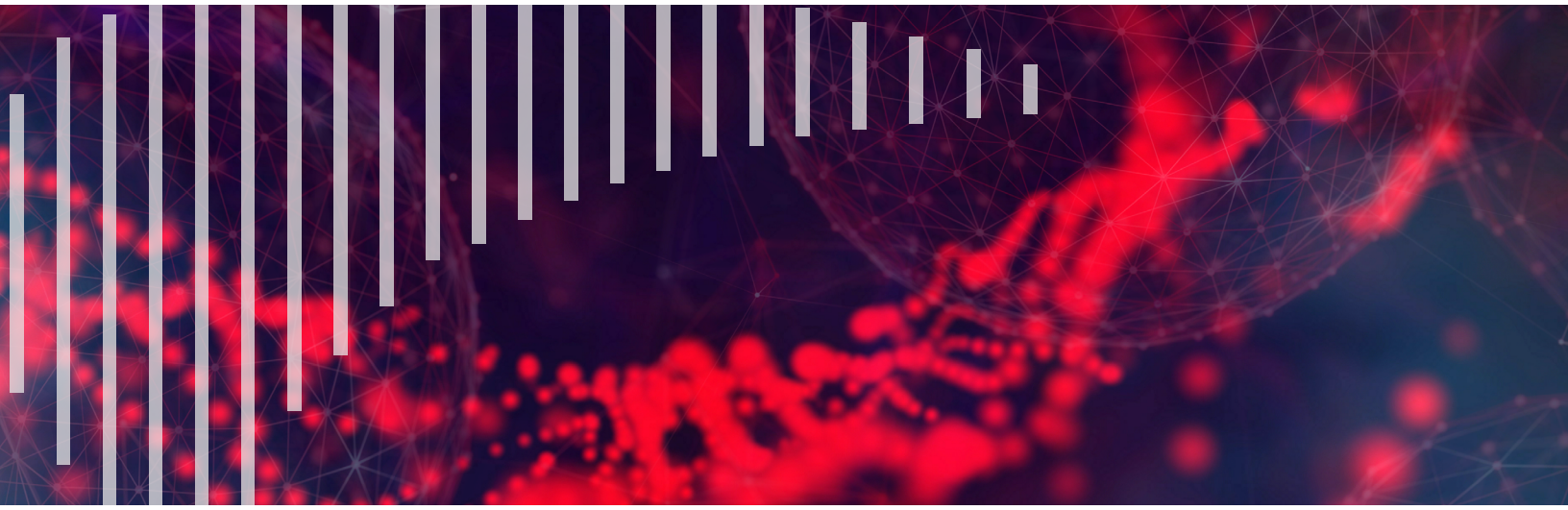


EXECUTIVE BRIEF

Il costo reale del ransomware

Introduzione

Con attacchi sempre più sofisticati, budget di cybersecurity stagnanti e scarsità di personale, è importante che le aziende comprendano quali conseguenze concrete può avere un attacco informatico, in modo da allocare le giuste risorse e dare priorità alle strategie di prevenzione più adatte.

Purtroppo, nel campo della sicurezza informatica è spesso difficile quantificare il rischio, e alcuni dei metodi più comuni che utilizziamo per valutare il rischio non sono in grado di rilevare gli effetti di alcuni attacchi, in particolare quelli ransomware.

Quantificare il rischio

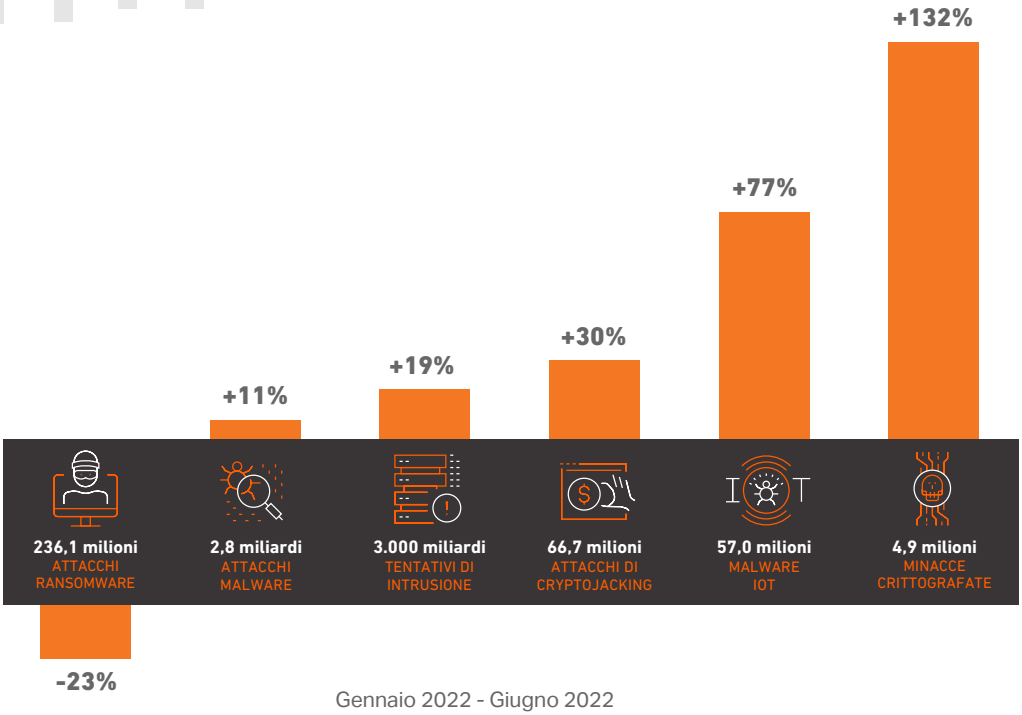
La maggior parte dei professionisti di cybersecurity conosce la matrice a "mappa di calore", comunemente utilizzata per valutare il rischio di sicurezza informatica. Su un asse, la probabilità procede da "raro", "remoto" o "molto improbabile" a "quasi certo", "molto probabile" o "frequente". Sull'altro asse, l'impatto degli attacchi viene classificato con termini come "trascurabile" e "insignificante" da un lato e "catastrofico" o "grave" dall'altro. Per classificare il potenziale rischio basta trovare il punto d'intersezione degli assi a seconda del tipo di incidente previsto.

Queste matrici sono uno strumento utile, ma non possono essere l'unica base per prendere decisioni sulla sicurezza informatica. Forniscono un contesto prezioso, ma non sono in grado di riprodurre in modo adeguato la portata dei rischi posti da attacchi come il ransomware.

Quanto è rischioso il ransomware?

Nell'ultimo rapporto sul costo degli incidenti informatici di CISA, il ransomware era classificato come la seconda causa di perdite più comune per le PMI, a notevole distanza dall'ingegneria sociale. Tra le grandi aziende intervistate è stato registrato un unico caso di ransomware, rispetto ai 18 per "malware/virus" e ai 20 casi nella categoria "hacker".

Probabilità	TRASCURABILE	MINIMO	MODERATO	SIGNIFICATIVO	GRAVE
	Impatto				
MOLTO PROBABILE	Medio-basso	Medio	Medio-alto	Alto	Alto
PROBABILE	Basso	Medio-basso	Medio	Medio-alto	Alto
POSSIBILE	Basso	Medio-basso	Medio	Medio-alto	Medio-alto
IMPROBABILE	Basso	Medio-basso	Medio-basso	Medio	Medio-alto
MOLTO IMPROBABILE	Basso	Basso	Medio-basso	Medio	Medio



Gennaio 2022 - Giugno 2022
Fonte: Aggiornamento semestrale del Rapporto SonicWall sul Cybercrime

Recentemente, IBM ha rivelato che il 28% delle aziende prese in esame è stata vittima di un attacco ransomware o "distruttivo", rispetto all'83% che ha subito più di una violazione di dati. In effetti il ransomware rappresentava solo l'11% degli incidenti segnalati, rispetto al 21% per errori umani e al 24% per errori informatici, risultando così la categoria più bassa dopo la voce "varie".

I dati più recenti di SonicWall mostrano un calo del ransomware di circa un quarto nel primo semestre del 2022, con una riduzione del 42% in Nord America, mentre tutti gli altri tipi di minacce hanno registrato un aumento.

Supponendo che l'impatto finanziario di una minaccia sia proporzionale alla sua gravità, i dati sembrano suggerire che il ransomware non è un problema serio. Secondo l'ultimo rapporto dell'Internet Crime Complaint Center (IC3), le violazioni informatiche più costose nel 2021 sono stati gli attacchi BEC/EAC, che hanno causato perdite per 2.395.953.296 dollari, superando ampiamente i 49.207.908 dollari dovuti al ransomware.

Sulla base di queste statistiche, cioè le stesse generalmente utilizzate per le matrici di rischio, sarebbe facile classificare il ransomware come una minaccia di livello "medio" e allentare le misure di prevenzione del ransomware. Ma questo potrebbe rivelarsi un errore molto costoso.

Una visione più completa del rischio ransomware

Sebbene i dati storici siano uno strumento decisamente prezioso, i professionisti della sicurezza devono assicurarsi di analizzare le statistiche del ransomware nel giusto contesto. Ad esempio, i dati di SonicWall e altri mostrano che nel 2022 il ransomware è diminuito rispetto al picco del 2021, ma il suo volume nel 2022 è stato comunque il secondo più alto degli ultimi cinque anni.

Anche se i vendor di cybersecurity hanno un'idea piuttosto precisa di quanto ransomware passi attraverso le loro soluzioni, non significa necessariamente che tutti questi incidenti vengano segnalati.

Esiste quindi il timore che il volume reale di ransomware sia sottostimato. In un'audizione alla Commissione giudiziaria del Senato degli Stati Uniti, il vice procuratore generale Richard Downing ha dichiarato che la sua agenzia ritiene che "solo un quarto delle intrusioni ransomware venga effettivamente segnalato".

Questa preoccupazione non si limita agli Stati Uniti. Un rapporto dell'NCSC pubblicato nel novembre 2022 segnalava che in Europa non è possibile valutare con precisione l'impatto del ransomware. Secondo il rapporto, "il numero reale di attacchi ransomware compiuti ogni anno nel Regno Unito è molto più elevato [rispetto a quanto dichiarato], dato che le aziende spesso non segnalano la compromissione dei loro sistemi".

Il numero di incidenti non è tuttavia l'unico aspetto sottovalutato. A causa della complessità di questi attacchi, gran parte dei dati esistenti sul ransomware mostra un quadro incompleto dei costi associati agli attacchi segnalati.

Ad esempio, i 49.207.908 dollari di perdite totali dovute al ransomware secondo l'IC3 sembrano una cifra quasi incoraggiante rispetto alle perdite complessive derivanti da altri tipi di minacce. Ma una nota a margine del rapporto spiega che le perdite stimate derivanti dal ransomware "non includono perdite stimate di opportunità commerciali, tempo, retribuzioni, file, apparecchiature o misure correttive di terze parti".

Si tratta di un'omissione significativa, dato che l'importo del riscatto rappresenta solo il 15% circa del costo totale di un attacco ransomware.

Allo stesso modo, IBM ha rilevato che il 28% delle aziende ha subito un attacco ransomware – una cifra inferiore rispetto ad altri tipi di minacce –, ma il costo di un attacco ransomware era superiore alla media globale delle violazioni di dati (4,54 milioni di dollari rispetto a 4,35 milioni di dollari). E questo senza contare i soldi spesi per il riscatto, che in media si aggira intorno ai 2,2 milioni di dollari.

Ma anche tenendo conto di questi aspetti, non abbiamo ancora un quadro completo del rischio associato al ransomware. Oltre al riscatto pagato e alle spese che la maggior parte delle vittime di ransomware deve sostenere, come perdita di operatività aziendale, retribuzioni, file, apparecchiature e misure correttive di terze parti, ci sono diverse altre variabili che possono trasformare un qualsiasi attacco ransomware da "grave" a "catastrofico".

Qual è la cosa peggiore che può accadere?

Anche se comunemente parliamo di "attacchi ransomware", il ransomware non è tanto un incidente isolato, quanto una serie di potenziali reazioni a catena. Le vittime più "fortunate" ottengono una chiave di decrittazione valida dopo aver pagato il riscatto, oppure riescono a ripristinare velocemente i sistemi utilizzando i backup attuali e intatti, il tutto senza ulteriori conseguenze. Purtroppo questa prassi è sempre meno probabile, dato che le bande di ransomware diventano sempre più creative e spietate.

Per una valutazione completa del rischio è necessario considerare anche altri problemi che insorgono dopo un attacco ransomware, come ad esempio:

Codici di decrittazione errati/incompleti
Nonostante le rassicurazioni degli autori del ransomware, anche pagando un riscatto non si ha la garanzia che i file vengano poi decrittografati. Non è affatto raro che la chiave di decrittografia ricevuta a caro prezzo non consenta di decifrare completamente i dati … o non funzioni affatto. Secondo un sondaggio condotto dalla società di ricerca e marketing CyberEdge Group, quasi 1 su 5 vittime di ransomware ha pagato il riscatto e ha comunque perso tutti i suoi dati per sempre. E dato che i cybercriminali non operano esattamente secondo il principio "soddisfatti o rimborsati", queste aziende hanno perso l'importo totale del riscatto e il costo necessario per un ripristino completo.

Tempi di inattività
Dopo un attacco ransomware, le aziende hanno bisogno di quasi tre settimane di fermo per riprendere il lavoro. Questo periodo di inattività può avere un impatto significativo sui guadagni: negli Stati Uniti, il costo economico del ransomware è stato di oltre 159 miliardi di dollari solo in tempi di inattività.

Doppia e tripla estorsione
A volte, un attacco ransomware è molto più di un semplice attacco ransomware. Quasi due terzi degli attacchi ransomware attuali prevede anche operazioni di esfiltrazione dei dati, con un aumento del 106% rispetto a soli cinque anni fa. Sebbene un furto di dati sensibili durante un attacco con doppia estorsione sia già di per sé una catastrofe, molti cybercriminali non si limitano a questo.

Negli ultimi due anni si è verificato un aumento di tecniche a tripla estorsione. In questi attacchi, i cybercriminali non solo minacciano di pubblicare i dati sensibili, ma li filtrano anche per trovare clienti, pazienti, parti interessate e chiunque abbia qualcosa da perdere rendendo pubblici questi dati, e richiedono un ulteriore riscatto.

Attacchi ripetuti
Nonostante le promesse ricevute, pagando un riscatto non si ha la garanzia che i criminali elimineranno effettivamente i dati che hanno già rubato. Il fatto che un'azienda abbia già mostrato la propria disponibilità a pagare la rende un bersaglio ancora più allettante. Secondo ZDNet, circa otto aziende su 10 che hanno pagato le richieste di riscatto sono state attaccate di nuovo, e circa la metà di queste vittime ritiene che il secondo attacco sia stato compiuto dagli stessi criminali del primo.

Cause legali
A causa del tipo di dati che vengono sottratti durante un attacco ransomware, a volte le vittime degli attacchi devono poi affrontare azioni legali intentate da una o più parti interessate. Rackspace, Canon, Epiq Systems, TransLink, US Fertility e Scripps Health sono solo alcune delle aziende che hanno dovuto affrontare azioni legali collettive in seguito a un attacco ransomware.

Danno alla reputazione
Anche le aziende che non vengono portate in tribunale dopo un attacco ransomware devono spesso difendersi dal giudizio dell'opinione pubblica. A differenza dei costi per le indagini forensi e il disaster recovery, le assicurazioni informatiche spesso coprono solo in parte i costi necessari per ripristinare la reputazione aziendale, come ad esempio la pubblicazione di annunci, l'acquisto di servizi di monitoraggio del credito per migliaia (o milioni) di persone colpite e altre attività per riconquistare la fiducia e mantenere in vita il business.

Multe e sanzioni
Se i dati esfiltrati includono determinati tipi di informazioni personali, come dati finanziari e relativi alle carte di credito (PCI, Payment Card Industry), cartelle cliniche e altre informazioni sanitarie riservate (HIPAA), le aziende possono incorrere in sanzioni e multe di grande entità.

Il potere delle misure preventive

Sebbene il rischio del ransomware sia maggiore di quanto molte aziende credano, la buona notizia è che esistono numerose misure per bloccare questi attacchi.

- **Aggiornamento:** quando possibile, automatizzate il monitoraggio e l'enumerazione delle vulnerabilità per le applicazioni e i dispositivi della vostra rete. Applicate le patch tempestivamente e spesso.
- **Upgrade:** tanto più vecchio è un sistema operativo, quanto più malware e altre minacce vengono create per attaccarlo.

Disinstallate tutto il software e l'hardware obsoleto o non più supportato dal produttore.

- **Duplicazione:** tutti i dati importanti devono essere archiviati in un luogo inaccessibile ai cybercriminali. La presenza di backup adeguati e aggiornati semplifica notevolmente il ripristino in caso di attacchi ransomware.
- **Formazione:** il 91% di tutti i cyber attacchi inizia quando un utente apre un'email di phishing. Insegnate ai dipendenti a prestare attenzione ogni volta che ricevono un'email, in particolare i messaggi con un allegato o un link.
- **Verifica:** una volta impostate le procedure di risposta agli incidenti, è necessario verificarle regolarmente. Controllate se il vostro piano di continuità aziendale funziona ed è aggiornato. Determinate quanto tempo occorre per ripristinare un backup (e assicuratevi che i backup vengano aggiornati regolarmente). Verificate che siano presenti controller di dominio isolati tramite air-gap.
- **Salvaguardia:** le misure sopra descritte sono "buone prassi" e non "prassi universali" per un semplice motivo. Se le aziende tralasciano alcune di queste misure, o trovano nuovi metodi per evitarle, avranno bisogno di un'ultima linea di difesa molto efficace. Una piattaforma multilivello avanzata con sicurezza degli endpoint, servizi firewall di nuova generazione, protezione e-mail e accesso mobile sicuro può essere la soluzione ideale per eliminare i punti ciechi e bloccare le minacce note e sconosciute.

Tutte queste informazioni possono aiutare le organizzazioni a prendere decisioni più informate, ma in ultima analisi spetta ad ogni azienda stabilire quale sia il proprio profilo di rischio individuale e la propria tolleranza al rischio. Adottando un approccio proattivo, le aziende possono ridurre il rischio di attacchi e aumentare la loro capacità di reagire e di riprendersi dopo un attacco.

Nota: i dati sulle minacce citati in questo documento provengono dall'aggiornamento di metà anno del Rapporto SonicWall sul Cybercrime.

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL®