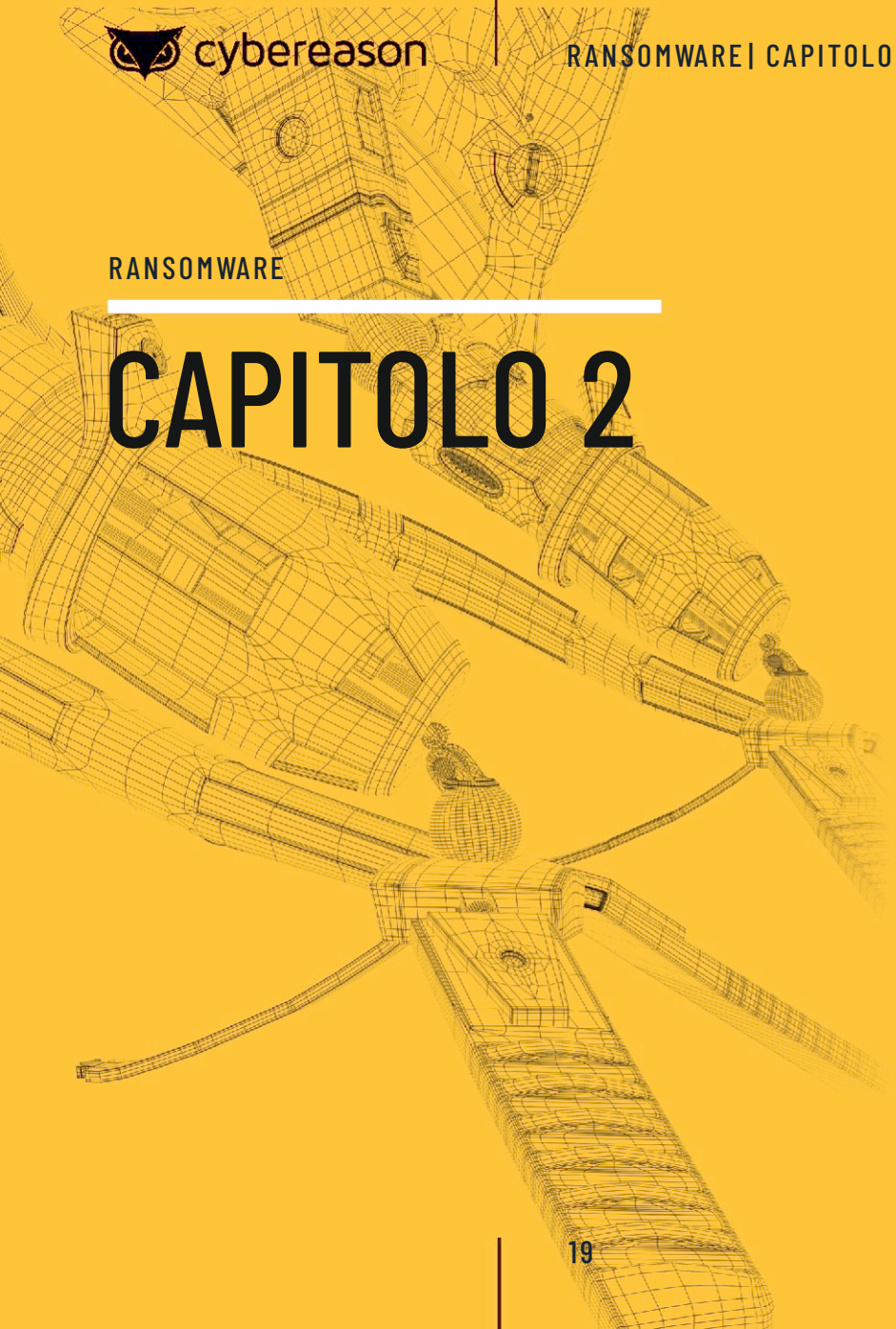
SCANSIONE E-MAIL
41%

BACKUP DEI DATI
43%

PROTEZIONE DEGLI ENDPOINT
44%

CENTRO OPERATIVO DI SICUREZZA
48%

FORMAZIONE SULLA SICUREZZA
48%



RANSOMWARE

CAPITOLO 2

RANSOMWARE: CHI È A RISCHIO? TUTTI

Uno degli insegnamenti principali di questa ricerca è al tempo stesso preoccupante e rassicurante. Alla domanda "Quanto è grande la vostra preoccupazione sul rischio di subire un attacco ransomware?" più di quattro intervistati su cinque (81%) hanno risposto di essere notevolmente preoccupati per i rischi di un attacco ransomware. Questo risultato è preoccupante per due motivi. Mostra il livello a cui la minaccia ransomware è dilagante e l'urgenza della sua gestione. Se lavoriamo nel mondo della sicurezza informatica e non abbiamo alcuna preoccupazione nei confronti degli attacchi ransomware, vuol dire che non stiamo ponendo la giusta attenzione.

Quasi il
75%
degli intervistati hanno dichiarato di essere in possesso di un piano specifico per gestire in modo efficace un attacco ransomware

La realtà è che la grande maggioranza delle persone riconoscono il rischio degli attacchi ransomware. I nostri dati mostrano tuttavia una certa disconnessione o una falsa sensazione di sicurezza quando si tratta di quanto preparate siano in realtà le organizzazioni contro gli attacchi ransomware. Quasi il 75% degli intervistati ha dichiarato di essere in possesso di un piano specifico per gestire in modo efficace un attacco ransomware e poco meno del 60% ritiene di possedere le persone giuste per risolvere il problema. Se le organizzazioni sono in possesso di un piano e delle persone giuste, qual è il motivo della preoccupazione?

Gli Stati Uniti hanno un numero più elevato di persone che ritengono di avere le persone giuste (69%) rispetto a coloro che hanno risposto di essere in possesso di piani o procedure (58%). Questi dati fanno pensare che varie aziende statunitensi abbiano una tale fiducia nei loro membri del dipartimento IT da RITENERE che ciò sia sufficiente per proteggerli anche senza procedure definite.

Nel frattempo, gli Stati Uniti continuano a subire i danni degli attacchi ransomware di maggiore rilievo e una ricerca come questa dovrebbe essere in grado di offrire una visione più chiara delle potenziali implicazioni di un attacco ransomware per le organizzazioni. In nazioni come Regno Unito, Germania, Spagna e Francia, tra il 73% e l'87% degli intervistati ha dichiarato di essere in possesso di un piano o di procedure, mentre la percentuale di persone che ha dichiarato di possedere le persone giuste per risolvere il problema è stata tra il 45% e il 66%, in contrasto con i risultati relativi agli Stati Uniti.

UN ATTACCO CON
DOPPIA ESTORSIONE
PRIMA ESFILTRA DATI SENSIBILI E PROPRIETÀ INTELLETTUALE. POI SI HA LA MINACCIA DI DIFFUSIONE O DI VENDITA DEI DATI TRAFUGATI NEL CASO IN CUI NON VENGA PAGATO IL RISCATTO,
RISCHIO DA CUI IL BACKUP DEI DATI NON PUÒ PROTEGGERE.

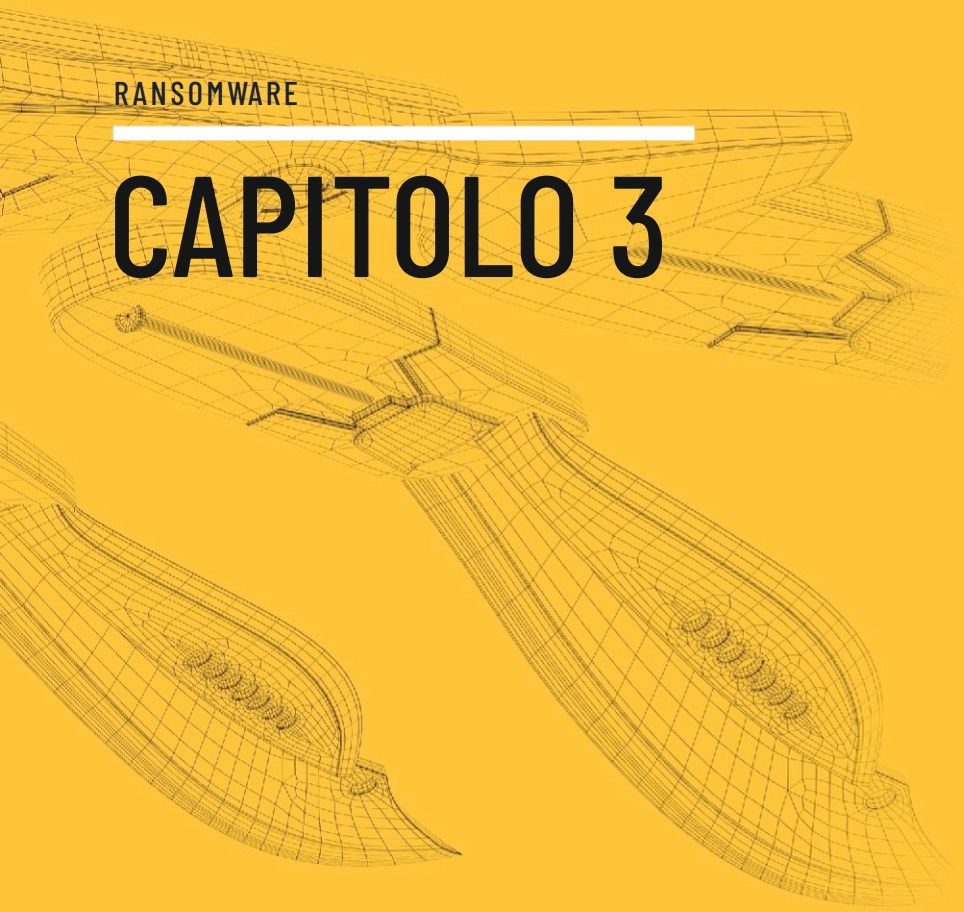
Nonostante la grande percentuale di organizzazioni che hanno indicato di essere in possesso di procedure e di avere le persone giuste per difendersi dagli attacchi ransomware, l'ultimo anno è stato insolitamente arduo. I criminali informatici hanno colto l'opportunità di guadagno dal caos e dalla confusione che hanno dovuto affrontare le aziende di tutto il mondo a causa della pandemia di COVID-19, con molte aziende che hanno dovuto convertirsi da un giorno all'altro a una struttura completamente remota di lavoro da casa. Ciò ha creato notevoli difficoltà ai dipartimenti di IT, espandendo quindi la superficie di attacco e rendendo più difficile la visibilità. Gli attacchi ransomware permettono ai criminali di continuare a compromettere i sistemi e a ricevere i riscatti rimanendo al sicuro nelle loro case, in quarantena e nl rispetto delle procedure di distanziamento sociale.

Il volume complessivo di questo tipo di attacco sembra essere in diminuzione, ma gli attacchi diventano più sofisticati e con un impatto più devastante. Le aziende hanno migliorato i loro processi di backup e le tecnologie di risposta per contrastare l'aumento degli attacchi In caso cadano vittima, possono semplicemente ignorare la richiesta di riscatto e ripristinare i sistemi grazie ai backup, riprendendo le operazioni normali. I criminali si sono però adattati e hanno creato gli attacchi malware di doppia estorsione. Invece di crittografare semplicemente i dati, un primo attacco esfiltra dati sensibili e proprietà intellettuale. Poi si ha la minaccia di diffusone o di vendita dei dati trafugati nel caso in cui non venga pagato il riscatto, rischio da cui il backup dei dati non può proteggere.

Allo stesso tempo, le cifre richieste sono salite alle stelle. Nel 2018, la richiesta di riscatto media era stimata sui 6.000 dollari. Questa cifra risulta essere moltiplicata per 14 nel 2019, per un valore di 84.000 dollari, con un raddoppio nel 2020, per un valore di 178.000. Abbiamo visto alcuni attacchi nel 2021 che sovrastano queste cifre. Colonial Pipeline ha dichiarato di aver pagato un riscatto di 5 milioni di dollari a DarkSide, mentre sia Acer che Apple hanno ricevuto richieste di riscatti di 50 milioni di dollari.

La collaborazione tra i settori pubblico e privato è un passo verso la corrispondenza tra la percezione di essere sufficientemente preparati e la realtà. Il governo degli Stati Uniti ha creato una task force contro le attività di ransomware, a cui partecipa anche Cybereason. La task force è composta da rappresentanti di varie agenzie governative e di organizzazioni dei settori pubblico e privato, con l'obiettivo di collaborare per gestire la crisi degli attacchi ransomware.

LE AREE DI LAVORO DELLA TASK FORCE CONTRO IL RANSOMWARE SONO TRE: PREPARAZIONE, DISTURBO E RISPOSTA. IL RANSOMWARE È UN PROBLEMA GLOBALE E INTERESSA TUTTI, QUINDI È IMPORTANTE COLLABORARE PER LIMITARE LE OPERAZIONI DI RANSOMWARE E PRENDERE UN VANTAGGIO RISPETTO ALL'AVVERSARIO.



RANSOMWARE

CAPITOLO 3

NELLA MAGGIOR PARTE DEI CASI NON CONVIENE PAGARE

Uno dei problemi principali che le organizzazioni devono affrontare quando subiscono un attacco ransomware è il dubbio se pagare o meno. L'interesse personale è sicuramente un fattore importante, ma ci sono molti aspetti da prendere in considerazione e anche la scelta di pagare comporta dei rischi.

Conviene all'organizzazione assumere uno specialista per negoziare i termini del pagamento? I criminali onoreranno la loro parte dell'accordo e restituiranno l'accesso ai dati? E se i dati sono stati corrotti nel processo? E se i criminali sono in un paese soggetto a sanzioni che rendono il pagamento una violazione delle leggi? Il pagamento aumenta la probabilità di subire un altro attacco ransomware? Quali son i rischi per l'organizzazione in caso di mancato pagamento?

Per qualsiasi organizzazione, si tratta di una situazione difficile in cui trovarsi e non ci sono "procedure consigliate", dato che ogni infiltrazione, gruppo di attacco, organizzazione vittima, insieme di dati a rischio e terze parti potenzialmente interessate rendono ogni situazione diversa dalle altre. Nella scelta se pagare o meno si hanno vari fattori da valutare, quindi la maggior parte degli attacchi ransomware deve essere analizzata singolarmente.

DOPPIA ESTORSIONE

Con la doppia estorsione, i criminali prima esfiltrano i dati sensibili e minacciano di divulgarli in caso di mancato pagamento del riscatto. Ciò significa che la vittima si ritrova nella situazione di dover pagare il riscatto anche nel caso in cui abbia utilizzato un sistema di backup per precauzione.

Ultimamente, alcuni criminali hanno adottato l'approccio della doppia estorsione per aumentare la probabilità di ricevere il pagamento del riscatto. Per esempio, nell'aprile del 2021 è stato segnalato che il gruppo di ransomware DarkSide stava esercitando una maggiore pressione sulle vittime minacciando di divulgare informazioni riservate basate sui dati esfiltrati agli operatori di borsa in modo che potessero sfruttarle nei confronti delle società quotate in caso di rifiuto di pagamento del riscatto.

QUASI
METÀ DEGLI INTERVISTATI (46%) HA DICHIARATO
DI AVER RIOTTENUTO ACCESSO AI PROPRI DATI DOPO IL PAGAMENTO, MA CHE
ALCUNI O TUTTI
I DATI ERANO CORROTTI.

E SE SI DECIDE DI PAGARE?

Con rischi così alti, conviene pagare? Tra coloro che hanno dichiarato che le loro organizzazioni avevano pagato il riscatto in seguito all'attacco, quasi metà degli intervistati (46%) ha dichiarato di aver riottenuto accesso ai propri dati dopo il pagamento, ma che alcuni o tutti i dati erano corrotti.

Altre organizzazioni sono state più fortunate. Più della metà (51%) ha dichiarato di aver riottenuto accesso ai dati crittografati senza alcuna perdita. Solo il 3% ha dichiarato di non essere riuscita a riottenere accesso a nessuno dei dati crittografati.

Il pagamento del riscatto rende l'organizzazione più vulnerabile ad attacchi ransomware successivi? Può dipendere dalle azioni compiute per comprendere e ridurre le vulnerabilità che hanno permesso al primo attacco di andare a segno.

Un'organizzazione anonima che è stata vittima di un attacco ransomware e ha deciso di pagare una richiesta che si ritiene essere di milioni di dollari è stata evidentemente vittima di un secondo attacco ransomware da parte degli stessi criminali due settimane dopo perché non ha preso le contromisure necessarie per comprendere come era avvenuto il primo attacco e per costruire difese addizionali per respingere gli attacchi successivi.

Questa ricerca ha evidenziato che, tra le organizzazioni che hanno deciso di pagare un riscatto, l'80% ne ha subito un secondo. Tra coloro che sono stati vittima di un secondo attacco, quasi la metà (46%) ha dichiarato di ritenere di essere stata colpita dalle stesse persone, mentre solo il 34% ha dichiarato di credere che il secondo attacco fosse opera di un diverso gruppo di persone.

LA DIFESA CONTRO IL RANSOMWARE

Una volta che un'organizzazione viene compromessa da ransomware, non ci sono valide opzioni. Se il riscatto non viene pagato, l'attività può essere costretta a fermarsi per giorni, fino al ripristino dei sistemi e dei dati di backup. Nel caso di un attacco con doppia estorsione, non pagare il riscatto porta ad accettare il rischio che informazioni riservate o proprietà intellettuale vengano divulgate o vendute al maggiore offerente sul mercato nero. Il danno economico della perdita di operatività e di produttività e il costo delle attività di ripristino possono superare la somma richiesta.

L'alternativa è il pagamento del riscatto, che ha però i suoi rischi e le sue conseguenze. Molte organizzazioni che hanno pagato il riscatto sono state in grado di riottenere accesso ai propri dati, ma alcuni o tutti sono risultati corrotti. Lo strumento di decodifica fornito dagli autori dell'attacco è spesso malfunzionante o lento e obbliga le aziende a effettuare il ripristino partendo dai propri backup nonostante il pagamento del riscatto. Inoltre, pur pagando il riscatto, non c'è garanzia che i propri dati non vengano venduti.

3 CONSIGLI PER DIFENDERSI DAL RANSOMWARE

1 **Segui le procedure consigliate per la sicurezza** gestione rapida delle patch, backup dei dati in un luogo diverso, formazione del personale sulla sicurezza

2 **Utilizza sistemi di prevenzione multi-livello** su tutti gli elementi di rete dell'azienda

3 **Adotta soluzioni estese di rilevazione e risposta** in tutto l'ambiente per avere la giusta visibilità allo scopo di bloccare gli attacchi ransomware avanzati prima che possano farsi strada nella rete

L'unica opzione valida è non essere colpiti da ransomware neanche una prima volta. Gli strumenti di sicurezza informatica tradizionali e le soluzioni di endpoint di nuova generazione sono inadeguati perché puntano sul riconoscere i metodi di attacco identificati in precedenza e su indicatori di compromissione.

Le organizzazioni hanno bisogno di sicurezza cibernetica con una visibilità completa dell'ambiente e la capacità di analizzare indicatori di comportamento in aggiunta agli indicatori di compromissione. Gli indicatori di comportamento forniscono indizi su ciò che sta avvenendo al momento o su ciò che potrebbe avvenire nell'immediato futuro, mentre gli indicatori di compromissione si basano sulla reazione dopo che un'azione malevola è già avvenuta.

Poter osservare l'intera operazione malevola (chiamata anche Malop) è importante, così come lo è anche comprendere l'ambito dell'attacco e capire le relazioni tra le azioni e i comportamenti che potrebbero sembrare innocui se osservati singolarmente. La Malop fornisce una comprensione più completa di ciò che sta avvenendo e offre la visibilità, il contesto e le informazioni necessarie per individuare e prevenire gli attacchi ransomware prima che creino danni.

Conclusioni e insegnamenti

Il messaggio è molto semplice: l'effetto di un attacco ransomware andato a segno nei confronti di un'organizzazione è significativo qualsiasi siano la regione, il settore e le dimensioni dell'azienda. Gli attacchi ransomware possono generare una serie di effetti ad ampio spettro in grado di mettere in pericolo un'organizzazione fino alle sue fondamenta. Il risultato è spesso un danno alla reputazione, la perdita di posti di lavoro, la perdita di profitti e, nel caso peggiore, la chiusura dell'attività.

Una valida gestione del rischio richiede che l'organizzazione abbia un piano di emergenza per la gestione delle conseguenze di un attacco ransomware su tutti i livelli; la strategia più cauta per evitare notevoli perdite per l'organizzazione consiste in un forte investimento nelle strategie di prevenzione. Anche con solidi sistemi di difesa in grado di bloccare la maggioranza degli attacchi ransomware, alcuni riusciranno inevitabilmente a superare le barriere, quindi le organizzazioni devono investire anche in sistemi di individuazione e risposta.

Le soluzioni di backup dei dati sono caldamente consigliate, in quanto sono in grado di semplificare le operazioni di ripristino, ma le organizzazioni devono rendersi conto che i criminali utilizzano strategie per rendere l'uso dei backup tutt'altro che semplici in alcune circostanze. In modo simile, il giusto livello di copertura di un'assicurazione informatica può significare la differenza tra il recupero totale delle perdite causate da un attacco ransomware e il recupero di solo una porzione dei costi o di nessuno.

Le organizzazioni devono assicurarsi di avere il personale giusto, con le conoscenze adeguate e le soluzioni di sicurezza adatte per bloccare gli attacchi ransomware con appropriate soluzioni e controlli o, come minimo, vengano individuate all'inizio della loro attività dannosa e limitate prima che l'attacco cresca fino al punto da causare seri danni all'intera attività.

METODOLOGIA DEL SONDAGGIO

Il sondaggio è stato realizzato da Censuswide nell'aprile del 2021 per conto di Cybereason. Vi hanno preso parte 1.263 professionisti del settore della sicurezza cibernetica in Stati Uniti (24%), Regno Unito (24%), Spagna (12%), Germania (12%), Francia (12%), Emirati Arabi Uniti (8%) e Singapore (8%). Tra gli intervistati si ha una diversità di esperienza lavorativa sia all'interno dell'azienda che nel ruolo attuale.

Il campione considerato nel sondaggio include risposte da una serie di settori. Il settore tecnologico è il più rappresentato, con un 44%, seguito dal settore manifatturiero (16%) e dal settore finanziario (11%). I rimanenti intervistati fanno parte di aziende dei settori sanitario, automobilistico, governativo, legale e altri.

Sono inoltre rappresentate aziende di diverse dimensioni. Il gruppo più ampio ha oltre 500 dipendenti (30%) e altre risposte sono giunte da aziende con 250-500 dipendenti (23%), 100-249 dipendenti (25%), 50-99 dipendenti (11%), 10-49 dipendenti (10%) e meno di 10 dipendenti (1%).

CYBEREASON

Cybereason è tra i leader nel mercato nella cybersecurity al giorno d'oggi e fornisce una protezione all'avanguardia dagli attacchi grazie alla sua copertura globale dalle singole postazioni all'intera azienda e ovunque si svolga la battaglia. La piattaforma di difesa di Cybereason combina le più avanzate tecniche di individuazione e risposta (EDR e XDR), gli antivirus di nuova generazione (NGAV) e una ricerca delle minacce proattiva per offrire un'analisi nel contesto di ogni elemento di Malop (operazione malevola). Il risultato è che i sistemi difesa sono in grado di porre fine agli attacchi cibernetici dalla singola postazione a ogni elemento. Cybereason è una società internazionale di proprietà privata con sede principale a Boston e clienti in oltre 30 paesi.

Scopri di più su **www.cybereason.com**