Relazione GeDInfo per BANDO VOUCHER DIGITALI I4.0- edizione 2019

Gli obiettivi indicati nel progetto sono stati esattamente implementati cosi come descritti nel progetto stesso e nelle offerte dedicate.

Al fine di facilitare la verifica, di seguito si riporta nella colonna di sinistra il testo originale del progetto presentato e nella colonna di destra le note esplicative delle attività svolte.

TITOLO DEL PROGETTO:	
CYBERSICUREZZA AZIENDALE GRUPPO CIMA	
DESCRIZIONE DELL'INTERVENTO: **Backup Remoto (CLOUD)** Consulenza finalizzata alla realizzazione di una soluzione di backup dei dati aziendali, con la possibilità di inviare in CLOUD copia dei dati stessi al fine della messa in sicurezza del patrimonio informativo dell'azienda. Attività necessaria, anche in relazione alla necessità di implementare alcune misure richieste dall'entrata in vigore delle nuove normative sul regolamento generale della privacy (GDPR). Il backup remoto è il processo di conservazione delle copie di backup di dati e applicazioni in una sede geografica diversa da quella in cui risiedono gli originali ed è una pratica essenziale per le aziende, in sua assenza infatti si potrebbe essere costretti a sostenere costi potenzialmente ingenti in caso di prolungata inattività dei sistemi di IT produttivi. La conservazione di dati, documenti e applicazioni essenziali in un unico luogo genera un forte rischio di indisponibilità totale del servizio, qualora si verificasse un guasto come un'interruzione dell'alimentazione, un sabotaggio, un terremoto, una alluvione e così via oppure una infezione di Virus, Malware o Ransomware. Un'interruzione prolungata dei servizi IT potrebbe comportare costi immediati, come mancate opportunità di vendita, e costi a più lungo termine quali danni alla reputazione, erosione della fiducia dei clienti e indebolimento della posizione concorrenziale. Il backup remoto consente quindi di garantire la protezione dei dati e la business continuity, evitando al contempo eventuali perdite di entrate e danni alla reputazione che possono derivare da una consistente perdita di dati e da interruzioni del servizio. Il backup remoto prevede l'esecuzione con cadenza regolare della copia del backup locale nel Data Center di Parma (BTEnia+Lepida).	**ATTIVITA' SVOLTE** L'implementazione del servizio di Backup Remoto (CLOUD) si è definita e conclusa tra i mesi di novembre e inizio dicembre 2019. Il servizio è configurato e attivo. A parte le attività di consulenza necessarie alla progettazione del servizio da integrare nel SIA (Sistema Informativo Aziendale), allo startup del servizio con relativa configurazione dei dati da sottoporre a backup remoto e verifica del corretto funzionamento, si è provveduto a istruire il personale del Cliente in merito a quali sono le comunicazioni da monitorare per avere l'evidenza degli esiti del backup giornaliero e di come sono cambiate le procedure rispetto a quelle precedentemente implementate in azienda.

A seconda dell'RPO (Recovery Point Objective) e dell'RTO (Recovery Time Objective) di una determinata organizzazione, il backup remoto può essere frequente ed esteso, oltre a coinvolgere una vasta gamma di tipi di dati, applicazioni e sistemi.

FIREWALL, SWITCH MANAGED, ANTIVIRUS (CYBERSICUREZZA)

Consulenza finalizzata a garantire maggiori livelli di sicurezza del SIA (Sistema informativo aziendale) sia da minacce esterne che attacchi generati da vulnerabilità interne.

Con anche la possibilità di garantire maggior stabilità di connessione alla rete internet con l'implementazione di un sistema wifi utilizzando un firewall che gestisce 4 access point, l'installazione e configurazione di 3 switch per segmentare la rete aziendale in vlan e separare logicamente e fisicamente la fruizione dei dati, l'aggiornamento della protezione antivirus per server(6) e postazioni di lavoro(45) e quindi garantire meglio la sicurezza ed integrità dei dati aziendali. Con l'eventuale implementazione di una linea di connettività aggiuntiva e quindi garantire l'operatività dei sistemi e dell'azienda.

La consulenza erogata riguarda la definizione corretta dei bisogni aziendali, l'individuazione della soluzione tecnica più adeguata, la scelta della migliore offerta presente sul mercato, il rendere edotti gli operatori aziendali alle opportunità offerte dalla soluzione implementata e il renderli il più possibile autonomi nella gestione di quanto a loro disposizione, e naturalmente il monitoraggio e la consulenza/assistenza a garanzia della funzionalità del servizio.

La soluzione proposta si basa sulla configurazione di filtri sulla navigazione sia da dispositivi mobili, sia da computer.

Potranno essere applicati filtri in base alla tipologia di siti\servizi che si vorranno bloccare.

Verrà fatta distinzione tra rete dedicata agli operatori, e rete dedicata agli ospiti, ogni attività di comunicazione da e verso le reti verrà monitorata e gestita tramite regole.

Potranno essere applicare regole per dare priorità ai protocolli utilizzati per la comunicazione di posta elettronica.

Potrà essere configurata un'eventuale linea aggiuntiva o di backup.

OBIETTIVI E RISULTATI ATTESI:

Le attività di consulenza sono state svolte presso il cliente, da almeno 2 tecnici, per quanto riguarda le attività di installazione, configurazione, messa in esercizio, test, verifica funzionale, assistenza e manutenzione costante.

Sono partite alla consegna del materiale e sono state erogate settimanalmente, con diversi carichi di lavoro. Le attività di consulenza dedicate al materiale acquistato ed ai servizi grazie ad esso erogati, continuano tuttora. Sono legate in particolare a monitoraggio del corretto funzionamento degli apparati stessi e dei servizi in essere e all'assistenza/manutenzione generata degli eventuali problemi intercettati dai nuovi strumenti di sicurezza o dalle esigenze legate ad essi richieste del personale aziendale.

Questo ha comportato oltre alle normali attivazioni e configurazioni fatte sulle singole postazioni di lavoro, anche attività di istruzione del personale al fine di comprendere e gestire eventuali nuove procedure imposte dall'inserimento in azienda dei nuovi prodotti/servizi. In particolare per l'Antivirus.

Migliorare e rafforzare l'intero sistema di sicurezza aziendale con l'implementazione di servizi e di dispositivi aggiornati dal punto di vista tecnologico e nel rispetto delle normative vigenti. Conseguente coinvolgimento del personale addetto nelle attività di gestione e comunicazione di tutte le nuove opportunità offerte.	
TECNOLOGIE OGGETTO DI INTERVENTO PER L'ATTIVITA' DI CONSULENZA con esplicita indicazione relativa a quali tecnologie, tra quelle previste all'art. 2, comma 3, della parte generale del presente Bando, esso si riferisce:	
Cloud, Cybersicurezza e business continuity	
TECNOLOGIE OGGETTO DI INTERVENTO PER IL PERCORSO FORMATIVO con esplicita indicazione relativa a quali tecnologie, tra quelle previste all'art. 2, comma 3, della parte generale del presente Bando, esso si riferisce:	
Consulenza all'utilizzo corretto necessaria agli operatori addetti all'utilizzo dei sistemi installati e del servizio implementato, (Cloud, Cybersicurezza e business continuity). Una volta installati gli apparati acquistati, opportunamente configurati e attivati i servizi relativi, si potrà procedere alla individuazione del personale da formare. Questo in relazione anche delle responsabilità assegnate dal Titolare del trattamento dei dati aziendale o suoi incaricati come prevede il GDPR. Le persone coinvolte nel percorso formativo verranno informate e istruite all'uso degli apparati e dei servizi, al loro monitoraggio, all'uso e all'eventuale attivazione dell'assistenza in caso di alert, guasti o blocco dei servizi stessi. Si prevedono diverse sessioni formative d'aula con il personale interessato, e la messa a disposizione di documentazione dedicata prodotta ad hoc per l'azienda.	
RIPORTARE UNA SINTETICA DESCRIZIONE DEI BENI E SERVIZI STRUMENTALI DA ACQUISTARE, CON L'INDICAZIONE DELLE TECNOLOGIE COME DA ELENCO 1 ED ELENCO 2, (art. 2 *comma* 3 della parte generale del bando) A CUI SI COLLEGANO:	

DESCRIZIONE DELLA TECNOLOGIA ACQUISTATA/DA ACQUISTARE	Indicare a quali Tecnologie di cui Elenco 1 ed Elenco 2, tale acquisto si riferisce
ACCESS POINT (4) : SOPHOS AP15 REV.1 ACCESS POINT (ETSI) WITH MULTIREGION POWER	cybersicurezza e business continuity
FIREWALL (1) : XG 115W REV.3 TOTALPROTECT, 3-YEAR (EU/UK/US POWER CORD)	cybersicurezza e business continuity
SWITCH (3) : 24PT GIGABIT SMART SWITCH	cybersicurezza e business continuity
Antivirus Server (6) : CL SRV PROT STD-5-9 SRV 36	cybersicurezza e business continuity
Antivirus Client (45) EP PR STD-CUP-25-49 US-36M	cybersicurezza e business continuity
Backup remote in CLOUD (1) : BRaaS – Backup e Restore as a Service	Cloud