Chubb Easy Solutions
Polizza di Assicurazione Cyber Enterprise Risk Management

Versione 2.2 - Ed.10/2022

QUESTIONARIO

Questo documento permette a Chubb di raccogliere le informazioni necessarie per valutare i rischi connessi ai sistemi informatici della Società che richiede la quotazione del rischio. Resta inteso che il completamento di questo questionario non vincola Chubb né la Società alla conclusione di un accordo per l'emissione di una polizza

Parametri di accesso:

1. La Società presenta un fatturato consolidato inferiore o uguale a € 100 milioni
2. La Società presenta almeno un'annualità di bilancio
3. La Società NON è quotata in Borsa
4. La Società NON ha controllate negli Stati Uniti
5. La Società NON è già assicurata, direttamente o tramite società controllanti, da polizza Cyber in vigore con Chubb
6. Negli ultimi 3 anni NON ha avuto sinistri in ambito di sicurezza informatica o privacy
7. La Società NON sia e NON controlli Società che operino nei seguenti settori:
   - Servizi di Accreditamento/Certificazione
   - Servizi di contenuti per adulti
   - Centrale Rischi/Informazioni Creditizie
   - Scambio di criptovalute o tecnologia blockchain
   - Prodotti o servizi di sicurezza informatica
   - Aggregatori di dati personali, intermediazione/warehousing di dati
   - Istituzioni finanziarie
   - Aste online/Centro scommesse/Centro scommesse sportive/ Gioco d'azzardo
   - Pubblica Amministrazione Locale o Regionale
   - Prodotti e/o Servizi per la sicurezza (es. antinfortunistica, antincendio)
   - Attivitá settore media (trasmissione, produzione, creazione di contenuti multimediali)
   - Elaborazione dei pagamenti o piattaforma di Trading
   - Condivisione file peer to peer
   - Piattaforme di Social Media
   - Sorveglianza (fisica o digitale)
   - Amministrazione sinistri/reclami di terze parti
   - Intermediari assicurativi
   - Difesa/Sicurezza nazionale/Aerospaziale
   - Compagnie Aeree/Controllo del traffico aereo

Dati della Società (Contraente)			
Denominazione Sociale			
Indirizzo			
Codice Fiscale/P.IVA			
Fatturato Annuo Consolidato			
% Fatturato Annuo generato in USA e/o Canada	[ ] <= 20% [ ] > 20%		
% Fatturato Annuo generato dalle vendite online	[ ] <= 25% [ ] <= 50% [ ] > 50%		
Nr. Dipendenti			
Sito web della Società			
Attività Svolta - Descrizione			
Attività Svolta – NAIC (se disponibile)			
Dati di Contratto			
Periodo Assicurativo	Data Effetto ore 24.00 del: [ ] Data Scadenza ore 24.00 del: [ ]		
Frazionamento:	[ ] Annuale [ ] Semestrale		
Indicare Limite di Polizza per il quale si desidera ricevere quotazione	Quotazione - Opzione 1	Quotazione - Opzione 2	Quotazione - Opzione 3
	[ ] Euro 100.000	[ ] Euro 100.000	[ ] Euro 100.000
	[ ] Euro 250.000	[ ] Euro 250.000	[ ] Euro 250.000
	[ ] Euro 500.000	[ ] Euro 500.000	[ ] Euro 500.000
	[ ] Euro 750.000	[ ] Euro 750.000	[ ] Euro 750.000
	[ ] Euro 1.000.000	[ ] Euro 1.000.000	[ ] Euro 1.000.000
	[ ] Euro 2.000.000	[ ] Euro 2.000.000	[ ] Euro 2.000.000
	[ ] Euro 3.000.000	[ ] Euro 3.000.000	[ ] Euro 3.000.000
Indicare il Sottolimite per Eventi a Impatto Diffuso per il quale si desidera ricevere quotazione	[ ] = 10% del Limite di Polizza [ ] = 50% del Limite di Polizza [ ] = 100 % del Limite di Polizza		
La Società è già titolare di una polizza RC Professionale in vigore con Chubb?	[ ] SI, indicare Nr. di Polizza: [ ] NO		
Dati di contatto del Responsabile della sicurezza dei dati e della rete			
Nome e cognome			
Ruolo			
e-mail	Telefono		

	Informazioni sul Rischio	
1	La Contraente ha sede in Italia e NON è una controllata, filiale, franchisee o un'entità di un'organizzazione più grande? Se la Società è una filiale/controllata di un fondo di Prive Equity, selezionare "SI'"	□ SI □ NO
2	La Società fornisce servizi o ha rapporti commerciali con Individui e/o Organizzazioni in territori sanzionati (inclusi - a titolo esemplificativo ma non esaustivo, Iran, Siria, Nord Sudan, Crimea e Cuba) o qualsiasi altro territorio soggetto a sanzioni USA, UE, ONU e/o altre restrizioni nazionali?	□ SI □ NO
3	La Società e/o le sue controllate, operano in uno dei seguenti settori:	
	• Servizi di Accreditamento/Certificazione	□
	• Servizi di contenuti per adulti	□
	• Centrale Rischi/Informazioni Creditizie	□
	• Scambio di criptovalute o tecnologia blockchain	□
	• Prodotti o servizi di sicurezza informatica	□
	• Aggregatori di dati personali, intermediazione/warehousing di dati	□
	• Istituzioni finanziarie	□
	• Aste online/Centro scommesse/Centro scommesse sportive/ Gioco d'azzardo	□
	• Pubblica Amministrazione Locale o Regionale	□
	• Prodotti e/o Servizi per la sicurezza (es. antinfortunistica, antincendio)	□
	• Attivitá settore media (trasmissione, produzione, creazione di contenuti multimediali)	□
	• Elaborazione dei pagamenti o piattaforma di Trading	□
	• Condivisione file peer to peer	□
	• Piattaforme di Social Media	□
	• Sorveglianza (fisica o digitale)	□
	• Amministrazione sinistri/reclami di terze parti	□
	• Intermediari assicurativi	□
	• Difesa/Sicurezza nazionale/Aerospaziale	□
	• Compagnie Aeree/Controllo del traffico aereo	□
4	La Contraente sviluppa Software e/o fornisce servizi IT ad aziende terze o individui?	□ SI □ NO
5	La Contraente conferma che le politiche inerenti la protezione dei dati personali e la tutela della privacy sono periodicamente riviste al fine di essere allineate alle **normative vigenti** nelle giurisdizioni in cui opera	□ SI □ NO
6	La Contraente dichiara che non si è mai verifica-to un qualunque **Incidente Cyber**, **Data Breach** o reclamo in materia di privacy nei precedenti 3 anni e non è al corrente di qualsiasi circostanza che possa dare origine ad un sinistro nell'ambito della polizza Cyber	□ SI □ NO
	Se sì, indicare il numero di sinistri e l'importo totale pagato:	
	• Numero di Sinistri	□ <=2 □ > 2
	• Importo totale pagato	□ <= € 500.000 □ > € 500.000
7	La Società è già assicurata, direttamente o tramite società controllanti, da polizza Cyber in vigore con Chubb?	□ SI □ NO
8	La Contraente ha Società Controllate con sede in Paesi extra UE per le quali è richiesta la copertura assicurativa?	□ SI □ NO
9	La Contraente, o il provider a cui è affidato il servizio, accetta pagamento con carte di credito/debito?	□ SI □ NO
	Se sì, è compliant con gli standard **PCI-DSS (Payment Card Industry – Data Security Standards)**?	□ SI □ NO
10	La rete o alcuni dei sistemi aziendali consentono l'accesso da remoto?	□ SI □ NO
	- Se sì, è previsto l'utilizzo di soluzioni **MFA (Multi-Factor Authentication)** per gli accessi da remoto a tali sistemi?	□ SI □ NO
11	In caso di violazione delle **Informazioni di Identificazione Personale**, la notifica da parte della Società potrebbe riguardare un numero maggiore di 500.000 individui?	□ SI □ NO
	Se sì il numero di individui	□ <= 1.000.0000 □ > 1.000.000
12	Selezionare le misure che la Società utilizza a protezione dei back up dei sistemi critici per l'attività aziendale	
	• *Una o più misure di protezione selezionate = copertura **Ransomware** full limit* • *Se viene selezionata "Nessuna delle protezioni elencate" = Sottolimite **Ransomware** pari a € 100.000*	
	Immutable back up: i back up, una volta memorizzati su uno storage, non possono essere modificati (**Write Once Read Many - WORM**)	□ SI □ NO
	I back up vengono **archiviati offline o presso una ambiente/storage separato** (es. nastro, dischi completamente disconnessi rispetto al resto della rete)	□ SI □ NO
	l'accesso ai backup è limitato solo ad **Account Privilegiati** dedicati che non sono collegati all' **Active Directory** o ad altri domini	□ SI □ NO
	l'accesso ai backup è protetto tramite l'autenticazione a più fattori **MFA (Multi-Factor Authentication)**	□ SI □ NO
	Nessuna delle protezioni elencate precedenti	□ SI □ NO
13	Selezionare quali tecnologie la Società utilizza a protezione degli endpoint su tutti i laptop, desktop e server	
	• *Due o più misure di protezione selezionate = copertura **Ransomware** full limit* • *Se viene selezionata solo una o "Nessuna delle protezioni elencate" = Sottolimite **Ransomware** pari a € 100.000*	
	Sistemi di Advanced Endpoint Protection o in grado di effettuare **Analisi di tipo Euristico**	□ SI □ NO
	Filtro URL o Web - filtering	□ SI □ NO
	Tecnologie di **isolamento e contenimento delle applicazioni**	□ SI □ NO

	Piattaforma centralizzata per la Endpoint Protection	□ SI □ NO
	EDR (Endpoint Detection and Response), **XDR (Extended Detection and Response)**, o **MDR (Managed Detection and Response)**	□ SI □ NO
	Nessuna delle protezioni elencate precedenti	□ SI □ NO
14	Selezionare quali misure la Società utilizza a protezione delle e-mail	
	• *Due o più misure di protezione selezionate = copertura **Ransomware** full limit* • *Se viene selezionata solo una o "Nessuna delle protezioni elencate" = Sottolimite **Ransomware** pari a € 100.000*	
	Servizio di quarantena per e-mail sospette	□ SI □ NO
	Disponibilità di **Sandbox** per la verifica di allegati potenzialmente sospetti	□ SI □ NO
	Applicazione del **Sender Policy Framework (SPF)**.	□ SI □ NO
	Le macro di Microsoft Office sono disabilitate sui documenti per impostazione predefinita	□ SI □ NO
	Simulazioni di phishing o altra formazione per i dipendenti con cadenza almeno annuale	□ SI □ NO
	Nessuna delle protezioni elencate precedenti	□ SI □ NO

Il sottoscritto certifica che tutte le dichiarazioni contenute nel presente questionario sono complete e corrette. Tutte le modifiche che avvengono dopo la presentazione del questionario o durante il periodo di assicurazione devono essere comunicate a Chubb European Group SE, immediatamente. I dati personali relativi al firmatario (nome, cognome, funzione e firma) sono obbligatori e saranno trattati da Chubb European Group SE in ottemperanza alle vigenti leggi. Tali dati saranno trattati dai sottoscrittori autorizzati e dal personale del gruppo Chubb incaricati della gestione di applicazioni di protezione dei dati relative a Rischi e offerte. Il titolare dei dati ha il diritto di ottenere una copia dei propri dati personali che lo riguardano, ottenere la rettifica o la cancellazione dei dati personali scaduti o inesatti e di opporsi al loro trattamento per motivi legittimi. Se si desidera esercitare tali diritti alla privacy, si prega di inviare la tua richiesta scritta, insieme a una copia di un documento d'identità, al seguente indirizzo: Chubb European Group SE, Via Fabio Filzi n. 29 - 20124 – Milano.

Nome e Cognome del firmatario	**Ruolo**
Ruolo	**Firma**

Glossario

Active Directory: è una raccolta di oggetti all'interno di una rete "Microsoft Active Directory". Un oggetto può essere un singolo utente, un gruppo di utenti, oppure un componente hardware (come un computer o una stampante). Ogni dominio contiene un database con informazioni sull'identità degli oggetti.

Sistemi di Advanced Endpoint Protection: un dispositivo o un software che fornisce protezione e monitoraggio degli endpoint sulla rete. Gli endpoint includono computer desktop e laptop, tablet, telefoni cellulari, server e qualsiasi altro dispositivo connesso alla rete

EDR (Endpoint Detection and Response): è una soluzione che registra e archivia i comportamenti a livello di sistema degli endpoint, utilizza varie tecniche di analisi dei dati per rilevare comportamenti sospetti del sistema, fornire informazioni, bloccare attività dannose e fornire suggerimenti per ripristinare i sistemi compromessi.

MDR (Managed Detection and Response): è un servizio di sicurezza informatica che rileva le intrusioni di malware e/o attività dannose nella rete e assiste nella risposta rapida agli incidenti per eliminare tali minacce con brevi azioni di remediation.

XDR (Extended Detection and Response): è un servizio di sicurezza informatica che raccoglie e correla automaticamente i dati tra più livelli di sicurezza: email, endpoint, server, workload in cloud e rete. Ciò permette di rilevare più velocemente le minacce e di migliorare i tempi di indagine e di risposta attraverso l'analisi della sicurezza.

Isolamento e contenimento delle applicazioni: un insieme di tecnologie per bloccare, limitare o isolare endpoint specifici dall'esecuzione di azioni potenzialmente dannose tra endpoint e altre applicazioni o risorse, con l'obiettivo di limitare l'impatto di un sistema o di un endpoint compromesso.

Piattaforma centralizzata per la Endpoint Protection: è una soluzione distribuita sui i dispositivi endpoint per prevenire attacchi di malware basati su file, rilevare attività dannose, e fornire avvisi dinamici di sicurezza e servizi di indagine e remediation necessari per rispondere agli incidenti.

Incidente Cyber: gli incidenti includono qualunque accesso non autorizzato a qualunque computer, sistema informatico, database, intrusione o attacco, impossibilità d'utilizzo di qualunque computer o sistema, interruzione premeditata, corruzione, o distruzione di dati, programmi, o applicazioni, qualunque evento di cyber estorsione; o qualunque altro incidente simile ai precedenti, inclusi quelli che hanno generato una richiesta di risarcimento, azione amministrativa, o procedimento da parte di un'autorità di vigilanza.

Data Breach: una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Analisi di tipo Euristico: è un metodo di rilevazione dei virus basato sull'esame del codice per la ricerca di caratteristiche sospette dello stesso. È stata progettata per individuare virus nuovi e sconosciuti e versioni modificate delle minacce esistenti.

Multi-Factor Authentication (MFA): è uno strumento che aggiunge un livello di protezione al processo di accesso da remoto: gli utenti forniscono un ulteriore verifica dell'identità, come la scansione di un'impronta digitale o l'inserimento di un codice ricevuto per telefono.

Quali sono le misure MFA più efficaci?

1. Hardware token o security key (e.g: Yubikey, Cisco DUO, or other toke with OTP)
2. Software based token (e.g. Symantec VIP, MS/Google authenticator). Questa misura aumenta il grado di protezione se il token viene fornito su un dispositivo diverso da quello utilizzato per effettuare l'accesso (e.g. smartphone, hardware token, etc.)
3. Unique software certificate: il dispositivo viene autenticato attraverso un software specifico installato sul dispositivo stesso.
4. SMS di conferma
5. Riconoscimento biometrico (impronta digitale, iride, scan facciale, etc.)
6. Accesso ai sistemi tramite access provider di terze parti (e.g. CyberArk, Beyond Trust)

Quali sono le misure MFA che <u>NON</u> riteniamo accettabili?

1. Una shared key su VPN: è una chiave fissa, che non cambia mai nel tempo
2. Autenticazione tramite indirizzo IP o MAC address del device
3. VPN (senza MFA)/RDP/SSH/Citrix: garantiscono una connessione sicura tra server e client, ma non l'autenticazione dello utente
4. Autenticazione MFA su base periodica (e.g. l'utente si autentica una volta al mese o alla settimana)

Archiviazione offline o presso ambiente/storage separato: è un metodo di archiviazione dei dati di back up in ambiente disconnesso e separato dal resto della rete.
PCI DSS: è uno standard per la sicurezza informatica sviluppato per prevenire i furti di dati dei titolari di carte di pagamento e rendere più sicure le transazioni online
Normative vigenti: l'insieme di leggi che stabilisce i requisiti e le normative per la raccolta, l'archiviazione e l'utilizzo di informazioni di identificazione personale, informazioni sanitarie personali, informazioni finanziarie di individui e altri dati sensibili che possono essere raccolti da organizzazioni pubbliche o private o da altri individui.
Sandbox: è un sistema che filtra le e-mail con collegamenti URL, allegati o altri file sconosciuti, consentendo loro di essere testati in un ambiente separato e sicuro prima di consentire loro di passare alla rete o ai server di posta.
Sender Policy Framework (SPF): è un metodo di validazione delle e-mail utilizzato per impedire a persone non autorizzate di inviare messaggi, aiuta a proteggere gli utenti e i destinatari e-mail dallo spam e da altre e-mail potenzialmente pericolose.
Informazioni di Identificazione Personale: indica qualsiasi dato che può essere utilizzato per identificare un individuo specifico. Può includere cartelle cliniche o sanitarie di dipendenti o clienti, numeri di identificazione emessi dal governo, credenziali di accesso, indirizzi e-mail, numeri di carte di credito, informazioni biometriche e altre informazioni personali correlate.
Account Privilegiati: Account con profilo di tipo amministrativo o specializzato, con un livello di autorizzazioni maggiori rispetto agli altri Account
Filtro URL o Web (URL Filtering or Web): è una tecnologia che limita i siti Web che un utente o un browser può visitare sul proprio computer, in genere filtrando siti Web dannosi o vulnerabili.
Write Once Read Many: un dispositivo di archiviazione dati in cui le informazioni, una volta scritte, non possono essere modificate.