DOI: 10.26314/GARR-Conf24-proceedings-17

Sovranità digitale: DPO, protezione dei dati e cybersicurezza

Lucio Badiali

INGV Istituto Nazionale di Geofisica e Vulcanologia

Abstract. La sovranità digitale ha tra le sue iniziali priorità la difesa del perimetro cibernetico al cui interno si trova anche il dato personale, vero asset strategico di ogni pubblica amministrazione (PA) l'insieme delle quali formano i punti di contatto tra cittadino e Stato. La protezione del dato richiede diverse abilità specialistiche distribuite spesso tra più figure

Keywords. RDT, Referente per la cybersicurezza, CIO, DPO, PA

Introduzione

Il DPO non può ridursi a essere un esperto di sterile normativa, perché la data protection è una prassi, e deve iniziare a palesarsi come una delle voci che analizza il rischio e che collabora con gli altri attori implicati nella difesa degli asset. E' un ruolo sì ausiliario ma che può supportare il passaggio alla tanto attesa resilienza del perimetro cyber della PA.

1. Sovranità digitale: DPO, protezione dei dati e cybersicurezza

Il ruolo del DPO in un soggetto pubblico, sia un ente di ricerca nazionale che una infrastruttura di ricerca (IR) europea, è chiaramente simile. Le sfumature emergono nell'interazione con i vari delegati e gli uffici distribuiti nel territorio dell'Unione, e nei paesi che collaborano pur essendone fuori. Nel caso di EPOS l'interazione è con un policy team in cui nell'ultimo periodo, prima delle periodiche rotazioni, il responsabile per le politiche di sicurezza ICT e l'esperto legale erano in UK in quanto tra i partecipanti compare il BGS. Abbiamo, pertanto, vissuto anche noi il pre- e il post- Brexit nella data protection. La sede legale di EPOS è in Italia per cui vale, oltre il fondamentale GDPR, la normativa italiana che va condivisa con i partner stranieri per determinare le best practice in materia.
Nonostante la complessità di una IR, gli asset e i processi sono limitati e ben distinguibili rispetto alla realtà nazionale che deve scontare, almeno nel nostro caso, frequenti riorganizzazioni con spostamenti e cambi di mansione del personale.
L'attività privacy non si esprime solo nella verifica degli agreement e nelle relative informative, nel registro trattamenti, lato più epidermico e visibile, bensì nel lavoro di pianificazione che ha nei due termini la ragione della sua azione: protezione e dati personali.
I dati sono l'asset fondamentale, il vero patrimonio dell'ente, con un valore difficilmente stimabile e che è sottoposto a potenziali aggressioni per essere sottratto (data leak e data breach), modificato o cancellato trovandosi cosi a non garantirne la celebre triade alla base

Conferenza GARR 2024 - Navigare la complessità - Selected Papers
Brescia 29-31 maggio 2024 - ISBN: 978-88-946629-3-1

della sicurezza delle informazioni: riservatezza, integrità e disponibilità.
Una infrastruttura di rete ed i suoi servizi possono essere messi fuori uso temporaneamente. La protezione del dato è una azione da pianificare su più dimensioni e da realizzare ben prima dell'evento sinistro, infatti il dato una volta esfiltrato è perso per sempre e diventa patrimonio di altri, mentre i servizi di rete alla fine, comunque, tornano su.
Il DPO oggi non è solo l'esperto della normativa di settore, ma deve capire il pensiero ed il modo di operare dell'esperto di sicurezza informatica, deve cioè necessariamente muoversi agevolmente in entrambi i temi e legarli con una approfondita conoscenza dell'analisi del rischio. Quando il dato è compromesso e si attiva un confronto con l'Autorità garante, e non solo quella, non serve parlare di leggi e norme, perché la domanda è solo una e richiama il principio di accountability: "cosa avete fatto prima dell'evento?", "Come avete analizzato lo stato del vostro sistema e messo ragionevolmente in sicurezza gli asset?". In quel "ragionevolmente" si gioca la partita. Un DPO che assecondi le scelte tecniche di sicurezza, perché non in grado di comprenderle e non interagisce in maniera dialettica con gli specialisti, non fornisce alcun valore aggiunto. Né può esercitare il suo ruolo sul tema assicurandosi, passivamente, con i vari specialisti che i dati siano ben protetti. Sarebbe come chiedere all'oste: "come è il vino?". E la sua difesa si fa debole se non inutile.
In tema di sicurezza informatica e cybersicurezza, soprattutto nel nostro Paese, si tende ad allungare a dismisura la catena di comando. In questo momento, vigente la NIS, siamo in attesa dell'attuazione in autunno della direttiva NIS2, ma si è sentito il bisogno di anticipare con un "decreto cybersicurezza" che inserisce una nuova figura quella del referente per la cyber sicurezza, fondamentale elemento per difendere le pubbliche amministrazioni dalle minacce digitali e assicurare la protezione dei dati sensibili, nonché la continuità delle operazioni. Come se prima non ci fosse stata una simile esigenza. Tanto per ricordare, un inciso che vale come esempio, anche con la NIS un settore strategico come la sanità, è stato ritenuto una filiera strategica che rientrava completamente nell'ambito di applicazione della disciplina di cybersicurezza, ma nonostante questo, si sono vissuti drammatici attacchi alle strutture sanitarie con servizi in down completo ed esfiltrazioni di dati personali particolari (e parliamo di casi noti finiti spesso in cronaca, e alcuni sono casi ancora aperti). Se nel recente passato gli effetti sono stati negativamente impattanti, forse il problema potrebbe trovarsi negli investimenti, nelle scelte, o proprio nella catena di controllo e comando. Stratificare e complicare la normativa è una pratica nazionale tipica e, quando non si riesce a gestire la complessità, purtroppo, se ne si aumenta il livello. A causa delle incomprimibilità dei bilanci, in genere le PP.AA. devono spesso operare senza variazioni, senza maggiori spese, tanto che la figura del referente può essere il responsabile della transizione digitale. Diversi sono gli specialisti con cui il DPO si confronta per questo tema. Il referente cyber (potremmo vederci una sorta di CISO della PA), il cui testo di riferimento è il succitato recente d.d.l. cybersicurezza (insieme alle varie NIS) ha il suo punto di contatto in ACN, e il responsabile della transizione digitale (RTD), il cui riferimento normativo principale è il CAD e che ha il suo contatto in AgID, sono figure che vengono create per facilitare cambiamenti verso un futuro di resilienza, anchee cibernetica. Da non dimenticare che esiste anche il responsabile informatico, il CIO, equivalente

ormai al sergente in trincea che lotta per avere personale e finanziamenti, ma oltre ai vari direttori ha due nuovi ufficiali in capo. Allo stato attuale, la gestione delle strategie e della prassi della sicurezza ICT è assimilata a un vettore a tre figure componenti (RTD, CISO, CIO) ma che per la situazione della PA italiana, si può ridurre a un vettore che perde, per motivi di finanziamento, una ad una le sue dimensioni fino collassare sulla stessa unica componente personale. Generando un paradosso in cui chi deve definire le strategie è anche quello che le applica, cosa che genera sottili conflitti di interessi e identifica controllore e controllato. Una catena di comando in linea di principio forse troppo lunga ma che si può ridurre ad una sola persona con cappelli diversi da indossare in contesti diversi. E in un attimo, siamo di nuovo ai tempi in cui esisteva il solo responsabile IT.
Tornando alla situazione internazionale molto più elastica in termini di operatività e dove è anche più facile reperire risorse umane preparate, esiste una difficoltà nello spiegare la versione sartoriale in cui produciamo normative e berretti da indossare secondo chi si incontra, e allunghiamo i riferimenti autoritativi con cui interagire. Come ben evidenziato da quasi tutti i relatori durante la Conferenza del GARR 2024, un problema sentito risiede proprio nel reperire il personale preparato, spesso anche formato da noi, che decida poi di restare nell'ente di appartenenza.

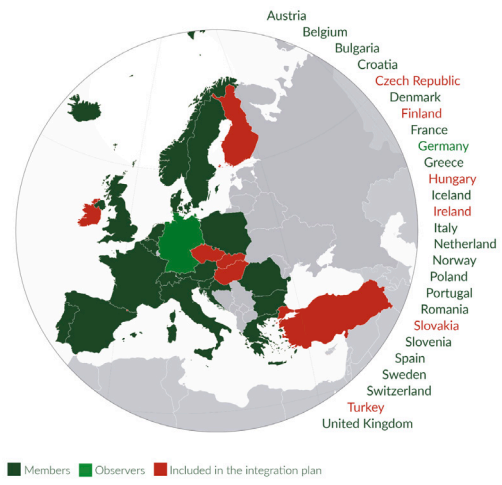

Fig. 1
EPOS European Research Infrastructure Consortium (ERIC)

2. Conclusioni

In questo periodo la figura del DPO può rinnovarsi per diventare forse quella che era stata immaginata durante la genesi del GDPR. Grazie alle spinte esterne, dovute pure alla sfida della IA e alle sempre più originali minacce cyber, il suo ruolo si ridefinisce. Per esempio, si nota che a ridosso del decreto cyber è stato accolto un ordine del giorno che impegna il governo a specificare che le pubbliche amministrazioni, almeno quelle centrali, per quanto riguarda la cybersicurezza, debbano coinvolgere il responsabile per la transizione digitale e il responsabile della protezione dei dati. Se si riesce ad usare questa opzione anche noi, se il DPO riesce a parlare la lingua degli esperti in materia cyber senza usare interpreti e traduttori avremo una risorsa in più dove di risorse necessarie non se ne trovano molte. E

questo ha senso perché GDPR e normative cyber hanno uno stesso obiettivo, far adottare misure tecniche e organizzative adeguate, per raggiungere il più elevato livello di sicurezza compatibile con il periodo presente, guardando al futuro.

Autore

Lucio Badiali lucio.badiali@ingv.it
DPO di INGV e EPOS.
Laurea in Fisica, specializzazione in cibernetica, Dottorato in Metodologie Fisiche Innovative per la Ricerca Ambientale. Laurea in Scienze politiche, Master Universitario di 2° livello (CMU-2) in Scienze Giuridiche Diritto della Protezione dei Dati Personali.