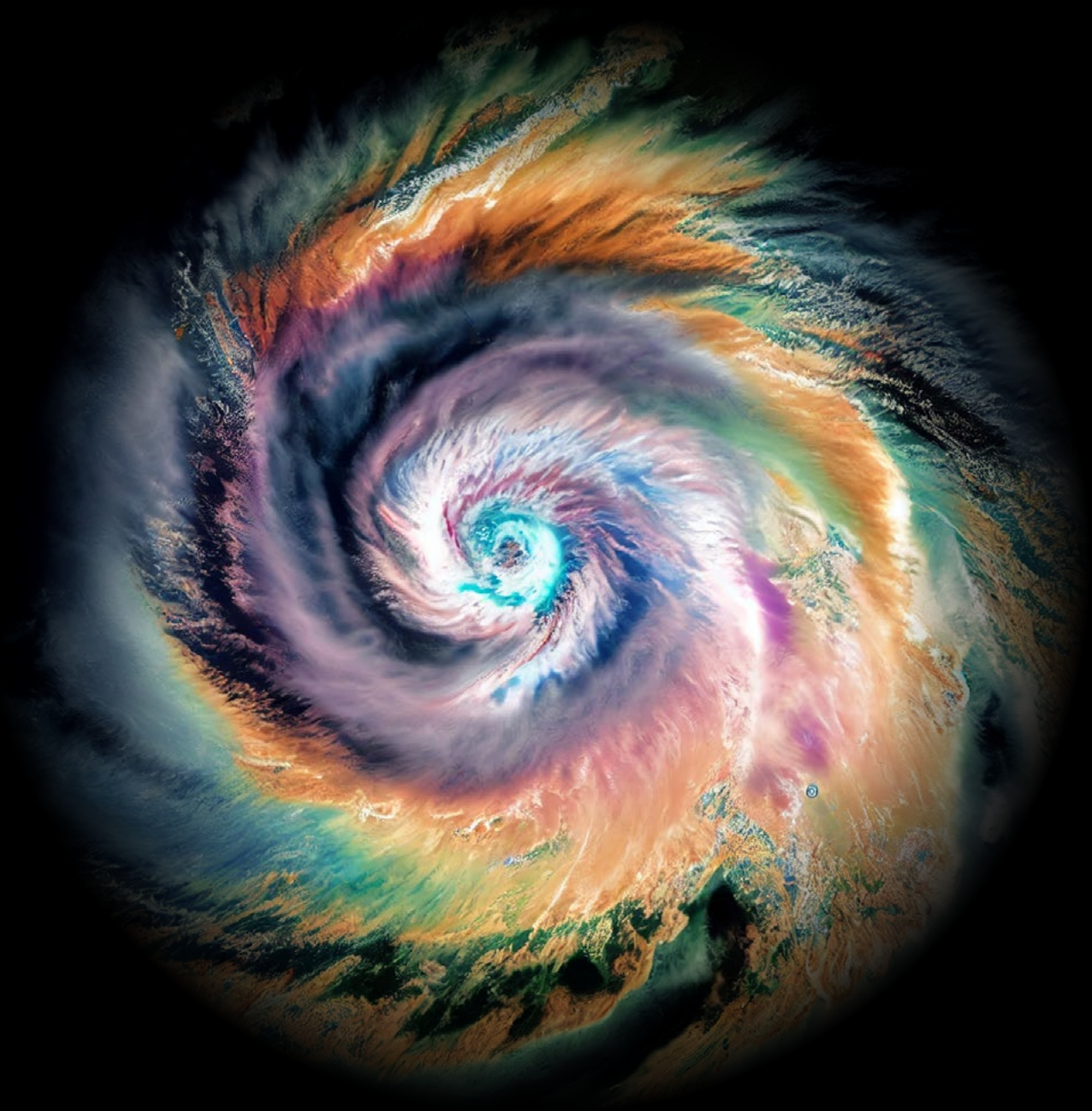
Deloitte.
Private



L’ERM e la sfida per contenere le minacce alla cybersicurezza

Introduzione

Poiché le organizzazioni di tutte le dimensioni e tipologia di proprietà si muovono sempre più online, automatizzano i processi e impiegano lavoratori da remoto, i rischi da attacchi informatici aumentano. In questo contesto, le risorse legate alle informazioni come la posta elettronica, la proprietà intellettuale aziendale e i dati dei clienti possono diventare bersagli per hacker, cybercriminali e attori dello spionaggio per sfruttare gli utenti aziendali, i dipendenti o altri stakeholder d'impresa. Pur non avendo un profilo di rischio elevato quanto gli omologhi operatori "pubblici", le imprese private, incluse quelle familiari, sono comunque soggette ad attacchi informatici e obiettivi di hackeraggio. Questo potenzialmente le espone a sostenere costi elevati per ripristinare sistemi, qualora le loro pratiche di sicurezza non siano mature.

È importante che il personale di tutta l'organizzazione - soprattutto in realtà i cui team di *cybersecurity* potrebbero non avere le risorse necessarie per implementare un efficace programma di sicurezza informatica - impari a proteggere sistemi e informazioni dalle crescenti minacce. Il vantaggio di avere una spiccata sensibilità a rilevare e rispondere alla minaccia di attacchi cyber all'interno di un programma di gestione del rischio aziendale (ERM) è molto simile a un radar Doppler, che lavora in background per la sorveglianza e il monitoraggio delle tempeste, consentendo ai team di rilevare e rispondere alle minacce cyber quando si presentano.

Una minaccia multi-fronte

Gli hacker in ambito cyber stanno diventando sempre più sofisticati e le organizzazioni potrebbero non rilevare un attacco se non a mesi di distanza dall'accaduto. Una survey del 2023 mostra che le organizzazioni hanno impiegato 204 giorni per identificare una violazione e una media di 73 giorni per contenerla o risolverla una volta identificata.

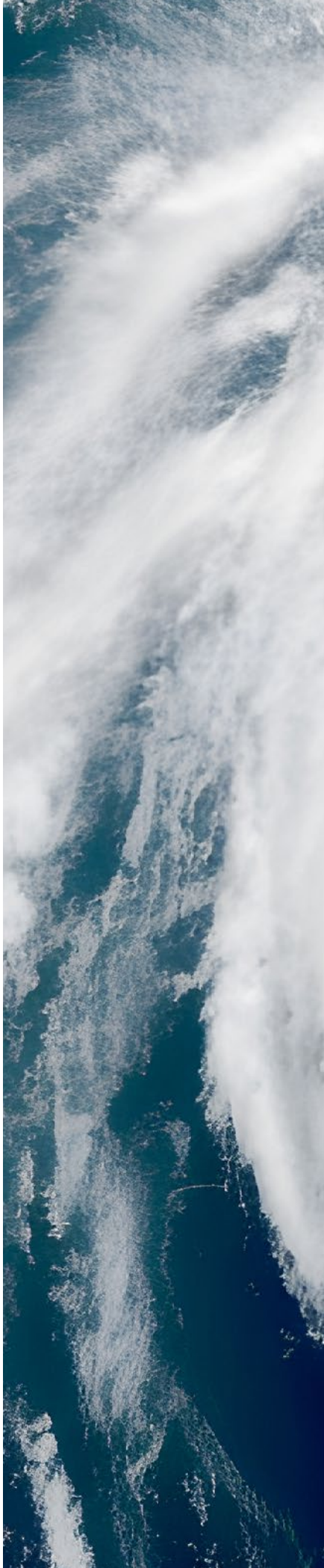
Una comune tipologia di attacco rivolta alle aziende private è il "ransomware", tramite cui gli hacker estorcono informazioni alle organizzazioni o ne bloccano l'operatività a fronte di un riscatto. Nel 2022, Deloitte ha osservato più di oltre 100 famiglie di *ransomware*, che condividono codici comuni e comandi dannosi; le modalità predominanti con cui si manifestano gli attacchi includono credenziali compromesse, servizi e applicazioni esterne violate da remoto e problematiche nell'autenticazione multi-fattore. Nei primi sei mesi del 2023, le "bande" di *ransomware* hanno estorto più di 449 milioni di dollari dalle vittime, compiendo attacchi che li hanno avvicinati al picco dei quasi 940 milioni di dollari toccato nel 2021.

Inoltre, la ricerca Deloitte mostra altri tipi di attacchi che hanno un impatto negativo sulle aziende, tra cui il furto d'identità digitale dei C-level sui social media tramite account fraudolenti, la presenza di account social media malevoli ai loro danni, nonché attacchi di phishing che compromettono gli account di posta elettronica aziendali.

Le violazioni perpetrate tramite terze parti e i rischi informatici associati sono un'altra area di preoccupazione. In un recente studio Deloitte, è emerso che il 74% degli intervistati ha affrontato almeno un incidente prodotto da terze parti negli ultimi tre anni.

Esistono anche azioni malevole da parte di soggetti che utilizzano le informazioni per condizionare gli affari geopolitici, utilizzando fughe di dati, attacchi ideologici e deturpazione dei siti web. Questi attacchi possono talvolta essere rivolti in generale a fazioni e regimi governativi, ma gli effetti si ripercuotono sui servizi pubblici e sulle imprese.

Una comune tipologia di attacco rivolta alle aziende private è il "ransomware", tramite cui gli hacker estorcono informazioni alle organizzazioni o ne bloccano l'operatività a fronte di un riscatto.



Valutare le probabilità di rischio

L'automazione dei processi produttivi, il ricorso al digitale e il lavoro da remoto concorrono all'aumento delle minacce informatiche e questo fa sì che il rischio aziendale cresca e aumenti l'onere di disporre di sistemi di rilevamento e prevenzione efficaci. Una delle principali pratiche che le aziende private e le imprese familiari possono prendere in considerazione è quella di implementare una analisi che identifichi un proprio profilo di rischio informatico, valutando la probabilità e l'impatto delle minacce ad esso connesse. Ciò comporta la determinazione della propensione generale al rischio per l'impresa, al fine di definire il *tone at the top* strategico aziendale nel suo complesso.

È possibile implementare alcune procedure fondamentali per la gestione delle identità e degli accessi ed evitare potenziali violazioni o perdite di dati. Ad esempio, disporre di un sistema di gestione delle identità e degli accessi che comprenda funzioni quali la gestione degli accessi con privilegi, la governance, il *single sign-on* e l'autenticazione a più fattori, può essere un valido approccio al rischio. Inoltre, la costruzione di un'architettura informatica aziendale in cui solo a determinati individui viene concesso l'accesso o i privilegi, di cui hanno bisogno in base al proprio ruolo, può limitare le potenziali violazioni dei dati e delle informazioni.

Un altro passo tangibile che può essere fatto dai manager è identificare quali siano gli asset più importanti dell'organizzazione. Queste risorse preziose possono comprendere i dati dei clienti, le informazioni sulle transazioni bancarie o la proprietà intellettuale, come formule e brevetti. La specificità degli asset dipende dal settore, dalla mission dell'organizzazione e dalla natura delle sue operazioni. Non basta solo sapere quali siano gli asset, in quanto le organizzazioni dovrebbero sapere anche dove sono, come sono accessibili e, quindi, come tali asset possono essere protetti al meglio.

Le aziende devono anche prendere in considerazione i fornitori con riferimento alla loro capacità di rilevamento e opposizione al rischio informatico. Come per le verifiche continue all'interno della propria organizzazione, è importante considerare e monitorare anche le minacce provenienti dall'interno dell'ecosistema delle terze parti. A tal fine, una buona prassi è interrogarsi sulla gestione dei rischi da parte dei fornitori e terze parti. Ciò potrebbe includere domande sullo stato della catena di fornitura, sull'ubicazione dei fornitori all'interno della catena del valore e se tali soggetti terzi abbiano mai subito violazioni.

Un altro passo tangibile che può essere fatto dai manager è identificare quali siano gli asset più importanti dell'organizzazione. Queste risorse preziose possono comprendere i dati dei clienti, le informazioni sulle transazioni bancarie o la proprietà intellettuale, come formule e brevetti.

Diffondere la responsabilità

Gestire i rischi all'interno dell'ecosistema di un'organizzazione richiede un coordinamento significativo e una giusta struttura di *risk management*. Per un'azienda di piccole dimensioni o meno matura il cui responsabile della sicurezza ha più ruoli, questo significa che lo stesso dovrebbe avere competenze IT, privacy e digitali. Queste sono difficilmente presenti in un unico soggetto, il quale spesso non ha un ruolo e formazione ben distinta e fa parte del management o del Consiglio di Amministrazione, con competenze non approfondite in ambito di rischio informatico.

Deloitte prevede che i costi della criminalità informatica saliranno a 10,5 trilioni di dollari entro il 2025, sottolineando la necessità di misure di sicurezza efficaci. I tradizionali tempi di rilevamento delle violazioni possono subire ritardi di mesi, probabilmente richiedendo un approccio più proattivo in merito alla protezione di dati e sistemi.

Il Consiglio di Amministrazione è infine responsabile della salvaguardia della governance e della vitalità dell'organizzazione. La domanda ora è se i consigli di amministrazione sono in grado di ottenere le informazioni giuste per prendere decisioni "consapevoli" in relazione al tema del rischio.

Pianificare una strategia di risposta agli incidenti

Ci sono una serie di domande che i leader possono porre alla propria organizzazione, a prescindere dal grado di preparazione e maturità dell'impresa:

- La sicurezza informatica è una priorità sufficiente per l'organizzazione e c'è qualcuno che si dedica al ruolo e ha il livello di competenza per svolgere il lavoro?
- Se e quando si subisce una violazione di dati, qual è il *playbook* di risposta agli incidenti? Esiste una protezione efficace degli asset e delle risorse chiave per evitare un impatto significativo?
- Se si è vittime di un attacco *ransomware*, sono disponibili sistemi di backup e ripristino adeguati? È possibile operare in modo resiliente durante un attacco e mantenere le operazioni aziendali essenziali?
- Il processo per affrontare i rischi legati alle terze parti si verifica con una frequenza corretta e ci si pone le domande giuste per determinare il profilo di rischio dei fornitori in essere e delle terze parti con cui si è in contatto?

Nel prossimo articolo, verranno esaminati alcuni rischi operativi comuni e il modo in cui le aziende private possono integrare la gestione dei rischi operativi assumendo un "posizionamento" più efficace sui rischi.

In virtù dell'esperienza maturata nei contesti più diversi, **Deloitte Private** sviluppa progetti di collaborazione che si fondano sulle reali esigenze espresse dai clienti, creando per loro soluzioni su misura in base alle loro dimensioni e alla loro storia. Partendo dall'ascolto dei bisogni, Deloitte Private affianca l'imprenditore posizionandosi come *Trusted Business Advisor* di soluzioni multidisciplinari destinate a:

- Le imprese familiari e i loro imprenditori e famiglie
- I *Family Office* e gli investitori privati con i loro consulenti (*private banker* e *wealth manager*)
- Le Piccole e Medie Imprese quotate e non quotate
- I *Private Equity*, con portafoglio dedicato alle Piccole e Medie Imprese
- Le micro-imprese, anche in forma di start-up

CONTATTI ITALIA

Ernesto Lanzillo
Deloitte Private Leader Deloitte Central Mediterranean (Italia, Grecia e Malta)

elanzillo@deloitte.it

Ezio Pagliano
Partner Deloitte Risk Advisory, Enterprise Risk Management Expert

epagliano@deloitte.com

AUTORI

Kevan Flanigan
US Deloitte Private Leader, Risk & Financial Advisory US Deloitte Private Leader, Private Equity

keflanigan@deloitte.com

Tiffany Kleemann
Cyber & Strategic Risk Managing Director

tkleemann@deloitte.com

Deloitte.

Deloitte Creative Team - Italia | SG.008.24