SOPHOS

Guida Alle Assicurazioni Informatiche Di Sophos

L'importanza dell'applicazione di controlli informatici efficaci per migliorare le condizioni di assicurazione e ridurre i premi.

Il mercato delle assicurazioni informatiche continua a evolversi e, per rispondere a richieste di indennizzo sempre più ingenti e numerose, i requisiti da soddisfare per stipulare una polizza restano molto severi. Anche se la maggior parte delle organizzazioni ha già una qualche forma di assicurazione informatica, per molte altre i livelli di cybersecurity necessari per soddisfare i requisiti di idoneità sono eccessivamente elevati e le polizze sono troppo complesse. Inoltre, i premi assicurativi continuano ad aumentare.

La disponibilità di assicurazioni informatiche è adeguata, ma le compagnie di assicurazioni sono estremamente selettive e scelgono con estrema attenzione i propri clienti, evitando quelli che presentano maggiori rischi. Investendo in difese informatiche di ottima qualità, le organizzazioni si tutelano dal rischio e con questa strategia possono anche migliorare la propria posizione assicurativa. Dal rendere le polizze più accessibili, all'abbassare i premi e sbloccare limiti di indennizzo più alti, l'adozione di difese informatiche efficaci offre diverse opportunità dal punto di vista assicurativo.

Questa guida descrive il quadro generale del mercato delle assicurazioni informatiche e indica come in molti casi la sicurezza informatica può incidere positivamente sulla stipulazione di una polizza. Inoltre, offre informazioni dettagliate sulle tecnologie e sui servizi offerti da Sophos che possono aiutarti a ridurre il rischio informatico e a migliorare la tua posizione assicurativa.

Whitepaper Sophos. Dicembre 2023

I concetti di base

Perché stipulare una cyberassicurazione?

Le cyberassicurazioni, chiamate anche assicurazioni per il rischio informatico e assicurazioni sulla responsabilità informatica, proteggono dall'impatto che una violazione informatica può avere sull'organizzazione (anche se non proteggono dal crimine stesso). In linea generale, le polizze assicurative per la cybersecurity prevedono quattro vantaggi principali:

1. **Vantaggi finanziari.** L'assicurazione copre i costi in caso di incidente informatico
2. **Vantaggi commerciali.** La copertura cyberassicurativa è un prerequisito sempre più presente nelle condizioni previste per instaurare un rapporto commerciale con molte organizzazioni
3. **Vantaggi operativi.** Se si dovesse verificare un incidente, il team assicurativo offre accesso immediato a esperti in materia, inclusi tecnici IT specializzati in analisi approfondite, consulenti legali sulla privacy e professionisti delle pubbliche relazioni
4. **Tranquillità.** Le cyberassicurazioni rassicurano clienti, partner, fornitori e dipendenti, in quanto dimostrano un certo livello di preparazione e copertura qualora si verificasse un incidente informatico

Motivi delle richieste di indennizzo per le cyberassicurazioni

Sebbene le richieste di indennizzo assicurativo possano derivare da vari tipi di incidenti, secondo il report Cyber Claims Study 2023 di NetDiligence i motivi più frequenti sono:

1. Ransomware
2. Business Email Compromise
3. Hacker
4. Furto di denaro
5. Errori del personale[1]

1 Report Cyber Claims Study 2023 di NetDiligence

Cosa includono le cyberassicurazioni?

Le cyberassicurazioni coprono i costi sostenuti come conseguenza di un attacco informatico.
Anche se le polizze individuali possono variare, di solito includono:

- Costi dovuti all'interruzione delle attività commerciali
- Analisi dettagliate per identificare l'origine dell'attacco
- Richieste di riscatto e specialisti incaricati di negoziare il riscatto
- Costi legati al recupero dell'accesso ai dati o al loro ripristino da backup o altre fonti
- Spese legali
- Servizi di pubbliche relazioni
- Comunicazione ai clienti e/o agli enti normativi
- Servizi di monitoraggio del credito per le persone coinvolte

Quando si cerca una polizza e si mettono a confronto i prezzi, è utile tenere presente che i costi legati all'interruzione di attività (come la perdita di reddito o costi aggiuntivi per le ore lavorative extra a causa dell'attacco) sono inclusi in alcune polizze, ma non in altre.

Se si dovesse verificare un incidente informatico, la compagnia di assicurazioni si attiverà e metterà a disposizione persone esperte che possano assistere nella gestione della situazione. Nel caso di un attacco informatico, tipicamente prenderà i seguenti provvedimenti:

- Nominerà un consulente che possa assistere durante la gestione della richiesta di riscatto e la negoziazione
- Identificherà il modo più economico per ripristinare i dati (pagamento del riscatto, backup, etc.)
- Metterà a disposizione esperti che sappiano come affrontare il problema

La differenza tra copertura di prime e terze parti

Molte polizze includono copertura sia di prime che di terze parti. La copertura di prime parti include i costi diretti associati alla risposta all'attacco, ad esempio le spese legali, le analisi, le comunicazioni ai clienti, le pubbliche relazioni e così via. La copertura di terze parti riguarda principalmente le spese legate alle cause legali.

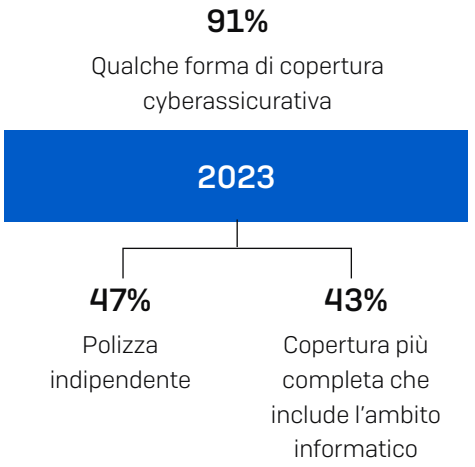
In una polizza ci potrebbero essere dei limiti specifici per la copertura di prime parti e persino per voci specifiche della copertura di prime parti. Per esempio, la copertura di prime parti potrebbe essere limitata a 500.000 $, che includono un limite di 50.000 $ per i costi legati alle pubbliche relazioni.

Le realtà delle cyberassicurazioni

La prevalenza delle cyberassicurazioni

Più che un'eccezione, avere un'assicurazione informatica è ora la regola: ssecondo un sondaggio indipendente commissionato da Sophos, il 91%[2] delle organizzazioni sostiene di aver stipulato una qualche forma di cyberassicurazione nel 2023. Questa percentuale è in netto aumento rispetto all'84% registrato nel 2020[3], ed è in linea con il 92% del 2022. Tra le organizzazioni che hanno dichiarato di aver sottoscritto una polizza assicurativa nel 2023, alcune hanno stipulato polizze indipendenti (47%), mentre altre hanno optato per una copertura più completa che include l'ambito informatico (43%).

Tuttavia, queste statistiche non bastano per comprendere completamente la situazione. Le condizioni possono variare e non tutte le polizze includono il ransomware, che a oggi è il principale motivo di richiesta di indennizzo per le cyberassicurazioni. Quasi un'organizzazione su dieci tra quelle che avevano stipulato un'assicurazione informatica nel 2022 non era assicurata contro il ransomware. Di conseguenza, queste aziende sono rimaste completamente esposte ai costi proibitivi e alle difficoltà estreme implicate nel cercare di riprendere le normali attività dopo questi tipi di attacco.



2 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos
3 La Vera Storia Del Ransomware 2021, Sophos

Aziende Con Una Cyberassicurazione, In Base Al Settore

A livello dei vari settori, dal sondaggio è emerso che quello dell'istruzione (sia scolastica che superiore), ha registrato la più alta percentuale complessiva di assicurazioni informatiche (96%), sebbene queste organizzazioni siano più propense a scegliere coperture più complete che includono l'ambito informatico, piuttosto che polizze indipendenti.

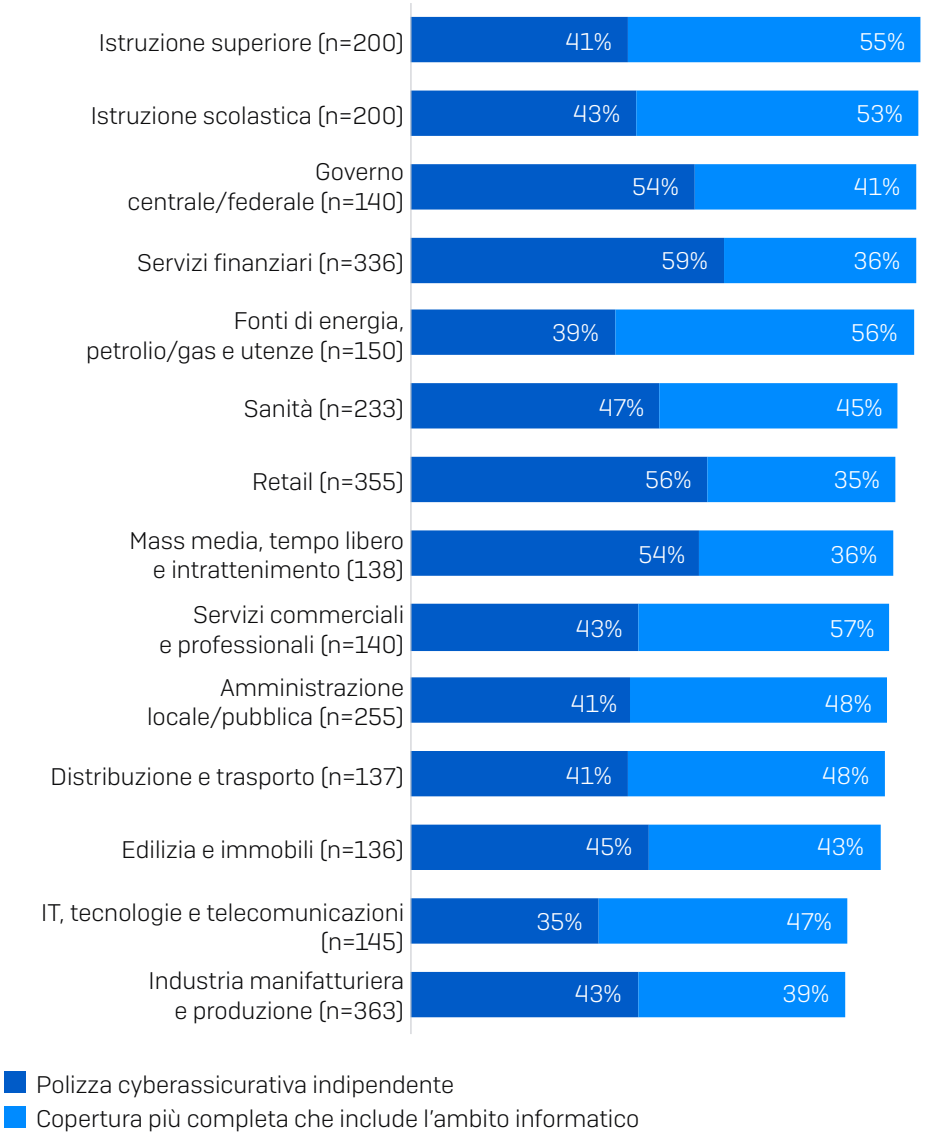
L'alto tasso di adozione è comprensibile visto che, in base al nostro studio La Vera Storia Del Ransomware 2023, in questo settore si è anche riscontrata la percentuale più elevata di attacchi ransomware: l'80% degli istituti di istruzione superiore e il 79% di quelli di istruzione scolastica sostengono infatti di essere stati colpiti dal ransomware durante i 12 mesi precedenti. Il settore dei servizi finanziari ha registrato la maggiore propensione ad adottare una polizza cyberassicurativa indipendente (59%), seguito a distanza ravvicinata dal retail (56%).

Aziende Con Una Cyberassicurazione, In Base Al Fatturato

Probabilmente non sorprende il fatto che il tasso di adozione delle assicurazioni informatiche cresce in maniera direttamente proporzionale al fatturato. Il 96% delle organizzazioni con un volume di affari annuo superiore ai 5 miliardi di USD ha stipulato una forma di cyberassicurazione, mentre per le aziende con fatturato inferiore ai 50 milioni di USD questa statistica scende al 79%.

Le organizzazioni con un fatturato più alto sono anche quelle più propense a scegliere una polizza cyberassicurativa indipendente, rispetto alle aziende con entrate finanziarie meno voluminose: il 58% delle organizzazioni che dichiarano un fatturato annuo superiore ai 5 miliardi di USD ha infatti adottato una polizza indipendente, a differenza delle aziende con entrate inferiori ai 10 milioni di USD, per le quali l'adozione è del 34%. Complessivamente, il nostro studio indica un incremento costante e parallelo al fatturato, nel tasso di stipulazione di polizze indipendenti[4].

Aziende con una cyberassicurazione, in base al settore, 2023



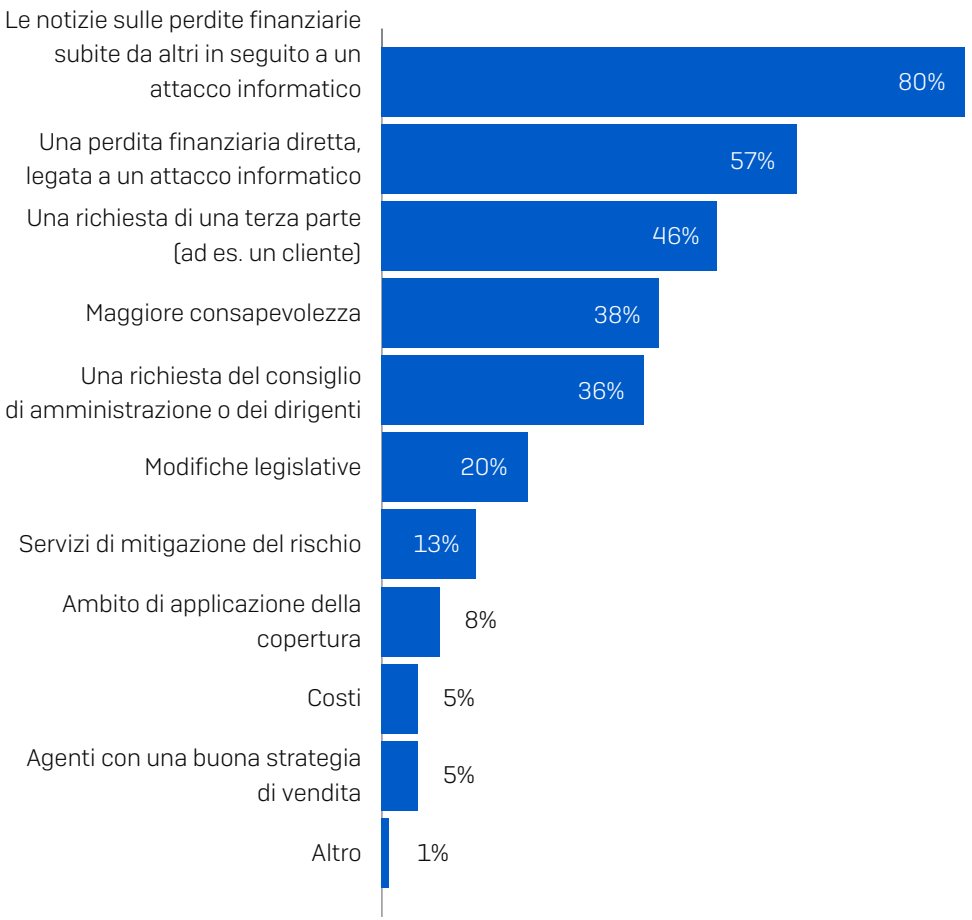
La tua organizzazione ha una polizza cyberassicurativa? Sì, abbiamo una polizza cyberassicurativa indipendente, Sì, abbiamo una copertura più completa che include l'ambito informatico (ad es. come parte di una polizza di responsabilità civile generale). Base di partecipanti indicata nel grafico

4 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos

Gli attacchi informatici contribuiscono all'aumento delle cyberassicurazioni

Un sondaggio condotto da Advisen e PartnerRe tra broker assicurativi e assicuratori in tutto il mondo ha rivelato informazioni interessanti sui principali fattori che influenzano l'aumento delle vendite di nuove cyberassicurazioni, nonché l'incremento dei prezzi delle polizze. Probabilmente non sorprende che i due principali motivi alla base della stipulazione di una cyberassicurazione siano le notizie sulle perdite finanziarie subite da altri in seguito a un attacco informatico e l'aver subito direttamente una perdita finanziaria legata a un attacco informatico. Al terzo posto troviamo tuttavia la risposta "Una richiesta di una terza parte". Con l'incremento degli attacchi alle supply chain, le organizzazioni sono sempre più frequentemente costrette a stipulare una cyberassicurazione per potersi aggiudicare un incarico: è infatti il cliente a richiederla, in modo che possa essere tutelato in caso di incidenti derivati dalla partnership.

Più di un partecipante al sondaggio su tre (36%[5]) sostiene che uno dei principali motivi che ha spinto la sua organizzazione ad acquistare una cyberassicurazione è stata una richiesta del consiglio di amministrazione o dei dirigenti. Questo elevato numero di richieste dei team di leadership aziendale riflette i danni devastanti che un grave incidente di cybersecurity può causare a varie organizzazioni. Proteggersi contro le implicazioni di un attacco informatico è ora una questione aziendale di primaria importanza, non solo un problema minore per il reparto IT.



Le Assicurazioni Informatiche: The Market's View – Advisen, PartnerRe

5 Cyber Insurance: The Market's View, PartnerRe and Advisen

I costi delle cyberassicurazioni

Proprio come per tutte le altre assicurazioni, i costi dipendono da vari fattori, che includono:

- **Dati demografici:** dimensioni, settore, ambito, luogo geografico, utili ecc.
- **Potenziale livello di esposizione:** tipo e volume di dati sensibili memorizzati/raccolti/elaborati
- **Livello di cybersecurity:** le difese di sicurezza adottate da un'organizzazione
- **Precedenti:** le richieste di indennizzo passate implicano automaticamente un premio assicurativo più alto
- **Termini della polizza:** copertura/limite di responsabilità ecc.

È importante essere consapevoli della differenza tra polizze con franchigia deducibile e polizze con franchigia ritenuta. Con una franchigia deducibile, la franchigia (detta anche "massimale" in alcuni contesti) viene inclusa nel limite complessivo della polizza. Con una franchigia ritenuta, invece, la franchigia va sommata al limite della polizza.

CON FRANCHIGIA DEDUCIBILE	CON FRANCHIGIA RITENUTA
100mila $: limite della polizza, 10mila $ di franchigia deducibile (massimale)	Limite della polizza: 100mila $, 10mila $ di franchigia ritenuta
Paghi i primi 10mila $, la compagnia di assicurazioni paga 90mila $	Paghi i primi 10mila $, la compagnia di assicurazioni paga 100mila $
Copertura totale: 100mila $	**Copertura totale: 100mila $**

Gruppi di polizze

Nel mercato delle PMI, spesso capita che ci sia un'unica società assicurativa per le cyberassicurazioni. Tuttavia, nel mercato delle imprese di grandi dimensioni, sono molto diffusi i gruppi di polizze, in quanto una singola compagnia di assicurazioni non può sostenere l'intero trasferimento del rischio. I broker assicurativi compongono gruppi di polizze per i singoli clienti, mettendo insieme due, tre o più fornitori. Il primo fornitore copre il trasferimento di rischio primario, mentre i restanti coprono il trasferimento di rischio eccedente.

Panel delle compagnie di assicurazioni

Spesso gli assicuratori collaborano con fornitori pre-approvati, ovvero un "panel", a cui si possono rivolgere qualora si verificasse un incidente. Se l'azienda che subisce l'incidente non ha stabilito un rapporto commerciale con dei fornitori, gli assicuratori consiglieranno (e a volte esigeranno) una collaborazione con le organizzazioni di questo "panel".

Detto questo, la maggior parte degli assicuratori è anche disposta a collaborare con altri fornitori che godono di un'ottima reputazione, specialmente se esiste già una partnership e/o se sono stati definiti termini contrattuali specifici. Viene quindi fornita l'autorizzazione a collaborare con organizzazioni esterne al panel. Naturalmente, collaborare con fornitori che conoscono già l'organizzazione che ha subito l'attacco presenta diversi vantaggi finanziari e operativi; inoltre, questi fornitori avranno dimestichezza con la configurazione informatica e commerciale del loro cliente.

Se il tuo fornitore di fiducia non fa parte del "panel" della tua compagnia di assicurazioni, puoi richiederne il coinvolgimento. È fondamentale comunicare questo desiderio al tuo assicuratore il prima possibile, in modo che il team del tuo fornitore possa contattare la compagnia di assicurazioni per ottenere le approvazioni necessarie.

Esigenze di copertura

Quando si seleziona una polizza di assicurazione cyber, è importante scegliere il livello di copertura che più si addice alle esigenze della propria organizzazione. La polizza deve permettere un ritorno a un'operatività completa nel minor tempo possibile e deve mantenere l'azienda in attività in caso di attacco informatico. Allo stesso tempo deve anche essere caratterizzata da un premio assicurativo non troppo elevato.

I costi necessari per riprendere le attività dopo un attacco informatico sono molto elevati e non accennano a diminuire. Il costo medio sostenuto da un'organizzazione per fronteggiare l'impatto di un attacco ransomware nel 2023 è stato pari a 1,82 milioni di USD[6], in aumento rispetto agli 0,76 milioni di USD del 2020. È interessante osservare che questo calo (minimo, ma pur sempre ben accetto) rispetto agli 1,85 milioni di USD del 2021 riflette probabilmente il fatto che i danni alla reputazione causati da un attacco sono diminuiti, per via della maggiore diffusione del ransomware. Allo stesso tempo, le compagnie di assicurazione sono ora in grado di fornire più velocemente migliori indicazioni alle vittime durante il processo di risposta agli incidenti, diminuendo così i costi di riparazione dei danni.

6 La Vera Storia Del Ransomware 2023, Sophos

Il mercato delle cyberassicurazioni

Le Condizioni Cyberassicurative Sono Diventate Più Severe

Quello delle cyberassicurazioni è stato per molti anni un mercato "facile", caratterizzato da limiti di copertura elevati e premi assicurativi bassi. Tuttavia, per la prima volta in oltre 15 anni di storia in qualità di polizza indipendente, nel 2021 il mercato si è irrigidito, visto che le compagnie di assicurazioni hanno notato come i pagamenti di indennizzi tendessero ad aumentare a una velocità superiore rispetto all'aumento del reddito generato dai premi assicurativi: il tasso di perdita del settore ha subito un incremento stabile dal 2018, raggiungendo il 72,8% nel 2020[7] (il coefficiente di perdita rappresenta il risultato della divisione tra i costi assicurativi e il totale dei premi assicurativi ottenuti. Per esempio, se una compagnia di assicurazioni paga 80 $ di indennizzo per ogni 160 $ di premi assicurativi ricevuti, il coefficiente di perdita corrisponde al 50%).

L'irrigidimento del mercato è stato causato da diversi fattori:

- Gli attacchi informatici hanno subito un aumento sia in termini di volume, sia di complessità -
  - Il 57% degli IT Manager ha dichiarato di avere osservato un aumento del volume degli attacchi informatici[8]
  - Il 59% ha ammesso di avere riscontrato un aumento della complessità degli attacchi informatici[9]
- I costi necessari per riprendere le attività dopo un attacco informatico sono aumentati: come accennato, nel 2023 la somma media necessaria per rimediare ai danni di un attacco ransomware ha raggiunto la cifra esorbitante di 1,82 milioni di USD

Il risultato di questo irrigidimento del mercato è stata una maggiore difficoltà a soddisfare i requisiti necessari per stipulare una cyberassicurazione. Questa situazione problematica è stata confermata da un nostro studio, condotto all'inizio del 2022, a cui avevano partecipato 5.600 IT Manager. Dalle nostre ricerche è emerso che il 94% delle organizzazioni che avevano stipulato una cyberassicurazione sosteneva che la procedura per ottenere una copertura assicurativa fosse cambiata nei 12 mesi precedenti:

- Il 54% dichiarava che il livello di cybersecurity necessario per soddisfare i requisiti di idoneità era più elevato
- Il 47% riteneva che le polizze fossero più complesse
- Secondo il 40% degli intervistati, c'erano meno compagnie di assicurazioni che offrivano un'assicurazione cyber
- Il 37% aveva notato che il processo di approvazione richiedeva più tempo
- Il 34% sosteneva che i costi fossero aumentati[10]

"Dobbiamo pagare la nostra cyberassicurazione e ci troviamo in grandissima difficoltà, molto più che in passato."

Agenzia di viaggi aziendali

Questo irrigidimento del mercato costituiva una sfida molto particolare per gli enti pubblici, che spesso, per via dei loro sistemi di difesa deboli, venivano considerati bersagli facili per i cybercriminali. Di conseguenza, le organizzazioni pubbliche che cercavano di stipulare o rinnovare una polizza assicurativa si sono trovate di fronte a una minore scelta di fornitori e a condizioni meno favorevoli, oltre a prezzi che in alcuni casi potevano raddoppiare di anno in anno.

"Un tempo [gli assicuratori] offrivano un limite di 10 milioni di $, ora di soli 5 milioni di $."

Jack Kudale, CEO, Cowbell Cyber Inc.

Nella seconda metà del 2023 si è osservata un'inversione di tendenza, con un mercato delle cyberassicurazioni meno rigido. L'entrata nel mercato di nuovi player offre ora maggiori possibilità. Tuttavia le compagnie di assicurazioni sono molto selettive e scelgono con estrema attenzione i propri clienti: le organizzazioni che presentano un minore rischio stanno ricevendo offerte assicurative migliori, mentre quelle più a rischio continuano a fare fatica a trovare compagnie disposte ad assicurarle.

7 S&P Global, 1º giugno 2021
8 La Vera Storia Del Ransomware 2022, Sophos
9 La Vera Storia Del Ransomware 2023, Sophos
10 Le Cyberassicurazioni Nel 2022: La Realtà Degli Esperti Di InfoSec In Prima Linea, Sophos

Le cyberassicurazioni mantengono le loro promesse

La buona notizia per chiunque abbia stipulato un'assicurazione informatica è che, se succede il peggio e un'azienda cade vittima di un attacco informatico, le cyberassicurazioni mantengono le loro promesse. Nel sondaggio Sophos "La Vera Storia Del Ransomware 2022", il 98% dei partecipanti assicurati e colpiti dal ransomware ha dichiarato che la compagnia di assicurazioni ha coperto i costi derivati dall'attacco. In quasi tre quarti (73%) degli incidenti, la compagnia di assicurazioni ha coperto i costi di rimozione del ransomware per permettere all'organizzazione colpita di riprendere le proprie attività. Nel 36% degli incidenti, l'assicurazione ha pagato il riscatto e nel 33% altri costi come quelli sostenuti a causa dei tempi di inattività e della perdita di opportunità commerciali.

Le cyberassicurazioni influiscono sull'evoluzione dei sistemi di difesa

Per far fronte all'irrigidimento del mercato, quasi tutte le organizzazioni (97%) che hanno stipulato una polizza hanno cambiato strategia di difesa informatica per migliorare la propria posizione assicurativa.

- Il 64% delle organizzazioni ha implementato nuovi servizi e/o tecnologie
- Il 56% ha incrementato le attività di formazione e sensibilizzazione del personale
- Il 52% ha cambiato procedure e/o attitudini[11]

Ma quali sono i cambiamenti che devi introdurre?
Quali sono le strategie che possono aiutarti a migliorare la tua posizione cyberassicurativa?

11 Le Cyberassicurazioni Nel 2022: La Realtà Degli Esperti Di InfoSec In Prima Linea, Sophos

Una Cybersecurity Efficace Aiuta A Migliorare La Posizione Cyberassicurativa

Esiste una correlazione diretta tra la cybersecurity e le cyberassicurazioni: il 95% delle organizzazioni che hanno acquistato un'assicurazione nel 2023 sostiene infatti che la qualità dei sistemi di difesa ha avuto un impatto diretto sulla loro posizione assicurativa[12]. Investire in sistemi di protezione efficaci garantisce molti vantaggi in termini assicurativi:

1. Rende le polizze più accessibili

Il 60% delle organizzazioni con un'assicurazione informatica dichiara che la qualità delle proprie difese ha influito sulla capacità di ottenere una copertura assicurativa[13]. Gli assicuratori si focalizzano sempre di più sulla gestione (e riduzione) del rischio. Una cybersecurity efficace aiuta a ridurre il rischio informatico, il che a sua volta aumenta il valore di un potenziale cliente agli occhi di una compagnia di cyberassicurazioni. Anche se i requisiti specifici variano a seconda dell'assicuratore, esistono molti controlli comuni che vengono generalmente tenuti in considerazione in questo mercato:

Autenticazione a fattori multipli (Multi-Factor Authentication, MFA)

La Multi-Factor Authentication è spesso un requisito fondamentale per soddisfare i criteri di idoneità di una polizza, in quanto gli assicuratori desiderano risolvere le lacune di sicurezza più comuni, per ammortizzare il rischio.

"Il rinnovo della nostra cyberassicurazione si basa sull'implementazione da parte nostra dell'autenticazione a fattori multipli per l'accesso remoto."

Fornitore di supporto tecnico e servizi IT, Stati Uniti

"Mi è stato detto che se entro un anno non avessimo implementato l'autenticazione a fattori multipli, non avremmo potuto rinnovare la nostra cyberassicurazione."

Azienda sanitaria, Stati Uniti

12 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos
13 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos

Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR)

Una protezione endpoint di ottima qualità, in grado di bloccare automaticamente le minacce, costituisce un livello di sicurezza di base indispensabile per garantire l'efficacia delle difese informatiche. Tuttavia, gli attacchi informatici continuano a evolversi, sfruttando strumenti IT legittimi, credenziali compromesse e vulnerabilità a cui non sono state applicate patch. Ormai la protezione endpoint, da sola, non è più abbastanza. Per prevenire le violazioni e gli attacchi ransomware più avanzati (nonché le richieste di indennizzo che ne conseguirebbero) è fondamentale anche svolgere attività di monitoraggio, indagine e risposta per le attività sospette, prima che i cybercriminali abbiano la possibilità di sferrare i loro attacchi.

EDR e XDR sono strumenti che permettono ai tecnici di sicurezza di rilevare i potenziali tentativi di compromissione e svolgere indagini, nonché di neutralizzare un attacco informatico avanzato prima che vengano causati danni irreversibili. Come suggerisce il nome stesso, EDR raccoglie informazioni solo dalle tecnologie di protezione endpoint. XDR, invece, sfrutta i dati ottenuti dalle origini dei dati delle soluzioni endpoint e di altri ambiti dello stack informatico (inclusi firewall e soluzioni di protezione per e-mail, cloud e dispositivi mobili), per offrire una visibilità superiore e accelerare il processo di rilevamento e risposta. L'EDR è particolarmente importante, poiché spesso è un prerequisito obbligatorio per la maggior parte delle compagnie di cyberassicurazione e le organizzazioni che non hanno questa capacità fanno fatica a stipulare una polizza.

Managed Detection and Response (MDR)

MDR è un servizio operativo 24/7 e completamente gestito, a cura di esperti specializzati nel rilevamento e nella risposta agli attacchi informatici; previene gli incidenti che sarebbero impossibili da fermare con l'uso delle sole tecnologie. Garantisce il massimo livello di protezione contro le minacce informatiche, riducendo al minimo il rischio e di conseguenza la probabilità che il cliente invii una richiesta di indennizzo. Sebbene sia raro che venga ritenuto un requisito indispensabile per una copertura assicurativa, le organizzazioni che usano un servizio MDR vengono spesso considerate clienti di "livello 1" dalle compagnie di assicurazioni, poiché presentano il rischio minore.

"Il reparto legale ha richiesto un'assicurazione contro il ransomware ed [MDR] è il passo che dobbiamo compiere per ottenerla."

Fornitore di tecnologie e soluzioni IT di livello globale

Piano strategico di risposta agli incidenti

Il modo migliore per impedire che un attacco informatico diventi un vero e proprio caso di violazione è prepararsi in anticipo. Dopo una violazione, spesso le organizzazioni si rendono conto che avrebbero potuto evitare molti dei costi, problemi e disagi subiti, se solo avessero avuto un piano strategico di risposta. Preparare un piano dettagliato, in grado di mitigare l'impatto di un incidente, ridurrà il tuo rischio informatico, aumentando il valore della tua organizzazione agli occhi di una compagnia di cyberassicurazioni

2. Riduce i premi assicurativi

Il 62% delle organizzazioni con un'assicurazione informatica sostiene che la qualità delle proprie difese ha influito sul costo della copertura assicurativa[14]. Esattamente come l'installazione di un sistema di allarme e di serrature alle finestre aiuta a diminuire il premio dell'assicurazione per la casa, allo stesso modo l'implementazione di difese informatiche avanzate permette di limitare i costi delle cyberassicurazioni. Anche se gli algoritmi specifici per il calcolo dei premi delle compagnie di assicurazioni sono un segreto ben custodito, i clienti dichiarano frequentemente che la qualità della propria protezione influisce sui premi assicurativi.

"Non avendo installato EDR sul 100% delle nostre appliance, i costi di assicurazione sono raddoppiati."
Azienda di web hosting, Stati Uniti

"Con Measured, i clienti che hanno implementato Sophos MDR o Sophos Endpoint possono ottenere un premio assicurativo fino al 25% più basso."
Measured Insurance, Stati Uniti

3. Riduce la probabilità di dover chiedere un indennizzo

Proprio come per gli altri tipi di assicurazioni, l'invio di una richiesta di indennizzo potrebbe impedirti di rinnovare la polizza in futuro. Le organizzazioni che hanno richiesto un indennizzo hanno anche registrato un incremento nei premi assicurativi degli anni successivi. Mitigando il rischio di subire un attacco grazie all'implementazione di difese informatiche efficaci, si diminuisce anche la probabilità di dover ricorrere alla propria polizza. Di conseguenza, i premi assicurativi saranno meno cari.

4. Riduce il rischio di mancato pagamento

Un sistema di cybersecurity con uno stato di integrità scadente può impedire di ricevere sostegno finanziario in caso di incidente. Se l'assicuratore ritiene che la vittima abbia "lasciato una porta aperta" a causa di pratiche di sicurezza inadeguate, potrebbe essere intitolato a non pagare l'indennizzo. Eliminando queste vulnerabilità, è possibile accertarsi che, se dovesse succedere il peggio, la compagnia di assicurazioni interverrebbe.

"Non paghiamo indennizzi per perdite, violazioni, indagini sulla privacy o minacce in presenza di software o sistemi obsoleti o non supportati."
Tratto dalla polizza di Hiscox Cyberclear™, Regno Unito, giugno 2021

5. Limita l'impatto e i costi in caso di incidente

Una risposta rapida e appropriata a un attacco informatico può ridurre significativamente l'impatto e i costi causati dall'incidente. Preparare un piano di incident response in caso di incidenti malware e poter contare sull'assistenza di esperti in materia aiuta ad ammortizzare le conseguenze di un attacco.

14 Il Ruolo Fondamentale Delle Difese Informatiche Nella Stipulazione Di Un'Assicurazione, Sophos

L'Aiuto Che Offre Sophos

Ottimizza le tue difese informatiche

Sophos offre alle organizzazioni tutto quello di cui hanno bisogno per applicare gran parte dei controlli informatici che sono fondamentali sia per soddisfare i requisiti di idoneità delle coperture assicurative, sia per ottenere prezzi e condizioni più vantaggiosi nelle polizze. L'intera infrastruttura si basa sui dati di intelligence sulle minacce e sull'esperienza di cybersecurity di Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

Sophos EDR offre l'approccio incentrato sulla prevenzione di Sophos Endpoint, più potenti capacità di rilevamento e risposta che permettono agli analisti di sicurezza e agli amministratori IT di individuare proattivamente le minacce, svolgere indagini e rispondere alle attività sospette identificate in tutti gli endpoint e i server. I rilevamenti ricevono una priorità, grazie alle analisi basate sull'IA. Questa strategia ti fa risparmiare tempo prezioso, poiché ti aiuta a capire dove devi concentrare la tua attenzione. Il team di sicurezza della tua organizzazione può quindi accedere ai dispositivi da remoto per svolgere varie azioni, ad esempio: indagare sui problemi, installare e disinstallare software, terminare i processi attivi, eseguire script o programmi, modificare i file di configurazione e molto di più.

Sophos Extended Detection and Response (XDR)

Più vedi, più velocemente puoi agire. Sophos XDR sfrutta i dati di telemetria raccolti dalle soluzioni Sophos e non Sophos che già usi, per aiutarti a rilevare le minacce, svolgere indagini e rispondere alle attività sospette nel tuo intero ambiente informatico.

- **Rilevamento:** i rilevamenti basati su intelligenza artificiale garantiscono visibilità immediata sulle attività sospette intercettate nelle principali superfici di attacco, mentre la nostra ricerca semplice non richiede competenze SQL e permette di individuare le minacce con estrema rapidità
- **Indagine:** creazione automatica di casi con assegnazione di priorità ai rilevamenti, per permetterti di focalizzarti sugli elementi più importanti; allo stesso tempo, la nostra UX progettata da analisti esperti ti offre tutte le informazioni e gli strumenti necessari per svolgere indagini con estrema facilità
- **Risposta:** ampia scelta di strumenti di gestione dei casi e azioni di risposta, che ti permettono di collaborare con i membri del team e neutralizzare tempestivamente gli attacchi

Sophos Managed Detection and Response (MDR)

Sophos MDR è il servizio MDR numero uno al mondo, in quanto protegge più organizzazioni di qualsiasi altro vendor. Sophos MDR offre un servizio gestito di rilevamento, indagine e risposta alle minacce operativo 24/7 e fornito da un team di esperti, per una protezione assoluta. Con un tempo medio di risoluzione degli incidenti pari ad appena 38 minuti, Sophos MDR riduce significativamente il rischio di incorrere in un incidente informatico grave e migliora la tua posizione assicurativa.

Riduce la probabilità di dover chiedere un indennizzo

Sophos offre protezione leader a livello mondiale contro ransomware, hacking a scopo malevolo e altre minacce avanzate. Le nostre soluzioni aiutano a minimizzare il rischio di incidenti informatici gravi, riducendo la probabilità di dover chiedere un indennizzo, così da mantenere bassi i premi assicurativi in futuro.

"Non possiamo bloccare tutti gli attacchi da soli: è per questo che ci affidiamo a Sophos."
Vancouver Canucks, Canada

Le soluzioni Sophos godono dell'approvazione di clienti e analisti

Le soluzioni Sophos vantano l'approvazione di moltissimi clienti e della comunità di analisti; inoltre, hanno un'efficacia riconosciuta ufficialmente da vari test indipendenti. Ecco alcuni esempi:

Sophos Managed Detection and Response (MDR)

- Nominata tra le 2023 Gartner® Customers' Choice™ per la Managed Detection and Response (MDR), con un punteggio dei clienti pari a 4,8/5 su Gartner Peer Insights
- Nominata Leader Complessivo di Managed Detection and Response (MDR) nei report Grid ® di G2 dell'autunno 2023
- Vendor con i migliori risultati nella valutazione MITRE Engenuity ATT&CK del 2022 per i provider di servizi gestiti

Sophos Extended Detection and Response (XDR)

- Nominata Leader Complessivo di XDR nei report Grid ® di G2 dell'autunno 2023
- Vendor con i migliori risultati nelle valutazioni MITRE Engenuity ATT&CK 2023 (Turla)
- Riconosciuta come leader al 1° posto complessivo da Omdia Universe nella categoria Comprehensive Extended Detection and Response (XDR)

Sophos Endpoint Detection and Response (EDR)

- Nominata Leader nel 2022 Gartner® Magic Quadrant™, categoria Endpoint Protection Platforms (piattaforme di protezione endpoint), per la 13ª volta consecutiva
- Nominata tra le 2023 Gartner® Customers' Choice™ per le Endpoint Protection Platforms per il secondo anno consecutivo, con un punteggio dei clienti pari a 4,8/5 su Gartner Peer Insights
- Nominata Leader Complessivo delle Endpoint Protection Suites e di EDR nei report Grid ® di G2 dell'autunno 2023Vendor con i migliori risultati nelle valutazioni MITRE Engenuity ATT&CK 2023 (Turla)
- Punteggi AAA e del 100% di protezione totale nell'Endpoint Security Report Q3 2023 degli SE Labs, sia nella categoria Enterprise che SMB (PMI).

Per maggiori informazioni sulle soluzioni Sophos, clicca qui

Sophos offre soluzioni di cybersecurity leader di settore, ideali per le aziende di tutte le dimensioni; inoltre, protegge i sistemi in tempo reale contro minacce avanzate quali malware, ransomware e phishing. Grazie alle funzionalità Next-Gen dall'efficacia comprovata, garantisce una protezione efficace per i dati aziendali, con prodotti basati su tecnologie di Intelligenza Artificiale e Machine Learning.

2024-01-12 (WP-PC)

SOPHOS