BANDO VOUCHER DIGITALI I4.0 - ANNO 2019

RELAZIONE CONCLUSIVA DELLE ATTIVITÀ

DENOMINAZIONE IMPRESA CONTAINERS FIDENZA CONSORZIO C.F./P.IVA 00908430341

INDIRIZZO SEDE LEGALE IMPRESA PIACENZA (PC) VIA F. COPPALATI 6 CAP 29122 FRAZIONE: LE MOSE

LEGALE RAPPRESENTANTE/TITOLARE IMPRESA

A seguito della domanda relativa alla richiesta di contributo del "Bando Voucher Digitali I4.0 anno 2019" con la quale questa impresa ha previsto la realizzazione dei seguenti obiettivi:

- ottenere un'analisi approfondita sui propri sistemi informatici al fine di comprendere i livelli di rischio in ambito di sicurezza informatica e definire un piano di mitigazione dei rischi e per l'adeguamento dei processi interni aziendali, mediante la futura adozione di strumenti tecnologici innovativi.
- individuare gli interventi necessari e progettare l'adozione di misure di protezione su vari livelli per prevenire il furto e la perdita di dati sensibili e, conseguentemente, di danni sia a livello economico sia produttivo.
- Definire una serie di procedure interne e introdurre in azienda strumenti in grado di offrire una protezione avanzata dei dati intra aziendali ed extra aziendali

Sono state svolte, presso la sede sita a Piacenza (PC) in Via F. Coppalati, 6 le seguenti attività:

Con riferimento al primo obiettivo, è stato svolto un check up completo dell'infrastruttura ICT presente in azienda, con particolare riferimento alle soluzioni tecniche ed alle dotazioni tecnologiche adottate per garantire la sicurezza dei dati informatici. Con il supporto del consulente sono state individuate le seguenti lacune ed indicate le relative azioni correttive da intraprendere:

1. **Implementare politica di disaster recovery e backup dati pc amministrativi**

Nella sede di Piacenza vengono gestiti tutti i flussi di tipo amministrativo e finanziario del gruppo Container Fidenza. Dalle analisi e interviste effettuate presso l'azienda è stato rilevato che molti utenti tendono a salvare localmente sulle postazioni di lavoro file/documenti anziché utilizzare le apposite share di rete ad accesso protetto condivise con la struttura Cloud.
Sono state indicate le procedure corrette per il salvataggio e la condivisione in quanto la perdita di queste informazioni comporterebbe un danno significativo all'azienda e, in aggiunta al back up, è stato consigliato di implementare un sistema di backup delle singole macchine con schedulazione giornaliera.

Prima dell'intervento in oggetto, la rete era protetta da un firewall hardware di vecchia generazione. È stato introdotto e configurato un nuovo firewall Watchguard con licenza UTM per la protezione attiva dalle potenziali minacce.

Infine, con riferimento alla gestione dei backup, sono state illustrate le procedure e le modalità di effettuare alcuni test di ripristino dati e simulare un disaster recovery al fine di verificare tempi, modalità e procedure attuabili in caso di malfunzionamenti o perdite dati del sistema IT.

2. **Aggiornamenti software programmati**

Sulle postazioni di lavoro è stato riscontrato che sono installati software di terze parti non aggiornati: JAVA, MICROSOFT OFFICE. Si consiglia aggiornamento periodico per evitare problemi legati alla sicurezza e bug.

3. **Cablaggio strutturato rete Lan e armadio rack**

A seguito del sopralluogo svolto consigliamo all'azienda la sistemazione dell'armadio rack verificando l'affidabilità dei gruppi di continuità presenti nell'area CED.

Per quanto riguarda il cablaggio della rete consigliamo la rimozione dei vari switch presenti sotto alle scrivanie e di collegare direttamente gli apparati al patch pannel. Si consiglia inoltre di sostituire tutti i cavi e frutti di rete con cavo di categoria 6.

Data 20/12/2019

Firma digitale legale rappresentante