Spett.Le
AGCI SICILIA

Via S. Cuccia 11
90144 Palermo

Oggetto: Proposta Convenzione 2019-2021 Riservata agli Associati

Egr. Presidente Dott. Michele Cappadona, ed Egr.i Consiglieri, con la presente desideriamo sottoporre alla Vostra cortese attenzione una proposta di convenzione da estendere a tutti I Vs. associati della Regione Sicilia.

I dati sono uno dei beni più preziosi per ogni business: analizzati e gestiti in modo efficace, infatti, possono avere un impatto positivo su molti aspetti operativi, dal marketing alle vendite, alla gestione della clientela. Ecco perché mettere in atto puntuali strategie di protezione dei dati è fondamentale per il successo di ogni azienda.

Il cammino verso la sicurezza informatica, in uno scenario in cui le cyber minacce si fanno sempre più aggressive e sofisticate, non è di certo lineare. Occorre prendere in considerazione molteplici aspetti e questo, talvolta, può essere fonte di confusione. Con il GDPR, inoltre, entrato in vigore il 25 maggio 2018, oggi più che mai, diventa di vitale importanza che ogni azienda inizi a rivalutare la propria gestione della sicurezza informatica.

La Cerebro Cyber Security Srls, azienda specializzata nel settore della sicurezza informatica e della informatica forense, propone una convenzione a favore dei Vostri iscritti che volessero dotarsi di sistemi avanzati per la protezione dei propri sistemi informatici aziendali e dei servizi di assistenza correlati.

In particolare, con la presente convenzione, si propone una soluzione avanzata per la protezione dei dati che sono sempre più importanti per ogni azienda, soprattutto alla luce delle nuove regole imposte dal GDPR.

Il prodotto Cerebro permette di elevare i sistemi di protezione a livelli superiori rispetto a quelli già esistenti; infatti le nuove forme di comunicazione, sempre più digitali ed interconnessi, richiedono forme di sicurezza superiore per prevenire e contrastare le nuove mutevoli minacce.

Difesa Informatica Gestita (SOC – Security Operating Center)

La difesa informatica dei dati e della privacy non è più una novità e non è prescindibile per nessuna tipologia o dimensione di azienda.

Cerebro Cyber Security Srls, grazie alla notevole esperienza acquisita sul campo dai suoi soci ed alla disponibilità delle soluzioni Sophos MSP, offre soluzioni avanzate di sicurezza gestita per piccole e grandi realtà imprenditoriali h24/365gg.

In più la nostra modalità di proposta rende la soluzione fiscalmente conveniente: un costo detraibile nell'anno di esercizio a differenza delle licenze acquistate che sono cespiti in ammortamento.

Cerebro Cyber Security Srls - Viale San Martino IS 79 n.261 SC A 98122 Messina P.Iva 03541980839
Email: cerebrocybersecurity@protonmail.com cerebrocybersecurity@pec.it
Social: facebook.com/cerebrocybersec/ Tel. : 346.1885974 / 366.2477486

L M

CEREBRO
cyber-security

Offerta Economica

Sui prodotti, di seguito elencati, sarà applicato uno sconto del **40%** :

Central Intercept X Advanced for Server

Agente Windows Server - Deep Learning Anti-malware, Prevenzione exploit, Protezione attiva contro avversari, CryptoGuard e WipeGuard Anti-Ransomware, Analisi delle cause principali, Whitelisting delle applicazioni [Blocco del server], Protezione dal vivo, Rilevamento del traffico malevolo, Analisi del comportamento / HIPS, Monitoraggio dell'integrità dei file , Sicurezza Web, Download Reputation, Controllo Web, Controllo periferiche, Controllo applicazioni, Prevenzione perdita di dati, Controllo Windows Firewall, Sicurezza sincronizzata, Rimozione malware sicura, Esclusioni scansione automatica, Rilevamento carico di lavoro AWS / Azure Cloud.

Linux Server Agent - Anti-malware, Live Protection, rilevamento del traffico malevolo, sicurezza sincronizzata, rilevamento del carico di lavoro di AWS / Azure Cloud.

Sophos per ambienti virtuali (alternativa a Server Agent completo) - Per i server Windows su VMware ESXi e Microsoft Hyper-V, un agente VM guest leggero scarica la scansione del malware in una VM di sicurezza centralizzata. Anti-malware, Live Protection, rimozione malware.

Central Intercept X Advanced with EDR

Include la scelta di:

- Agente Endpoint: (Windows / macOS) Anti-malware, Protezione dal vivo, Sicurezza Web, Controllo Web, Rimozione malware, Controllo periferiche, Controllo applicazioni, Sicurezza sincronizzata Heartbeat (solo Windows) Analisi del comportamento / HIPS, Prevenzione perdita di dati, Reputazione download, Rilevamento del traffico malevolo, Prevenzione exploit, Cryptoguard Anti-Ransomware, Sophos Clean, Analisi delle cause principali.

- Sophos for Virtual Environments, scansione esterna di Light Agent: (VM desktop di Windows) Anti-malware, Live Protection, rimozione malware

* La funzionalità Security Heartbeat è disponibile quando Endpoint Advanced viene utilizzato insieme a uno dei seguenti abbonamenti di Sophos Firewall: Network Protection, FullGuard o EnterpriseGuard.

Cerebro Cyber Security Srls - Viale San Martino IS 79 n.261 SC A 98122 Messina P.Iva 03541980839
Email: cerebrocybersecurity@protonmail.com cerebrocybersecurity@pec.it
Social: facebook.com/cerebrocybersec/ Tel. : 346.1885974 / 366.2477486

L M

CEREBRO
cyber-security

Central Email Standard

Include: gestito da Sophos Central, Sophos Email blocca gli attacchi di phishing e offre il rilevamento di spam e malware multistrato, insieme alla sincronizzazione di Active Directory, alla casella di posta in arrivo di emergenza e al portale self-service per gli utenti finali.

Central Device Encryption

Include: Gestione della crittografia completa del disco in Sophos Central. Supporta BitLocker su Windows e FileVault su macOS. Ripristino di auto-aiuto con il portale di Sophos Central Self Service.

SafeGuard Enterprise Encryption

Include: Crittografia basata su applicazioni (Crittografia sincronizzata), Crittografia dispositivo SafeGuard, Scambio dati SafeGuard, Crittografia dispositivo nativo SafeGuard, Crittografia SafeGuard per condivisioni file, Crittografia SafeGuard per archiviazione cloud, Crittografia file SafeGuard per Mac, SafeGuard Management Center

Prodotti Hardware

Sull'installazione di hardware Cerebro, come Firewall e Hot-Spot Wifi, si applicherà uno sconto del **30%.**

Altri servizi

Gli interventi sistemistici di bonifica e pulizia delle apparecchiature, saranno espletati senza alcun costo aggiuntivo al contratto

Allegati: 1 (Descrizione Tecnica)

ASSOCIAZIONE GENERALE COOPERATIVE ITALIANE - A.G.C.I.
FEDERAZIONE REGIONALE SICILIANA PALERMO

Cerebro Cyber Security Srls
Lorenzo Malara

Cerebro Cyber Security Srls - Viale San Martino IS 79 n.261 SC A 98122 Messina P.Iva 03541980839
Email: cerebrocybersecurity@protonmail.com cerebrocybersecurity@pec.it
Social: facebook.com/cerebrocybersec/ Tel. : 346.1885974 / 366.2477486

(ALLEGATO 1)

Il tema della cyber security in ambito privato e pubblico, e in generale della messa in sicurezza dello sterminato patrimonio informativo gestito attraverso sistemi informativi più o meno evoluti, comincia finalmente a diventare un argomento di prioritaria importanza.

Vediamone i dettagli.

GDPR, l'accountability investe le aziende private e (anche) la PA

La fisiologica trasformazione dei servizi offerti dai privati, che stanno gradualmente migrando verso canali e modalità di interlocuzione con la collettività sempre più digitali ed informatizzati, ha reso necessario ed urgente l'introduzione di regole certe, omogenee ed in grado di assicurare la massima tutela possibile rispetto alle minacce cibernetiche e ai danni potenzialmente disastrosi che possono derivare da attacchi deliberati o accidentali.

Un primo importante segnale lo ha lanciato la Commissione Europea che, già nel 2016, aveva approvato il Regolamento Generale per la Protezione dei Dati Personali (GDPR), entrato in vigore il 25 maggio 2018, legando in maniera indissolubile i concetti di privacy con quelli di sicurezza dei sistemi di elaborazione e lasciando di fatto il compito di gestire gli aspetti prettamente operativi ad ogni singola organizzazione.

E' fondamentale, in tal senso, rimarcare come il GDPR, introducendo il principio della cosiddetta "accountability", che assegna ai titolari del trattamento responsabilità decisionali ed esecutive sintetizzabili nell'obbligo di adottare comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'efficace protezione dei dati personali, affidi anche a tutti i destinatari pubblici e privati il gravoso compito di decidere autonomamente le modalità, le garanzie e i limiti dei trattamenti, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento stesso.

Le macro-categorie di servizi previsti ed erogati

In dettaglio, la procedura comprende un'ampia gamma di servizi connessi ai temi della cyber-security, che possono essere ricondotti alle seguenti macro-categorie:

Sicurezza applicativa, prevenzione e gestione degli incidenti informatici

Anche attraverso l'analisi delle vulnerabilità dei sistemi informativi, che includono interventi di "Static application security testing" (sicurezza del codice delle applicazioni), "Dynamic application security testing" (sicurezza del software in modalità esecuzione), "Mobile

L M

application security testing" (sicurezza delle applicazioni mobili), secondo quanto descritto di seguito in maniera più analitica.

- L'attività di analisi statica del codice è svolta secondo le best practice internazionali, a partire da quanto previsto dalla metodologia OWASP, ed include almeno i controlli di Data Validation, ossia verifica della presenza di vulnerabilità che possono riguardare eventuali dati corrotti in ingresso e possono condurre a un comportamento anomalo dell'applicazione; Control Flow, che consiste nella verifica dei rischi collegati all'assenza di specifiche sequenze di operazioni che, se non eseguite in un certo ordine, potrebbero portare a violazioni sulla memoria o l'uso scorretto di determinati componenti; Analisi Semantica, che include la rilevazione di eventuali problematiche legate all'uso pericoloso di determinate funzioni o API (come ad esempio le funzioni deprecate); Verifica delle Configurazioni, ossia dei parametri intrinseci di configurazione dell'applicazione; Buffer Validation, che verifica la presenza di "buffer overflow exploitabile" attraverso la scrittura o lettura di un numero di dati superiore alla reale capacità del buffer stesso.
- Le verifiche dinamiche, invece, permettono di controllare i meccanismi di gestione delle sessioni e della loro robustezza; analizzare il sistema di gestione degli errori dell'applicazione; controllare, laddove applicabile, i meccanismi di crittografia; verificare i meccanismi di logging e il metodo di gestione delle informazioni; verificare le comunicazioni dell'applicativo con soggetti esterni come client, DB, LDAP; identificare e rilevare tipologie di vulnerabilità potenziali.

Il test delle app mobili, che consente di verificare il livello di sicurezza delle applicazioni per dispositivi mobile nel corso dell'intero ciclo di sviluppo software, attraverso tecniche di analisi statica e dinamica, include non solo l'analisi del codice e l'esecuzione delle applicazioni ma anche tutte le interfacce verso altri sistemi e/o applicazioni così come altre risorse collegate che potrebbero avere un impatto sulla sicurezza globale del sistema.

Le attività di "vulnerability assessment"

Forniscono una panoramica dello stato di sicurezza dell'infrastruttura e dello stato di esposizione alle vulnerabilità attraverso la raccolta di informazioni concernenti i servizi erogati, l'architettura e le configurazioni del sistema, consentono una verifica dinamica della sicurezza dei dispositivi di rete, allo scopo di identificare eventuali debolezze, configurazioni di sicurezza errate, carenze sui livelli di protezione attivi che espongano il contesto ad attacchi interni ed esterni.

L M

Data loss/leak prevention

Nel perimetro di questa sezione ricade anche il servizio di "**data loss/leak prevention**" (o **DLP**) che, consentendo la protezione dei dati da accessi non autorizzati o violazioni delle policy di sicurezza e riducendo il rischio di perdita, danno o svantaggio competitivo, garantisce supervisione e controllo dei dati indipendentemente dal fatto che siano archiviati o in transito sulla rete ed include attività di monitoraggio e protezione dei dati *in-use* (accesso tramite endpoint – desktop e laptop), *in-motion* (traffico rete) e *at-res* (sui supporti di memorizzazione).

Database security

Le operazioni di "**database security**", infine, includono l'esecuzione di una vasta gamma di controlli della sicurezza per la protezione del database nel suo complesso (dati, procedure o "*funzioni stored*", il sistema di gestione, i server ed i collegamenti di rete associati) allo scopo di salvaguardarne la riservatezza, integrità e disponibilità e consentono la protezione in tempo reale delle basi di dati da minacce esterne o interne oltre che la difesa da eventuali exploit presenti nelle basi dati relazionali.

I servizi professionali e la compliance con il GDPR

Molto interessante ed utile è, infine, la previsione di servizi professionali che possono essere utilizzati, secondo una mappatura, per migliorare il proprio grado di conformità al GDPR attraverso la realizzazione di attività riconducibili a tre fasi:

Fase di Analisi, attraverso la quale è possibile giungere alla predisposizione del "Registro delle operazioni di trattamento", contenente tutte le informazioni richieste dalla normativa ed in particolare dall'art. 30 dell'GDPR, che prevede due tipologie distinte di registri per titolari (con maggiori dettagli) e responsabili esterni (ossia una versione semplificata).

- Fase di Progettazione, che prevede la definizione del Sistema di Gestione dei dati personali, in analogia a quanto previsto da norme internazionali quali lo standard "ISO – 27001", ed in particolare del modello organizzativo, dei processi di "privacy by Design" (articolo 25 del Regolamento), "data breach notification" (articolo 29), "privacy impact assessment" (articolo 35), della modulistica (soprattutto connessa alle informative di cui all'articolo 13, per le quali la normativa introduce rilevanti novità) e del piano di implementazione degli interventi;

L M

CEREBRO
cyber-security

- Fase di Esecuzione, che include il supporto alla stesura di processi e procedure e architetture per la gestione del rischio, l'accompagnamento alle attività di audit e alla gestione dei "data breach", la formazione obbligatoria per il personale (fortemente rivista ed "appesantita", dagli articoli 29 e 32, rispetto alle previgenti disposizioni normative).

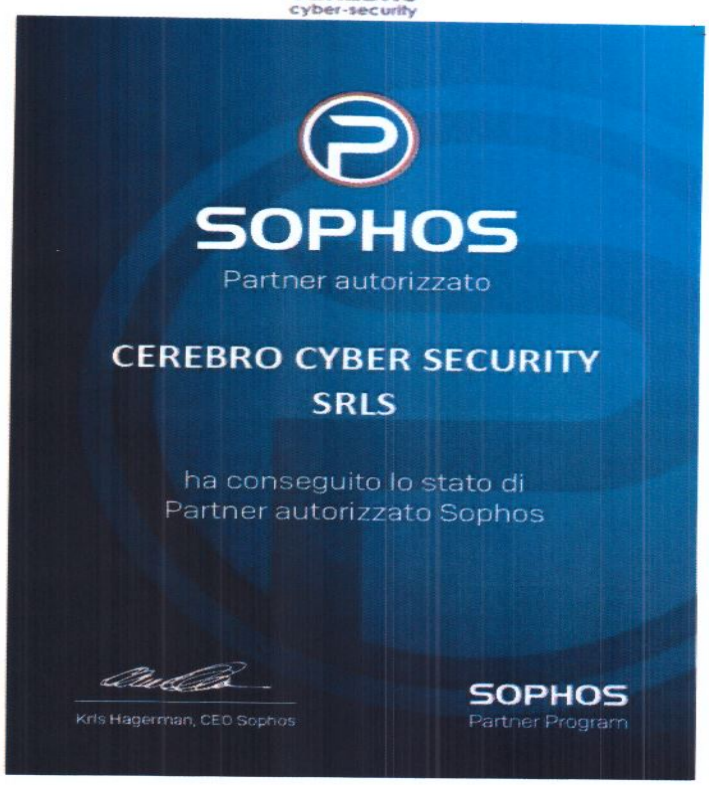
I servizi professionali, inoltre, possono essere sfruttati per ottenere supporto alla prevenzione e gestione degli incidenti informatici, per l'analisi delle vulnerabilità dei sistemi hardware e software; per attività di supporto al Security Operating Center (SOC) di Cerebro; per attività di "penetration test" di tipo applicativo e infrastrutturale; per la crittografia dei dati memorizzati sulle postazioni di lavoro.

Cerebro Cyber Security Srls
Lorenzo Malara

A.G.C.I. - ASSOCIAZIONE GENERALE COOPERATIVE ITALIANE
FEDERAZIONE REGIONALE SICILIANA PALERMO

Cerebro Cyber Security Srls - Viale San Martino IS 79 n.261 SC A 98122 Messina P.Iva 03541980839
Email: cerebrocybersecurity@protonmail.com cerebrocybersecurity@pec.it
Social: facebook.com/cerebrocybersec/ Tel. : 346.1885974 / 366.2477486

CEREBRO
cyber-security



Cerebro Cyber Security Srls - Viale San Martino IS 79 n.261 SC A 98122 Messina P.Iva 03541980839
Email: cerebrocybersecurity@protonmail.com cerebrocybersecurity@pec.it
Social: facebook.com/cerebrocybersec/ Tel. : 346.1885974 / 366.2477486

L M