



Microbyte di Massa Elio
Via Piero Gobetti 7 - 12100 CUNEO
Tel/fax 0171/480074 - Cell. 0335/266422
P.ta Iva 02476280041 C.Fisc. MSSLEI57C10D205U
www.eliomassa.it – email info@eliomassa.it

Spett.le
Comune di Cervasca
Via Roma 34
12100 CERVASCA (CN)

Cuneo lì 27/12/2017

RELAZIONE SULLO STATO DELLA SICUREZZA INFORMATICA COMUNALE

In relazione al quadro normativo sulle misure minime ICT per la sicurezza informatica si descrive la situazione attuale del Comune di Cervasca e le modifiche da apportare per l'adeguamento alla direttiva del Consiglio dei Ministri del 26 aprile 2016.

La direttiva verte principalmente su 5 argomenti:

- 1) Inventario dei dispositivi e dei software presenti nella struttura informatica.
- 2) Protezione delle configurazioni dei computer
- 3) Valutazione e correzione delle vulnerabilità software
- 4) Difese contro i malware
- 5) Copie di sicurezza e loro protezione

- 1) Inventario dei dispositivi e dei software presenti nella struttura informatica.

L'inventario dell'hardware, completo di indirizzi ip, porte di commessione allo switch, descrizione dell'hardware ed utilizzatore abituale della postazione è presente da sempre nel Comune, redatto manualmente dal sottoscritto ed aggiornato ogniqualvolta si verifichi un cambio di dispositivo hardware.

L'inventario del software presenti sui pc invece non esiste ed è da realizzare. Questo inventario verrà realizzato tramite il software gratuito Ocs Inventory
Non si prevedono quindi spese per questo punto.

- 2) Protezione delle configurazioni dei computer

I computer sono utilizzati normalmente da utenti senza diritti di amministratore

In caso ci sia necessità d'installare software o modificare le configurazione dei pc client ogni utente ritenuto informaticamente preparato per tale attività è stato dotato di un secondo utente con diritti di amministratore.

Non viene effettuata copia dell'immagine dell'hard disk dei Pc Client in quanto la compromissione di tali Pc avviene rarissimamente (ad oggi è successo una volta in 30 anni) e sarebbe quindi troppo dispendioso effettuare mensilmente copie d'immagine di ogni pc.

Si opta quindi, in caso di compromissione, per la totale formattazione e reinstallazione del sistema operativo e dei programmi preesistenti.

I dati utente vengono tutti giornalmente salvati in copia sul server e sono quindi ripristinabili senza problemi.

3) Valutazione e correzione delle vulnerabilità software

Le vulnerabilità che si creano nel sistema operativo o nei software residenti vengono monitorate periodicamente mediante il software Retina CS Community ed in caso di loro presenza viene immediatamente applicata la patch di sicurezza.

Gli operatori sono normalmente istruiti per l'installazione degli aggiornamenti di sistema operativo (windows update) ogni secondo martedì del mese e per gli aggiornamenti di sicurezza degli altri software presenti sul pc quali, principalmente, Java, Flash Player ed Acrobat Reader.

Il software Retina CS è gratuito

4) Difese contro i malware

Su ogni postazione è installato l'antivirus Kaspersky Endpoint ad aggiornamento automatico giornaliero.

Non si ritiene necessario installare altri software.

I firewall presenti in windows sono attivi su tutte le postazioni

L'antivirus Kaspersky è a pagamento ed ha una licenza di durata triennale che viene rinnovata alla scadenza.

La scadenza prossima sarà in data 11/06/2020 e pertanto al momento non si prevedono spese.

5) Copie di sicurezza e loro protezione

Le copie di sicurezza vengono effettuate dal server, di notte, su 4 supporti diversi.

Programmi e dati sono dislocati sul disco D: del server ed occupano al momento 385 GB

Oltre alle copie del giorno vengono mantenute anche copie storiche, utili in caso di cancellazione accidentale di file o cartelle da parte degli operatori di cui gli operatori stessi non si accorgano immediatamente.

Le copie storiche sono mantenute, non su tutti i supporti, in ragione di:

Una copia giornaliera per gli ultimi 5 giorni

Una copia settimanale per le ultime 5 settimane

Una copia mensile per gli ultimi 12 mesi

I supporti su cui vengono effettuate le copie sono i seguenti

1) N. 1 disco interno al server, non condiviso in rete, con capacità da 8 TB

Su questo disco vengono effettuate le 5 copie giornaliere, 2 settimanali e le 12 mensili

2) N. 2 dischi esterni usb 3.0 da 4 TB ciascuno non condivisi in rete.

Questi dischi vengono alternati settimanalmente, uno viene collegato al server al 1° piano mentre il secondo viene custodito nella cassaforte dell'anagrafe al piano terreno in modo da avere una robusta protezione in caso di terremoto ed una discreta distanza dal server in caso d'incendio.

Su questi dischi vengono salvati sia le 5 copie giornaliere che le 5 settimanali.

3) N. 1 spazio di archiviazione sul server cloud di siscom dislocato presso il data center di Rozzano (MI)

Su questo cloud viene effettuata un'unica copia, ogni notte

Lo spazio attualmente acquistato sul cloud è di 250 GB, per cui vengono solo copiati i dati ed i programmi di Siscom e di Technical Design, mentre non vengono copiate tutte le cartelle dei documenti e delle foto.

E' opportuno chiedere un preventivo a Siscom per portare le dimensioni dello spazio cloud da 250 a 500 GB in modo da poter salvare anche tutti i documenti.

Ritengo opportuno acquistare anche un apparato Nas, da dislocare nella biblioteca nuova in modo da poter eseguire, ogni notte, le copie degli ultimi 5 giorni.

Il fatto di posizionare il apparato Nas in biblioteca è utile, in caso d'incendio, per avere una copia in un locale diverso dal fabbricato comunale.

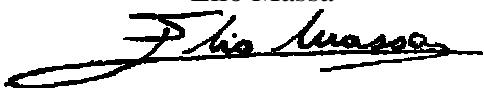
Il costo di un Nas con 2 hard disk in raid 1 da 2 TB è di circa 500 euro + iva

Con il Nas e l'ampliamento del cloud ritengo completa la configurazione delle copie di sicurezza, anche a livello di copie storiche.

Resto a disposizione per ulteriori informazioni.

Cordiali saluti

Elio Massa

A handwritten signature in black ink, appearing to read "Elio Massa".