Flor
INFORMATICA

Spett.le

COMUNITA' DELLA VALLE DI CEMBRA

PIAZZA S. ROCCO NR. 9

38034 CEMBRA LISIGNAGO TN

Relazione dell'amministratore di sistema riferita all'anno 2023

Relativamente all'incarico di Amministratore di Sistema dell'Ente Comunità della Valle di Cembra (contratto nr 27/2023 valido fino al 30/09/2026) ed in particolare al compito di riferire alla Comunità della Valle di Cembra sullo svolgimento dei compiti svolti, mediante presentazione di relazione degli interventi effettuati corredata dalla dimostrazione di conformità a tutti i suoi obblighi in materia di protezione dei dati personali, è stata eseguita una verifica e mappatura della struttura informatica dell'Ente al fine di garantire il regolare funzionamento dell'infrastruttura tecnologica e il corretto utilizzo della stessa da parte degli utenti interni ed esterni alla rete. La relazione fornisce inoltre una panoramica sui livelli di sicurezza e di protezione dei dati.
La presente relazione intende illustrare le principali attività svolte nel corso del 2023, i problemi riscontrati e le relative soluzioni adottate, nonché sottoporre all'Ente proposte di miglioramento.
L'amministratore di sistema ha adottato una serie di misure generali per proteggere i dati personali dell'Ente, in particolare:

- Limitazione dell'accesso ai dati solo al personale autorizzato
- Aggiornamento delle politiche di sicurezza dei dati personali
- Analisi dei rischi per identificare eventuali vulnerabilità del sistema
- Utilizzo di password complesse e sicure
- Backup regolari dei dati
- Crittografia dei dati in transito e di storage (chi lo fa?)
- Monitoraggio costante delle attività
- Segnalazione delle criticità riscontrate
- Proposte di miglioramento
- Supporto per la gestione di eventuali violazioni dati personali
- Formazione del personale in materia di cybersecurity

DESCRIZIONE DELL'INFRASTRUTTURA

RETE: nella rete sono presenti circa 25 pc che sono tutti collegati al dominio. Il server si trova in cloud, sull'infrastruttura di trentino digitale. Ogni pc è dotato di antivirus, mentre a protezione della rete è presente un firewall Sophos.

SOGGETTI/DITTE ESTERNE CHE ACCEDONO ALLA RETE: ad es. Trentino Digitale per connettività

FIGURE INTERNE INCARICATE CON RUOLI SPECIFICI: non esistono persone interne incaricate

SERVER FISICI: non in possesso, l'Ente usufruisce del servizio in cloud fornito da Trentino digitale

SERVER VIRTUALI: CVC-DC2k19(WINDOWS SERVER 2019)

BACKUP: è responsabile per questa parte Trentino digitale

DISASTER RECOVERY: è responsabile per questa parte Trentino digitale

CONNETTIVITÀ: Linea TELPAT privata e una linea pubblica entrambe di trentino digitale

CONNESSIONI PER L' ACCESSO DA REMOTO: l'accesso da remoto è possibile sui pc, solo agli utenti autorizzati tramite VpnSSL

CREDENZIALI DI ACCESSO/GESTIONE DEI PERMESSI UTENTE SULLE CARTELLE E LORO DISMISSIONE: tempistica/procedura per la verifica dei profili da rimuovere ogni 90 giorni vanno rinnovate; ci sono cartelle con permessi esclusivi

AGGIORNAMENTI DI SICUREZZA AUTOMATICI: aggiornamenti automatici attivati di default su tutti i dispositivi, anche se per l'installazione di patch di software specifici potrebbe essere necessario l'intervento dell'operatore

Sono stati effettuati test di vulnerabilità e analisi del rischio per individuare eventuali punti deboli nella rete e nelle applicazioni?

a) Sì ☐
b) No ☒
c) Altro: .....

Sono state aggiornate tutte le patch di sicurezza dei sistemi operativi, delle applicazioni e dei dispositivi di rete?

a) Sì ☒
b) No ☐
c) Altro: .....

Sono state attuate politiche di sicurezza robuste, come l'utilizzo di password complesse, l'attivazione della crittografia dei dati sensibili e la restrizione degli accessi privilegiati?

a) Sì ☒
b) No ☐
c) Altro: l'utilizzo di password complesse e la restrizione degli accessi privilegiati sono attivati

Sono state implementate, dove possibile, delle politiche di accesso a sistemi, applicazioni, dati ecc., basate sui principi del "meno privilegiato" e della "necessità di conoscenza".

a) Sì ☒
b) No ☐
c) Altro: .....

Sono stati eseguiti backup regolari e test di ripristino per garantire la disponibilità dei dati in caso di necessità e/o incidenti?

a) Sì ☐
b) No ☐
c) Altro: è responsabile per questa parte Trentino digitale

Sono stati implementati metodi di sicurezza nella configurazione della rete wi-fi? (Ad esempio Nat e log di traffico)

a) Sì ☒
b) No ☐
c) Altro: sono presenti 2 access point sophos, dove sono state create 3 reti wifi distinte:

- CVC-236: rete delle comunità ad uso solo degli operatori della comunità
- CVC-Ospiti: wifi usato per gli utenti esterni che hanno necessità di utilizzare internet. È stata creata una rete separata da quella principale per una maggiore sicurezza.
- WifiSAT: wifi ad uso esclusivo degli utente della SAT. È stata creata una rete separata da quella principale per una maggiore sicurezza.

Sono stati aggiornati i criteri di accesso alla rete locale (Ad esempio per utenti non più in servizio)

a) Sì ☒
b) No ☐
c) Altro: gli utenti non più in servizio devono essere segnalati all'amministratore che provvede a disattivarli

È stata consegnata la configurazione relativa alla rete, completa di nome utente e password amministrativa?

a) Sì ☒
b) No ☐
c) Altro: sono state consegnate le credenziali amministrative della rete

È stato aggiornato l'elenco dei software in black list?

a) Sì ☒
b) No ☐
c) Altro: gestito automaticamente dal farewall

Sono stati configurati e aggiornati tutti i sistemi operativi e i software con patch di sicurezza e qualsiasi altro correttivo al fine di contenere le vulnerabilità di sistema?

a) Sì ☒

b) No ☐
c) Altro: .....

Il sistema firewall hardware è stato correttamente aggiornato ed implementato con nuovi plug-in di sicurezza necessari per aumentare il grado di protezione della rete?

a) Sì ☒
b) No ☐
c) Altro: .....

È stato aggiornato l'elenco dei siti web in black list?

a) Sì ☒
b) No ☐
c) Altro: .....

Sono stati forniti ai dipendenti corsi di formazione sulla sicurezza informatica e sono state adottate politiche di utilizzo responsabile della rete e degli strumenti informatici?

a) Sì ☐
b) No ☒
c) Altro: .....

Il firewall hardware, se presente, è stato aggiornato e configurato per garantire un livello elevato di controllo sulla rete senza l'utilizzo di tracciamento dati relativi agli utenti?

a) Sì ☒
b) No ☐
c) Altro: .....

Sono stati implementati piani futuri per migliorare la sicurezza informatica dell'Ente?

a) Sì ☐
b) No ☒
c) Altro: si procederà alla sostituzione di tutti i PC con windows 10 e office 2019 entro ottobre 2025

È presente un "Piano di Disaster Recovery"?

a) Sì ☐
b) No ☒
c) Altro: è responsabile per questa parte Trentino digitale

È stata effettuato una valutazione del rischio informatico nell'ultimo anno?

a) Sì ☐
b) No ☒
c) Altro: ma l'amministratore di sistema si mette a disposizione per effettuare l'intervento se richiesto

SEGNALAZIONI, PROPOSTE DI SVILUPPO E MIGLIORAMENTO

Si consiglia all'Ente di procurarsi dei software per la valutazione del rischio informatico (vulnerability assesment)

CONCLUSIONI

L' amministratore di sistema ritiene che le misure adottate siano adeguate per garantire la sicurezza dei dati personali degli utenti. In caso di eventuali cambiamenti normativi o tecnologici, l'amministratore di sistema si impegna a revisionare le politiche e le misure di sicurezza esistenti per garantire la conformità continua al GDPR.

Cles, 26/09/2024

Firma dell'amministratore di sistema

Luca Lorgalli