Documento	ISTRUZIONE OPERATIVA SUL "DATA BREACH"
Classe / tipologia	RAPPORTO OPERATIVO/ Politiche della Sicurezza privacy e PD
Adempimenti	PROVV. "**DATA BREACH**" 2/7/2015 - Artt. **32 e 33 REG.679/16**
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, **RV-DB01**, DVR/IP, **DP-PG679**
Basi giuridiche	Piano di adeguamento 2018-19 con migrazione dal Codice Privacy

CONTENUTI

- Rapporto Operativo delle Misure ICT Data Breach
- ANNESSO A – copia del *journalling* delle attività associate al Rapporto Operativo

Il presente Rapporto spiega tipologicamente quali misure ICT sono state adottate a fronte dei rischi informatici legati ai trattamenti individuati nei trattamenti per garantire la "massima" protezione e prevenzione agli incidenti informatici previsti dal provvedimento "Data Breach". Tutti gli elementi del *Report* sono associati al verbale dell' **Annesso A**

Continuità elettrica apparati critici

Una unità UPS è stata installata e configurata tramite connessione USB al Server principale dell'armadio tecnico della Azienda. Il dimensionamento dell' UPS è stato calcolato in modo da garantire il dopiio dell'assorbimento richiesto rispetto alle specifiche tecniche elettriche del Server principale di LAN (vedi censimento HW)

Anti-intrusione e videosorveglianza in sede

Un impianto di antifurto IR è installato in tutti i punti di controllo delle aree di lavoro della sede. L'impianto anti-intrusione non è collegato o interattivo con gli apparati ICT. Nessuna Video Sorveglianza è installata alla data di rilascio di questo rapporto.

Controllo di accesso fisico

Tutti gli ambienti fisici dei locali di trattamenti cartacei sono controllati e dotati di serramenti meccanici in dotazione ai Soggetti Autorizzati secondo mansionamento e istruzioni di formazione da loro sottoscritte in sede di nomina/designazione/delega.

Controllo degli apparati WI-FI

Gli apparati Access Point come ripetitori (APs) della connessione wi-fi aziendale sono posti ad altezza e/o inseriti in mobili con serramento. Durante le ore di ufficio gli APs sono posti in aree normalmente presidiate e/o sorvegliate.

Tutti gli APs sono stati configurati in modo proprietario rispetto alla dotazione di fabbrica. Le chiavi crittografiche sono conservate in un sistema Vault Digitale la cui Master Pass-phrase è nelle disponibilità dei soli ADS e del TDT

☐	TITOLARE	.....
☐	RESPONSABILE	.....
☐	TEAM DI LAVORO	.....
☐	ADS / DBA	.....

Licenze SW e aggiornamenti di sicurezza

Tutto il SW aziendale, sia esso di Sistema o applicativo, è acquistato con licenze di utilizzo proprietarie e con contratto automatico di rinnovo e aggiornamento di sicurezza.

Il c.d. "Patches Management", è comunque oggetto di revisione / supervizione su base annuale e/o in occasione delle scadenze di rinnovo delle Licenze. Sia ADS/DBA informano il TDT su base almeno annuale circa indicenti e/o malfunzionamenti e/o anomalie di fornitura

Sicurezza ICT perimetrale

Tutto il flusso del traffico di connettività (entrata/uscita e WAN/LAN) è sottoposto ad un controllo di *appliance* continuo su un dispositivo Firewall. Oltre alle *appliance* del produttore per Data Loss Prevention (DLP) e monitoraggio IDS/IDP/IPS sono state opportunamente applicate politiche di:

- ***DHCP statico (associazione IP / MAC-address)***
- ***Instradamenti NAT (Network Address Translation) di segmentazione di rete secondo toponomastica aderente ai vari operatori/funzioni aziendali***
- ***Instradamenti PAT (Port Address Translation) secondo protocolli di servizi critici quali RDP/TV/DBserver***
- ***Black e White lists per le URL di navigazione***
- ***Community Registry: WOT, GHOSTERY, uBLOCK su tutte le stazioni di lavoro***

NOTA: La classe di Firewall adottata è di tipo UTM con *Pattern Recognition*, quindi anche tutto il traffico legato alla posta elettronica corporativa, è posto sotto misure di sicurezza adeguate (anti-virus, antispam, signature malware ecc.)

Copie di Sicurezza e storicizzazioni di Dati e Sistemi

Ai fini delle procedure adeguate di sicurezza informatica relative a copie/repliche digitali dei repertori aziendali legati al trattamento dei dati personali, l'Azienda ha centralizzato prassi automatiche e semi-manuali su un apparato NAS. Questo dispositivo dotato di sistema embedded Linix con IDE proprietario centralizza la gestione dello stoccaggio di LOG, alberature di cartelle di rete, di repliche di Database oltre che di immagini di backup dei sistemi operativi di Servers critici.

Ai fini delle misure di sicurezza di livello "adeguato" ad uno standard di disaster recovery, tutto il patrimonio delle copie INTRALAN sono replicate in storicizzazioni CLOUD.

La replica viene svolta con protocolli di trasmissione HTTPS e SFTP/FTPS di contenuti che sono anche cifrati prima (o durante) il trasferimento di stoccaggio *alter sito*.

Sicurezza ICT per ACL e accountability

Ai Per la Gestione globale degli accessi alle risorse di LAN, le misure di cui sopra in merito alla segmentazione toponomastica della architettura di rete, sono state armonizzate con quelle logche di gestione della paternità e tipologia delle Access Control Lists (ACLs).

A questo scopo la centralizzazione delle ACLs è stata assicurata dalla stazione Server di LAN grazie al servizio MS Active Directory (MS-AD). Questa scelta ha dato modo di:

- ***assegnare (accountability) a livello personale discrete porzioni di visibilità delle alberature delle cartelle di LAN (sincronicità funzionale su NAS)***
- ***discriminare i processi di manutenzione e controllo sistemistici (ADS) dai SS.AA.***
- ***separare i volumi di rete condivisi in LAN rispetto alle aree di script/bash/batches per le prassi di manutenzione e procedure/servizi di LOG / Backup***
- ***integrare le ACLs degli apparati di Firewall e NAS a livello di Gateway.***

Sicurezza dei Soggetti Autorizzati con accesso a Dati e Sistemi

La sicurezza informatica deve essere assicurata sia a livello HW-SW che a livello di Consapevolezza dei SSAA. Oltre al Piano di Formazione verbalizzato e aggiornato dai ruoli di Responsabilità delegati dal TDT, gli operatori che agiscono all'interno del perimetro dei Sistemi Informativi aziendali, sono costantemente supervizionati anche nella navigazione Internet

Tutte le postazioni LAN hanno e/o implementano:

- ***Sistema di trasmissione LOG di accesso alla postazione***
- ***Controllo di instradamento e traduzione porta di servizi da e per esterno LAN***
- ***Constrollo di accesso riservato a risorse LAN personalizzate in base al mansionamento e al ruolo di attività per i trattamenti di cui in nomina/designazione***
- ***Traffic Community Monitor SW (Es. Ghostery, WOT e uBlock) ad ogni livello di istanza di navigazione internet (sia Chrome, Safari, Firefox, Opera e ovviamente MS-Edge)***
- ***SW Host resilience Anti-ramsonware a livello di client***