Misure esistenti o pianificate per il canale di segnalazione interna YESNOLOGY

Patch management

I sistemi utilizzati dal fornitore del canale sono sottoposti a regolare processo di patch management che permette di sanare tempestivamente le vulnerabilità rilevate. La piattaforma Azure si auto-aggiorna. Per quanto riguarda il software di terze parti utilizzato per lo sviluppo della piattaforma, il fornitore effettua periodicamente un aggiornamento mano a mano che vengono rilasciate nuove release.

Controllo degli accessi

Il fornitore del canale:
- dispone di un sistema di videosorveglianza perimetrale
- ha formalizzato la procedura di accesso nella struttura in modo da sapere in ogni momento chi è presente all'interno della stessa.

Archiviazione atti e documenti

La documentazione cartacea è conservata e custodita all'interno di contenitori chiusi a chiave e accessibili solo a personale autorizzato.

Sicurezza della rete

Il fornitore ha implementato misure di sicurezza atte a contrastare attacchi malevoli adottando firewall, sistemi antivirus, antispam. I sistemi sono aggiornati periodicamente.

Sicurezza logica degli accessi

Il fornitore ha disciplinato le modalità di accesso agli strumenti elettronici, il loro utilizzo e la gestione delle password.

Sicurezza dei dati

Tutte le trasmissioni dei dati avvengono tramite protocolli di sicurezza cifrati (SSL/HTTPS).
La piattaforma YesNology implementa diversi livelli di cifratura dei dati. Tutte le API sono accessibili solamente in forma crittografata HTTPS. I database sono crittografati sia a livello di file system (file di database) sia a livello di campi laddove vengano memorizzati dati "particolari".

Software malevolo

Il fornitore del canale di comunicazione utilizza host, client e server su cui sono installati software anti malware costantemente aggiornati in grado di identificare e bloccare software malevoli. I PC

client del fornitore sono protetti da antivirus Norton e i dischi sono crittografati con BitLocker. L'ambiente Azure è protetto per definizione con strumenti di protezione standard. Il fornitore ha adottato un sistema serverless, quindi senza server e/o macchine virtuali pertanto non è possibile installare software malevolo. Il fornitore ha inoltre introdotto dei sistemi di logging che consentono di tener monitorato gli accessi alle routine riservate del software (vedi ad esempio gli accessi a MailUp e ai database). Per una maggior sicurezza il fornitore ha crittografato ulteriormente le routine in modo tale che anche in caso di accesso non si riescano a reperire le credenziali dei suddetti servizi.

Backup dei dati e ripristino

Il fornitore del canale interno adotta procedure giornaliere per il backup dei dati e il ripristino degli stessi. Il backup avviene in locale. Il backup dei dati (database) avviene ogni 5 minuti ed in modo automatico. Non avviene in locale ma direttamente sulla piattaforma Azure. Il periodo di retention delle copie è di 7 giorni. Questo significa che il fornitore può tornare indietro nel tempo per al massimo 7 giorni. Periodicamente il fornitore effettua una copia in locale sul proprio NAS, la procedura è utilizzata per individuare eventuali bug e sarà dismessa all'occorrenza. Da sottolineare che i backup contengono dati crittografati quindi anche un eventuale ripristino comporterebbe l'inaccessibilità ai dati "sensibili" se non si è in possesso delle chiavi di crittografia.

Gestione degli incidenti

Il fornitore del canale è dotato di procedura per la gestione degli incidenti che prevede:
- analisi dell'incidente (cause e impatto complessivo)
- produzione di un report (riepilogo e cronologia dell'incidente)
- indicazione delle misure adottate

In definitiva dal momento in cui si manifesta un problema il fornitore si attiva per cercarne la causa. Qualora sia necessario effettuare un ripristino del database, se possibile, salva i dati allo stato attuale prima del ripristino per valutare eventuali dati che andrebbero persi. Eventuale documentazione viene prodotta dal fornitore manualmente.

Analisi generale e preliminare

Il fornitore del canale ha eseguito in relazione alla piattaforma Yesnology un'analisi preliminare in merito a:
- progettazione della piattaforma secondo un approccio volto al perseguimento, nei limiti del possibile, di principio di data protection-by-design e by-default
- mappatura delle tipologie di utenti interessati
- mappatura delle finalità del trattamento della piattaforma (ferme restando le finalità del titolare del trattamento)
- allocazione dei ruoli
- censimento basi giuridiche e tempi di conservazione nelle attività in cui è titolare del trattamento
- analisi del rischio

Individuazione dei soggetti autorizzati al trattamento con attibuzione di funzioni e compiti

Tutti i soggetti autorizzati vengono designati con apposito atto di nomina

Istruzioni alle persone autorizzate al trattamento

Il titolare fornisce procedure ed istruzioni scritte agli autorizzati e li vincola alla riservatezza

Sottoscrizione contratti ex art.28 del GDPR

Il titolare ha regolato i rapporti con i responsabili del trattamento mediante idonei contratti ex art. 28 GDPR.

Formazione degli autorizzati al trattamento, dei ruoli apicali e dei collaboratori

Viene garantita la formazione periodica degli autorizzati del trattamento e dei ruoli apicali che operano nella società.