Proposta contrattuale da **CyberSecure S.p.A.**
per **PharmaLife S.p.A.** Via della Ricerca 56, 20139 Milano (MI), Italia

Progetto di Cybersecurity Integrata e Compliance Normativa

Audit, Implementazione Tecnologica e Formazione per la Sicurezza Informatica

Proposta Contrattuale
Validità: 90 giorni

Destinatario:
Dr. Stefano Lombardi – CIO
s.lombardi@pharmalife.it

Redatta da:
Ing. Martina Rizzi
martina.rizzi@cybersecure.it

Revisionata da:
Prof. Luca Ferrara
l.ferrara@polimi.it

Executive Summary

La presente proposta progettuale, redatta da CyberSecure S.p.A., mira a garantire a PharmaLife S.p.A., azienda leader nel settore farmaceutico, un significativo innalzamento degli standard di sicurezza informatica, assicurando la completa conformità con le più recenti normative europee e nazionali sulla protezione dei dati (Regolamento GDPR e Direttiva NIS2).

In risposta alla crescente sofisticazione e frequenza degli attacchi informatici nel settore farmaceutico, il progetto affronta sistematicamente i principali rischi relativi alla gestione e protezione di dati sensibili dei pazienti e informazioni proprietarie relative alla ricerca e sviluppo, fondamentali per PharmaLife. La strategia proposta è basata su tre pilastri principali:

1. **Audit di Sicurezza Informatica**: Saranno condotte analisi rigorose, penetration test periodici e revisioni approfondite delle policy interne, per identificare tempestivamente vulnerabilità e potenziali punti di accesso sfruttabili da minacce esterne e interne.
2. **Implementazione di Tecnologie Avanzate**: Verranno introdotti strumenti di sicurezza avanzati, tra cui sistemi IDS/IPS (Intrusion Detection/Prevention Systems), soluzioni avanzate per la protezione degli endpoint, firewall di nuova generazione e piattaforme SIEM (Security Information and Event Management) per garantire una difesa proattiva e in tempo reale.
3. **Formazione e Sensibilizzazione del Personale**: Un programma completo e continuativo di formazione mirato a tutto il personale aziendale, attraverso sessioni formative dedicate, simulazioni periodiche di attacchi phishing e la produzione e diffusione di materiale informativo aggiornato, per costruire una cultura della sicurezza consapevole e responsabile.

Gli interventi proposti saranno realizzati nell'arco temporale di quattro mesi, suddivisi in milestone mensili per garantire un costante monitoraggio e una efficace gestione del progetto.

Al termine delle attività, PharmaLife S.p.A. otterrà una documentazione completa e dettagliata sulla compliance normativa e un piano concreto e realistico di interventi correttivi e migliorativi, oltre ad attestati formali per tutte le attività formative effettuate.

La proposta economica complessiva è fissata in 60.000€, con una formula trasparente e pianificata di fatturazione correlata ai risultati raggiunti nelle diverse fasi del progetto. È previsto un periodo di assistenza post-progetto della durata di 180 giorni per assicurare continuità e supporto immediato, eventualmente estendibile.

Questa iniziativa rappresenta un investimento strategico di PharmaLife per proteggere il suo patrimonio informativo e consolidare la sua posizione di leadership attraverso una robusta governance della sicurezza informatica.

1. Contesto Aziendale

PharmaLife S.p.A. rappresenta una realtà di riferimento nel settore farmaceutico italiano ed europeo, specializzata nella produzione e distribuzione di farmaci innovativi e nella ricerca

scientifica avanzata. L'azienda gestisce un ampio spettro di informazioni critiche, che spaziano dai dati altamente sensibili dei pazienti – compresi dati sanitari personali e clinici – fino alle informazioni riservate di proprietà intellettuale derivanti da progetti di ricerca e sviluppo.

La natura sensibile di questi dati impone un alto livello di attenzione e responsabilità nella loro gestione, sia per assicurare la conformità alle rigorose normative europee sulla privacy (GDPR) e sulla sicurezza delle reti e delle informazioni (Direttiva NIS2), sia per garantire la continuità operativa e preservare la reputazione aziendale.

Negli ultimi anni, il settore farmaceutico è diventato un bersaglio prioritario di attacchi informatici mirati, spesso sofisticati e di natura persistente (Advanced Persistent Threats, APT). Tali attacchi sono diretti sia all'acquisizione illecita di proprietà intellettuale sia all'accesso indebito ai dati personali dei pazienti. Questo scenario rende cruciale per PharmaLife un rafforzamento proattivo e continuo della propria infrastruttura di sicurezza informatica.

Inoltre, PharmaLife ha recentemente avviato progetti di digitalizzazione e automazione avanzata dei processi produttivi e amministrativi, aumentando ulteriormente la superficie potenziale di attacco e, di conseguenza, il rischio cyber correlato. L’integrazione di tecnologie IoT e sistemi informatici di gestione della produzione (Manufacturing Execution Systems - MES) richiede soluzioni di sicurezza robuste e specifiche.

Pertanto, il presente progetto intende rispondere concretamente alle esigenze di sicurezza informatica e compliance normativa di PharmaLife, assicurando non solo la protezione completa dei dati, ma anche un vantaggio competitivo attraverso una governance della cybersecurity rigorosa e al passo con gli standard più elevati.

2. Scopo e Obiettivi

L'obiettivo principale del presente progetto è garantire a PharmaLife S.p.A. un livello di sicurezza informatica allineato agli standard internazionali e conforme alle normative vigenti, con particolare riferimento al GDPR (Regolamento UE 2016/679) e alla Direttiva NIS2. Questo intervento mira a proteggere i dati sensibili, prevenire minacce cyber e rafforzare la resilienza dell’infrastruttura IT aziendale.

Le finalità del progetto si articolano in tre obiettivi principali:

1. **Adeguamento Normativo e Conformità**
    - Implementazione di policy e procedure per assicurare la piena adesione alle disposizioni GDPR e NIS2.
    - Verifica e aggiornamento delle misure di protezione dei dati personali e sensibili.
    - Creazione di reportistica dettagliata e documentazione per audit interni ed esterni.
2. **Protezione e Prevenzione da Minacce Cyber**

    - Identificazione e mitigazione delle vulnerabilità attraverso un audit approfondito e penetration testing.
    - Implementazione di strumenti avanzati per la protezione della rete, tra cui IDS/IPS, firewall di nuova generazione e sistemi SIEM.
    - Monitoraggio continuo delle attività anomale per rilevare e neutralizzare tempestivamente eventuali tentativi di attacco.
3. **Cultura della Sicurezza e Formazione del Personale**
    - Organizzazione di sessioni formative su cybersecurity awareness per i dipendenti.
    - Simulazioni periodiche di attacchi phishing per rafforzare la capacità di riconoscimento delle minacce.
    - Redazione di linee guida e best practices aziendali per la gestione sicura delle informazioni.

L'implementazione del progetto fornirà a PharmaLife non solo una protezione efficace contro le minacce informatiche, ma anche una governance strutturata della sicurezza informatica, migliorando la resilienza operativa e la fiducia degli stakeholder.

3. Metodologia e Piano di Intervento

L'approccio adottato per l'implementazione del presente progetto segue una metodologia strutturata, che combina best practice di cybersecurity, framework di sicurezza consolidati (NIST, ISO/IEC 27001) e un piano operativo basato su milestone precise. L'intervento è articolato in tre macro-attività distinte, ciascuna finalizzata a garantire la massima protezione dell'infrastruttura IT di PharmaLife S.p.A.

Attività 1: Audit della Sicurezza Informatica

Questa fase ha l'obiettivo di individuare le vulnerabilità dell'attuale infrastruttura IT e valutare i rischi associati ai sistemi aziendali.

- **Valutazione delle vulnerabilità**: Identificazione di punti deboli nei sistemi, applicazioni e processi.
- **Penetration test periodici**: Simulazione di attacchi mirati per valutare la robustezza delle difese esistenti.
- **Revisione delle policy interne**: Analisi e aggiornamento delle procedure aziendali di gestione della sicurezza.
- **Risk assessment e compliance check**: Confronto con i requisiti normativi (GDPR, NIS2) per determinare eventuali gap.

Attività 2: Implementazione Tecnologica

Una volta identificate le aree di miglioramento, verranno introdotte soluzioni avanzate di cybersecurity per rafforzare la protezione dei sistemi aziendali.

- **Deployment di sistemi IDS/IPS**: Implementazione di strumenti di Intrusion Detection e Prevention per il monitoraggio delle attività di rete.
- **Protezione degli endpoint**: Adozione di soluzioni EDR (Endpoint Detection & Response) per prevenire minacce avanzate.
- **Firewall di nuova generazione e SIEM**: Configurazione di strumenti per la gestione centralizzata degli eventi di sicurezza e la correlazione delle minacce in tempo reale.
- **Segmentazione della rete**: Isolamento dei sistemi critici per ridurre il rischio di compromissioni laterali in caso di attacco.

Attività 3: Formazione e Sensibilizzazione del Personale

L'elemento umano rappresenta spesso il punto più vulnerabile nella catena della sicurezza informatica. Per questo motivo, è fondamentale investire nella formazione e nella consapevolezza del personale.

- **Sessioni formative interattive**: Programmi dedicati a tutti i livelli aziendali per migliorare la comprensione delle minacce cyber.
- **Simulazioni di attacchi phishing**: Test periodici per valutare la capacità di riconoscere e reagire a tentativi di attacco.
- **Redazione di linee guida di sicurezza**: Creazione di documentazione aziendale con best practices per l'uso sicuro dei sistemi IT.

L'intero piano di intervento sarà suddiviso in milestone mensili, garantendo un monitoraggio costante e un miglioramento progressivo della postura di sicurezza di PharmaLife. Alla conclusione del progetto, l'azienda avrà a disposizione una strategia di difesa solida e strutturata, in grado di contrastare le minacce informatiche più avanzate e di assicurare la compliance normativa.

4. Deliverables

Il progetto di cybersecurity integrata per PharmaLife S.p.A. prevede la consegna di una serie di output tangibili, strutturati per garantire trasparenza e tracciabilità delle attività svolte. I deliverables rappresentano il risultato concreto delle tre macro-attività del piano di intervento e forniscono a PharmaLife strumenti operativi e documentali per il mantenimento della sicurezza nel lungo periodo.

Audit e Valutazione della Sicurezza

- **Report di analisi delle vulnerabilità**: Documento dettagliato contenente i risultati del vulnerability assessment con indicazione delle criticità individuate e delle raccomandazioni per la mitigazione dei rischi.
- **Report di penetration testing**: Documento tecnico che descrive i test di attacco simulati eseguiti sui sistemi aziendali, evidenziando i punti di ingresso potenzialmente sfruttabili da un attaccante.

- **Compliance Assessment Report**: Documento che verifica il grado di conformità alle normative GDPR e NIS2, con identificazione di eventuali misure correttive necessarie.

Implementazione Tecnologica

- **Configurazione e Deployment di IDS/IPS**: Implementazione di sistemi di rilevamento e prevenzione delle intrusioni con configurazioni personalizzate per PharmaLife.
- **Installazione e tuning del SIEM**: Setup di un sistema centralizzato per la gestione degli eventi di sicurezza e l'analisi in tempo reale delle minacce.
- **Policy di sicurezza aggiornate**: Redazione e implementazione di nuove policy interne per l'uso sicuro delle risorse IT aziendali.
- **Segmentazione della rete e firewall**: Implementazione di strategie di segmentazione della rete e configurazione avanzata dei firewall per isolare e proteggere i sistemi critici.

Formazione e Sensibilizzazione del Personale

- **Sessioni di formazione e attestati di partecipazione**: Conduzione di workshop su cybersecurity awareness e rilascio di attestati di completamento per i dipendenti coinvolti.
- **Test di simulazione attacchi phishing**: Report sui risultati delle simulazioni di attacco per misurare la risposta degli utenti e definire eventuali azioni correttive.
- **Manuale aziendale di cybersecurity**: Redazione di un documento di riferimento con le migliori pratiche per la sicurezza IT e le procedure da seguire in caso di incidente informatico.

Documentazione Finale e Piani di Continuità

- **Piano di risposta agli incidenti (Incident Response Plan - IRP)**: Documento strategico che descrive il processo di gestione e contenimento di un attacco informatico.
- **Piano di mantenimento e monitoraggio della sicurezza**: Linee guida per il monitoraggio periodico delle misure di sicurezza implementate, inclusa la programmazione di audit futuri.
- **Report finale di progetto**: Sintesi dell'intero intervento, con riepilogo delle azioni svolte, risultati ottenuti e raccomandazioni per il mantenimento della postura di sicurezza aziendale.

Questi deliverables forniranno a PharmaLife una roadmap chiara per la gestione della sicurezza informatica, assicurando la protezione continua dei dati aziendali e la conformità alle normative vigenti.

5. Offerta Economica

L'offerta economica per l'implementazione del progetto di cybersecurity integrata per PharmaLife S.p.A. è strutturata in modo trasparente e modulare, garantendo una chiara visibilità sui costi delle diverse attività e sulla loro suddivisione temporale.

Dettaglio dei Costi

Attività	**Costo (€)**
Audit di Sicurezza Informatica	15.000
Implementazione Tecnologica	35.000
Formazione e Sensibilizzazione	10.000
Totale	**60.000**

Condizioni di Pagamento

Il pagamento avverrà secondo le seguenti modalità:

- **20.000 €** alla sottoscrizione del contratto e avvio delle attività.
- **20.000 €** al completamento dell'implementazione tecnologica.
- **20.000 €** al termine delle attività formative e di sensibilizzazione.

Assistenza Post-Progetto

Per garantire la continuità delle attività e il mantenimento della sicurezza informatica nel lungo periodo, CyberSecure S.p.A. offre un servizio di assistenza post-progetto della durata di **180 giorni** incluso nel costo iniziale.

Successivamente, sarà disponibile un piano di supporto annuale opzionale con i seguenti servizi:

- Monitoraggio proattivo degli eventi di sicurezza.
- Audit periodici e simulazioni di attacco.
- Aggiornamenti e adeguamenti normativi.
- Supporto operativo per incident response.

Costo del piano di supporto annuale: **8.000 €**, IVA esclusa.

6. Conclusioni

L'implementazione del presente progetto permetterà a PharmaLife S.p.A. di ottenere un significativo rafforzamento della propria infrastruttura di sicurezza informatica, garantendo protezione avanzata contro le minacce cyber e piena conformità alle normative vigenti.

Attraverso un approccio strutturato basato su best practice internazionali, l'integrazione di strumenti tecnologici all'avanguardia e un investimento nella formazione del personale, PharmaLife potrà ridurre il rischio di violazioni, migliorare la resilienza operativa e rafforzare la fiducia degli stakeholder nei confronti della sicurezza aziendale.

CyberSecure S.p.A. rimane a disposizione per eventuali chiarimenti e per definire nel dettaglio i prossimi passi verso l'attuazione del piano di cybersecurity proposto.

Per accettazione integrale della presente offerta:

Il Committente

Data

_____